JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

RENATE SCHEIDLER

Ideal arithmetic and infrastructure in purely cubic function fields

Journal de Théorie des Nombres de Bordeaux, tome 13, n^{o} 2 (2001), p. 609-631

<http://www.numdam.org/item?id=JTNB_2001__13_2_609_0>

Journal de Théorie des Nombres
de Bordeaux **13** (2001), 609–631

Ideal arithmetic and infrastructure in purely cubic function fields

par Renate SCHEIDLER

RÉSUMÉ. Dans cet article, nous étudions l'arithmétique des idéaux fractionnnaires dans les corps de fonctions cubiques purs, ainsi que l'infrastructure de la classe des idéaux principaux lorsque le groupe des unités du corps est de rang 1. Nous décrivons d'abord la décomposition des polynômes irréductibles dans l'ordre maximal du corps. Nous construisons ensuite des bases d'idéaux, dites canoniques, bien adaptées pour les calcul. Nous énonçons des algorithmes permettant de multiplier les idéaux, et même de les réduire lorsque le groupe des unités est de rang 1 et la caractéristique au moins 5, L'article se termine avec une analyse de l'infrastructure de l'ensemble des idéaux fractionnaires réduits principaux dans le cas des corps cubiques purs de groupe des unités de rang 1 et de caractéristique au moins 5.

ABSTRACT. This paper investigates the arithmetic of fractional ideals of a purely cubic function field and the infrastructure of the principal ideal class when the field has unit rank one. First, we describe how irreducible polynomials decompose into prime ideals in the maximal order of the field. We go on to compute so-called canonical bases of ideals; such bases are very suitable for computation. We state algorithms for ideal multiplication and, in the case of unit rank one and characteristic at least five, ideal reduction. The paper concludes with an analysis of the infrastructure in the set of reduced fractional principal ideals of a purely cubic function field of unit rank one and characteristic at least five.

1. Introduction

The infrastructure of a number field of unit rank one refers to the structure of the set of reduced representatives in an equivalence class of ideals in the maximal (or any) order of the field: informally speaking, while this set does not form a group under the operation multiplication with subsequent reduction — the associative law does not hold — it behaves "almost" like

Manuscrit reçu le 19 octobre 1999.

a group. First discovered for real quadratic fields by Shanks [3], who gave it its name, it has since been used as the basis for many number theoretic algorithms, including regulator, class number, and class group computation. More recently, it was discovered that elliptic and hyperelliptic (i.e. quadratic) function fields share many similarities with their number field counterparts, and that real quadratic function fields exhibit an infrastructure much like that of real quadratic number fields. As in the number field case, this infrastructure can be used to compute the regulator and the ideal class number of these fields [6].

While there are only three types of number fields of unit rank one — real quadratic, complex cubic, and totally complex quartic fields — there are function fields of arbitrarily high degree that have a representation as a unit rank one extension of some field of rational functions over a finite field; presumably, many or perhaps all of these fields exhibit some kind of infrastructure. This is certainly the case for purely cubic function field representations of unit rank one, the function field analogue of purely cubic number fields. Ideal arithmetic and the infrastructure in purely cubic number fields were investigated by Williams et al. in [11, 12, 10], and much of the work in this paper was guided by these sources. As in the case of quadratic function fields, the infrastructure can be used to compute the regulator and the ideal class number, and hence the order of the group of rational points of the Jacobian of a purely cubic function field.

For a general introduction to function fields, we refer the reader to [7]. Purely cubic function fields are discussed in detail in [5]. Let $k = \mathbb{F}_q$ be a finite field of order q whose characteristic is not equal to 3. Denote by $k[x]$ and $k(x)$ the ring of univariate polynomials and the field of rational functions, respectively, over k in the indeterminate x. Let $D = D(x) \in k[x]$ be a cubefree polynomial, write $D = GH^2$ with $G, H \in k[x]$ squarefree and coprime. We choose a cube root ρ of D in some algebraic closure of $k(x)$. Then the field $K = k(x, \rho)$ is a *purely cubic function field*; it is the function field of the plane curve $y^3 - D(x) = 0$ over k and is an extension of degree 3 over $k(x)$. We assume that the leading coefficient $\operatorname{sgn}(D)$ of D is a cube in $k^* = k \setminus \{0\}$; this can always be achieved by replacing k by a suitable cubic extension of k if necessary.

The *ring of integer functions* or *maximal order* of $K/k(x)$ is the integral closure $\mathcal{O}$ of $k[x]$ in K. $\mathcal{O}$ is a $k[x]$-module of rank 3 that is generated by the *integral basis* $\{1, \rho, \omega\}$ where $\omega = \rho^2/H$, so ω is a cube root of G^2H. The *discriminant* of $K/k(x)$ is $\Delta = -27G^2H^2$. The *unit group* of $K/k(x)$, i.e. the group of units $\mathcal{O}^*$ of the ring $\mathcal{O}$, is an Abelian group with torsion part k^*; it is equal to k^* if $\deg(D)$ is not a multiple of 3 and infinite otherwise. In the latter case, the *unit rank* of $K/k(x)$ is the rank of this group; it is 1 if $q \equiv -1 \bmod 3$ and 2 if $q \equiv 1 \bmod 3$ (see Theorem 2.1 of [5]). An independent set of generators of the torsionfree part of $\mathcal{O}^*$ is a system of *fundamental units* of $K/k(x)$.

If $\mathcal{O}^*$ is infinite, then it is possible to choose ρ in the field $k\langle x^{-1}\rangle$ of *Puiseux series* over k; nonzero elements in $k\langle x^{-1}\rangle$ have the form $\alpha = \sum_{i=-m}^{\infty} a_i x^{-i} = \sum_{i=-\infty}^{m} a_{-i} x^i$. The degree valuation on $k(x)$ extends canonically to $k\langle x^{-1}\rangle$ (and hence to K) via $\deg(\alpha) = m$. We also set $|\alpha| = q^{\deg(\alpha)}$ and $\lfloor \alpha \rfloor = \sum_{i=0}^{m} a_{-i} x^i$ (with $|0| = 0$ and $\lfloor 0 \rfloor = 0$).

Elements in K and in $\mathcal{O}$ are represented in terms of the integral basis $\{1, \rho, \omega\}$ of $K/k(x)$. If $\alpha = a + b\rho + c\omega \in K$, denote the *conjugates* of α by $\alpha' = a + b\iota\rho + c\iota^2\omega$ and $\alpha'' = a + b\iota^2\rho + c\iota\omega$ where ι is a fixed primitive cube root of unity. Since $\iota \in k$ if and only if $q \equiv 1 \bmod 3$, it follows that $\alpha', \alpha'' \in K$ if $q \equiv 1 \bmod 3$, whereas $\alpha', \alpha'' \notin K$, but $\alpha'\alpha'' \in K$, if $q \equiv -1 \bmod 3$. In the latter case, set $\deg(\alpha') = \deg(\alpha'\alpha'')/2$ and $|\alpha'| = q^{\deg(\alpha')} = |\alpha'\alpha''|^{1/2}$. The *norm* of α is $N(\alpha) = \alpha\alpha'\alpha'' = a^3 + b^3GH^2 + c^3G^2H - 3abcGH \in k(x)$.

The above introduction enables us to compare purely cubic function fields with their number field analogues and point out similarities as well as differences between the two. We recall that a purely cubic number field has the form $K = \mathbb{Q}(\sqrt[3]{D})$ with $D = GH^2$ where $G, H \in \mathbb{Z}$ are squarefree and coprime. While $K/\mathbb{Q}$ is always a cubic extension, regardless of the generator, a purely cubic function field K can have representations as an extension of some rational function field $k(x)$ that are not cubic, although K/k will always have transcendence degree 1. Once a purely cubic representation has been fixed, the integral basis $\{1, \rho, \omega\}$, maximal order $\mathcal{O}$, discriminant Δ, and the definitions of conjugates and norm are essentially the same as in the number field setting. However, while purely cubic number fields are complex cubic fields and thus always have unit rank one, the corresponding function fields can have unit rank 0, 1, or 2. The case of unit rank 1 is similar to the number field situation in many respects, generally exhibiting large regulators (where the regulator is half the degree of the fundamental unit of positive degree), small ideal class numbers, and an infrastructure on the set of reduced principal fractional ideals that is discussed in this paper. Embedding K into the field of Puiseux series is akin to embedding a purely cubic number field into the reals; however, the valuation $|\cdot|$ is discrete, i.e. nonarchimedian. Consequently, the results on ideal reduction and the infrastructure are somewhat simpler and cleaner in the function field setting.

The discussion of ideals, their decomposition into prime ideals, ideal bases, and ideal multiplication in Sections 2 – 5 is essentially the same as for number fields, and the results in these sections hold for purely cubic function fields of any unit rank. In Sections 6 (on ideal reduction) and 7 (on the infrastructure in the set of reduced principal ideals), we will restrict ourselves to the case of unit rank 1 and characteristic at least 5.

2. Ideals and fractional ideals

An (*$\mathcal{O}$-integral*) *ideal* is a subset $\mathfrak{a}$ of $\mathcal{O}$ such that $\alpha + \beta \in \mathfrak{a}$ and $\theta\alpha \in \mathfrak{a}$ for all $\alpha, \beta \in \mathfrak{a}$ and $\theta \in \mathcal{O}$. A(n *$\mathcal{O}$-)fractional ideal* is a subset $\mathfrak{f}$ of K such that there exists a nonzero $d \in k[x]$ such that $d\mathfrak{f}$ is an integral ideal. Note that every integral ideal is also a fractional ideal. Every fractional ideal $\mathfrak{f}$ is *generated* by at most two elements $\theta, \phi \in K$; that is, $\mathfrak{f} = \{\alpha\theta + \beta\phi \mid \alpha, \beta \in \mathcal{O}\}$. Write $\mathfrak{f} = (\theta, \phi)$. If $\mathfrak{f}$ is generated by only one element θ, then $\mathfrak{f}$ is *principal*; write $\mathfrak{f} = (\theta)$. Nonzero fractional ideals are $k[x]$-modules of rank 3; if $\{\lambda, \mu, \nu\}$ is a $k[x]$-basis of a fractional ideal $\mathfrak{f}$, write $\mathfrak{f} = [\lambda, \mu, \nu]$. The *discriminant* of $\mathfrak{f}$ is the rational function

$$\Delta(\mathfrak{f}) = \det \begin{pmatrix} \lambda & \lambda' & \lambda'' \\ \mu & \mu' & \mu'' \\ \nu & \nu' & \nu'' \end{pmatrix}^2 ;$$

it is independent of the choice of $k[x]$-basis of $\mathfrak{f}$ up to a factor that is a square in k^*.

Henceforth, all ideals (fractional and integral) are assumed to be nonzero, so the term "ideal" will always be synonymous with "nonzero ideal". The product of two fractional ideals $\mathfrak{f}_1 = (\theta_1, \phi_1)$ and $\mathfrak{f}_2 = (\theta_2, \phi_2)$ is the fractional ideal $\mathfrak{f}_1\mathfrak{f}_2 = (\theta_1\theta_2, \theta_1\phi_2, \phi_1\theta_2, \phi_1\phi_2)$. Two nonzero fractional ideals are *equivalent* if they differ by a factor that is a principal fractional ideal; this is easily seen to be an equivalence relation. The set of equivalence classes is a finite Abelian group under multiplication of representatives, the *ideal class group* of $K/k(x)$; its order h' is the *ideal class number* of $K/k(x)$.

An integral ideal is *primitive* if it is not contained in any nontrivial principal integral ideal (f) with $f \in k[x]$. The unique monic polynomial of minimal degree contained in a primitive integral ideal $\mathfrak{a}$ is denoted by $L(\mathfrak{a})$; it is the greatest common divisor of all polynomials in $\mathfrak{a}$ and can always be included in a $k[x]$-basis of $\mathfrak{a}$ (see Section 3 of [5]). Similarly, if a fractional ideal $\mathfrak{f}$ contains 1, then 1 can always be included in a $k[x]$-basis of $\mathfrak{f}$.

Primitive ideals and fractional ideals that contain 1 are in one-to-one correspondence as follows: to a primitive ideal $\mathfrak{a} = [L(\mathfrak{a}), \alpha, \beta]$ corresponds the unique fractional ideal $\mathfrak{f}_{\mathfrak{a}} = (L(\mathfrak{a})^{-1})\mathfrak{a} = [1, \alpha/L(\mathfrak{a}), \beta/L(\mathfrak{a})]$. Conversely, let $\mathfrak{f} = [1, \mu, \nu]$ be a fractional ideal where $\mu = (m_0 + m_1\rho + m_2\omega)/d$ and $\nu = (n_0 + n_1\rho + n_2\omega)/d$ with $m_0, m_1, m_2, n_0, n_1, n_2, d \in k[x]$, d monic, and $\gcd(m_0, m_1, m_2, n_0, n_1, n_2, d) = 1$. Then to $\mathfrak{f}$ corresponds the unique primitive integral ideal $\mathfrak{a}_{\mathfrak{f}} = d\mathfrak{f} = [d, d\mu, d\nu]$. The polynomial $d = d(\mathfrak{f})$ is unique and is the *denominator* of $\mathfrak{f}$. We have $d(\mathfrak{f}) = L(\mathfrak{a}_{\mathfrak{f}})$ and $L(\mathfrak{a}) = d(\mathfrak{f}_{\mathfrak{a}})$.

The *norm* of a fractional ideal $\mathfrak{f} = [1, (m_0 + m_1\rho + m_2\omega)/d, (n_0 + n_1\rho + n_2\omega)/d]$ (m_0, m_1, m_2, n_0, n_1, n_2, $d \in k[x]$ jointly coprime) is $N(\mathfrak{f}) = a(m_1n_2 - m_2n_1)/d^2 \in k(x)$ where $a \in k^*$ is chosen so that $N(\mathfrak{f})$ is monic. $N(\mathfrak{f})$ is independent of the $k[x]$-basis of $\mathfrak{f}$. We have $\Delta(\mathfrak{f}) = bN(\mathfrak{f})^2\Delta$ for some $b \in k^*$ and $N(\mathfrak{f}_1\mathfrak{f}_2) = N(\mathfrak{f}_1)N(\mathfrak{f}_2)$ for fractional ideals $\mathfrak{f}_1, \mathfrak{f}_2$ of $\mathcal{O}$. If $\mathfrak{a}$ is an integral ideal, then $L(\mathfrak{a}) \mid N(\mathfrak{a})$. If in addition, $\mathfrak{a}$ is primitive, then $N(\mathfrak{a}) \mid L(\mathfrak{a})^2$.

3. Prime ideals

Voronoi [8] found bases of all prime ideals of a purely cubic number field, their powers, and certain products of their powers. His results, easily adapted to the function field setting, are stated here without proof:

Theorem 3.1. *Let $P \in k[x]$ be an irreducible polynomial. Then the principal ideal (P) splits into prime ideals in $\mathcal{O}$ as follows:*

1. *If $P \mid G$, then $(P) = \mathfrak{p}^3$ where $\mathfrak{p} = [P, \rho, \omega]$ and $\mathfrak{p}^2 = [P, P\rho, \omega]$. $\mathfrak{p}$ is called a* type 1 *prime ideal.*
2. *If $P \mid H$, then $(P) = \mathfrak{p}^3$ where $\mathfrak{p} = [P, \rho, \omega]$ and $\mathfrak{p}^2 = [P, \rho, P\omega]$. $\mathfrak{p}$ is called a* type 2 *prime ideal.*
3. *If $P \nmid GH$, D is a cube* $\bmod P$, *and $q^{\deg(P)} \equiv -1 \bmod 3$, then D has a unique cube root X mod P in $k[x]$. In this case, $(P) = \mathfrak{p}\mathfrak{q}$ where*

$$\mathfrak{p}^i = [P^i, -X_i + \rho, -X_i^2 Y_i + \omega], \quad \mathfrak{q}^i = [P^i, P^i\rho, X_i^2 Y_i + X_i Y_i \rho + \omega]$$

for $i \in \mathbb{N}$ with

$$X_1 \equiv \begin{cases} X & \bmod P, \\ 0 & \bmod H, \end{cases} \quad \textit{or equivalently, } X_1 \equiv XY_1H \bmod PH$$

and

$$\begin{aligned} X_{i+1} &= X_i + A_i(D - X_i^3) \quad \textit{where } 3X_i^2 A_i \equiv 1 \bmod P^i, \\ Y_i H &\equiv 1 \bmod P^i \end{aligned}$$

for $i \in \mathbb{N}$. Note that $X_i, Y_i \in k[x]$, $X_i^3 \equiv D \bmod P^i$ and $X_i \equiv 0 \bmod H$ for all $i \in \mathbb{N}$. $\mathfrak{p}$ and $\mathfrak{q}$ are called type 3 *prime ideals.*

4. *If $P \nmid GH$, D is a cube* $\bmod P$, *and $q^{\deg(P)} \equiv 1 \bmod 3$, then D has three distinct cube roots X, X', X'' mod P in $k[x]$. In this case, $(P) = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ where*

$$\begin{aligned} \mathfrak{p}^i &= [P^i, -X_i + \rho, -X_i^2 Y_i + \omega], \\ (\mathfrak{p}\mathfrak{p}')^i &= [P^i, P^i\rho, (X_i'')^2 Y_i + X_i'' Y_i \rho + \omega], \\ \mathfrak{p}^{i+j}(\mathfrak{p}')^i &= [P^{i+j}, P^i(-X_j + \rho), (X_i'')^2 Y_i + P^i Q_{ij} + X_i'' Y_i \rho + \omega] \end{aligned}$$

for $i, j \in \mathbb{N}$ with

$$X_1 \equiv \begin{cases} X & \bmod P, \\ 0 & \bmod H \end{cases} \quad \textit{or equivalently, } X_1 \equiv XY_1H \bmod PH$$

and

$$\begin{aligned} X_{i+1} &= X_i + A_i(D - X_i^3) \quad \textit{where } 3X_i^2 A_i \equiv 1 \bmod P^i, \\ Y_i H &\equiv 1 \bmod P^i, \\ Q_{ij}(X_j - X_i'')/H &\equiv (X_i''^3 - D)/H^2 P^i \bmod P^j \end{aligned}$$

for $i, j \in \mathbb{N}$. Analogous congruences hold for X_i' and X_i'' (with corresponding A_i' and A_i'', respectively), and similar bases can be found for $(\mathfrak{p}')^i$, $(\mathfrak{p}'')^i$, $(\mathfrak{p}\mathfrak{p}'')^i$, $(\mathfrak{p}'\mathfrak{p}'')^i$, $\mathfrak{p}^{i+j}(\mathfrak{p}'')^i$, $(\mathfrak{p}')^{i+j}\mathfrak{p}^i$, $(\mathfrak{p}')^{i+j}(\mathfrak{p}'')^i$, $(\mathfrak{p}'')^{i+j}\mathfrak{p}^i$, $(\mathfrak{p}'')^{i+j}(\mathfrak{p}')^i$ for $i, j \in \mathbb{N}$. Note that $X_i, X_i', X_i'', Y_i, Q_{ij} \in k[x]$, $X_i^3 \equiv (X_i')^3 \equiv (X_i'')^3 \equiv D \bmod P^i$ and $X_i \equiv X_i' \equiv X_i'' \equiv 0 \bmod H$ for all $i \in \mathbb{N}$. $\mathfrak{p}$ and $\mathfrak{q}$ are called type 4 *prime ideals.*

5. *If D is not a cube* mod P, *then $(P) = \mathfrak{p}$ is inert. Here, $\mathfrak{p} = [P, P\rho, P\omega]$. $\mathfrak{p}$ is called a* type 5 *prime ideal.*

Note that if $q \equiv 1 \bmod 3$, then K does not contain any type 3 prime ideals.

4. Canonical bases and ideal multiplication

In this section, we introduce two special types of $k[x]$-module bases (which we call "triangular" and "canonical", respectively) that lend themselves well to computation. For primitive ideals, such bases always exist, and the two types of bases will turn out to be the same. We describe how to find such a basis, determine containment and equality of ideals using triangular bases, and compute the product of two coprime ideals using triangular bases. We also show that a nonzero $k[x]$-module is a primitive ideal if and only if it has a triangular basis that is also canonical, in which case all of its triangular bases are canonical. Several of the results in the next two sections as well as their derivations are analogous to the number field case discussed in [12], so we omit some of the details here.

We define a basis of a $k[x]$-module in $\mathcal{O}$ to be *triangular* if it is of the form

$$\{s, s'(u+\rho), s''(v + w\rho + \omega)\} \text{ with } s, s', s'', u, v, w \in k[x] \text{ and } ss's'' \neq 0.$$

Let $\{s, \alpha, \beta\}$ be a triangular basis of a primitive ideal $\mathfrak{a}$ with $\alpha = s'(u+\rho)$ and $\beta = s''(v+w\rho+\omega)\}$. Then $s\rho \in \mathfrak{a}$ implies $s' \mid s$; similarly, $s\omega \in \mathfrak{a}$ implies $s'' \mid s$. Since $\mathfrak{a}$ is primitive, we must have $\gcd(s', s'') = 1$. Furthermore, $s = \operatorname{sgn}(s)L(\mathfrak{a})$, and $ss's'' = \operatorname{sgn}(ss's'')N(\mathfrak{a})$.

Triangular bases provide an easy means for comparing modules and primitive ideals.

Lemma 4.1. *Let $\mathfrak{a}_1 = [s_1, s_1'(u_1+\rho), s_1''(v_1+w_1\rho+\omega)]$ and $\mathfrak{a}_2 = [s_2, s_2'(u_2+\rho), s_2''(v_2+w_2\rho+\omega)]$ be two $k[x]$-modules given in terms of triangular bases.*

1. $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$ *if and only if*

$$\begin{array}{rcl} s_2 & \mid & s_1, \qquad s_2' \mid s_1', \qquad s_2'' \mid s_1'', \\ s_1' u_1 & \equiv & s_1' u_2 \bmod s_2, \\ s_1'' w_1 & \equiv & s_1'' w_2 \bmod s_2', \\ s_1'' v_1 & \equiv & s_1''(v_2 + u_2(w_1 - w_2)) \bmod s_2. \end{array}$$

2. If $\mathfrak{a}_1$ *and* $\mathfrak{a}_2$ *are primitive ideals, then* $\mathfrak{a}_1 = \mathfrak{a}_2$ *if and only if*

$$\begin{array}{rcl} s_1 & = & a s_2, \qquad s_1' = a' s_2', \qquad s_1'' = a'' s_2'' \qquad (a, a', a'' \in k^*), \\ u_1 & \equiv & u_2 \bmod s_1/s_1', \\ w_1 & \equiv & w_2 \bmod s_1', \\ v_1 & \equiv & v_2 + u_2(w_1 - w_2)) \bmod s_1/s_1''. \end{array}$$

Every primitive ideal in $\mathcal{O}$ has a triangular basis which can be easily be found:

Lemma 4.2. *Let* $\mathfrak{a} = [L(\mathfrak{a}), \mu, \nu]$ *be a primitive ideal where* $\mu = m_0 + m_1\rho + m_2\omega$, $\nu = n_0 + n_1\rho + n_2\omega$ *with* $m_0, m_1, m_2, n_0, n_1, n_2 \in k[x]$. *Then* $\mathfrak{a}$ *has a triangular basis which can be obtained as follows. Set*

$$s'' = \gcd(m_2, n_2), \qquad s' = (m_1 n_2 - n_1 m_2)/s'', \qquad s = L(\mathfrak{a}),$$

and let $a', b', t \in k[x]$ *satisfy* $a'm_2 + b'n_2 = s''$ *and* $s't \equiv a'm_1 + b'n_1 \bmod s''$. *Set* $a = a' - tn_2/s''$, $b = b' + tm_2/s''$,

$$u = \frac{m_0 n_2 - n_0 m_2}{s's''}, \qquad v = \frac{a m_0 + b n_0}{s''}, \qquad w = \frac{a m_1 + b n_1}{s''}.$$

Then $\{s, s'(u + \rho), s''(v + w\rho + \omega)\}$ *is a triangular basis of* $\mathfrak{a}$.

Proof. Since $N(\mathfrak{a}) \mid L(\mathfrak{a})^2$, we have $s's'' \mid s$. Let $U = (m_0 n_2 - n_0 m_2)/s''$, $V = a'm_0 + b'n_0$, and $W = a'm_1 + b'n_1$. Then $U, V, W \in k[x]$, and if $\alpha = (n_2\mu - m_2\nu)/s'' = U + s'\rho$ and $\beta = a'\mu + b'\nu = V + W\rho + s''\omega$, then $\{s, \alpha, \beta\}$ is a basis of $\mathfrak{a}$. Since $\beta\rho \in \mathfrak{a}$, we have $s'' \mid WH$; similarly, $\beta\omega$ implies $s'' \mid V$, and $s \mid WGH$. By expressing $\alpha\rho$ and $\alpha\omega$ in terms of s, α, and β, we see that $s' \mid U$.

Now suppose s' and s'' had an irreducible common divisor $p \in k[x]$. Then $p^2 \mid s's'' \mid s \mid WGH$, so $p \mid W$ and hence $(p) \mid \mathfrak{a}$, contradicting the primitivity of $\mathfrak{a}$. So $\gcd(s', s'') = 1$ and t as given above exists. Now $\{s, \alpha, \beta - t\alpha\}$ is the desired triangular basis. □

We note that by part 2 of Lemma 4.1, all other triangular basis (up to constant factors in the basis elements) are given by

$$\{s, s'(\tilde{u} + \rho), s''(\tilde{v} + \tilde{w}\rho + \omega)\}$$

where

$$\tilde{u} \equiv u \bmod s/s', \quad \tilde{w} = w \bmod s', \quad \tilde{v} \equiv v + u(\tilde{w} - w) \bmod s/s''.$$

Example 4.3. Let $k = \mathbb{F}_2$, $G(x) = x^4 + x + 1$, $H(x) = x + 1$, so $D(x) = x^6 + x^4 + x^3 + x^2 + x + 1$. We wish to find a triangular basis $\{s, s'(u + \rho), s''(v + w\rho + \omega)\}$ of the ideal $\mathfrak{a} = [x, (x + 1) + (x^2 + x + 1)\rho + \omega, 1 + (x^3 + x + 1)\rho + (x + 1)\omega]$. According to Lemma 4.2, $s'' = \gcd(1, x + 1) = 1$, $s' = (x^2 + x + 1)(x + 1) + (x^3 + x + 1) \cdot 1 = x$, and $s = x$. We set $a = 1$ and $b = 0$, then $u = x$, $v = x + 1$, and $w = x^2 + x + 1$. By the remark following Lemma 4.2, $\mathfrak{a} = [x, x(x + \rho), (x + 1) + (x^2 + x + 1)\rho + \omega] = [x, x\rho, 1 + \rho + \omega]$.

Theorem 4.4. *Let* $\mathfrak{a}_1 = [s_1, s_1'(u_1 + \rho), s_1''(v_1 + w_1\rho + \omega)]$ *and* $\mathfrak{a}_2 = [s_2, s_2'(u_2 + \rho), s_2''(v_2 + w_2\rho + \omega)]$ *be two primitive ideals given in terms of triangular bases with* $\gcd(s_1, s_2) = 1$. *Then* $\{s_3, s_3'(u_3 + \rho), s_3''(v_3 + w_3\rho + \omega)\}$ *is a triangular basis of* $\mathfrak{a}_1\mathfrak{a}_2$ *where*

$$
\begin{aligned}
s_3 &= s_1 s_2, \qquad s_3' = s_1' s_2', \qquad s_3'' = s_1'' s_2'',\\
u_3 &\equiv \begin{cases} u_1 \bmod s_1/s_1', \\ u_2 \bmod s_2/s_2', \end{cases}\\
w_3 &\equiv \begin{cases} w_1 \bmod s_1', \\ w_2 \bmod s_2', \end{cases}\\
v_3 &\equiv \begin{cases} v_1 + u_1(w_3 - w_1) \bmod s_1/s_1'', \\ v_2 + u_2(w_3 - w_2) \bmod s_2/s_2''. \end{cases}
\end{aligned}
$$

Proof. Let $\{s_3, s_3'(u_3 + \rho), s_3''(v_3 + w_3\rho + \omega)\}$ be a triangular basis of $\mathfrak{a}_1\mathfrak{a}_2$ and assume that s_i, s_i', s_i'' are monic for $i = 1, 2, 3$. Since $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1, \mathfrak{a}_2$, by part 1 of Lemma 4.1 $s_1 s_2 \mid s_3$, $s_1' s_2' \mid s_3'$, $s_1'' s_2'' \mid s_3''$. Examining $N(\mathfrak{a}_1\mathfrak{a}_2)$ shows that these divisibilities are in fact all equalities. The congruences for u_3, v_3, w_3 also follow from part 1 of Lemma 4.1. □

Example 4.5. Let k, G, H be as in Example 4.3 and let $\mathfrak{a}_1 = [x^2, x + 1 + \rho, x + 1 + \omega]$, $\mathfrak{a}_2 = [(x + 1)(x^4 + x + 1), (x^4 + x + 1)\rho, (x + 1)\omega]$. Here, $\mathfrak{a}_1 = \mathfrak{p}^2$ where $\mathfrak{p}$ is the prime ideal divisor of degree 1 of the principal ideal (x), and $\mathfrak{a}_2 = \mathfrak{q}^2$ with $\mathfrak{q}^3 = (GH)$, so both $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are ideals. By Theorem 4.4, $\mathfrak{a}_1\mathfrak{a}_2 = [s, s'(u + \rho), s''(v + w\rho + \omega)]$ where $s = x^2(x + 1)(x^4 + x + 1)$, $s' = x^4 + x + 1$, $s'' = x + 1$, $w = 0$,

$$
u \equiv \begin{cases} x + 1 & \bmod x^2, \\ 0 & \bmod x + 1 \end{cases}, \qquad v \equiv \begin{cases} x + 1 & \bmod x^2, \\ 0 & \bmod x^4 + x + 1 \end{cases},
$$

so $u = x + 1$ and $v = x^4 + x + 1$.

We call a triangular basis $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$ of a $k[x]$-submodule of $\mathcal{O}$ *canonical* if and only if the following conditions hold.

$$(4.1)\quad s's'' \mid s, \quad \gcd\left(\frac{s}{s_G s_H}, GH\right) = 1, \quad \gcd(s', H) = 1, \quad s'' \mid H,$$

$$(4.2)\quad H(uw - v) \equiv u^2 \bmod s/s',$$

$$(4.3)\quad v \equiv Hw^2 \bmod s's_H/s'',$$

$$(4.4)\quad H(G - vw) \equiv u(v - Hw^2) \bmod s,$$

where $s_G = \gcd(s, G)$ and $s_H = \gcd(s, H)$.

It is easily seen that all the prime ideals of types 1–4 and their primitive powers have canonical bases. Canonical bases satisfy a number of additional divisibility conditions:

Lemma 4.6. *Let $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$ be a canonical basis of some $k[x]$-submodule of $\mathcal{O}$. Then*

$$(4.5)\quad s_H \mid u, \qquad (s_H/s'') \mid v$$

$$(4.6)\quad vw \equiv G \bmod s',$$

$$(4.7)\quad u(v - uw) \equiv GH \bmod s/s'$$

$$(4.8)\quad v(v + Hw^2) \equiv 2GHw + u(Hw^3 - G) \bmod s/s''.$$

$$(4.9)\quad u^3 \equiv -D \bmod s/s'$$

$$(4.10)\quad Hw^3 \equiv G \bmod s'$$

Proof. (4.5) and (4.6) are immediate consequences of (4.1) – (4.4). (4.7) is obtained by multiplying (4.2) by w and subtracting (4.4). Multiplying (4.2) by (4.3) produces $s \mid (Huw - Hv - u^2)(v - Hw^2)$. From (4.4), $s \mid GH - Hvw - uv + Huw^2$. Multiplying the latter by $2Hw - u$ and taking sums yields $s \mid H(v(v + Hw^2) - 2GHw - u(Hw^3 - G))$, so both s/s_H and s_H/s'' divide $v(v+Hw^2) - 2GHw - u(Hw^3 - G)$. Since by (4.1), s/s_H and s_H/s'' are coprime, (4.8) follows. Multiplying (4.4) by H, (4.2) by $u + Hw$, and taking differences generates (4.9). Finally, (4.10) follows directly from (4.3) and (4.6). □

Canonical bases characterize $k[x]$-modules as ideals:

Theorem 4.7. *A $k[x]$-module $\mathfrak{a}$ in $\mathcal{O}$ is a primitive ideal if and only if it has a triangular basis that is canonical. In this case, every triangular basis of $\mathfrak{a}$ is canonical.*

Proof. Let $\mathfrak{a}$ be a $k[x]$-module in $\mathcal{O}$. If $\mathfrak{a}$ is a primitive ideal, then $\mathfrak{a}$ has a triangular basis $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$ by Lemma 4.2. By Theorems 3.1 and 4.4, $\gcd(s/s_G s_H, GH) = 1$, and the fact that $\mathfrak{a}$ is closed under multiplication by ρ and ω implies the rest of (4.1) and (4.2) – (4.4). Conversely, if $\mathfrak{a}$ has a basis $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$ that satisfies (4.1) – (4.4), then it also satisfies (4.5) – (4.10). In this case, $\mathfrak{a}$ is closed under multiplication by ρ and ω, and $\mathfrak{a}$ is primitive by (4.1). The remainder of the theorem follows from part 2 of Lemma 4.1. □

Given the correspondence between primitive ideals and fractional ideals containing 1, all the above results can immediately be applied to the latter:

Theorem 4.8.

1. *Every fractional ideal containing 1 has a canonical basis, i.e. a basis of the form* $\{1, s'(u+\rho)/s, s''(v+w\rho+\omega)/s\}$ *where* $s, s', s'', u, v, w \in k[x]$ *satisfy (4.1) – (4.4) and hence (4.5) – (4.10). Here,* $s = \mathrm{sgn}(s)d(\mathfrak{f})$.
2. *If* $\{1, s_1'(u_1+\rho)/s_1, s_1''(v_1+w_1\rho+\omega)/s_1\}$ *and* $\{1, s_2'(u_2+\rho)/s_2, s_2''(v_2+w_2\rho+\omega)/s_2\}$ *are canonical bases of two fractional ideals* $\mathfrak{f}_1$ *and* $\mathfrak{f}_2$, *respectively, such that* $\gcd(s_1, s_2) = 1$, *then a canonical basis of the product ideal* $\mathfrak{f}_1\mathfrak{f}_2$ *is given by* $\{1, s_3'(u_3+\rho)/s_3, s_3''(v_3+w_3\rho+\omega)/s_3\}$ *where* $s_3, s_3', s_3'', u_3, v_3, w_3$ *are given as in Theorem 4.4.*
3. *If* $\{1, s'(u+\rho)/s, s''(v+w\rho+\omega)/s\}$ *is a basis of some* $k[x]$*-submodule* $\mathfrak{f}$ *of* K, *then* $\mathfrak{f}$ *is a fractional ideal if and only if the basis is canonical. In this case, every basis of* $\mathfrak{f}$ *of this form is canonical.*

5. Ideal squaring

In this section, we describe how to find a canonical basis of the square of a primitive ideal, given a canonical basis of the original ideal. We give a more detailed proof of the following lemma as it is slightly different from its number field equivalent due to the nature of our underlying finite field k of constants.

Lemma 5.1. *Let* $\{s, s'(u+\rho), v+w\rho+\omega\}$ *be a canonical basis of some ideal* $\mathfrak{a}$ *such that* $\gcd(s, GH) = 1$. *Then there exists* $f \in k[x]$ *such that if* $w' = w + fs'$ *and* $v' = v + fus'$, *then* $\{s, s'(u+\rho), v'+w'\rho+\omega\}$ *is also a canonical basis of* $\mathfrak{a}$ *and* $\gcd(2v' + H(w')^2, s) = 1$.

Proof. Note that $\gcd(s, GH) = 1$ implies that s'' can be chosen to be 1 in any canonical basis of $\mathfrak{a}$. If $w' = w + fs'$ and $v' = v + fus'$ with $f \in k[x]$ arbitrary, then $\{s, s'(u+\rho), v'+w'\rho+\omega\}$ is also a canonical basis of $\mathfrak{a}$ by part 2 of Lemma 4.1. Furthermore, $\gcd(2v' + H(w')^2, s') = 1$, for if $p \in k[x]$ is any irreducible polynomial divisor of this gcd, then by (4.3) $2v' + H(w')^2 \equiv 3v' \equiv 3H(w')^2 \bmod s'$, so $p \mid v'$ and $p \mid w'$ as $\gcd(s', H) = 1$. But then (4.4) would imply $p \mid GH$, contradicting $\gcd(s, GH) = 1$.

Suppose that $s/s' \notin k$ and let a be a square root of 3 (possibly in some extension of k). Choose $f \in k[x]$ so that $Hs'f \not\equiv (-1 \pm a)u - Hw \bmod p$ in $k(a)[x]$ for any irreducible polynomial p dividing s but not s' (such an f certainly exists). Set $w' = w + fs'$, $v' = v + fus'$, and let p be any irreducible divisor of s, but not s'. Then $Hw' \not\equiv (-1 \pm a)u \bmod p$, so

$$p \nmid (Hw' + u)^2 - 3u^2 = H^2(w')^2 + 2Huw' - 2u^2.$$

Now by (4.2), $Huw' - u^2 \equiv Hv' \bmod p$, so since $p \nmid H$: $p \nmid H(w')^2 + 2v'$. Thus, $\gcd(2v' + H(w')^2, s) = 1$. □

In practice, it is easy to find a suitable f by trial and error. $f = 0$ or $f \in k^*$ is almost always sufficient.

We now have all the tools to compute canonical bases of ideal squares.

Theorem 5.2. *Let $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$ be a canonical basis of an ideal $\mathfrak{a}$. Set*

$$s_G = \gcd(s, G), \qquad s_H = \gcd(s, H), \qquad s'_G = \gcd(s', G),$$

and assume that $\gcd(2v + Hw^2, s/s_G s_H) = 1$. *Then* $\mathfrak{a}^2 = (s'_G s'')[S, S'(U + \rho), S''(V + W\rho + \omega)]$ *where* S, S', S'', U, V, W *are given as follows.*

$$S = s^2/s_G s_H, \qquad S' = (s')^2 s_G/(s'_G)^3, \qquad S'' = s_H/s'',$$

$$U \equiv \begin{cases} 0 & \bmod s_H s'_G, \\ u - y(u^3 + D) & \bmod (s s'_G/s_G s_H s')^2, \end{cases}$$

$$W \equiv \begin{cases} 0 & \bmod s_G/s'_G, \\ w - z(Hw^3 - G) & \bmod (s'/s'_G)^2, \end{cases}$$

$$V \equiv \begin{cases} 0 & \bmod s_G s'', \\ v + U(W - w) + z\big(U(Hw^3 - G) \\ \quad +2GHw - v(v + Hw^2)\big) & \bmod (s/s_G s_H)^2, \end{cases}$$

with $3u^2 y \equiv 1 \bmod s s'_G/s_G s_H s'$ *and* $(2v + Hw^2)z \equiv 1 \bmod s/s_G s_H$.

Proof. Write $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$ where $\mathfrak{a}_1$ is the product of type 1 prime ideals, $\mathfrak{a}_2$ is the product of type 2 prime ideals, and $\mathfrak{a}_3$ is the product of type 3 or type 4 prime ideals. By Theorems 3.1 and 4.4, $\mathfrak{a}_3 = [\tilde{s}, \tilde{s}'(u+\rho), v+w\rho+\omega]$ where $\tilde{s} = s/s_G s_H$ and $\tilde{s}' = s'/s'_G$. We note that since $\gcd(\tilde{s}, GH) = 1$ by (4.1), it is always possible to achieve $\gcd(2v + Hw^2, \tilde{s}) = 1$ by Lemma 5.1. Therefore, z exists, and y exists by (4.9).

By Theorem 3.1, $\mathfrak{a}_1^2\mathfrak{a}_2^2 = (s'_G s'')[s_G s_H, (s_G/s'_G)\rho, (s_H/s'')\omega]$ and $\mathfrak{a}_3^2 = [\tilde{s}^2, (\tilde{s}')^2(\tilde{u} + \rho), \tilde{v} + \tilde{w}\rho + \omega]$ with suitable $\tilde{u}, \tilde{v}, \tilde{w} \in k[x]$. Thus, $\mathfrak{a}^2 = (s'_G s'')[S, S'(U + \rho), S''(V + W\rho + \omega)]$ where S, S', and S'' are as given above and

$$U \equiv \begin{cases} 0 & \bmod s_H s'_G, \\ \tilde{u} & \bmod (\tilde{s}/\tilde{s}')^2, \end{cases} \qquad W \equiv \begin{cases} 0 & \bmod (s_G/s'_G), \\ \tilde{w} & \bmod (\tilde{s}')^2, \end{cases}$$

$$V \equiv \begin{cases} 0 & \bmod s_G s'', \\ \tilde{v} + \tilde{u}(W - \tilde{w}) & \bmod \tilde{s}^2. \end{cases}$$

By considering that $\tilde{s}\tilde{s}'(u+\rho), (v+w\rho+\omega)^2 \in \mathfrak{a}_3^2$ and using (4.8) – (4.10), it can be shown that

$$\begin{aligned} \tilde{u} &\equiv u - y(u^3 + D) \bmod (\tilde{s}/\tilde{s}')^2, \\ \tilde{w} &\equiv w - z(Hw^3 - G) \bmod (\tilde{s}')^2, \\ \tilde{v} + \tilde{u}(W - \tilde{w}) &\equiv v + U(W - w) \\ &\quad + z\left(U(Hw^3 - G) + 2GHw - v(v + Hw^2)\right) \bmod \tilde{s}^2. \end{aligned}$$

□

Corollary 5.3. *Let $\{1, s'(u+\rho)/s, s''(v+w\rho+\omega)/s\}$ be a canonical basis of a fractional ideal $\mathfrak{f}$.*
Then $\mathfrak{f}^2 = (F^{-1})\tilde{\mathfrak{f}}$ where $F = \gcd(s, GH)/\gcd(s', G)s'' \in k[x]$, $\tilde{\mathfrak{f}}$ is a fractional ideal with canonical basis $\{1, S'(U+\rho)/S, S''(V+W\rho+\omega)/S\}$, and S, S', S'', U, V, W are given as in Theorem 5.2.

Proof. Let s_G, s_H, s'_G be as in the previous Theorem. Then $((s)\mathfrak{f})^2 = (s'_G s'')\mathfrak{a}$ where $\mathfrak{a} = [S, S'(U+\rho), S''(V+W\rho+\omega)]$. Hence, $\tilde{\mathfrak{f}} = (S^{-1})\mathfrak{a}$ is a fractional ideal with canonical basis $\{1, S'(U+\rho)/S, S''(V+W\rho+\omega)/S\}$, and $\mathfrak{f}^2 = (s'_G s'' S/s^2)\tilde{\mathfrak{f}} = (s'_G s''/s_G s_H)\tilde{\mathfrak{f}} = (F^{-1})\tilde{\mathfrak{f}}$. □

Example 5.4. Let k, G, H be as in Example 4.3 and let

$$\begin{aligned} \mathfrak{f} = \Bigg[1, &\frac{(x^4+x+1)}{x(x+1)(x^4+x+1)}(x+1+\rho), \\ &\frac{(x+1)}{x(x+1)(x^4+x+1)}(x^4+x+1+\omega)\Bigg]. \end{aligned}$$

We have $s = x(x+1)(x^4+x+1)$, $s' = v = x^4+x+1$, $s'' = u = x+1$, $w = 0$, and the given basis is canonical. We wish to compute a canonical basis $\{1, S'(U+\rho)/S, S''(V+W\rho+\omega)/S\}$ of the primitive ideal $(F)\mathfrak{f}^2$ with F as in Corollary 5.3.

We see that $s_G = s'_G = G = x^4+x+1$, $s_H = H = x+1$, so $F = 1$. Since $\gcd(2v + Hw^2, s/s_G s_H) = x \neq 1$, we try $f = 1$ and replace w by $w + fs' = x^4+x+1$ and v by $v + ufs' = x(x^4+x+1)$, thereby achieving $\gcd(2v + Hw^2, s/s_G s_H) = 1$. We then compute $S = x^2(x+1)(x^4+x+1)$, $S' = S'' = 1$, and $y = z = 1$. Now

$$U \equiv \begin{cases} 0 \bmod (x+1)(x^4+x+1), \\ (x+1) + (x+1)^3 + (x^4+x+1)(x+1)^2 \bmod x^2, \end{cases}$$

so $U = (x^2+1)(x^4+x+1) = D$. Also, $W = 0$ as $s_G/s'_G = s'/s'_G = 1$. Finally, it is easy to verify that

$$V \equiv \begin{cases} 0 \bmod (x^4+x+1)(x+1), \\ x+1 \bmod x^2, \end{cases}$$

giving $V = D$. So $\mathfrak{f}^2 = [1, (D+\rho)/S, (D+\omega)/S]$ with $D = (x^4+x+1)(x^2+1)$ and $S = x^2(x^4 + x + 1)(x + 1)$.

6. Reduced bases and ideal reduction

For the remainder of this paper, we only consider the situation where $q \equiv -1 \bmod 3$, so K has unit rank 1, and $\mathrm{char}(k) \geq 5$. We use the notation of [5]. Let $\theta = l + m\rho + n\omega \in K$ with $l, m, n \in k(x)$. We define

$$\begin{array}{lllll} \xi_\theta & = & \theta - l & = & m\rho + n\omega, \\ \eta_\theta & = & (1 + 2\iota)^{-1}(\theta' - \theta'') & = & m\rho - n\omega, \\ \zeta_\theta & = & \theta' + \theta'' & = & 2l - m\rho - n\omega, \end{array} \tag{6.1}$$

where ι ($\notin k$) is a primitive cube root of unity. Then

$$\theta = \frac{1}{2}(3\xi_\theta + \zeta_\theta), \qquad \theta'\theta'' = \frac{1}{4}(3\eta_\theta^2 + \zeta_\theta^2). \tag{6.2}$$

If $\theta, \phi \in K$ and $a, b \in k(x)$, then $\xi_{a\theta+b\phi} = a\xi_\theta + b\xi_\phi$, similarly for the other quantities of (6.1). Also $\xi_a = \eta_a = 0$ and $\zeta_a = 2a$.

For a fractional ideal $\mathfrak{f}$ and an element $\theta \in \mathfrak{f}$, set

$$\mathcal{N}_\mathfrak{f}(\theta) = \{\phi \in \mathfrak{f} \; : \; |\phi| \leq |\theta| \text{ and } |\phi'| \leq |\theta'|\}.$$

Lemma 6.1. *Let $\mathfrak{f}$ be a fractional ideal containing 1. Then $\mathcal{N}_\mathfrak{f}(1)$ is finite.*

Proof. Let $\phi = (l + m\rho + n\omega)/d \in \mathcal{N}_\mathfrak{f}(1)$ where $l, m, n \in k[x]$ and $d = d(\mathfrak{f})$. Then from (6.1) and (6.2) $|\xi_\phi|, |\eta_\phi| \leq 1$, so $|l| = |d(\phi - \xi_\phi)| \leq |d|$, $|m\rho| = |d(\xi_\phi + \eta_\phi)| \leq |d|$, and $|n\omega| = |d(\xi_\theta - \eta_\phi)| \leq |d|$. □

An element θ in a fractional ideal $\mathfrak{f}$ is a *minimum* in $\mathfrak{f}$ if $\mathcal{N}_\mathfrak{f}(\theta) = k\theta$; that is, $\mathcal{N}_\mathfrak{f}(\theta)$ contains only constant multiples of θ. $\mathfrak{f}$ is *reduced* if $1 \in \mathfrak{f}$ and 1 is a minimum in $\mathfrak{f}$, i.e. $\mathcal{N}_\mathfrak{f}(1) = k$. An integral ideal $\mathfrak{a}$ is *reduced* if $\mathfrak{a}$ is primitive and $(L(\mathfrak{a})^{-1})\mathfrak{a}$ is reduced, or equivalently, $L(\mathfrak{a})$ is a minimum in $\mathfrak{a}$. Every ideal equivalence class contains at least one and at most finitely many reduced representatives. If $\mathfrak{f}$ is a fractional ideal and $\theta \in K^*$, then it is easy to infer from the definition of a minimum that θ is a minimum in $\mathfrak{f}$ if and only if $(\theta^{-1})\mathfrak{f}$ is reduced. In particular, an element θ is a minimum in $\mathcal{O}$ if and only if the fractional principal ideal (θ^{-1}) is reduced.

We summarize some properties of reduced fractional and integral ideals:

Lemma 6.2.

1. *If $\mathfrak{f}$ is a fractional ideal containing 1, then $|d(\mathfrak{f})|^{-2} \leq |N(\mathfrak{f})| \leq |d(\mathfrak{f})|^{-1}$.*
2. *If $\mathfrak{f}$ is a reduced fractional ideal, then $|\Delta(\mathfrak{f})| > 1$, so $|N(\mathfrak{f})| > |\Delta|^{-1/2}$.*
3. *If $\mathfrak{f}$ is a reduced fractional ideal, then $|d(\mathfrak{f})| < |\Delta|^{1/2}$, so $|N(\mathfrak{f})| < |\Delta||d(\mathfrak{f})|^{-3}$.*

4. *If $\mathfrak{f}$ is a fractional ideal containing 1 with $|\Delta(\mathfrak{f})| > |d(\mathfrak{f})|^2$, i.e. $|d(\mathfrak{f})| < |N(\mathfrak{f})||\Delta|^{1/2}$, then $\mathfrak{f}$ is reduced.*

Proof. For brevity, write $d = d(\mathfrak{f})$.

1. Follows from $d = L(d\mathfrak{f}) \mid N(d\mathfrak{f}) \mid L(d\mathfrak{f})^2 = d^2$ and $N(d\mathfrak{f}) = d^3 N(\mathfrak{f})$.
2. See Theorem 4.5 of [5].
3. See Corollary 4.6 of [5] for the first inequality. The second inequality follows from $|N(\mathfrak{f})| \le |d|^{-1} < (|\Delta||d|^{-2})|d|^{-1}$.
4. Let $\theta \in \mathcal{N}_{\mathfrak{f}}(1)$ and set $\Delta(\theta) = ((\theta - \theta')(\theta' - \theta'')(\theta'' - \theta))^2 \in k(x)$. Then $|\Delta(\theta)| \le 1$. Let $\{\lambda, \mu, \nu\}$ be a $k[x]$-basis of $\mathfrak{f}$. Since $d\theta^2 \in \mathfrak{f}$, there exists a 3 by 3 matrix M with entries in $k[x]$ such that
$$\begin{pmatrix} 1 & 1 & 1 \\ \theta & \theta' & \theta'' \\ d\theta^2 & d(\theta')^2 & d(\theta'')^2 \end{pmatrix} = M \begin{pmatrix} \lambda & \lambda' & \lambda'' \\ \mu & \mu' & \mu'' \\ \nu & \nu' & \nu'' \end{pmatrix}.$$
Taking determinants and squares on both sides yields $d^2\Delta(\theta) = \det(M)^2\Delta(\mathfrak{f})$, therefore $1 \ge |\Delta(\theta)| = |\det(M)|^2|\Delta(\mathfrak{f})||d|^{-2} > |\det(M)|$. So $\det(M) = \Delta(\theta) = 0$, implying $\theta = \theta' = \theta''$ and hence $\theta \in k$.

□

Let $\mathfrak{f}$ be a fractional ideal and let θ be a minimum in $\mathfrak{f}$. An element $\phi \in \mathfrak{f}$ is the *neighbor of θ* in $\mathfrak{f}$ if ϕ is also a minimum in $\mathfrak{f}$, $|\theta| < |\phi|$, and for no $\psi \in \mathfrak{f}$, $|\theta| < |\psi| < |\phi|$ and $|\psi'| < |\theta'|$ ([5] uses the terminology "minimum adjacent to θ"). By Theorem 5.1 of [5], ϕ always exists and is unique up to nonzero constant factors.

According to [5], the *Voronoi chain* $(\theta_n)_{n\in\mathbb{N}}$ of successive minima in $\mathcal{O}$ where $\theta_1 = 1$ and θ_{n+1} is the neighbor of θ_n in $\mathcal{O}$ yields the entirety of minima in $\mathcal{O}$ of nonnegative degree. This chain is given by the recurrence $\theta_{n+1} = \mu_n\theta_n$ where μ_n is the neighbor of 1 in the reduced fractional principal ideal $\mathfrak{f}_n = (\theta_n^{-1})$ $(n \in \mathbb{N})$. The first nontrivial unit $\epsilon = \theta_{p+1}$ $(p \in \mathbb{N})$ encountered in this chain is the fundamental unit of $K/k(x)$ of positive degree (unique up to nonzero constant factors). Since the recurrence for the Voronoi chain implies $\theta_{mp+n} = \epsilon^m\theta_n$ for $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$, $\{\mathfrak{f}_1, \mathfrak{f}_2, \cdots, \mathfrak{f}_p\}$ is the complete set of reduced principal fractional ideals in K. We call p the *period* of ϵ.

We will see later on that a process very similar to the computation of the Voronoi chain can be used to obtain from a nonreduced fractional ideal an equivalent reduced one. For this purpose, we introduce the concept of a *reduced basis* of a (reduced or nonreduced) fractional ideal $\mathfrak{f}$; that is, a $k[x]$-basis $\{1, \mu, \nu\}$ of $\mathfrak{f}$ such that

$$(6.3) \qquad \begin{array}{l} |\xi_\mu| > |\xi_\nu|, \quad |\zeta_\mu| < 1, \quad |\zeta_\nu| \le 1, \quad |\eta_\mu| < 1 \le |\eta_\nu|, \\ \text{and if } |\eta_\nu| = 1, \text{ then } |\nu| \ne 1. \end{array}$$

Voronoi ([9], see also pp. 282–290 of [2], and [12] for the purely cubic version) essentially described how to obtain the equivalent of a reduced basis of a fractional ideal in a cubic number field. A function field version for reduced ideals was first given as Algorithm 7.1 in [5]. Here, we give a more general version of the method which includes the nonreduced case.

Algorithm 6.3.

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

Output: μ, ν where $\{1, \mu, \nu\}$ is a reduced basis of $\mathfrak{f}$.

Algorithm:

1. Set $\mu = \tilde{\mu}$, $\nu = \tilde{\nu}$.
2. If $|\xi_\mu| < |\xi_\nu|$ or if $|\xi_\mu| = |\xi_\nu|$ and $|\eta_\mu| < |\eta_\nu|$, replace
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \text{ by } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
3. If $|\eta_\mu| \geq |\eta_\nu|$
   3.1. While $|\xi_\nu \eta_\nu| > |\Delta(\mathfrak{f})|^{1/2}$, replace
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \text{ by } \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu / \xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
   3.2. Replace
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \text{ by } \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu / \xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
   3.3. If $|\eta_\mu| = |\eta_\nu|$, replace
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \text{ by } \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$$
   where $a = \operatorname{sgn}(\eta_\mu)\operatorname{sgn}(\eta_\nu)^{-1} \in k^*$.
4. While $|\eta_\nu| \leq 1$, replace
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \text{ by } \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu / \xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
   While $|\eta_\mu| > 1$, replace
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \text{ by } \begin{pmatrix} \lfloor \eta_\nu / \eta_\mu \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
5. If $|\zeta_\mu| \geq 1$, replace μ by $\mu - \lfloor \zeta_\mu \rfloor / 2$.
   If $|\zeta_\nu| \geq 1$, replace ν by $\nu - \lfloor \zeta_\nu \rfloor / 2$.
6. If $|\nu| = |\eta_\nu| = 1$, replace ν by $\nu - \lfloor \nu \rfloor$.

Theorem 6.4. *Algorithm 6.3 computes a reduced basis of the input ideal.*

Proof. In Proposition 7.2 in [5], it was shown that steps 1-5 compute a basis $\{1, \mu, \nu\}$ such that $|\xi_\mu| > |\xi_\nu|$, $|\zeta_\mu| < 1$, $|\zeta_\nu| < 1$, $|\eta_\mu| < 1 \leq |\eta_\nu|$. Suppose $|\eta_\nu| = |\nu| = 1$, so step 6 is entered. Set $\tilde{\nu} = \nu - \lfloor \nu \rfloor$, then $|\tilde{\nu}| < 1$, $|\xi_{\tilde{\nu}}| = |\xi_\nu|$, $|\eta_{\tilde{\nu}}| = |\eta_\nu|$, and $|\zeta_{\tilde{\nu}}| = |\zeta_\nu - 2\lfloor \nu \rfloor| = 1$. Hence at the end of the algorithm, the basis is reduced. □

If $\mathfrak{f}$ is reduced, then μ is the neighbor of 1 in $\mathfrak{f}$ by Theorem 7.5 of [5], so repeated application of Algorithm 6.3, beginning and ending with input ideal $\mathfrak{f} = \mathcal{O}$ generates the fundamental unit ϵ of $K/k(x)$. Furthermore, it can be shown that in this situation, the conditions in step 3.1, the first loop of step 4, and step 6 cannot occur, so these steps can be omitted (see [4]).

The process of computing from the reduced fractional ideal $\mathfrak{f}_n$ ($n \in \mathbb{N}$) a reduced basis of the next reduced fractional ideal $\mathfrak{f}_{n+1} = (\mu_n^{-1})\mathfrak{f}_n$ where μ_n is the neighbor of 1 in $\mathfrak{f}_n$ is referred to as a *baby step.*

Example 6.5. For illustrative purposes, we compute the fundamental unit ϵ of an extension $k/k(x)$ with an unusually short period. Let q be any odd prime power with $q \geq 7$ and $q \equiv -1 \bmod 3$ and let $D(x) = G(x) = x^6 - x$ and $H(x) = 1$. Then $\rho = x^2 + O(x^{-3})$ and $\omega = \rho^2 = x^4 + O(x^{-1})$. We call Algorithm 6.3 on the input $\mu = \rho$ and $\nu = \rho^2$. After step 2, we have $\mu = -\rho^2$ and $\nu = \rho$, and we proceed to step 3.2. We have $\lfloor \xi_\mu/\xi_\nu \rfloor = -\lfloor \rho \rfloor = -x^2$, so we obtain $\mu = \rho$ and $\nu = -x^2\rho + \rho^2$. Since $|\eta_\mu| = |\rho| = q^2 \geq 1$ and $|\eta_\nu| = q^4 \neq |\eta_\mu|$, we enter the second while loop of step 4. Here, $\lfloor \eta_\nu/\eta_\mu \rfloor = \lfloor -x^2 - \rho \rfloor = -2x^2$, so after the first iteration $\mu = -x^2\rho - \rho^2$ and $\nu = \rho$. Now $|\eta_\mu| = |x^2\rho - \rho^2| \leq |x^{-1}| < 1$, so we go on to step 5. We see that $-\lfloor \zeta_\mu \rfloor/2 = -x^4$ and $-\lfloor \zeta_\nu \rfloor = x^2/2$, so we have $\mu = -(x^4 + x^2\rho + \rho^2)$ and $\nu = x^2/2 + \rho$. The inputs to our next call of Algorithm 6.3 are $\mu^{-1} = (-x^2 + \rho)/x$ and $\nu\mu^{-1} = (-x^4 - x^2\rho + 2\rho^2)/x$.

The following table shows the complete computation of the Voronoi chain up to ϵ. For simplicity, certain constant factors (such as -1 and $1/2$) of the basis elements have been removed. Here, $\mathfrak{f}_i$ is the input ideal of the i-th round of the algorithm.

Round i	Inputs for $\mathfrak{f}_i$	$d(\mathfrak{f}_i)$	Outputs for $\mathfrak{f}_i$
1	ρ ρ^2	1	$\mu_1 = x^4 + x^2\rho + \rho^2$ $\nu_1 = x^2 + 2\rho$
2	$\mu_1^{-1} = (x^2 - \rho)/x$ $\nu_1\mu_1^{-1} = (x^4 + x^2\rho - 2\rho^2)/x$	x	$\mu_2 = (x^4 + x^2\rho + \rho^2)/x$ $\nu_2 = (x^2 + 2\rho)/x$
3	$\mu_2^{-1} = x^2 - \rho$ $\nu_2\mu_2^{-1} = (x^4 + x^2\rho - 2\rho^2)/x$	x	$\mu_3 = (x^4 + x^2\rho + \rho^2)/x$ $\nu_3 = x^2 + 2\rho$
4	$\mu_3^{-1} = x^2 - \rho$ $\nu_3\mu_3^{-1} = x^4 + x^2\rho - 2\rho^2$	1	— —

At this point, the input ideal has denominator 1, hence $\mathfrak{f}_4 = \mathcal{O}$ and $p = 3$. The Voronoi chain up to the fundamental unit ϵ is given by

$$\begin{aligned}\theta_1 &= 1,\\ \theta_2 &= \mu_1\theta_1 = x^4 + x^2\rho + \rho^2,\\ \theta_3 &= \mu_2\theta_2 = (3x^7 - 2x^2) + (3x^5 - 1)\rho + 3x^3\rho^2,\\ \theta_4 &= \mu_3\theta_3 = (9x^{10} - 9x^5 + 1) + (9x^8 - 6x^3)\rho + (9x^6 - 3x)\rho^2 = \epsilon.\end{aligned}$$

A reduced basis provides an easy means for recognizing whether or not the ideal generated by this basis is reduced:

Theorem 6.6. *Let $\{1, \mu, \nu\}$ be a reduced basis of a fractional ideal $\mathfrak{f}$. Then $\mathfrak{f}$ is reduced if and only if $|\mu| > 1$ and $\max\{|\nu|, |\eta_\nu|\} > 1$.*

Proof. By (6.2) and (6.3) $|\mu'| < 1$. If $|\mu| \leq 1$, then $\mu \in \mathcal{N}_\mathfrak{f}(1)$, so $\mathfrak{f}$ is not reduced. Similarly, if $\max\{|\nu|, |\eta_\nu|\} \leq 1$, then by (6.2) $|\nu'| \leq 1$, so $\nu \in \mathcal{N}_\mathfrak{f}(1)$ and again, $\mathfrak{f}$ is nonreduced.

Conversely, suppose that $|\mu| > 1$, $\max\{|\nu|, |\eta_\nu|\} > 1$, and let $\theta = l + m\mu + n\nu \in \mathcal{N}_\mathfrak{f}(1)$ with $l, m, n \in k[x]$. By (6.1) $|\zeta_\theta|, |\eta_\theta| \leq 1$ and by (6.2) $|\xi_\theta| \leq 1$. Assume $|m| < |n|$, then $|m\eta_\mu| < |n\eta_\nu|$, so $1 \leq |n| \leq |n\eta_\nu| = |m\eta_\mu + n\eta_\nu| = |\eta_\theta| \leq 1$, implying $|\eta_\nu| = |n| = 1$. It follows that $m = 0$ and $|\nu| > 1$; also $|l| = |\zeta_\theta - n\zeta_\nu| \leq 1$. But then $1 = |n| < |n\nu| = |\theta - l| \leq 1$, a contradiction. So $|m| \geq |n|$.

Suppose $m \neq 0$, then $|n\xi_\nu| < |m\xi_\mu|$, so $1 \leq |m| < |m\xi_\mu| = |\xi_\theta| \leq 1$, a contradiction. Hence, $m = n = 0$ and $|l| = |\theta| \leq 1$, implying $l = \theta \in k$. $\square$

Corollary 6.7. *Let $\{1, \mu, \nu\}$ be a reduced basis of a fractional ideal $\mathfrak{f}$. Then $\mathfrak{f}$ is nonreduced if and only if $|\mu| \leq 1$ or $|\nu| < |\eta_\nu| = 1$.*

Let $\mathfrak{f}$ be any nonreduced fractional ideal and define a sequence $(\mathfrak{f}_n)_{n\in\mathbb{N}}$ of fractional ideals as follows.

$$(6.4)\quad \mathfrak{f}_1 = \mathfrak{f}, \quad \mathfrak{f}_{n+1} = (\phi_n^{-1})\mathfrak{f}_n \quad \text{where } \phi_n = \begin{cases} \mu_n & \text{if } |\mu_n| \leq 1, \\ \nu_n & \text{if } |\mu_n| > 1, \end{cases} \quad (n \in \mathbb{N})$$

and $\{1, \mu_n, \nu_n\}$ is a reduced basis of $\mathfrak{f}_n$. Clearly, all the $\mathfrak{f}_n$ are equivalent. Here, the process of obtaining $\mathfrak{f}_{n+1}$ from $\mathfrak{f}_n$ is also called a baby step; the difference to the reduced case is that by Corollary 6.7, the ideal $\mathfrak{f}_n$ is always divided by an element of nonpositive degree, whereas in the reduced case, one divides by the element μ of positive degree. We note that as in the recursion for the Voronoi chain, we always divide by μ_n except for one special case where we do not need Algorithm 6.3 to produce a reduced basis (see [4]):

Lemma 6.8. *Let $\{1, \mu, \nu\}$ be a reduced basis of a nonreduced ideal $\mathfrak{f}$ with $|\mu| > 1$. Then $(\nu^{-1})\mathfrak{f}$ is reduced with a reduced basis $\{1, \mu\nu^{-1}, \nu^{-1}\}$.*

From (6.4), we see that

$$(6.5)\quad \mathfrak{f}_n = (\psi_n^{-1})\mathfrak{f}_1 \qquad \text{where} \quad \psi_1 = 1 \quad \text{and} \quad \psi_n = \prod_{i=1}^{n-1} \phi_i \quad \text{for} \quad n \geq 2.$$

If $\mathfrak{f}_n$ is nonreduced, then it follows from (6.4), Corollary 6.7, and the fact that $|\mu_i'| < 1$ for all $i \in \mathbb{N}$ that one of $|\phi_n|$ and $|\phi_n'|$ is always strictly less than 1, while the other is no bigger than 1. Therefore $|\psi_n| \leq 1$ and $|\psi_n'| \leq 1$, where at least one of the inequalities is strict. Furthermore, $\psi_n \in \mathfrak{f}_1$ implies $|N(\psi_n)| \geq |N(\mathfrak{f}_1)|$, so $|\psi_n| \geq |N(\mathfrak{f}_1)|$ and $|\psi_n'| \geq |N(\mathfrak{f}_1)|^{1/2}$, where again inequality holds in at least one of the two cases.

We claim that a finite number of baby steps applied to a nonreduced fractional ideal will yield an equivalent reduced one:

Lemma 6.9. *Let $\mathfrak{f} = \mathfrak{f}_1$ be a nonreduced fractional ideal. Then there exists $m \in \mathbb{N}$ such that $\mathfrak{f}_m$ is reduced, where $\mathfrak{f}_m$ is as in (6.5).*

Proof. From our above observation, $|N(\psi_n)| < |N(\psi_{n+1})|$ for all $n \in \mathbb{N}$. If no $\mathfrak{f}_n$ $(n \in \mathbb{N})$were reduced, then $(\psi_n)_{n \in \mathbb{N}}$ would be an infinite sequence of pairwise distinct elements in $\mathcal{N}_{\mathfrak{f}}(1)$, contradicting Lemma 6.1. □

Theorem 6.10. *Let $m \in \mathbb{N}$ be such that $\mathfrak{f}_m$ is reduced and $\mathfrak{f}_n$ is not reduced for $n < m$, where $\mathfrak{f}_n$ is as in (6.5) for $n \in \mathbb{N}$. Then*

$$m \leq \max\left\{1, \frac{1}{2}\left(5 - \deg(N(\mathfrak{f}_1)) - \frac{1}{4}\deg(\Delta)\right)\right\}.$$

Proof. If $\mathfrak{f}_1$ is reduced, then $m = 1$, so suppose $\mathfrak{f}_1$ is not reduced and set $d_n = \deg(N(\mathfrak{f}_n))$ for $n \in \mathbb{N}$. By Lemma 6.8, $\phi_n = \mu_n$ for $1 \leq n \leq m-2$, so $d_n \geq d_{n-1} + 2$ for $2 \leq n \leq m-2$ and $d_{m-1} \geq d_{m-2} + 1$. Hence inductively, $d_{m-2} \geq d_1 + 2(m-3)$ and $d_{m-1} \geq d_1 + 2m - 5$, so $m \leq (5 - d_1 + d_{m-1})/2$.

Since $\mathfrak{f}_{m-1}$ is not reduced, by part 4 of Lemma 6.2 $|N(\mathfrak{f}_{m-1})| \leq |d(\mathfrak{f}_{m-1})||\Delta|^{-1/2}$. By part 1 of the same lemma $|d(\mathfrak{f}_{m-1})N(\mathfrak{f}_{m-1})| \leq 1$, so together, we obtain $|N(\mathfrak{f}_{m-1})| \leq |\Delta|^{-1/4}$ or $d_{m-1} \leq -\deg(\Delta)/4$. □

Corollary 6.7, together with Lemma 6.8 gives rise to the following ideal reduction algorithm. The number of iterations of the while loop in this algorithm is given by Theorem 6.10.

Algorithm 6.11.

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

Output: μ, ν where $\{1, \mu, \nu\}$ is a reduced basis of a reduced fractional ideal equivalent to $\mathfrak{f}$.

Algorithm:

1. Set $\mu = \tilde{\mu}$, $\nu = \tilde{\nu}$.
2. While $|\mu| \leq 1$

2.1. Set $\{\tilde{\mu}, \tilde{\nu}\} = \{\mu^{-1}, \nu\mu^{-1}\}$.
2.2. From the basis $\{1, \tilde{\mu}, \tilde{\nu}\}$, compute a reduced basis $\{1, \mu, \nu\}$ using Algorithm 6.3.

3. If $|\nu| < |\eta_\nu| = 1$
replace (μ, ν) by $(\mu\nu^{-1}, \nu^{-1})$.

7. The infrastructure of the principal class

According to Section 6, every reduced principal fractional ideal is generated by the inverse of an element of the Voronoi chain $(\theta_n)_{n\in\mathbb{N}}$. For $\mathfrak{f}_n = (\theta_n^{-1})$ with $1 \leq n \leq p$ (where p is the period of the fundamental unit ϵ), we define the *distance* of $\mathfrak{f}_n$ to be $\delta(\mathfrak{f}_n) = \delta_n = \deg(\theta_n)$. Then the distance is a nonnegative function on the set of reduced fractional ideals that strictly increases with n and is easily seen to satisfy the properties

$$(7.1) \quad d_1 = 0, \qquad \delta_n = \delta_{n-1} + \deg(\mu_{n-1}), \qquad 1 \leq \delta_n - \delta_{n-1} \leq \frac{\deg(\Delta)}{2}$$

for any $n \in \{2, 3, \dots, p\}$, where, as usual, μ_{n-1} is the neighbor of 1 in $\mathfrak{f}_{n-1}$. Here, the last inequality follows from the fact that $|\mu_n| \leq |\Delta|^{1/2}$ by Theorem 7.6 of [5]. It follows that for all $n \in \mathbb{N}$:

$$(7.2) \qquad n - 1 \leq \delta_n \leq (n-1)\frac{\deg(\Delta)}{2}.$$

Let $\mathfrak{f}_i = (\theta_i^{-1})$ and $\mathfrak{f}_j = (\theta_j^{-1})$ be two reduced principal fractional ideals $(1 \leq i, j \leq p)$ such that $\delta_i + \delta_j \leq \deg(\epsilon)$. Then the product ideal $\mathfrak{f}_i\mathfrak{f}_j$ is generally not reduced; however, there is a reduced principal fractional ideal $\mathfrak{f}_m$ "close to" it, i.e. $\delta_m \approx \delta_i + \delta_j$, and from (7.2) $m \approx i + j$. Shanks first observed this behavior for the set of principal ideals of a real quadratic number field and coined it the *infrastructure* of the principal class [3]. More exactly:

Theorem 7.1. *Let $\mathfrak{f}_i$ and $\mathfrak{f}_j$ be two reduced principal fractional ideals with $\gcd(d(\mathfrak{f}_i), d(\mathfrak{f}_j)) = 1$ and $\delta_i + \delta_j \leq \deg(\epsilon)$. Then there exists a reduced principal fractional ideal $\mathfrak{f}_m$ which we denote by $\mathfrak{f}_i * \mathfrak{f}_j$ such that $\delta_m = \delta_i + \delta_j + \delta$ with $0 \geq \delta \geq 2 - \deg(\Delta)$.*

Proof. Let $\mathfrak{f} = \mathfrak{f}_i\mathfrak{f}_j$. By Lemma 6.9, there exists $\psi = \psi_m \in \mathfrak{f}$ such that $\mathfrak{f}_m = (\psi^{-1})\mathfrak{f}$ is reduced for some $m \in \{1, 2, \dots, p\}$. Then $\mathfrak{f}_m = (\psi^{-1})\mathfrak{f}_i\mathfrak{f}_j$, so $\theta_m = \psi\theta_i\theta_j$ and $\delta_m = \delta_i + \delta_j + \deg(\psi)$. Since $\psi \in \mathfrak{f}$, we have $|N(\mathfrak{f})| \leq |\psi| \leq 1$. Set $\delta = \deg(\psi)$, then $0 \geq \delta \geq \deg(N(\mathfrak{f})) = \deg(N(\mathfrak{f}_i)) + \deg(N(\mathfrak{f}_j))$. By part 2 of Lemma 6.2, $\deg(N(\mathfrak{f}_i)), \deg(N(\mathfrak{f}_j)) \geq -(\deg(\Delta)/2 - 1)$ (note that Δ has even degree), so $\delta \geq 2 - \deg(\Delta)$. □

Theorem 7.2. *Let $\mathfrak{f}_i$ be a reduced principal fractional ideal with $\delta_i \leq \deg(\epsilon)/2$. Then there exists a reduced fractional principal ideal $\mathfrak{f}_m$ which we denote by $\mathfrak{f}_i * \mathfrak{f}_i$ such that $\delta_m = 2\delta_i + \delta$ where $0 \geq \delta \geq 3(1 - \deg(\Delta)/2)$.*

Proof. Let $\{1, s'(u+\rho)/s, s''(v+w\rho+\omega)/s\}$ be a canonical basis of $\mathfrak{f}_i$. By Corollary 5.3, $\mathfrak{f}_i^2 = (F^{-1})\mathfrak{f}$, where $\mathfrak{f}$ is a fractional ideal containing 1 and $F = \gcd(s, GH)/\gcd(s', G)s''$. We have $0 \le \deg(F) \le \deg(s) = \deg(d(\mathfrak{f}_i)) \le \deg(\Delta)/2 - 1$ by part 3 of Lemma 6.2. As in the proof of the previous Theorem, there exists $m \in \mathbb{N}$ and $\psi = \psi_m \in \mathfrak{f}$ such that $\mathfrak{f}_m = (\psi^{-1})\mathfrak{f} = (F\psi^{-1})\mathfrak{f}_i^2$ is reduced and $0 \ge \deg(\psi) \ge 2 - \deg(\Delta)$. Then $\delta_m = 2\delta_i + \delta$ where $\delta = \deg(\psi) - \deg(F)$ satisfies the bounds of the Theorem. □

By (7.2), distances can be as large as $\Theta(p)$ [1]. Since by Theorem 6.5 of [5], $p = O(q^{(\deg(\Delta)/2)-2})$, the quantities δ in Theorems 7.1 and 7.2 are generally logarithmically small relative to the distances of the initial fractional ideal(s). In other words, the ideal $\mathfrak{f}_m$ is essentially where one would expect it to be, namely δ_m is very close to $\delta_i + \delta_j$, respectively, $2\delta_i$. Furthermore, $\mathfrak{f}_m$ can be obtained quickly:

Corollary 7.3.

1. *Let $\mathfrak{f}_i, \mathfrak{f}_j, \mathfrak{f}_m$ be as in Theorem 7.1. Then the number of baby steps required to compute $\mathfrak{f}_m$ from $\mathfrak{f}_i\mathfrak{f}_j$ is at most $\lfloor 3(\deg(\Delta)+4)/8 \rfloor$.*
2. *Let $\mathfrak{f}_i$ be as in Theorem 7.2. Then the number of baby steps required to compute $\mathfrak{f}_m$ from $\mathfrak{f} = (F^{-1})\mathfrak{f}_i^2$ is at most $\lfloor 3(\deg(\Delta)+4)/8 \rfloor$.*

Proof. From the proof of Theorem 7.1, we have $\deg(N(\mathfrak{f}_i\mathfrak{f}_j)) \ge 2 - \deg(\Delta)$ in the situation of Theorem 7.1; similarly, $\deg(N(\mathfrak{f})) = 2\deg(N(\mathfrak{f}_i)) + 3\deg(F) \ge 2 - \deg(\Delta)$ in the case of Theorem 7.2. The corollary now follows from Theorem 6.10. □

Note that we did not specify how to multiply two distinct fractional ideals $\mathfrak{f}_i$ and $\mathfrak{f}_j$ whose denominators are not coprime. It is possible to develop multiplication formulas for this situation; however, the details are very tedious. Instead, we compute a reduced fractional principal ideal very close to $\mathfrak{f}_i * \mathfrak{f}_j$ as follows. Begin by finding the first reduced fractional ideal $\mathfrak{f}_{i-n}$ $(0 \le n < i)$ such that $\gcd(d(\mathfrak{f}_{i-n}), d(\mathfrak{f}_j)) = 1$. In many applications, such as the computation of the fundamental unit (or the regulator), the infrastructure is used in such a way that $\mathfrak{f}_i$ is fixed, and usually, some or all of the ideals $\mathfrak{f}_1 = \mathcal{O}, \mathfrak{f}_2, \dots, \mathfrak{f}_{i-1}, \mathfrak{f}_i$ are precomputed and stored, so it is easy to find our desired ideal $\mathfrak{f}_{i-n}$.

Next, we compute $\mathfrak{f}_{i-n} * \mathfrak{f}_j$. Then $\delta(\mathfrak{f}_{i-n} * \mathfrak{f}_j) = \delta_i + \delta_j + \tilde{\delta}$ where $\tilde{\delta} = \delta + \delta_{i-n} - \delta_i$ and $0 \ge \delta = \delta(\mathfrak{f}_{i-n} * \mathfrak{f}_j) - \delta_{i-n} - \delta_j \ge 2 - \deg(\Delta)$. We have

$$\delta_i - \delta_{i-n} = \deg(\mu_{i-n}) + \deg(\mu_{i-n+1}) + \cdots + \deg(\mu_{i-1}),$$

[1] For two functions $f(n), g(n)$ defined on $\mathbb{N}$, we say that $f(n) = \Theta(g(n))$ if there exist positive constants c, d such that $cg(n) \le f(n) \le dg(n)$ for sufficiently large $n \in \mathbb{N}$, i.e. if $f(n) = O(g(n))$ and $g(n) = O(f(n))$.

so by (7.1), $n \le \delta_i - \delta_{i-n} \le n\deg(\Delta)/2$ and hence $-n \ge \tilde{\delta} \ge 2 - (n+2)\deg(\Delta)/2$, so $\mathfrak{f}_{i-n} * \mathfrak{f}_j$ is within n baby steps of the ideal $\mathfrak{f}_i * \mathfrak{f}_j$. n is generally very small; most of the time, $n = 0$ or 1 will be sufficient.

Given two reduced fractional ideals $\mathfrak{f}_i$ and $\mathfrak{f}_j$, it is now easy to compute the reduced fractional ideal $\mathfrak{f}_i * \mathfrak{f}_j$, or at least one that is only a few baby steps short of $\mathfrak{f}_i * \mathfrak{f}_j$. This process is called a *giant step*. Note that a giant step does not use distances explicitly.

Algorithm 7.4.

Input: Reduced bases of two reduced principal fractional ideals $\mathfrak{f}_i$ and $\mathfrak{f}_j$.

Output:

If $\mathfrak{f}_i = \mathfrak{f}_j$: a reduced basis of a reduced principal fractional ideal $\mathfrak{f}$ and $\delta = \delta(\mathfrak{f}) - 2\delta(\mathfrak{f}_i)$ with $0 \ge \delta \ge 3(1 - \deg(\Delta)/2)$.

If $\mathfrak{f}_i \ne \mathfrak{f}_j$: a reduced basis of a reduced principal fractional ideal $\mathfrak{f}$; also $n \in \mathbb{N}$ and $\delta = \delta(\mathfrak{f}) - \delta(\mathfrak{f}_i) - \delta(\mathfrak{f}_j)$ with $-n \ge \delta \ge 2 - (n+2)\deg(\Delta)/2$ ($n = 0$ if and only if $\gcd(d(\mathfrak{f}_i), d(\mathfrak{f}_j)) = 1$).

Precomputed: Reduced bases of a list of ideals $\{\mathfrak{f}_i, \mathfrak{f}_{i-1}, \ldots \mathfrak{f}_{i-m}\}$ with $m \le i-1$ sufficiently large (required only if $\mathfrak{f}_i \ne \mathfrak{f}_j$ and $\gcd(d(\mathfrak{f}_i), d(\mathfrak{f}_j)) \ne 1$).

Algorithm:

1. Set $\delta = n = 0$.
2. If $\mathfrak{f}_i \ne \mathfrak{f}_j$
   while $\gcd(d(\mathfrak{f}_i), d(\mathfrak{f}_j)) \ne 1$
   2.1. Replace n by $n + 1$.
   2.2. Replace $\mathfrak{f}_i$ by $\mathfrak{f}_{i-1}$.
3. Compute canonical bases of $\mathfrak{f}_i$ and $\mathfrak{f}_j$ using Lemma 4.2.
4. If $\mathfrak{f}_i \ne \mathfrak{f}_j$, compute a canonical basis of $\mathfrak{f} = \mathfrak{f}_i\mathfrak{f}_j$ using Theorem 4.4.
   If $\mathfrak{f}_i = \mathfrak{f}_j$, compute a canonical basis of $\mathfrak{f} = (F)\mathfrak{f}_i^2$ using Theorem 5.2, where F is given as in Corollary 5.3. Replace δ by $\delta - \deg(F)$.
5. Compute a reduced basis $\{1, \mu, \nu\}$ of $\mathfrak{f}$ using Algorithm 6.3.
6. While $\deg(\mu) \le 0$
   6.1. Replace δ by $\delta + \deg(\mu)$.
   6.2. Replace $\mathfrak{f}$ by $\mu^{-1}\mathfrak{f}$ (i.e. compute the basis $\{1, \mu^{-1}, \nu\mu^{-1}\}$).
   6.3. Compute a reduced basis $\{1, \mu, \nu\}$ of $\mathfrak{f}$.
7. If $\deg(\nu) < \deg(\eta_\nu) = 0$
   7.1. Replace δ by $\delta + \deg(\nu)$.
   7.2. Replace $\mathfrak{f}$ by $\nu^{-1}\mathfrak{f}$ (i.e. compute the reduced basis $\{1, \mu\nu^{-1}, \nu^{-1}\}$).

8. Conclusion and open problems

Equation (7.2) implies $\delta_n = \Theta(n)$, or informally, $\delta_n \approx n$. The motivation of the terms "baby" and "giant" step is now clear: by Theorems 7.1 and 7.2, a giant step $\mathfrak{f}_i * \mathfrak{f}_j$ represents a gain of approximately $i + j$ in distance, about as much as $i + j$ baby steps. Thus, giant steps allow for much faster travel through the set of reduced fractional ideals than baby steps. This fact can be exploited to compute the fundamental unit ϵ of $K/k(x)$.

The naive way to compute ϵ (and the method employed in [5]) is to apply baby steps to the ideal $\mathfrak{f}_1 = \mathcal{O}$ until a unit is encountered, thus obtaining $\epsilon = \theta_{p+1}$ after p baby steps. Instead, one can apply approximately $\sqrt{p}$ baby steps to $\mathfrak{f}_1$ to find an ideal $\mathfrak{f}_m$ with $\delta_m \approx m \approx \sqrt{p}$, and subsequently execute m giant steps $\mathfrak{g}_1 = \mathfrak{f}_m$, $\mathfrak{g}_2 = \mathfrak{g}_1 * \mathfrak{f}_m$, $\cdots$, $\mathfrak{g}_m = \mathfrak{g}_{m-1} * \mathfrak{f}_m$, each resulting in a distance jump of approximately m. Then the total advance in distance is roughly $m^2 \approx p \approx \deg(\epsilon)$. This reduces the run time from order p to order $\sqrt{p}$, and it is likely that further improvements are possible; for example, clever search techniques find the fundamental unit of a real quadratic function field in time $O(p^{2/5})$. The difficulty here is that one needs to know a good approximation of p ahead of time.

Similar methods generate the ideal class number h' of $K/k(x)$ and hence the order $h = h' \deg(\epsilon)/2$ of the group of k-rational points of the Jacobian of K/k; work on finding h is currently in progress. We point out that h is independent of the transcendental element x and hence the particular purely cubic representation of $K/k(x)$; it is a true invariant of K.

We expect that our results in [5] and in this paper extend to arbitrary cubic function fields — function fields of curves $F(x, y) = 0$ of degree 3 in y — of unit rank 1 and characteristic different from 3. While the characterization of these extensions according to unit rank will not be as beautifully simple as the one given in Theorem 2.1 of [5] for the purely cubic case, much of the arithmetic may be similar, particular if one uses a basis of the form $1, \rho, \omega$ with $\rho\omega \in k[x]$ as described by Voronoi in the number field case (see [2, pp. 108–112]). Furthermore, it may be possible to use elements of Algorithm 6.3 in the case of unit rank 2, where the two fundamental units correspond to two different embeddings of K into $k\langle x^{-1}\rangle$. We also mention that purely cubic function fields of unit rank 0 are currently being investigated by M. Bauer, currently a Ph. D. student at the University if Illinois at Urbana-Champaign, who gave an efficient algorithm for finding the unique reduced representative in every ideal class if D is squarefree, i.e. the curve representing $K/k(x)$ is nonsingular [1]. Finally, it is as yet unclear how to define and compute a reduced basis in the case of even characteristic. Preliminary investigations suggest that an approach quite different from the one given in Section 6 is needed; work on this case is ongoing. Lastly, cubic function fields of characteristic 3 have not yet been explored; their arithmetic is likely somewhat different from their counterparts of characteristic different from 3.

Acknowledgments. The author is indebted to Mark Bauer for pointing out an error in the initial version of Theorem 3.1 and to Andreas Stein for some useful ideas that were incorporated into Section 4. I also thank two anonymous referees for their careful reading and helpful suggestions for improvement of this paper.

References

[1] M. BAUER, *The arithmetic of certain cubic function fields.* Submitted to Math. Comp.

[2] 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.

[3] D. SHANKS, *The infrastructure of a real quadratic field and its applications.* Proc. 1972 Number Theory Conf., Boulder (Colorado) 1972, 217–224.

[4] R. SCHEIDLER, *Reduction in purely cubic function fields of unit rank one.* Proc. Fourth Algorithmic Number Theory Symp. ANTS-IV, Lect. Notes Comp. Science **1838**, Springer, Berlin, 2000, 151–532.

[5] R. SCHEIDLER, A. STEIN, *Voronoi's algorithm in purely cubic congruence function fields of unit rank 1.* Math. Comp. **69** (2000), 1245–1266.

[6] A. STEIN, H. C. WILLIAMS, *Some methods for evaluating the regulator of a real quadratic function field.* Exp. Math. **8** (1999), 119–133.

[7] H. STICHTENOTH, *Algebraic function fields and codes.* Universitext, Springer-Verlag, Berlin, 1993.

[8] G. F. VORONOI, *Concerning algebraic integers derivable from a root of an equation of the third degree* (in Russian). Master's Thesis, St. Petersburg (Russia), 1894.

[9] G. F. VORONOI, *On a generalization of the algorithm of continued fractions* (in Russian). Doctoral Dissertation, Warsaw (Poland), 1896.

[10] H. C. WILLIAMS, *Continued fractions and number-theoretic computations.* Rocky Mountain J. Math. **15** (1985), 621–655.

[11] H. C. WILLIAMS, G. CORMACK, E. SEAH, *Calculation of the regulator of a pure cubic field.* Math. Comp. **34** (1980), 567–611.

[12] 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.

Renate SCHEIDLER
Department of Mathematics and Statistics
University of Calgary
2500 University Drive N.W.
Calgary, AB T2N 1N4
Canada
E-mail : rscheidl@math.ucalgary.ca