MATHEMATICS OF COMPUTATION
Volume 69, Number 231, Pages 1245–1266
S 0025-5718(99)01136-9
Article electronically published on March 11, 1999

VORONOI'S ALGORITHM IN PURELY CUBIC CONGRUENCE FUNCTION FIELDS OF UNIT RANK 1

R. SCHEIDLER AND A. STEIN

ABSTRACT. The first part of this paper classifies all purely cubic function fields over a finite field of characteristic not equal to 3. In the remainder, we describe a method for computing the fundamental unit and regulator of a purely cubic congruence function field of unit rank 1 and characteristic at least 5. The technique is based on Voronoi's algorithm for generating a chain of successive minima in a multiplicative cubic lattice, which is used for calculating the fundamental unit and regulator of a purely cubic number field.

1. INTRODUCTION

In 1896, Voronoi [17] presented his algorithm for computing a system of fundamental units of a cubic number field. His technique, described in terms of binary forms, was later restated in the language of multiplicative lattices — we use the term fractional ideal — by Delone and Faddeev [7]. The method is based on computing chains of successive minima in the maximal order $\mathcal{O}$ of the field K. An implementation in purely cubic fields was given by Williams et al. [20], and improvements based on Shanks' idea of the infrastructure of the set of reduced principal integral ideals in K [13] were given in [21] and [19]. In the case of a real quadratic number field, Voronoi's method reduces to the well-known continued fraction algorithm for quadratic irrationalities given in [22] and [19]. Buchmann [1] generalized Voronoi's ideas to arbitrary number fields of unit rank 1 and 2. He extended his ideas to number fields of any rank [3, 4] and subsequently incorporated the infrastructure concept in [6] and [5].

In a real algebraic number field K of unit rank one (i.e. a real quadratic field or a complex cubic field), a chain of successive minima in $\mathcal{O}$ is generated by starting with $\theta_1 = 1$ and computing adjacent minima $\theta_1 < \theta_2 < \theta_3 < \cdots$ in $\mathcal{O}$. Here $\theta_{n+1} = \mu_n \theta_n$, where μ_n is the minimum adjacent to 1 in the reduced fractional principal ideal $\mathfrak{a}_n = (1/\theta_n)$ $(n \in \mathbb{N})$. Since the number of reduced fractional ideals in K is at most $O(\sqrt{\Delta})$, where Δ is the discriminant of K (see [1]), and is thus finite, one must obtain a reduced fractional ideal $\mathfrak{a}_{n+1}$ so that $\mathfrak{a}_{n+1} = \mathfrak{a}_1 = \mathcal{O}$ after at most $O(\sqrt{\Delta})$ steps, in which case $\theta_{n+1} = \epsilon$ is the fundamental unit of K. Thus, at the heart of Voronoi's algorithm lies the problem of computing the minimum

Received by the editor March 31, 1998 and, in revised form, August 14, 1998.
1991 *Mathematics Subject Classification.* Primary 11R16, 11R27; Secondary 11R58, 11-04.
Key words and phrases. Purely cubic function field, Voronoi's algorithm, minimum, reduced ideal, fundamental unit, regulator.
The first author was supported by NSF grant DMS-9631647.

adjacent to 1 in a reduced fractional ideal. Specific implementations describing how to accomplish this, together with numerical examples, were given for the real quadratic case in [22], the purely cubic case in [20], and the totally complex quartic case in [2].

Stein [14], see also [15], adjusted the continued fraction algorithm of [22] to compute the fundamental unit and regulator of a real quadratic congruence function field. He discovered that the reduced principal integral ideals of such fields also obey Shanks' infrastructure concept. This successful adaptation of number field algebra and arithmetic to function fields motivated the authors to design and implement a version of Voronoi's algorithm for purely cubic congruence function fields of characteristic at least 5. Fittingly, our work began in 1996, the centennial year of the publication of Voronoi's original work. Improvements similar to those given in [21] incorporating an analogous infrastructure can likely be added and will be investigated in the future.

We should point out that Mang [10] was the first to compute systems of fundamental units of purely cubic congruence function fields of both unit rank 1 and 2. His technique is based on the Pohst-Zassenhaus method used for number fields [11, Chapter 5]. First, a succession of elements of decreasing norm in the maximal order is generated until a set of independent units is found whose cardinality is equal to the unit rank. Then the fundamental units are computed by essentially "extracting roots" from the independent units. By Mang's own admission, his technique is slow and is infeasible for even modest degrees and sizes of the constant field. An example over the ground field $\mathbb{F}_5$ with a generating polynomial of degree 6 that took 273 seconds of CPU time on a Siemens mainframe using Mang's method required only 0.04 seconds on a Silicon Graphics Challenge workstation with our algorithm.

In adapting the ideas of [20] to purely cubic congruence function fields, we encountered many similarities between the number field and the function field situations. However, there are also significant differences between the two settings. In the function field setting, the role of the absolute value is taken on by a discrete (i.e. non-archimedian) valuation which frequently does not satisfy the inequalities and bounds used in the number field case. In addition, many of the number field results are derived from geometric concepts, such as Minkowski's lattice point theorem or facts about the minimum of a certain binary quadratic form over the rational integers. In function fields, this geometry is lost, and the corresponding results need to be derived arithmetically. We will identify further differences between the two environments throughout the paper. In short, while many of our conclusions are similar to results in the number field framework, the way by which we arrive at these facts is largely new and quite different from the derivations in [21] and [19].

2. Classification of purely cubic congruence function fields

A general introduction to congruence function fields can be found in [8]. The purely cubic case is discussed in [10], see also p. 196 of [16]. The identities involving the unit group, regulator, and the ideal and divisor class numbers are given in [12] and [18].

Let $k = \mathbb{F}_q$ be a finite field of order q whose characteristic is not 3 and let K be a cubic extension of the rational function field over k in one variable. If $t \in K$ is transcendental over k, we denote by $k(t)$ the rational function field and by $k[t]$ the ring of polynomials over k in the variable t. K is a *purely cubic congruence function*

field over the *field of constants* k if there exists a polynomial $D = D(t) \in k[t]$ which is not a cube in $k[t]$ such that $K = k(t, \rho)$, where $\rho \in K$ and $\rho^3 = D$, i.e. ρ is a zero in K of the polynomial $F(t, y) = y^3 - D(t) \in k[t, y]$. Henceforth, we assume D to be cubefree in $k[t]$ and write $D = GH^2$, where $G, H \in k[t]$ are relatively prime and squarefree; then G and H are unique up to a constant factor. The algebraic closure $\mathcal{O} = \overline{k[t]}$ of $k[t]$ in K is a $k[t]$-module of rank 3 with a *(t-)integral basis* $\{1, \rho = \sqrt[3]{GH^2}, \omega = \rho^2/H = \sqrt[3]{G^2H}\}$. Its unit group $\mathcal{O}^*$ is the *(t-)unit group* of K. $\mathcal{O}^* = k^* \times \mathcal{E}$, where $\mathcal{E}$ is either trivial or the product of finitely many infinite cyclic groups. In the latter case, an independent set of generators of $\mathcal{E}$ is a system of *fundamental (t-)units* and the rank of $\mathcal{E}$ is the *(t-)unit rank* of K. The units in k^* are the *trivial units*.

Let $\mathfrak{p}_\infty$ be the infinite place of $k(t)$ corresponding to the negative degree valuation ν_∞ on $k(t)$. Then the completion $k(t)_{\mathfrak{p}_\infty}$ of $k(t)$ with respect to $\mathfrak{p}_\infty$ is the field $k((1/t))$ of Puiseux series $\sum_{i=m}^{\infty} a_i/t^i$ ($m \in \mathbb{Z}, a_i \in k$ for $i \geq m$) over k. Denote by r the number of distinct extensions of the valuation ν_∞ onto K. Then r is equal to the number of irreducible factors of $F(t, y) = y^3 - D$ in $k((1/t))[y]$, and the unit rank of K is $r - 1$.

Let $\mathcal{D}$ be the *divisor group* of K over k, $\mathcal{D}^0$ the subgroup of $\mathcal{D}$ of *divisors of degree 0*, and $\mathcal{P} \leq \mathcal{D}^0$ the group of *principal divisors* of $K|k$. The *divisor class group (of degree 0)* of $K|k$ is the factor group $\mathcal{C}^0 = \mathcal{D}^0/\mathcal{P}$; its order $h = \#\mathcal{C}^0$ is the *divisor class number* of K. In analogy to $\mathcal{D}$ and $\mathcal{D}^0$, denote by $\mathcal{U}$ the subgroup of $\mathcal{D}$ generated by the infinite places (with respect to t) of K and by $\mathcal{U}^0$ the subgroup of divisors in $\mathcal{U}$ of degree 0. Then $\mathcal{E}$ is isomorphic to $\mathcal{P} \cap \mathcal{U}^0$. The *($t$-)regulator* of K is the index $R = [\mathcal{U}^0 : \mathcal{P} \cap \mathcal{U}^0]$. If $\mathcal{I}$ is the group of *fractional (t-)ideals* of K and $\mathcal{H}$ the subgroup of fractional *principal (t-)ideals* of K, then the *(t-)ideal class group* of K is $\mathcal{C} = \mathcal{I}/\mathcal{H}$; its order $h' = \#\mathcal{C}$ is the *(t-)ideal class number* of K. Both h and h' are finite and are related through the identity

$$h = \frac{R}{f} h', \tag{2.1}$$

where f is the greatest common divisor of the degrees of all the infinite places of K.

Let g denote the *genus* of K and let $\deg(D)$ and $\operatorname{sgn}(D)$ denote the degree and the leading coefficient of D, respectively. The following theorem classifies all purely cubic congruence function fields. Note that $k = \mathbb{F}_q$ contains a primitive cube root of unity if and only if $q \equiv 1 (\mathrm{mod}\ 3)$.

Theorem 2.1 (Classification of Purely Cubic Congruence Function Fields). *Let $K = k(t, \rho)$ be a purely cubic congruence function field over a finite field k of characteristic $\neq 3$, where $\rho^3 = D = GH^2 \in k[t]$ with G, H squarefree and $\gcd(G, H) = 1$.*

1. *Suppose $\deg(D) \not\equiv 0 (\mathrm{mod}\ 3)$. Then $\mathfrak{p}_\infty$ is totally ramified in K and $F(t, y)$ is irreducible over $k((1/t))$, so $\rho \notin k((1/t))$. Hence $r = 1$, $O^* = k^*$, $R = 1$, and $h = h'$. Also $g = \deg(GH) - 1$.*
2. *Suppose $\deg(D) \equiv 0 (\mathrm{mod}\ 3)$. Then $\mathfrak{p}_\infty$ is unramified in K and $g = \deg(GH) - 2$. There are two cases:*
   (a) *Suppose $\operatorname{sgn}(D)$ is not a cube in k. Then $\mathfrak{p}_\infty$ is inert in K and $F(t, y)$ is irreducible over K, so again $\rho \notin k((1/t))$, $r = 1$, $O^* = k^*$, $R = 1$, and $h = h'/3$.*
   (b) *Suppose $\operatorname{sgn}(D)$ is a cube in k. Then $\rho \in k((1/t))$ and the unit group is nontrivial. Here, we have two further subcases:*

(i) *If* $q \equiv -1 \pmod 3$, *then* $\mathfrak{p}_\infty = \mathfrak{P}_1\mathfrak{P}_2$ *in* K *with* $f_{\mathfrak{P}_1} = 1$ *and* $f_{\mathfrak{P}_2} = 2$, *where* $f_{\mathfrak{P}_1}$ *and* $f_{\mathfrak{P}_2}$ *are the degrees of the places* $\mathfrak{P}_1$ *and* $\mathfrak{P}_2$, *respectively.* $F(t,y)$ *splits over* $k((1/t))$ *as*

$$F(t,y) = (y-\rho)(y^2+\rho y+\rho^2),$$

where $y^2+\rho y+\rho^2$ *is irreducible over* $k((1/t))$. *Here,* $r = 2$, $O^* = k^* \times \langle \epsilon \rangle$ *with a fundamental unit* $\epsilon \in \mathcal{O}^*$, $R = |\nu_2(\epsilon)| = |\nu_1(\epsilon)|/2$, *and* $h = Rh'$, *where* ν_1 *and* ν_2 *are the normalized valuations on* K *corresponding to the places* $\mathfrak{P}_1$ *and* $\mathfrak{P}_2$, *respectively.*

(ii) *If* $q \equiv 1 \pmod 3$, *then* $\mathfrak{p}_\infty = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ *in* K, *where* $f_{\mathfrak{P}_1} = f_{\mathfrak{P}_2} = f_{\mathfrak{P}_3} = 1$. $F(t,y)$ *splits over* $k((1/t))$ *as*

$$F(t,y) = (y-\rho)(y-u\rho)(y-u^2\rho),$$

where $u \in k$ *is a primitive cube root of unity. Hence* $r = 3$, $O^* = k^* \times \langle \epsilon_1, \epsilon_2 \rangle$ *with fundamental unit* $\epsilon_1, \epsilon_2 \in \mathcal{O}^*$,

$$R = \left| \det \begin{pmatrix} \nu_1(\epsilon_1) & \nu_2(\epsilon_1) \\ \nu_1(\epsilon_2) & \nu_2(\epsilon_2) \end{pmatrix} \right|,$$

and $h = Rh'$, *where* ν_1 *and* ν_2 *are the normalized valuations on* K *corresponding to the places* $\mathfrak{P}_1$ *and* $\mathfrak{P}_2$, *respectively. In addition, this is the only case where* K *is a normal extension of* $k(t)$ *whose Galois group is cyclic of order 3.*

Proof. Let $d = \gcd(3, \deg(D))$. Then by [16, Proposition VI.3.1, p. 196], $g = \deg(GH) - 1 - (d-1)/2$, so $g = \deg(GH) - 1$ if $\deg(D) \not\equiv 0 \pmod 3$ and $g = \deg(GH) - 2$ if $\deg(D) \equiv 0 \pmod 3$.

We have $\mathfrak{p}_\infty = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}$ where $\sum_{i=1}^r e_i f_i = [K : k(t)] = 3$ and f_i is the degree of the place $\mathfrak{P}_i$ for $i = 1, 2, \dots, r$. Then $f = \gcd(f_1, f_2, \dots, f_r)$. By the same theorem in [16] cited above, all infinite places have the same ramification index $e = 3/d$. Thus, if $\deg(D) \not\equiv 0 \pmod 3$, then $e = 3$, so $r = 1$, and $\mathfrak{p}_\infty = \mathfrak{P}^3$ in K, where the degree of $\mathfrak{P}$ is $f_{\mathfrak{P}} = 1$. Hence $\mathcal{O}^* = k^*$. Since $\mathcal{U}^0$ is trivial, $R = 1$. Since $f = 1$, by (2.1) $h = h'$.

Suppose now that $\deg(D) \equiv 0 \pmod 3$. Then $e = 1$, so $\mathfrak{p}_\infty$ is unramified. In this case, we obtain the unit rank from [10, Theorem 3.6, p. 77]. If $\operatorname{sgn}(D)$ is not a cube in k, then again $r = 1$. Thus, $\mathfrak{p}_\infty = \mathfrak{P}$ in K, where $f_{\mathfrak{P}} = 3$, so, as before, $\mathcal{O}^* = k^*$, $\mathcal{U}^0$ is trivial, and $R = 1$. Since $f = 3$, by (2.1) $h = h'/3$.

Now assume that $\operatorname{sgn}(D)$ is a cube in k. If $q \equiv -1 \pmod 3$, then k does not contain a primitive cube root of unity, so $r = 2$ [10]. Hence $\mathfrak{p}_\infty = \mathfrak{P}_1\mathfrak{P}_2$ with respective degrees $f_1 = 1$, $f_2 = 2$. Then $\mathcal{U} = \langle \mathfrak{P}_1, \mathfrak{P}_2 \rangle$ and

$$\mathcal{U}^0 = \langle \mathfrak{P}_1^{\alpha_1}\mathfrak{P}_2^{\alpha_2} \mid \alpha_1, \alpha_2 \in \mathbb{Z},\ \alpha_1 + 2\alpha_2 = 0 \rangle = \langle \mathfrak{P}_1^{-2}\mathfrak{P}_2 \rangle.$$

Also $\mathcal{P} \cap \mathcal{U}^0 = \langle (\epsilon) \rangle$, where (ϵ) is the principal divisor corresponding to the fundamental unit ϵ. Denoting by f_ϵ the degree of the divisor (ϵ), we have $0 = f_\epsilon = \nu_1(\epsilon) + 2\nu_2(\epsilon)$, so $(\epsilon) = (\mathfrak{P}_1^{-2}\mathfrak{P}_2)^{\nu_2(\epsilon)}$. Thus, $R = |\nu_2(\epsilon)| = |\nu_1(\epsilon)|/2$, and since $f = 1$, by (2.1) $h = Rh'$.

If $q \equiv 1 \pmod 3$, then k contains primitive cube roots of unity, so K is a Kummer extension of $k(t)$ of degree 3 and is hence normal with Galois group $\mathbb{Z}/3\mathbb{Z}$. In this case, [10] yields $r = 3$, so $\mathfrak{p}_\infty = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ with respective degrees $f_1 = f_2 = f_3 = 1$. Then $\mathcal{U} = \langle \mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3 \rangle$, $\mathcal{U}^0 = \langle \mathfrak{P}_1^{\alpha_1}\mathfrak{P}_2^{\alpha_2}\mathfrak{P}_3^{\alpha_3} \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z},\ \alpha_1 + \alpha_2 + \alpha_3 = 0 \rangle = \langle \mathfrak{P}_1\mathfrak{P}_3^{-1}\mathfrak{P}_2\mathfrak{P}_3^{-1} \rangle$. Also $\mathcal{P} \cap \mathcal{U}^0 = \langle (\epsilon_1), (\epsilon_2) \rangle$. If we again denote the degree of

(ϵ_i) by f_{ϵ_i}, then for $i = 1, 2$ we have $0 = f_{\epsilon_i} = \nu_1(\epsilon_i) + \nu_2(\epsilon_i) + \nu_3(\epsilon_i)$, so for the principal divisors (ϵ_1) and (ϵ_2) corresponding to the two fundamental units ϵ_1 and ϵ_2, respectively, $(\epsilon_i) = (\mathfrak{P}_1\mathfrak{P}_3^{-1})^{\nu_1(\epsilon_i)}(\mathfrak{P}_2\mathfrak{P}_3^{-1})^{\nu_2(\epsilon_i)}$. Thus,

$$R = \left|\det \begin{pmatrix} \nu_1(\epsilon_1) & \nu_2(\epsilon_2) \\ \nu_1(\epsilon_2) & \nu_2(\epsilon_2) \end{pmatrix}\right|,$$

and since $f = 1$, by (2.1) $h = Rh'$. □

Note that this classification differs from that of purely cubic number fields in that purely cubic number fields are complex cubic fields and thus always have unit rank 1.

Henceforth, we assume the unit rank 1 case as described in part 2 (b) (i) in the theorem above, i.e. $\deg(D)$ is divisible by 3, $\operatorname{sgn}(D)$ is a cube in k^*, and $q \equiv -1 (\mathrm{mod}\ 3)$, so q is an odd power of a prime $p \equiv -1 (\mathrm{mod}\ 3)$. Let ι be a primitive cube root of unity in some algebraic closure of k, so $\iota^2 + \iota + 1 = 0$ and $\iota^3 = 1$. Then $K(\iota)$ is a quadratic extension of K whose nontrivial K-automorphism is "complex conjugation" $\bar{} : K(\iota) \to K(\iota)$ via $\bar{\iota} = \iota^{-1}$. $K(\iota) = k(\iota, t, \rho)$ is a cyclic extension of $k(\iota, t)$ of degree 3 for which we fix the $k(\iota, t)$-automorphism $' : K(\iota) \to K(\iota)$ via $\rho' = \iota\rho$. Write γ'' for $(\gamma')'$ $(\gamma \in K(\iota))$. Note that $\overline{\alpha'} = \alpha''$ for $\alpha \in K$. For $\alpha \in K$, the *norm of* α *(over* $k(t)$*)* is $N(\alpha) = \alpha\alpha'\alpha''$. We have $N(\alpha) \in k(t)$, and if $\alpha \in \mathcal{O}$, then $N(\alpha) \in k[t]$. Also, $\alpha \in \mathcal{O}$ is a unit if and only if $N(\alpha) \in k^*$.

As before, let ν_1 and ν_2 be the two normalized valuations on K corresponding to the two infinite places $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of K, respectively. Since $f_{\mathfrak{P}_1} = 1$, the completion $K_{\mathfrak{P}_1}$ of K with respect to $\mathfrak{P}_1$ is isomorphic to $k(t)_{\mathfrak{p}_\infty} = k((1/t))$. For $\alpha = \sum_{i=m}^{\infty} a_i/t^i \in k((1/t))$ $(m \in \mathbb{Z}, a_i \in k$ for $i \geq m, a_m \neq 0)$, we define

$$\begin{aligned} \deg(\alpha) &= -m = -\nu_1(\alpha), \\ |\alpha| &= q^{-m} = q^{\deg(\alpha)}, \\ \operatorname{sgn}(\alpha) &= a_m, \\ \lfloor \alpha \rfloor &= \sum_{i=m}^{0} \frac{a_i}{t^i}. \end{aligned}$$

We also set $\deg(0) = -\infty$ and $\lfloor 0 \rfloor = 0$. Note that $\lfloor \alpha \rfloor \in k[t]$ and $|\alpha - \lfloor \alpha \rfloor| < 1$.

Since the only fundamental units (up to multiples by trivial units) are ϵ and ϵ^{-1}, we may assume without loss of generality that $\deg(\epsilon) > 0$. Then for the regulator we have $R = \deg(\epsilon)/2$.

The valuation ν_1 on $k((1/t))$ has a unique extension to $k((1/t))(\iota)$ (which we will also denote by ν_1) defined as follows: for $\phi \in k((1/t))(\iota)$, we have $\nu_1(\phi) = \nu_1(\phi\bar{\phi})/2$. Then we can define

$$\begin{aligned} \deg(\phi) &= \frac{1}{2}\deg(\phi\bar{\phi}), \\ |\phi| &= \sqrt{|\phi\bar{\phi}|} = q^{\frac{1}{2}\deg(\phi\bar{\phi})} = q^{\deg(\phi)}. \end{aligned}$$

3. Ideals

We summarize without proof some basics about ideals; the terminology, notation, and proofs are completely analogous to those for number fields.

A subset $\mathfrak{a}$ of $\mathcal{O}$ is an *integral ($\mathcal{O}$-)ideal* if for all $\alpha, \beta \in \mathfrak{a}$ and $\theta \in \mathcal{O}$ we have $\alpha + \beta \in \mathfrak{a}$ and $\theta\alpha \in \mathfrak{a}$. A subset $\mathfrak{a}$ of K is a *fractional ($\mathcal{O}$-)ideal* if there exists a nonzero $d \in k[t]$ such that $d\mathfrak{a}$ is an integral ideal of $\mathcal{O}$. If $\alpha_1, \alpha_2, \ldots, \alpha_l \in K$, then the set $\mathfrak{a} = \{\theta_1\alpha_1 + \theta_2\alpha_2 + \ldots + \alpha_l\theta_l \mid \theta_i \in \mathcal{O} \text{ for } 1 \leq i \leq l\}$ is a fractional ideal with *generators* $\alpha_1, \alpha_2, \ldots, \alpha_l$; write $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_l)$. If $\alpha_1, \alpha_2, \ldots, \alpha_l \in \mathcal{O}$, then $\mathfrak{a}$ is an integral ideal. A fractional or integral ideal $\mathfrak{a}$ is *principal* if $\mathfrak{a} = (\alpha)$ has one generator.

Henceforth, we assume all ideals (fractional and integral) to be nonzero, i.e. the term "ideal" will be synonymous with "nonzero ideal". Then a multiplication is defined on the set of fractional ideals as follows. If $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_r)$ and $\mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_s)$ are fractional ideals, then the fractional ideal $\mathfrak{ab}$ is defined to be the fractional ideal generated by $\alpha_i\beta_j$ $(1 \leq i \leq r, 1 \leq j \leq s)$. For integral ideals $\mathfrak{a}$, $\mathfrak{b}$, we say that $\mathfrak{a}$ *divides* $\mathfrak{b}$ if there exists an (integral) ideal $\mathfrak{c}$ such that $\mathfrak{ac} = \mathfrak{b}$. We write $\mathfrak{a} \mid \mathfrak{b}$. Then $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$. An ideal $\mathfrak{a}$ is *primitive* if it has no nontrivial polynomial divisors, that is, if $f \in k[t], f \neq 0$ with $(f) \mid \mathfrak{a}$, then $f \in k^*$.

Proposition 3.1. *Every integral ideal of $\mathcal{O}$ is a $k[t]$-module of rank 3. Specifically, every integral ideal $\mathfrak{a}$ has a $k[t]$-basis of the form $\{l, \mu, \nu\}$ where*

$$\begin{aligned} l &\in k[t] \text{ is monic,} \\ \mu &= m_0 + m_1\rho, \\ \nu &= n_0 + n_1\rho + n_2\omega, \end{aligned} \tag{3.1}$$

with $m_0, m_1, n_0, n_1, n_2 \in k[t]$ and $m_1n_2 \neq 0$.

Here, l is unique and is the monic polynomial of minimal degree in $\mathfrak{a}$; write $l = L(\mathfrak{a})$. Every polynomial in $\mathfrak{a} \cap k[t]$ is a multiple of $L(\mathfrak{a})$.

Corollary 3.2. *Every fractional ideal of $\mathcal{O}$ is a $k[t]$-module of rank 3. More specifically, every fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ that contains 1 has a $k[t]$-basis of the form $\{1, \mu, \nu\}$ where*

$$\begin{aligned} \mu &= (m_0 + m_1\rho)/d, \\ \nu &= (n_0 + n_1\rho + n_2\omega)/d, \end{aligned} \tag{3.2}$$

with $m_0, m_1, n_0, n_1, n_2, d \in k[t]$ and $dm_1n_2 \neq 0$. If $\gcd(m_0, m_1, n_0, n_1, n_2, d) = 1$, then $d\mathfrak{a}$ is a primitive integral ideal with $L(d\mathfrak{a}) = \operatorname{sgn}(d)^{-1}d$.

If $\{\lambda, \mu, \nu\}$ is a $k[t]$-basis of a fractional or integral ideal $\mathfrak{a}$ of $\mathcal{O}$, write $\mathfrak{a} = [\lambda, \mu, \nu]$.

Proposition 3.3. *Let $\mathfrak{a} = [\lambda_1, \mu_1, \nu_1]$, $\mathfrak{b} = [\lambda_2, \mu_2, \nu_2]$ be fractional or integral ideals. Then $\mathfrak{a} = \mathfrak{b}$ if and only if there exists $T \in Gl_3(k[t])$ (i.e. $\det(T) \in k^*$) such that*

$$\begin{pmatrix} \lambda_1 \\ \mu_1 \\ \nu_1 \end{pmatrix} = T \begin{pmatrix} \lambda_2 \\ \mu_2 \\ \nu_2 \end{pmatrix}.$$

The *(t-)norm* of a fractional ideal $\mathfrak{a} = [\lambda, \mu, \nu]$ is $N(\mathfrak{a}) = \operatorname{sgn}(\det(T))^{-1} \det(T) \in k(t)^*$, where $T \in Gl_3(k(t))$ is such that

$$\begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} = T \begin{pmatrix} 1 \\ \rho \\ \omega \end{pmatrix}.$$

By Proposition 3.3, $N(\mathfrak{a})$ is independent of the choice of bases for $\mathfrak{a}$ and $\mathcal{O}$. If $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$ that contains 1 with a basis $\{1, \mu, \nu\}$ as given in (3.2), then

$$N(\mathfrak{a}) = a\frac{m_1 n_2}{d^2} \quad \text{for some } a \in k^*. \tag{3.3}$$

The norm of an integral ideal $\mathfrak{a}$ is $N(\mathfrak{a}) = L(\mathfrak{a})^3 N((1/L(\mathfrak{a}))\mathfrak{a}) \in k[t]$. If $\mathfrak{a} = [L(\mathfrak{a}), \mu, \nu]$ where μ and ν are as in (3.1), then $N(\mathfrak{a}) = aL(\mathfrak{a})n_1 m_2$ for some $a \in k^*$. We have $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ for any fractional or integral ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}$. The *absolute norm* of a fractional or integral ideal $\mathfrak{a}$ is $|N(\mathfrak{a})| = q^{\deg(N(\mathfrak{a}))}$.

Proposition 3.4. *If $\mathfrak{a}$ is an integral ideal, then $L(\mathfrak{a}) \mid N(\mathfrak{a})$. If $\mathfrak{a}$ is primitive, then $N(\mathfrak{a}) \mid L(\mathfrak{a})^2$.*

The (t-)*discriminant* of a fractional or integral ideal $\mathfrak{a} = [\lambda, \mu, \nu]$ is the quantity

$$\Delta(\mathfrak{a}) = \det \begin{pmatrix} \lambda & \lambda' & \lambda'' \\ \mu & \mu' & \mu'' \\ \nu & \nu' & \nu'' \end{pmatrix}^2 \in \begin{cases} k(t) & \text{if } \mathfrak{a} \text{ is a fractional ideal,} \\ k[t] & \text{if } \mathfrak{a} \text{ is an integral ideal.} \end{cases}$$

By Proposition 3.3, $\Delta(\mathfrak{a})$ is independent of the choice of $k[t]$-basis of $\mathfrak{a}$. The discriminant of $\mathcal{O} = [1, \rho, \omega]$ is $\Delta = -27G^2H^2$. We have

$$\Delta(\mathfrak{a}) = a^2 N(\mathfrak{a})^2 \Delta \quad \text{for some } a \in k^*. \tag{3.4}$$

4. Minima and reduced ideals

If $\mathfrak{a}$ is a fractional ideal and $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, then α is a *minimum* in $\mathfrak{a}$ if for $\beta \in \mathfrak{a}$ with $\beta \neq 0$, $|\beta| \leq |\alpha|$ and $|\beta'| \leq |\alpha'|$ imply $\beta \in k^*\alpha$, i.e. β and α differ only by a factor that is a trivial unit. $\mathfrak{a}$ is *reduced* if $1 \in \mathfrak{a}$ and 1 is a minimum in $\mathfrak{a}$. An integral ideal $\mathfrak{a}$ is reduced if the fractional ideal $(1/L(\mathfrak{a}))\mathfrak{a}$ is reduced, i.e. if and only if $L(\mathfrak{a})$ is a minimum in $\mathfrak{a}$. We show that reduced ideals exist and establish certain properties.

Theorem 4.1. *$\mathcal{O}$ is reduced.*

Proof. Let $\alpha \in \mathcal{O}$, $\alpha \neq 0$, with $|\alpha| \leq 1$ and $|\alpha'| \leq 1$. Then $|\alpha'\alpha''| = |\alpha'|^2 \leq 1$, so $|N(\alpha)| \leq 1$. Since $N(\alpha) \in k[t]$ and $N(\alpha) \neq 0$, we must have $|N(\alpha)| = 1$, so α is a unit. Also $|\alpha| = |\alpha'| = 1$, so α is a trivial unit, i.e. $\alpha \in k^*$. □

Proposition 4.2. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$ and let θ be a minimum in $\mathfrak{a}$. Then $\eta\theta$ is a minimum in $\mathfrak{a}$ for every unit $\eta \in \mathcal{O}^*$.*

Proof. Let $\eta \in \mathcal{O}^*$. Clearly, $\eta\theta \in \mathfrak{a}$. Let $\alpha \in \mathfrak{a}$ be nonzero with $|\alpha| \leq |\eta\theta|$ and $|\alpha'| \leq |\eta'\theta'|$. Set $\beta = \alpha\eta^{-1}$; then $\beta \in \mathfrak{a}$, $\beta \neq 0$, $|\beta| \leq |\theta|$, and $|\beta'| \leq |\theta'|$. Since θ is a minimum in $\mathfrak{a}$, we have $\beta \in k^*\theta$, hence $\alpha \in k^*\eta\theta$. □

Corollary 4.3. *Every unit in $\mathcal{O}$ is a minimum in $\mathcal{O}$.*

Lemma 4.4. *Let $\mathfrak{a}$ be a reduced fractional ideal and let $\alpha = a + b\rho + c\omega \in \mathfrak{a}$ $(a, b, c \in k(t))$. If $|a|, |b\rho|, |c\omega| \leq 1$, then $b = c = 0$ and $\alpha = a \in k$.*

Proof. $|\alpha| \leq \max\{|a|, |b\rho|, |c\omega|\} \leq 1$, and similarly

$$|\alpha'|^2 = |\alpha'\alpha''| = |a^2 - bc\rho\omega + c^2\omega^2 - ab\rho + b^2\rho^2 - ac\omega| \leq 1.$$

Since 1 is a minimum in $\mathfrak{a}$, $\alpha \in k$. □

Theorem 4.5. *If $\mathfrak{a}$ is a reduced fractional ideal, then $|\Delta(\mathfrak{a})| > 1$, i.e. $|N(\mathfrak{a})| > 1/|\sqrt{\Delta}|$.*

Proof. Let $\{1, \mu, \nu\}$ be a basis of $\mathfrak{a}$ as given in (3.2). By first subtracting a suitable $k[t]$-multiple of μ from ν and then subtracting suitable polynomials in $k[t]$ from μ and ν, we may assume that $|n_1| < |m_1|$ and $|m_0|, |n_0| < |d|$. Since μ is not constant, by Lemma 4.4, $|m_1\rho| > |d|$. From (3.3), we obtain $|N(\mathfrak{a})| = |m_1 n_2|/|d|^2$, so by (3.4), $|\sqrt{\Delta(\mathfrak{a})}| = |m_1 n_2 \sqrt{\Delta}|/|d|^2 = |m_1 n_2 \rho\omega|/|d|^2$.

Case 1. $|n_2\omega| > |d|$. Then $|\sqrt{\Delta(\mathfrak{a})}| > 1$, and the theorem is proved.

Case 2. $|n_2\omega| \leq |d|$. Then by Lemma 4.4 $|n_1\rho| > |d|$. Assume that $|\Delta(\mathfrak{a})| \leq 1$. Then

$$1 < \left|\frac{n_1\rho}{d}\right| < \left|\frac{m_1\rho}{d}\right| = \left|\frac{d\sqrt{\Delta(\mathfrak{a})}}{n_2\omega}\right| \leq \left|\frac{d}{n_2\omega}\right|. \tag{4.1}$$

Let

$$\left|\frac{m_1}{n_1}\right| = q^m, \qquad \left|\frac{m_1\rho}{d}\right| = q^n, \qquad \left|\frac{n_2\omega}{d}\right| = q^{-l}, \tag{4.2}$$

where $m, n, l \in \mathbb{N}$. We claim that

$$0 < m < n \leq l. \tag{4.3}$$

To see this, note that $|n_1| < |m_1|$ implies $0 < m$. Since $|n_1\rho|/|d| > 1$, we have $|m_1\rho|/|d| = |m_1 n_1 \rho|/|n_1 d| > |m_1|/|n_1|$, so $m < n$. Finally, from (4.1), we obtain $|m_1\rho|/|d| \leq |d|/|n_2\omega|$, so $n \leq l$.

Let $n_1/m_1 = \sum_{i=1}^{\infty} r_i t^{-i}$ ($r_i \in k$ for $i \in \mathbb{N}$, $r_m \neq 0$, $r_i = 0$ for $i < m$). Set

$$R = \begin{pmatrix} r_{l+1} & r_l & r_{l-1} & \cdots & r_{l-n+1} \\ r_{l+2} & r_{l+1} & r_l & \cdots & r_{l-n+2} \\ r_{l+3} & r_{l+2} & r_{l+1} & \cdots & r_{l-n+3} \\ \vdots & \vdots & \vdots & & \vdots \\ r_{l+n} & r_{l+n-1} & r_{l+n-2} & \cdots & r_l \end{pmatrix} \in Mat_{n\times(n+1)}(k)$$

and let $(c_{-l}, c_{-l+1}, c_{-l+2}, \ldots, c_{-l+n})^t \in k^{n+1}$ be a nonzero solution of

$$R \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Set $c = c_{-l}t^l + c_{-l+1}t^{l-1} + \cdots + c_{-l+n}t^{l-n}$. By (4.3), $c \in k[t]$.

Now let $(n_1/m_1)c = \sum_{i=m-l}^{\infty} s_i t^{-i}$ ($s_i \in k$ for $i \geq m-l$, $s_{m-l} \neq 0$). Then

$$\begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} r_{l+1} & r_l & r_{l-1} & \cdots & r_{l-n+1} \\ r_{l+2} & r_{l+1} & r_l & \cdots & r_{l-n+2} \\ r_{l+3} & r_{l+2} & r_{l+1} & \cdots & r_{l-n+3} \\ \vdots & \vdots & \vdots & & \vdots \\ r_{l+n} & r_{l+n-1} & r_{l+n-2} & \cdots & r_l \end{pmatrix} \begin{pmatrix} c_{-l} \\ c_{-l+1} \\ c_{-l+2} \\ \vdots \\ c_{-l+n} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

so

$$\frac{n_1}{m_1}c = \sum_{i=m-l}^{0} s_i t^{-i} + \sum_{i=n+1}^{\infty} s_i t^{-i}. \tag{4.4}$$

Set $b = -\lfloor (n_1/m_1)c \rfloor = -s_{-l+m}t^{l-m} - s_{-l+m-1}t^{l-m-1} - \cdots - s_0$. Then by (4.3), $b \in k[t]$, and by (4.4)

$$\left| \frac{n_1}{m_1} c + b \right| < q^{-n}. \tag{4.5}$$

Finally, set $a = -\lfloor (bm_0 + cn_0)/d \rfloor \in k[t]$ and let $\alpha = a + b\mu + c\nu \in \mathfrak{a}$. Then

$$\alpha = \frac{1}{d}\left((da + bm_0 + cn_0) + (bm_1 + cn_1)\rho + cn_2\omega\right)$$

and from (4.2) and (4.5)

$$\begin{aligned} \left|\frac{da + bm_0 + cn_0}{d}\right| &= \left|\frac{bm_0 + cn_0}{d} - \left\lfloor \frac{bm_0 + cn_0}{d} \right\rfloor\right| < 1, \\ \left|\frac{(bm_1 + cn_1)\rho}{d}\right| &= \left|b + \frac{n_1}{m_1}c\right| \left|\frac{m_1\rho}{d}\right| < q^{-n}q^n = 1, \\ \left|\frac{cn_2\omega}{d}\right| &\le q^l q^{-l} = 1, \end{aligned}$$

where the last inequality uses $\deg(c) = l$. By Lemma 4.4, $\alpha \in k$. So in particular $c = 0$, contradicting $(c_{-l}, c_{-l+1}, \ldots, c_{-l+n}) \neq (0, 0, \ldots, 0)$. Hence the assumption that $|\Delta(\mathfrak{a})| \le 1$ is false. $|N(\mathfrak{a})| > 1/|\sqrt{\Delta}|$ follows from (3.4). □

Corollary 4.6. *If $\mathfrak{a}$ is a reduced integral ideal, then $|L(\mathfrak{a})| < |\sqrt{\Delta}|$ and $|N(\mathfrak{a})| < |\Delta|$.*

Proof. Since $\mathfrak{a}$ is reduced, $\mathfrak{b} = (1/L(\mathfrak{a}))\mathfrak{a}$ is reduced, so by Proposition 3.4 and Theorem 4.5, $|L(\mathfrak{a})|^2 \ge |N(\mathfrak{a})| = |L(\mathfrak{a})|^3|N(\mathfrak{b})| > |L(\mathfrak{a})|^3/|\sqrt{\Delta}|$, so $|L(\mathfrak{a})| < |\sqrt{\Delta}|$ and, again by Proposition 3.4, $|N(\mathfrak{a})| \le |L(\mathfrak{a})|^2 < |\Delta|$. □

Corollary 4.7. *If $\mathfrak{a}$ is a reduced fractional ideal and $\alpha \in \mathfrak{a}$ is nonzero, then $|N(\alpha)| > 1/|\Delta|$.*

Proof. Let $d \in k[t]$ be of minimal degree so that $\mathfrak{b} = d\mathfrak{a}$ is an integral ideal. Then $d\alpha \in \mathfrak{b}$, so $(d\alpha)(d^2\alpha'\alpha'') = N(d\alpha) = d^3N(\alpha) \in \mathfrak{b}$. Hence $L(\mathfrak{b}) = d \mid d^3N(\alpha)$, so $|N(\alpha)| \ge 1/|d|^2 = 1/|L(\mathfrak{b})|^2 > 1/|\Delta|$ by Corollary 4.6. □

5. Adjacent minima

Let $\mathfrak{a}$ be a fractional ideal and let $\theta \in \mathfrak{a}$ be a minimum in $\mathfrak{a}$. An element $\phi \in \mathfrak{a}$ is a *minimum adjacent to θ in $\mathfrak{a}$* if

(M1) ϕ is a minimum in $\mathfrak{a}$,
(M2) $|\theta| < |\phi|$,
(M3) for no $\alpha \in \mathfrak{a}$ do we have $|\theta| < |\alpha| < |\phi|$ and $|\alpha'| < |\theta'|$.

Note that conditions (M1) and (M2) imply $|\phi'| < |\theta'|$, as $|\theta'| \le |\phi'|$ would yield $\theta \in k^*\phi$ by (M1) and hence $|\theta| = |\phi|$, contradicting (M2).

In the number field setting, the existence of adjacent minima is easily seen. Simply expand the cylinder of elements $(x, y, z) \in \mathbb{R}^3$ with $|x| \le |\theta|$ and $y^2 + z^2 \le |\theta'\theta''|$ in the x direction until the next point $\phi \in \mathfrak{a}$ is encountered. Minkowski's lattice point theorem guarantees the existence of such an element ϕ provided the volume of the cylinder is sufficiently large. In our function fields, we need to establish the existence of adjacent minima analytically.

Theorem 5.1. *Let $\mathfrak{a}$ be a fractional ideal and let $\theta \in \mathfrak{a}$ be a minimum in $\mathfrak{a}$. Then a minimum ϕ adjacent to θ in $\mathfrak{a}$ exists and is unique up to a trivial unit factor.*

Proof. Consider the set $H(\theta) = \{\alpha \in \mathfrak{a} \mid |\alpha| > |\theta| \text{ and } |\alpha'| < |\theta'|\}$. Then $H(\theta)$ is nonempty, as $\epsilon\theta \in H(\theta)$. The set $\{\deg(\alpha) \mid \alpha \in H(\theta)\}$ is a nonempty subset of $\mathbb{Z}$, and is bounded below by $\deg(\theta)$. By the Well-Ordering Principle, it has a smallest element, so there exists $\alpha \in H(\theta)$ with $|\alpha|$ minimal. Then the set $\{\deg(N(\alpha)) \mid \alpha \in H(\theta), |\alpha| \text{ is minimal}\}$ is also a nonempty subset of $\mathbb{Z}$, and is bounded below by $-\deg(\Delta)$ by Corollary 4.7. So it has a smallest element as well. Let $\phi \in H(\theta)$ be such that $|\phi|$ is minimal and $N(\phi)$ is such a smallest element. Then

a) $|\phi| > |\theta|$ and $|\phi'| < |\theta'|$,
b) if $\alpha \in \mathfrak{a}$ with $|\alpha| > |\theta|$ and $|\alpha'| < |\theta'|$, then $|\alpha| \geq |\phi|$,
c) if $\alpha \in \mathfrak{a}$ with $|\alpha| = |\phi|$ and $|\alpha'| < |\theta'|$, then $|\alpha'| \geq |\phi'|$.

Condition a) holds because $\phi \in H(\theta)$. Property b) follows from the minimality of $|\phi|$. To see c), suppose $|\alpha| = |\phi|$ and $|\alpha'| < |\theta'|$. Then by a), $|\alpha| > |\theta|$, so $\alpha \in H(\theta)$. By minimality of $|N(\phi)|$, $|N(\alpha)| \geq |N(\phi)|$, so with $|\alpha| = |\phi|$, we obtain $|\alpha'| \geq |\phi'|$.

Now conditions (M2) and (M3) for adjacent minima follow from properties a) and b), respectively, so we only need to show that ϕ is a minimum in $\mathfrak{a}$. Let $\alpha \in \mathfrak{a}$, $\alpha \neq 0$ with $|\alpha| \leq |\phi|$ and $|\alpha'| \leq |\phi'|$. By a), $|\alpha'| < |\theta'|$. Suppose $|\alpha| \leq |\theta|$; then $\alpha \in k^*\theta$ as θ is a minimum in $\mathfrak{a}$. But then $|\theta'| = |\alpha'| < |\theta'|$. So $|\alpha| > |\theta|$. By b), $|\alpha| \geq |\phi|$, so $|\alpha| = |\phi|$. Hence by c), $|\alpha'| \geq |\phi'|$, so $|\alpha'| = |\phi'|$. Thus we have $|\alpha| = |\phi|$ and $|\alpha'| = |\phi'|$.

Let $\beta = \alpha - (\operatorname{sgn}(\alpha)/\operatorname{sgn}(\phi))\phi$; then $\beta \in \mathfrak{a}$, $|\beta| < |\phi|$ and $|\beta'| \leq \max\{|\alpha'|, |\phi'|\} < |\theta'|$. Suppose $\beta \neq 0$; then by (M3), $|\beta| \leq |\theta|$, so $\beta \in k^*\theta$. But then $|\theta'| = |\beta'| < |\theta'|$. So we must have $\beta = 0$, and thus $\alpha \in k^*\phi$. Therefore, ϕ is a minimum in $\mathfrak{a}$.

To see that ϕ is unique up to a factor in k^*, let ϕ_1, ϕ_2 be two minima in $\mathfrak{a}$ adjacent to θ. Then both ϕ_1 and ϕ_2 are minima in $\mathfrak{a}$ by (M1), and $|\theta| < |\phi_1|, |\phi_2|$ by (M2). Suppose $|\phi_1| < |\phi_2|$; then by (M3), $|\phi_1'| \geq |\theta'|$, so since ϕ_1 is a minimum in $\mathfrak{a}$, $\theta \in k^*\phi_1$. But then $|\theta| = |\phi_1| > |\theta|$. Similarly we can rule out $|\phi_1| > |\phi_2|$. Hence $|\phi_1| = |\phi_2|$. Assume without loss of generality that $|\phi_1'| \leq |\phi_2'|$; then $\phi_1 \in k^*\phi_2$. □

We will henceforth speak of *the* minimum adjacent to an element in a fractional ideal, keeping in mind that it is only unique up to a trivial unit factor.

Let $\mathfrak{a}$ be a fractional ideal and let $\theta = \theta_1$ be a minimum in $\mathfrak{a}$. A sequence $(\theta_n)_{n\in\mathbb{N}}$ of elements in $\mathfrak{a}$ where θ_{n+1} is the minimum adjacent to θ_n in $\mathfrak{a}$ ($n \in \mathbb{N}$) is a *chain of successive minima in* $\mathfrak{a}$. Note that by (M2), $|\theta_n| < |\theta_{n+1}|$, and thus by (M1), $|\theta_n'| > |\theta_{n+1}'|$ for $n \in \mathbb{N}$.

Proposition 5.2. *Let $\mathfrak{a}$ be a reduced fractional ideal, θ a minimum in $\mathfrak{a}$, and $\mathfrak{a}^* = (1/\theta)\mathfrak{a}$. Then $\mathfrak{a}^*$ is reduced.*

Proof. Let $\alpha \in \mathfrak{a}^*$, $\alpha \neq 0$, $|\alpha| \leq 1$ and $|\alpha'| \leq 1$. Then $\beta = \theta\alpha \in \mathfrak{a}$, $\beta \neq 0$, $|\beta| \leq |\theta|$ and $|\beta'| \leq |\theta'|$, so $\beta \in k^*\theta$. Hence $\alpha = \beta/\theta \in k^*$. □

Proposition 5.3. *Let $\mathfrak{a}$ be a reduced fractional ideal, θ a minimum in $\mathfrak{a}$, $\mathfrak{a}^* = (1/\theta)\mathfrak{a}$, so $\mathfrak{a}^*$ is reduced by Proposition 5.2. Let θ^* be the minimum adjacent to 1 in $\mathfrak{a}^*$. Then $\theta\theta^*$ is the minimum adjacent to θ in $\mathfrak{a}$.*

Proof. For brevity, set $\phi = \theta\theta^*$. Clearly $\phi \in \theta\mathfrak{a}^* = \mathfrak{a}$. To show (M1), let $\alpha \in \mathfrak{a}$, $\alpha \neq 0$ with $|\alpha| \leq |\phi|$ and $|\alpha'| \leq |\phi'|$. Let $\beta = \alpha/\theta$; then $\beta \in (1/\theta)\mathfrak{a} = \mathfrak{a}^*$, $\beta \neq 0$, $|\beta| \leq |\theta^*|$ and $|\beta'| \leq |(\theta^*)'|$. Since θ^* is a minimum in $\mathfrak{a}^*$, $\beta \in k^*\theta^*$, so $\alpha = \beta\theta \in k^*\phi$. So ϕ is a minimum in $\mathfrak{a}$. Now since $|\theta^*| > 1$, $|\phi| > |\theta|$, so (M2)

holds. Finally, suppose there exists $\alpha \in \mathfrak{a}$ with $|\theta| < |\alpha| < |\phi|$ and $|\alpha'| < |\theta'|$. Then $\beta = \alpha/\theta \in \mathfrak{a}^*$, $\beta \neq 0$, $1 < |\beta| < |\theta^*|$ and $|\beta'| < 1$, contradicting (M3) for the minimum θ^* adjacent to 1 in $\mathfrak{a}^*$. So (M3) is also satisfied. □

6. Outline of the algorithm

The basic idea for our algorithm is the same as in the unit rank 1 case of number fields. Start with a reduced fractional ideal $\mathfrak{a} = \mathfrak{a}_1$, for example $\mathfrak{a}_1 = \mathcal{O}$, and define a sequence of reduced fractional ideals $\mathfrak{a}_n$ and elements $\theta_n \in \mathfrak{a}$ $(n \in \mathbb{N})$ as follows. Let μ_n be the minimum adjacent to 1 in $\mathfrak{a}_n$ and set $\mathfrak{a}_{n+1} = (1/\mu_n)\mathfrak{a}_n$. Then $\mathfrak{a}_{n+1}$ is reduced by Proposition 5.2. If we set

$$\theta_1 = 1, \quad \theta_n = \prod_{i=1}^{n-1} \mu_i \quad \text{for } n \geq 2, \tag{6.1}$$

then $\mathfrak{a}_n = (1/\theta_n)\mathfrak{a}$. Since $\theta_{n+1} = \mu_n\theta_n$, θ_{n+1} is the minimum adjacent to θ_n in $\mathfrak{a}$ by Proposition 5.3. Thus we have a chain

$$\theta_1 = 1, \ \theta_2, \ \theta_3, \ \ldots \tag{6.2}$$

of successive minima in $\mathfrak{a}$. The following proposition shows that the chain (6.2) in fact contains all the minima in $\mathfrak{a}$ of nonnegative degree.

Proposition 6.1. *Let $\mathfrak{a}$ be a reduced fractional ideal and let θ be a minimum in $\mathfrak{a}$ with $|\theta| \geq 1$. Then there exist $n \in \mathbb{N}$ and $a \in k^*$ such that $\theta = a\theta_n$.*

Proof. The sequence $(|\theta_n|)_{n\in\mathbb{N}}$ is strictly increasing and unbounded. Hence there exists $n \in \mathbb{N}$ with $|\theta_n| \leq |\theta| < |\theta_{n+1}|$. If $|\theta_n'| \leq |\theta'|$, then $\theta_n \in k^*\theta$ and our claim is proved. If $|\theta'| < |\theta_n'|$, then $|\theta_n| \leq |\theta| < |\theta_{n+1}|$ and $|\theta'| < |\theta_n'|$ imply $|\theta_n| = |\theta|$ by (M3), so $\theta \in k^*\theta_n$ by (M1). □

Corollary 6.2. $|N(\theta)| < |\sqrt{\Delta}|$ *for every minimum $\theta \in \mathcal{O}$ with $|\theta| \geq 1$.*

Proof. If $\mathfrak{a}_1 = \mathcal{O}$, then we have $|N(\theta_n)| = 1/|N(\mathfrak{a}_n)|$ for all $n \in \mathbb{N}$, and the corollary follows from the previous proposition and Theorem 4.5. □

In particular, the fundamental unit ϵ must appear in the sequence (6.2) by Corollary 4.3. More exactly, since ϵ is the unit of smallest positive degree, the first index $n > 1$ such that $N(\theta_n) \in k^*$ satisfies $\theta_n \in k^*\epsilon$. If $l \in \mathbb{N}$ is minimal such that $\theta_{l+1} \in k^*\epsilon$ $(l \in \mathbb{N})$, then $\mathfrak{a}_{l+1} = \mathfrak{a}_1$, $\mu_{l+1} = \mu_1$ (possibly up to a constant factor), and in fact $\mu_{ml+i} = \mu_i$ for $m, i \in \mathbb{N}$ (again, possibly up to a trivial unit factor). Hence the sequence (6.2) is equal to

$$1, \theta_2, \ldots, \theta_l, \epsilon, \epsilon\theta_2, \ldots, \epsilon\theta_l, \epsilon^2, \epsilon^2\theta_2, \ldots, \epsilon^3, \ldots$$

and contains all nonnegative powers of ϵ. We call l the *period* of ϵ (or of K).

Thus, to find ϵ, we need to compute a sequence of elements $(\mu_n)_{n\in\mathbb{N}}$ where $\mathfrak{a}_1 = \mathcal{O}$, $\mathfrak{a}_{n+1} = (1/\mu_n)\mathfrak{a}_n$, and μ_n is the minimum adjacent to 1 in $\mathfrak{a}_n$ $(n \in \mathbb{N})$. We terminate as soon as $N(\theta_{l+1}) \in k^*$, where θ_{l+1} is defined as in (6.1), at which point $\epsilon = \theta_{l+1}$ and $R = \deg(\theta_{l+1})/2$. Hence the key portion of our algorithm is a method for generating the minimum μ adjacent to 1 in a reduced fractional $\mathfrak{a}$. This is accomplished by applying a sequence of suitable unimodular transformations to the pair (ϕ, ψ), where $\{1, \phi, \psi\}$ is a $k[t]$-basis of $\mathfrak{a}$, until a basis $\{1, \mu, \nu\}$ is obtained such that μ is our desired minimum. We call a basis that contains μ a *reduced basis* of $\mathfrak{a}$. Details on how to compute a reduced basis are given in section 7.

Before we present our unit and regulator algorithms, we give a simpler condition that determines exactly when $N(\theta_n) \in k^*$ and avoids computing norms.

Proposition 6.3. *Let* $\mathfrak{a} = (1/\theta) = [1, \mu, \nu]$, *where* θ *is an element of the chain (6.2) and* $\mu = (m_0+m_1\rho+m_2\omega)/d$, $\nu = (n_0+n_1\rho+n_2\omega)/d$ *with* $m_0, m_1, m_2, n_0, n_1, n_2, d$ $k[t]$ *and* $\gcd(m_0, m_1, m_2, n_0, n_1, n_2, d) = 1$. *Then* $N(\theta) \in k^*$ *if and only if* $d \in k^*$.

Proof. Since $N(\mathfrak{a}) = \operatorname{sgn}(N(\theta))/N(\theta)$, we have $N(\theta) \in k^*$ if and only if $N(\mathfrak{a}) = 1$, which is the case if and only if $\mathfrak{a} = \mathcal{O}$, or equivalently $\mu, \nu \in \mathcal{O}$. But because of the gcd condition, μ and ν are in $\mathcal{O}$ if and only if $d \in k^*$. □

We are now ready to present our algorithm for computing the fundamental unit of K. In each iteration, we have a basis $\{1, \mu_n = (m_0 + m_1\rho + m_2\omega)/d, \nu_n = (n_0 + n_1\rho + n_2\omega)/d\}$ of our current fractional ideal $\mathfrak{a}_n = (1/\theta_n)$, where $\theta_n = (e_0 + e_1\rho + e_2\omega)/f$ ($m_i, n_i, d, e_i, f \in k[t]$ for $i = 0, 1, 2$). This basis is replaced by a reduced basis (also called $\{1, \mu_n, \nu_n\}$). Then θ_n is updated to $\theta_{n+1} = \mu_n\theta_n$, and since $\mathfrak{a}_{n+1} = (1/\mu_n)\mathfrak{a}_n$, μ_n and ν_n are replaced by $\mu_{n+1} = 1/\mu_n = \mu'_n\mu''_n/N(\mu_n)$ and $\nu_{n+1} = \nu_n/\mu_n = \nu_n\mu_{n+1}$, respectively. Initially, $\theta_1 = 1$, $\mu_1 = \rho$, and $\nu_1 = \omega$. Using Proposition 6.3, we terminate the algorithm as soon as we encounter a basis denominator d that is a constant.

Algorithm 6.4 (Fundamental unit algorithm).

Input: The polynomials G, H, *where* $D = GH^2$.

Output: $e_0, e_1, e_2 \in k[t]$, *where* $\epsilon = e_0 + e_1\rho + \epsilon_2\omega$ *is the fundamental unit of* K.

Algorithm:

1. *Set* $e_0 = f = 1$, $e_1 = e_2 = 0$; $m_0 = m_2 = n_0 = n_1 = 0$, $m_1 = n_2 = d = 1$.
2. *Repeat*
   (a) { Reduce the basis }
   Use Algorithm 7.1 below to replace $m_0, m_1, m_2, n_0, n_1, n_2, d$ *by the coefficients of a reduced basis.*
   (b) { Update θ_n }
   (i) *Replace*

$$\begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ f \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} e_0m_0 + (e_1m_2 + e_2m_1)GH \\ e_0m_1 + e_1m_0 + e_2m_2G \\ e_0m_2 + e_1m_1H + e_2m_0 \\ df \end{pmatrix}.$$

   (ii) *Compute* $g = \gcd(e_0, e_1, e_2, f)$. *For* $i = 0, 1, 2$, *replace* e_i *by* e_i/g *and* f *by* f/g.
   (c) { Update μ and ν }
   (i) *Set*

$$\begin{aligned} a_0 &= m_0^2 - m_1m_2GH, \\ a_1 &= m_2^2G - m_0m_1, \\ a_2 &= m_1^2H - m_0m_2, \\ b &= m_0^3 + m_1^3GH^2 + m_2^3G^2H - 3m_0m_1m_2GH. \end{aligned}$$

   (ii) *Replace*

$$\begin{pmatrix} m_0 \\ m_1 \\ m_2 \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} a_0d \\ a_1d \\ a_2d \end{pmatrix}.$$

(iii) *Replace*

$$\begin{pmatrix} n_0 \\ n_1 \\ n_2 \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} a_0n_0 + (a_1n_2 + a_2n_1)GH \\ a_0n_1 + a_1n_0 + a_2n_2G \\ a_0n_2 + a_1n_1H + a_2n_0 \end{pmatrix}.$$

(iv) *Replace* d *by* b.

(v) *Compute* $h = \gcd(m_0, m_1, m_2, n_0, n_1, n_2, d)$. *For* $i = 0, 1, 2$, *replace* m_i *by* m_i/h, n_i *by* n_i/h *and* d *by* d/h.

until $d \in k^*$.

Since the computation of ϵ requires l reduction steps, where l is the period of ϵ, it is desirable to have an upper bound on l. In general, l can be quite large.

Theorem 6.5. *For the period* l *of* ϵ, *we have* $l \leq 2R = \deg(\epsilon) = O(q^{\deg \Delta/2-2})$.

Proof. For $n \in \mathbb{N}$, let $\delta_n = \deg(\theta_n) \in \mathbb{N}_0$. Since $\delta_1 = 0$ and δ_n strictly increases with n, a simple induction argument shows $\delta_n \geq n - 1$. Hence $l \leq \deg(\theta_{l+1}) = \deg(\epsilon) = 2R$. From the Hasse-Weil Theorem (see [16, Theorem V.1.15, p. 166, and Theorem V.2.1 , p. 169]), we can infer that $(\sqrt{q} - 1)^{2g} \leq h \leq (\sqrt{q} + 1)^{2g}$. Hence, using (2.1) and the identity $g = \deg(\sqrt{\Delta}) - 2$ for the genus g of K (see Theorem 2.1), we obtain $R \leq (\sqrt{q} + 1)^{\deg(\Delta)-4} = O(q^{\deg(\Delta)/2-2})$. □

Corollary 6.6. $|\epsilon| = O(q^{q^{\deg(\Delta)/2-2}})$.

Corollary 6.6 shows that the coefficients e_0, e_1, e_2 of ϵ can be so huge that it might be infeasible to compute or even simply write down the fundamental unit for large values of $|\Delta|$. For this situation, we modify Algorithm 6.4 to compute only the regulator R of K. We show in the next section that if $\mu = (m_0 + m_1\rho + m_2\omega)/d$ is the minimum adjacent to 1 in some reduced fractional ideal, then $\deg(\mu) = \deg(m_0/d)$ (see Lemma 7.4), so we only need to add $\deg(m_0) - \deg(d)$ in each iteration to update the regulator. After step 2 of the algorithm below, the degree of ϵ is stored in R, so we need to divide by 2 in step 3.

Algorithm 6.7 (Regulator algorithm).

Input: The polynomials G, H, *where* $D = GH^2$.

Output: The regulator R *of* K.

Algorithm:

1. *Set* $R = 0$; $m_0 = m_2 = n_0 = n_1 = 0$, $m_1 = n_2 = d = 1$.
2. *Repeat*
   (a) *Use Algorithm 7.1 below to replace* $m_0, m_1, m_2, n_0, n_1, n_2, d$ *by the coefficients of a reduced basis.*
   (b) *Replace* R *by* $R + \deg(m_0) - \deg(d)$.
   (c) (i) *Set*

$$\begin{aligned} a_0 &= m_0^2 - m_1m_2GH, \\ a_1 &= m_2^2G - m_0m_1, \\ a_2 &= m_1^2H - m_0m_2, \\ b &= m_0^3 + m_1^3GH^2 + m_2^3G^2H - 3m_0m_1m_2GH. \end{aligned}$$

   (ii) *Replace*

$$\begin{pmatrix} m_0 \\ m_1 \\ m_2 \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} a_0d \\ a_1d \\ a_2d \end{pmatrix}.$$

(iii) *Replace*

$$\begin{pmatrix} n_0 \\ n_1 \\ n_2 \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} a_0n_0 + (a_1n_2 + a_2n_1)GH \\ a_0n_1 + a_1n_0 + a_2n_2G \\ a_0n_2 + a_1n_1H + a_2n_0 \end{pmatrix}.$$

(iv) *Replace* d *by* b.

(v) *Compute* $h = \gcd(m_0, m_1, m_2, n_0, n_1, n_2, d)$. *For* $i = 0, 1, 2$, *replace* m_i *by* m_i/h, n_i *by* n_i/h *and* d *by* d/h.

until $d \in k^*$.

3. *Replace* R *by* $R/2$.

7. Computation of a minimum adjacent to 1

The above discussion shows that the task of finding ϵ (or R) reduces to the problem of computing a reduced basis of a reduced fractional ideal $\mathfrak{a}$. In particular, we need to be able to generate the minimum adjacent to 1 in $\mathfrak{a}$. Before we illustrate how to do this, we require several somewhat technical definitions. Here, we let ourselves be guided by the terminology and techniques in [20]. As mentioned before, in the number field case, these concepts are geometrically motivated. While they lose their geometric significance in the function field case, they can nevertheless be used to accomplish our goal.

Henceforth, we exclude the characteristic 2 case, that is, we require k to be a finite field of characteristic at least 5. Let $\alpha = a + b\rho + c\omega \in K$ with $a, b, c \in k(t)$. We define the quantities

$$\begin{aligned} \xi_\alpha &= b\rho + c\omega &&= \alpha - a, \\ \eta_\alpha &= b\rho - c\omega &&= \frac{1}{2\iota + 1}(\alpha' - \alpha''), \\ \zeta_\alpha &= 2a - b\rho - c\omega &&= \alpha' + \alpha'', \end{aligned} \tag{7.1}$$

where we recall that ι is a primitive cube root of unity. Then $\xi_{f\alpha+g\beta} = f\xi_\alpha + g\xi_\beta$, $\eta_{f\alpha+g\beta} = f\eta_\alpha + g\eta_\beta$, $\zeta_{f\alpha+g\beta} = f\zeta_\alpha + g\zeta_\beta$ for any $\alpha, \beta \in K$ and $f, g \in k(t)$. Simple calculations show

$$\alpha = \frac{1}{2}(3\xi_\alpha + \zeta_\alpha), \qquad \alpha'\alpha'' = \frac{1}{4}(3\eta_\alpha^2 + \zeta_\alpha^2). \tag{7.2}$$

and if $\mathfrak{a} = [1, \mu, \nu]$ is a fractional ideal, then

$$\det \begin{pmatrix} \xi_\mu & \eta_\mu \\ \xi_\nu & \eta_\nu \end{pmatrix} = \xi_\mu\eta_\nu - \xi_\nu\eta_\mu = -2\sqrt{\Delta(\mathfrak{a})}, \tag{7.3}$$

so this determinant is independent of the choice of basis of $\mathfrak{a}$.

We now give the algorithm that on input of a basis of some reduced fractional ideal produces a reduced basis of that same ideal.

Algorithm 7.1 (Reduction algorithm).

Input: $\tilde{\mu}$, $\tilde{\nu}$, *where* $\{1, \tilde{\mu}, \tilde{\nu}\}$ *is a basis of some reduced fractional ideal* $\mathfrak{a}$.

Output: μ, ν, *where* $\{1, \mu, \nu\}$ *is a basis of* $\mathfrak{a}$ *such that* $|\zeta_\mu| < 1$, $|\zeta_\nu| < 1$, $|\xi_\mu| > |\xi_\nu|$, $|\eta_\mu| < 1 \leq |\eta_\nu|$.

Algorithm:

1. *Set* $\mu = \tilde{\mu}$, $\nu = \tilde{\nu}$.
2. *If* $|\xi_\mu| < |\xi_\nu|$ *or if* $|\xi_\mu| = |\xi_\nu|$ *and, replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

3. *If* $|\eta_\mu| \geq |\eta_\nu|$
   (a) *while* $\lfloor \xi_\mu/\xi_\nu \rfloor = \lfloor \eta_\mu/\eta_\nu \rfloor$, *replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   (b) *Replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   (c) *If* $|\eta_\mu| = |\eta_\nu|$, *replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   where $a = \operatorname{sgn}(\eta_\mu)\operatorname{sgn}(\eta_\nu)^{-1} \in k^*$.
4. (a) *While* $|\eta_\nu| < 1$, *replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu/\xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   (b) *While* $|\eta_\mu| \geq 1$, *replace*

$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} \lfloor \eta_\nu/\eta_\mu \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

5. *If* $|\zeta_\mu| \geq 1$, *replace* μ *by* $\mu - (1/2)\lfloor \zeta_\mu \rfloor$.
   If $|\zeta_\nu| \geq 1$, *replace* ν *by* $\nu - (1/2)\lfloor \zeta_\nu \rfloor$.

Proposition 7.2. *Algorithm 7.1 terminates and produces the output specified above.*

Proof. It is easy to see that all transformations of μ and ν in steps 2, 3 and 4 maintain a basis $\{1, \mu, \nu\}$ of $\mathfrak{a}$, because the basis transformation matrices all have determinant 1.

We claim that after step 3, we have

$$|\xi_\mu| > |\xi_\nu|, \quad |\eta_\mu| < |\eta_\nu|. \tag{7.4}$$

This can be seen as follows. Since step 2 replaces μ by ν and ν by $-\mu$, we have $|\xi_\mu| > |\xi_\nu|$ or $|\xi_\mu| = |\xi_\nu|$ and $|\eta_\mu| \geq |\eta_\nu|$ after step 2. If at the beginning of step 3, $|\eta_\mu| < |\eta_\nu|$, then from the previous step $|\xi_\mu| > |\xi_\nu|$, so conditions (7.4) hold and step 3 is skipped.

Assume now that $|\eta_\mu| \geq |\eta_\nu|$, so step 3 is entered. Consider step 3 (a) and set $\alpha = \nu$ and $\beta = \lfloor \xi_\mu/\xi_\nu \rfloor \nu - \mu$, so α and β are obtained by applying the linear transformation of step 3 (a) to μ and ν. Then

$$\begin{aligned} |\xi_\beta| &= \left| \left\lfloor \frac{\xi_\mu}{\xi_\nu} \right\rfloor \xi_\nu - \xi_\mu \right| < |\xi_\nu| = |\xi_\alpha|, \\ |\eta_\beta| &= \left| \left\lfloor \frac{\eta_\mu}{\eta_\nu} \right\rfloor \eta_\nu - \eta_\mu \right| < |\eta_\nu| = |\eta_\alpha|. \end{aligned}$$

Hence, $|\xi_\nu|$ and $|\eta_\nu|$ strictly decrease in each iteration, so the loop must terminate at the latest before $|\xi_\nu \eta_\nu| \leq 1$, for otherwise by (7.3)

$$|\sqrt{\Delta(\mathfrak{a})}| = |\xi_\nu \eta_\nu||\eta_\mu/\eta_\nu - \xi_\mu/\xi_\nu| < |\xi_\nu \eta_\nu| \leq 1,$$

contradicting Theorem 4.5. After step 3 (b), we have $|\xi_\beta| < |\xi_\nu| = |\xi_\alpha|$ and

$$|\eta_\beta| = \left| \left(\left\lfloor \frac{\xi_\mu}{\xi_\nu} \right\rfloor - \left\lfloor \frac{\eta_\mu}{\eta_\nu} \right\rfloor \right) \eta_\nu + \left(\left\lfloor \frac{\eta_\mu}{\eta_\nu} \right\rfloor \eta_\nu - \eta_\mu \right) \right| \geq |\eta_\nu| = |\eta_\alpha|,$$

because $|\lfloor \xi_\mu/\xi_\nu \rfloor - \lfloor \eta_\mu/\eta_\nu \rfloor| \geq 1$ and $|\lfloor \eta_\mu/\eta_\nu \rfloor \eta_\nu - \eta_\mu| < |\eta_\nu|$. Finally, observe that in step 3 (c), $a = \lfloor \eta_\mu/\eta_\nu \rfloor$. If we set $\alpha = \mu - a\nu$ and $\beta = \nu$, then as before $|\eta_\alpha| < |\eta_\beta|$, and since $|\xi_\mu| > |\xi_\nu|$, we have $|\xi_\alpha| = |\xi_\mu - a\xi_\nu| = |\xi_\mu| > |\xi_\nu| = |\xi_\beta|$. So step 3 achieves the inequalities (7.4) above.

In step 4, we ensure that $|\eta_\mu| < 1 \leq |\eta_\nu|$. From (7.4), it is clear that at most one of the while loops in step 4 is entered. Consider first the case $|\eta_\nu| < 1$, i.e. case 4 (a). Set $\alpha = \nu$ and $\beta = \lfloor \xi_\mu/\xi_\nu \rfloor \nu - \mu$. Then

$$|\xi_\beta| < |\xi_\nu| = |\xi_\alpha|, \quad |\eta_\beta| = \left| \left\lfloor \frac{\xi_\mu}{\xi_\nu} \right\rfloor \eta_\nu - \eta_\mu \right| > |\eta_\nu| = |\eta_\alpha|, \quad |\eta_\alpha| = |\eta_\nu| < 1,$$

so inequalities (7.4) and the condition $|\eta_\mu| < 1$ are maintained throughout the loop. Furthermore, $|\eta_\nu|$ strictly increases in each iteration, so the while loop will terminate with the desired basis. In step 4 (b), if we set $\beta = \mu$ and $\alpha = \lfloor \eta_\nu/\eta_\mu \rfloor \mu - \nu$, then

$$|\eta_\alpha| < |\eta_\mu| = |\eta_\beta|, \quad |\xi_\alpha| = \left| \left\lfloor \frac{\eta_\nu}{\eta_\mu} \right\rfloor \xi_\mu - \xi_\nu \right| > |\xi_\mu| = |\xi_\beta|, \quad |\eta_\beta| = |\eta_\mu| \geq 1,$$

so again (7.4) and the condition $|\eta_\nu| \geq 1$ are maintained throughout the loop. In addition, $|\eta_\mu|$ strictly decreases in each iteration, so in this case the while loop also terminates with the desired basis.

Finally, step 5 achieves $|\zeta_\mu|, |\zeta_\nu| < 1$ while preserving the inequalities obtained in the first 4 steps. To see this, let $\alpha = \mu - (1/2)\lfloor \zeta_\mu \rfloor$; then by (7.1) $|\zeta_\alpha| = |\zeta_\mu - \frac{1}{2}\zeta_{\lfloor \zeta_\mu \rfloor}| = |\zeta_\mu - \lfloor \zeta_\mu \rfloor| < 1$. Similarly for ν. □

We proceed to prove that the basis of Algorithm 7.1 is indeed a reduced basis,

Lemma 7.3. *Let $\alpha \in K$. Then $|\alpha'| < 1$ if and only if $|\eta_\alpha| < 1$ and $|\zeta_\alpha| < 1$.*

Proof. If $|\eta_\alpha| < 1$ and $|\zeta_\alpha| < 1$, then from (7.2) $|\alpha'|^2 \leq \max\{|\eta_\alpha|^2, |\zeta_\alpha|^2\} < 1$. Conversely, if $|\alpha'| < 1$, then $|\zeta_\alpha| = |\alpha' + \alpha''| \leq |\alpha'| < 1$, and from (7.2) $|\eta_\alpha|^2 = |4\alpha'\alpha'' - \zeta_\alpha^2| < 1$. □

Lemma 7.4. *Let $\alpha = a + b\rho + c\omega \in K$ with $|\alpha| > 1$ and $|\alpha'| < 1$. Then $|\alpha| = |\xi_\alpha| = |a| = |b\rho| = |c\omega|$.*

Proof. By Lemma 7.3, we have $|\eta_\alpha| < 1$ and $|\zeta_\alpha| < 1$. From $|\alpha| > 1$ and $|\zeta_\alpha| = |3a - \alpha| < 1$, it follows that $|\alpha| = |a|$. The inequality $|\zeta_\alpha| = |2a - \xi_\alpha| < 1$ implies $|\xi_\alpha| = |a| > 1$. Finally, from $|\xi_\alpha| > 1$ and $|\eta_\alpha| < 1$, we obtain $|b\rho| = |c\omega| = |\xi_\alpha|$. □

Theorem 7.5. *Let $\{1, \mu, \nu\}$ be a basis of a reduced fractional ideal $\mathfrak{a}$ such that $|\zeta_\mu| < 1$, $|\zeta_\nu| < 1$, $|\xi_\mu| > |\xi_\nu|$, $|\eta_\mu| < 1 \leq |\eta_\nu|$. Then μ is the minimum adjacent to 1 in $\mathfrak{a}$, so $\{1, \mu, \nu\}$ is a reduced basis of $\mathfrak{a}$.*

Proof. Let θ be the minimum adjacent to 1 in $\mathfrak{a}$, $\theta = l + m\mu + n\nu$ with $l, m, n \in k[t]$. We wish to show that $l = n = 0$ and $m \in k^*$. Since $|\theta'| < 1$, we have $|\zeta_\theta| < 1$ and $|\eta_\theta| < 1$ by Lemma 7.3. By the same lemma, $|\mu'| < 1$, as $|\zeta_\mu| < 1$ and $|\eta_\mu| < 1$. Then $|\mu| > 1$, as otherwise $\mu \in k$. Hence $|\mu| \geq |\theta|$, since otherwise $1 < |\mu| < |\theta|$ and $|\mu'| < 1$, contradicting (M3) for θ.

If $n = 0$, then $m \neq 0$ as $\theta \notin k[t]$, so $|m| > |n|$ and $|m\xi_\mu| > |n\xi_\nu|$. If $n \neq 0$, then $1 > |\eta_\theta| = |m\eta_\mu + n\eta_\nu|$ with $|n\eta_\nu| \geq 1$ implies $|m\eta_\mu| = |n\eta_\nu|$. Thus, $|n| \leq |n\eta_\nu| =$

$|m\eta_\mu| < |m|$, so $|m| > |n|$ and $|m\xi_\mu| > |n\xi_\nu|$ as well. It follows from Lemma 7.4 that

$$|\theta| = |\xi_\theta| = |m\xi_\mu + n\xi_\nu| = |m\xi_\mu| = |m\mu| \geq |m\theta|,$$

so $|m| \leq 1$. Thus, $1 \geq |m| > |n|$, so $n = 0$ and $m \in k^*$.

Now $1 > |\zeta_\theta| = |\zeta_{l+m\mu}| = |2l + \zeta_\mu|$, so since $|\zeta_\mu| < 1$, $|l| < 1$, so $l = 0$ and $\theta = m\mu \in k^*\mu$. □

The coefficients of the basis generated by Algorithm 7.1 are small:

Theorem 7.6. *Let $\mathfrak{a}$ be a reduced fractional ideal and let $\{1, \mu, \nu\}$ be the basis of $\mathfrak{a}$ produced by Algorithm 7.1. Let $\mu = (m_0 + m_1\rho + m_2\omega)/d$, $\nu = (n_0 + n_1\rho + n_2\omega)/d$ with $m_0, m_1, m_2, n_0, n_1, n_2, d \in k[t]$ and $\gcd(m_0, m_1, m_2, n_0, n_1, n_2, d) = 1$. Then $|d| < |d\mu| = |m_0| = |m_1\rho| = |m_2\omega| \leq |\sqrt{\Delta}|$ and $|n_0|, |n_1\rho|, |n_2\omega| < |\sqrt{\Delta}|$, so $|m_1| \leq |\omega|$, $|n_1| < |\omega|$, $|m_2| \leq |\rho|$, and $|n_2| < |\rho|$.*

Proof. From Lemma 7.4, $|d| < |d\mu| = |d\xi_\mu| = |m_0| = |m_1\rho| = |m_2\omega|$. Now by Corollary 3.2, $d\mathfrak{a}$ is a reduced integral ideal with $L(d\mathfrak{a}) = \operatorname{sgn}(d)^{-1}d$. By Proposition 3.4, $d^3N(\mathfrak{a}) = N(d\mathfrak{a}) \mid d^2$, so $|dN(\mathfrak{a})| \leq 1$. From (3.4) and (7.3), we obtain

$$|\sqrt{\Delta}| \geq |dN(\mathfrak{a})\sqrt{\Delta}| = |d\sqrt{\Delta(\mathfrak{a})}| = |d(\xi_\mu\eta_\nu - \xi_\nu\eta_\mu)| \geq |d\xi_\mu|,$$

as $|\xi_\mu| > |\xi_\nu|$ and $|\eta_\mu| < 1 \leq |\eta_\nu|$.

Since $|\xi_\mu| > |\xi_\nu|$, we have $|\sqrt{\Delta}| \geq |m_1\rho + m_2\omega| > |n_1\rho + n_2\omega|$. Also, $|\sqrt{\Delta(\mathfrak{a})}| = |\xi_\mu\eta_\nu| > |\eta_\nu|$, so $|\sqrt{\Delta}| \geq |d\sqrt{\Delta(\mathfrak{a})}| > |d\eta_\nu| = |n_1\rho - n_2\omega|$. Hence $|n_1\rho|, |n_2\omega| < |\sqrt{\Delta}|$. Finally, $|\zeta_\nu| < 1$ implies $|2n_0 - n_1\rho - n_2\omega| < |d| < |\sqrt{\Delta}|$, so $|n_0| < |\sqrt{\Delta}|$.

The rest of the inequalities follow from the identity $\rho\omega = \sqrt{\Delta}$. □

8. Implementation

Our algorithm was implemented using the computer algebra system SIMATH developed by the research group of Professor H. G. Zimmer at the Universität des Saarlandes in Saarbrücken, Germany. All our computations were done on a Silicon Graphics Challenge workstation. Since much of our method required manipulation of Puiseux series, it was necessary to write routines for arithmetic of power series. For this purpose, we had to use truncated series as approximations for our Puiseux series, in analogy to using rational approximations when computing with real numbers. However, in contrast to Voronoi's algorithm in number fields, we were able to establish conditions to check throughout the algorithm whether our approximations were sufficiently accurate and increase the accuracy if necessary.

Define an *approximation $\hat{\alpha}_n$ of precision $n \in \mathbb{N}_0$* to an element $\alpha = \sum_{i=m}^{\infty} a_i/t^i \in k((1/t))$ to be $\hat{\alpha}_n = \sum_{i=m}^{n} a_i/t^i$. Then $|\alpha - \hat{\alpha}_n| < q^{-n}$. An approximation to α of degree 0 is simply the principal part $\lfloor\alpha\rfloor$ of α. We used the method for extracting cube roots as described in [9] and implemented by Mang in [10] to compute approximations $\hat{\rho}$ and $\hat{\omega}$ of precision δ of the basis elements ρ and ω, respectively, at the beginning of each unit or regulator computation. Here, $\delta = \deg(\Delta)$ turned out to be always sufficient. Examples show that reducing the value of δ to $\deg(\Delta)/2$ or even $\deg(\Delta)/4$ often still produced correct results, but computation times improved only marginally with smaller precision.

Since the polynomials and series approximations in our algorithm generally had few zero coefficients, they were given in *dense representation*; that is, as a list starting with the degree of the polynomial or the series, followed by the coefficients in

order of decreasing degree of monomial. The main difficulty in our implementation was the computation of the principal parts of quotients as required in steps 3 – 5 of Algorithm 7.1. Here, an approximation $\hat{\xi}_\mu$ of $\xi_\mu = (m_1\rho + m_2\omega)/d$ was represented as a pair (α_μ, d) where $\alpha_\mu = m_1\hat{\rho}_\delta + m_2\hat{\omega}_\delta$; similarly for ξ_ν, η_μ, and η_ν. To compute a quotient, $\lfloor \xi_\mu/\xi_\nu \rfloor$ for example, we performed "division with remainder" on the quantities α_μ and $\alpha_\nu = n_1\hat{\rho}_\delta + n_2\hat{\omega}_\delta$. It is easy to check whether this gives the correct result:

Lemma 8.1. *Let $\alpha, \beta \in k((1/t))$, $\beta \neq 0$. Let $\hat{\alpha}_m$ be an approximation of α of precision m and let $\hat{\beta}_n$ be an approximation of β of precision n. If $m \geq -\deg(\beta)$ and $n \geq \deg(\alpha) - 2\deg(\beta)$, then $\lfloor \alpha/\beta \rfloor = \lfloor \hat{\alpha}_m/\hat{\beta}_n \rfloor$.*

Now let $M = m_1$ if $|m_1| \geq |m_2|$ and $M = m_2$ otherwise, so

$$|M| = \max\{|m_1|, |m_2|\}.$$

Similarly, set $N = n_1$ if $|n_1| \geq |n_2|$ and $N = n_2$ otherwise. Also, let $m = \delta + \deg(d) - \deg(M)$ and $n = \delta + \deg(d) - \deg(N)$. Then

$$|\xi_\mu - \hat{\xi}_\mu| = \left| \frac{m_1(\rho - \hat{\rho}) + m_2(\omega - \hat{\omega})}{d} \right| < \frac{|M|}{|d|} q^{-\delta} = q^{-m},$$

so $\hat{\xi}_\mu$ is an approximation of ξ_μ of precision m. Similarly, we obtain $|\xi_\nu - \hat{\xi}_\nu| < q^{-n}$. Lemma 8.1 guarantees that $\lfloor \xi_\mu/\xi_\nu \rfloor = \lfloor \hat{\xi}_\mu/\hat{\xi}_\nu \rfloor$, provided

$$|\xi_\nu| \geq q^{-m} \qquad \text{and} \qquad \left| \frac{\xi_\mu}{\xi_\nu^2} \right| \leq q^n.$$

A simple calculation shows that these conditions can be made independent of the denominator d and are equivalent to

$$|\alpha_\nu| \geq \frac{|M|}{q^\delta} \qquad \text{and} \qquad \left| \frac{\alpha_\mu}{\alpha_\nu^2 \cdot} \right| \leq \frac{q^\delta}{|N|}. \tag{8.1}$$

Now let μ_i and ν_i be the values of μ and ν after the i-th iteration of step 3 (a) of Algorithm 7.1. Then

$$\frac{\xi_{\mu_i}}{\xi_{\nu_i}} = \left(\left\lfloor \frac{\xi_{\mu_{i-1}}}{\xi_{\nu_{i-1}}} \right\rfloor - \frac{\xi_{\mu_{i-1}}}{\xi_{\nu_{i-1}}} \right)^{-1} \qquad (i \in \mathbb{N}),$$

so ξ_{μ_i}/ξ_{ν_i} is the i-th partial quotient of the continued fraction expansion of ξ_{μ_0}/ξ_{ν_0}. Our computations indicate that these partial quotients satisfy a "Gauss-Kuz'min law for Puiseux series"; that is, they almost always have small degree, and frequently the degree is 0. We never encountered a partial quotient whose degree exceeded $g - 1$, where g is the genus of the field.

To simplify conditions (8.1), suppose that $|\alpha_\mu/\alpha_\nu| = |\xi_\mu/\xi_\nu| = q^s$, where $s \in \mathbb{N}_0$ is small. Then (8.1) is equivalent to

$$|n_1\rho + n_2\omega| \geq \max\{|M|, q^s|N|\} q^{-\delta}. \tag{8.2}$$

Our computations show that the absolute values of the coefficients m_1, m_2, n_1, and n_2 are almost always significantly smaller that the theoretical bound of $|\Delta|^{3/2}$ obtained from the formulas in step 2 (c) of Algorithm 6.4 together with Theorem 7.6; in fact, their degrees were always less than g. Since $|m_1n_2 - m_2n_1| = |d^2N(\mathfrak{a})| = |N(d\mathfrak{a})/d| < |\Delta|/|d|$ by Corollary 4.6, we expect that $|M|$ and $q^s|N|$ are usually of roughly the same size and not too large. This was once again confirmed by our computations, which always yielded $\deg(M) = s + \deg(N) < 2g = \delta - 4$. It is a

simple matter to check in each iteration of step 3 (b) of the reduction algorithm whether (8.2) holds, and we found that the inequality was always satisfied. Similar inequalities can be derived and arguments made for the other quotients occurring in Algorithm 7.1.

Note that it is possible to reduce the division with remainder of two truncated series to a division of a truncated series by just a polynomial by using formulas such as

$$\frac{\xi_\mu}{\xi_\nu} = \frac{A - B\eta_\nu}{C},$$

where

$$A = m_1 n_1^2 H + m_2 n_2^2 G, \quad B = m_1 n_2 - m_2 n_1, \quad C = n_1^3 H + n_2^3 G.$$

Then $\lfloor \xi_\mu/\xi_\nu \rfloor = \lfloor (A - B\hat{\eta}_\nu)/C \rfloor$, with an approximation $\hat{\eta}_\nu$ of precision $\deg(B)$ to η_ν, provided $|n_1|, |n_2| < |C|$, which we always found to be the case. Similar formulas, involving different values of A and C, but using the same B value, hold for the other quotients. Note that $N(d\mathfrak{a}) = dB/\mathrm{sgn}(dB)$, so B is independent of the basis and need only be computed once per reduction. Furthermore, $|B| < |\Delta|/|d| \leq |\Delta|$ by Corollary 4.6. We performed computations with both explicit division with remainder and the above formulas, and the division with remainder version of the algorithm turned out to be about 20 percent faster.

In step 5 of Algorithm 6.4, we approximate $\zeta_\mu = 2m_0/d + \xi_\mu$ by

$$\hat{\zeta}_\mu = (2m_0 + \alpha_\mu)/d.$$

Then the principal part $\lfloor \zeta_\mu \rfloor$ of ζ_μ can be computed as simply $\lfloor (2m_0 - \alpha_\mu)/d \rfloor$. This will always produce the correct polynomial, as

$$|\zeta_\mu - (2m_0 + \alpha_\mu)/d| \leq \max\{|m_1|, |m_2|\}/|d| \cdot q^{-\delta} < 1,$$

since $|d| \geq 1$ and at this point $|m_1|, |m_2| < |\sqrt{\Delta}|$ by Theorem 7.6. Similarly for ζ_ν.

9. Numerical examples

All our examples were done over prime fields $k = \mathbb{F}_p$, where p is a prime with $p \equiv -1 (\mathrm{mod}\ 3)$, and used monic polynomials G and H. Among many examples, we recomputed all of Mang's examples of unit rank 1 in [10]. Not surprisingly, we found that our regulator algorithm was significantly faster than our unit algorithm, due to the time-consuming polynomial arithmetic involved in updating θ_n in step 2 (b) of each iteration of Algorithm 6.4.

The largest unit we computed was the fundamental unit ϵ of $K = \mathbb{F}_{17}(\sqrt[3]{GH^2})$ where $G = t + 4$ and $H = t^4 + t^3 + 11t^2 + 5t + 12$. Here $\epsilon = e_0 + e_1\rho + e_2\omega$, where $\deg(e_0) = 1554$, $\deg(e_1) = 1551$, and $\deg(e_2) = 1552$, so by Lemma 7.4, $|\epsilon| = 17^{1554}$, a number of 3109 decimal digits. The period of ϵ is 775. It took just under 15 CPU minutes to compute ϵ.

For the examples given in Table 1, we randomly generated monic polynomials $G, H \in \mathbb{F}_p[t]$ so that $\deg(GH^2) \equiv 0 (\mathrm{mod}\ 3)$, G and H are both squarefree, and $\gcd(G, H) = 1$. Each row of the table specifies the prime p, the polynomials G and H, the period l of the fundamental unit ϵ of $K = \mathbb{F}_p(t, \sqrt[3]{GH^2})$, the regulator R of K, and the CPU time required to compute R.

TABLE 1. Regulator Computations

p	G	H	l	R	**Time**
5	$t+4$	$t^7+t^6+t^5+4t^4+2t^3+t^2+t+1$	6387	6655	38.52 sec
5	t^2+t	$t^5+4t^4+t^3+2t^2+4$	743	770	3.80 sec
5	t^2+4t+2	$t^8+t^7+3t^5+3t^4+3t^3+2t^2+t+2$	57105	59501	8 min 13 sec
5	t^3+t^2+4t+1	t^3+2t^2+3t+1	347	361	1.54 sec
5	$t^4+3t^3+t^2+2$	$t+4$	36	38	0.09 sec
5	$t^4+t^3+2t^2+3t+3$	t^4+t^2+2t+3	2834	2950	17.31 sec
5	$t^5+t^4+3t^3+2t^2+2t+4$	$t^5+t^4+4t^3+4t^2+3$	251783	262322	37 min 9 sec
11	$t+2$	$t^4+7t^3+9t^2+9t+9$	479	484	1.53 sec
11	$t+4$	$t^7+4t^6+2t^5+9t^3+t^2+4t+10$	189893	191487	22 min 58 sec
11	t^2+9t+8	t^2+5	21	22	0.05 sec
11	t^3+4t^2+7t+8	t^3+2t^2+t+1	855	870	3.97 sec
11	t^4+10t^2+2t+6	$t^4+2t^3+10t^2+6t+6$	122619	123718	15 min 7 sec
11	$t^5+2t^4+8t^3+t^2+t+2$	t^2+4t+8	61702	62204	8 min 45 sec
17	$t+1$	$t^4+15t^3+16t^2+16t+11$	587	588	2.29 sec
17	$t^2+9t+15$	t^2+3t+3	45	46	0.11 sec
17	$t^3+9t^2+12t+2$	t^3+5t^2+3t+5	31987	32077	2 min 40 sec
17	$t^4+15t^3+12t^2+14t+6$	$t+3$	892	894	3.38 sec
17	$t^5+3t^4+13t^3+15t^2+7t+13$	t^2+6t+3	562601	564510	58 min 3 sec
23	$t+3$	$t^4+3t^3+17t+13$	1145	1146	4.20 sec
23	$t^2+22t+13$	$t^2+17t+22$	93	94	0.25 sec
23	t^3+5t+2	t^3+22t^2+2t+2	102347	102553	8 min 42 sec
23	$t^4+22t^3+16t^2+4t+4$	$t+7$	4251	4256	16.50 sec
23	$t^5+15t^4+16t^3+16t^2+4t+16$	$t^2+21t+10$	744378	745808	1 h 21 min
29	$t^2+24t+14$	$t^2+17t+13$	298	299	0.77 sec
29	$t^3+24t^2+12t+24$	$t^3+16t^2+10t+1$	80008	80103	7 min 3 sec
29	$t^4+22t^3+17t^2+12$	$t+5$	8508	8520	33.62 sec
29	$t^5+27t^4+13t^3+10t^2+23t+3$	$t^2+4t+17$	1483564	1485310	2 h 44 min

TABLE 1. (Continued)

p	G	H	l	R	**Time**
41	$t^2+23t+26$	$t^2+12t+4$	291	292	0.77 sec
41	$t^4+15t^3+4t^2+37t+14$	$t+28$	24238	24248	1 min 37 sec
41	$t^3+30t^2+35t+9$	$t^3+29t^2+15t+38$	961413	962005	1 h 25 min
71	$t^2+19t+63$	$t^2+29t+66$	550	551	1.50 sec
71	$t^4+9t^3+9t^2+3t+20$	$t+56$	41058	41064	2 min 49 sec
71	$t^3+30t^2+37t+2$	$t^3+13t^2+66t+34$	1408409	1408658	2 h 7 min
89	$t^2+8t+56$	$t^2+22t+67$	1317	1318	3.87 sec
89	$t^4+23t^3+50t^2+67t+35$	$t+79$	116511	116520	8 min 1 sec
107	$t^2+58t+74$	$t^2+54t+86$	3862	3863	11.98 sec
197	$t^2+27t+125$	$t^2+65t+158$	6525	6526	20.20 sec
401	$t^2+51t+400$	$t^2+71t+59$	26925	26926	1 min 24 sec
797	$t^2+526t+353$	$t^2+765t+687$	70680	70681	3 min 42 sec
983	$t^2+15t+279$	$t^2+740t+864$	107574	107575	5 min 33 sec

We point out that for small genus and large field of constants, knowledge of the regulator sometimes uniquely determines the divisor class number h of the field, or at least narrows h down to only a few possible values. By (2.1), h is a multiple of R. We also have the inequality $(\sqrt{q}-1)^{2g} \le h \le (\sqrt{q}+1)^{2g}$, already used in the proof of Theorem 6.5. Usually, there are only a few multiples of R that fall within these bounds. For example, the last five examples in Table 1 each permit only three possible values for h. We plan to investigate the computation of a suitable approximation of h by means of truncated Euler products in a forthcoming paper.

ACKNOWLEDGMENTS

The authors wish to thank an anonymous referee for helpful suggestions. The second author is grateful to Hugh C. Williams for inviting him to the University of Manitoba for post-doctoral work, during which time this paper was written.

REFERENCES

1. J. A. Buchmann, A generalization of Voronoi's algorithm I, II. *J. Number Theory* **20** (1985), 177–209. MR **86g:**11062a,b
2. J. A. Buchmann, The computation of the fundamental unit of totally complex quartic orders. *Math. Comp.* **48** (1987), 39–54. MR **87m:**11126
3. J. A. Buchmann, On the computation of units and class numbers by a generalization of Lagrange's algorithm. *J. Number Theory* **26** (1987), 8–30. MR **89b:**11104
4. J. A. Buchmann, On the period length of the generalized Lagrange algorithm. *J. Number Theory* **26** (1987), 31–37. MR **88g:**11078
5. J. A. Buchmann, *Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper*. Habilitationsschrift, Universität Düsseldorf, Germany 1987.

6. J. A. Buchmann & H. C. Williams, On the infrastructure of the principal ideal class of an algebraic number field of unit rank one. *Math. Comp.* **50** (1988), 569–579. MR **89g:**11098
7. B. N. Delone & D. K. Faddeev, *The Theory of Irrationalities of the Third Degree.* Transl. Math. Monographs **10**, Amer. Math. Soc., Providence, Rhode Island 1964. MR **28:**3955
8. M. Deuring, *Lectures on the Theory of Algebraic Functions in One Variable.* Lect. Notes in Math. **314**, Springer, Berlin 1973. MR **49:**8970
9. E. Jung, *Theorie der Algebraischen Funktionen einer Veränderlichen.* Berlin 1923.
10. M. Mang, *Berechnung von Fundamentaleinheiten in algebraischen, insbesondere reinkubischen Kongruenzfunktionenkörpern.* Diplomarbeit, Universität des Saarlandes, Saarbrücken, Germany 1987.
11. M. Pohst & H. Zassenhaus, *Algorithmic Algebraic Number Theory.* Cambridge University Press, 1st paperback ed., Cambridge 1997. MR **98f:**11111
12. F. K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik *p*. *Math. Zeitschrift* **33** (1931), 1–32.
13. D. Shanks, The infrastructure of a real quadratic field and its applications. *Proc. 1972 Number Theory Conf.*, Boulder, Colorado 1972, 217–224. MR **52:**10672
14. A. Stein, *Baby Step-Giant Step-Verfahren in reell-quadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2.* Diplomarbeit, Universitat des Saarlandes, Saarbrücken, Germany 1992.
15. A. Stein & H. C. Williams, Some methods for evaluating the regulator of a real quadratic function field. To appear in *Exp. Math.*
16. H. Stichtenoth, *Algebraic Function Fields and Codes.* Springer, Berlin 1993. MR **94k:**14016
17. G. F. Voronoi, *On a Generalization of the Algorithm of Continued Fractions* (in Russian). Doctoral Dissertation, Warsaw 1896.
18. B. Weis & H. G. Zimmer, Artins Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen. *Mitt. Math. Ges. Hamburg* **XII** (1991), 261–286. MR **93e:**11141
19. H. C. Williams, Continued fractions and number-theoretic computations. *Rocky Mountain J. Math.* **15** (1985), 621–655. MR **87h:**11129
20. H. C. Williams, G. Cormack & E. Seah, Calculation of the regulator of a pure cubic field. *Math. Comp.* **34** (1980), 567–611. MR **81d:**12003
21. H. C. Williams, G. W. Dueck & B. K. Schmid, A rapid method of evaluating the regulator and class number of a pure cubic field. *Math. Comp.* **41** (1983), 235–286. MR **84m:**12010
22. H. C. Williams & M. C. Wunderlich, On the parallel generation of the residues for the continued fraction algorithm. *Math. Comp.* **48** (1987), 405–423. MR **88i:**11099

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF DELAWARE, NEWARK, DE 19716
E-mail address: scheidle@math.udel.edu

DEPARTMENT OF COMBINATORICS & OPTIMIZATION, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO N2L 3G1, CANADA
E-mail address: astein@cacr.math.uwaterloo.ca