Contributions to Discrete Mathematics

Volume 8, Number 1, Pages 66–99
ISSN 1715-0868

COMPUTATIONS IN CUBIC FUNCTION FIELDS OF CHARACTERISTIC THREE

MARK BAUER AND JONATHAN WEBSTER

Abstract. This paper contains an account of arbitrary cubic function fields of characteristic three. We define a standard form for an arbitrary cubic curve and consider its function field. By considering an integral basis for the maximal order of these function fields, we are able to calculate the field discriminant and the genus. We also give explicit algorithms for ideal arithmetic which for certain cubic function fields give rise to composition and reduction algorithms for computing in the associated ideal class group.

1. Introduction

Calculating invariants of a global field and its maximal order remains one of the central problems in computational number theory. Motivated by hyperelliptic curve cryptography and well-studied cubic number fields, a host of authors have researched computational properties of cubic function fields. From calculating fundamental units [12], to computing in the ideal class group [1], to tabulating [9], to describing and classifying arbitrary cubic function fields [6, 11], the results (mostly) exclude characteristic three.

In the case in which characteristic three is considered, it is often through generic methods. The function field analogue of the Round 2 algorithm, algebraic methods involving desingularization, or using Groebner basis to do ideal arithmetic, all may be applied to the problems considered in this paper. However, these methods are often inefficient and can make it difficult to understand how the basic invariants of a function field arise from the defining curve. For elliptic curves and hyperelliptic curves, we may compute the desired quantities directly from the defining curve and the underlying finite field. For cubic function fields in characteristic greater than three, much progress has been made in this regard; our goal is to extend these computations to characteristic three. It is important to mention that some work to this end has also been undertaken independently in [2]. The work presented here is completely general and does not assume a square free index as in [2]. Furthermore, the aim of our project is also different — as

Received by the editors January 3, 2011, and in revised form February 28, 2013.
2010 *Mathematics Subject Classification.* 11Y40.

opposed to developing a coherent theory for signatures across different characteristics, we have chosen to completely analyze all cubic function fields in characteristic three and develop the associated algorithms for computations.

We begin by developing the basic invariants of cubic function fields. Section 2 defines function fields and states the standard model that will be used to define the field. Section 3 contains the calculation of the integral basis and the field discriminant for the fixed model. The following section describes the splitting behavior for places that is used in Section 5 to calculate the genus. Next we review the relationship between the ideal class group and the Jacobian to motivate an explicit means of doing computations in the ideal class group. We state integral basis for the prime ideals and their powers in Section 7. Using this basis motivates arbitrary ideal arithmetic which is given over the next two sections. Finally, we state an algorithm to do composition and reduction (the latter requires $3 \not| \deg(FI^2)$ – see Theorem 6.3) in the ideal class group for most cubic function fields with unit rank 0 and conclude with an example computation.

2. Standard Form

As there are many good introductions to algebraic function fields (for example [7, 13]), we will only seek to clarify the notation used in this paper. As usual, let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q[x]$ and $\mathbb{F}_q(x)$ be the ring of polynomials and the field of rational functions, respectively, in x over $\mathbb{F}_q$. An algebraic function field is a finite extension $\mathcal{F}$ of $\mathbb{F}_q(x)$; it thus may be written as $\mathcal{F} = \mathbb{F}_q(x, y)$ with y a root of $H(T)$, where $H(T)$ is an absolutely irreducible monic polynomial in $(\mathbb{F}_q[x])[T]$ of degree $n = [\mathcal{F} : \mathbb{F}_q(x)]$.

When $\mathrm{char}(\mathbb{F}_q) \neq 3$, cubic function fields may be studied by examining the standard form for the defining polynomial that is given by $T^3 - AT + B = 0$ with $A, B \in \mathbb{F}_q[x]$ provided there is no non-constant $Q \in \mathbb{F}_q[x]$ such that $Q^2|A$ and $Q^3|B$ (see [11] for details). By considering these birationally equivalent curves, it is possible to study arbitrary curves as a two-parameter family. Our goal will be to find a model which gives a similar two-parameter family in characteristic three. Henceforth, let $\mathrm{char}(\mathbb{F}_q) = 3$ unless explicitly stated otherwise.

Write $H(x, T) = T^3 + UT^2 + VT + W$ with $U, V, W \in \mathbb{F}_q[x]$ and $W \neq 0$. If $U = V = 0$, then the function field associated with this curve is purely inseparable, and hence isomorphic to the rational function field. We thus require $U \neq 0$ or $V \neq 0$ to avoid this degenerate case. If $U = 0$ then making the polynomial monic yields a curve in of the form $T^3 - AT + B = 0$. Otherwise, complete the square and consider the monic, integral, reciprocal polynomial to get a curve in the form $T^3 - AT + B = 0$.

Henceforth, we will restrict our attention to curves of the form $T^3 - AT + B = 0$. In what follows we use the fact that for any $a \in \mathbb{F}_q[x]$, the transformation $T \to T + a$ yields a birationally equivalent curve $T^3 - AT + (a^3 - aA + B) = 0$. Our goal is to minimize the repeated factors dividing

A and then reduce the degree of B sufficiently to determine whether or not wild ramification occurs at infinity.

If there is a polynomial $Q \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ such that $Q^2 | A$ and $Q^3 | (a^3 - aA + B)$ for some $a \in \mathbb{F}_q[x]$ then it is possible to consider the curve given by

$$T^3 - \left(\frac{A}{Q^2}\right) T + \left(\frac{a^3 - aA + B}{Q^3}\right) = 0. \tag{2.1}$$

The existence of such a Q and a implies $(y+a)/Q$ is integral and has minimal polynomial given by (2.1). In this situation, the polynomial Q corresponds to removable singularities that preserve the shape of the model for the given curve.

To find Q and a, it is sufficient to check irreducible polynomials P such that $P^2 | A$. We may write $a = a_0 + a_1 P + a_2 P^2$ with $a_0, a_1, a_2 \in \mathbb{F}_q[x]$, with a_0 and a_1 having degree less than that of P. Since only a_0 affects the congruence $a^3 - aA + B \equiv 0 \pmod{P^3}$, we solve $a_0^3 + B \equiv 0 \pmod{P}$ which has a unique solution because the field has characteristic three. It then becomes a matter of checking whether $a_0^3 - a_0 A + B \equiv 0 \pmod{P^3}$. If the congruence holds, redefine A as A/P^2 and B as $(a_0^3 - a_0 A + B)/P^3$. This process may be repeated until all repeated factors of A that can be removed have been removed.

We now turn our focus to reducing the degree of B. Consider the set of transformations of the form $T \to T + \gamma_n x^n$. After using one of these transformations, the curve will be given by the equation

$$T^3 - A(x)T + B(x) + \gamma_n^3 x^{3n} - \gamma_n x^n A(x) = 0.$$

We are therefore only interested in those transformations that satisfy $\deg\left(B(x) + \gamma_n^3 x^{3n} - \gamma_n x^n A(x)\right) < \deg B(x)$. If $2 \deg B > 3 \deg A$, the only such transformation that can satisfy this criterion is when $3 \mid \deg B$. Letting $n = (\deg B)/3$ and b_{3n} be the leading coefficient of $B(x)$, we choose $\gamma_n = -b_{3n}^{1/3} \in \mathbb{F}_q$. By successively using transformations of this form, it is possible to force the curve to satisfy one of the following two distinct criteria:

$$3 \nmid \deg B \quad \text{and} \quad 2 \deg B > 3 \deg A \tag{2.2}$$

or

$$2 \deg B \leq 3 \deg A. \tag{2.3}$$

For our purposes, this reduction is sufficient to identify wild ramification of the infinite place. However, when the latter condition is satisfied, it may still be possible to do additional transformations to reduce the degree of B if desired. In this situation, let k and m denote the degree of $A(X)$ and $B(x)$, respectively, with leading coefficients a_k and b_m. If $2 \deg B = 3 \deg A$, then the transformation that reduces the degree has $n = m/3 = k/2$ and γ_n is a root of the equation $\gamma^3 - a_k \gamma + b_m$ (which may or may not have a root in $\mathbb{F}_q$). Note, we will see this equation arise again when considering the proof

of Theorem 4.2. For $2 \deg B < 3 \deg A$, choosing $n = m - k$ and $\gamma_n = b_m/a_k$ will work (provided $m \geq k$).

Definition 2.1. *A curve is said to be a* standard model *(or in* standard form*) for a cubic function field if it is of the form $T^3 - AT + B = 0$ with no $Q, a \in \mathbb{F}_q[x]$, Q non-constant, such that $Q^2|A$ and $Q^3|a^3 - aA + B$ and satisfies either (2.2) or (2.3).*

It will also be useful to have a simple criterion to detect singularities.

Proposition 2.2. *The curve $T^3 - A(x)T + B(x) = 0$ is nonsingular if and only if $\deg d = 0$ where $d = \gcd(A(x), A'(x)^3B(x) + B'(x)^3)$.*

Proof. A singular point $(\alpha, \beta) \in \overline{\mathbb{F}}_q^2$ satisfies the following three equations.

$$\beta^3 - A(\alpha)\beta + B(\alpha) = 0. \tag{2.4}$$

$$A(\alpha) = 0. \tag{2.5}$$

$$-A'(\alpha)\beta + B'(\beta) = 0. \tag{2.6}$$

From (2.5), α is a root of $A(x)$, and combined with (2.4) we see that $-\beta^3 = B(\alpha)$. Cubing (2.6) we get $-A'(\alpha)^3\beta^3 + B'(\alpha)^3 = 0$ which implies $A'(\alpha)^3B(\alpha) + B'(\alpha)^3 = 0$. Thus α is a common root of $A(x)$ and $A'(x)^3B(x) + B'(x)^3$.

For the converse let a be a common root of $A(x)$ and $A'(x)^3B(x)+B'(x)^3$. Since a is a root of $A(x)$, (2.5) is satisfied. Since $\overline{\mathbb{F}_q}$ is perfect, we can find β such that $\beta^3 = -B(\alpha)$ in order to satisfy (2.4). With (2.4) and (2.5) satisfied, it is clear that (2.6) is also satisfied by the above construction. □

Note that for large q we do not expect a curve selected in standard form to be singular. That is, if singularity is detected by $\deg d$ not being 0, then it is a question of when two "random" polynomials are relatively prime. This happens with probability roughly $1 - 1/q$.

Calculating the standard form and the integral basis, as well as finding the field discriminant and the genus are all closely related to singularity. In fact, if the standard form is nonsingular, then $\{1, y, y^2\}$ is an integral basis for the maximal order and $\Delta = D = \operatorname{disc}(y) = A^3$ (for the reader who is unfamiliar with this concept, it will be defined more formally below). In the next section we will show that the square factors of $d = \gcd(A(x), A'(x)^3B(x) + B'(x)^3)$ are $I = \operatorname{ind}(y)$. With D and I in hand, we can compute $\Delta = \operatorname{disc}(\mathcal{F})$.

Knowing that $D = A^3$ and that Δ differs from D by square factors is enough to determine when $\mathcal{F}$ is an Artin-Schreier extension.

Theorem 2.3. *$\mathcal{F}$ is an Artin-Schreier extension if and only if $A(x)$ is a square.*

Proof. Cubic extensions are Galois (which is to say an Artin-Schreier extension in characteristic 3) if and only if their discriminant is a square. In order to have a square discriminant, $A(x)$ must be a square. Conversely, if $T^3 - T = f/g$ with $f, g \in \mathbb{F}_q[x]$ is an Artin-Schreier extension then

$T^3 - g^2T = fg^2$ is an integral model for this equation. By renaming, we have $A(x) = g(x)^2$ a square. □

3. Integral basis and field discriminant

We will follow Chapter 2 Section 17 of [3] to find an integral basis for $\mathcal{O}_\mathcal{F}$, the integral closure of $\mathbb{F}_q[x]$ in $\mathcal{F}$. Recall that the powers $1,\ y,\ y^2$ form a basis of the $\mathbb{F}_q(x)$-vector space $\mathcal{F}$. An $\mathbb{F}_q(x)$-basis given by $\{\alpha_0, \alpha_1, \alpha_2\}$ is triangular if α_0 and α_1 are an $\mathbb{F}_q(x)$-linear combination of 1 and $1, y$, respectively. The three conjugate mappings taking y to the three roots, $y = y^{(0)}, y^{(1)}, y^{(2)}$, define for every $\alpha \in \mathcal{F}$ its three conjugates $\alpha = \alpha^{(0)}, \alpha^{(1)}, \alpha^{(2)}$, and allows for the following definition of the discriminant of three elements:

$$\operatorname{disc}(\alpha_0, \alpha_1, \alpha_2) = \det(\alpha_i^{(j)})^2_{0\le i,j\le 2} \in \mathbb{F}_q(x).$$

The ring $\mathcal{O}_\mathcal{F}$ always admits a triangular basis, one element of which is (obviously) in $\mathbb{F}_q^*$. The discriminant of $\mathcal{F}/\mathbb{F}_q(x)$ is $\operatorname{disc}(\mathcal{F}) = \operatorname{disc}(\alpha_0, \alpha_1, \alpha_2)$ where $\{\alpha_0, \alpha_1, \alpha_2\}$ is an integral basis of $\mathcal{F}/\mathbb{F}_q(x)$, i.e. a basis for $\mathcal{O}_\mathcal{F}$. For any element $\alpha \in \mathcal{F}$, the index of α satisfies $\operatorname{disc}(\alpha) = \operatorname{ind}(\alpha)^2 \operatorname{disc}(\mathcal{F})$, which will be crucial in determining a basis for $\mathcal{O}_\mathcal{F}$.

Writing down a basis in triangular form, we will be able to deduce restrictions on the elements of the basis simply by using the fact that they are integral. These restrictions arise naturally by examining the minimal polynomial of each element. Following [3], we may choose the product of the latter two basis elements to be in $\mathbb{F}_q[x]$, but we may not assume that $I_1 = 1$. Consider the integral basis given by

$$\left[1, \frac{y - i}{I_1}, \frac{c + by + y^2}{I_2}\right] = [1, \rho, \omega]$$

with $I_1, I_2, i, c, b \in \mathbb{F}_q[x]$, I_1 and I_2 monic (the choice to use i is to emphasize its relationship with the index, which we will denote I). As mentioned before, the integral basis construction was a motivation for the choice of the standard model; in particular, the minimal polynomial of ρ is given by

$$\rho^3 - \frac{A}{I_1^2}\rho + \frac{i^3 - iA + B}{I_1^3} = 0.$$

Since this is an integral equation in ρ, it must be that $I_1^2 | A$ and $I_1^3 | i^3 - iA + B$. This is the same criterion as (2.1). Thus the reduction to standard form forces $I_1 = 1$. Now consider $\rho\omega \in \mathbb{F}_q[x]$ to get additional criteria on i, b, c, and I_2:

$$\rho\omega = \frac{(b - i)y^2 + (A - ib + c)y - (ic + B)}{I_2}.$$

This implies $i = b$, $c = i^2 - A$, and $I_2 | ic + B$. Combining the last two statements, $I_2 | i^3 - iA + B$. Rewrite ω as $(y^2 + iy + i^2 - A)/I_2$ and consider

its minimal polynomial to get our final criterion:

$$\omega^3 + \frac{A}{I_2}\omega^2 - \frac{(i^3 - iA + B)^2}{I_2^3} = 0.$$

This gives $I_2|A$ and $I_2^3|(i^3-iA+B)^2$. Choosing i such that I_2 is of maximal degree yields the basis. This observation will in fact force I_2, which is the index of y, to be square-free. From this point forward the subscript of I_2 will be dropped and the index of y will be denoted I.

Proposition 3.1. *A curve in standard form has $I = \mathrm{ind}(y)$ being square-free.*

Proof. Let $P \in \mathbb{F}_q(x)$ be irreducible such that $P|I$, the index. If $v_P(A) = 1$ then $v_P(I) = 1$. So assume $v_P(A) \geq 2$ and consider i such that $I^3|(i^3 - iA + B)^2$. If $v_P(i^3 - iA + B) = 2$ then $v_P(I) = 1$. However, if $v_P(A) \geq 2$ and $v_P(i^3 - iA + B) \geq 3$ then the curve is not in standard form. □

Having established that the index is square free, it can be calculated directly from the square-free factorization of d (defined in Proposition 2.2). This allows us to calculate i as it is unique modulo I and hence determined by its residue class modulo each distinct prime dividing I. For each irreducible polynomial $P|I$, we solve $(i^3 - iA + B)^2 \equiv 0 \pmod{P^3}$ and construct the solution using the Chinese Remainder Theorem. As we did when removing singularities, we write $i = i_0 + i_1P + i_2P^2$ and solve congruence equations modulo P, P^2, and P^3.

With the index of y calculated, it is straightforward to determine the discriminant of the function field simply by noting that $D = A^3$ and hence $\Delta = A^3/I^2$. Letting $A = EI$ and $FI^2 = i^3 - iA + B$, we have the following identities for various products of integral basis elements:

$$\rho^2 = I\omega + A, \quad \omega^2 = -E\omega - F\rho, \quad \rho\omega = -FI. \tag{3.1}$$

4. Splitting of Places

The places of $\mathbb{F}_q(x)$ consist of finite places, identified with the monic irreducible polynomials in $\mathbb{F}_q[x]$, and the place at infinty P_∞, identified with $1/x$. Every place P has a corresponding discrete valuation on $\mathbb{F}_q(x)$ denoted v_P and a discrete valuation ring $\mathcal{O}_P = \{G \in \mathbb{F}_q(x) | v_P(G) \geq 0\}$. These definitions may be naturally extended to the field $\mathcal{F}$. That is, the finite places are associated with the non-zero prime ideals in $\mathcal{O}_\mathcal{F}$ and the infinite places are associated to the non-zero prime ideals in the integral closure of $\mathcal{O}_{P_\infty}$. If $\mathfrak{p}$ is a place of $\mathcal{F}$ then let $v_\mathfrak{p}$ denote its associated discrete valuation and $\mathcal{O}_\mathfrak{p} = \{\alpha \in \mathcal{F} | v_\mathfrak{p}(\alpha) \geq 0\}$ its discrete valuation ring. There exists a place $P \in \mathbb{F}_q(x)$ with $v_\mathfrak{p}(P) > 0$; we say $\mathfrak{p}$ lies above P and write $\mathfrak{p}|P$. The positive integer $e(\mathfrak{p}|P) = v_\mathfrak{p}(P)$ is the ramification index and we say P is ramified if $e(\mathfrak{p}|P) > 1$ and unramified otherwise. Further, if $\gcd(e(\mathfrak{p}|P), q) = 1$ a place is called tamely ramified and wildly ramified otherwise. The inertial degree

of a place is denoted $f(\mathfrak{p}|P)$ and has value $[\mathcal{O}_\mathfrak{p}/\mathfrak{p} : \mathcal{O}_P/(P)]$ if P is a finite place and $[\mathcal{O}_\mathfrak{p}/\mathfrak{p} : \mathbb{F}_q]$ for the infinite place.

Knowing the splitting behavior of places is a key component to determine the genus of the function field $\mathcal{F}$. We now turn our attention to characterizing the splitting behavior of all the places, starting with the finite places and concluding with the infinite place.

Theorem 4.1. *Let $P \in \mathbb{F}_q[x]$ be an irreducible polynomial and let $q_1 = q^{deg(P)}$. Also let $a \equiv A, b \equiv B \pmod{P}$. Then the principal ideal (P) splits into prime ideals in $\mathcal{O}_\mathcal{F}$ as follows:*

1. *If $v_P(\Delta) > 2$, then $(P) = \mathfrak{p}^3$.*
2. *If $v_P(\Delta) = 1$, then $(P) = \mathfrak{q}\mathfrak{p}^2$.*
3. *Otherwise $P \nmid A$, $d = gcd(T^{q_1} - T, T^3 - aT + b)$, and we consider three cases:*
   (a) *If $\deg d = 0$, then $(P) = \mathfrak{p}$.*
   (b) *If $\deg d = 1$, then $(P) = \mathfrak{p}\mathfrak{q}$.*
   (c) *If $\deg d = 3$, then $(P) = \mathfrak{p}\mathfrak{q}\mathfrak{r}$.*

Proof. For primes not dividing A, $\{1, y, y^2\}$ is an integral basis of $\mathcal{O}_P[y]/\mathcal{O}_P$ and thus Kummer's Theorem may be applied to get the desired result. By Dedekind's Different Theorem, ramified primes are distinguished by the multiplicity with which they divide the field discriminant and thus the the two ramified cases are as claimed (see Theorem III.5.1 in [13]). □

While we could consider a transformation to bring the infinite place to a finite place and invoke Kummer's Theorem as above, there is no guarantee that the infinite place is nonsingular. We will avoid this approach and appeal to completions using Theorem 3.1 of [6]. Begin by defining $\phi(T) = T^3 - At + B$ to be the defining polynomial for the curve. Then there will be a root of $\phi(T)$ in $\mathbb{F}\langle x^{-1}\rangle$, where $\mathbb{F}$ is some finite extension of $\mathbb{F}_q$, if and only if the infinite place is not wildly ramified. A curve in the form of (2.3) characterizes the infinite place being tamely ramified or unramified by constructing just such a root in $\mathbb{F}\langle x^{-1}\rangle$. From the construction, it will then be a matter of counting the number of roots, and hence finding $[\mathbb{F} : \mathbb{F}_q]$ as this corresponds to the inertial degree. If such a root can not be constructed then the place at infinity is wildly ramified.

Assume the curve is in standard form and satisfies (2.3). Consider constructing a root $y \in \mathbb{F}\langle x^{-1}\rangle$ of $\phi(T)$. We can write

$$y = y_n x^n + y_{n-1} x^{n-1} + \cdots$$

where $y_i \in \mathbb{F}$. Let $A(x) = a_{2n}x^{2n} + \cdots + a_0$ and $B(x) = b_{3n}x^{3n} + \cdots + b_0$ with $a_i, b_i \in \mathbb{F}_q$. By writing the polynomials this way, we only assume that either a_{2n} or a_{2n-1} is nonzero. If $a_{2n} = 0$, then $b_{3n} = 0$ and $b_{3n-1} = 0$ in order to satisfy (2.3). The coefficients of the powers of x in the equation $y^3 - A(x)y + B(x) = 0$ are as follows:

$$\begin{aligned}
x^{3n} &: y_n^3 - a_{2n}y_n + b_{3n} \\
x^{3n-1} &: -a_{2n-1}y_n - a_{2n}y_{n-1} + b_{3n-1} \\
x^{3n-2} &: a_{2n-2}y_n - a_{2n-1}y_{n-1} - a_{2n}y_{n-2} + b_{3n-2} \\
x^{3n-3} &: y_{n-1}^3 - a_{2n-3}y_n - a_{2n-2}y_{n-1} - a_{2n-1}y_{n-2} - a_{2n}y_{n-3} + b_{3n-3} \\
\vdots &\qquad \vdots
\end{aligned}$$

The equation associated with x^{3n} is cubic in y_n. After the initial cubic equation, we have an equation associated to x^{3n-i} that is linear in y_{n-i} for $i > 0$. That is, the values for y_{n-i} are uniquely determined by the initial choice for y_n. It is worth noting that these are intrinsically related to the transformations that are used to reduce the degree of B in the standard model. Determining the number of solutions to the equation $Y^3 - a_{2n}Y + b_{3n} = 0$ and the fields they lie in completely answers the question. If the curve is in standard form and satisfies (2.2), then this same process immediately leads to an impossibility since the first equation derived will dictate that the leading coefficient of B needs to be 0. This gives us the following theorem.

Theorem 4.2. *The place at infinity splits as follows.*

(1) If $\phi(T)$ satisfies (2.2), then $(\infty) = \mathfrak{p}^3$.
(2) If $\phi(T)$ satisfies (2.3) and $\deg(A)$ is odd, then $(\infty) = \mathfrak{pq}^2$.
(3) If $\phi(T)$ satisfies (2.3) and $\deg(A)$ is even, then $d = \gcd(T^q - T, T^3 - a_{2n}T + b_{3n})$ determines the splitting type.
  (a) If $\deg d = 0$, then $(\infty) = \mathfrak{p}$.
  (b) If $\deg d = 1$, then $(\infty) = \mathfrak{pq}$.
  (c) If $\deg d = 3$, then $(\infty) = \mathfrak{pqr}$.

We now turn our attention to calculating the genus of the function field.

5. Genus

We will calculate the genus with the Hurwitz Genus Formula, which requires knowledge of the degree of the different. Having the field discriminant, Dedekind's Different Theorem gives the different exponents for the finite places. For the infinite place, it is either split or totally ramified in which case determining the different exponent is a matter of finding a uniformizer for the place and evaluating a particular valuation (see Theorem III.5.12 of [13]).

Lemma 5.1. *If the place at infinity is totally ramified then it has different exponent $\delta_\infty = 2\deg B - 3\deg A + 2$.*

Proof. Let $\mathfrak{p}$ be the place at infinity in $\mathcal{F}$. Since it is totally ramified and must lie above the unique infinite place in $\mathbb{F}_q(x)$ with uniformizer $1/x$,

$v_{\mathfrak{p}}(x) = -3$. By examining the equation $y^3 - A(x)y + B(x) = 0$, we can determine $v_{\mathfrak{p}}(y) = -\deg B$.

If $\deg B = 3m - 1$ then a uniformizer of $\mathfrak{p}$ is given by $t = y/x^m$. The minimal polynomial for t is $f(t) = t^3 - Atx^{-2m} + Bx^{-3m}$. Applying the theorem we see

$$\delta_\infty = v_{\mathfrak{p}}(f'(t)) = v_{\mathfrak{p}}(Ax^{-2m}) = -3\deg A + 6m = 2\deg B - 3\deg A + 2.$$

The case $\deg B = 3m + 1$ follows in a similar manner. □

Theorem 5.2. *If* (2.2) *holds then the genus of* $\mathcal{F}$ *is*

$$g = \deg B - \deg I - 1.$$

If (2.3) *holds, then*

$$g = (3\deg A - 2\deg I + \delta_\infty - 4)/2$$

where $\delta_\infty = 0$ *if* $\deg A$ *is even and* $\delta_\infty = 1$ *if* $\deg A$ *is odd.*

Proof. The Hurwitz Genus Formula gives

$$2g - 2 = -2[\mathcal{F} : \mathbb{F}_q(x)] + \sum_{\mathfrak{p}\in\mathbb{P}_\mathcal{F}} d(\mathfrak{p}|P).$$

In the first case this yields

$$2g - 2 = -6 + (3\deg A - 2\deg I) + (2\deg B - 3\deg A + 2),$$

which upon simplification gives the desired result. In the second case the infinite place is not wildly ramified, and hence its different exponent δ_∞ can only take the values 0 or 1. Since the genus is an integer, the parity of $\deg A$ determines the value of δ_∞. □

Note that the degree of B is only involved in the case when (2.2) holds, and hence the degree of B is an invariant for the model.

With the basic invariants of cubic function fields in hand, the focal point for the remainder of this paper is to develop the arithmetic of ideals. As in the previous sections, one can appeal to generic algorithms to solve this problem. However, these algorithms typically require operations on large matrices or an appeal to Groebner basis. We desire, like elliptic curves and hyperelliptic curves (using Cantor's algorithm), a method to do computations that depends only on the underlying curve parameters and the finite field.

6. Divisor Class Groups and Ideal Class Groups

This section provides an overview of the relationship between the Jacobian of a curve and the ideal class group of a function field. As there are many sources for this material (see e.g.[1, 4, 5, 10, 11]), we will be relatively brief and only provide the relevant definition and results where needed. Once this is completed, it will be possible to develop arithmetic on ideals and, for a

certain class of curves, fully realize arithmetic in the ideal class group and hence the Jacobian of the curve.

A divisor is a finite formal sum of places in $\mathcal{F}$. The set of all divisors forms a free abelian group. We will work in a specific finite subgroup of this group. Let S be the set of finite places in $\mathcal{F}$. There is an isomorphism between the divisors with support in S, $\mathcal{D}_F(S)$, and the fractional ideals in $\mathcal{O}_\mathcal{F}$, $\mathcal{I}(\mathcal{O}_\mathcal{F})$. The *Fundamental theorem of ideal theory in an algebraic function field* [4, p 401] gives the isomorphism as

$$\Phi \ : \ \mathcal{D}^0_\mathcal{F}(S) \to \mathcal{I}(\mathcal{O}_\mathcal{F}), \quad D \longmapsto \left\{ \alpha \in F^\times \;\middle|\; \sum_{P\in S} v_P(\alpha)P \geq D \right\} \cup \{0\}. \tag{6.1}$$

This may also be defined by

$$\sum n_P P \longmapsto \prod_{P\in S} (P \cap \mathcal{O}_\mathcal{F})^{n_P}.$$

In general, the ideal class group is related to the Jacobian by the following exact sequence (see Theorem 14.1 of [8])

$$(0) \to \mathcal{D}_\mathcal{F}(S^c)/\mathcal{P}_\mathcal{F}(S^c) \to \mathcal{J}_\mathcal{F} \to \mathcal{C}l(\mathcal{O}_F) \to \mathbb{Z}/f\mathbb{Z} \to (0),$$

where S^c is the set of infinite places (the set compliment of S in $\mathbb{P}_\mathcal{F}$) and f is the greatest common divisor of the degree of the places at infinity. Specifically, if a function field has a unique place at infinity of degree 1, the points on the Jacobian will be isomorphic to the ideal class group.

We use the hierarchy of divisors (and hence ideals) defined in [1] so that there is a way to represent elements of the divisor class group of degree zero in a unique way with minimal information. A divisor D is *effective* if $D > 0$ (that is, $n_P \geq 0$ for all $P \in \mathbb{P}_F$) and denote its effective part as D^+, i.e.

$$D = \sum_{P\in\mathbb{P}_\mathcal{F}} n_P P \quad \Longrightarrow \quad D^+ = \sum_{P\in\mathbb{P}_\mathcal{F}, n_P>0} n_P P.$$

A degree zero divisor is called *finitely effective* if its finite part is effective; it can be shown that every divisor $D \in \mathcal{D}^0_\mathcal{F}$ is equivalent to a finitely effective divisor. This is the first step in the hierarchy.

A finitely effective divisor is *semi-reduced* if there does not exist a non-empty sub-sum of the form (α) where $\alpha \in \mathbb{F}_q[x]\backslash\mathbb{F}_q$. Again, it is straightforward to show that every divisor is equivalent to a semi-reduced divisor, extending the hierarchy. A *semi-reduced* divisor D is *reduced* if $\deg D^+ \leq g$ where g is the genus of the curve. Using the Riemann-Roch Theorem, it is possible to prove that every divisor class also contains a reduced divisor.

To complete the hierarchy, we define a *distinguished* divisor to be a divisor D such that for all other equivalent finitely effective divisors D_1, we have that $\deg D_1^+ \leq \deg D^+$ implies $D = D_1$. If a divisor is distinguished, it is reduced [1, Lemma 1.12]. Unfortunately, we have no apriori way of knowing if such a divisor exists or of verifying that a divisor is distinguished.

The above definitions for a divisor D can immediately be transferred to fractional ideals by first considering D^+ and then applying the isomorphism (6.1). Finitely effective divisors map to integral ideals, and hence we can do computations in this context. Note that in the ideal class group we will mostly work with primitive ideals, that is: $\mathfrak{a}$ is primitive if and only if there is no non-constant polynomial $a(x) \in \mathbb{F}_q[x]$ such that $\langle a(x)\rangle \mid \mathfrak{a}$ where $\langle a(x)\rangle$ represents $a(x)\mathcal{O}_F$. Under the above correspondence, we see that primitive integral ideals give an equivalent notion to semi-reduced divisors. We will call an ideal reduced (resp. distinguished) if it is the image under the above correspondence of a reduced (resp. distinguished) divisor. We now turn our attention to determining when it is possible to show that each divisor class, or equivalently, ideal class, contains a distinguished element.

Let $\alpha = a + b\rho + c\omega \in \mathcal{F}$ with $a, b, c \in \mathbb{F}_q(x)$. Then the norm of α is given by

$$\begin{aligned} N_{\mathcal{F}/\mathbb{F}_q(x)}(\alpha) &= N(a + b\rho + c\omega) \\ &= a^3 - a^2cE + abcIF - ab^2A + b^2cAE + bc^2AF - bc^2EFI \\ &\quad - c^3F^2I - b^3FI^2 \end{aligned}$$

where E and F are as defined in (3.1).

Theorem 6.1. *Let $\alpha = a + b\rho + c\omega \in \mathcal{O}_\mathcal{F}$, $2\deg B > 3\deg A$, and $3 \nmid \deg FI^2$. Then $\deg N(\alpha) = \max\{\deg a^3, \deg b^3FI^2, \deg c^3F^2I\}$.*

The proof follows from a careful analysis of the degrees of the relative terms in the norm expression, and noting that the criterion that $3 \nmid \deg FI^2$ actually forces $\deg FI^2 = \deg B$ and thus the curve satisfies (2.2). A detailed version of the proof can be found in [15].

It is natural to wonder if (2.2) implies $3 \nmid \deg FI^2$. Unfortunately, it is easy to construct a class of curves such that $3 \nmid \deg B$ and $3 | \deg FI^2$. In general we do not expect to deal with such curves; it requires a very special sort of singularity. An example of this type of singularity is given in the following construction.

Example 6.2. *Consider the function field given with parameters $A = (x^2 + x - 1)(x^2 + 1)$ and $B = -x^8 + x^6 + x^5 + x^4 + x^2 + 1$. These parameters define a curve that is in standard form and satisfies (2.2). Both divisors of A are singular, $I = (x^2 + x - 1)(x^2 + 1)$, and $i = -x^3 - x^2$. Thus $\deg FI^2 = \deg(i^3 - iA + B) = 9$.*

Now consider $\alpha = -x^3 + \rho$. A straightforward calculation yields $N(\alpha) = x^8 - x^6 + x^5 - x^4 - x^2 - 1$, while $\max\{\deg a^3, \deg b^3FI^2, \deg c^3F^2I\} = 9$.

Having established this property of the norm, we can now return to the specifics of distinguished ideals. In particular, Theorem 6.1 is exactly what is needed to extend Theorem 5.1 of [1] to this case.

Theorem 6.3. *If $2\deg B > 3\deg A$, and $3 \nmid \deg FI^2$, then every nonzero ideal contains a nonzero element of minimal norm (i.e. the norm has minimal degree) which is unique up to multiplication by an element in $\mathbb{F}_q^\times$.*

The proof is identical to that in [1] but we sketch the key points. The validity is established using Theorem 6.1. Assume there are two elements $\alpha_i = a_i + b_i\rho + c_i\omega$ for $i = 1, 2$ whose norm has the same degree and suppose $\deg N(\alpha_i) = \deg a_i^3$. Let k be the quotient of the leading term of a_1 divided by the leading term of a_2. Then $\alpha_3 = \alpha_1 - k\alpha_2$ has smaller norm. A similar argument works when the degree of the norm is determined by b_i or c_i.

Theorem 6.4 (Corollary 5.2 of [1])**.** *If* $2\deg B > 3\deg A$, *and* $3 \nmid \deg FI^2$, *then every ideal class contains a unique distinguished ideal.*

All the theoretical pieces are in place to develop arithmetic in the ideal class group. Ideal inversion and multiplication pose no major theoretical obstacles, and the above establishes a unique way to find a distinguished ideal in a given class. Combining all of the pieces will allow composition and reduction in the ideal class group. The remaining sections make the above explicit for the considered function fields.

7. Triangular basis for prime ideals

Having described how the finite places split, it will be helpful to have a concrete description of generators for the prime ideals in terms of the basis elements developed in Section 4. Scheidler provided a comparable statement in Theorem 3.1 of [10] for all prime ideals in a purely cubic function field of characteristic not 3 that was an analog of the theorem of Voronoi [14] for number fields. Having classified the splitting type of prime ideals, we follow their lead and give the triangular bases along with basic products and powers of the prime ideals. This is done because a triangular basis is easier to compute with than a Dedekind basis and is in fact necessary for the reduction algorithms.

Throughout the following sections, proofs will occasionally be omitted for the sake of brevity. In particular, when a particular technique may be used successfully to compute the basis in multiple cases, it will only be included once. The interested reader may always refer to [15] for complete proofs.

7.1. **Ramified primes.** There are three cases to consider for the ramified primes. When calculating powers of primes, ramification tends to make the treatment here a little easier for a given prime. For totally ramified primes, $\mathfrak{p}^3 = (P)\mathcal{O}_\mathcal{F} = (P)[1, \rho, \omega]$ for some irreducible polynomial $P \in \mathbb{F}_q[x]$, and hence we only need to calculate the basis for $\mathfrak{p}$ and $\mathfrak{p}^2$.

Proposition 7.1. *There are three cases to consider.*

(1) If $v_P(A) \geq 1$ *and* $v_P(I) = 0$ *so that* $(P) = \mathfrak{p}^3$, *then*

$$\mathfrak{p} = [P, f + \rho, -I^{-1}f^2 + \omega] \quad \textit{and} \quad \mathfrak{p}^2 = [P, P\rho, I^{-1}f^2 - I^{-1}f\rho + \omega]$$

where $f^3 \equiv FI^2 \pmod{P}$, *and* $I^{-1}I \equiv 1 \pmod{P}$.

(2) *If* $v_P(A) > 1$ *and* $v_P(I) = 1$ *so that* $(P) = \mathfrak{p}^3$, *then*

$$\mathfrak{p} = [P, \rho, \omega] \quad \textit{and} \quad \mathfrak{p}^2 = [P, \rho, P\omega].$$

(3) *If* $v_P(A) = 1$ *and* $v_P(I) = 1$ *so that* $(P) = \mathfrak{p}\mathfrak{q}^2$, *then*

$$\mathfrak{p} = [P, \rho, E + \omega], \quad \mathfrak{q} = [P, \rho, \omega],$$

$$\mathfrak{q}^2 = [P, P\rho, E^{-1}F\rho + \omega], \ \textit{and} \ \ \mathfrak{p}\mathfrak{q} = [P, \rho, P\omega]$$

where E^{-1} *is the inverse of* E *modulo* P.

Proof. For the above results we apply Kummer's theorem to either the minimal polynomial of ρ or ω. This gives two of the three basis elements. The last element is linearly dependent upon these two and may be found using algebra. □

7.2. **Unramified primes.** In the course of doing calculations, we expect to compute almost exclusively with unramified primes. Below we deal with all the various unramified primes and their powers.

Proposition 7.2. *There are three cases to consider.*

(1) *Let* $\mathfrak{p}|P$ *have inertial degree 1 and ramification index 1, such that* $P \nmid A$. *Then*

$$\mathfrak{p} = [P, -\alpha + \rho, -I^{-1}(\alpha^2 - A) + \omega]$$

where α *is a root of the minimal polynomial of* ρ *modulo* P *and* $I^{-1}I \equiv 1 \pmod{P}$.

(2) *For* $\mathfrak{p}$ *with ramification index 1 and inertial degree 1, we have*

$$\mathfrak{p}^i = [P^i, -X_i + \rho, -Z_i + \omega]$$

where
- $Z_{i+1} = Z_i + kP^i$,
- $k \equiv C_i(EZ_i)^{-1} \pmod{P}$,
- $C_i = (Z_i^3 + EZ_i^2 + F^2I)/P^i$,
- $X_{i+1} \equiv -FIZ_{i+1}^{-1} \pmod{P}$,

and X_1 *and* Z_1 *are defined and given in Propositions 7.1 (1) and 7.2 (1).*

(3) *Let* $\mathfrak{q}$ *be a prime with inertia degree 2. Then*

$$\mathfrak{q} = [P, P\rho, I^{-1}(W + A) - I^{-1}M\rho + \omega]$$

where $\rho^3 - A\rho + FI^2 \equiv (\rho - \alpha)(\rho^2 - M\rho + W) \pmod{P}$.

Proof. For case 1, the ideal $\mathfrak{p}$ is generated by $\langle P, -\alpha + \rho\rangle$, and the rest follows.

For case 2, the definitions in this proposition make it important that Z_1 be invertible modulo P. In Proposition 7.1 (3), E is invertible modulo P. For Proposition 7.2 (1) the element Z_1 is invertible because it is a nonzero root of the minimal polynomial of ω modulo P, that is to say only ramified primes correspond to 0 being a root modulo P.

Since $P^i | N(\omega - Z_i)$, that basis element can be written as $\omega - (Z_i + kP^i)$. We now describe how to choose k so that the element is correct for $\mathfrak{p}^{i+1}$.

$$\begin{aligned} N(-(Z_i + kP^i) + \omega) &= -[(Z_i + kP^i)^3 + E(Z_i + kP^i)^2 + F^2 I] \\ &\equiv EZ_i kP^i - (Z_i^3 + EZ_i^2 + F^2 I) \pmod{P^{i+1}} \\ &\equiv EZ_i kP^i - C_i P^i \pmod{P^{i+1}} \end{aligned}$$

Since we want $C_i P^i - EZ_i kP^i \equiv 0 \pmod{P^{i+1}}$, we can choose k so that $k \equiv C_i (EZ_i)^{-1} \pmod{P}$. Such an inverse exists because P is relatively prime to both E and Z_i. Now that $-Z_{i+1} + \omega \in \mathfrak{p}^{i+1}$ we can see that $(Z_{i+1} - \omega)\rho = FI + Z_{i+1}\rho \in \mathfrak{p}^{i+1}$. This gives the term with $-X_{i+1} + \rho$ as claimed.

For case 3, Kummer's theorem gives $\mathfrak{q} = \langle P, \rho^2 - M\rho + W\rangle$, and similar techniques complete the proof. □

Notice the form of the product of two distinct unramified primes lying over a completely split prime:

$$\begin{aligned} \mathfrak{pq} &= \langle P, -\alpha_1 + \rho\rangle\langle P, -\alpha_2 + \rho\rangle \\ &= \langle P^2, P(-\alpha_1 + \rho), P(-\alpha_2 + \rho), A + \alpha_1\alpha_2 - (\alpha_1 + \alpha_2)\rho + I\omega\rangle \\ &= [P, P\rho, I^{-1}(A + \alpha_1\alpha_2) - I^{-1}(\alpha_1 + \alpha_2)\rho + \omega]. \end{aligned}$$

Here the last line is justified by the fact that $(\alpha_1 - \alpha_2)$ is relatively prime to P. Thus, the greatest common divisor of $P(\alpha_1 - \alpha_2)$ and P^2 is P. There are three types of ideals that can have the form $[P, P\rho, -N_1 - M_1\rho + \omega]$:

- $\mathfrak{q} = [P, P\rho, \omega - M\rho - W]$ from Proposition 7.2 (3),
- $\mathfrak{q}^2 = [P, P\rho, E^{-1}F\rho + \omega]$ from Proposition 7.1 (3), and
- $\mathfrak{pq} = [P, P\rho, I^{-1}(A + \alpha_1\alpha_2) - I^{-1}(\alpha_1 + \alpha_2)\rho + \omega]$ from the exposition above.

Proposition 7.3. *Let $\mathfrak{r}$ represent any of the three ideals above and $i > 1$. Then*

$$\mathfrak{r}^i = [P^i, P^i\rho, N_i - M_i\rho + \omega]$$

where

- $L(M_{i-1}M_1 I + N_{i-1} + N_1 - E) \equiv 1 \pmod{P^i}$,
- $M_i \equiv -L(F + M_{i-1}N_1 + M_1 N_{i-1}) \pmod{P^i}$, *and*
- $N_i \equiv L(M_1 FI + M_{i-1}FIM_{i-1}M_1 AN_{i-1}N_1) \pmod{P^i}$.

Proof. The previous work establishes the base case $i = 1$ and we argue by induction. Consider the product

$$\mathfrak{r}^{i-1}\mathfrak{r} = [P^{i-1}, P^{i-1}\rho, \omega - M_i\rho + N_i][P, P\rho, \omega - M_1\rho + N_1].$$

In the nine possible products of the basis elements only $(\omega - M_i\rho + N_i)(\omega - M_1\rho + N_1)$ does not contain a factor of P. Thus the coefficient of ω has to be relatively prime to P. If it were not, the product would not be primitive. Multiplying through by its inverse modulo P^i gives the desired basis element.

The product contains P^i and $P^i\rho$. A norm argument shows that $\mathfrak{r}^i$ cannot contain P^{i-1} nor $P^{i-1}\rho$. Thus the ideal has the desired norm and the elements stated form a basis. □

All that remains is to handle $\mathfrak{p}^i\mathfrak{q}^{i+j}$ where $j > 0$ and each prime has inertia degree 1. By Proposition 7.3 we know

$$(\mathfrak{p}\mathfrak{q})^i = [P^i, P^i\rho, N_i - M_i\rho + \omega] \tag{7.1}$$

and by Proposition 7.2 (2)

$$\mathfrak{q}^j = [P^j, -X_{\mathfrak{q}_j} + \rho, -Z_{\mathfrak{q}_j} + \omega], \tag{7.2}$$

$$\mathfrak{q}^{i+j} = [P^{i+j}, -X_{\mathfrak{q}_{i+j}} + \rho, -Z_{\mathfrak{q}_{i+j}} + \omega], \quad \text{and} \tag{7.3}$$

$$\mathfrak{p}^i = [P^i, -X_{\mathfrak{p}_i} + \rho, -Z_{\mathfrak{p}_i} + \omega]. \tag{7.4}$$

Combinations of the above products will help determine the proper basis of $\mathfrak{p}^i\mathfrak{q}^{i+j}$.

Proposition 7.4. *Using notation as above,*

$$\mathfrak{p}^i\mathfrak{q}^{i+j} = [P^{i+j}, P^i(-X_{\mathfrak{q}_j} + \rho), H + G\rho + \omega]$$

where we let N be defined by $NX_{\mathfrak{p}_i} \equiv 1 \pmod{P^{i+j}}$ and

$$G \equiv NZ_{\mathfrak{q}_{i+j}} \pmod{P^i} \quad \text{and} \quad H \equiv N(-FI - X_{\mathfrak{p}_i}Z_{\mathfrak{q}_{i+j}}) \pmod{P^{i+j}}.$$

Proof. Considering the product of (7.1) and (7.2), we see that P^{i+j} and $P^i(-X_{\mathfrak{q}_j} + \rho)$ are in $\mathfrak{p}^i\mathfrak{q}^{i+j}$. By considering the product of (7.3) and (7.4), we can see that

$$(-X_{\mathfrak{p}_i} + \rho)(-Z_{\mathfrak{q}_{i+j}} + \omega) \in \mathfrak{p}^i\mathfrak{q}^{i+j}.$$

Since $X_{\mathfrak{p}_i}$ is relatively prime to P it is invertible modulo P^{i+j}. Multiplying through by its modular inverse gives the third element of the basis. The other two elements are in the ideal by construction. It remains to establish that they are indeed basis elements, which is easily accomplished by a norm argument. □

We have dealt with all of the prime ideals and their possible powers and products. We now turn to arbitrary ideal arithmetic. Any given ideal J can be factored into the product of four ideals whose prime decomposition falls into one of four categories. In particular, define four ideals J_1, J_2, J_3 and J_4 to be a factorization of J such that for each $\mathfrak{p}|P$, we have

- $\mathfrak{p}$ divides J_1 if and only if P is unramified,
- $\mathfrak{p}$ divides J_2 if and only if P is totally ramified and does not divide the index,
- $\mathfrak{p}$ divides J_3 if and only if P is totally ramified and divides the index, and
- $\mathfrak{p}$ divides J_4 if and only if P is split ramified.

We call these ideals (and their corresponding primes) Type I, Type II, Type III and Type IV, respectively. The bases of these four ideals have the form:

$$\begin{aligned} J_1 &= [s_1, s_1'(u_1+\rho), v_1 + w_1\rho + \omega], \\ J_2 &= [s_2, s_2'(u_2+\rho), v_2 + w_2\rho + \omega], \\ J_3 &= [s_3, \rho, s_3''\omega], \text{ and} \\ J_4 &= [s_4, s_4'(u_4+\rho), s_4''(v_4 + w_4\rho + \omega)]. \end{aligned}$$

The particular shape of each basis can be derived from the previous propositions which describe the powers of individual primes and then applying Theorem 4.4 of [10].

Recombining ideals factored in this way is a straightforward application of the Chinese Remainder Theorem, while finding the factorization for a given ideal is an application of polynomial factorization. There are a few reasons for this approach. The first is for simplicity as deriving the results in the following propositions is far easier for ideals of a given type. The second reason is that the difficulty often lies in a particular case and this allows the exposition to highlight the trouble.

Furthermore, from a computational perspective, we are also drawn to this approach. Two of the four cases involve curves that have singularities, and hence we can choose to avoid them. We could also easily choose a curve with no finite ramification and ignore three of the four cases. Even in the worst case scenario where all types of primes are possible, we still do not expect to deal with three of the four products in the course of doing arithmetic. A rough heuristic argument shows that probability of two randomly chosen ideals with degree less than g contain a ramified prime is $4g/q$, which will be small if q is large.

8. Inversion and Division

Some basic properties of the structure of ideals in cubic function fields developed in [10] remain true even in characteristic three. We cite without proof the containment criterion for ideals written with a triangular basis.

Proposition 8.1 (Lemma 4.1 of [10]). *Let $I_i = [s_i, s_i'(u_i+\rho), s_i''(v_i+w_i\rho+\omega)]$ for $i = 1, 2$ be two ideals. Then $I_1 \subseteq I_2$ if and only if*

$$s_2 | s_1, \quad s_2' | s_1', \quad s_2'' | s_1'', \quad s_1'u_1 \equiv s_1'u_2 \pmod{s_2},$$

$$s_1''w_1 \equiv s_1''w_2 \pmod{s_2'}, \quad \text{and} \quad s_1''v_1 \equiv s_1''(v_2 + u_2(w_1 - w_2)) \pmod{s_2}.$$

Our first goal is to develop ideal inversion. As we only wish to work with integral ideals, we compute a primitive ideal that is in the ideal class of the inverse of a given ideal. As a reminder, the notation for such an inverse will be $\overline{J}$ and the notation for division will be J^{-1}.

Proposition 8.2 (Inversion)**.** *Let $I_1 = [s, s'(u+\rho), s''(v+w\rho+\omega)]$ be a primitive ideal of Type I , II, III or IV. Then $I_2 = \overline{I_1} = \langle s \rangle I_1^{-1}$ is given as follows.*

(1) **(Type I and II ideals)** *Then $s'' = 1$ and $I_2 = [S, S'(U+\rho), V + W\rho + \omega]$, where*

$$S = s, \quad S' = s/s', \quad U \equiv -Iw \pmod{s'},$$
$$W \equiv -uI^{-1} \pmod{s/s'}, \quad \text{and} \quad V \equiv E - v - WIw \pmod{s}.$$

(2) **(Type III ideals)** *Then $s' = 1$, $u = v = w = 0$, and $I_2 = [s, \rho, (s/s'')\omega]$.*

(3) **(Type IV ideals)** *Then $I_2 = [S, S'(U+\rho), S''(V+W\rho+\omega)]$, where*

$$S = s, \quad S' = \frac{s}{s's''s_I}, \quad S'' = s_I = \gcd\left(\frac{s}{s's''}, v\right),$$

$$U \equiv \begin{cases} 0 & \pmod{s''s_I} \\ -Iw & \pmod{s'} \end{cases}, \qquad V \equiv \begin{cases} 0 & \pmod{s''} \\ 0 & \pmod{s/(s's''s_I)} \\ E & \pmod{s'} \end{cases},$$

$$W \equiv E^{-1}F \pmod{s/(s's''s_I)},$$

and s'', $s/(s's''s_I)$, and s' are pairwise coprime.

Proof. For the first case, since $s \in I_1$, it is clear that $\langle s \rangle I_1^{-1}$ is an integral ideal. We show that the above choices provide a correct $\mathbb{F}_q[x]$ basis for I_2. The fact that $I_1 I_2 = \langle s \rangle$ will be used extensively in this proof. Since $s \in I_2$, $S|s$. Examining $S(v + w\rho + \omega) \in \langle s \rangle$, we conclude $s|S$ and hence $s = S$. Consider the norm of the ideal $\langle s \rangle$ to determine S':

$$s^3 = N(\langle s \rangle) = N(I_1)N(I_2) = ss'sS'.$$

Therefore $S' = s/s'$ as claimed. We now turn to $S'(U+\rho)(v+w\rho+\omega)$ and examine the coefficient of ω:

$$S'(U+\rho)(v+w\rho+\omega) \in \langle s \rangle \Rightarrow s \,\Big|\, \frac{s}{s'}(U+Iw) \Rightarrow U \equiv -Iw \pmod{s'}.$$

The congruence for W (resp. V) follows by considering the coefficient of ω in the product $s'(u+\rho)(V+W\rho+\omega)$ (resp. $(V+W\rho+\omega)(v+w\rho+\omega)$) and arguing as above.

The argument for Type III ideals follows immediately from Proposition 7.1 (2). For the Type IV ideals, we factor I_1 as

$$I_1 = [s'', \rho, s''\omega][s', s'\rho, w\rho + \omega] \left[\frac{s}{s's''}, u + \rho, v + w\rho + \omega\right]$$

and proceed to find the inverse of each factor. The inverse of the first two factors is an immediate consequence of Proposition 7.1 (3). The inverse of the last ideal in the above factorization has two factors since it could contain either ramified primes or powers of unramified primes, which is determined by the term associated with ω and s_I. For the ramified primes in this product, the inverse is $[s_I, \rho, s_I\omega]$ and hencee $V \equiv 0 \pmod{s_I}$. The remaining factor of the inverse has the form

$$\left[\frac{s}{s's''s_I}, \frac{s}{s's''s_I}\rho, E^{-1}F\rho + \omega\right],$$

yielding the only congruence for W and the remaining congruence for V. The above immediately shows that the choices for S', and S'' are correct. A quick norm argument shows that $S = s$ as claimed. □

We note that the Proposition 8.2 (1) is simpler for nonsingular curves because $I = 1$ and most of the congruences can be replaced by equalities. Furthermore, the later two cases in the proposition do not occur if $I = 1$.

The remaining portion of this section leads to arbitrary ideal division. We begin with a series of lemmata that will handle the simplest case of division, and will later be used to handle the general case.

Lemma 8.3 (Simple Division)**.** *Let I_1 and I_2 be two ideals such that $I_2 \subseteq I_1$ and I_2 is of type I, II, III, or IV. Then $J = I_2 I_1^{-1}$ is given as follows.*

(1) **(Type I and II ideals)** *Then $I_2 = [s, s\rho, v_2 + w_2\rho + \omega]$ and $I_1 = [s, u_1 + \rho, v_1 + \omega]$, and $J = [s, U + \rho, V + \omega]$, where*

$$U \equiv Iw_2 - u_1 \pmod{s}, \quad V \equiv v_2 - Iw_2^2 + u_1w_2 \pmod{s}.$$

(2) **(Type III ideals)** *Then $I_2 = [s, \rho, s\omega]$ and $I_1 = [s, \rho, \omega]$, and $J = [s, \rho, \omega]$.*

(3) **(Type IV ideals)** *Then $I_2 = [s's'', s'\rho, s''(v_2 + w_2\rho + \omega)]$ and $I_1 = [s's'', \rho, v_1 + \omega]$, and $J = [s's'', \rho, V + \omega]$, where*

$$V \equiv E \pmod{d}, \quad V \equiv 0 \pmod{s's''/d}, \quad \text{and} \quad d = \gcd(s'', v_1).$$

Proof. By Proposition 8.2 (1), $I_2 = \langle s \rangle [s, Iw_2 + \rho, E - v_2 + \omega]^{-1}$ for the first case. Therefore we can write

$$J[s, u_1 + \rho, v_1 + \omega][s, Iw_2 + \rho, u_2 w_2 - v_2 + \omega] = \langle s \rangle.$$

Since $J = [s, \rho + U, \omega + V]$, it is only a matter of finding the correct congruences for V and U. Using $(U+\rho)(u_1+\rho)(Iw_2+\rho) \in \langle s \rangle$ and the coefficient of ω, we find $U \equiv Iw_2 - u_1 \pmod{s}$. To find V, we note that $v_2 + w_2\rho + \omega \in J$ and subtract $w_2(U + \rho)$.

The second case follows immediately from Proposition 7.1 (2). Finally, for the last case, by Proposition 7.1 (3), $J = [s's'', \rho, V + \omega]$ for some V. For a given prime P, I_2 contains either $\mathfrak{pq}$ or $\mathfrak{q}^2$ and no higher powers, and the ideal I_1 contains either $\mathfrak{p}$ or $\mathfrak{q}$. The quantity d corresponds to the ramified primes in I_1. For these primes the unramified conjugate is the inverse, and hence justifies the choice for V modulo d. □

Rather than proceed straight to the division propositions, we illustrate the method behind the division in Figure 1. The hardest part of division is tracking the various products lying over completely split primes. The figure illustrates the order of operations (as described in the proof) used to complete ideal division. For $\mathfrak{p}$ and $\mathfrak{q}$ lying over a completely split prime P we will walk through the division process in the case that the dividend is $\mathfrak{p}^8\mathfrak{q}^6$ and the divisor is $\mathfrak{p}^5\mathfrak{q}$.

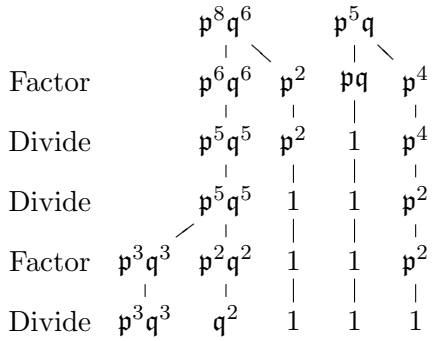

FIGURE 1. Division of $\mathfrak{p}^8\mathfrak{q}^6$ by $\mathfrak{p}^5\mathfrak{q}$

The tree for the dividend ends with three branches. It should be noted that the last two nodes on the left tree are relatively prime; more specifically, at least one of them is one. This will be key for the next proof because it relies on the product of the those two nodes being relatively prime.

Proposition 8.4 (Division)**.** *Let* $I_i = [s_i, s_i'(u_i + \rho), s''(v_i + w_i\rho + \omega)]$ *for* $i = 1, 2$ *be such that* $I_2 \subseteq I_1$ *and they are of the same type. Then* $J = I_2 I_1^{-1} = [S, S'(U + \rho), S''(V + W\rho + \omega)]$*, where these values are given in the table below.*

	Type I & II	*Type III*	*Type IV*
S	$\dfrac{s_2}{s_1 d_1}$	$\dfrac{s_2}{s_1'' d_1}$	$\dfrac{s_2}{s_1' s_1'' d_2}$
S'	$\dfrac{s_2' d_1}{s_1}$	1	$\gcd\left(\frac{d_2 s_2' s_2''}{s_1}, \frac{s_2'}{s_1'}\right)$
U	$Iw_2 - u_1 \pmod{\frac{s_1}{(s_1' d)}}$ $u_2 \pmod{\frac{s_2}{(s_2' d)}}$	0	$0 \pmod{\frac{s_1}{s_1' s_1'' d_2}}$ $u_2 \pmod{\frac{s_2}{s_2' s_2'' d_2}}$
S''	1	$\dfrac{s_2'' d_1}{s_1}$	$\gcd\left(\frac{d_2 s_2' s_2''}{s_1}, \frac{s_2''}{s_1''}\right)$
$S''W$	$w_2 \pmod{S'}$	0	$s_2'' w_2 \pmod{S'}$
$S''V \pmod{S}$	$(W - w_2)U + v_2$	0	$s_2''((W - w_2)U + v_2)$

The terms d_1 and d_2 are defined by

$$d_1 = \gcd\left(\frac{s_2}{s_2'}, \frac{s_1}{s_1'}, u_1 - u_2\right)$$

and

$$d_2 = \gcd\left(\frac{s_2}{s_2' s_2''}, \frac{s_1}{s_1' s_1''}, v_1 - w_1 u_1 - v_2 + w_2 u_2\right).$$

Proof. For Type I and II ideals, we begin by factoring both I_1 and I_2 into two different ideals,

$$I_i = I_{i,1} I_{i,2} = [s_i', s_i'\rho, v_i + w_i\rho + \omega]\left[\frac{s_i}{s_i'}, u_i + \rho, v_i - u_i w_i + \omega\right].$$

The first division is

$$I_{2,1} I_{1,1}^{-1} = \left[\frac{s_2'}{s_1'}, \frac{s_2'}{s_1'}\rho, v_2 + w_2\rho + \omega\right]. \tag{8.1}$$

All that remains of the divisor is $I_{1,2} = [s_1/s_1', u_1 + \rho, v_1 - u_1 w_1 + \omega]$. We consider the greatest common divisor of this ideal with the corresponding

ideal arising from I_2. This is the justification for d in the proposition statement. We perform the following division:

$$\left[\frac{s_2}{s_2'}, u_2+\rho, v_2-u_2w_2+\omega\right][d, u_1+\rho, v_1-u_1w_1+\omega]^{-1} = \left[\frac{s_2}{s_2'd}, u_2+\rho, v_2-u_2w_2+\omega\right],$$

which justifies one of the two congruences for U. We factor out of the ideal in (8.1) the part that matches the remaining divisor. That is,

$$\left[\frac{s_2'}{s_1'}, \frac{s_2'}{s_1'}\rho, v_2+w_2\rho+\omega\right] = \left[\frac{s_2'd}{s_1}, \frac{s_2'd}{s_1}\rho, v_2+w_2\rho+\omega\right]\left[\frac{s_1}{s_1'd}, \frac{s_1}{s_1'd}\rho, v_2+w_2\rho+\omega\right]. \tag{8.2}$$

We then apply Lemma 8.3 (1) to the right hand ideal of (8.2) and the remainder of the divisor to get

$$\left[\frac{s_1}{s_1'd}, \frac{s_1}{s_1'd}\rho, v_2+w_2\rho+\omega\right]\left[\frac{s_1}{s_1'd}, u_1+\rho, v_1-w_1u_1+\omega\right]^{-1} = \left[\frac{s_1}{s_1'd}, Iw_2-u_1+\rho, v_2-Iw_2^2+u_1w_2+\omega\right].$$

This ideal gives the other congruence for U and the division is complete at this step. The choice for S is justified by looking at the first term in the three ideals that remain; likewise S' is the product of the coefficients of ρ:

$$S = \left(\frac{s_1}{s_1'd}\right)\left(\frac{s_2'd}{s_1}\right)\left(\frac{s_2}{s_2'd}\right) = \frac{s_2}{s_1'd} \quad \text{and} \quad S' = \frac{s_2'd}{s_1}.$$

Since $v_2+w_2\rho+\omega \in J$, it just remains to modify this element so that it is canonical. This justifies the choice for V and W.

For Type III ideals, this follows by using the same arguments presented in the proof of Proposition 8.4. The key distinction is how the ideals are factored:

$$I_i = [s_i'', \rho, s_i''\omega]\left[\frac{s_i}{s_i''}, \rho, \omega\right].$$

The rest of the arguments are simplified given that these are products of totally ramified primes.

Finally, for Type IV ideals, we begin by factoring both I_1 and I_2 into the ideals $I_{i,1}$ and $I_{i,2}$ as above. The first division is

$$I_{2,1}I_{1,1}^{-1} = \left[\frac{s_2's_2''}{s_1's_1''}, \frac{s_2'}{s_1'}\rho, \frac{s_2''}{s_1''}(v_2 + w_2\rho + \omega)\right]. \tag{8.3}$$

Proceeding as above, the next division yields

$$\left[\frac{s_2}{s_2's_2''d}, u_2 + \rho, v_2 - u_2w_2 + \omega\right],$$

which justifies the latter congruence for U. We decompose the ideal on the right in (8.3) to get a factor that matches the remaining divisor:

$$\left[\frac{s_2's_2''d}{s_1}, S'\rho, S''(v_2 + w_2\rho + \omega)\right]\left[\frac{s_1}{s_1's_1''d}, s_3'\rho, s_3''(v_2 + w_2\rho + \omega)\right], \tag{8.4}$$

where

$$s_3' = \gcd\left(\frac{s_1}{s_1's_1''d}, \frac{s_2'}{s_1'}\right) \text{ and } s_3'' = \gcd\left(\frac{s_1}{s_1's_1''d}, \frac{s_2''}{s_1''}\right).$$

Note that $S'S'' = s_2's_2''d/s_1$ and $s_3's_3'' = s_1/(s_1's_1''d)$. Apply Lemma 8.3 (3) to the right most ideal of (8.4) and the remainder of the divisor to get

$$\left[\frac{s_1}{s_1's_1''d}, s_3'\rho, s_3''(v_2 + w_2\rho + \omega)\right]\left[\frac{s_1}{s_1's_1''d}, u_1 + \rho, v_1 - w_1u_1 + \omega\right]^{-1} = \left[\frac{s_1}{s_1's_1''d}, \rho, v_3 + \omega\right],$$

where v_3 is given in Lemma 8.2 (3). This ideal gives the other congruence for U and the division is complete at this step. The choice for S is justified by looking at the first term in the three ideals that remain:

$$S = \left(\frac{s_1}{s_1's_1''d}\right)\left(\frac{s_2's_2''d}{s_1}\right)\left(\frac{s_2}{s_2's_2''d}\right) = \frac{s_2}{s_1's_1''d}.$$

The choices for S' and S'' are justified in (8.4). Since $s_2''(v_2+w_2\rho+\omega) \in J$, it just remains to modify this element so that it is canonical and this justifies the choice for V and W. The argument here is the same as above except we have to account for the coefficient of ω. □

We close this section with a proposition on dividing a nonprimitive ideal by a primitive ideal. Consider an ideal of the form $\langle d\rangle I_2$, where I_2 is primitive, and a primitive ideal I_1. To compute $\langle d\rangle I_2 I_1^{-1}$, we begin by removing as much of I_1 from $\langle d\rangle$ as is possible. The remaining factor of I_1 is then removed from I_2. The primitive parts of the two divisions are I_d and I_m, and their product is not necessarily primitive. While this might seem problematic, the propositions on multiplication can be used calculate the product.

Proposition 8.5 (Nonprimitive Division)**.** *Let* $I_2 = [s_2, s_2'(u_2+\rho), s_2''(v_2 + w_2\rho+\omega)]$, $I_1 = [s_1, s_1'(u_1+\rho), s_1''(v_1+w_1\rho+\omega)]$ *and* $d \in \mathbb{F}_q[x]$ *be such that* $dI_2 \subseteq I_1$. *Then* $J = dI_2I_1^{-1} = (D)I_dI_m$ *where*

$$I_d = I_2\left[\frac{s_1}{D_1D_2D_3}, \frac{s_1'}{D_1}(u_1+\rho), D_2(v_1+w_1\rho+\omega)\right]^{-1}$$

is calculated by Proposition 8.4 or 8.2 (1),

$$I_m = \overline{[D_1D_2D_3, D_1(u_1+\rho), D_2(v_1+w_1\rho+\omega)]}$$

and the quantities involved are defined as follows.

$$D_1 = \gcd(s_1', d), \quad D_2 = \gcd(s_1'', d),$$

$$D_3 = \gcd\left(\frac{s_1}{s_1's_1''}, \frac{d}{D_1D_2}\right), \text{ and } D = \frac{d}{D_1D_2D_3}.$$

Proof. We note that in ideals of type I (or II), $s_1'' = s_2'' = 1$, and hence $D_2 = 1$. Furthermore $\overline{I_m} \subseteq \langle d\rangle$ and $\overline{I_m}[s_1/D_1D_3, s_1'/D_1(u_1+\rho), v_1+w_1\rho+\omega] = I_1$. Therefore $\langle d\rangle\overline{I_m}^{-1} = I_m$. After this division, the factors that remain in I_1 are $[s_1/D_1D_3, s_1'/D_1(u_1+\rho), v_1+w_1\rho+\omega]$ and this is contained in I_2. The remaining ideal types may be proved similarly. □

9. Ideal Multiplication

Theoretically, ideal multiplication is the easiest operation that will be discussed since it may be achieved by performing brute force linear algebra. The goal of these propositions is to eliminate much of the excess work that would be required to reduce the nine cross products arising in the multiplication of two ideals down to a basis. The extreme amount of redundancy is obvious for certain products. For example, the product of two relatively prime ideals may be computed quickly using the Chinese Remainder Theorem. Computationally, relatively prime operands are to be expected and the product may be calculated as Scheidler did in Theorem 4.4 of [10].

In contrast to cubic function fields of unit rank one, we can not assume that the two operands will be relatively prime. Thus, we will be forced to develop ideal multiplication systematically. The first proposition assumes that the product of the two ideals is primitive and this will be used to aid in the case where the product is not assumed to be primitive. We have bundled all four products into one proposition for easier referencing, although it makes for a somewhat cumbersome presentation.

Proposition 9.1. *Let* $I_i = [s_i, s_i'(u_1+\rho), s_i''(v_i+w_i\rho+\omega)]$ *for* $i = 1, 2$ *be such that* $I_1I_2 = I_3$ *is a primitive ideal, and* I_1 *and* I_2 *are ideals of the same type. Then* $I_3 = [S, S'(U+\rho), S''(V+W\rho+\omega)]$, *where these values are in the table below.*

	Type I	*Type II*	*Type III*	*Type IV*
S	$\frac{s_1 s_2 d'}{d}$	$\frac{s_1 s_2}{d}$	$\frac{s_1 s_2}{d}$	$\frac{s_1 s_2}{dd'}$
S'	$\frac{s_1' s_2' d}{d'}$	$s_1' s_2' d$	1	$s_1' s_2' d$
U	$u_3 + k\frac{s_1 s_2 d'}{s_1' s_2' d^2}$	f	0	$u_3 s_2'' s_2'' d'$
S''	1	1	$s_1'' s_2'' d$	$s_1'' s_2'' d'_{IV}$
W	$w_I - qS'$	$f^2 I^{-1}$	0	$w_{IV} - qS'$
V	$v_I - qS'U$	fI^{-1}	0	$v_{IV} - qS'U$

The values for d and d' are given by

	$TypeI, II, III$	$TypeIV$
d	$\gcd\left(\frac{s_1}{s_1' s_2''}, \frac{s_2}{s_2' s_2''}\right)$	$\gcd(s_{\mathfrak{q}1}, s_{\mathfrak{q}2})$
d'	$\gcd(d, u_1 - u_2)$	$\gcd\left(s_{\mathfrak{q}2}, \frac{s_1}{s_1' s_1'' s_{\mathfrak{q}1}}\right) \cdot \gcd\left(s_{\mathfrak{q}1}, \frac{s_2}{s_2' s_2'' s_{\mathfrak{q}2}}\right)$

where

$$s_{\mathfrak{q}i} = \gcd\left(\frac{s_i}{s_i' s_i''}, v_i - w_i u_i\right) \text{ for } i = 1, 2.$$

For Type I and Type IV ideals, we define u_3 by the following congruences,

$$u_3 \equiv u_1 \begin{cases} \left(\mod \frac{s_1 d_1}{s_1' s d}\right) & \text{for Type I,} \\ \left(\mod \frac{s_1}{s_1' s_1'' dd'}\right) & \text{for Type IV,} \end{cases}$$

$$u_3 \equiv u_2 \begin{cases} \left(\mod \frac{s_2 d_1}{s_2' d}\right) & \text{for Type I,} \\ \left(\mod \frac{s_2}{s_2' s_2'' dd'}\right) & \text{for Type IV.} \end{cases}$$

For Type I ideals, k is chosen such that

$$d' \left| \frac{(u_3^3 - u_3 A - FI^2)S'd'}{S} + kA, \right.$$

and for Type II ideals, we define f to satisfy the congruence

$$f^3 \equiv FI^2 \pmod{S}.$$

Finally, defining a_i for $i = 1, \ldots, 6$ to be polynomials calculated using the Extended Euclidean Algorithm that satisfy

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

w_3 and v_3 are defined by the relations

$$\begin{aligned} S'' w_3 = {} & a_1 s_2 s_1'' w_1 + a_2 s_1 s_2'' w_2 + a_3 s_1' s_2'(u_1 + u_2) + a_4 s_1' s_2''(v_2 + u_1 w_2) \\ & + a_5 s_2' s_1''(v_1 + u_2 w_1) + a_6 s_1'' s_2''(v_1 w_2 + v_2 w_1 - F), \end{aligned}$$

and

$$\begin{aligned} S'' v_3 = {} & a_1 s_2 s_1'' v_1 + a_2 s_1 s_2'' v_2 + a_3 s_1' s_2'(u_1 u_2 + A) + \\ & a_4 s_1' s_2''(u_1 v_2 - FI + w_2) + a_5 s_2' s_1''(u_2 v_1 - FI + w_1 A) + \\ & a_6 s_1'' s_2''(v_1 v_2 + w_1 w_2 - w_1 FI - W_2 FI). \end{aligned}$$

The value of q is simply chosen to minimize the degree of V and W, and the values of U and V are unique only modulo S/S' and S/S'', respectively.

Proof. Since we assume I_3 is primitive, it has a canonical basis of the form claimed. For Type II and III ideals, the proof follows directly from Proposition 7.1 (1) and 7.1 (2). The proof for Type I and Type IV is considerably more involved.

For Type I ideals, we begin by factoring I_1 and I_2 and deal with their product using smaller and simpler ideals. The easiest part of the product is

$$[s_1', s_1'\rho, v_1 + w_1\rho + \omega][s_2', s_2'\rho, v_2 + w_2\rho + \omega] = [s_1' s_2', s_1' s_2'\rho, V + W\rho + \omega].$$

While we still need to find congruences for V and W, we will return to those later and focus on the difficult part of the product:

$$\left[\frac{s_1}{s_1'}, u_1 + \rho, v_1 - w_1 u_1 + \omega\right] \left[\frac{s_2}{s_2'}, u_2 + \rho, v_2 - w_2 u_2 + \omega\right]. \tag{9.1}$$

The quantity d signifies common possible prime factors in this product, and d' indicates those primes that appear as squares in the product. Thus, we can rewrite the above product as

$$\left[\frac{S}{S'}, U + \rho, V + \omega\right] \left[\frac{d}{d_1}, \frac{d}{d'}\rho, V + W\rho + \omega\right].$$

We conclude from this that $S' = s_1' s_2' d/d'$ and by equating norms that $S = s_1 s_2 d/d'$. Combining the two previous statements we see that

$$\left[\frac{S}{S'}, U+\rho, V+\omega\right] = \left[\frac{s_1 d'}{s_1' d}, u_1+\rho, v_1 - w_1 u_1 + \omega\right]\left[\frac{s_2 d'}{s_2' d}, u_2+\rho, v_2 - w_2 u_2 + \omega\right].$$

This justifies the choice for u_3, which is only defined uniquely modulo the least common multiple of $s_1 d'/s_1' d$ and $s_2 d'/s_2' d$. Thus we can write $U = u_3 + kS/(S'd')$ and consider

$$\frac{S}{S'} \,\Big|\, N(U+\rho) \Rightarrow \frac{S}{S'} \,\Big|\, (u_3^3 - u_3 A - FI^2) + kA\frac{S}{S'd'}.$$

From the definition of u_3, $S/S'd'$ divides $u_3^3 - u_3 A - FI^2$ so we can conclude

$$d' \,\Big|\, \frac{(u_3^3 - u_3 A - FI^2)S'd'}{S} + kA$$

gives the proper choice for k. This determines U modulo S/S' as needed. To calculate V and W, we find any element of the form $v_3 + w_3\rho + \omega \in I_3$. Since I_3 is primitive and contains no index divisors, the greatest common divisor of the coefficients of ω arising from all possible products of basis elements of I_1 and I_2 must be 1. By using the previously calculated elements, this last element is modified to construct the canonical basis.

Much of the argument is similar for Type IV ideals. We will try and note only the key distinctions. This time we factor I_i into three factors as

$$\begin{aligned} I_i &= J_{i,1}J_{i,2}J_{i,3} \\ &= \left[\frac{s_i}{s_i' s_i''}, u_i+\rho, v_i - w_i u_i + \rho\right][s_i'', \rho, s_i''\omega][s_i', s_i'\rho, v_i + w_i\rho + \omega]. \end{aligned}$$

Since I_3 is primitive, all three of $\gcd(s_2'', s_1''), \gcd(s_2', s_1'')$, and $\gcd(s_2'', s_1')$ are one. This simplifies the number of possible products to consider. We factor $J_{i,1}$ further to distinguish ramified primes (denoted with a subscript $\mathfrak{q}$) from the unramified primes:

$$J_{i,1} = [s_{\mathfrak{q}i}, \rho, \omega]\left[\frac{s_i}{s_i' s_i'' s_{\mathfrak{q}i}}, u_i+\rho, v_i - w_i u_i + \omega\right].$$

Now there are three possible type of products these two ideals can form. Products corresponding to a common place of $\mathbb{F}_q(x)$ lying below $\mathfrak{p}$ and $\mathfrak{q}$ indicate the presence of that polynomial being a factor of the coefficent of ω. This justifies the choice of d'. There are at most single powers of $\mathfrak{q}$ in either of the two ideals that correspond to that part of the factorization. Their greatest common divisor justifies the choice of d. We remove these factors from their corresponding ideals in $J_{i,1}$ and choose u_3 from these two divisors of $J_{i,1}$. This gives u_3 unique modulo $S/(S'S'')$. Since S'' divides U this justifies the choice of U. Lastly, we construct V and W in the same manner as above. However, the fact that these ideals correspond to index

divisors means that the greatest common divisor of the terms with ω will no longer be 1 but S''. □

It is important to note the calculation of W and V is not as difficult as it looks. If s_1 and s_2 are relatively prime, the above proposition is superfluous and the multiplication can be done via the Chinese Remainder Theorem. Assuming s_1 and s_2 are not relatively prime, we still expect that we will be able to write S'' as a linear combination of fewer than all six terms.

Now we deal with the case that the product of two ideals is not primitive. The key to these propositions is finding and removing the nonprimitive factors. The remaining product is primitive and the previous propositions may then be invoked.

Proposition 9.2 (Multiplication)**.** *For $i = 1, 2$ let $I_i = [s_i, s_i'(u_1+\rho), s_i''(v_i+w_i\rho+\omega)]$ be two ideals of the same type (I through IV). Then $I_1 I_2 = (D)I_3$ where $I_3 = I_1' I_2' J$ with*

$$I_1' = \left[\frac{s_1}{D_1}, \frac{s_1'}{D_1'}(u_1+\rho), \frac{s_1''}{D_1''}(v_1+w_1\rho+\omega)\right],$$

$$I_2' = \left[\frac{s_2}{D_2}, \frac{s_2'}{D_2'}(u_2+\rho), \frac{s_2''}{D_2''}(v_2+w_2\rho+\omega)\right]$$

and these quantities are as follows:

	Type I	*Type II*	*Type III*
d_1	$\gcd\left(s_2', \frac{s_1}{s_1'}, u_1+Iw_2\right)$	$\gcd\left(s_2', \frac{s_1}{s_1'}\right)$	$\gcd\left(s_2'', \frac{s_1}{s_1''}\right)$
d_2	$\gcd\left(s_1', \frac{s_2}{s_2'}, u_2+Iw_1\right)$	$\gcd\left(s_1', \frac{s_2}{s_2'}\right)$	$\gcd\left(s_1'', \frac{s_2}{s_2''}\right)$
d_3	$\frac{\gcd\left(\frac{s_1'}{d_2}, \frac{s_2'}{d_1}\right)}{\gcd\left(\frac{s_1'}{d_2}, \frac{s_2'}{d_1}, w_1-w_2\right)}$	$\gcd(s_2', s_1')$	$\gcd(s_2'', s_1'')$

For Type IV ideals, the values for the d_i are given as

$$d_1 = \gcd\left(s_2'', \frac{s_1}{s_1's_1''}, v_1-u_1w_1\right), \quad d_2 = \gcd\left(s_1'', \frac{s_2}{s_2's_2''}, v_2-w_2u_2\right),$$

$$d_3 = \frac{\gcd\left(\frac{s_1}{s_1's_1''}, s_2''\right)}{\gcd\left(\frac{s_1}{s_1's_1''}, s_2'', v_1-w_1u_1\right)}, \quad d_4 = \frac{\gcd\left(\frac{s_2}{s_2's_2''}, s_1''\right)}{\gcd\left(\frac{s_2}{s_2's_2''}, s_1'', v_2-w_2u_2\right)},$$

$$d_5 = \gcd\left(\frac{s_1'}{d_4}, \frac{s_2''}{d_1}\right), \quad d_6 = \gcd\left(\frac{s_2'}{d_3}, \frac{s_1''}{d_2}\right), \quad d_7 = \gcd\left(\frac{s_2''}{d_1 d_5}, \frac{s_1''}{d_2 d_6}\right).$$

The D_i are given in the table below.

	Type I & II	*Type III*	*Type IV*
D_1	$d_1 d_2 d_3$	$d_1 d_2 d_3$	$d_2 d_4 d_5 d_6 d_7$
D_2	$d_1 d_2 d_3$	$d_1 d_2 d_3$	$d_1 d_3 d_5 d_6 d_7$
D_1'	$d_2 d_3$	1	$d_4 d_5$
D_2'	$d_1 d_3$	1	$d_3 d_6$
D_1''	1	$d_2 d_3$	$d_2 d_6 d_7$
D_2''	1	$d_1 d_3$	$d_1 d_5 d_7$

Finally, the ideal J is defined by the ideal type as follows

Type I
$\langle d_3 \rangle \left(\overline{[d_3, d_3\rho, v_1 + w_1\rho + \omega]}\ \overline{[d_3, d_3\rho, v_2 + w_2\rho + \omega]} \right)^{-1}$

Type II	*Type III*	*Type IV*
$[D_3, f + \rho, I^{-1}f^2 + \omega]$	$[D_3, \rho, \omega]$	$[d_5 d_6, \rho, \omega][d_7, \rho, \omega + E]$

Proof. For type I ideals, recall that $s_1'' = s_2'' = 1$. We factor I_1 and I_2 as in Proposition 8.4,

$$I_i = I_{i,1} I_{i,2} = [s_i', s_i'\rho, v_i + w_i\rho + \omega] \left[\frac{s_i}{s_i'}, u_i + \rho, v_i + w_i\rho + \omega\right]$$

Of these four factors the non-primitive part of the product does not arise from $I_{1,2}I_{2,2}$. We find the non-primitive part from the product $I_{1,2}I_{2,1}$ (resp. $I_{2,2}I_{1,1}$). It suffices to consider the coefficient of ω. Hence $D_1 = \gcd(s_2', s_1/s_1', u_1 + Iw_2)$ (resp. $D_2 = \gcd(s_1', s_2/s_2', u_2 + Iw_1)$). We remove D_1 (resp. D_2) from $I_{1,1}$ and $I_{2,2}$ (resp. $I_{2,1}$ and $I_{1,2}$) and rename as follows:

$$I_{1,2}' = \left[\frac{s_1}{s_1' D_1}, u_1 + \rho, v_1 + w_1\rho + \omega\right], \quad I_{1,2}' = \left[\frac{s_1'}{D_2}, \frac{s_1'}{D_2}\rho, v_1 + w_1\rho + \omega\right],$$
$$I_{2,2}' = \left[\frac{s_2}{s_2' D_2}, u_2 + \rho, v_2 + w_2\rho + \omega\right], \quad I_{2,1}' = \left[\frac{s_2'}{D_1}, \frac{s_2'}{D_1}\rho, v_2 + w_2\rho + \omega\right].$$

The product $I_1 I_2$ now has the form $(D_1 D_2) I'_{1,1} I'_{1,2} I'_{2,1} I'_{2,2,}$ and any remaining nonprimitive factor comes from $I'_{1,1} I'_{2,1}$. Let

$$I_{1,3} = [D_3, D_3\rho, v_1 + w_1\rho + \omega] \text{ and } I_{2,3} = [D_3, D_3\rho, v_2 + w_2\rho + \omega],$$

where D_3 is defined above. The choice of D_3 is justified because $\gcd(s'_1/D_2, s'_2/D_1)$ is the possible primes that could be part of the nonprimitive product. However, the previous greatest common divisor contains too many primes. For a given prime P we need to be able to distinguish between $\mathfrak{pq}$ and $\mathfrak{p}^2$. If $w_1 - w_2 = 0$ then the associated primes correspond to a square and that justifies the choice for the denominator in D_3. We justify the claim for the ideal J by noting the following equalities.

$$\begin{aligned} I_{1,3} I_{2,3} &= I_{1,3} I_{2,3} \overline{I_{1,3}}\ \overline{I_{2,3}} (\overline{I_{1,3}}\ \overline{I_{2,3}})^{-1} \\ &= \langle D_3 \rangle^2 (\overline{I_{1,3}}\ \overline{I_{2,3}})^{-1} \\ &= \langle D_3 \rangle \left(\langle D_3 \rangle / (\overline{I_{1,3}}\ \overline{I_{2,3}}) \right) \\ &= \langle D_3 \rangle J \end{aligned}$$

The last ideal is the one given in the proposition statement and it is primitive. We remove the factor $I_{1,3}$ from $I'_{1,2}$ and $I_{2,3}$ from $I'_{2,2}$ to get the other two primitive ideals. The product of these three ideals is primitive and can be calculated by Proposition 9.1.

Type II and III ideals are much easier to deal with. For the two types, appealing to the propositions that govern their powers from Section 7 will be sufficient. Again we factor the ideals and find where the nonprimitive factors arise. Unlike the previous proposition, constructing the equivalent ideal J is trivial. This is because D_3 is squarefree and Proposition 7.1 states the form of these ramified primes.

The final part of the proof proceeds analogously to the other cases. Again, we seek only to highlight the differences. We begin by factoring I_1 into three ideals as

$$\begin{aligned} I_1 &= I_{1,1} I_{1,2} I_{1,3} \\ &= \left[\frac{s_1}{s'_1 s''_1}, u_1 + \rho, v_1 - w_1 u_1 + \omega \right] [s'_1, s'_1\rho, v_1 + w_1\rho + \omega][s''_1, \rho, s''_1\omega], \end{aligned}$$

and likewise with I_2. The quantity D_1 (resp. D_2, D_3, D_4) is the nonprimitive part from $I_{1,1}I_{2,3}$ (resp. $I_{2,1}I_{1,3}$, $I_{1,1}I_{2,2}$, $I_{2,1}I_{1,2}$). We remove these factors from the ideals and consider $I_{1,2}I_{2,3}$ (resp. $I_{2,2}I_{1,3}$). Here we are considering the case in which one ideal contains squares of the ramified prime (say, $\mathfrak{q}^2$) and the other ideal contains products of a ramified prime with its corresponding unramified prime (say, $\mathfrak{pq}$). The product of $\mathfrak{q}^2\mathfrak{pq}$ is $(P)\mathfrak{q}$. Thus we get $(D_5)[D_5, \rho, \omega]$ (resp $(D_6)[D_6, \rho, \omega]$). We remove the factor D_5 (resp. D_6) from $I_{1,2}$ and $I_{2,3}$ (resp. $I_{2,2}$ and $I_{1,3}$) and consider one last product of $I_{1,3}I_{2,3}$. This is a product where each ideal has primes of the form $\mathfrak{pq}$ and therefore the product must be of the form $(P)\mathfrak{p}$. We get $(D_7)[D_7, \rho, \omega + E]$. □

We have stated the basic ideal operations necessary for arithmetic. The key now is to give a method to find a distinguished element in an ideal class. From this point forward, $\mathcal{F}/K$ will be assumed to have a totally ramified infinite place with $3 \nmid \deg FI^2$. This latter assumption is necessary since we rely on Theorem 6.1. These assumptions also ensure that the ideal class group is isomorphic to the Jacobian of the curve.

10. Elements of Minimal Norm

The content in this section closely mirrors Section 8 of [1]. We begin by embedding an ideal into a matrix and using elementary row operations to find an element of minimal norm. The correctness output of this algorithm relies on $3 \nmid deg(FI^2)$.

Algorithm 1: MinElement

Input: Minimal Element Algorithm. A curve in standard form satisfying (2.2) and $3 \nmid \deg(FI^2)$. Let $J = [s, s'(u+\rho), s''(v+w\rho+\omega)]$.

Output: $\alpha \in J$ non-zero so that $N(\alpha)$ has minimal degree.

Precomputation: Use the ideal to define $b_1 = (b_{1,1}, b_{1,2}, b_{1,2}) = (s, 0, 0)$, $b_2 = (b_{2,1}, b_{2,2}, b_{2,2}) = (s'u, s', 0)$, $b_3 = (b_{3,1}, b_{3,2}, b_{3,2}) = (s''v, s''w, s'')$. Assign weights $w_{i,1} = 3\deg b_{i,1}$, $w_{i,2} = 3\deg b_{i_2} + \deg FI^2$, and, $w_{i,3} = 3\deg b_{i,3} + \deg F^2 I$.

1: 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 and their associated values so that $w_1 \leq w_2 \leq w_3$.
2: **while** $a_1 = a_2$ or $a_2 = a_3$ or $a_1 = a_3$ **do**
3: **case I:** $a_1 = a_2$
4: $b_{2,a_2} = b_{1,a_1}c + r$
5: replace $b_2 := b_2 - cb_1$ and recalculate a_2, w_2.
6: **end case**
7: **case II:** $a_1 = a_3$
8: $b_{3,a_3} = b_{1,a_1}c + r$
9: replace $b_3 := b_3 - cb_1$ and recalculate a_3, w_3.
10: **end case**
11: **case III:** $a_2 = a_3$
12: $b_{3,a_2} = b_{2,a_2}c + r$
13: replace $b_3 := b_3 - cb_2$ and recalculate a_3, w_3.
14: **end case**
15: Reorder the b_i's and associated values.
16: **end while**
17: **Return:** $b_{1,1} + b_{1,2}\rho + b_{1,3}\omega$, the element of minimal norm.

Now that we can calculate an element of minimal norm, our goal will be to construct a canonical basis for the principal ideal generated by this element.

11. Canonical Basis

The algorithm for finding a canonical basis for a principal ideal generated by an element of $\mathcal{O}_{\mathcal{F}}$ is straightforward.

Algorithm 2: CanBasis

Input: $a + b\rho + c\omega \in \mathcal{O}_F$
Output: A canonical basis of the ideal $J = \langle \alpha \rangle$.

1: Create the matrix

$$\begin{bmatrix} a & b & c \\ bA - cFI & a & bI \\ -bFI & -cF & a - cE \end{bmatrix}.$$

2: Using elementary row operations transform it into a lower triangular matrix

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

3: Set $d = \gcd(a_1, b_2)$, $s = c_3/d$, $s' = b_2/d$, $s'' = a_1/d$ and $u \equiv c_2/(s'd) \pmod{s/s'}$.
4: Compute c and w such that $b_1/d = s'c + w$ and $\deg(w) < \deg(s')$.
5: Compute $v \equiv c_1/d - s'qu \pmod{s}$.
6: **Return:** The ideal $d\,[s, s'(\rho + u), s''\omega + w\rho + v]$ generated by α, given in terms of a canonical basis.

Since we used only elementary row operations, the algorithm gives a valid $\mathbb{F}_q[x]$-basis for the principal ideal generated by $a + b\rho + c\omega$. The latter steps in the algorithm ensure the basis is canonical.

12. Composition and Reduction in the ideal class group

We have all the tools we need to do composition and reduction in the ideal class group. Given two ideals I_1 andI_2 we find a distinguished representative in the class of $I_1 I_2$ as follows:

Algorithm 3: CompRed

Input: Two ideals I_1 and I_2 with canonical representations.
Output: The distinguished ideal J equivalent to $I_1 I_2$.

1: Calculate $I_3 = I_1 I_2$.
2: Find $\overline{I_3}$.
3: Find $\alpha \in \overline{I_3}$ of minimal norm using Algorithm 1.
4: Compute $\langle \alpha \rangle = \langle d \rangle [s, s'(u+\rho), v + w\rho + \omega]$ using Algorithm 2.
5: Compute $J = \langle \alpha \rangle / \overline{I_3}$.
6: **Return:** J.

The proof of correctness has been established in the previous sections by invoking the appropriate theorems. For almost all cubic function field in characteristic three with a totally ramified place at infinity, we have given composition and reduction in the ideal class group. There are, however, some exceptions - see Example 1 in Section 6 for a function field with a totally ramified place for which the above algorithm will fail to succeed at reduction in the ideal class group.

13. Conclusion

This work was chiefly motivated by two sources. We wanted comparable results of [6, 11] in the characteristic 3 case and a generalization along the lines of Bauer's [1] computation in the ideal class group. Finding fundamental units when the infinite place is unramified is an ongoing investigation. We conclude with an example to illustrate the above algorithms.

14. Example Computation

We present an example to illustrate the algorithms. The field of constants is $\mathbb{F}_9 = \mathbb{F}_3[\alpha]/\langle \alpha^2 - \alpha - 1 \rangle$ and the cubic function field is $\mathbb{F}_9(x, y)$ where y is a root of $T^3 - \alpha T + x^4 - 1$. Since α is not a square in $\mathbb{F}_9$, this extension is not galois and has no finite ramification. The infinite place is totally ramified and the genus of the function field is 3. We let

$$I_1 = [x, -\alpha - 1 + \rho, \alpha - 1 + \omega]$$

and we will find the reduced ideal in the class of I_1^6 following Algorithm 3.

Step 1. We calculating I_1^2 and I_1^3 followed by I_1^6 invoking Proposition 9.1 each time. We state only the the parameters used to define I_1^6 which has the form $[s_2, u_2 + \rho, v_2 + \omega]$, where

$$s_2 = x^6, \quad u_2 = x^4 - \alpha - 1, \text{ and } v_2 = -(\alpha + 1)x^4 + \alpha + 1.$$

Step 2. We compute $I_3 = \overline{I_2}$. It is clear that this inverse will have the form $[s_3, s_3\rho, v_3 + w_3\rho + \omega]$. By appealing to Proposition 8.2 (1), we have $s_3 = x^6$, $v_3 = -v_2$, and $w_3 = -u_2$.

Step 3. We apply Algorithm 1 to the above ideal. We note that the while-loop finishes in two iterations to give $a + b\rho + c\omega$ as the element of minimal norm, where

$$a = -x^2, \ b = (\alpha + 1)x^2, \text{ and } c = x^2.$$

Step 4. Applying Algorithm 2 to the above parameters gives

$$\langle x^2 \rangle [x^4, x^4\rho, 1 - (\alpha + 1)\rho + \omega].$$

Step 5. Finally, we calculate $\langle \alpha \rangle / I_3$ according to Proposition 8.4. This has the form $[s_4, u_4 + \rho, v_4 + \omega]$ where

$$s_4 = x^2, \ u_4 = -\alpha - 1, \text{ and } v_4 = \alpha - 1.$$

Note that this happens to be I_1^2.

References

1. M. Bauer, *The arithmetic of certain cubic function fields*, Math. Comp. **73** (2004), no. 245, 387–413 (electronic). MR 2034129 (2004k:11179)
2. T. Bembom, *Arithmetic problems in cubic and quartic function fields*, Master's thesis, Universitaẗ Oldenburg, 2009.
3. B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol. 10, American Mathematical Society, Providence, R.I., 1964. MR 0160744 (28 #3955)
4. H. Hasse, *Number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 229, Springer-Verlag, Berlin, 1980, Translated from the third German edition and with a preface by Horst Günter Zimmer. MR 562104 (81c:12001b)
5. E. Landquist, *Infrastructure, arithmetic, and class number computations in purely cubic function fields of characteristic at least 5*, Ph.D. thesis, University of Illinois at Urbana-Champaign, 2009.
6. E. Landquist, P. Rozenhart, R. Scheidler, J. Webster, and Q. Wu, *An explicit treatment of cubic function fields with applications*, Canadian Journal of Mathematics **62** (2010), 787–807.
7. D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996. MR 1376367 (97e:14035)
8. M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR 1876657 (2003d:11171)
9. P. Rozenhart and R. Scheidler, *Tabulation of cubic function fields with imaginary and unusual Hessian*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 357–370. MR 2467858 (2009m:11213)
10. R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 2, 609–631. MR 1879675 (2002k:11209)
11. ———, *Algorithmic aspects of cubic function fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 395–410. MR 2138010 (2006c:11136)
12. R. Scheidler and A. Stein, *Voronoi's algorithm in purely cubic congruence function fields of unit rank* 1, Math. Comp. **69** (2000), no. 231, 1245–1266. MR 1653974 (2000j:11177)
13. H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR 2464941 (2010d:14034)
14. G. Voronoi, *Concerning algebraic integers derivable from a root of an equation of the third degree*, Master's thesis, St. Petersburg, Russia, 1894.
15. J. Webster, *Cubic function fields in characteristic three*, Ph.D. thesis, University of Calgary, 2010.

Department of Mathematics and Statistics, University of Calgary,
Calgary AB T2L 1N4, CANADA
E-mail address: mbauer@math.ucalgary.ca

Department of Mathematics, Bates College,
Lewiston ME 04240, USA
E-mail address: jwebster@bates.edu