MATHEMATICS OF COMPUTATION
Volume 73, Number 245, Pages 387–413
S 0025-5718(03)01559-X
Article electronically published on June 17, 2003

THE ARITHMETIC OF CERTAIN CUBIC FUNCTION FIELDS

MARK L. BAUER

ABSTRACT. In this paper, we discuss the properties of curves of the form $y^3 = f(x)$ over a given field $\mathbf{K}$ of characteristic different from 3. If $f(x)$ satisfies certain properties, then the Jacobian of such a curve is isomorphic to the ideal class group of the maximal order in the corresponding function field. We seek to make this connection concrete and then use it to develop an explicit arithmetic for the Jacobian of such curves. From a purely mathematical perspective, this provides explicit and efficient techniques for performing arithmetic in certain ideal class groups which are of fundamental interest in algebraic number theory. At the same time, it provides another source of groups which are suitable for Diffie-Hellman type protocols in cryptographic applications.

INTRODUCTION

Elliptic curves provide a beautiful introduction to the concept of the Jacobian of a curve. In this, the most simple case, it is possible to show that the Jacobian is isomorphic to the curve itself. Furthermore, the group structure can be described in terms of the standard chord-secant, chord-tangent construction. This straightforward geometric description of the group law makes it possible to write down explicit formulas for addition and inversion without using the more obscure and difficult definition of the Jacobian. For higher genus curves, however, the Jacobian is a variety of dimension equal to the genus, so this simpler geometric description for the group law is missing. In the case of hyperelliptic curves, Cantor developed an explicit arithmetic for the Jacobian using algebraic techniques (see [C]).

In both cases, the underlying group and the efficiency of the arithmetic have made these objects practical for industrial implementation of cryptographic protocols in Diffie-Hellman type systems. This provides motivation for developing analogous results in other algebraic settings, with such applications in mind.

The main purpose of this paper will be to make explicit the arithmetic of the Jacobian for another class of curves and to establish connections to certain ideal class groups. Such objects are of interest in both algebraic geometry and algebraic number theory.

The focal point of this paper is to develop an arithmetic for the Jacobian of these curves which is efficient enough for cryptographic applications. The work of Galbraith, Paulus and Smart in [GPS] provides an explicit arithmetic in a more general setting than what is presented here, but the generality of the context leads

Received by the editor April 10, 2001 and, in revised form, July 18, 2002.
2000 *Mathematics Subject Classification.* Primary 11R58, 94A60.

to certain unavoidable inefficiencies. By handling a narrower class of curves and exploiting the underlying structure, it is possible to construct a better arithmetic.

In the next two sections of this paper, we will lay the foundation upon which the rest of this paper is based. The first defines the Jacobian of a curve and proposes various definitions that will be used herein. In the second section, an explicit isomorphism between the Jacobian of a curve and the ideal class group of its ring of regular functions (provided the curve is of a certain form) is constructed. It is from this equivalence that the arithmetic for our restricted class of curves will be derived.

Starting in Section 3, we will only consider curves of the form $y^3 = f(x)$ defined over $\mathbf{K}$, a field of characteristic different from three, where $f(x)$ is a monic polynomial with simple roots and degree not divisible by three. The next two sections of the paper will discuss invariants of the curve related to the ring of regular functions and the corresponding function field. The main interest in these sections lies in showing that the ring of regular functions has no units of infinite order and that there is a way to represent ideals uniquely.

In the fifth section of the paper, we will discuss the consequence of considering our restricted class of curves and what this allows us to deduce about the structure of their Jacobians. The results in this section rely heavily on the connection between the Jacobian and the ideal class group of the ring of regular functions. In particular, by exploiting the explicit isomorphism between these two objects, we will reduce the problem of performing arithmetic in the Jacobian of the curve to a matter of performing arithmetic in the ideal class group.

The remaining sections of the paper will focus on developing the various operations that are necessary for performing computations in the ideal class group, i.e., multiplication, inversion and reduction. In these sections we will present both lemmata and algorithms concerning computations with integral ideals. Algorithms will only be presented in support of the lemmata when there is some question as to how one would compute the necessary information.

1. Jacobians

We will restrict our attention to *affine planar curves*, i.e., to curves whose points may be described as the solution set to an equation of the form $F(x, y) = 0$ over some algebraically closed field $\overline{\mathbf{K}}$. If we have $F(x, y) \in \mathbf{K}[x, y]$, and there is a solution in $\mathbf{K} \times \mathbf{K}$ to the equation $F(x, y) = 0$, then we say that the curve is defined over $\mathbf{K}$.

We will further suppose that our curve has a smooth affine planar model. This condition is equivalent to requiring the defining polynomial $F(x, y)$ to have the property that there is no affine point in $\overline{\mathbf{K}} \times \overline{\mathbf{K}}$ that simultaneously satisfies

$$F(x,y) = 0, \qquad \frac{\partial F(x,y)}{\partial y} = 0, \qquad \text{and} \qquad \frac{\partial F(x,y)}{\partial x} = 0\ .$$

Finally, we will suppose that the smooth projective closure of the curve contains only one point that is not contained in the smooth affine planar model, and this point is defined over $\mathbf{K}$. This unique point will be called the point at infinity.

Inherently when we are speaking of a curve, we will start by fixing a model which satisfies the above criteria, since the criteria do not guarantee uniqueness of the model. Let C represent the fixed model of the curve that we have chosen, and consider the following definitions.

The *ring of regular functions of* C are maps from C to $\mathbf{K}$ that are quotients of polynomials on C with coefficients in $\overline{\mathbf{K}}$ and that are well defined for all points of C. Since the model for our curve is smooth, this ring is isomorphic to $\overline{\mathbf{K}}[x,y]/(F(x,y))$. We denote this ring by $\overline{\mathbf{K}}[C]$. If we wish to restrict our attention to those functions defined over $\mathbf{K}$, in which case we write $\mathbf{K}[C]$, then this ring is isomorphic to $\mathbf{K}[x,y]/(F(x,y))$. Notice that this second definition only makes sense if C is defined over $\mathbf{K}$. The *function field of* C is the field of fractions of $\overline{\mathbf{K}}[C]$, which we denote by $\overline{\mathbf{K}}(C)$. A similar definition applies for $\mathbf{K}(C)$.

The Jacobian of a curve is a g-dimensional abelian variety, where g is the genus of the curve. For our purposes, we are only interested in the set of points on this variety which form an abelian group, and in particular, only those points defined over $\mathbf{K}$. It thus suffices to use the definition of the Jacobian given in [St].

A *place* P in $\mathbf{K}(C)$ corresponds to a discrete valuation ring $\mathcal{O}_P$ such that Frac($\mathcal{O}_P$)=$\mathbf{K}(C)$. We associate the maximal ideal in $\mathcal{O}_P$ to P and denote it by $\mathfrak{m}_P$. We define the valuation at P, v_P, as follows. For $\alpha \in \mathbf{K}(C)^* \cap \mathcal{O}_P$, we take $v_P(\alpha) = n$, where n is the largest integer such that $\alpha \in \mathfrak{m}_P^n$, and for $\alpha \in \mathbf{K}(C)^* \backslash \mathcal{O}_P$, we set $v_P(\alpha) = -v_P(1/\alpha)$. The *degree* of a place is defined to be $[\mathcal{O}_P/\mathfrak{m}_P : \mathbf{K}]$. If P is a place of degree 1, then we may associate a point on the curve defined over $\mathbf{K}$ to P by examining the images of x and y in the residue map to $\mathbf{K}$; in this case, $\mathcal{O}_P$ is the ring of functions which are regular at P, i.e., do not have a pole at P.

To each place, we may also associate a prime ideal of $\mathbf{K}[C]$ to P by defining $\mathfrak{P} = \mathfrak{m}_P \cap \mathbf{K}[C]$. Since the smooth projective closure only contains one point at infinity, there is a unique place in $\mathbf{K}(C)$ such that $\mathfrak{P}$ is (0), and we will call this the *place at infinity.* It corresponds to the unique point in the projective closure at infinity, and has degree one by assumption. We will say that all other places are *finite.* Conversely, every nonzero prime ideal gives rise to a valuation on $\mathbf{K}[C]$, and hence corresponds to a unique place in $\mathbf{K}(C)$. We will frequently rely on this one-to-one correspondence between finite places and nonzero prime ideals of $\mathbf{K}[C]$.

Definition 1.1. The *divisor group of* C, $\mathrm{Div}_{\mathbf{K}}(C)$, is defined to be the free abelian group on the places in $\mathbf{K}(C)$. A *divisor* $D \in \mathrm{Div}_{\mathbf{K}}(C)$ is a formal sum $D = \sum_P m_P(P)$, where P ranges over all places in $\mathbf{K}(C)$. For all P we have $m_P \in \mathbf{Z}$, and $m_P = 0$ for all but finitely many places. The *degree* $\deg(D)$ of a divisor is equal to $\sum_P m_P \deg P$.

It is easy to see from this definition that the divisors of degree zero over $\mathbf{K}$ form a subgroup. This gives rise to the following definition.

Definition 1.2. The *divisor group of degree zero of* C, $\mathrm{Div}^0_{\mathbf{K}}(C)$, is the subgroup of $\mathrm{Div}_{\mathbf{K}}(C)$ containing all the divisors of degree zero.

Given an element $\alpha \in \mathbf{K}[C]^*$, we may assign a divisor to α by taking $m_P = v_P(\alpha)$ and setting $\mathrm{div}(\alpha) = \sum_P m_P(P)$. Since C is a smooth projective curve, we note that the degree of such a divisor is always zero.

Definition 1.3. A divisor D is called *principal* if $D = \mathrm{div}(\alpha)$ for some $\alpha \in \mathbf{K}(C)^*$.

The properties of valuation imply that the principal divisors form a subgroup of $\mathrm{Div}^0_{\mathbf{K}}(C)$, denoted $\mathrm{Prin}_{\mathbf{K}}(C)$. Using these two definitions, we can now define the Jacobian of a curve.

Definition 1.4. The points on the *Jacobian* of a curve C over $\mathbf{K}$ are

$$J_C(\mathbf{K}) \cong \operatorname{Div}^0_{\mathbf{K}}(C)/\operatorname{Prin}_{\mathbf{K}}(C).$$

We will say two divisors are *equivalent* if their difference is principal, and we will write $D_1 \sim D_2$.

Definition 1.5. Let $D \in \operatorname{Div}^0_{\mathbf{K}}(C)$. We will call D *finitely effective* if, for all finite places P in $\mathbf{K}(C)$, $m_P \geq 0$.

Lemma 1.6. *Every divisor $D \in \operatorname{Div}^0_{\mathbf{K}}(C)$ is equivalent to a finitely effective divisor.*

Proof. Let $D \in \operatorname{Div}^0_{\mathbf{K}}(C)$ be a divisor such that D is not finitely effective. Hence, there exists a finite place P such that $m_P < 0$. Since P is finite, the corresponding prime ideal $\mathfrak{P}$ is a nonzero ideal in $\mathbf{K}[C]$ and hence there exists $\alpha \in \mathfrak{P}^{-m_P}$ with $\alpha \neq 0$. Therefore, $v_P(\alpha) \geq -m_P$. Furthermore, for any other finite place P' we have $v_{P'}(\alpha) \geq 0$, since $\mathbf{K}[C] \subseteq \mathcal{O}_{P'}$. Consider $D' = D + \operatorname{div}(\alpha)$, which is also a divisor in $\operatorname{Div}^0_{\mathbf{K}}(C)$, but has the additional property that for all finite places P', $m'_{P'} \geq m_{P'}$ and $m'_P \geq 0$. Furthermore, D' is equivalent to D since $D' - D = \operatorname{div}(\alpha)$. Since D has only finitely many nonzero coefficients, by repeating this process we can find a finitely effective divisor equivalent to D. □

For the definitions that follow, we will assume that we have fixed a model for our curve. To this fixed model, we will associate a projection onto $\mathbb{A}^1$, the affine line. The ring of regular functions on $\mathbb{A}^1$ is $\mathbf{K}[x]$, and its corresponding function field is $\mathbf{K}(x)$. Its projective closure is called the projective line, and is denoted by $\mathbb{P}^1$. For our purposes, the projection will come from the canonical injection of $\mathbf{K}[x]$ into $\mathbf{K}[C]$, which induces a map Ψ from $\operatorname{Div}^0_{\mathbf{K}}(\mathbb{P}^1)$ to $\operatorname{Div}^0_{\mathbf{K}}(C)$. For a divisor $D \in \operatorname{Div}^0_{\mathbf{K}}(\mathbb{P}^1)$, we will let $\overline{D} = \Psi(D) \in \operatorname{Div}^0_{\mathbf{K}}(C)$. The definitions given below are motivated by the common definitions used for hyperelliptic curves. We have generalized these notions to make sense in our broader setting.

Definition 1.7. Let D be a finitely effective divisor in $\operatorname{Div}^0_{\mathbf{K}}(C)$. We will call D *semi-reduced* if, for any divisor D_1 also of degree zero which is a nonempty subsum of D, D_1 is not equal to $\overline{D_2}$ for some $D_2 \in \operatorname{Div}^0_{\mathbf{K}}(\mathbb{P}^1)$.

Given a divisor D in $\operatorname{Div}_{\mathbf{K}}(\overline{C})$, we will let D^+ denote the effective part of D, that is,

$$D^+ = \sum_{\{P \mid m_P \geq 0\}} m_P P.$$

Lemma 1.8. *Every divisor D in $\operatorname{Div}^0_{\mathbf{K}}(C)$ is equivalent to a semi-reduced divisor.*

Proof. By Lemma 1.6, it is sufficient to prove the result for finitely effective divisors. Let D be a finitely effective divisor in $\operatorname{Div}^0_{\mathbf{K}}(C)$. Assume there exists a divisor D_1 also of degree zero which is a nonempty sub-sum of D, such that D_1 is equal to $\overline{D_2}$ for some $D_2 \in \operatorname{Div}^0_{\mathbf{K}}(\mathbb{P}^1)$. However, the Jacobian of the projective line is trivial, so $D_2 \sim 0$ and hence $\overline{D_2} \sim 0$. Therefore, $D - D_1 \sim D$ is also finitely effective, and $\deg(D - D_1)^+ < \deg D^+$. After finitely many iterations, we will arrive at a finitely effective divisor equivalent to D which is semi-reduced. □

The impetus for the previous definition is to eliminate some of the useless information from a divisor. Our goal will be to find a unique representative in each divisor class, and hence yield a way of describing elements in the Jacobian uniquely. To that end, we will use the following definition.

Definition 1.9. If D is a finitely effective divisor, then we call D *reduced* if $\deg D^+ \leq g$ and D is semi-reduced.

Lemma 1.10. *Every divisor class contains a reduced divisor.*

Proof. Applying Lemma 1.6 again, we note that it suffices to prove the result for finitely effective divisors. Let D_1 be a finitely effective divisor and $d = \deg D_1^+$. If $d > g$, then, by the Riemann-Roch Theorem,

$$\begin{aligned} L(D_1^+ - (d-g)\infty) = deg(D_1^+ - (d-g)\infty) - g + 1 \\ + L(W - (D^+ - (d-g)\infty)) \geq g - g + 1 \geq 1 \end{aligned}$$

(where W is a canonical divisor for the curve). Therefore, there exists an $\alpha \in L(D_1^+ - (d-g)\infty)$ with $\alpha \notin \mathbf{K}$. If $d \leq g$, we may take $\alpha \in \mathbf{K}^*$. Hence, $D_2 = D_1 + \operatorname{div}(\alpha)$ is also a finitely effective divisor, and $d_2 = \deg D_2^+ \leq g$. Following the proof of Lemma 1.8, we may find a semi-reduced divisor $D_3 \sim D_2$ which has the property that $\deg D_3^+ \leq d_2$. D_3 is therefore a reduced divisor which is equivalent to D. □

From a geometric perspective, this merely shows that the g-fold symmetric product of the curve maps onto the Jacobian. For hyperelliptic curves, this is all that needs to be said. That is, if D is a reduced divisor in a given class, then it is the unique reduced divisor in that class. However, for cubic function fields of genus larger than 2, this is not always the case. We will demonstrate that there can exist two reduced divisors in a given class in this more general situation (see Example 5.6). Hence, we need to be more restrictive if we want to represent divisor classes uniquely.

Definition 1.11. Let D be a finitely effective divisor in $\operatorname{Div}^0_{\mathbf{K}}(C)$. We will call D *distinguished* if, for all other finitely effective divisors D_1, $D \sim D_1$ and $\deg D_1^+ \leq \deg D^+$ imply $D = D_1$.

Naturally, this definition is not ideal, because there is no way of knowing a priori if such a divisor exists in a given class, nor does it give an easy way to verify if a divisor is distinguished. Since every divisor class contains a reduced divisor, however, we can make the following observation.

Lemma 1.12. *If D is a distinguished divisor, then D is reduced.*

Thus, we have established a hierarchy for divisors. Distinguished divisors are the most restricted type of divisors, and from Lemma 1.12, we know that distinguished implies reduced. We have also shown that every divisor class contains a reduced divisor (Lemma 1.10), and from the definitions, it follows that a reduced divisor is semi-reduced. Finally, semi-reduced divisors are, by definition, finitely effective.

2. The Jacobian as an ideal class group

Using the above construction for performing computations in the Jacobian of a curve can prove to be cumbersome. Fortunately, we are able to circumvent this difficulty by exploiting the relationship between the Jacobian and the ideal class group of $\mathbf{K}[C]$.

Let $\mathcal{I}(\mathbf{K}[C])$ represent the group of fractional ideals of $\mathbf{K}[C]$, and $\mathcal{P}(\mathbf{K}[C])$ represent the subgroup of principal fractional ideals. The *ideal class group of* $\mathbf{K}[C]$ is $\mathcal{I}(\mathbf{K}[C])/\mathcal{P}(\mathbf{K}[C])$.

Definition 2.1. Let I be a fractional ideal in $\mathcal{I}(\mathbf{K}[C])$. I is said to be *integral* if I is also an ideal in $\mathbf{K}[C]$.

We have already fixed an embedding $\mathbf{K}[x] \hookrightarrow \mathbf{K}[C]$. If $J \subset \mathbf{K}[x]$ is an ideal, we will let J^e denote the ideal that comes from extending J to an ideal in $\mathbf{K}[C]$ induced by the natural inclusion of rings.

Definition 2.2. We will call a nonzero ideal I of $\mathbf{K}[C]$ *primitive* if the only ideal J of $\mathbf{K}[x]$ having the property that $I \subseteq J^e$ is $\mathbf{K}[x]$.

Given a nonzero prime ideal in $\mathbf{K}[C]$, we may define the degree of $\mathfrak{P}$ to be $[\mathbf{K}[C]/\mathfrak{P} : \mathbf{K}]$. Since we have fixed a smooth model for our curve, $\mathbf{K}[C]$ is a Dedekind domain and every integral ideal may be factored uniquely into a product of prime ideals. Hence we may extend this definition of degree to any nonzero ideal by first factoring the ideal into a product of primes, and then taking the summation of the corresponding degrees, counting with appropriate multiplicity.

Definition 2.3. Let I be an integral ideal of $\mathbf{K}[C]$. We will say that I is *reduced* if $\deg I \leq g$.

It will turn out that every ideal class contains at least one reduced ideal, and may in fact contain more than one. Hence, we will need the following definition.

Definition 2.4. Let I be an integral ideal of $\mathbf{K}[C]$. We will say that I is *distinguished* if for any other integral ideal J equivalent to I, $\deg J \leq \deg I$ implies $J = I$.

As with divisors, we now have a hierarchy of ideals. Distinguished implies reduced, reduced implies primitive, and all primitive ideals are, by definition, integral. In what follows, we will solidify the correspondence between ideals and divisors, and prove that the hierarchy outlined here is the same as the one constructed for divisors.

Theorem 2.5. *Let C be a smooth affine planar curve whose smooth projective closure contains only one point at infinity, and it is defined over $\mathbf{K}$. Then $J_{\mathbf{K}}(C)$ is isomorphic to the ideal class group of* $\mathbf{K}[C]$.

Proof. Assume C is a smooth affine planar curve with the model $f(x,y) = 0$, and let $\bar{C}$ denote the smooth projective closure of C. The Jacobian of C is the degree 0 part of the Weil class group of $\bar{C}$. We note that C is an open subvariety of $\bar{C}$, since $\bar{C}\backslash\infty = C$. We thus have the following short exact sequence:

$$0 \to \mathbb{Z} \to \mathrm{Cl}(\bar{C}) \to \mathrm{Cl}(C) \to 0.$$

The map from $\mathrm{Cl}(\bar{C})$ to $\mathrm{Cl}(C)$ is induced by the inclusion of $C \to \bar{C}$, so it is necessarily surjective. The kernel of the map consists of exactly those divisors with support outside C. Hence, the map on the left is defined by $1 \to 1(\infty)$. This map is injective because $\bar{C}$ is a smooth projective curve, whereby all principal divisors have degree 0. But, now we note that $\mathrm{Cl}(\bar{C})/\langle\infty\rangle \cong J_{\mathbf{K}}(C)$, whence we have an isomorphism of $J_{\mathbf{K}}(C) \cong \mathrm{Cl}(C)$. C is a smooth affine curve, so as a variety it is isomorphic to $\operatorname{Spec} K[x,y]/(f(x,y))$, and furthermore, $\mathbf{K}[x,y]/(f(x,y))$ is a Dedekind domain. However, for Dedekind domains, we know that the Weil class group is isomorphic to the ideal class group of the ring. □

In fact, the proof gives us a way to construct an explicit map between the Jacobian and the ideal class group. As mentioned in the previous section, the finite places of $\mathbf{K}(C)$ are in one-to-one correspondence with the nonzero prime ideals of $\mathbf{K}[C]$ via the association $\mathfrak{P} = \mathfrak{m}_P \cap \mathbf{K}[C]$. If we take $D = \sum_P m_P P$ to be a divisor of degree zero, then we define the map

$$\Psi : \sum_P m_P P \mapsto \prod_{P\text{finite}} \mathfrak{P}^{m_P}. \tag{2.1}$$

The ideal associated to D will be denoted by I_D, and is defined by this map. This map is an isomorphism between $\operatorname{Div}^0_{\mathbf{K}}(C)$ and $\mathcal{I}(\mathbf{K}[x])$, which induces the isomorphism described in the previous theorem. Exploiting this relationship, we can equate the definitions for divisors to those given above for ideals.

For example, it is now easy to see that D is a finitely effective divisor if and only if the ideal I_D is integral. Furthermore, since the ring $\mathbf{K}[C]$ is a Dedekind domain, divides and contains are equivalent notions for ideals. Therefore any nonprimitive ideal may be written as the product of a primitive ideal and a principal ideal, where the principal ideal is generated by an element in $\mathbf{K}[x]$. This gives us an equivalence between semi-reduced divisors and primitive ideals.

Lemma 2.6. *If D is a finitely effective divisor, then D is semi-reduced if and only if I_D is primitive.*

Proof. By Theorem 2.5, we also obtain an isomorphism between $J_{\mathbf{K}}(\mathbb{P}^1)$ and the ideal class group of $\mathbf{K}[x]$. The lemma follows from the following commutative diagram and the above definitions.

$$\begin{tikzcd}
\operatorname{Div}^0_{\mathbf{K}}(C) \arrow[r, "\cong"] & \mathcal{I}(\mathbf{K}[C]) \\
\operatorname{Div}^0_{\mathbf{K}}(\mathbb{P}^1) \arrow[u] \arrow[r, "\cong"] & \mathcal{I}(\mathbf{K}[x]) \arrow[u]
\end{tikzcd}$$ □

Lemma 2.7. *Let D be a finitely effective divisor. Then* $\deg(D^+) = \deg I_D$.

Proof. Let P be a finite place of $\mathbf{K}[C]$. The degree of P is defined as $[\mathcal{O}_P/\mathfrak{m}_P : \mathbf{K}]$, and for the corresponding prime $\mathfrak{P}$, it is defined as $[\mathbf{K}[C]/\mathfrak{P} : \mathbf{K}]$. We merely note that $\mathcal{O}_P/\mathfrak{m}_P \cong \mathbf{K}[C]/\mathfrak{P}$, and hence the corresponding degrees are equal. □

Combining the previous two lemmata, we may deduce the following results.

Lemma 2.8. *Let D be a divisor and I_D its corresponding ideal. Then D is reduced if and only if I_D is reduced.*

Lemma 2.9. *Let D be a divisor and I_D its corresponding ideal. Then D is distinguished if and only if I_D is distinguished.*

3. The function field of a purely cubic curve

We will consider $\mathbf{K}$ to be a field of characteristic different from 3, and let $\overline{\mathbf{K}}$ be its algebraic closure. Define a *purely cubic curve* C over $\mathbf{K}$ to be a curve which admits a model of the form

$$y^3 = f(x), \text{ with } f(x) \in \mathbf{K}[x]\backslash\mathbf{K}.$$

If $f(x)$ has no repeated roots, then C is a smooth affine curve. From here on, we will restrict our attention to curves of this form, with the added constraint that

$f(x)$ must be monic. Since our curve is nonsingular, the ring of regular functions is isomorphic to $\mathbf{K}[x,y]/(y^3 - f(x))$; we will let $\mathbf{K}(C)$ denote its field of fractions.

When working with the function field $\mathbf{K}(C)$, it helps to exploit the analogy between function fields and number fields. We will implicitly take advantage of this relationship, and the reader should keep this in mind when looking for motivation of the techniques employed. The function field $\mathbf{K}(C)$ may be considered as a cubic extension $\mathbf{K}(x,y)$ over $\mathbf{K}(x)$ with $y^3 - f = 0$. If $\mathbf{K}$ contains a primitive cube root of unity, which we will call ζ_3, then there are two natural nontrivial automorphisms of the curve, given by

$$\sigma: \; x \mapsto x, \text{ and } y \mapsto \zeta_3 y,$$
$$\sigma^2: \; x \mapsto x, \text{ and } y \mapsto \zeta_3^2 y.$$

These automorphisms correspond to the nontrivial elements of a Galois group G of $\mathbf{K}(C)$ over $\mathbf{K}(x)$. Regardless of whether the primitive cube root of unity is in the ground field, the norm map $N : \mathbf{K}(C) \to \mathbf{K}(x)$ is well defined. For an ideal I, a suitable notion for norm is the unique monic polynomial in $\mathbf{K}[x]$ that generates the ideal $\left(\prod_{\sigma\in G} \sigma(I)\right) \cap \mathbf{K}[x]$. The norm of an element $\alpha \in \mathbf{K}[C]$ is defined to be $\prod_{\sigma\in G} \sigma(\alpha)$. Since every element of $\mathbf{K}(C)$ may be written as $ay^2 + by + c$, with $a, b, c \in \mathbf{K}(x)$, the norm of such an element is

$$N(ay^2 + by + c) = a^3 f^2 + (b^3 - 3abc)f + c^3.$$

Although not immediately obvious, the fact that the norm has this shape means that the function field, or more precisely the ring of regular functions, has two very nice properties. They both follow from the following proposition.

Proposition 3.1. *Let $\alpha = ay^2 + by + c \in \mathbf{K}[C]$, where C is defined by the nonsingular equation $y^3 = f(x)$. If 3 does not divide the degree of $f(x)$, then*

$$\deg\, N(\alpha) = \max\{\deg\, a^3 f^2, \deg\, b^3 f, \deg\, c^3\}.$$

Proof. We note the following congruences:

$$\deg\, a^3 f^2 \equiv 2 \deg\, f, \quad \deg\, b^3 f \equiv \deg\, f, \quad \deg\, c^3 \equiv 0 \pmod 3.$$

Since $\deg\, f \not\equiv 0 \pmod 3$, the degrees of $a^3 f^2$, $b^3 f$ and c^3 must all lie in distinct residue classes modulo 3. This reduces the proof of the proposition to showing that $\deg(3abcf) < \max\{\deg\, a^3 f^2, \deg\, b^3 f, \deg\, c^3\}$. If this inequality were not true, then one of three conditions must occur.

Assume $\deg\, a^3 f^2 = \max\{\deg\, a^3 f^2, \deg\, b^3 f, \deg\, c^3\}$ and $\deg\, 3abcf \geq \deg\, a^3 f^2$. Using the additive property of degrees and cancelling the like terms on both sides of the inequality, we have that $2 \deg\, a + \deg\, f \leq \deg\, b + \deg\, c$. Hence, either $\deg\, b \geq \deg\, a + \frac{1}{3} \deg\, f$ or $\deg\, c \geq \deg\, a + \frac{2}{3} \deg\, f$. If the former is true, then $\deg\, b^3 f \geq \deg\, a^3 f^2$, and if the latter, is true then $\deg\, c^3 \geq \deg\, a^3 f^2$. Either way, we have contradicted the maximality of $\deg\, a^3 f^2$ with respect to the other two terms.

A similar argument holds for the remaining two cases. □

Using the above proposition, one can deduce that there are no units of infinite order in $\mathbf{K}[C]$. Combining this with the Riemann-Hurwitz formula, it then becomes possible to calculate the genus of the curve. These results also follow from Theorem 2.1 of [SchSt].

Corollary 3.2. *Let C be a purely cubic curve with a smooth affine model of the form $y^3 = f(x)$ with $f(x)$ a monic polynomial in $\boldsymbol{K}[x]$. Set n equal to the degree of $f(x)$. If 3 does not divide n, then $\mathbf{K}(C)$ is a rank 0 cubic function field. Moreover, $\mathbf{K}[C]^* = \boldsymbol{K}^*$ and C has genus equal to $n - 1$.*

Another interesting consequence of Lemma 3.1 is that assigning a weight of 3 to x and a weight of $\deg f$ to y yields an ordering of the monomials in $\mathbf{K}[C]$. This, in fact, allows for Gröbner basis computations and may be used to prove the existence of a unique element of minimal norm (up to multiplication by elements in $\mathbf{K}^*$) in a given ideal. We will discuss this in more detail later when it becomes relevant. However, for the application in which we are interested, using this approach would lead to rather slow computations, so we will develop explicit techniques for doing calculations in this ring using other methods.

4. Ideals of $\mathbf{K}[C]$

Since we will derive our arithmetic by exploiting the connection between the ideal class group of $\mathbf{K}[C]$ and the Jacobian, it is necessary to discuss how ideals in this ring may be represented. Although this ring is a Dedekind domain and we could represent ideals with two generators, it will be easier and more convenient to use a canonical basis representation. That is, our representations will be with respect to $\mathbf{K}[x]$, since all ideals are rank 3 free modules over this ring. For further details on this subject, in the case of cubic function fields, we refer the reader to [Sch].

Any primitive ideal I in $\mathbf{K}[C]$ has a basis as a free $\mathbf{K}[x]$-module of the form $[s, s'(u+y), v+wy+y^2]$, where s, s', u, v and w are polynomials in $\mathbf{K}[x]$ (see Corollary 4.4 [Sch]). In general, the square bracket notation ([ ]) will denote a $\mathbf{K}[x]$ basis for an ideal, while the angled bracket notation ($\langle\ \rangle$) will denote a $\mathbf{K}[C]$ generating set for an ideal. There are various conditions that need to be satisfied for a canonical basis to form a proper ideal in $\mathbf{K}[C]$. We omit a comprehensive treatment of them, instead directing the reader to [Sch]. Here is a list of the properties we will find most useful:

$$\begin{aligned} &s' \mid s, \qquad u^3 \equiv -f \pmod{s/s'}, \qquad v \equiv w^2 \pmod{s'}, \\ &v - uw + u^2 \equiv 0 \pmod{s/s'}, \qquad uv - uw^2 \equiv f - vw \pmod{s}. \end{aligned} \tag{4.1}$$

If we restrict our attention to ideals with a canonical basis of the form $[s, u + y, v + wy + y^2]$, i.e., $s' = 1$, it is easy to deduce that $[s, u+y, v+wy+y^2] = \langle s, u+y\rangle$ using the congruences stated above. Furthermore, if we consider an ideal of the form $[s, sy, v+wy+y^2]$, it is also straightforward that $[s, sy, v+wy+y^2] = \langle s, v+wy+y^2\rangle$. The canonical representation can be used to uniquely represent an ideal provided we place certain restrictions on these polynomials. In particular, by Corollary 4.2 of [Sch], it is clear that the polynomials s, s', u, v, and w as defined in a minimal canonical basis below are unique.

Definition 4.1. Let I be a primitive ideal in $\mathbf{K}[C]$, with a canonical basis

$$[s, s'(u + y), v + wy + y^2].$$

This basis will be called a *minimal canonical basis* if it satisfies the following properties:

- s and s' are monic,
- the degrees of $s'u$ and v are less than the degree of s,
- the degree of w is less than the degree of s'.

The norm of an ideal, given by $[s, s'(u+y), v+wy+y^2]$ with s and s' monic, is ss' (again, see [Sch]). Considering the action of the Galois group, we also have the following correlation between the degree of an ideal and the degree of the norm.

Lemma 4.2. *If I is an integral ideal, then* $\deg I = \deg N(I)$.

It will also be to our benefit to discuss what the prime ideals in $\mathbf{K}[C]$ look like. Since f was chosen to be square-free, we have 4 types of prime ideals, under the classifications given in [Sch]. We will use a different nomenclature here for convenience.

Ramified primes correspond to ideals in $\mathbf{K}[C]$ such that $\mathfrak{P}^3 = \langle p \rangle$ where $p = p(x)$ is an irreducible polynomial in $\mathbf{K}[x]$.

Partially split primes correspond to ideals in $\mathbf{K}[C]$ such that there exist two distinct prime ideals $\mathfrak{P}$ and $\mathfrak{P}'$ with $\mathfrak{P}\mathfrak{P}' = \langle p \rangle$ for some irreducible polynomial $p = p(x)$ in $\mathbf{K}[x]$.

Completely split primes correspond to ideals in $\mathbf{K}[C]$ for which there exist three distinct prime ideals $\mathfrak{P}$, $\mathfrak{P}'$ and $\mathfrak{P}''$ such that $\mathfrak{P}\mathfrak{P}'\mathfrak{P}'' = \langle p \rangle$ for some irreducible polynomial $p = p(x)$ in $\mathbf{K}[x]$.

Inert primes are prime ideals generated by an irreducible polynomial in $\mathbf{K}[x]$.

This classification becomes much more intuitive if we assume that $\mathbf{K}$ does contain a primitive cube root of unity. Then, partially split primes do not occur. For completely split primes, we may take $\mathfrak{P}'$ to be $\sigma(\mathfrak{P})$ and $\mathfrak{P}''$ to be $\sigma^2(\mathfrak{P})$. In some sense, the choice given for completely split primes should be made to agree with this choice, i.e., we may extend $\mathbf{K}$ to include a primitive cube root of unity, and then define $\mathfrak{P}' = \sigma(\mathfrak{P}) \cap \mathbf{K}[C]$.

We will find it beneficial to be able to write an arbitrary primitive ideal as the product of two ideals with a very specific form. In [Sch], a complete description is given for the canonical basis of products of prime ideals lying above the same irreducible in $\mathbf{K}[x]$. Using this description, we may deduce that

$$[s, s'(u+y), v+wy+y^2] = \left[\frac{s}{s'}, u+y, v+wy+y^2\right][s', s'y, v+wy+y^2], \tag{4.2}$$

and, by previous arguments, this is equal to

$$\left\langle \frac{s}{s'}, u+y \right\rangle \left\langle s', v+wy+y^2 \right\rangle . \tag{4.3}$$

5. The ideal class group of $\mathbf{K}[C]$

Our goal in this section will be to glean what information we can about the Jacobian of C by using the analogy with the ideal class group. Of primary importance will be determining if two elements lie in the same class. We have shown that we only need to examine distinguished and reduced ideals. In this section, we will give necessary and sufficient conditions for an ideal to be distinguished.

Our first goal is to determine whether or not a distinguished element exists in every class. Fortunately, we have placed sufficient limitations on our curve that will force such elements to exist, as was true for hyperelliptic curves.

Theorem 5.1. *Every nonzero ideal contains a nonzero element of minimal norm which is unique up to multiplication by an element in* $\mathbf{K}^*$.

Proof. Let I be a nonzero integral ideal in $\mathbf{K}[C]$. Assigning a weight of 3 to x and a weight of $\deg f$ to y, we obtain a strict ordering of the monomials in $\mathbf{K}[C]$ written in the standard form. If $\alpha_1 = a_1y^2 + b_1y + c_1$ and $\alpha_2 = a_2y^2 + b_2y + c_2$ are two elements in a given ideal whose norms have the same degree but are not constant multiples of each other, then, applying Lemma 3.1, we see that one of the following three conditions must hold. The first possibility is deg $a_1 =$ deg a_2 and deg $N(\alpha_1)$=deg $a_1^3f^2$, in which case we let $k \in \mathbf{K}^*$ be the quotient of the leading term in the polynomial a_1 by the leading term in the polynomial a_2. Then $\alpha_3 = \alpha_1 - k\alpha_2$ is also a nonzero element of the ideal, and the degree of $N(\alpha_3)$ is less than the degree of $N(\alpha_1)$. The other two cases occur when both deg $b_1 =$ deg b_2 and deg $N(\alpha_1)$=deg b_1^3f, and when both deg $c_1 =$ deg c_2 and deg $N(\alpha_1)$=deg c_1^3. Arguing in a similar fashion, we may find a nonzero element of the ideal whose norm has smaller degree. This completes the proof of the theorem. □

Corollary 5.2. *Every ideal class contains a (unique) distinguished ideal.*

Proof. Let I be a nonzero integral ideal in $\mathbf{K}[C]$. By the previous theorem, we may find a nonzero element α of minimal norm. We then note that the ideal $I' = \langle\alpha\rangle I^{-1}$ is also integral and primitive. If I_1 is an ideal equivalent to I' with deg $N(I_1) \leq$ deg $N(I')$, then $I_1 I = \langle\alpha'\rangle$, with $\alpha' \in I$. But deg $N(I') =$ deg $N(\alpha)-$ deg $N(I) \geq$ deg $N(I_1) =$ deg $N(\alpha')-$ deg $N(I)$, which implies that deg $N(\alpha) \geq$ deg $N(\alpha')$. Combining this with the fact that α is unique up to multiplication by an element in $\mathbf{K}^*$, we have that $\alpha' = k\alpha$ for some $k \in \mathbf{K}^*$, and hence $I' = I_1$. This proves that every inverse class contains a unique distinguished ideal. □

Combining this result with Lemma 2.9, we may conclude the following (in a more general context, we refer the reader to [GPS]).

Corollary 5.3. *Every divisor class contains a (unique) distinguished divisor.*

Now that we know that distinguished elements exist, we would like to consider their size. By Lemma 1.12, a necessary condition for a semi-reduced divisor D to be distinguished is $\deg D^+ \leq g$. We will now attempt to derive a sufficient condition for a semi-reduced divisor to be distinguished.

Proposition 5.4. *Let I be a primitive ideal such that* $\deg N(I) < \frac{2}{3}g + 1$. *Then I is distinguished.*

Proof. Assume that I_1 is a primitive ideal such that $\deg N(I_1) < \frac{2}{3}g + 1$ and I_1 is not distinguished. Then there exists a primitive ideal I_2 which is distinguished and equivalent to I_1. Furthermore, since I_2 is distinguished, we must have $\deg N(I_1) > \deg N(I_2)$. For an ideal I, let $\hat{I} = \sigma(I)\sigma^2(I) \cap \mathbf{K}[C]$, which is a proper ideal in $\mathbf{K}[C]$. Since I_1 and I_2 are equivalent, $I_1\hat{I_2}$ and $\hat{I_1}I_2$ are both principal. Neither of these two ideals can have a generator in $\mathbf{K}[x]$, or else $I_1 = I_2$, since they are both primitive. Instead, we must have $I_1\hat{I_2} = \langle d(ay^2+by+c)\rangle$ and $\hat{I_1}I_2 = \langle d'(a'y^2+b'y+c')\rangle$, where $a, b, c, d, a', b', c', d' \in \mathbf{K}[x]$, with $GCD(a, b, c) = GCD(a', b', c') = 1$, $a = 0 \Rightarrow b \neq 0$ and $a' = 0 \Rightarrow b' \neq 0$. Now we know that $I_1\hat{I_2}\hat{I_1}I_2 = \langle u\rangle$ for some $u \in \mathbf{K}[x]$, because it is the ideal generated by $N(I_1I_2)$. Therefore,

$$d(ay^2 + by + c)d'(a'y^2 + b'y + c') = ku,$$

where $k \in \mathbf{K}[C]^* = \mathbf{K}^*$. If both a, a' are 0 (so that b and b' are not), this simplifies to $dd'(bb'y^2 + (bc' + b'c)y + cc') = ku$. Since this is a basis representation, bb' must also be zero, implying that b or b' is zero, a contradiction. Hence either a or a' is nonzero. We note that the norm of an element $ay^2 + by + c$ with a nonzero is at least $2g + 2$. Thus, we have that either

$$\begin{aligned}\deg N(I_1) + 2(\deg\ N(I_1) - 1) &\geq \deg N(I_1) + 2\deg N(I_2) = \deg N(I_1\overline{I_2})\\ &= \deg N(d\langle ay^2 + by + c\rangle) \geq 2g + 2\end{aligned}$$

or

$$\begin{aligned}2\deg N(I_1) + (\deg\ N(I_1) - 1) &\geq \deg N(I_1^2) + \deg N(I_2) = \deg N(\overline{I_1}I_2)\\ &= \deg N(d'\langle a'y^2 + b'y + c'\rangle) \geq 2g + 2.\end{aligned}$$

□

Using Lemma 2.7, we derive the following corollary.

Corollary 5.5. *Let D be a semi-reduced divisor such that* $\deg D^+ < \frac{2}{3}g + 1$. *Then D is distinguished.*

Hence, we now know that a sufficient condition for a semi-reduced divisor D to be distinguished is $\deg D^+ < \frac{2}{3}g + 1$. Comparing this with our necessary condition, we see that there is a gap between these conditions when the genus is larger than 2. We note that this is in contrast to the situation that arises with hyperelliptic curves, where D is reduced if and only if D is distinguished. At first glance, one might hope to close this gap and show that for cubic function fields, all reduced divisors are distinguished. However, this is not possible. We give an example to demonstrate where the problem may arise.

Example 5.6. We start by considering the curve

$$C : y^3 = x^4 - 1 \qquad \text{over}\ \ \mathbf{K},$$

where $\mathbf{K}$ is a field of characteristic different from 2 or 3 (note that this curve is nonsingular under these restrictions). We consider the following two primitive ideals:

$$I_1 = [x - 1, (x - 1)y, y^2] \quad \text{and} \quad I_2 = [x^3 + x^2 + x + 1, y, y^2].$$

It is relatively easy to see that $I_1 = \langle x - 1, y\rangle^2$ and $I_2 = \langle x^3 + x^2 + x + 1, y\rangle$. The ideals therefore have degree 2 and 3 respectively, and, since the curve has genus 3, this implies they are both reduced ideals. However, we also note that

$$I_1[x - 1, y, y^2] = \langle x - 1\rangle \quad \text{and} \quad I_2[x - 1, y, y^2] = \langle y\rangle,$$

since $\langle x - 1, y\rangle^3 = \langle x - 1\rangle$ and $\langle x - 1, y\rangle\langle x^3 + x^2 + x + 1, y\rangle = \langle y\rangle$. This implies that I_1 and I_2 lie in the same equivalence class, and I_1 has smaller degree than I_2, so I_2 is not distinguished. In fact, by Corollary 5.5, we see that I_1 must be the unique distinguished ideal in this class. In terms of the Jacobian, if we set

$$P_1 = (1, 0), \quad P_2 = (-1, 0), \quad P_3 = (i, 0), \quad \text{and} \quad P_4 = (-i, 0),$$

where $i^2 = -1$, then

$$3P_1 - 3(\infty) \sim 0 \quad \text{and} \quad P_1 + P_2 + P_3 + P_4 - 4(\infty) \sim 0.$$

Therefore,

$$2P_1 - 2(\infty) \sim P_2 + P_3 + P_4 - 3(\infty),$$

which gives us the analogous example for reduced divisors.

Unfortunately, a combinatorial argument also shows that there must exist primitive ideals whose norms have degree equal to the genus, which are distinguished since the Jacobian has size roughly q^g. A consequence of this is that there is no hope of pushing the bound for the degree in the necessary condition down to meet the bound for the degree in the sufficient condition. The proof for the sufficient condition also indicates a method for constructing ideals whose degrees are just above $\frac{2}{3}g + 1$ and are not distinguished. The example given above was constructed using precisely this method; i.e., we search for a polynomial a such that $f + a^3$ has two factors, one with degree less than or equal to one third the genus and the remaining factor having degree less than or equal to the genus. Computationally, this is not a serious concern, since we will present an algorithm for determining the distinguished element in a given class. Now that we know the size of reduced ideals/divisors, it is possible to quantify the amount of storage space required to uniquely represent such an element.

Corollary 5.7. *The minimal canonical basis of a distinguished ideal may be represented with at most* $3g$ *elements in the finite field.*

Proof. By Definition 4.1, the total space required is

$$\begin{aligned}\deg s + &\deg s' + (\deg u + 1) + (\deg v + 1) + (\deg w + 1)\\ &\le \deg s + \deg s' + (\deg s - \deg s') + \deg s + \deg s'\\ &= 3\deg s + \deg s'.\end{aligned}$$

Since the ideal is reduced, the norm of the ideal has degree less than or equal to the genus. The norm of the ideal is ss', and hence we achieve the desired result. □

We will show later on that we can do slightly better than this using a different representation. The cost of using the alternate representation will be a small precomputation to determine the canonical basis of the ideal.

6. Ideal inversion and division in $\mathbf{K}[C]$

For the remainder of the paper, we will assume that all ideals under consideration are represented by a minimal canonical basis. If this is not the case, we will still obtain a proper canonical basis, but not necessarily the minimal one.

Strictly speaking, we will not be computing the inverse of an ideal, since we only want to work with integral ideals. Instead, we compute a primitive ideal in the class of the inverse of a given ideal.

Lemma 6.1. *If* $I_1 = [s_1, s_1'(u_1 + y), v_1 + w_1 y + y^2]$, *then* $I_2 = \langle s_1\rangle I_1^{-1}$ *is given by* $I_2 = [S, S'(U + y), V + Wy + y^2]$, *where*

$$S = s_1, \qquad S' = s_1/s_1', \qquad U = -w_1,$$
$$W = -u_1, \quad \textit{and} \quad V = w_1u_1 - v_1.$$

Proof. Since $s_1 \in I_1$, it is clear that $\langle s_1\rangle I_1^{-1}$ is an integral ideal. We only need to show that the above choices provide a correct $k[x]$ basis for I_2. One easily verifies that the basis constructed above satisfies the criteria for a minimal canonical basis. We use the fact that $I_1I_2 = \langle s_1\rangle$ to deduce information about the basis. We first note that $s_1 \in I_2$ and therefore $S|s_1$. Furthermore, $S(v_1 + w_1y + y^2) \in \langle s_1\rangle$, which implies that $s_1|S$ and hence $S = s_1$. Examining norms, we see that

$$s_1^3 = N(\langle s_1\rangle) = N(I_1I_2) = s_1s_1'SS'.$$

Since $S = s_1$, this implies that $S' = s_1/s_1'$. We also know that

$$S'(U+y)(v_1+w_1y+y^2) \in \langle s_1\rangle \Rightarrow s_1 | S'(U+w_1) \Rightarrow s_1' | (U+w_1).$$

Since we are looking for the minimal canonical basis of I_2, $\deg(S'U) < \deg s_1$. This forces $\deg U < \deg s_1'$, and it must satisfy the relation $U \equiv -w_1 \pmod{s_1'}$. But, $\deg w_1 < \deg s_1'$, so U must be equal to $-w_1$. Now consider the product $s_1'(u_1+y)(V+Wy+y^2) \in \langle s_1\rangle$. Examining the coefficient of y^2, we deduce that $s_1 | s_1'(u_1+W) \Rightarrow W \equiv -u_1 \pmod{s_1/s_1'}$. However, we have already shown that $s_1/s_1' = S'$, and $\deg u_1 < \deg(s_1/s_1')$, whereby $W = -u_1$. Finally, we consider $(V+Wy+y^2)(v_1+w_1y+y^2) \in \langle s_1\rangle \Rightarrow s_1 | (w_1W+V+v_1)$. This implies $V \equiv -w_1W - v_1 \pmod{s_1}$. Since V is uniquely determined mod S and $S = s_1$, a comparison of degrees shows that $V = -w_1W - v_1 = w_1u_1 - v_1$. □

We can use this lemma to show that, in fact, we don't need quite as much information as previously stated to uniquely determine an ideal.

Corollary 6.2. *If I is a distinguished ideal, then we can uniquely represent I with at most $2g$ elements of the field $\boldsymbol{K}$.*

Proof. Let I be a distinguished ideal with minimal canonical basis

$$[s, s'(u+y), v+wy+y^2].$$

Consider the two ideals

$$I_1 = \left[\frac{s}{s'}, u+y, v+wy+y^2\right] \text{ and } I_2 = \left[s', s'y, v+wy+y^2\right].$$

As mentioned previously, we can show that $I = I_1I_2$. Since I_1 is uniquely determined by $\frac{s}{s'}$ and u, it requires at most 2 deg $\frac{s}{s'}$ elements of $\mathbf{K}$ to represent it. From $I_2 = \langle s'\rangle\overline{I_2}^{-1}$ and $\overline{I_2} = [s', -w+y, v'+w'y+y^2] = \langle s', -w+y\rangle$, we deduce that $\overline{I_2}$ is uniquely determined by s' and $-w$. This also uniquely determines I_2 and requires at most 2 deg s' elements of $\mathbf{K}$. Therefore, we simply need $2\deg(\frac{s}{s'}) + 2\deg(s') = 2\deg(s)$ elements of $\mathbf{K}$ to determine I_1 and I_2, and hence I, uniquely. Since I is distinguished, I is also reduced, so deg $s \leq$ deg $ss' =$ deg $N(I) \leq g$. □

We next consider the quotient of two integral ideals, which, in general, will not be integral. Again, since we are working in the ideal class group, it is sufficient to find an integral ideal equivalent to this fractional ideal. In this setting, we may obviously use the inversion Lemma 6.1 and then use the multiplication Lemma 7.1 to determine a canonical basis for an integral ideal equivalent to the quotient of two primitive ideals. However, in certain situations, particularly those that will arise in our context, there is often a shortcut. We will first prove a lemma which will help to simplify the proof of the more general case.

Lemma 6.3. *Let $I_2 = [s, sy, v_2+w_2y+y_1^2]$ and $I_1 = [s, u_1+y, v_1+w_1y+y^2]$ be two ideals such that $I_1 \supseteq I_2$. Then $I = I_2I_1^{-1} = [s, w_2-u_1+y, v_2+w_2y+y^2]$.*

Proof. Let $I = I_2I_1^{-1}$. By Lemma 6.1, $I_2 = \langle s\rangle[s, -w_2+y, -v_2+y^2]^{-1} = \langle s\rangle\langle s, -w_2+y\rangle^{-1}$. Hence,

$$I\langle s, -w_2+y\rangle\langle s, u_1+y\rangle = \langle s\rangle.$$

Therefore, $I = \langle s, U+y\rangle$, where we just need to determine U. We note that

$$(U+y)(u_1+y)(-w_2+y) \in \langle s\rangle.$$

Upon multiplying the terms out, we see that the coefficient of y^2 is $U + u_1 - w_2$. Therefore, $s|(U + u_1 - w_2)$; that is to say, $U \equiv w_2 - u_1 \pmod{s}$. U is only unique modulo s, so $U = w_2 - u_1$. □

Lemma 6.4. *Let $I_i = [s_i, s_i'(u_i + y), v_i + w_i y + y^2]$ for $i = 1, 2$ be such that $I_1 \supseteq I_2$. Then $I = I_2 I_1^{-1} = [S, S'(U + y), V + Wy + y^2]$, where*

$$S = \frac{s_2}{s_1' d_1}, \qquad W = w_2 - qS',$$
$$S' = \frac{s_2' d_1}{s_1}, \qquad V \equiv v_2 - qS'U \pmod{S},$$
$$U \equiv u_3 - k\frac{s_1 s_2}{s_2' s_1' d d_1} \pmod{S/S'} \text{ of minimal degree,}$$

where the values for d, d_1, k and u_3 are given as follows, and q is chosen to make the degree of W minimal.

$$d = GCD\left(\tfrac{s_2}{s_2'}, \tfrac{s_1}{s_1'}\right), \qquad u_3 \equiv \begin{cases} u_2 & \left(\text{mod } \tfrac{s_2}{s_2' d_1}\right), \\ w_2 - u_1 & \left(\text{mod } \tfrac{s_1}{s_1' d_1}\right), \end{cases}$$
$$d_1 = GCD(d, u_1 - u_2),$$

and k is such that

$$\frac{d}{d_1} \left| \frac{(u_3^3 + f)s_1' s_2' d d_1}{s_1 s_2} - 3u_3^2 k \right. .$$

Proof. As we will see with multiplication in Section 7, the primary complication is in determining U. We perform the division in two stages by noting that

$$[s_2', s_2' y, v_2 + w_2 y + y^2] \subseteq [s_1', s_1' y, v_1 + w_1 y + y^2],$$

and hence

$$[s_2', s_2' y, v_2 + w_2 y + y^2][s_1', s_1' y, v_1 + w_1 y + y^2]^{-1} = \left[\frac{s_2'}{s_1'}, \frac{s_2'}{s_1'} y, v_2 + w_2 y + y^2\right].$$

Therefore, we deduce that

$$\begin{aligned} &[s_2, s_2'(u_2 + y), v_2 + w_2 y + y^2][s_1', s_1' y, v_1 + w_1 y + y^2]^{-1} \\ &\quad = \left[\frac{s_2}{s_1'}, \frac{s_2'}{s_1'}(u_2 + y), v_2 + w_2 y + y^2\right]. \end{aligned}$$

All that remains is to calculate

$$\left[\frac{s_2}{s_1'}, \frac{s_2'}{s_1'}(u_2 + y), v_2 + w_2 y + y^2\right] \left[\frac{s_1}{s_1'}, (u_1 + y), v_1 + w_1 y + y^2\right]^{-1}.$$

We factor the ideal on the left as

$$\left[\frac{s_2}{s_2'}, u_2 + y, v_2 + w_2 y + y^2\right] \left[\frac{s_2'}{s_1'}, \frac{s_2'}{s_1'} y, v_2 + w_2 y + y^2\right].$$

We then calculate the greatest common divisor of the two ideals

$$[s_1/s_1', u_1 + y, v_1 + w_1 y + y^2] \text{ and } [s_2/s_2', u_2 + y, v_2 + w_2 y + y^2],$$

which we will call I'. It is easy to see that $d \in I'$. We also know that $u_1 + y - (u_2 + y) = u_1 - u_2 \in I'$, so in fact, $d_1 = GCD(d, u_1 - u_2) \in I'$, and it divides all other polynomials in $\mathbf{K}[x]$ that are in I'. Hence, $I' = [d_1, u_1 + y, v_1 + w_1 y + y^2] = [d_1, u_2 + y, v_2 + w_2 y + y^2]$. We break up our quotient into two pieces,

$$[s_2/s_2', u_2 + y, v_2 + w_2 y + y^2][d_1, u_1 + y, v_1 + w_1 y + y^2]^{-1},$$

which is easily seen to be equal to

$$[s_2/(s_2'd_1), u_2 + y, v_2 + w_2y + y^2],$$

and

$$\left[\frac{s_2'}{s_1'}, \frac{s_2'}{s_1'}y, v_2 + w_2y + y^2\right] [s_1/(s_1'd_1), u_1 + y, v_1 + w_1y + y^2]^{-1}$$
$$= [s_2'/s_1', s_2'd_1/s_1(w_2 - u_1 + y), v_2 + w_2y + y^2],$$

which follows from Lemma 6.3. Hence, all that remains is to calculate

$$(6.1)\quad [s_2/(s_2'd_1), u_2 + y, v_2 + w_2y + y^2][s_2'/s_1', s_2'd_1/s_1(w_2 - u_1 + y), v_2 + w_2y + y^2].$$

The result must be of the form

$$\left[S, S'(U + y), v_2 + w_2y + y^2\right],$$

where the third element in the basis follows trivially from the fact that the ideal contains I_2. Considering how the two ideals were constructed as factors of I_2, we can deduce that $S = \frac{s_2}{s_1'd_1}$ and $S' = \frac{s_2'd_1}{s_1}$. All that remains is to determine U modulo $\frac{s_2s_1}{s_2's_1'd_1^2}$. From equation (6.1) we know U satisfies

$$U \equiv u_2 \pmod{\frac{s_2}{s_2'd_1}} \quad \text{and} \quad U \equiv w_2 - u_2 \pmod{\frac{s_1}{s_1'd_1}}.$$

This uniquely determine U modulo $LCM(\frac{s_2}{s_2'd_1}, \frac{s_1}{s_1'd_1}) = \frac{Sd_1}{S'd}$. Let u_3 be a polynomial satisfying these two congruences. Hence, $U \equiv u_3 \pmod{\frac{Sd_1}{S'd}}$ and $\frac{Sd_1}{S'd}|N(u_3 + y)$. We also know that $\frac{S}{S'}|N(U + y)$, so, writing $U = u_3 - k\frac{Sd_1}{S'd}$, we have

$$N\left(u_3 - k\frac{Sd_1}{S'd} + y\right) = u_3^3 + f - 3u_3^2k\frac{Sd_1}{S'd} + 3u_3k^2\left(\frac{Sd_1}{S'd}\right)^2 - k^3\left(\frac{Sd_1}{S'd}\right)^3.$$

It is easy to see that whatever we choose k to be, the last two terms of this expression will be divisible by $\frac{S}{S'}$. Since $N(u_3 + y) = u_3^3 + f$, this means that $\frac{Sd_1}{S'd}$ divides the first two terms as well. Therefore, we have to find a k such that

$$\frac{d}{d_1}\left|\frac{(u_3^3 + f)S'd}{Sd_1} - 3u_3^2k,\right.$$

and we are guaranteed that such a k exists. We simply take U to be the polynomial of minimal degree satisfying $U \equiv u_3 - k\frac{Sd_1}{S'd} \pmod{\frac{S}{S'}}$. The final step is modifying $v_2+w_2y+y^2$ so that the constructed basis satisfies the criteria of a minimal canonical basis. □

Since calculating U in the above lemma is nontrivial, we present the following algorithm.

Algorithm 6.5. Ideal Division. Input: $I_i = [s_i, s_i'(u_i+y), v_i+w_iy+y^2]$ for $i = 1, 2$ such that $I_1 \supseteq I_2$.

Step 1. Compute, using the half-extended Euclidean algorithm, r_1 and d such that

$$GCD\left(\frac{s_2}{s_2'}, \frac{s_1}{s_1'}\right) = d = r_1\frac{s_2}{s_2'} + r_2\frac{s_1}{s_1'}.$$

Step 2. Compute

$$d_1 = GCD(d, u_1 - u_2).$$

Step 3. Set

$$S = \frac{s_2}{s_1'd_1} \qquad S' = \frac{s_2'd_1}{s_1}.$$

Step 4. Set

$$u = u_2 + (w_2 - u_1 - u_2)\left(r_1\frac{s_2}{s_2'd}\right).$$

Step 5. Compute, using the half-extended Euclidean algorithm, d_2 and r_3 such that

$$GCD\ \left(\frac{d}{d_1}, 3u^2\right) = d_2 = 3r_3u^2 + r_4\frac{d}{d_1}.$$

Step 6. Set

$$U' = u - r_3\left(\frac{u^3+f}{d_2}\right).$$

Step 7. Calculate $U \equiv U' \pmod{S/S'}$ such that $\deg U < \deg S/S'$.
Step 8. Compute q and W such that $W = w_2 - qS'$ and $\deg W < \deg S'$.
Step 9. Calculate $V \equiv v_2 - qS'U \pmod{S}$ such that $\deg V < \deg S$.
Output: $[S, S'(U+y), V + Wy + y^2]$.

While most parts of the algorithm are justified in a straightforward manner from Lemma 6.4, perhaps a little explanation is needed as to why U' is indeed going to give us an element that satisfies the requirements of the lemma. We note that u is chosen so that $u \equiv u_2 \pmod{\frac{s_2}{s_2'd_1}}$ and $u \equiv w_2 - u_1 \pmod{\frac{s_1}{s_1'd_1}}$. According to Lemma 6.4, all that remains is to find a k such that

$$\frac{d}{d_1}\left|\frac{(u^3+f)S'd}{Sd_1} - 3u^2k.\right.$$

Since such a k exists, $d_2 = \text{GCD}\left(\frac{d}{d_1}, 3u^2\right)$, d_2 divides $\frac{d}{d_1}$ and $3u^2$ implies that d_2 divides $\frac{(u^3+f)S'd}{Sd_1}$, i.e., $\frac{u^3+f}{d_2}$ is a multiple of $\frac{Sd_1}{S'd}$. Choosing

$$k = r_3\frac{(u^3+f)S'd}{Sd_1d_2},$$

we see that

$$\begin{aligned}\frac{(u^3+f)S'd}{Sd_1} - 3u^2k &= \frac{(u^3+f)S'd}{Sd_1} - \left(1 - r_4\frac{d}{d_1d_2}\right)\frac{(u^3+f)S'd}{Sd_1}\\ &= \frac{d}{d_1d_2}\frac{(u^3+f)S'd}{Sd_1}.\end{aligned}$$

But d_2 divides the second term and hence this is a multiple of $\frac{d}{d_1}$, as desired. Therefore, we may take

$$U' = u - r_3\frac{(u^3+f)S'd}{Sd_1d_2}\left(\frac{Sd_1}{S'd}\right) = u - r_3\left(\frac{u^3+f}{d_2}\right).$$

U is just chosen to be congruent to U' modulo $\frac{S}{S'}$, but with minimal degree. The justification for the rest of the algorithm follows from Lemma 6.4.

In terms of the arithmetic that we will be performing, it may be the case that we will wish to take the quotient of a nonprimitive ideal by a primitive ideal. A slight modification to the previous lemma will yield the desired result.

Lemma 6.6. *Let $I_2 = d[s_2, s_2'(u_2+y), v_2+w_2y+y^2]$ and $I_1 = [s_1, s_1'(u_1+y), v_1 + w_1y+y^2]$ be such that $I_1 \supseteq I_2$. Then $I = I_2I_1^{-1} = (D_3)I_dI_m$, where*

$$I_d = [S_d, S_d'(U_d+y), V_d+W_dy+y^2]$$

and

$$I_m = [S_m, S_m'(U_m+y), V_m+W_my+y^2]$$

are given by

$$I_m = \overline{[D_1D_2, D_1(u_1+y), v_1+w_1y+y^2]}$$

and

$$I_d = [s_2, s_2'(u_2+y), v_2+w_2y+y^2]([s_1/(D_1D_2), s_1'/D_1(u_1+y), v_1+w_1y+y^2])^{-1},$$

where

$$D_1 = GCD(s_1', d) \qquad D_2 = GCD(\frac{s_1}{s_1'}, d/D_1) \qquad D_3 = \frac{d}{D_1D_2}$$

and the quotient for I_d is given by Lemma 6.4.

Proof. We merely note that $\overline{I_m} \subseteq \langle d\rangle$ and $\overline{I_m}[s_1/(D_1D_2), s_1'/D_1(u_1+y), v_1 + w_1y+y^2] = I_1$. Therefore, $\langle d\rangle\overline{I_m}^{-1} = I_m$ and $[s_2, s_2'(u_2+y), v_2+w_2y+y^2] \supseteq [s_1/(D_1D_2), s_1'/D_1(u_1+y), v_1+w_1y+y^2]$, whereby I_d may be computed from the previous lemma. □

7. Ideal multiplication in $\mathbf{K}[C]$

In this section, we focus on constructing a canonical basis for the product of two primitive ideals. It is important to note that one expects two reduced ideals to have norms which are relatively prime. In such situations, the formulas presented in [Sch] are sufficient. However, this may not always be the case. Of particular difficulty is the case when their product is no longer primitive. We will first handle the case when this is not an issue.

Lemma 7.1. *Let $I_1 = [s_1, s_1'(u_1+y), v_1+w_1y+y^2]$ and $I_2 = [s_2, s_2'(u_2+y), v_2 + w_2y+y^2]$ be such that $I_1I_2 = I_3$ is a primitive ideal. Then $I_3 = [S, S'(U+y), V + Wy+y^2]$, where*

$$\begin{array}{ll} S = s_1s_2\frac{d_1}{d}, & W = w_3 - qS', \\ S' = s_1's_2'\frac{d}{d_1}, & V \equiv v_3 - qS'U \pmod{S}, \end{array}$$

$$U \equiv u_3 - k\frac{s_1s_2d_1}{s_1's_2'd^2} \pmod{S/S'}$$

where the values of d, d_1, k, u_3, w_3 and v_3 are defined as follows, and q may be chosen to make the degree of W minimal:

$$\begin{array}{ll} d = GCD(s_1/s_1', s_2/s_2'), & \\ d_1 = \frac{GCD(d, u_1-u_2)}{GCD(d,f)}, & \end{array} \qquad u_3 \equiv \begin{cases} u_1 & \pmod{\frac{s_1d_1}{s_1'd}}, \\ u_2 & \pmod{\frac{s_2d_1}{s_2'd}}, \end{cases}$$

k is such that

$$d_1 \left| \frac{(u_3^3+f)s_1's_2'd^2}{s_1s_2d_1} - 3u_3^2k \right. ,$$

$$\begin{aligned} w_3 = {} & a_1s_1w_2 + a_2s_1's_2'(u_1+u_2) + a_3s_1'(u_1w_2+v_2) \\ & + a_4s_2w_1 + a_5s_2'(u_2w_1+v_1) + a_6(w_1v_2+v_1w_2) \end{aligned}$$

and

$$\begin{aligned} v_3 = {} & a_1 s_1 v_2 + a_2 s_1' s_2' u_1 u_2 + a_3 s_1'(u_1 v_2 + f) \\ & + a_4 s_2 v_1 + a_5 s_2'(u_2 v_1 + f) + a_6(v_1 v_2 + w_1 f + w_2 f), \end{aligned}$$

where

$$1 = a_1 s_1 + a_2 s_1' s_2' + a_3 s_1'(u_1 + w_2) + a_4 s_2 + a_5 s_2'(u_2 + w_1) + a_6(v_1 + v_2 + w_1 w_2).$$

Proof. We will rely heavily on the fact that in a Dedekind domain, divides and contains are equivalent notions for ideals. Assume $I_1 I_2 = I_3$ is primitive, and hence has a canonical basis of the form $I_3 = [S, S'(U + y), V + Wy + y^2]$. We begin by dividing each ideal up into factors using equation (4.2), and calculating their respective products. The easiest part to handle is the product

$$[s_1', s_1'y, v_1 + w_1 y + y^2][s_2', s_2'y, v_2 + w_2 y + y^2] = [s_1's_2', s_1's_2'y, V + Wy + y^2].$$

Here, we still need to determine V and W, and show that they may in fact be chosen as stated in the lemma. The difficult part of determining the product, as was the case with division, corresponds to the term

$$\left[\frac{s_1}{s_1'}, u_1 + y, v_1 + w_1 y + y^2\right]\left[\frac{s_2}{s_2'}, u_2 + y, v_2 + w_2 y + y^2\right]. \tag{7.1}$$

Set $d' = GCD(d, f)$. Computing the greatest common divisor of these two ideals, we get $[d'd_1, u_1 + y, v_1 + w_1 y + y^2] = [d'd_1, u_2 + y, v_2 + w_2 y + y^2]$. Thus, the factors $[d/(d_1 d'), u_1 + y, v_1 + w_1 y + y^2]$ and $[d/(d_1 d'), u_2 + y, v_2 + w_2 y + y^2]$ are relatively prime, but both contain $\langle d/(d_1 d')\rangle$. Their product must therefore be $[d/(d_1 d'), d/(d_1 d')y, v_3 + w_3 y + y^2]$. The only complication that can arise in calculating the rest of the product is the ramified primes in $[d_1 d', u_1 + y, v_1 + w_1 y + y^2]$. However, the ramified primes in this ideal are precisely $[d', y, v_1 + w_1 y + y^2]$. Squaring yields $[d', d'y, V + Wy + y^2]$. Hence, the product in equation (7.1) is equal to

$$\left[\frac{S}{S'}, U + y, v_3 + w_3 y + y^2\right]\left[\frac{d}{d_1}, \frac{d}{d_1}y, v_3 + w_3 y + y^2\right].$$

Therefore, $S' = \frac{s_1's_2'd}{d_1}$, and upon equating norms, $S = \frac{s_1 s_2 d_1}{d}$. Now for any irreducible polynomial $p \in \mathbf{K}[x]$ dividing S/S', the value of U determines which of the primes lying above p contain $[S/S', U + y, V + Wy + y^2]$ and satisfies $v_p(S/S') \leq v_p(N(U + y))$. From the above argument, we see that the ideal $[S/S', U + y, v_3 + w_3 y + y^2]$ is equal to

$$\left[\frac{s_1 d_1}{s_1' d}, u_1 + y, v_1 + w_1 y + y^2\right]\left[\frac{s_2 d_1}{s_2' d}, u_2 + y, v_2 + w_2 y + y^2\right].$$

Therefore, $U + y$ is an element of both ideals, and hence

$$U \equiv u_1 \pmod{\frac{s_1 d_1}{s_1' d d'}} \quad \text{and} \quad U \equiv u_2 \pmod{\frac{s_2 d_1}{s_2' d d'}}.$$

This determines U up to the least common multiple of $s_1 d_1/(s_1' d)$ and $s_2 d_1/(s_2' d)$, which is $s_1 s_2 d_1/(s_1' s_2' d^2)$. We choose u_3 to be any polynomial satisfying the above two congruences. In order to determine U modulo S/S', we note that $U = u_3 - k\frac{S}{S'd_1}$ and $S/S' | N(U + y)$. Using arguments similar to those presented in Lemma 6.4, this reduces to finding any polynomial k such that

$$d_1 \left| \frac{(u_3^3 + f)s_1's_2'd^2}{s_1 s_2 d_1} - 3u_3^2 k \right. .$$

This determines the value of U uniquely modulo S/S', which is what was needed. All that remains is to determine V and W. Given the information we have already calculated, it is quickest to merely find any element $v_3 + w_3y + y^2 \in I_3$. Since the ideal is primitive, the greatest common divisor of all of the y^2 terms given by the product of the canonical bases must be 1, and so we compute the element $v_3 + w_3y + y^2 \in I_3$ corresponding to this combination of elements. Finally, we subtract off $\mathbf{K}[x]$ multiples of the two basis elements previously found to construct the third element in the minimal canonical basis. □

Although the last step involving v_3 and w_3 looks quite complicated, in general, s_1 and s_2 are relatively prime, so the expression becomes quite simple. As with division, some difficulty may arise in computing U, so we present the corresponding algorithm for clarification.

Algorithm 7.2. Ideal Multiplication. Input: $I_1 = [s_1, s_1'(u_1 + y), v_1 + w_1y + y^2]$ and $I_2 = [s_2, s_2'(u_2 + y), v_2 + w_2y + y^2]$.

Step 1. Compute, using the half-extended Euclidean algorithm, d and r_1 such that

$$d = GCD(s_1/s_1', s_2/s_2') = r_1s_1/s_1' + r_2s_2/s_2'.$$

Step 2. Compute, using the Euclidean algorithm,

$$d_1 = \frac{GCD(d, u_1 - u_2)}{GCD(d, f)}.$$

Step 3. Set

$$s_3 = s_1s_2\frac{d_1}{d}, \quad s_3' = s_1's_2'\frac{d}{d_1}, \quad \text{and} \quad u = u_1 - (u_1 - u_2)\left(r_1\frac{s_1}{s_1'd}\right).$$

Step 4. Compute, using the half-extended Euclidean algorithm, d_2 and r_3 such that

$$GCD\ \left(d_1, 3u^2\right) = d_2 = 3r_3u^2 + r_4d_1.$$

Step 5. Set

$$U' = u - r_3\left(\frac{u^3 + f}{d_2}\right).$$

Step 6. Compute $U \equiv U' \pmod{S/S'}$ such that $\deg U < \deg(S/S')$.

Step 7. Compute, using the extended Euclidean algorithm,

$$\begin{aligned} 1 &= GCD(s_1, s_1's_2', s_1'(u_1 + w_2), s_2, s_2'(u_2 + w_1), v_1 + v_2 + w_1w_2) \\ &= a_1s_1 + a_2s_1's_2' + a_3s_1'(u_1 + w_2) + a_4s_2 + a_5s_2'(u_2 + w_1) + a_6(v_1 + v_2 + w_1w_2). \end{aligned}$$

Step 8. Set

$$\begin{aligned} V' = {} & a_1s_1v_2 + a_2s_1's_2'u_1u_2 + a_3s_1'(u_1v_2 + f) + a_4s_2v_1 \\ & + a_5s_2'(u_2v_1 + f) + a_6(v_1v_2 + w_1f + w_2f). \end{aligned}$$

Step 9. Set

$$\begin{aligned} W' = {} & a_1s_1w_2 + a_2s_1's_2'(u_1 + u_2) + a_3s_1'(u_1w_2 + v_2) + a_4s_2w_1 \\ & + a_5s_2'(u_2w_1 + v_1) + a_6(w_1v_2 + v_1w_2). \end{aligned}$$

Step 10. Compute $W = W' + qS'$ such that $\deg W < \deg S'$.

Step 11. Compute $V \equiv V' + qS'U \pmod{S}$ such that $\deg V < \deg S$.

Output: $[S, S'(U + y), V + Wy + y^2]$.

The justification for this algorithm is analogous to the one given for Algorithm 6.5. On first glance, steps 7, 8, and 9 seem computationally rather inefficient. However, as stated before, in almost all cases, we expect s_1 and s_2 to be relatively prime, which reduces those steps to a very simple operation. Even if this is not the case, it is reasonable to assume that we will reach a greatest common divisor of 1 without performing an undue number of operations.

If the product of the ideals is not primitive, we must determine where this nonprimitive part arises. The following lemma allows one to find the product of two ideals whose product is not primitive by removing this nonprimitive part.

Lemma 7.3. *Let I_1 and I_2 be as above with a given canonical basis. Then $I_1 I_2 = (D)I_3$, where $I_3 = I_1' I_2' I$ is given by Lemma 7.1, $D = D_1 D_2 D_3$, and I_1', I_2' and I are given as follows:*

$$I_1' = \left[\frac{s_1}{D_1 D_2 D_3}, \frac{s_1'}{D_2 D_3}(u_1 + y), v_1 + w_1 y + y^2\right],$$

$$I_2' = \left[\frac{s_2}{D_1 D_2 D_3}, \frac{s_2'}{D_1 D_3}(u_2 + y), v_2 + w_2 y + y^2\right],$$

and

$$I = [D_3, w_1 + w_2 + y, -(w_1 + w_2)^2 + y^2];$$

D_1, D_2 and D_3 are defined as follows:

$$D_1 = GCD(s_1/s_1', s_2', u_1 + w_2), \qquad D_2 = GCD(s_2/s_2', s_1', u_2 + w_1)$$

and

$$D_3 = \frac{GCD(s_2'/D_1, s_1'/D_2) \cdot GCD(s_2'/D_1, s_1'/D_2, f)}{GCD\,(s_2'/D_1, s_1'/D_2, w_1 - w_2)}.$$

Proof. We begin as before by splitting the problem into smaller (and hopefully simpler) parts. We decompose I_1 and I_2 into four ideals using equation (4.2):

$$I_{1,1} = \left[\frac{s_1}{s_1'}, u_1 + y, v_1 + w_1 y + y^2\right], \quad I_{1,2} = \left[s_1', s_1' y, v_1 + w_1 y + y^2\right],$$

$$I_{2,1} = \left[\frac{s_2}{s_2'}, u_2 + y, v_2 + w_2 y + y^2\right], \quad \text{and} \quad I_{2,2} = \left[s_2', s_2' y, v_2 + w_2 y + y^2\right],$$

The product $I_{1,1} I_{2,1}$ is primitive, so the nonprimitive part of $I_1 I_2$ must arise from a different combination of the factors. This leaves us with the three other products to check. If $I_{1,1} I_{2,2}$ (or $I_{2,1} I_{1,2}$) has a nonprimitive divisor, call it D_1 (or D_2, respectively). A $\mathbf{K}[x]$ basis for this ideal is generated by the pairwise product of the elements in the respective canonical bases. Considering these terms, the coefficients of y^2 are $s_2', s_1/s_1', u_1 + w_2$ (respectively $s_1', s_2/s_2', u_2 + w_1$). As mentioned previously, this ideal may be written as the product of an element in $\mathbf{K}[x]$ and a primitive ideal in $\mathbf{K}[C]$, where the latter has a canonical basis. Therefore, D_1 (D_2) must be the greatest common divisor of $s_2', s_1/s_1', u_1 + w_2$ (respectively $s_1', s_2/s_2', u_2 + w_1$). We remove this factor from the ideals to derive

$$I_{1,1}' = \left[\frac{s_1}{s_1' D_1}, u_1 + y, v_1 + w_1 y + y^2\right], \quad I_{1,2}' = \left[\frac{s_1'}{D_2}, \frac{s_1'}{D_2} y, v_1 + w_1 y + y^2\right],$$

$$I_{2,1}' = \left[\frac{s_2}{s_2' D_2}, u_2 + y, v_2 + w_2 y + y^2\right], \quad \text{and} \quad I_{2,2}' = \left[\frac{s_2'}{D_1}, \frac{s_2'}{D_1} y, v_2 + w_2 y + y^2\right],$$

with $I_1 I_2 = I'_{1,1} I'_{1,2} I'_{2,1} I'_{2,2}(D_1 D_2)$. Any remaining nonprimitive factor must be a divisor of the product $I'_{1,2} I'_{2,2}$.

Consider

$$I_{1,3} = \left[D_3, D_3 y, v_1 + w_1 y + y^2\right]$$

and

$$I_{2,3} = \left[D_3, D_3 y, v_2 + w_2 y + y^2\right],$$

where D_3 is defined as above. By Lemma 7.1,

$$\begin{aligned}&[D_3, -w_1 + y, -w_1^2 + y^2][D_3, -w_2 + y, -w_2^2 + y^2] \\ &\quad = [D_3, D_3 y, w_1 w_2 - (w_1 + w_2) y + y^2]\end{aligned}$$

which is to say that $\overline{I_{1,3}}\;\overline{I_{2,3}} \subseteq \langle D_3 \rangle$. Therefore,

$$\begin{aligned} I_{1,3} I_{2,3} &= I_{1,3} I_{2,3} \overline{I_{1,3}}\;\overline{I_{2,3}} \left(\overline{I_{1,3}}\;\overline{I_{2,3}}\right)^{-1} \\ &= \langle D_3 \rangle^2 \left(\overline{I_{1,3}}\;\overline{I_{2,3}}\right)^{-1} \\ &= \langle D_3 \rangle \left(\langle D_3 \rangle / \left(\overline{I_{1,3}}\;\overline{I_{2,3}}\right)^{-1}\right) \\ &= \langle D_3 \rangle [D_3, w_1 + w_2 + y, -(w_1 + w_2)^2 + y^2]. \end{aligned}$$

The primitive ideal on the right is the ideal I given in the statement of the lemma. Removing $I_{1,3}$ from $I'_{1,2}$, and $I_{2,3}$ from $I'_{2,2}$, we are left with

$$\left[\frac{s'_1}{D_2 D_3}, \frac{s'_1}{D_2 D_3} y, v_1 + w_1 y + y^2\right]$$

and

$$\left[\frac{s'_2}{D_1 D_3}, \frac{s'_2}{D_1 D_3} y, v_1 + w_1 y + y^2\right].$$

Finally, recombining the remaining pieces, we are left to compute the (primitive) product

$$\left[\frac{s_1}{D_2 D_3}, \frac{s'_1}{D_2 D_3} y, v_1 + w_1 y + y^2\right] \left[\frac{s_2}{D_1 D_3}, \frac{s'_2}{D_1 D_3} y, v_1 + w_1 y + y^2\right] I.$$

□

8. Elements of minimal norm

As mentioned earlier, it is possible to compute an element of minimal norm in an ideal using Gröbner bases, but we will instead use a related method which we believe to be computationally more efficient. The method proposed here is closely related to the algorithm given in [GPS], but with some slight differences. It is important to point out that both methods are modifications of the algorithm proposed by Lenstra in [L].

Algorithm 8.1. Minimal Element Algorithm. Let $I_1 = [s_1, s'_1(u_1 + y), v_1 + w_1 y + y^2]$.

Precomputations. Set $b_1 = (b_{1,1}, b_{1,2}, b_{1,2}) = (s_1, 0, 0)$, $b_2 = (b_{2,1}, b_{2,2}, b_{2,2}) = (s'_1 u_1, s'_1, 0)$, and $b_3 = (b_{3,1}, b_{3,2}, b_{3,2}) = (v_1, w_1, 1)$. Assign weights $w_{i,1} = 3 \deg b_{i,1}$, $w_{i,2} = 3 \deg b_{i_2} + \deg f$, and, $w_{i,3} = 3 \deg b_{i,3} + 2 \deg f$ (these weights are the degree of the norm of the respective components of b_i).

Set $w_i = \max\{w_{i,1}, w_{i,2}, w_{i,3}\}$, and choose a_i so that $w_i = w_{i,a_i}$ (i.e., $w_i = w_{i,a_i} = \deg N(b_i)$). Order the b_i's and their associated values so that $w_1 \leq w_2 \leq w_3$.

```
**While** $a_1 = a_2$ **or** $a_2 = a_3$ **or** $a_1 = a_3$.
**I: if** $a_1 = a_2$ **do**
    $b_{2,a_2} = b_{1,a_1}c + r$
    replace $b_2 := b_2 - cb_1$ and recalculate $a_2, w_2$.
**II: if** $a_1 = a_3$ **do**
    $b_{3,a_3} = b_{1,a_1}c + r$
    replace $b_3 := b_3 - cb_1$ and recalculate $a_3, w_3$.
**III: if** $a_2 = a_3$ **do**
    $b_{3,a_2} = b_{2,a_2}c + r$
    replace $b_3 := b_3 - cb_2$ and recalculate $a_3, w_3$.
Reorder the $b_i$'s and associated values. End **While**.
    **Output**: $b_{1,1} + b_{1,2}y + b_{1,3}y^2$, the element of minimal norm.
```

It is easier to understand how the algorithm performs by putting it in a more conceptual framework. Let us begin by denoting the weight of a polynomial in $\mathbf{K}[x]$ as three times its degree. Writing the canonical basis for the ideal in matrix form, we see that we are assigning different weights to each column as follows:

$$\begin{array}{ccc} \multicolumn{3}{c}{\begin{bmatrix} s_1 & 0 & 0 \\ s_1'u_1 & s_1' & 0 \\ v_1 & w_1 & 1 \end{bmatrix}} \\ \uparrow & \uparrow & \uparrow \\ \text{wt} & \text{wt} + & \text{wt} + \\ & \deg f & 2 \deg f \end{array}$$

This algorithm presents a method for performing elementary row operations (which may be viewed as elements of $GL_3(\mathbf{K}[x])$, acting on the left) to reduce the weight of each row until they are all as small as possible. The row with minimal weight after carrying out these operations corresponds to the unique (up to multiplication by an element in $\mathbf{K}^*$) element of minimal norm in the ideal. Such a conclusion is possible because each row carries its weight uniquely in one of the three positions (see Lemma 3.1). If two rows have their weight coming from the same position, it is possible to reduce the weight of one of the rows (as discussed in the proof of Lemma 5.2). This algorithm merely prescribes an order in which to perform these operations.

9. Canonical basis

Having now calculated an element of minimal norm, we would like to construct a canonical basis for the principal ideal generated by this element. This will then allow us to use the division Algorithm 6.4 to compute a distinguished ideal.

Algorithm 9.1. Canonical Basis. Let $ay^2 + by + c \in \mathbf{K}[C]$:
Step 1. Start with the matrix

$$\begin{bmatrix} c & b & a \\ af & c & b \\ bf & af & c \end{bmatrix}$$

and, using elementary row operations, transform it into a lower triangular matrix

$$\begin{bmatrix} c_3 & 0 & 0 \\ c_2 & b_2 & 0 \\ c_1 & b_1 & a_1 \end{bmatrix}.$$

Step 2. Set $d = a_1$. Set

$$s' = b_2/d, \quad s = c_3/d, \quad \text{and} \quad u \equiv c_2/(s'd) \pmod{s/s'} \quad \text{with} \quad \deg u < \deg(s/s').$$

Step 3. Compute q and w such that deg $w <$ deg s' and

$$b_1/d = s'q + w.$$

Step 4. Compute

$$v \equiv c_1/d - s'qu \pmod{s}$$

such that $\deg v < \deg s$.

Output: $d[s, s'(u + y), v + wy + y^2]$.

The algorithm is valid since, after elementary row operations, the resulting elements still form a $\mathbf{K}[x]$ basis for the ideal. Steps 2 through 4 convert this basis to a minimal canonical basis of the desired form.

10. Summary

We are left with combining the various algorithms to do computations in the ideal class group. Consider two ideal classes, given by their respective unique distinguished representatives I_1 and I_2 in canonical representation. The algorithm below outputs the distinguished representative in the class of $I_1 I_2$.

Algorithm 10.1. Composition and Reduction. Let I_1 and I_2 be two ideals given with canonical representations.

Step 1: Calculate $I_3 = I_1 I_2$. (Lemmata 7.3 and 7.2)

Step 2: Calculate $\overline{I_3}$. (Lemma 6.1)

Step 3: Find $\alpha \in \overline{I_3}$, an element of minimal norm. (Algorithm 8.1)

Step 4: Compute a representation for $\langle \alpha \rangle = \langle d \rangle [s_\alpha, s'_\alpha(u_\alpha + y), v_\alpha + w_\alpha y + y^2]$. (Algorithm 6.5)

Step 5: Use the representation for $\langle \alpha \rangle$ generated in step 4 to compute $I = \langle \alpha \rangle \overline{I_3}^{-1}$. (Algorithm 6.5)

Output: A distinguished ideal I which is equivalent to $I_1 I_2$.

The validity of the algorithm follows from the validity of the aforementioned lemmata and algorithms. It is important to point out here that certain steps may be interchanged and combined. In particular, one could invert the two ideals I_1 and I_2 first, and then perform the ideal multiplication, so switching steps 1 and 2. The ideal generated would be the same, but, depending on the original structure of the ideals, this may be faster. Furthermore, steps 4 and 5 can also be combined into one procedure to speed up the implementation. These and related issues will be dealt with in a subsequent paper which addresses implementation issues.

11. Examples

We will present two examples in this section to help illustrate the computations involved. The first example will be what we expect to happen if we multiply two random distinguished ideals together. The second example will illustrate a more complicated situation. For the sake of readability, we have chosen to use a small finite field that is clearly not suitable for cryptographic applications. Hopefully it is clear to the reader that scaling to larger finite fields is not problematic.

Example 11.1. Let $K = \mathbb{F}_{87181}$, and let $f(x)$ be the polynomial

$$x^4 + 2882x^3 + 79087x^2 + 65817x + 38743,$$

so our curve has genus 3. We will consider the product of the two following distinguished ideals and determine the unique distinguished representative in that class. Let $I_1 = [s_1, s_1'(u_1 + y), v_1 + w_1 y + y^2]$, where

$$\begin{aligned} s_1 &= x^3 + 86915x^2 + 13147x + 74593, & s_1' &= 1, & w_1 &= 0, \\ u_1 &= 74142x^2 + 286x + 70688, & v_1 &= 80905x^2 + 25441x + 15689, \end{aligned}$$

and $I_2 = [S_2, s_2(u_2 + y), v_2 + w_2 y + y^2]$, where

$$\begin{aligned} s_2 &= x^3 + 37037x^2 + 78256x + 41191, & s_2' &= 1, & w_1 &= 0, \\ u_2 &= 63029x^2 + 50418x + 8770, & v_2 &= 36363x^2 + 20865x + 4024. \end{aligned}$$

Step 1. We begin by calculating $I_3 = I_1 I_2 = [s_3, s_3'(u_3 + y), v_3 + w_3 y + y^2]$. Using Algorithm 7.2, we have

$$s_3 = x^6 + 36771x^5 + 3833x^4 + 68320x^3 + 58883x^2 + 28477x + 40280,$$
$$s_3' = 1, \quad u_3 = 23786x^5 + 78427x^4 + 42856x^3 + 798x^2 + 34083x + 39670,$$
$$v_3 = 39324x^5 + 61659x^4 + 4965x^3 + 4197x^2 + 80846x + 10040, \quad w_3 = 0.$$

Step 2. We compute the inverse $I_4 = \overline{I_3} = [s_4, s_4', u_4 + y, v_4 + w_4 y + y^2]$, where

$$s_4 = s_4' = x^6 + 36771x^5 + 3833x^4 + 68320x^3 + 58883x^2 + 28477x + 40280,$$
$$u_4 = 0, \quad v_4 = 47857x^5 + 25522x^4 + 82216x^3 + 82984x^2 + 6335x + 77141,$$
$$w_4 = 63395x^5 + 8754x^4 + 44325x^3 + 86383x^2 + 53098x + 47511.$$

Step 3. The element of minimal norm in I is

$$\begin{aligned} \alpha = {} & 14437x^5 + 12418x^4 + 47789x^3 + 40726x^2 + 72702x + 8382 \\ & + (47574x^3 + 77483x^2 + 31215x + 25022)y + (24532x^2 + 822x + 29087)y^2. \end{aligned}$$

Step 4. We then calculate the canonical basis for the ideal generated by α, $[s_5, s_5'(u_5 + y), v_5 + w_5 y + y^2]$, where

$$\begin{aligned} s_5 &= x^9 + 15912x^8 + 53138x^7 + 35276x^6 + 46854x^5 \\ &\quad + 77875x^4 + 1011x^3 + 45854x^2 + 21706x + 70451, \\ s_5' &= x^6 + 36771x^5 + 3833x^4 + 68320x^3 + 58883x^2 + 28477x + 40280, \\ u_5 &= 35972x^2 + 23411x + 34488, \\ w_5 &= 63395x + 8754x + 44325x + 86383x + 53098x + 47511, \\ v_5 &= 78469x^8 + 2050x^7 + 27283x^6 + 40343x^5 + 10729x^4 \\ &\quad + 39885x^3 + 15840x^2 + 87166x + 47527. \end{aligned}$$

Step 5. Finally we calculate $\langle\alpha\rangle / I_4 = I = [S, S'(U + y), V + Wy + y^2]$, the distinguished representative in the class of $I_1 I_2$:

$$\begin{aligned} S &= x^3 + 66322x^2 + 37156x + 11882, & S' &= 1, & W &= 0, \\ U &= 35972x^2 + 23411x + 34488, & V &= 69203x^2 + 795x + 49915. \end{aligned}$$

Example 11.2. Let $K = \mathbb{F}_{1621}$, and let $f(x)$ be the polynomial

$$x^5 + 999x^4 + 991x^3 + 1368x^2 + 869x + 407,$$

so our curve has genus 3. This time we will consider the product of two distinguished ideals which are not relatively prime. Let $I_1 = [s_1, s_1'(u_1 + y), v_1 + w_1y + y^2]$, where

$$s_1 = x^3 + 1023x^2 + 119x + 1412, \qquad s_1' = x + 384,$$
$$u_1 = 286x + 737, \qquad v_1 = 1124x^2 + 954x + 444, \qquad w_1 = 904,$$

and $I_2 = [S_2, s_2(u_2 + y), v_2 + w_2y + y^2]$, where

$$s_2 = x^3 + 1239x^2 + 73x + 491, \qquad s_2' = x + 384,$$
$$u_2 = 916x + 596, \qquad v_2 = 356x^2 + 957x + 191, \qquad w_1 = 1344.$$

Step 1. This time, when we calculate $I_3 = I_1I_2$, we note that there is a nonprimitive factor. Our ideal is of the form $\langle D\rangle[s_3, s_3'(u_3 + y), v_3 + w_3y + y^2]$, where

$$D = x + 384, \quad s_3 = x^5 + 257x^4 + 260x^3 + 987x^2 + 1080x + 1282, \quad s_3' = 1,$$
$$u_3 = 832x^4 + 874x^3 + 834x^2 + 543x + 572,$$
$$v_3 = 85x + 1410x + 1310x + 970x + 334, \quad w_3 = 0.$$

We throw away the factor $\langle D\rangle$ and continue with

$$I_3 = [s_3, s_3'(u_3 + y), v_3 + w_3y + y^2].$$

Step 2. We compute the inverse $I_4 = \overline{I_3} = [s_4, s_4', u_4 + y, v_4 + w_4y + y^2]$, where

$$s_4 = s_4' = x^5 + 257x^4 + 260x^3 + 987x^2 + 1080x + 1282,$$
$$u_4 = 0, \quad v_4 = 1536x^4 + 211x^3 + 311x^2 + 651x + 1287,$$
$$w_4 = 789x^4 + 747x^3 + 787x^2 + 1078x + 1049.$$

Step 3. The element of minimal norm in I is

$$\alpha = 999x^4 + 191x^3 + 833x^2 + 1300x + 907$$
$$+ (373x^3 + 1104x^2 + 476x + 589)y + (1404 + 754x)y^2.$$

Step 4. We then calculate the canonical basis for the ideal generated by α, $[s_5, s_5'(u_5 + y), v_5 + w_5y + y^2]$, where

$$s_5 = x^9 + 1511x^8 + 1444x^7 + 1354x^6 + 1155x^5 + 1247x^4$$
$$+ 1066x^3 + 782x^2 + 405x + 1548,$$
$$s_5' = x^5 + 257x^4 + 260x^3 + 987x^2 + 1080x + 1282,$$
$$u_5 = 79x^3 + 35x^2 + 320x + 961, \qquad w_5 = 789x^4 + 747x^3 + 787x^2 + 1078x + 1049,$$
$$v_5 = 1062x^8 + 1610x^7 + 206x^6 + 805x^5 + 1142x^4 + 793x^3 + 878x^2 + 1607x + 428.$$

Step 5. Finally we calculate $\langle\alpha\rangle/I_4 = I = [S, S'(U + y), V + Wy + y^2]$, the distinguished representative in the class of I_1I_2:

$$S = x^4 + 1254x^3 + 1485x^2 + 1059x + 684, \quad S' = 1, \qquad W = 0,$$
$$U = 79x^3 + 35x^2 + 320x + 961, \qquad V = 204x^3 + 971x^2 + 1482x + 1314.$$

Acknowledgments

The author would like to extend his thanks to the referee for many valuable suggestions that have greatly improved this paper, and to Renate Scheidler and Andreas Stein for fruitful discussions on this topic.

References

[C] Cantor, David G. Computing in the Jacobian of a hyperelliptic curve. Math. Comp. 48 (1987), no. 177, 95–101. MR **88f:**11118

[GPS] Galbraith, Paulus, Smart. Arithmetic of Superelliptic Curves. Math. Comp. 71 (2002), 393–405. MR **2002h:**14102

[H] Hartshorne, Robin. Algebraic Geometry. Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York - Heidelberg, 1997. MR **57:**3116

[L] Lenstra, A. K. Factoring multivariate polynomials over finite fields. J. of Comput. System Sci. 30 (1985),no. 2, 235–248. MR **87a:**11124

[Sch] Scheidler, R. Ideal arithmetic and infrastructure in purely cubic function fields. J. Théor. Nombres Bordeaux 13 (2002), 609–631. MR **2002k:**11209

[SchSt] Scheidler, R., Stein, A. Unit computation in purely cubic function fields of unit rank 1. *Algorithmic number theory (Portland, OR, 1998)* 592-606, Lecture Notes in Comput. Sci., 1423, Springer-Verlag, Berlin, 1998. MR **2000k:**11145

[St] Stichtenoth, Henning. Algebraic Function Fields and Codes. Universitext. Springer-Verlag, Berlin, 1993. MR **94k:**14016

Department of Mathematics, University of Illinois, Urbana, Illinois 61801

Current address: Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario N2G 3L1 Canada

E-mail address: `m-bauer@math.uiuc.edu, mbauer@math.uwaterloo.ca`