Ideal Arithmetic and Infrastructure in Purely Cubic Function Fields

R. Scheidler
Department of Mathematical Sciences
University of Delaware, Newark DE 19716, USA
scheidle@math.udel.edu

September 21, 1999
CORR #99-45

Abstract

This paper investigates the arithmetic of fractional ideals and the infrastructure of the principal ideal class of a purely cubic function field of unit rank one. We first describe how irreducible polynomials split into prime ideals in purely cubic function fields of nonzero unit rank. This decomposition behavior is used to compute so-called canonical bases of fractional ideals; such bases are very suitable for computation. We state algorithms for ideal multiplication and, in the case of unit rank one, 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.

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 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 a group. First discovered for real quadratic fields by Shanks [1], 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 counter parts, 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 [3].

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 [6, 7, 5], and much of the work in this paper was guided by these sources. Research on the use of the infrastructure to compute the regulator and the ideal class number of a purely cubic function field (and hence the order of the group of rational points of the Jacobian) is currently in progress.

For a general introduction to function fields, we refer the reader to [4]. Purely cubic function fields are discussed in detail in [2]. 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 $k(x)$.

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 $\Delta = -27G^2H^2$. We assume that the leading coefficient $\mathrm{sgn}(D)$ of D is a cube in $k^* = k \setminus \{0\}$ and that the degree $\deg(D)$ is divisible by 3. Then by Theorem 2.1 of [2], K has *unit rank* 1 or 2 over $k(x)$; that is, the *unit group* of $K/k(x)$, i.e. the group of units $\mathcal{O}^*$ of the ring $\mathcal{O}$, is an infinite Abelian group of rank 1 (if $q \equiv -1 \pmod 3$) or 2 (if $q \equiv 1 \pmod 3$). Furthermore, 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 $q \equiv 1 \pmod 3$, it follows that $\alpha', \alpha'' \in K$ if $q \equiv 1 \pmod 3$, whereas $\alpha', \alpha'' \notin K$, but $\alpha'\alpha'' \in K$, if $q \equiv$

$-1 \pmod 3$). 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 $N(\alpha) = \alpha\alpha'\alpha'' = a^3 + b^3GH^2 + c^3G^2H - 3abcGH \in k(x)$.

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 $d\mathfrak{a}$ 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 $\mathfrak{f} = (\theta)$. Fractional ideals are also $k[x]$-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 $\mathfrak{f}$.

An integral ideal is *primitive* if it is not contained in any principal integral ideal other than $\mathcal{O}$. 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 [2]). Similarly, if a fractional ideal contains 1, then 1 can always be included in a $k[x]$-basis of the fractional ideal.

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 $\nu = (n_0 + n_1\rho + n_2)/d$ 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 $\mathfrak{a}_{\mathfrak{f}} = d\mathfrak{f} = [d, d\mu, d\nu]$. $d = d(\mathfrak{f})$ 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 product of two fractional ideals $\mathfrak{f}_1 = (\theta_1, \phi_1)$ and $\mathfrak{f}_2 = (\theta_2, \phi_2)$ is the fractional ideal $\mathfrak{f}_1\mathfrak{f}_2 = (\theta_1\phi_1, \theta_1\phi_2, \theta_2\phi_1, \theta_2\phi_2)$. 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 forms 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 $K/k(x)$.

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_2, 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

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 $\pmod P$, and $q \equiv -1 \pmod 3$, then D has a unique cube root $X \pmod P$ 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 $X_i, Y_i \in k[x]$ and
$$\begin{aligned} X_1 &\equiv \begin{cases} X & \pmod P, \\ 0 & \pmod H, \end{cases} \quad \text{or equivalently, } X_1 \equiv XY_1H \pmod{PH}, \\ X_{i+1} &= X_i + A_i(D - X_i^3) \quad \text{where } 3X_i^2 A_i \equiv 1 \pmod{P^i}, \\ Y_i H &\equiv 1 \pmod{P^i} \qquad (i \in \mathbb{N}). \end{aligned}$$
Note that $X_i^3 \equiv D \pmod{P^i}$ and $X_i \equiv 0 \pmod H$ 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 $\pmod P$, and $q \equiv 1 \pmod 3$, then D has three distinct cube roots $X, X', X'' \pmod P$ in $k[x]$. In this case, $(P) = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ where for $i, j \in \mathbb{N}$:*
$$\begin{aligned} \mathfrak{p}^i &= [P^i, -X_i + \rho, -X_i^2 Y_i + \omega], \\ (\mathfrak{p}\mathfrak{p}')^i &= [P^i, P^i\rho, (X_i'')^2 Y_i + X_i'' Y_i \rho + \omega], \\ \mathfrak{p}^{i+j}(\mathfrak{p}')^i &= [P^{i+j}, P^i(-X_j + \rho), (X_i'')^2 Y_i + P^i Q_{ij} + X_i'' Y_i \rho + \omega], \end{aligned}$$
with $X_i, X_i', X_i'', Y_i, Q_{ij} \in k[x]$ and
$$\begin{aligned} X_1 &\equiv \begin{cases} X & \pmod P, \\ 0 & \pmod H, \end{cases} \quad \text{or equivalently, } X_1 \equiv XY_1H \pmod{PH}, \\ X_{i+1} &= X_i + A_i(D - X_i^3) \text{ where } 3X_i^2 A_i \equiv 1 \pmod{P^i}, \\ Y_i H &\equiv 1 \pmod{P^i}, \\ Q_{ij}(X_j - X_i'')/H &\equiv (X_i''^3 - D)/H^2 P^i \pmod{P^j} \qquad (i, j \in \mathbb{N}). \end{aligned}$$

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* $X_i^3 \equiv (X_i')^3 \equiv (X_i'')^3 \equiv D \pmod{P^i}$ *and* $X_i \equiv X_i' \equiv X_i'' \equiv 0 \pmod{H}$ *for all* $i \in \mathbb{N}$*.* $\mathfrak{p}$ *and* $\mathfrak{q}$ *are called* type 4 *prime ideals.*

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

Proof: We only consider type 1, type 3, and type 5 prime ideals; the proofs for type 2 and type 4 prime ideals are analogous to the type 1 and type 3 cases, respectively.

Type 1: If $P \mid G$, then $y^3 - D \equiv y^3 \pmod{P}$, so $(P) = \mathfrak{p}^3$ with $\mathfrak{p} = (P, \rho)$. Let $\mathfrak{a} = [P, \rho, \omega]$. Since $\rho\omega = P(G/P)H \in \mathfrak{a}$, $\mathfrak{a}$ is an ideal, and $\mathfrak{p} \subseteq \mathfrak{a}$. Since $P \nmid H$, there exist $U, V \in k[x]$ with $UP + VH = 1$, so $\omega = (UP + VH)\omega = UP + (V\rho)\rho \in \mathfrak{p}$ and hence $\mathfrak{a} \subseteq \mathfrak{p}$.

Now $\mathfrak{a}^2 = [P^2, P\rho, P\omega, H\omega, H(G/P)P, (G/P)P\rho] \subseteq [P, P\rho, \omega]$. Conversely, $\omega = U(P\omega) + V(H\omega) \in \mathfrak{a}^2$. Since $\gcd(P, GH/P) = 1$, $1 = SP + TGH/P$ for some $S, T \in k[x]$. Then $P = SP^2 + TH(G/P)P \in \mathfrak{a}^2$, so $[P, P\rho, \omega] \subseteq \mathfrak{a}^2$.

Type 3: If D is a nonzero cube $\pmod{P}$ and $q \equiv -1 \pmod{3}$, then

$$y^3 - D \equiv (y - X)(y^2 + Xy + X^2) \pmod{P}$$

where $y^2 + Xy + X^2$ is irreducible $\pmod{P}$. So $(P) = \mathfrak{p}\mathfrak{q}$ with $\mathfrak{p} = (P, X - \rho)$ and $\mathfrak{q} = (P, X^2 + X\rho + \rho^2)$. Let $\mathfrak{a}_i = [P^i, -X_i + \rho, -X_i^2 Y_i + \omega]$ where X_i, Y_i are defined as in the Theorem. It is easy to verify that

$$\begin{aligned}
P^i\rho &= X_iP^i + P^i(-X_i + \rho) \in \mathfrak{a}_i, \\
P^i\omega &= X_i^2Y_iP^i + P^i(-X_i^2Y_i + \omega) \in \mathfrak{a}_i, \\
(-X_i + \rho)\rho &= \left(X_i^2(HY_i - 1)/P^i\right)P^i - X_i(-X_i + \rho) + H(-X_i^2Y_i + \omega) \in \mathfrak{a}_i, \\
(-X_i + \rho)\omega &= \left((GH - X_i^3Y_i)/P^i\right)P^i - X_i(-X_i^2Y_i + \omega) \in \mathfrak{a}_i, \\
(-X_i^2Y_i + \omega)\rho &= \left((GH - X_i^3Y_i)/P^i\right)P^i - X_i^2Y_i(-X_i + \rho) \in \mathfrak{a}_i, \\
(-X_i^2Y_i + \omega)\omega &= \left(X_i(G - X_i^3Y_i^2)/P^i\right)P^i + G(-X_i + \rho) - X_i^2Y_i(-X_i^2Y_i + \omega) \in \mathfrak{a}_i,
\end{aligned}$$

so $\mathfrak{a}_i$ is an ideal for all $i \in \mathbb{N}$. We use induction on i to prove that $\mathfrak{a}_i = \mathfrak{p}^i$ for all $i \in \mathbb{N}$. $\mathfrak{p} \subseteq \mathfrak{a}_1$ is obvious. Since $-X_1 + \rho \in \mathfrak{p}$ and $-X_1^2Y_1 + \omega = -Y_1(X + \rho)(X - \rho) + AP \in \mathfrak{p}$ for some $A \in k[x]$, we have $\mathfrak{a}_1 = \mathfrak{p}$. Now the following congruences hold:

$$\begin{aligned}
P^iX_1 &\equiv P^iX_{i+1} \pmod{P^{i+1}}, \\
PX_i &\equiv PX_{i+1} \pmod{P^{i+1}},
\end{aligned}$$

Analogous congruences hold if the letter X is replaced by the letter Y, using the same subscripts. If is now simple to verify that any product of a basis element in $\mathfrak{p}^i$ by a basis element of $\mathfrak{p}$ is in $\mathfrak{a}_{i+1}$, hence $\mathfrak{p}^{i+1} \subseteq \mathfrak{a}_{i+1}$. For the other subset inequality, let $U = (X_i^4 Y_i/H)(Y_i H + 2)$, $V = G - 4X_i^3 Y_i/H$. Then $U, V \in k[x]$ and $V \equiv -3G \pmod{P}$, so $\gcd(V, P) = 1$. Let $ZV \equiv 1 \pmod{P^{i+1}}$. A straightforward computation shows that $V(2X_i^3 + D) + 3X_i^2 U \equiv 0 \pmod{P^{i+1}}$. It follows that

$$\begin{aligned} 0 &\equiv V(2X_i^3 + D) + 3X_i^2 U \equiv V(3X_i^3 + (D - X_i^3)) + 3X_i^2 U \\ &\equiv V(3X_i^3 + 3X_i^2 A_i(D - X_i^3)) + 3X_i^2 U \equiv 3X_i^2 (V X_{i+1} + U) \\ &\equiv 3X_i^2 V(X_{i+1} + UZ) \pmod{P^{i+1}}. \end{aligned}$$

Hence, $ZU \equiv -X_{i+1} \pmod{P^{i+1}}$. Let $\theta = (2X_i^2 Y_i/H)(X_i - \rho)^2 + (X_i^2 Y_i - \omega)^2 \in \mathfrak{p}^{2i} \subseteq \mathfrak{p}^{i+1}$. Then $\theta = U + V\rho$, so $Z\theta \equiv -X_{i+1} + \rho \pmod{P^{i+1}}$. Hence $-X_{i+1} + \rho \in \mathfrak{p}^{i+1}$ and

$$-X_{i+1}^2 Y_{i+1} + \omega = -Y_{i+1}(X_{i+1} + \rho)(X_{i+1} - \rho) + AP^{i+1} \in \mathfrak{p}^{i+1}$$

for some $A \in k[x]$, implying $\mathfrak{a}_{i+1} \subseteq \mathfrak{p}^{i+1}$. Analogous congruences can be used to show that $\mathfrak{q}^i = [P^i, P^i\rho, X_i^2 Y_i + X_i Y_i \rho + \omega]$ for all $i \in \mathbb{N}$.

Type 5: If D is not a cube $\pmod{P}$, then $y^3 - D$ is irreducible $\pmod{P}$, so (P) is inert and $(P) = P\mathcal{O} = [P, P\rho, P\omega]$. □

Clearly, a purely cubic function field contains either type 3 or type 4 prime ideals, but not both. Note also that prime ideals of types 1–4 are primitive, while type 5 prime ideals are not.

4 Canonical Bases and Ideal Multiplication

All the prime ideals of types 1–4 and their primitive powers have a $k[x]$-basis of the following kind:

$$\begin{aligned} &\{s,\ s'(u + \rho),\ s''(v + w\rho + \omega)\}; \\ &s, s', s'', u, v, w \in k[x] \quad \text{with} \quad s's'' \mid s,\ \gcd(s', H) = 1,\ s'' \mid H. \end{aligned}$$

Such a basis is called a *canonical basis* of the ideal. Note that the divisibility conditions above imply $\gcd(s', s'') = 1$. In addition, the following congruences are easily seen to be satisfied:

$$Hv - Huw + u^2 \equiv 0 \pmod{s/s'} \tag{4.1}$$

$$v \equiv Hw^2 \pmod{s'} \tag{4.2}$$

$$u(v - Hw^2) \equiv H(G - vw) \pmod{s/s''} \tag{4.3}$$

We will prove that every primitive ideal has a canonical basis, and that every such basis satisfies congruences (4.1) – (4.3) as well as (4.4) – (4.8) below. We also show how to determine containment and equality of ideals using canonical bases, compute the product of two ideals using canonical bases, and find a canonical basis from an arbitrary $k[x]$-basis.

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 ideals with* $s_i, s_i', s_i'', u_i, v_i, w_i \in k[x]$, $s_i's_i'' \mid s_i$, $s_i'' \mid H$, *and* $\gcd(s_i', H) = 1$ *for* $i = 1, 2$. *Then* $\mathfrak{a}_2 \subseteq \mathfrak{a}_1$ *if and only if*

$$\begin{aligned}
s_1 &\mid s_2, \quad s_1' \mid s_2', \quad s_1'' \mid s_2'', \\
s_2'u_2 &\equiv s_2'u_1 \ (mod\ s_1), \\
s_2''w_2 &\equiv s_2''w_1 \ (mod\ s_1'), \\
s_2''v_2 &\equiv s_2''(v_1+u_1(w_2-w_1)) \ (mod\ s_1).
\end{aligned}$$

Proof: $\mathfrak{a}_2 \subseteq \mathfrak{a}_1$ if and only if $s_2, s_2(u_2+\rho), s_2''(v_2+w_2\rho+\omega) \in \mathfrak{a}_1$, or equivalently, there exists a 3 by 3 matrix $A = (a_{ij})$ with polynomial entries such that

$$\begin{pmatrix} s_2 & 0 & 0 \\ s_2'u_2 & s_2' & 0 \\ s_2''v_2 & s_2''w_2 & s_2'' \end{pmatrix} = A \begin{pmatrix} s_1 & 0 & 0 \\ s_1'u_1 & s_1' & 0 \\ s_1''v_1 & s_1''w_1 & s_1'' \end{pmatrix}.$$

It is easy to infer that A is lower triangular and that $s_2 = a_{11}s_1$, $s_2' = a_{22}s_1'$, $s_2'' = a_{33}s_1''$, $s_2'u_2 = s_2'u_1 + a_{21}s_1$, $s_2''w_2 = s_2''w_1 + a_{32}s_1'$, and $s_2''v_2 = s_2''v_1 + s_2''u_1(w_2-w_1) + a_{31}s_1$. □

Corollary 4.2 *Let* $\mathfrak{a}_1$ *and* $\mathfrak{a}_2$ *be as in Lemma 4.1. Then* $\mathfrak{a}_1 = \mathfrak{a}_2$ *if and only if*

$$\begin{aligned}
s_1 &= as_2, \quad s_1' = a's_2', \quad s_1'' = a''s_2'' \qquad (a, a', a'' \in k^*), \\
u_1 &\equiv u_2 \ (mod\ s_1/s_1'), \\
w_1 &\equiv w_2 \ (mod\ s_1'), \\
v_1 &\equiv v_2 + u_2(w_1-w_2)) \ (mod\ s_1/s_1'').
\end{aligned}$$

Theorem 4.3 *Let* $\mathfrak{a}_1$ *and* $\mathfrak{a}_2$ *be as in Lemma 4.1, and suppose that* $\gcd(s_1, s_2) = 1$. *Then* $\mathfrak{a}_1\mathfrak{a}_2 = [s_3, s_3'(u_3+\rho), s_3''(v_3+w_3\rho+\omega)]$ *where*

$$\begin{aligned}
s_3 &= s_1s_2, \quad s_3' = s_1's_2', \quad s_3'' = s_1''s_2'', \\
u_3 &\equiv \begin{cases} u_1 \ (mod\ s_1/s_1'), \\ u_2 \ (mod\ s_2/s_2'), \end{cases} \\
w_3 &\equiv \begin{cases} w_1 \ (mod\ s_1'), \\ w_2 \ (mod\ s_2'), \end{cases} \\
v_3 &\equiv \begin{cases} v_1 + u_1(w_3-w_1) \ (mod\ s_1/s_1''), \\ v_2 + u_2(w_3-w_2) \ (mod\ s_2/s_2''). \end{cases}
\end{aligned}$$

Proof: Let $\mathfrak{a}_1\mathfrak{a}_2 = [s_3, s_3'(u_3+\rho), s_3''(v_3+w_3\rho+\omega)]$. We need to show that $s_3, s_3', s_3'', u_3, v_3, w_3$ are given as above. Assume without loss of generality that $s_i, s_i'.s_i''$ are monic for $i = 1, 2, 3$. Since $\gcd(s_1, s_2) = 1$ and $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1, \mathfrak{a}_2$, by Lemma 4.1 $s_1 s_2 \mid s_3$, $s_1' s_2' \mid s_3'$, $s_1'' s_2'' \mid s_3''$. Since $s_3 s_3' s_3'' = N(\mathfrak{a}_1\mathfrak{a}_2) = N(\mathfrak{a}_1)N(\mathfrak{a}_2) = s_1 s_1' s_1'' s_2 s_2' s_2''$, we have $s_3 = s_1 s_2$, $s_3' = s_1' s_2'$, $s_3'' = s_1'' s_2''$. Also by Lemma 4.1:

$$\begin{aligned} s_3' u_3 &\equiv s_3' u_1 \pmod{s_1}, \\ s_3'' w_3 &\equiv s_3'' w_1 \pmod{s_1'}, \\ s_3'' v_3 &\equiv s_3''(v_1 + u_1(w_3 - w_1)) \pmod{s_1}. \end{aligned}$$

Since $\gcd(s_1, s_2') = 1$, $s_1 \mid s_1' s_2'(u_3 - u_1)$ implies $(s_1/s_1') \mid u_3 - u_1$. Similarly, $\gcd(s_1', s_1'' s_2'') = 1$ implies $s_1' \mid w_3 - w_1$. Finally, we obtain $(s_1/s_1'') \mid v_3 - v_1 - u_1(w_3 - w_1)$. Analogous divisibility relations hold for u_2, v_2, w_2. □

Corollary 4.4 *Every primitive ideal* $\mathfrak{a}$ *has a canonical basis* $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$. *Furthermore,* $s = sgn(s)L(\mathfrak{a})$.

Proof: By Theorem 3.1, every primitive ideal $\mathfrak{a}$ is the product of pairwise coprime primitive powers of type 1–4 prime ideals, each of which has a canonical basis. By Theorem 4.3, the product of all these canonical bases is a canonical basis of $\mathfrak{a}$. $s = \mathrm{sgn}(s)L(\mathfrak{a})$ follows from the fact that s divides any polynomial in $\mathfrak{a}$. □

Lemma 4.5 *Let* $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ *be as in Theorem 4.3. If* $s_i, s_i', s_i'', u_i, v_i, w_i$ *satisfy the congruences (4.1) – (4.3) for* $i = 1, 2$, *then so do* $s_3, s_3', s_3'', u_3, u_3', u_3$.

Proof: Let $u_3 = u_1 + as_1/s_1'$, $w_3 = w_1 + bs_1'$, $v_3 = v_1 + bu_1 s_1' + cs_1/s_1''$ with $a, b, c \in k[x]$. Then $v_3 - u_3 w_3 \equiv v_1 - u_1 w_1 + cs_1/s_1'' \pmod{s_1/s_1'}$, hence since $s_1'' \mid H$,

$$H(v_3 - u_3 w_3) \equiv H(v_1 - u_1 w_1) \pmod{s_1/s_1'}.$$

Analogously, $H(v_3 - u_3 w_3) \equiv H(v_2 - u_2 w_2) \pmod{s_2/s_2'}$. Since $\gcd(s_1, s_2) = 1$ and $u_3 \equiv u_i \pmod{s_i/s_i'}$ for $i = 1, 2$, (4.1) follows. Since $s_i' \mid (s_i/s_i'')$ and $s_i' \mid w_3 - w_i'$ for $i = 1, 2$, (4.2) is clear. Finally,

$$\begin{aligned} u_3(v_3 - Hw_3^2) - H(G - v_3 w_3) & \\ &\equiv u_1(v_1 - Hw_1^2) - H(G - v_1 w_1) + a(v_1 - Hw_1^2)s_1/s_1' + b(u_1^2 - Hu_1 w_1 + Hv_1)s_1' \\ &\equiv 0 \pmod{s_1/s_1''}, \end{aligned}$$

using (4.1) – (4.3) for the basis of $\mathfrak{a}_1$; similarly for the basis of $\mathfrak{a}_2$. □

Lemma 4.6 *Every canonical basis satisfies congruences (4.1) – (4.3).*

Proof: Let $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$ be a canonical basis of an ideal $\mathfrak{a}$ satisfying (4.1) – (4.3); such a basis exists by Theorem 3.1 and Lemma 4.5. Let $\{\tilde{s}, \tilde{s}'(\tilde{u}+\rho), \tilde{s}''(\tilde{v}+\tilde{w}\rho+\omega)\}$ be another canonical basis of $\mathfrak{a}$. After normalizing appropriately, we infer from Corollary 4.2 that $s = \tilde{s}$, $s' = \tilde{s}'$, $s'' = \tilde{s}''$, and

$$\begin{aligned} u &\equiv \tilde{u} \pmod{s/s'}, \\ w &\equiv \tilde{w} \pmod{s'}, \\ v &\equiv \tilde{v} + \tilde{u}(w - \tilde{w}) \pmod{s/s''}. \end{aligned}$$

Let $u = \tilde{u} + as/s'$, $w = \tilde{w} + bs'$, and $v = \tilde{v} + b\tilde{u}s' + cs/s''$ with $a, b, c \in k[x]$. Proceeding analogously to the proof of the previous Lemma, we derive (4.1) – (4.3) for our second canonical basis. $\square$

Lemma 4.7 *Let $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$ be a canonical basis. Then the following congruences hold:*

$$\begin{aligned} u &\equiv 0 \ (mod\ s''), && (4.4) \\ vw &\equiv G \ (mod\ s'), && (4.5) \\ u^3 &\equiv -D \ (mod\ s/s'), && (4.6) \\ Hw^3 &\equiv G \ (mod\ s'), && (4.7) \\ Hv(v+Hw^2) &\equiv H\big(2GHw + u(Hw^3 - G)\big) \ \ (mod\ s/s''). && (4.8) \end{aligned}$$

Proof: By the previous Lemma, congruences (4.1) – (4.3) are satisfied. $s'' \mid u$ follows from (4.1) and the fact that $s'' \mid H$, $s'' \mid (s/s')$, and s'' is squarefree. $vw \equiv G \pmod{s'}$ can be obtained by combining (4.2) and (4.3). From (4.3),

$$(s/s') \mid (Hs/s'') \mid H^2vw + Huv - H^2uw^2 - D.$$

By (4.1) $(s/s') \mid H^2vw - H^2uw^2 + Hu^2w$. Taking differences yields

$$(s/s') \mid u(Hv - Huw) - D,$$

so again by (4.1) $(s/s') \mid u^3 + D$. From (4.2) and (4.5) $Hw^3 \equiv vw \equiv G \pmod{s'}$. Now from (4.1) and (4.2) $s \mid (v - Hw^2)(Hv - Huw + u^2)$, so

$$Hv(v - Hw^2) \equiv (Huw - u^2)(v - Hw^2) \pmod{s}$$

and

$$\begin{aligned} Hv(v+Hw^2) &= Hv(v-Hw^2)+2H^2vw^2 \\ &\equiv (Huw-u^2)(v-Hw^2)+H^2vw^2 \\ &\equiv (Hw-u)uv+H(Huw^3+u^2w^2+2Hvw^2) \pmod{s}. \end{aligned}$$

Substituting for uv using (4.3), we obtain

$$\begin{aligned} Hv(v+Hw^2) &\equiv H\left((Hw-u)(G-vw+uw^2)+Huw^3+u^2w^2+2Hvw^2\right) \\ &\equiv H\left(G(Hw-u)+w(Hvw+uv)\right) \pmod{s/s''}. \end{aligned}$$

Again by (4.3) $Hvw+uv \equiv GH+Huw^2 \pmod{s/s''}$, so

$$Hv(v+Hw^2) \equiv H(2GHw+u(Hw^3-G)) \pmod{s/s''}. \qquad \square$$

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* $s's'' \mid s$, $s'' \mid H$, *and* $\gcd(s', H) = 1$. *Here,* $s = sgn(s)d(\mathfrak{f})$.

2. *Every canonical basis* $\{1, s'(u+\rho)/s, s''(v+w\rho+\omega)/s\}$ *of a fractional ideal containing 1 satisfies congruences (4.1) – (4.8).*

3. *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 basis 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 4.3.*

The following Lemma describes how to obtain a canonical basis from any basis of a fractional ideal containing 1.

Lemma 4.9 *Let* $\mathfrak{f} = [1, \mu, \nu]$ *be a fractional ideal where* $\mu = (m_0+m_1\rho+m_2\omega)/d$, $\nu = (n_0+n_1\rho+n_2\omega)/d$ *with* $m_0, m_1, m_2, n_0, n_1, n_2, d \in k[x]$ *and* $\gcd(m_0, m_1, m_2, n_0, n_1, n_2, d) = 1$. *Then a canonical basis* $\{1, s'(u+\rho)/s, s''(v+w\rho+\omega)/s\}$ *of* $\mathfrak{f}$ *is given as follows:*

$$s'' = \gcd(m_2, n_2), \quad s' = (m_1n_2 - n_1m_2)/s'', \quad s = d.$$

Let $a', b', t \in k[x]$ *satisfy* $a'm_2 + b'n_2 = s''$ *and* $s't \equiv a'm_1 + b'n_1 \pmod{s''}$. *Set* $a = a' - tn_2/s''$, $b = b' + tm_2/s''$, $m_0' = m_0/s'' \in k[x]$, $n_0' = n_0/s'' \in k[x]$. *Then*

$$\begin{aligned} u &\equiv (m_0'n_2 - n_0'm_2)/s' \pmod{s/s'} \\ v &\equiv am_0' + bn_0' \pmod{s/s''}, \\ w &\equiv (am_1 + bn_1)/s'' \pmod{s'} \end{aligned}$$

Proof: Let $\{1, s'(u+\rho)/s', s''(v+w\rho+\omega)/s''\}$ be a canonical basis of $\mathfrak{f}$ and assume without loss of generality that s, s', s'', and d are monic. Then by Theorem 4.8, $s = d(\mathfrak{f}) = d$. Furthermore, $N(s\mathfrak{f}) = ss's'' = d(m_1n_2 - n_1m_2)$, so $s's'' = m_1n_2 - n_1m_2$. Let $A = (a_{ij})$ be the 3 by 3 nonsingular matrix with polynomial entries satisfying

$$\begin{pmatrix} d & 0 & 0 \\ m_0 & m_1 & m_2 \\ n_0 & n_1 & n_2 \end{pmatrix} = A \begin{pmatrix} s & 0 & 0 \\ s'u & s' & 0 \\ s''v & s''w & s'' \end{pmatrix}. \tag{4.9}$$

It is easy to see that the top row of A is $(1, 0, 0)$. Furthermore, the last column on both sides of equality (4.9) shows that $m_2 = a_{23}s''$ and $n_2 = a_{33}s''$. Since $\det(A) = 1$, we must have $\gcd(a_{23}, a_{33}) = 1$. It follows that $s'' = \gcd(m_2, n_2)$. Set $a = -(a_{32} + ta_{33})$ and $b = a_{22}+ta_{23}$ where $ts' \equiv a_{22}n_1 - a_{32}m_1 \pmod{s''}$. Then $am_2+bn_2 = -a_{32}a_{23}s''+a_{22}a_{33}s'' = s''$ and $am_1 + bn_1 = ts' + t(a_{23}n_1 - a_{33}m_1 \equiv 0 \pmod{s''}$. Therefore a and b are as specified in the Lemma. It is now easy to see that

$$A = \begin{pmatrix} 1 & 0 & 0 \\ g & b & m_2/s'' \\ h & -a & n_2/s'' \end{pmatrix}$$

for suitable $g, h \in k[x]$. The second column of the matrix equality (4.9) yields $bs' + m_2w = m_1$ and $-as' + n_2w = n_1$, implying $w = (am_1 + bn_1)/s''$. Similarly, by comparing the first columns of either side of equality (4.9), we obtain $bs'u + m_2v \equiv m_0 \pmod{s}$ and $-as'u + n_2v \equiv n_0 \pmod{s}$. It follows from (4.4) that $s'' \mid m_0$, $s'' \mid n_0$, $s's''u \equiv m_0n_2 - n_0m_2 \pmod{s}$, so $s' \mid m_0'n_2 - n_0'm_2$ and $u \equiv (m_0'n_2 - n_0'm_2)/s' \pmod{s/s'}$ with $m_0' = m_0/s''$, $n_0' = n_0/s''$. Finally, $v \equiv am_0' + bn_0' \pmod{s/s''}$. □

5 Squaring of Ideals

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.

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 $\{s, s'(u + \rho), s''(v' + w'\rho + \omega)\}$ is also a canonical basis of $\mathfrak{a}$ by Corollary 4.2.

Furthermore, $\gcd(2v' + H(w')^2, s') = 1$, for if $p \in k[x]$ is any irreducible polynomial divisor of this gcd, then by (4.2) $2v' + H(w')^2 \equiv 3v' \equiv 3H(w')^2 \pmod{s'}$, so $p \mid v'$ and $p \mid w'$ as $\gcd(s', H) = 1$. But then (4.3) would imply $p \mid GH$, contradicting $\gcd(s, GH) = 1$.

Suppose that $s/s' \notin k$ and let $p_1, p_2, \ldots, p_r \in k[x]$ be all the distinct irreducible polynomials dividing s, but not s'. Note that no p_i divides $s'H$. Let a be a square root of 3 (possibly in some extension of k) and choose $f \in k[x]$ so that $Hs'f \not\equiv (-1 \pm a)u - Hw \pmod{p_i}$ in $k(a)[x]$ for all $i \in \{1, 2, \ldots, r\}$ (such an f certainly exists). Set $w' = w + fs'$ and $v' = v + fus'$ and let $p \in \{p_1, p_2, \ldots, p_r\}$. Then $Hw' \not\equiv (-1 \pm a)u \pmod{p}$, so $p \nmid (Hw' + u)^2 - 3u^2 = H^2(w')^2 + 2Huw' - 2u^2$. Now by (4.1) $Huw' - u^2 \equiv Hv \pmod{p}$, 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.

Lemma 5.2 *Let $\mathfrak{a}$ be a primitive ideal.*

1. *If $\mathfrak{a}$ is the product of type 1 prime ideals, then $\mathfrak{a} = [s, s'\rho, \omega]$ and $\mathfrak{a}^2 = (s')[s, (s/s')\rho, \omega]$ with $s, s' \in k[x]$ and $s' \mid s \mid G$.*
2. *If $\mathfrak{a}$ is the product of type 2 prime ideals, then $\mathfrak{a} = [s, \rho, s''\omega]$ and $\mathfrak{a}^2 = (s'')[s, \rho, (s/s'')\omega]$ with $s, s'' \in k[x]$ and $s'' \mid s \mid H$.*
3. *If $\mathfrak{a}$ is the product of type 3 or type 4 prime ideals, then $\mathfrak{a} = [s, s'(u+\rho), v + w\rho + \omega]$ and $\mathfrak{a}^2 = [s^2, (s')^2(U + \rho), V + W\rho + \omega]$ with suitable $s, s', u, v, w, U, V, W \in k[x]$, $s' \mid s$, and $\gcd(s, GH) = 1$.*
4. *If $p \in k[x]$ is an irreducible divisor of $\gcd(L(\mathfrak{a}), GH)$, then $p^2 \nmid L(\mathfrak{a})$.*

Proof: Parts 1-3 follow immediately from Theorem 3.1. To prove part 4, write $\mathfrak{a} = \mathfrak{a}_2\mathfrak{a}_2\mathfrak{a}_3$ 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. Set $s = L(\mathfrak{a})$ and $s_i = L(\mathfrak{a}_i)$ for $i = 1, 2, 3$. By parts 1-3 of the Lemma, $s_1 \mid G$, $s_2 \mid H$, and $\gcd(s_3, GH) = 1$; in particular, s_1, s_2, and s_3 are pairwise coprime. By Theorem 4.3, $s = s_1s_2s_3$. Suppose $p \mid \gcd(s, GH)$, then $p \mid s_1s_2$, $p^2 \nmid s_1s_2$ (as GH is squarefree), and $p \nmid s_3$, so $p^2 \nmid s$. □

Lemma 5.3 *Let $\{s, s'(u + \rho), v + w\rho + \omega\}$ be a canonical basis of an ideal $\mathfrak{a}$ with* $\gcd(s, GH) = \gcd(s, 2v + Hw^2) = 1$. *Then a canonical basis of $\mathfrak{a}^2$ is given by $\{s^2, (s')^2(U + \rho), V + W\rho + \omega\}$ where*

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

with $3u^2y \equiv 1 \pmod{s/s'}$ *and* $(2v + Hw^2)z \equiv 1 \pmod{s}$.

Proof: By part 3 of Lemma 5.2, $\mathfrak{a}^2 = [s^2, (s')^2(U+\rho), V+W\rho+\omega]$ with suitable $U, V, W \in k[x]$, so we need to show that U, V, W are in fact given as above.

Since $ss'(u+\rho) \in \mathfrak{a}^2$, we have $ss'(u+\rho) = as^2 + b(s')^2(U+\rho)$ for some $a, b \in k[x]$. Comparing coefficients of ρ and 1 yields $b = s/s'$ and $U = u - as/s'$, so we need to find a. Since $\gcd(s, D) = 1$ and $u^3 \equiv -D \pmod{s/s'}$ by (4.6), we have $\gcd(u, s/s') = 1$, so y as given above exists. Furthermore, $3u^2y \equiv 1 \pmod{s/s'}$ implies $as/s' \equiv 3u^2ays/s' \pmod{(s/s')^2}$. Now (4.6) for U yields $-D \equiv U^3 \equiv u^3 - 3u^2as/s' \pmod{(s/s')^2}$, so

$$y(u^3 + D) \equiv 3u^2ays/s' \equiv as/s' \equiv u - U \pmod{(s/s')^2}.$$

Similarly, $(v + w\rho + \omega)^2 = (v^2 + 2GHw) + (G + 2vw)\rho + (Hw^2 + 2v)\omega \in \mathfrak{a}^2$ yields

$$(v^2 + 2GHw) + (G + 2vw)\rho + (Hw^2 + 2v)\omega = cs^2 + d(s')^2(U+\rho) + e(V + W\rho + \omega) \quad (5.1)$$

for some $c, d, e \in k[x]$. Then $e = Hw^2 + 2v$ and $G + 2vw \equiv (Hw^2 + 2v)W \pmod{(s')^2}$. Subtracting the equality $Hw^3 + 2vw = (Hw^2 + 2v)w$ yields

$$G - Hw^3 \equiv (Hw^2 + 2v)(W - w) \pmod{(s')^2}.$$

Since $\gcd(Hw^2 + 2v, s) = 1$, z as given above exists, and since $s' \mid G - Hw^3$ by (4.7), $z(G - Hw^3) \equiv W - w \pmod{(s')^2}$.

Finally, from (5.1), $G + 2vw = d(s')^2 + eW$ with $e = Hw^2 + 2v$, so

$$d(s')^2 = G + 2vw - (Hw^2 + 2v)W.$$

Then again by (5.1),

$$v^2 + 2GHw \equiv d(s')^2U + eV \equiv (G + 2vw)U - (Hw^2 + 2v)UW + (Hw^2 + 2v)V \pmod{s^2}$$

and hence

$$\begin{aligned}
(Hw^2 + 2v)V &\equiv v^2 + 2GHw - (G + 2vw)U + (Hw^2 + 2v)UW \\
&\equiv (Hw^2 + 2v)\left(v + U(W - w)\right) - Hw^2v - v^2 + Hw^3U + 2GHw - GU \\
&\equiv (Hw^2 + 2v)\left(v + U(W - w)\right) \\
&\qquad + U(Hw^3 - G) - v(Hw^2 + v) + 2GHw \pmod{s^2},
\end{aligned}$$

Now (4.7) together with the definition of U implies $U(Hw^3 - G) \equiv u(Hw^3 - G) \pmod{s}$, so from (4.8) $U(Hw^3 - G) - v(Hw^2 + v) + 2GHw \equiv 0 \pmod{s}$ and $V \equiv v + U(W - w) \pmod{s}$. Hence $V \equiv v + U(W - w) + z\left(U(Hw^3 - G) - v(Hw^2 + v) + 2GHw\right) \pmod{s^2}$. □

Theorem 5.4 *Let $\{s, s'(u+\rho), s''(v+w\rho+\omega)\}$ be a canonical basis of an ideal $\mathfrak{a}$. Let $s_G = \gcd(S,G)$, $s_H = \gcd(s,H)$, $s'_G = \gcd(s',G)$, and assume that $\gcd(2v+Hw^2, s/s_Gs_H) = 1$. Then $\mathfrak{a}^2 = (s'_Gs'')[S, S'(U+\rho), S''(V+W\rho+\omega)]$ where $\{S, S'(U+\rho), S''(V+W\rho+\omega)\}$ is a canonical basis that is given as follows.*

$$
\begin{aligned}
S &= s^2/s_Gs_H, \quad S' = (s')^2s_G/(s'_G)^3, \quad S'' = s_H/s'',\\
U &\equiv \begin{cases} 0 & (\mathit{mod}\ s_Hs'_G),\\ u - y(u^3+D) & (\mathit{mod}\ (ss'_G/s_Gs_Hs')^2),\end{cases}\\
W &\equiv \begin{cases} 0 & (\mathit{mod}\ s_G/s'_G),\\ w - z(Hw^3-G) & (\mathit{mod}\ (s'/s'_G)^2),\end{cases}\\
V &\equiv \begin{cases} 0 & (\mathit{mod}\ s_Gs''),\\ v + U(W-w) + z\left(U(Hw^3-G) + 2GHw - v(v+Hw^2)\right) & (\mathit{mod}\ (s/s_Gs_H)^2),\end{cases}
\end{aligned}
$$

where $3u^2y \equiv 1 \ (\mathit{mod}\ ss'/s_Gs_Hs'_G)$ and $(2v+Hw^2)z \equiv 1 \ (\mathit{mod}\ s/s_Gs_H)$.

Proof: We first observe that by part 4 of Lemma 5.2, $\gcd(s/s_Gs_H, GH) = 1$, so it is always possible to achieve $\gcd(2v+Hw^2, s/s_Gs_H) = 1$ by Lemma 5.1. 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 parts 1 and 2 of Lemma 5.2, $\mathfrak{a}_1 = [s_G, s'_G\rho, \omega]$, $\mathfrak{a}_2 = [s_H, \rho, s''\omega]$, $\mathfrak{a}_1^2 = (s'_G)[s_G, (s_G/s'_G)\rho, \omega]$, and $\mathfrak{a}_2^2 = (s'')[s_H, \rho, (s_H/s'')\omega]$. By Theorem 4.3, $\mathfrak{a}_1^2\mathfrak{a}_2^2 = (s'_Gs'')[s_Gs_H, (s_G/s'_G)\rho, (s_H/s'')\omega]$.

Again by Theorem 4.3, $\mathfrak{a}_3 = [\tilde{s}, \tilde{s}'(u+\rho), v+w\rho+\omega]$ where $\tilde{s} = s/s_Gs_H$ and $\tilde{s}' = s'/s'_G$. Since $\gcd(\tilde{s}, GH) = \gcd(\tilde{s}, 2v+Hw^2) = 1$, by Lemma 5.3 $\mathfrak{a}_3^2 = \{\tilde{s}^2, (\tilde{s}')^2(\tilde{u}+\rho), \tilde{v}+\tilde{w}\rho+\omega]$ where

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

with $3u^2u \equiv 1 \ (\mathrm{mod}\ \tilde{s}/\tilde{s}')$ and $(2v+Hw^2)z \equiv 1 \ (\mathrm{mod}\ \tilde{s})$, so y and z are as stated in the Theorem. Since $\gcd(s_Gs_H, \tilde{s}^2) = 1$, by Theorem 4.3,

$$\mathfrak{a}^2 = (s'_Gs'')[\tilde{s}^2s_Gs_H, (\tilde{s}')^2s_G/s'_G(U+\rho), (s_H/s'')(V+W\rho+\omega)]$$

where

$$U \equiv \begin{cases} 0 & (\mathrm{mod}\ s_Hs'_G),\\ \tilde{u} & (\mathrm{mod}\ (\tilde{s}/\tilde{s}')^2),\end{cases} \quad W \equiv \begin{cases} 0 & (\mathrm{mod}\ (s_G/s'_G)),\\ \tilde{w} & (\mathrm{mod}\ (\tilde{s}')^2),\end{cases} \quad V \equiv \begin{cases} 0 & (\mathrm{mod}\ s_Gs''),\\ \tilde{v} & (\mathrm{mod}\ \tilde{s}^2).\end{cases} \qquad \square$$

Corollary 5.5 *Let $\{1, s'(u+\rho)/s, s''(v+w\rho+\omega)/s\}$ be a canonical basis of a fractional basis $\mathfrak{f}$. 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 5.4.*

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 $\mathfrak{a} = [S, S'(U+\rho), S''(V+W\rho+\omega)]$. Therefore, $\tilde{\mathfrak{f}} = (S^{-1})\mathfrak{a}$ is a fractional ideal with canonical basis $\{1, S'(U+\rho)/S, S''(V+W\rho+\omega)/S\}$, and $\mathfrak{f}^2 = (s'_G s'' S/s^2)\tilde{\mathfrak{f}} = (s'_G s''/s_G s_H)\tilde{\mathfrak{f}} = (f^{-1})\tilde{\mathfrak{f}}$. □

6 Reduced Ideals and Ideal Reduction

For the remainder of this paper, we only consider the situation where $q \equiv -1 \pmod 3$, so K has unit rank 1. Let $\theta = l + m\rho + n\omega \in K$ with $l, m, n \in k(x)$. We define

$$\begin{array}{rcccl} f_\theta & = & (\iota - \iota^2)(\iota\theta' - \iota^2\theta'') & = & l - m\rho, \\ g_\theta & = & (\iota - \iota^2)(\theta' - \theta'') & = & m\rho - n\omega, \end{array} \tag{6.1}$$

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

$$\theta' = g_\theta - \iota f_\theta. \tag{6.2}$$

If $\theta, \phi \in K$ and $a, b \in k(x)$, then $f_{a\theta+b\phi} = af_\theta + bf_\phi$ and $g_{a\theta+b\phi} = ag_\theta + bg_\phi$. Also $f_a = a$ and $g_a = 0$.

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

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

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) $|f_\phi| \le 1$ and $|g_\phi| \le 1$, so $|l| = |d(\phi + \phi' + \phi'')| \le |d|$, $|m\rho| = |l - df_\phi| \le |d|$, and $|n\omega| = |m\rho - dg_\phi| \le |d|$. □

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:

1. Follows from $d(\mathfrak{f}) = L(d(\mathfrak{f})\mathfrak{f}) \mid N(d(\mathfrak{f})\mathfrak{f}) \mid L(d(\mathfrak{f})\mathfrak{f})^2 = d(\mathfrak{f})^2$ and $N(d(\mathfrak{f})\mathfrak{f}) = d(\mathfrak{f})^3 N(\mathfrak{f})$.
2. See Theorem 4.5 of [2].
3. See Corollary 4.6 of [2] for the first part. For the second part, observe that $|N(d(\mathfrak{f})\mathfrak{f})| \leq |L(d(\mathfrak{f})\mathfrak{f})|^2 = |d(\mathfrak{f})|^2 < |\Delta|$.
4. Suppose $\mathfrak{f}$ is not reduced and let $d = d(\mathfrak{f})$. Then there exists a nonconstant $\theta \in \mathfrak{f}$ with $|\theta| \leq 1$ and $|\theta'| \leq 1$. Set $\Delta(\theta) = \left((\theta - \theta')(\theta' - \theta'')(\theta'' - \theta)\right)^2 \in k(x)$. Since $\theta, \theta', \theta''$ are pairwise distinct, $\Delta(\theta) \neq 0$; also $|\Delta(\theta)| \leq 1$.

   Let $\{\lambda, \mu, \nu\}$ be a $k[x]$-basis of $\mathfrak{f}$. Since $d\theta^2 \in \mathfrak{f}$, there exists a nonsingular 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 $d^2\Delta(\theta) = \det(M)^2\Delta(\mathfrak{f})$, so since $|\Delta(\theta)| \leq 1 \leq |\det(M)|$: $1 \geq |\Delta(\theta)| \geq |\Delta(\mathfrak{f})d^{-2}| > 1$, a contradiction. □

Corollary 6.3 *1. If $\mathfrak{a}$ is a reduced integral ideal, then $|L(\mathfrak{a})|^3 < |N(\mathfrak{a})||\Delta|^{1/2}$.*

2. If $\mathfrak{a}$ is a reduced integral ideal, then $|L(\mathfrak{a})| < |\Delta|^{1/2}$, so $|N(\mathfrak{a})| < |\Delta|$.

3. If $\mathfrak{a}$ is a primitive integral ideal with $|L(\mathfrak{a})|^8 < |\Delta(\mathfrak{a})|$, i.e. $|L(\mathfrak{a})|^4 < |N(\mathfrak{a})||\Delta|^{1/2}$, then $\mathfrak{a}$ is reduced.

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 $|\psi'| < |\theta'|$ ([2] uses the terminology "minimum adjacent to θ"). By Theorem 5.1 of [2], ϕ always exists and is unique up to nonzero constant factors.

According to [2], 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 $\epsilon = \theta_{l+1}$ $(l \in \mathbb{N})$ encountered in this chain is a generator of the torsionfree part of the unit group $\mathcal{O}^*$; it is the *fundamental unit* of K of positive degree (unique up to nonzero constant factors). Since the recurrence for the Voronoi chain implies $\theta_{ml+n} = \epsilon^m\theta_n$ for $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$, $\{\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_l\}$ is the complete set of reduced principal fractional ideals in K. l is the *period* of ϵ.

Section 7 of [2] describes how to compute the Voronoi chain when k has odd characteristic. More exactly, it was shown how to compute the neighbor of 1 in a reduced principal fractional ideal. Here, we give a more inclusive treatment of ideal reduction that extends to the case where k has even characteristic (the method of [2] fails for this situation). We also explain how this process can be used to obtain a reduced principal fractional ideal from a nonreduced 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

$$|\mu| > |\nu|, \quad |f_\mu| < 1, |f_\nu| < 1, \quad |g_\mu| < 1 \leq |g_\nu|. \tag{6.3}$$

Before we show how to compute such a basis, we establish some bounds on the coefficients:

Lemma 6.4 *Let $\{1, \mu, \nu\}$ be a reduced basis of a fractional ideal $\mathfrak{f}$ with $\mu = (m_0 + m_1\rho + m_2\omega)/d$, $\nu = (n_0 + n_1\rho + n_2\omega)/d$, $m_0, m_1, m_2, n_0, n_1, n_2, d \in k[x]$ jointly coprime and $d = d(\mathfrak{f})$. Then $|d\mu| = |m_0| = |m_1\rho| = |m_2\omega| \leq \max\{|d|, |\Delta|^{1/2}\}$, $|n_0| = |n_1\omega|$, and $|d\nu|, |n_0|, |n_1\rho|, |n_2\omega| < \max\{|d|, |\Delta|^{1/2}\}$.*

Proof: Since $|f_\mu|, |g_\mu| < 1$, we have $|m_0| = |m_1\rho| = |m_2\omega| = |d\mu|$. If $|\mu| \leq 1$, then $|d\mu| \leq |d|$. If $|\mu| > 1$, then set $\theta = (\mu - f_\mu)g_\nu - (\nu - f_\nu)g_\mu$. Then $|\mu| \leq |\mu g_\nu| = |\theta|$ and a simple computations shows that $|\theta|^2 = |\Delta(\mathfrak{f})| = |N(\mathfrak{f})|^2|\Delta| \leq |\Delta|/|d|^2$, where the last inequality follows from part 1 of Lemma 6.2.

Similarly, $|f_\nu| < 1$ implies $|n_0| = |n_1\rho|$. Also $|d\nu| < |d\mu| \leq \max\{|d|, |\Delta|^{1/2}\}$. If $|n_2\omega| \leq |n_0|$, then $|n_2\omega| \leq |n_0| = |d\nu|$ and if $|n_2\omega| > |n_0|$, then $|n_2\omega| = |d\nu|$. □

Note that by part 3 of Lemma 6.2, $\max\{|d|, |\Delta|^{1/2}\} = |\Delta|^{1/2}$ if $\mathfrak{f}$ is reduced. The following algorithm (which is a modification of Algorithm 7.2 of [2]) computes a reduced basis of any fractional ideal.

Algorithm 6.5

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* $|\mu| < |\nu|$ *or if* $|\mu| = |\nu|$ *and* $|g_\mu| < |g_\nu|$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
3. *If* $|g_\mu| \geq |g_\nu|$

   3.1. *While* $\lfloor \mu/\nu \rfloor = \lfloor g_\mu / g_\nu \rfloor$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \mu/\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   3.2. *Replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \mu/\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$

   3.3. *If* $|g_\mu| = |g_\nu|$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$$
   where $a = sgn(g_\mu) sgn(g_\nu)^{-1} \in k^*$.
4. *While* $|g_\nu| < 1$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \mu/\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
   While $|g_\mu| \geq 1$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} \lfloor g_\nu / g_\mu \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
5. *If* $|f_\mu| \geq 1$, *replace* μ *by* $\mu - \lfloor f_\mu \rfloor$.
   If $|f_\nu| \geq 1$, *replace* ν *by* $\nu - \lfloor f_\nu \rfloor$.

Theorem 6.6 *Algorithm 6.5 computes a reduced basis of the input ideal.*

Proof: The proof of Proposition 7.2 in [2] remains almost entirely valid if the quantities $\xi_\theta, \zeta_\theta, \eta_\theta$ defined in [2] are replaced everywhere by $\theta, f_\theta, g_\theta$, respectively, for $\theta \in \{\mu, \nu\}$. There are only two places where the previous proof needs some adjustment: step 5 is slightly changed and is easily seen to achieve $|f_\mu|, |f_\nu| < 1$. In addition, we need to show that the loop in step 3.1 terminates (in [2], this was only discussed for the case where $\mathfrak{f}$ is reduced).

For any basis $\{1, \theta, \phi\}$, set $\gamma_{\theta,\phi} = \theta g_\phi - \phi g_\theta$. Let $\alpha = \nu$ and $\beta = \lfloor \mu/\nu \rfloor \nu - \mu$, so α and β are obtained by applying the linear transformation of step 3.1 to μ and ν. Suppose $\lfloor \mu/\nu \rfloor = \lfloor g_\mu / g a_\nu \rfloor$, then

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

Hence, $|\nu|$ and $|g_\nu|$ strictly decrease with each iteration of step 3.1. A simple calculation shows that $\gamma_{\mu,\nu} = \gamma_{\alpha,\beta}$, so this quantity (which we call γ for brevity) is invariant under the linear transformation of step 3.1 of the algorithm; in fact, any basis transformation introduces a factor into γ that is equal to the determinant of the transformation matrix, so γ is an invariant of the ideal $\mathfrak{f}$ up to nonzero constant factors. Hence the loop in step 3.1 terminates as soon as $|\nu g_\nu| < |\gamma|$, because in this case $|\mu/\nu - g_\mu/g_\nu| = |\gamma/\nu g_\nu| > 1$, violating the condition of the while statement. □

If $\mathfrak{f}$ is reduced, then the quantity μ generated by Algorithm 6.5 is in fact the same element μ that is needed to compute the Voronoi chain:

Theorem 6.7 *Let $\{1, \mu, \nu\}$ be a reduced basis of a fractional ideal $\mathfrak{f}$. If $\mathfrak{f}$ is reduced, then μ is the neighbor of 1 in $\mathfrak{f}$.*

Proof: Let $\theta = l + m\mu + n\nu$ be the neighbor of 1 in $\mathfrak{f}$ ($l, m, n \in k[x]$). Since $|\theta'| < 1$, by (6.1) $|f_\theta| < 1$ and $|g_\theta| < 1$. By (6.3) and (6.2) $|\mu'| < 1$, so $|\mu| > 1$ since $\mathfrak{f}$ is reduced. Since θ is the neighbor of 1 in $\mathfrak{f}$, we must have $|\mu| \geq |\theta|$.

If $n = 0$, then $m \neq 0$ as $\theta \notin k[x]$. If $n \neq 0$, then $|n| \leq |ng_\nu| = |g_\theta - ng_\nu| = |mg_\mu| < |m|$. In either case, $|n| < |m|$, therefore $|mf_\mu + nf_\nu| < |m|$.

Now $|l| = |f_\theta - mf_\mu - nf_\nu| < |m| < |m\mu|$ and $|n\nu| < |m\mu|$. It follows that $|\theta| = |m\mu| \geq |m\theta|$, so $|m| \leq 1$, and since $m \neq 0$: $m \in k^*$ and $l = n = 0$. So μ equals θ up to a nonzero constant factor. □

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

Theorem 6.8 *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 $\max\{|\nu|, |\nu'|\} > 1$.*

Proof: If $\mathfrak{f}$ is reduced, then by the previous theorem, μ is the neighbor of 1 in $\mathfrak{f}$, so $|\mu| > 1$. Furthermore, since 1 is a minimum in $\mathfrak{f}$ and $\nu \notin k$, $|\nu| > 1$ or $|\nu'| > 1$.

Now suppose that $|\mu| > 1$, $\max\{|\nu|, |\nu'|\} > 1$, and let $\theta \in \mathfrak{f}$ with $|\theta| \leq 1$ and $|\theta'| \leq 1$; say, $\theta = l + m\mu + n\nu$ with $l, m, n \in k[x]$. We need to show $\theta \in k$, i.e. $m = n = 0$ and $l \in k$. By (6.1) $|f_\theta| \leq 1$ and $|g_\theta| \leq 1$. Suppose $|m| < |n|$. Then

$$1 \leq |n| \leq |ng_\nu| = |g_\theta - mg_\mu| \leq \max\{1, |mg_\mu|\}.$$

Since $|n| > |m| > |mg_\mu|$, this maximum must be 1, so $|n| = |g_\nu| = 1$ and $m = 0$. Then from (6.2) $|\nu'| = 1$, so $|\nu| > 1$, implying $1 < |\nu| = |n(\nu - f_\nu)| = |\theta - f_\theta| \leq 1$, a contradiction. So $|m| \geq |n|$. If $m \neq 0$, then $|m\mu| > |n\nu|$, so $1 < |m\mu| = |m(\mu - f_\mu) + n(\nu - f_\nu)| = |\theta - f_\theta| \leq 1$, again a contradiction. So $m = n = 0$ and $|l| = |\theta| \leq 1$, implying $l \in k$. □

Corollary 6.9 *Let $\{1, \mu, \nu\}$ be a reduced basis of a fractional ideal $\mathfrak{f}$. Then $\mathfrak{f}$ is nonreduced if and only if either $|\mu| < 1$ or $|\mu| = |\nu'| = 1$ and $|\nu| < 1$.*

Proof: Suppose $\mathfrak{f}$ is not reduced. Then by Theorem 6.8 $|\mu| \leq 1$ or $|\nu|, |\nu'| \leq 1$. If $|\mu| < 1$, there is nothing to prove, so suppose that $|\mu| = 1$. Then $|\nu| < |\mu| = 1$ and from (6.2) $|\nu'| = |g_\nu| \geq 1$, so $|\nu'| = 1$.

Conversely, if either one of the (in)equalities in the Corollary hold, then $|\mu| \leq 1$ and from (6.3) and (6.2) $|\mu'| < 1$, so since $\mu \notin k$, $\mathfrak{f}$ is not reduced. □

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

$$\mathfrak{f}_1 = \mathfrak{f}, \qquad \mathfrak{f}_{n+1} = (\phi_n^{-1})\mathfrak{f}_n \quad (n \in \mathbb{N}) \tag{6.4}$$

where $\{1, \mu_n, \nu_n\}$ is a reduced basis of $\mathfrak{f}_n$ and $\phi_n = \mu_n$ if $|\mu_n| < |\nu_n|$ and $\phi_n = \nu_n$ otherwise. Clearly, all the $\mathfrak{f}_n$ are equivalent. The process of obtaining a reduced basis of $\mathfrak{f}_{n+1}$ from $\mathfrak{f}_n$ is also called a baby step, since the method is very similar to the one used on a reduced fractional ideal, except that in the reduced case, one always divides by the element of larger absolute value ($|\phi_n| = |\mu_n| > \max\{1, |\nu_n|\}$), whereas in the nonreduced situation, the ideal is divided by the basis element with the smaller absolute value ($|\phi_n| = \min\{|\mu_n|, |\nu_n|\} < 1$ by Corollary 6.9). From (6.4), it follows that

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

and $\psi_n \in \mathfrak{f}_1$ for $n \in \mathbb{N}$. If for $n \in \mathbb{N}$, $\mathfrak{f}_n$ is not reduced, then by (6.3) and Corollary 6.9 $|\phi_n| < 1$ and $|\phi_n'| \leq 1$. Hence, if none of $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_{n-1}$ is reduced, then $|\psi_n| < 1$ and $|\psi_n'| \leq 1$ for $n \geq 2$. We claim that there always exists $m \in \mathbb{N}$ such that $\mathfrak{f}_m$ is reduced:

Theorem 6.10 *Let $\mathfrak{f} = \mathfrak{f}_1$ be a nonreduced fractional ideal. Then there exists $m \in \mathbb{N}$ such that $\mathfrak{f}_m = (\psi_m)^{-1}\mathfrak{f}_1$ is reduced, where ψ_m is given by (6.5).*

Proof: Suppose the assumption is false and no $\mathfrak{f}_n$ $(n \in \mathbb{N})$ is reduced. Since $|\phi_n| < 1$ for all $n \geq 2$, we have $|\psi_n| > |\psi_{n+1}|$ for all $n \in \mathbb{N}$. It follows that $(\psi_n)_{n\in\mathbb{N}}$ is an infinite sequence of pairwise distinct elements in $\mathcal{N}_{\mathfrak{f}}(1)$, contradicting Lemma 6.1. □

Theorem 6.11 *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*

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

Proof: If $\mathfrak{f}_1$ is reduced, then $m = 1$, so suppose $\mathfrak{f}_1$ is not reduced. Since $|\phi_n| < 1$ and $|\phi_n| \leq 1$ for $n < m$, we have $|N(\phi_n)| < 1$, so $|N(\mathfrak{f}_n)| > |N(\mathfrak{f}_{n-1})|$ for $1 < n < m$. Set $d_n = \deg(N(\mathfrak{f}_n))$, then $d_n \geq d_{n-1} + 1$ and inductively, $d_n \geq d_1 + n - 1$ for $1 < n < m$.

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 $d_{m-1} \leq -\deg(\Delta)/4$. Thus, $m \leq d_{m-1} + 2 - d_1 \leq -\deg(\Delta)/4 + 2 - \deg(N(\mathfrak{f}_1))$. □

Corollary 6.12 *For $n \in \mathbb{N}$, let $\mathfrak{f}_n$ be given as in (6.5), and set $\mathfrak{a}_n = (d(\mathfrak{f}_n))\mathfrak{f}_n$. Let $m \in \mathbb{N}$ be such that $\mathfrak{a}_m$ is reduced and $\mathfrak{a}_n$ is not reduced for $n < m$. Then*

$$m \leq \max\{1, 2 + \deg\left(\frac{L(\mathfrak{a}_1)^3}{N(\mathfrak{a}_1)}\right) - \frac{1}{4}\deg(\Delta)\}.$$

Lemma 6.13 *Let $\mathfrak{f} = \mathfrak{f}_1$ be a nonreduced fractional ideal and let $m \in \mathbb{N}$ be such that $\mathfrak{f}_m = (\psi_m)^{-1}\mathfrak{f}_1$ is reduced, where ψ_m is given by (6.5). Then $1 > |\psi_m| \geq |N(\mathfrak{f})|$ and $1 \geq |\psi_m'| > |N(\mathfrak{f})|^{1/2}$.*

Proof: For brevity, write $\psi = \psi_m$. $|\psi| < 1$ and $|\psi'| \leq 1$ is clear. Since $d(\mathfrak{f})\psi \in d(\mathfrak{f})\mathfrak{f} \subseteq \mathcal{O}$, $N(d(\mathfrak{f})\mathfrak{f}) \mid N(d(\mathfrak{f})\psi)$, hence $|N(\mathfrak{f})| \leq |N(\psi)|$. Therefore

$$|\psi| = \frac{|N(\psi)|}{|\psi'|^2} \geq |N(\psi)| \geq |N(\mathfrak{f})|$$

and

$$|\psi'|^2 = \frac{|N(\psi)|}{|\psi|} > |N(\psi)| \geq |N(\mathfrak{f})|.$$

□

Theorem 6.8 and (6.4) give rise to the following ideal reduction algorithm. The number of iterations of the while loop in this algorithm is given by Theorem 6.11.

Algorithm 6.14

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 ideal equivalent to* $\mathfrak{f}$.

Algorithm:

1. *Set* $\mu = \tilde{\mu}$, $\nu = \tilde{\nu}$.
2. *While* $|\mu| \leq 1$ *or* $\max\{|\nu|, |\nu'|\} \leq 1$ *do*

   2.1. *If* $|\mu| < |\nu|$, *set* $\{\tilde{\mu}, \tilde{\nu}\} = \{\mu^{-1}, \nu\mu^{-1}\}$, *else set* $\{\tilde{\mu}, \tilde{\nu}\} = \{\nu^{-1}, \mu\nu^{-1}\}$.

   2.2. *From the basis* $\{1, \tilde{\mu}, \tilde{\nu}\}$, *compute a reduced basis* $\{1, \mu, \nu\}$ *using Algorithm 6.5.*

   end while

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 $1 \leq n \leq l$ (where l 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

$$\delta_1 = 0, \qquad \delta_n = \delta_{n-1} + \deg(\mu_{n-1}), \quad n - 1 \leq \delta_n < (n-1)\deg(\Delta)/2 \tag{7.1}$$

for any $n \in \{2, 3, \ldots, l\}$, where, as usual, μ_{n-1} is the neighbor of 1 in $\mathfrak{f}_{n-1}$. Here, the last inequality follows from Lemma 6.4. We note that if $\mu_i = (l_i + m_i\rho + n_i\omega)/d_i$ where $l_i, m_i, n_i, d_i \in k[x]$ coprime and $d_i = d(\mathfrak{f}_i)$ $(i \in \mathbb{N})$, than $|d_i\mu_i| = |l_i|$ by Lemma 6.4, so for computational purposes, $\deg(\mu_{n-1})$ in (7.1) can be replaced by $\deg(l_{n-1}) - \deg(d_{n-1})$.

Since $\deg(\epsilon) = \deg(\theta_{l+1})$, it follows that

$$l \leq \deg(\epsilon) \leq l\deg(\Delta)/2. \tag{7.2}$$

Let $\mathfrak{f}_i = (\theta_i^{-1})$ and $\mathfrak{f}_j = (\theta_j^{-1})$ be two reduced principal fractional ideals $1 \leq i, j \leq l$) 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 (7.1) $m \approx i + j$. 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 [1]. 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 Theorem 6.10, there exists $\psi = \psi_m \in \mathfrak{f}$ such that $\mathfrak{f}_m = \psi\mathfrak{f}$ is reduced for some $m \in \{1, 2, \ldots, l\}$. Since $\mathfrak{f}_m = (\psi^{-1})\mathfrak{f}_i\mathfrak{f}_j$, we have $\theta_m = \psi\theta_i\theta_j$ and $\delta_m = \delta_i + \delta_j + \deg(\psi)$. We have either $\psi = 1$ or $|N(\mathfrak{f})|^{-2} \leq |\psi| < 1$ by Lemma 6.13. Set $\delta = \deg(\psi)$, so $0 \geq \delta \geq \deg(N(\mathfrak{f})) = \deg(N(\mathfrak{f}_i)) + \deg(N(\mathfrak{f}_j))$. 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 $\{s, s'(u+\rho)/s, s''(v+w\rho+\omega)/s\}$ be a canonical basis of $\mathfrak{f}_i$. By Corollary 5.5, $\mathfrak{f}_i^2 = (f^{-1})\mathfrak{f}$, where $\mathfrak{f}$ is a fractional ideal containing 1 and $f = \gcd(s, GH)/\gcd(s', G)s''$. We have $0 \leq \deg(f) \leq \deg(s) = \deg(d(\mathfrak{f}_i)) \leq \deg(\Delta)/2 - 1$ 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 $0 \geq \deg(\psi) \geq 2 - \deg(\Delta)$. Then $\delta_m = 2\delta_i + \delta$ where $\delta = \deg(\psi) - \deg(f)$ satisfies the bounds of the Theorem. □

Since by (7.2), distances can generally be as large as $O(l) = O(q^{(\deg(\Delta)/2)-2})$ by Theorem 6.5 of [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 $\lfloor 3\deg(\Delta)/4 \rfloor$.*
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 $\lfloor 3\deg(\Delta)/4 \rfloor$.*

Proof: From the proof of Theorem 7.1, we have $\deg(N(\mathfrak{f}_i\mathfrak{f}_j)) \geq 2 - \deg(\Delta)$ in the situation of Theorem 7.1; similarly, $\deg(N(\mathfrak{f})) = 2\deg(N(\mathfrak{f}_i)) + 3\deg(f) \geq 2 - \deg(\Delta)$ in the case of Theorem 7.2. The Corollary now follows from Theorem 6.11. □

Note that we did not specify how to multiply two distinct fractional ideals $\mathfrak{f}_i$ and $\mathfrak{f}_j$ whose denominators are not relatively prime. It is possible to develop multiplication formulas for this situation; however, the details are very tedious. Instead, if we compute a reduced fractional principal ideal very close to $\mathfrak{f}_i * \mathfrak{f}_j$ as follows. Begin by finding a 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 regulator and other distance computations (see Section 8 below), 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

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

so by Lemma 6.4, $n \le \delta_i - \delta_{i-n} \le n \deg(\Delta)/2$ 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 $\{\mathfrak{f}_i, \mathfrak{f}_{i-1}, \dots \mathfrak{f}_{i-m}\}$ *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* $\mathfrak{f}_i \ne \mathfrak{f}_j$ *then*

   While $\gcd(d(\mathfrak{f}_i), d(\mathfrak{f}_j)) \ne 1$*, do*

   2.1. *Replace* n *by* $n + 1$*;*

   2.2. *Replace* $\mathfrak{f}_i$ *by* $\mathfrak{f}_{i-1}$ *and* i *by* $i - 1$*;*

   end while

   end if.
3. *Compute canonical bases of* $\mathfrak{f}_i$ *and* $\mathfrak{f}_j$ *using Lemma 4.9.*

4. *If* $\mathfrak{f}_i \neq \mathfrak{f}_j$, *compute a canonical basis of* $\mathfrak{f} = \mathfrak{f}_i\mathfrak{f}_j$ *using Theorem 4.3;*
   If $\mathfrak{f}_i = \mathfrak{f}_j$, *compute a canonical basis of* $\mathfrak{f} = (f)\mathfrak{f}_i^2$ *using Theorem 5.4, where* f *is given as in Corollary 5.5;*
5. *Compute a reduced basis* $\{1, \mu, \nu\}$ *of* $\mathfrak{f}$ *using Algorithm 6.5;*
6. *While* $\deg(\mu) \leq 0$ *or* $\max\{\deg(\nu), \deg(\nu'\nu'')\} \leq 0$ *do*

   If $\deg(\mu) < \deg(\nu)$ *then*

   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* $\mathfrak{f}$*;*

   else

   6.1. *Replace* δ *by* $\delta + \deg(\nu)$*;*

   6.2. *Replace* $\mathfrak{f}$ *by* $\nu^{-1}\mathfrak{f}$ *(i.e. compute the basis* $\{1, \nu^{-1}, \mu\nu^{-1}\}$*);*

   6.3. *Compute a reduced basis* $\{1, \mu, \nu\}$ *of* $\mathfrak{f}$*;*

   end if

   end while

If a list of precomputed reduced ideals is not available, and we wish to compute an ideal close to $\mathfrak{f}_i * \mathfrak{f}_j$ when $\gcd(d(\mathfrak{f}_i), d(\mathfrak{f}_j)) \neq 1$, we compute $\mathfrak{f}_{i+n} * \mathfrak{f}_j$ for some small $n \in \mathbb{N}$ instead. In this case, step 2 of the above algorithm can be replaced by a short sequence of baby steps:

2. *While* $\gcd(d(\mathfrak{f}_i), d(\mathfrak{f}_j)) \neq 1$ *do*

   2.1. *Replace* n *by* $n + 1$.

   2.2. *Replace* $\mathfrak{f}_i$ *by* $\mathfrak{f}_{i+1} = \mu_i^{-1}\mathfrak{f}_i$ *(i.e. compute the basis* $\{1, \mu_i^{-1}, \nu_i\mu_i^{-1}\}$*) and* i *by* $i+1$.

   2.3. *Compute a reduced basis* $\{1, \mu_i, \nu_i\}$ *of* $\mathfrak{f}_i$ *using Algorithm 6.5.*

   end while

Here, an easy calculation shows that $\delta(\mathfrak{f}_{i+n} * \mathfrak{f}_j) = \delta_i + \delta_j + \tilde{\delta}$ with $n + 2 - \deg(\Delta) \leq \tilde{\delta} \leq n \deg(\Delta)/2$, so once again, $\mathfrak{f}_{i+n} * \mathfrak{f}_j$ and $\mathfrak{f}_i * \mathfrak{f}_j$ are within a few baby steps of one another. Unfortunately, $\mathfrak{f}_{i+n} * \mathfrak{f}_j$ can be off in either direction, i.e. short or ahead of $\mathfrak{f}_i * \mathfrak{f}_j$ in the cycle of reduced fractional principal ideals.

8 Conclusion — A Note on Fundamental Unit and Regulator Computation

(7.1) implies $\delta_n/n = \Theta(1)$, 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.

The naive way to compute the fundamental unit ϵ (and the method employed in [2]) is to apply baby steps to the ideal $\mathfrak{f}_1 = \mathcal{O}$ until a unit is encountered, thus obtaining $\epsilon = \theta_{l+1}$ after l baby steps. As mentioned before, we unfortunately have $l = O(q^{(\deg(\Delta)/2)-2})$ by Theorem 6.5 of [2], so by (7.2), l, and hence the size of ϵ, can be (and generally are) exponentially large relative to the size of the discriminant of $K/k(x)$. Hence, we usually only compute the *regulator* $R = \deg(\epsilon)/2 = -\deg(\epsilon')$ if $|\Delta|$ is large. While the size of R is polynomial in the size of Δ, the computation of R still requires exponentially many baby steps. To this day, no polynomial time method for computing R is known; however, the infrastructure reduces the run time of the regulator algorithm from order l to order $l^{1/2}$, and sometimes further improvements are possible: for real quadratic fields, for example, an order of $l^{2/5}$ was achieved in [3]. We briefly outline the idea here.

For some $m \in \mathbb{N}$ (to be specified later), one generates the ideals $\mathfrak{f}_1 = \mathcal{O}, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$ and their distances using baby steps. Then one employs giant steps to compute reduced fractional ideals $\mathfrak{g}_1 = \mathfrak{f}_m * \mathfrak{f}_m$, $\mathfrak{g}_2 = \mathfrak{g}_1 * \mathfrak{f}_m$, $\mathfrak{g}_3 = \mathfrak{g}_2 * \mathfrak{f}_m$ etc., together with their distances. Now since $\delta(\mathfrak{f}_m) \approx m$, we have $\delta(\mathfrak{g}_1) \approx 2m$, $\delta(\mathfrak{g}_2) \approx 3m$, and in general, $\delta(\mathfrak{g}_i) \approx im$. By periodicity, we must eventually reach an index $n \in \mathbb{N}$ such that $\mathfrak{g}_n \in \{\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m\}$, say $\mathfrak{g}_n = \mathfrak{f}_j$. Then $(n-1)m \approx \delta(\mathfrak{g}_{n-1}) < \deg(\epsilon) < \deg(\epsilon) + j \approx \deg(\epsilon) + \delta(\mathfrak{g}_n) \approx nm$, so at most m baby steps applied to $\mathfrak{g}_{n-1}$ will determine R. In this way, R can be found in no more than $2m$ baby steps and n giant steps, hence $l \approx 2mn$. Setting $m = n \approx \sqrt{2}l$, that is, performing an equal number of baby steps and giant steps, the overall complexity of the procedure is of order $\sqrt{l}$.

The main difficulty here is that in order to decide on the number of baby steps and giant steps to be executed, it is necessary to know a sufficiently good approximation of l (and hence of R) ahead of time. Research on how to obtain such an approximation is currently in progress. We point out that similar techniques can be used to compute the ideal class number h' of $K/k(x)$. Hence this method makes it possible to compute the order $h = Rh'$ of the group of k-rational points of the Jacobian of the function field K. Details will be given in a forthcoming paper.

Acknowledgement. The author is grateful to the Centre for Applied Cryptographic Research at the University of Waterloo for their hospitality and support during her sabbatical year 1999/2000.

References

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

[2] R. Scheidler and A. Stein, Voronoi's Algorithm in Purely Cubic Congruence Function Fields of Unit Rank 1. To appear in *Math. Comp.*

[3] A. Stein and H. C. Williams, Some methods for evaluating the regulator of a real quadratic function field. *Exp. Math.* **8** (1999), 119-133.

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

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

[6] H. C. Williams, G. Cormack and E. Seah, Calculation of the regulator of a pure cubic field. *Math. Comp.* **34** (1980), 567–611.

[7] H. C. Williams, G. W. Dueck and B. K. Schmid, A rapid method of evaluating the regulator and class number of a pure cubic field. *Math. Comp.* **41** (1983), 235–286.