

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 describe the splitting behavior of any place, and give composition and reduction algorithms for arithmetic in the ideal class group.

1. INTRODUCTION

Calculating invariants of a 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 [11], to computing in the ideal class group [1], to tabulating [9], to describing and classifying arbitrary cubic function fields [6, 10], 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 impractical 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 work to this end has also been undertaken in [2]. However, the aim of our project is slightly different — as 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 and this is used in Section 5 to calculate the genus. This will conclude the calculation of basic invariants. We review the relationship between

2010 *Mathematics Subject Classification.* Primary 11Y40.

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 in the ideal class group and conclude with an example computation.

2. STANDARD FORM

As there are many good introductions to algebraic function fields (for example [13, 7]), we will only seek to clarify the notation used in this paper. As usual, let \mathbb{F}_q be a finite field 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 irreducible monic polynomial in $(\mathbb{F}_q[x])[T]$ of degree $n = [\mathcal{F} : \mathbb{F}_q(x)]$. Hence to study cubic function fields, we consider affine planar curves $H(x, T)$, where $H \in \mathbb{F}_q[x, T]$ is a bivariate polynomial that is absolutely irreducible and of degree three in T .

When $\text{char}(\mathbb{F}_q) \neq 3$, cubic function fields may be studied by examining the standard form for the defining polynomial which 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 [10] 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 $\text{char}(\mathbb{F}_q) = 3$ unless explicitly stated otherwise.

Write $H(x, T) = ST^3 + UT^2 + VT + W$ with $S, U, V, W \in \mathbb{F}_q[x]$ and $SW \neq 0$. If $U = V = 0$, then the function field associated with this curve is purely inseparable, and hence isomorphic to the rational function field (see Proposition III.9.2 of [13]). 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 $T^3 - AT + B = 0$. In terms of the original parameters, $A = -SV$ and $B = S^2W$. Otherwise, $U \neq 0$ and transform via $T \rightarrow (T + V)/U$ to eliminate the linear term. Considering the monic, integral, reciprocal polynomial, we get a curve in the form $T^3 - AT + B = 0$. If $N = S - U^2V + U^3W$, then $A = -N^2U^2$ and $B = N^2S$ in terms of the parameters of the original curve.

Henceforth, we will restrict our attention to curves of the form $T^3 - AT + B = 0$. In what follows we use the fact that $T \rightarrow T + i$ yields the birationally equivalent curve $T^3 - AT + (i^3 - iA + B) = 0$. Our goal will be two-fold — to minimize both the repeated factors dividing A and the degree of B .

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

$$(2.1) \quad T^3 - \left(\frac{A}{Q^2}\right)T + \left(\frac{i^3 - iA + B}{Q^3}\right) = 0.$$

If the characteristic is not three, the existence of a Q such that $Q^2|A$ and $Q^3|B$ implies that y/Q is integral. Likewise, in characteristic three the existence of Q and i implies $(y+i)/Q$ is integral and has a minimal polynomial (2.1). Hence this is the appropriate generalization from the case where the characteristic is different from

three. Also, in each case Q corresponds to removable singularities that preserve the shape of the model for the given curve.

To find Q and i , it is sufficient to check irreducible polynomials P such that $P^2|A$. Begin by writing $i = i_0 + i_1P + i_2P^2$ with $i_0, i_1, i_2 \in \mathbb{F}_q[x]$ with degree less than that of P . Since only i_0 affects the congruence $i^3 - iA + B \equiv 0 \pmod{P^3}$, we solve $i_0^3 + B \equiv 0 \pmod{P}$. It then becomes a matter of checking whether $i_0^3 - i_0A + B \equiv 0 \pmod{P^3}$. If the congruence holds, redefine A as A/P^2 and B as $(i^3 - iA + B)/P^3$. This process may be repeated as needed.

We now turn our focus to reducing the degree of B . If $3|\deg B$ and $2\deg B > 3\deg A$, we can write $B(x) = b_{3n}x^{3n} + b_{3n-1}x^{3n-1} + \dots + b_0$ with $b_{3n} \neq 0$. Then consider the linear transformation $T \rightarrow T - (b_{3n})^{1/3}x^n$ (note that $b_{3n}^{1/3} \in \mathbb{F}_q$ because \mathbb{F}_q is perfect). Under this map we get a new curve

$$T^3 - A(x)T + b_{3n-1}x^{3n-1} + \dots + b_0 + A(x)b_{3n}^{1/3}x^n = 0,$$

where the polynomial $b_{3n-1}x^{3n-1} + \dots + b_0 + A(x)b_{3n}^{1/3}x^n$ has a lower degree than $B(x)$. By repeating this procedure it is possible to force the curve to satisfy one of the following two distinct criteria:

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

or

$$(2.3) \quad 2\deg B \leq 3\deg A.$$

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 $Q, i \in \mathbb{F}_q[x]$ such that $Q^2|A$ and $Q^3|i^3 - iA + B$ 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 $(a, b) \in \overline{\mathbb{F}}_q^2$ satisfies the following three equations.

$$(2.4) \quad b^3 - A(a)b + B(a) = 0.$$

$$(2.5) \quad A(a) = 0.$$

$$(2.6) \quad -A'(a)b + B'(a) = 0.$$

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

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. The square factors

removed from A in the conversion to standard form correspond to singular points, which simplifies future calculations. In fact, if the standard form is nonsingular then $\{1, y, y^2\}$ is an integral basis for the maximal order (see Prop 5.10 of [7]). We now know that $D = \text{disc}(y) = A^3$ (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-free factorization of $d = \gcd(A(x), A'(x)^3 B(x) + B'(x)^3)$ is $I = \text{ind}(y)$. With D and I in hand, we will have $\Delta = \text{disc}(\mathcal{F})$.

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 $T^3 - g^2 T = fg^2$ is an integral model for this equation. By renaming, we have $A(x) = g(x)^2$ a square. \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 $y = y^{(0)}, y^{(1)}, y^{(2)}$ defines 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:

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

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 $\text{disc}(\mathcal{F}) = \text{disc}(\alpha_0, \alpha_1, \alpha_2)$ 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 $\text{disc}(\alpha) = \text{ind}(\alpha)^2 \text{disc}(\mathcal{F})$, 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 choose the product of the latter two basis elements to be in $\mathbb{F}_q[x]$. 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 $I_1, I_2, i, c, b \in \mathbb{F}_q[x]$ (the choice to reuse i will become clear). 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 $I = \text{ind}(y)$ 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. \square

Having established that the index is square free, it is possible to calculate i . Since i is unique modulo I , i is 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 $\Delta = A^3/I^2$. It is well known that the field discriminant is closely tied to ramification. This is developed more fully in the next section.

Letting $A = EI$ and $FI^2 = i^3 - iA + B$, we have the following identities for various products of integral basis elements:

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

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 infinity 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_∞} . 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 and b be defined by $T^3 - aT + b \equiv T^3 - AT + B \pmod{P}$. 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 $(P) = \mathfrak{p}\mathfrak{q}\mathfrak{t}$.*

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 (see Theorem III.3.7 of [13]) 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 two ramified cases are as claimed (see Theorem III.5.1 in [13]). \square

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]. This theorem implies that there will be a root 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. We will show that 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. After dealing with the four cases that arise in this situation, it will be clear why (2.2) implies that 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

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

where $y_i \in \mathbb{F}$. Let $A(x) = a_{2n}x^{2n} + \dots + a_0$ and $B(x) = b_{3n}x^{3n} + \dots + b_0$ 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:

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

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 . Therefore, we examine the solutions to $Y^3 - a_{2n}Y + b_{3n} = 0$.

If $\deg(A)$ is odd then $a_{2n} = 0$ and $Y^3 + b_{3n} = 0$ has exactly one solution. This occurs in the partially ramified case because there is exactly one root in $\mathbb{F}_q\langle x^{-1} \rangle$ and another distinct root in $\mathbb{F}_q\langle x^{-1/2} \rangle$. Otherwise when $a_{2n} \neq 0$, the finite field extension which contains y_n determines the splitting type. The completely split case has three distinct roots in $\mathbb{F}_q\langle x^{-1} \rangle$. In this case $Y^3 - a_{2n}Y + b_{3n}$ splits completely in $\mathbb{F}_q[Y]$. The inert case will have a root in $\mathbb{F}_{q^3}\langle x^{-1} \rangle$ and therefore $Y^3 - a_{2n}Y + b_{3n}$ is irreducible over $\mathbb{F}_q[Y]$. The last case corresponds to the polynomial factoring as a linear and an irreducible quadratic in $\mathbb{F}_q[Y]$. Therefore the place is partially split.

Suppose the curve in standard form satisfies (2.2). If we let b_k be the leading coefficient of $B(x)$ (with $3 \nmid k$, and $k > 3n$), then the first equation is $b_k = 0$ which is a contradiction. This forces the above system of equations to be inconsistent. Therefore a curve in standard form satisfying (2.2) must have a wildly ramified place at infinity. We summarize the above discussion in 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 $(\infty) = \mathfrak{p}\mathfrak{q}^2$.*
- (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 $(\infty) = \mathfrak{p}\mathfrak{q}$.*
 - (c) *If $\deg d = 3$ then $(\infty) = \mathfrak{p}\mathfrak{q}\mathfrak{r}$.*

This gives a classification of the signature of the function field that involves a simple computation using very basic parameters of the curve. We can now turn our attention to calculating the genus of the function field.

5. GENUS

We will calculate the genus with the Hurwitz Genus Formula (see Theorem III.4.12 in [13]), 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. The infinite place is more complicated. However, since the problematic case is when wild ramification occurs, we are fortunate in that wild ramification is also total ramification. For totally ramified places, 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 $v_{\mathfrak{p}}(y) = -\deg B$. We will apply Theorem III.5.12 of [13]. The uniformizer used in the theorem will depend on which residue class $\deg B$ resides in modulo 3.

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. \square

Theorem 5.2. *If \mathcal{F} has a totally ramified place at infinity then the genus of \mathcal{F} is $g = \deg B - \deg I - 1$.*

Proof. The Hurwitz Genus Formula gives

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

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. \square

Theorem 5.3. *If \mathcal{F} has a place at infinity that is tamely ramified or unramified, 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 proof follows as before except now that 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_∞ . \square

We have described the basic invariants of cubic function fields in characteristic three. 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], [5], [4] [10], [12]), 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.

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 $\mathcal{O}_F, \mathcal{I}(\mathcal{O}_F)$. The *Fundamental theorem of ideal theory in an algebraic function field* [4, p 401] gives the isomorphism as

$$(6.1) \quad \Phi : \mathcal{D}_F^0(S) \rightarrow \mathcal{I}(\mathcal{O}_F), \quad D \mapsto \left\{ \alpha \in F^\times \mid \sum_{P \in S} v_P(\alpha)P \geq D \right\} \cup \{0\}.$$

This may also be defined by

$$\sum n_P P \mapsto \prod_{P \in S} (P \cap \mathcal{O}_F)^{n_P}.$$

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

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

where S^c is the set of infinite places (the set compliment of S in \mathbb{P}_F). 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.

$$D = \sum_{P \in \mathbb{P}_F} n_P P \quad \Rightarrow \quad D^+ = \sum_{P \in \mathbb{P}_F, n_P > 0} n_P P.$$

A degree zero divisor is called *finitely effective* if its finite part is effective; it can be shown that every divisor $D \in \mathcal{D}_F^0$ 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 $\alpha \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$. 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

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

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, a class of curves exists for which this implication is not true. We can construct a curve such that $3 \nmid \deg B$ and $3 \mid \deg FI^2$. 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 $\deg FI^2 = \deg (i^3 - iA + B) = 9$.

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 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. *If $2 \deg B > 3 \deg A$, and $3 \nmid \deg FI^2$, then every ideal class contains a unique distinguished ideal.*

Proof. By Theorem 6.3 there exists $\alpha_1 \in J$ of minimal norm from some ideal J . We consider the primitive integral ideal $J_1 = \langle \alpha_1 \rangle J^{-1}$. Assume there is some integral primitive ideal J_2 equivalent to J_1 with $\deg N(J_2) \leq \deg N(J_1)$. Then $J_2J = \langle \alpha_2 \rangle$ with $\alpha_2 \in J$. This gives $\deg N(J_1) = \deg N(\alpha_1) - \deg N(J) \geq \deg N(J_2) = \deg N(\alpha_2) - \deg N(J)$ which implies $\deg N(\alpha_1) \geq \deg N(\alpha_2)$. By assumption α_1 is an element of minimal norm; therefore $\alpha_2 = k\alpha_1$ for $k \in \mathbb{F}_q^\times$ and $J_1 = J_2$. Thus every ideal class contains a unique distinguished ideal. \square

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. We start by describing an integral basis for primes and their powers which gives insight to how inversion and multiplication will work as explained afterward. Finally, we give explicit algorithms that produce the element of minimal norm and its corresponding distinguished ideal.

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 [12] 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.

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. A ramified prime is expected to be totally ramified so $\mathfrak{p}^3 = (P)\mathcal{O}_{\mathcal{F}} = (P)[1, \rho, \omega]$ for some irreducible polynomial $P \in \mathbb{F}_q[x]$. This leaves only the calculation of the basis for \mathfrak{p} and \mathfrak{p}^2 .

Proposition 7.1. *Let $v_P(A) \geq 1$ and $v_P(I) = 0$ so that $(P) = \mathfrak{p}^3$. Then*

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

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

Proof. Apply Kummer's theorem to the minimal polynomial of ρ to see

$$\rho^3 - A\rho + FI^2 \equiv \rho^3 + FI^2 \equiv (\rho + f)^3 \pmod{P}.$$

This implies $\mathfrak{p} = \langle P, f + \rho \rangle$. To get the last element we consider $\rho(f + \rho) = f\rho + I\omega + A \in \mathfrak{p}$. Using that I is relatively prime to P we get the last element as claimed.

For \mathfrak{p}^2 , consider $(f + \rho)^2 = f^2 - f\rho + I\omega + A \in \mathfrak{p}^2$ to see that the third term in the basis has the form claimed. Note $v_{\mathfrak{p}}(P) = 3$, so $P \in \mathfrak{p}^2$. Since the ideal has to have norm P^2 this forces the second element of the basis to be as stated. \square

The next two primes we consider both lie over primes dividing the index. Unlike the above primes and the unramified primes (as we will see in the next subsection), these primes can give rise to ideals that will have ω with a polynomial coefficient.

Proposition 7.2. *Let $v_P(A) > 1$ and $v_P(I) = 1$ so that $(P) = \mathfrak{p}^3$. Then*

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

Proof. By applying Kummer's theorem to the minimal polynomials of ρ and ω , we see that both are in \mathfrak{p} . Squaring \mathfrak{p} and considering the 9 resulting elements leads to the latter result. \square

Tamely ramified primes are all that remain to consider. We state their bases here, but we will treat powers of \mathfrak{p} and \mathfrak{q}^2 with unramified primes.

Proposition 7.3. *Let $v_P(A) = 1$ and $v_P(I) = 1$ so that $(P) = \mathfrak{p}\mathfrak{q}^2$. Then*

$$\begin{aligned}\mathfrak{p} &= [P, \rho, E + \omega], & \mathfrak{q} &= [P, \rho, \omega], \\ \mathfrak{q}^2 &= [P, P\rho, E^{-1}F\rho + \omega], & \text{and } \mathfrak{p}\mathfrak{q} &= [P, \rho, P\omega]\end{aligned}$$

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

Proof. Apply Kummer's theorem to the minimal polynomials of ρ and ω and proceed as before. \square

7.2. Unramified primes. The unramified primes are the primes that we expect to deal with most often in the course of doing computations. There are several different cases to be accounted for depending on the inertial degree and the primes involved in the product. First we deal with the case in which \mathfrak{p} has inertia degree 1, and then when \mathfrak{p} has inertia degree 2. This case will also handle the product of two primes of inertia degree 1 and the powers of \mathfrak{q}^2 for the split ramified case. The last case will be where $\mathfrak{p}, \mathfrak{q}$ both have inertia degree 1 and we need to consider products of the form $\mathfrak{p}^i\mathfrak{q}^j$ with $i \neq j$.

Proposition 7.4. *Let $\mathfrak{p}|P$ have inertial degree 1 and ramification index 1. 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 $I^{-1}I \equiv 1 \pmod{P}$.

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

The proposition below deals with primes that have ramification index 1 and inertia degree 1. It therefore also handles the unramified prime lying over the tamely ramified primes.

Proposition 7.5. *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 7.3 and 7.4.

Proof. The definitions in this proposition make it important that Z_1 be invertible modulo P . In Proposition 7.3, E is invertible modulo P . For Proposition 7.4 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} .

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

Since we want $C_i P^i - EZ_i k P^i \equiv 0 \pmod{P^{i+1}}$, we can choose $k \equiv C_i (EZ_i)^{-1} \pmod{P}$. 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. \square

Proposition 7.6. *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. Kummer's theorem gives $\mathfrak{q} = \langle P, \rho^2 - M\rho + W \rangle$, and similar techniques complete the proof. \square

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

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

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 7.6,
- $\mathfrak{q}^2 = [P, P\rho, E^{-1}F\rho + \omega]$ from Proposition 7.3, and
- $\mathfrak{p}\mathfrak{q} = [P, P\rho, I^{-1}(A + \alpha_1\alpha_2) - I^{-1}(\alpha_1 + \alpha_2)\rho + \omega]$ from the exposition above.

Proposition 7.7. *Let \mathfrak{r} represent any of the three ideals above. Then*

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

where

- $L(M_{i-1}M_1I + N_{i-1} + N_1 - E) \equiv 1 \pmod{P^i}$,
- $M_i \equiv -L(F + M_{i-1}N_1 + M_1N_{i-1}) \pmod{P^i}$, and
- $N_i \equiv L(M_1FI + M_{i-1}FIM_{i-1}M_1AN_{i-1}N_1) \pmod{P^i}$.

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

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

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} or $P^{i-1}\rho$. Thus the ideal has the desired norm and the elements stated form a basis. \square

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 7.7 we know

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

and by Proposition 7.5

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

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

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

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

Proposition 7.8. *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. \square

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 factors into the product of four ideals:

$$J = [s_1, s'_1(u_1 + \rho), v_1 + w_1\rho + \omega][s_2, s_2(u_2 + \rho), v_2 + w_2\rho + \omega] \\ [s_3, \rho, s''_3\omega][s_4, s'_4(u_4 + \rho), s''_4(v_4 + w_4\rho + \omega)] = J_1 J_2 J_3 J_4.$$

Each of the ideals is relatively prime to the others and is determined by which type of prime appears in the factorization. For $\mathfrak{p}|P$, we have four criteria:

- \mathfrak{p} divides J_1 iff P is unramified,
- \mathfrak{p} divides J_2 iff P is totally ramified and does not divide the index,
- \mathfrak{p} divides J_3 iff 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 primes Type I, Type II, Type III and Type IV, respectively. 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 the propositions are easier to state for a given type. The combined proposition would look much like each constituent part where the final result is an application of the Chinese Remainder Theorem. 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. Thus from a computational point of view, three of the four cases will rarely occur even when a curve is singular.

8. INVERSION AND DIVISION

Some basic properties of the structure of ideals in cubic function fields developed in [12] 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 [12]) *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*

$$\begin{aligned} s_2 | s_1, \quad s'_2 | s'_1, \quad s''_2 | s''_1, \quad s'_1 u_1 \equiv s'_1 u_2 \pmod{s_2}, \\ s''_1 w_1 \equiv s''_1 w_2 \pmod{s'_2}, \quad \text{and} \quad s''_1 v_1 \equiv s''_1 (v_2 + u_2(w_1 - w_2)) \pmod{s_2}. \end{aligned}$$

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 \bar{J} and the notation for division will be J^{-1} . We label the propositions depending on which of the four ideal types the proposition covers.

Proposition 8.2. (Inversion for Type I and II primes) *If $I_1 = [s, s'(u + \rho), v + w\rho + \omega]$, then $I_2 = \bar{I}_1 = \langle s \rangle I_1^{-1}$ is given by $I_2 = [S, S'(U + \rho), V + W\rho + \omega]$, where*

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

Proof. 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 (and the proofs to follow). 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. The other products of the two ideals give the remaining congruences. We start with $S'(U + \rho)(v + w\rho + \omega)$ and examine the coefficient of ω :

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

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. \square

We note that the above proposition is simpler for nonsingular curves because $I = 1$ and most of the congruences can be replaced by equalities. It was fortunate that we could deal with Type I and Type II primes with a single proposition without an appeal to the Chinese Remainder Theorem. We will often be able to deal with these two types of primes together.

Proposition 8.3. (Inversion for Type III primes) *If $I_1 = [s, \rho, s''\omega]$, then $I_2 = \bar{I}_1 = \langle s \rangle I_1^{-1}$ is given by $I_2 = [s, \rho, (s/s'')\omega]$.*

Proof. This follows immediately from Proposition 7.2. \square

Here the index divisors do not seem too complicated, but for Type IV ideals they will prove very troublesome. The approach taken for this case will become familiar. Just as factorization helps simplify the four cases, factorization within this case will prove useful. Our approach is to consider a factorization that most closely resembles some of the basic prime powers of Section 7. The treatment of Proposition 7.8, that dealt with products of the form $\mathfrak{p}^i \mathfrak{q}^{i+j}$, is enlightening here. In the proof we appeal to the fact that the product can be viewed as $(\mathfrak{p}\mathfrak{q})^i$ and \mathfrak{q}^j . This is the sort of factorization that we will use in many of the following propositions.

Proposition 8.4. (Inversion for Type IV) *If $I_1 = [s, s'(u + \rho), s''(v + w\rho + \omega)]$, then $I_2 = \overline{I}_1 = \langle s \rangle I_1^{-1}$ is given by $I_2 = [S, S'(U + \rho), S''(V + W\rho + \omega)]$, where*

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

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

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

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

Proof. Factor I_1 as

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

By factoring the ideal in this fashion, we can find the inverse of each factor. The inverse of the first two factors is an immediate consequence of Proposition 7.3. 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 this gives $V \equiv 0 \pmod{s_I}$. 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. \square

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. Consider two primes \mathfrak{p} and \mathfrak{q} lying over a completely split place P . Given $(\mathfrak{p}\mathfrak{q})^i$ and \mathfrak{p}^i , we find (somewhat trivially) $(\mathfrak{p}\mathfrak{q})^i \mathfrak{p}^{-i} = \mathfrak{q}^i$. Thus the product $(\mathfrak{p}\mathfrak{q})^i$ is split into two ideals of equal norm, \mathfrak{p}^i and \mathfrak{q}^i .

Lemma 8.5. (Splitting for Type I and II primes) *Let $I_2 = [s, s\rho, v_2 + w_2\rho + \omega]$ and $I_1 = [s, u_1 + \rho, v_1 + \omega]$ be two ideals such that $I_2 \subseteq I_1$. Then $J = I_2 I_1^{-1} = [s, U + \rho, V + \omega]$, where*

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

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

$$J[s, u_1 + \rho, v_1 + \omega][s, Iw_2 + \rho, u_2w_2 - v_2 + \omega] = \langle s \rangle.$$

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 $w_2(U + \rho)$. \square

Lemma 8.6. (Splitting for Type III primes) *Let $I_2 = [s, \rho, s\omega]$ and $I_1 = [s, \rho, \omega]$ be two ideals such that $I_1 \subseteq I_2$. Then $J = I_2I_1^{-1} = [s, \rho, \omega]$.*

Proof. This follows immediately from Proposition 7.2. \square

Lemma 8.7. (Splitting for Type IV primes) *Let $I_2 = [s's'', s'\rho, s''(v_2 + w_2\rho + \omega)]$ and $I_1 = [s's'', \rho, v_1 + \omega]$ be two ideals such that $I_2 \subseteq I_1$. Then $J = I_2I_1^{-1} = [s's'', \rho, V + \omega]$, where*

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

Proof. By Proposition 7.3, $J = [s's'', \rho, V + \omega]$ for some V . For a given prime P , I_2 contains either $\mathfrak{p}\mathfrak{q}$ 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 . \square

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 $\mathfrak{p}^5\mathfrak{q}$.

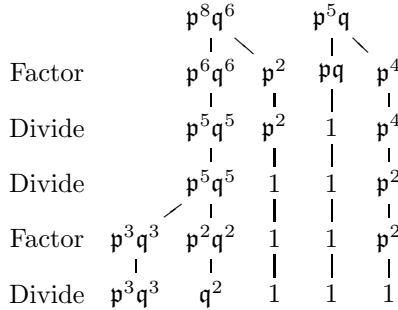


FIGURE 1. Division of $\mathfrak{p}^8\mathfrak{q}^6$ by $\mathfrak{p}^5\mathfrak{q}$

The tree for the dividend ends with three branches. It should be noted that the last two nodes on the 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 8.8. (Division for Type I and II primes) *Let $I_i = [s_i, s'_i(u_i + \rho), v_i + w_i\rho + \omega]$ for $i = 1, 2$ be such that $I_2 \subseteq I_1$. Then $J = I_2I_1^{-1} = [S, S'(U + \rho), V + W\rho + \omega]$, where*

$$S = \frac{s_2}{s'_1d}, \quad S' = \frac{s'_2d}{s_1}, \quad U \equiv \begin{cases} Iw_2 - u_1 & (\text{mod } s_1/(s'_1d)) \\ u_2 & (\text{mod } s_2/(s'_2d)) \end{cases},$$

$$V \equiv (W - w_2)U + v_2 \pmod{S}, \quad W \equiv w_2 \pmod{S'},$$

$$\text{and } d = \gcd\left(\frac{s_2}{s'_2}, \frac{s_1}{s'_1}, u_1 - u_2\right).$$

Proof. We begin by factoring both I_1 and I_2 into two different ideals:

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

The first division is

$$(8.1) \quad I_{2,1}I_{1,1}^{-1} = \left[\frac{s'_2}{s'_1}, \frac{s'_2}{s'_1}\rho, v_2 + w_2\rho + \omega \right].$$

All that remains of the divisor is $I_{1,2} = [s_1/s'_1, u_1 + \rho, v_1 - u_1w_1 + \omega]$. 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:

$$\left[\frac{s_2}{s'_2}, u_2 + \rho, v_2 - u_2w_2 + \omega \right] [d, u_1 + \rho, v_1 - u_1w_1 + \omega]^{-1} =$$

$$\left[\frac{s_2}{s'_2d}, u_2 + \rho, v_2 - u_2w_2 + \omega \right],$$

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,

$$\left[\frac{s'_2}{s'_1}, \frac{s'_2}{s'_1}\rho, v_2 + w_2\rho + \omega \right] =$$

$$(8.2) \quad \left[\frac{s'_2d}{s_1}, \frac{s'_2d}{s_1}\rho, v_2 + w_2\rho + \omega \right] \left[\frac{s_1}{s'_1d}, \frac{s_1}{s'_1d}\rho, v_2 + w_2\rho + \omega \right].$$

We apply Lemma 8.5 to the right hand ideal of (8.2) and the remainder of the divisor to get

$$\left[\frac{s_1}{s'_1d}, \frac{s_1}{s'_1d}\rho, v_2 + w_2\rho + \omega \right] \left[\frac{s_1}{s'_1d}, u_1 + \rho, v_1 - w_1u_1 + \omega \right]^{-1}$$

$$= \left[\frac{s_1}{s'_1d}, Iw_2 - u_1 + \rho, v_2 - Iw_2^2 + u_1w_2 + \omega \right].$$

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 :

$$S = \left(\frac{s_1}{s'_1d} \right) \left(\frac{s'_2d}{s_1} \right) \left(\frac{s_2}{s'_2d} \right) = \frac{s_2}{s'_1d} \quad \text{and} \quad S' = \frac{s'_2d}{s_1}.$$

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 . \square

Proposition 8.9. (Division for Type III primes) *Let $I_i = [s_i, \rho, s_i''\omega]$ for $i = 1, 2$ be such that $I_2 \subseteq I_1$. Then $J = I_2I_1^{-1} = [S, \rho, S''\omega]$, where*

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

Proof. This follows by using the same arguments presented in the proof of Proposition 8.8. 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. \square

Proposition 8.10. (Division for Type IV primes) *Let $I_i = [s_i, s_i'(u_i + \rho), s_i''(v_i + w_i\rho + \omega)]$ for $i = 1, 2$ be such that $I_2 \subseteq I_1$. Then $J = I_2I_1^{-1} = [S, S'(U + \rho), S''(V + W\rho + \omega)]$, where*

$$S = \frac{s_2}{s_1's_1''d}, \quad S' = \gcd\left(\frac{ds_2's_2''}{s_1}, \frac{s_2'}{s_1'}\right), \quad S'' = \gcd\left(\frac{ds_2's_2''}{s_1}, \frac{s_2''}{s_1''}\right),$$

$$U \equiv \begin{cases} 0 & (\text{mod } s_1/(s_1's_1''d)) \\ u_2 & (\text{mod } s_2/(s_2's_2''d)) \end{cases},$$

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

$$S''V \equiv s_2''(W - w_2)U + v_2 \pmod{S}, \quad \text{and} \quad S''W \equiv s_2''w_2 \pmod{S'}.$$

Proof. 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

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

Proceeding as in the proof of Proposition 8.8, 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:

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

where

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

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 8.7 to the right most ideal of (8.4) and the remainder of the divisor to get

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

where v_3 is given in Lemma 8.3. 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 in Proposition 8.8 except we have to account for the coefficient of ω . \square

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. A proposition on multiplication will invoke this proposition, but it is invoked under the assumption that I_1 completely divides $\langle d \rangle$ and that there is no corresponding factor I_2 .

Proposition 8.11. (Nonprimitive division for Type I and II primes)

Let $I_2 = d[s_2, s'_2(u_2 + \rho), v_2 + w_2\rho + \omega]$ and $I_1 = [s_1, s'_1(u_1 + \rho), v_1 + w_1\rho + \omega]$ be such that $\langle d \rangle I_2 \subseteq I_1$. Then $IJ = I_2 I_1^{-1} = (D_3) I_d I_m$, where

$$I_d = [s_2, s'_2(u_2 + \rho), v_2 + w_2\rho + \omega] \left[\frac{s_1}{D_1 D_2}, \frac{s'_1}{D_1}(u_1 + \rho), v_1 + w_1\rho + \omega \right]^{-1}$$

is calculated by Proposition 8.8,

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

is calculated by Proposition 8.2,

$$D_1 = \gcd(s'_1, d), \quad D_2 = \gcd\left(\frac{s_1}{s'_1}, \frac{d}{D_1}\right), \quad \text{and } D_3 = \frac{d}{D_1 D_2}.$$

Proof. We note that $\overline{I_m} \subseteq \langle d \rangle$ and $\overline{I_m}[s_1/D_1 D_2, s'_1/D_1(u_1 + \rho), v_1 + w_1\rho + \omega] = I_1$. Therefore $\langle d \rangle \overline{I_m}^{-1} = I_m$. After this division, the factors that remain in I_1 are $[s_1/D_1 D_2, s'_1/D_1(u_1 + \rho), v_1 + w_1\rho + \omega]$ and this is contained in I_2 . \square

The next two propositions are stated without proof. The proofs follow a similar argument as the proof above and rely, like this proof, nearly entirely on the previously proved propositions.

Proposition 8.12. (Nonprimitive division for Type III primes)

Let $I_2 = d[s_2, \rho, s''_2\omega]$ and $I_1 = [s_1, \rho, s'_1\omega]$ be such that $\langle d \rangle I_2 \subseteq I_1$. Then $J = I_2 I_1^{-1} = (D_3) I_d I_m$, where

$$I_d = [s_2, \rho, s''_2\omega] \left[\frac{s_1}{D_1 D_2}, \rho, \frac{s''_2}{D_1}\omega \right]^{-1}$$

is calculated by Proposition 8.9,

$$I_m = \overline{[D_1 D_2, \rho, D_1\omega]}$$

is calculated by Proposition 8.3,

$$D_1 = \gcd(s_1'', d), \quad D_2 = \gcd\left(\frac{s_1}{s_1'}, \frac{d}{D_1}\right), \quad \text{and } D_3 = \frac{d}{D_1 D_2}.$$

Proposition 8.13. (Nonprimitive division for Type IV primes)

Let $I_2 = d[s_2, s_2'(u_2 + \rho), s_2''(v_2 + w_2\rho + \omega)]$ and $I_1 = [s_1, s_1'(u_1 + \rho), s_1''(v_1 + w_1\rho + \omega)]$ be such that $\langle d \rangle I_2 \subseteq I_1$. Then $J = I_2 I_1^{-1} = (D_4) I_d I_m$, where

$$I_d = [s_2, s_2'(u_2 + \rho), v_2 + w_2\rho + \omega] \left[\frac{s_1}{D_1 D_2 D_3}, \frac{s_1'}{D_1}(u_1 + \rho), D_2(v_1 + w_1\rho + \omega) \right]^{-1}$$

is calculated by Proposition 8.10,

$$I_m = \overline{[D_1 D_2 D_3, D_1(u_1 + \rho), D_2(v_1 + w_1\rho + \omega)]}$$

is calculated by Proposition 8.4,

$$D_1 = \gcd(s_1', d), \quad D_2 = \gcd(s_1'', d), \quad D_3 = \gcd\left(\frac{s_1}{s_1' s_1''}, \frac{d}{D_1 D_2}\right), \quad \text{and } D_4 = \frac{d}{D_1 D_2 D_3}.$$

9. IDEAL MULTIPLICATION

Theoretically, ideal multiplication is the easiest operation that will be discussed since it may be achieved by simply performing 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 [12].

Theorem 9.1. (Theorem 4.4 of [12]) Let $I_i = [s_i, s_i'(u_i + \rho), s_i''(v_i + w_i\rho + \omega)]$ with $i = 1, 2, 3$ be two ideals such that $\gcd(s_1, s_2) = 1$. Then $I_3 = I_1 I_2$ is given by

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

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 set of propositions assumes that the product is primitive and this will be used to aid in the case where the product is not assumed to be primitive.

In proof of Proposition 8.8 the two congruences for U were sufficient in guaranteeing that U was determined uniquely modulo S/S' . This was because $s_1/(s_1'd)$ and $s_2/(s_2'd)$ were relatively prime. Had they shared a common factor, U would have been determined only up to the least common multiple of $s_1/(s_1'd)$ and $s_2/(s_2'd)$. This proposition is built to handle just such a situation.

Proposition 9.2. (Primitive Multiplication for Type I primes)

Let $I_i = [s_i, s'_i(u_1 + \rho), v_i + w_i\rho + \omega]$ for $i = 1, 2$ be such that $I_1 I_2 = I_3$ is a primitive ideal. Then $I_3 = [S, S'(U + \rho), V + W\rho + \omega]$, where

$$S = \frac{s_1 s_2 d_1}{d}, \quad S' = \frac{s'_1 s'_2 d}{d_1}, \quad W = w_3 - cS', \quad V \equiv v_3 - qS'U \pmod{S},$$

$$\text{and } U \equiv u_3 + k \frac{s_1 s_2 d_1}{s'_1 s'_2 d^2} \pmod{S/S'}.$$

We choose c to make $\deg W$ minimal and define u_3, v_3, w_3, d, d_1 as follows

$$\begin{aligned} d &= \gcd\left(\frac{s_1}{s'_1}, \frac{s_2}{s'_2}\right), & d_1 &= \gcd(d, u_1 - u_2), \\ u_3 &\equiv u_1 \pmod{s_1 d_1 / s'_1 s d}, & u_3 &\equiv u_2 \pmod{s_2 d_1 / s'_2 d}, \end{aligned}$$

$$\text{and } k \text{ is chosen such that } d_1 \mid \frac{(u_3^3 - u_3 A - FI^2)S'd_1}{S} + kA,$$

$$\begin{aligned} w_3 &= a_1 s_2 w_1 + a_2 s_1 w_2 + a_3 s'_1 s'_2 (u_1 + u_2) + a_4 s'_1 (v_2 + u_1 w_2) \\ &\quad + a_5 s'_2 (v_1 + u_2 w_1) + a_6 (v_1 w_2 + v_2 w_1 - F) \\ v_3 &= a_1 s_2 v_1 + a_2 s'_1 v_2 + a_3 s'_1 s'_2 (u_1 u_2 + A) + a_4 s'_1 s (u_1 v_2 - FI + w_2) \\ &\quad + a_5 s'_2 (u_2 v_1 - FI + w_1 A) + a_6 (v_1 v_2 + w_1 w_2 - w_1 FI - W_2 FI) \end{aligned}$$

and $a_1, a_2, a_3, a_4, a_5,$ and a_6 are given by the extended euclidian algorithm as:

$$\begin{aligned} 1 &= a_1 s_2 + a_2 s_1 + a_3 s'_1 s'_2 I + a_4 s'_1 (u_1 + I w_2) \\ &\quad + a_5 s'_2 (u_2 + I w_1) + a_6 (v_1 + v_2 + w_1 w_2 I - E). \end{aligned}$$

Proof. Since we assume I_3 is primitive, it has a canonical basis of the form claimed. 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:

$$(9.1) \quad \left[\frac{s_1}{s'_1}, u_1 + \rho, v_1 - w_1 u_1 + \omega \right] \left[\frac{s_2}{s'_2}, u_2 + \rho, v_2 - w_2 u_2 + \omega \right].$$

The goal will be to split this product up into two factors. The quantity d signifies common possible prime factors in this product, and d_1 indicates those primes that appear as squares in the product. Thus, we write the above product as

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

We conclude from this that $S' = s'_1 s'_2 d / d_1$ and by equating norms that $S = s_1 s_2 d / d_1$. Combining the two previous statements we see that

$$\left[\frac{S}{S'}, U + \rho, V + \omega \right] = \left[\frac{s_1 d_1}{s'_1 d}, u_1 + \rho, v_1 - w_1 u_1 + \omega \right] \left[\frac{s_2 d_1}{s'_2 d}, u_2 + \rho, v_2 - w_2 u_2 + \omega \right].$$

This justifies the choice for u_3 , and note that u_3 is defined uniquely modulo the least common multiple of s_1d_1/s'_1d and s_2d_1/s'_2d . Thus we can write $U = u_3 + kS/S'd_1$ and consider

$$\frac{S}{S'} \left| N(U + \rho) \Rightarrow \frac{S}{S'} \left| (u_3^3 - u_3A - FI^2) + kA \frac{S}{S'd_1} \right.$$

From the definition of u_3 , $S/S'd_1$ divides $u_3^3 - u_3A - FI^2$ so we can conclude

$$d_1 \left| \frac{(u_3^3 - u_3A - FI^2)S'd_1}{S} + kA \right.$$

as claimed. 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. Once this element is computed, it is a matter of subtracting multiples of the two previously calculated basis elements to ensure the third element is canonical. \square

The calculation of W and V is not as difficult as it looks. As we noted before, 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 1 as a linear combination of fewer than all six terms. \square

Proposition 9.3. (Primitive Multiplication for Type II primes) *Let $I_i = [s_i, s'_i(u_1 + \rho), v_i + w_i\rho + \omega]$ for $i = 1, 2$ be such that $I_1I_2 = I_3$ is a primitive ideal. Then $I_3 = [S, S'(U + \rho), V + W\rho + \omega]$, where*

$$S = s_1s_2/d, \quad S' = ds'_1s'_2, \quad d = \gcd\left(\frac{s_1}{s'_1}, \frac{s_2}{s'_2}\right),$$

$$U \equiv f \pmod{S/S'}, \quad W \equiv I^{-1}f \pmod{S'}, \quad V \equiv f^2I^{-1} \pmod{S},$$

where f is defined by $f^3 \equiv FI^2 \pmod{S}$.

Proof. We invoke Proposition 7.1 to calculate U , V , and W . \square

Proposition 9.4. (Primitive Multiplication for Type III primes) *Let $I_i = [s_i, \rho, s''_i\omega]$ for $i = 1, 2$ be such that $I_1I_2 = I_3$ is a primitive ideal. Then*

$$I_3 = \left[\frac{s_1s_2}{d}, \rho, (s''_1s''_2d)\omega \right] \text{ where } d = \gcd\left(\frac{s_1}{s''_1}, \frac{s_2}{s''_2}\right).$$

Proof. This follows from Proposition 7.2. \square

Proposition 9.5. (Primitive Multiplication for Type IV primes) *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. Then $I_3 = [S, S'(U + \rho), S''(V + W\rho + \omega)]$, where*

$$S = \frac{s_1s_2}{dd_1d_2}, \quad S' = s'_1s'_2d, \quad S'' = s''_1s''_2d_1d_2.$$

To define d_1 , d_2 , and d , let

$$s_{qi} = \gcd\left(\frac{s_i}{s'_is''_i}, v_i - w_iu_i\right) \text{ for } i = 1, 2,$$

then

$$d = \gcd(s_{q_1}, s_{q_2}), \quad d_1 = \gcd\left(s_{q_2}, \frac{s_1}{s'_1 s''_1 s_{q_1}}\right), \quad \text{and} \quad d_2 = \gcd\left(s_{q_1}, \frac{s_2}{s'_2 s''_2 s_{q_2}}\right).$$

We defined $U = (s'_1 s''_2 d_1 d_2) u_3$ where u_3 satisfies

$$u_3 \equiv u_1 \pmod{\frac{s_1}{s'_1 s''_1 d_1 d_2}}, \quad \text{and} \quad u_3 \equiv u_2 \pmod{\frac{s_2}{s'_2 s''_2 d_1 d_2}}.$$

Finally we can choose V and W as

$$S''W = S''w_3 - qS', \quad S''V \equiv S''v_3 - qS'U \pmod{S},$$

where q is chosen so that $\deg V$ and $\deg W$ are minimal and

$$\begin{aligned} S''w_3 = & a_1 s_2 s'_1 w_1 + a_2 s_1 s'_2 w_2 + a_3 s'_1 s'_2 (u_1 + u_2) + a_4 s'_1 s'_2 (v_2 + u_1 w_2) \\ & + a_5 s'_2 s'_1 (v_1 + u_2 w_1) + a_6 s'_1 s'_2 (v_1 w_2 + v_2 w_1 - F) \end{aligned}$$

$$\begin{aligned} S''v_3 = & a_1 s_2 s'_1 v_1 + a_2 s_1 s'_2 v_2 + a_3 s'_1 s'_2 (u_1 u_2 + A) + a_4 s'_1 s'_2 (u_1 v_2 - FI + w_2) \\ & + a_5 s'_2 s'_1 (u_2 v_1 - FI + w_1 A) + a_6 s'_1 s'_2 (v_1 v_2 + w_1 w_2 - w_1 FI - W_2 FI) \end{aligned}$$

where a_i for $i = 1, \dots, 6$ come from the extended greatest common divisor calculation,

$$\begin{aligned} S'' = & a_1 s_2 s'_1 + a_2 s_1 s'_2 + a_3 s'_1 s'_2 I + a_4 s'_1 s'_2 (u_1 + I w_2) \\ & + a_5 s'_2 s'_1 (u_2 + I w_1) + a_6 s'_1 s'_2 (v_1 + v_2 + w_1 w_2 I - E). \end{aligned}$$

Proof. The details of the proof are similar to those above. We will try and note only the key distinctions. We factor I_i into three factors as

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

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 q) from the unramified primes:

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

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 coefficient of ω . This justifies the choice of d_1 and d_2 . 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 $J_{i,1}$. We can 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 chose V and W in the same manner as in the previous proposition. 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'' . \square

Much like Proposition 9.2 the greatest common divisor calculation looks complicated but in general S'' can be found with fewer terms than the 6 given.

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 be invoked.

Proposition 9.6. (Multiplication for Type I primes) *For $i = 1, 2$ let $I_i = [s_i, s'_i(u_i + \rho), v_i + w_i\rho + \omega]$ be two ideals. Then $I_1I_2 = (D)I_3$ where $I_3 = I'_1I'_2J$ and $D = D_1D_2D_3$ and these quantities are as follows:*

$$D_1 = \gcd(s'_2, s_1/s'_1, u_1 + Iw_2), \quad D_2 = \gcd(s'_1, s_2/s'_2, u_2 + Iw_1),$$

$$D_3 = \frac{\gcd(s'_1/D_2, s'_2/D_1)}{\gcd(s'_1/D_2, s'_2/D_1, w_1 - w_2)},$$

$$I'_1 = \left[\frac{s_1}{D_1D_2D_3}, \frac{s'_1}{D_2D_3}(u_1 + \rho), v_1 + w_1\rho + \omega \right],$$

$$I'_2 = \left[\frac{s_2}{D_1D_2D_3}, \frac{s'_2}{D_1D_3}(u_2 + \rho), v_2 + w_2\rho + \omega \right], \text{ and}$$

$$J = \langle D_3 \rangle \left(\overline{[D_3, D_3\rho, v_1 + w_1\rho + \omega]} \overline{[D_3, D_3\rho, v_2 + w_2\rho + \omega]} \right)^{-1},$$

and the last calculation is done by invoking Propositions 8.2, 8.11, and 9.2.

Proof. We factor I_1 and I_2 as in Proposition 8.8,

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

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:

$$I'_{1,2} = \left[\frac{s_1}{s'_1D_1}, u_1 + \rho, v_1 + w_1\rho + \omega \right], \quad I'_{1,1} = \left[\frac{s'_1}{D_2}, \frac{s'_1}{D_2}\rho, v_1 + w_1\rho + \omega \right]$$

$$I'_{2,2} = \left[\frac{s_2}{s'_2D_2}, u_2 + \rho, v_2 + w_2\rho + \omega \right], \quad \text{and} \quad I'_{2,1} = \left[\frac{s'_2}{D_1}, \frac{s'_2}{D_1}\rho, v_2 + w_2\rho + \omega \right].$$

The product I_1I_2 now has the form $(D_1D_2)I'_{1,1}I'_{1,2}I'_{2,1}I'_{2,2}$, and any remaining non-primitive 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 non-primitive product. However, the previous greatest common divisor contains too many primes. For a given prime P we need to be able to distinguish between $\mathfrak{p}q$ 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.

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

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 9.2. \square

The totally ramified primes will be much easier to deal with. For the two types, appealing to the propositions that govern their powers from Section 7 will be sufficient.

Proposition 9.7. (Multiplication for Type II primes) *For $i = 1, 2$ let $I_i = [s_i, s'_i(u_1 + \rho), v_i + w_i\rho + \omega]$ be two ideals such that $I_1I_2 = (D)I_3$ with $I_3 = I'_1I'_2J$ and $D = D_1D_2D_3$. These quantities are given as follows:*

$$D_1 = \gcd\left(\frac{s_1}{s'_1}, s'_2\right), \quad D_2 = \gcd\left(\frac{s_2}{s'_2}, s'_1\right), \quad D_3 = \gcd(s'_2, s'_1),$$

$$I'_1 = \left[\frac{s_1}{D_1D_2D_3}, \frac{s'_1}{D_2D_3}(u_1 + \rho), v_1 - w_1u_1 + \omega \right],$$

$$I'_2 = \left[\frac{s_2}{D_1D_2D_3}, \frac{s'_2}{D_1D_3}(u_2 + \rho), v_2 - w_2u_2 + \omega \right],$$

$$J = [D_3, f + \rho, I^{-1}f^2 + \omega],$$

with f satisfying $f^3 \equiv FI^2 \pmod{D_3}$.

Proof. Much like the previous proposition, the key is to 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. \square

Proposition 9.8. (Multiplication for Type III primes) *For $i = 1, 2$ let $I_i = [s_i, \rho, s''_i\omega]$ be two ideals such then $I_1I_2 = (D)I_3$. $I_3 = I'_1I'_2J$ and $D = D_1D_2D_3$ where these quantities are given as follows:*

$$D_1 = \gcd\left(\frac{s_1}{s''_1}, s''_2\right), \quad D_2 = \gcd\left(\frac{s_2}{s''_2}, s''_1\right), \quad D_3 = \gcd(s''_2, s''_1),$$

$$I'_1 = \left[\frac{s_1}{D_1D_2D_3}, \rho, \frac{s''_1}{D_2D_3}\omega \right], \quad I'_2 = \left[\frac{s_2}{D_1D_2D_3}, \rho, \frac{s''_2}{D_1D_3}\omega \right], \text{ and}$$

$$J = [D_3, \rho, \omega].$$

Proof. This follows in the same manner as the previous proof. \square

Proposition 9.9. (Multiplication for Type IV primes) 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. Then $I_1 I_2 = (D)I_3$ where

$$I_3 = I'_1 I'_2 J \text{ and } D = D_1 D_2 D_3 D_4 D_5 D_6 D_7.$$

These quantities are defined as follows:

$$\begin{aligned} D_1 &= \gcd(s''_2, s_1/s'_1 s''_1, v_1 - u_1 w_1), & D_2 &= \gcd(s''_1, s_2/s'_2 s''_2, v_2 - w_2 u_2), \\ D_3 &= \frac{\gcd(s_1/s'_1 s''_1, s''_2)}{\gcd(s_1/s'_1 s''_1, s''_2, v_1 - w_1 u_1)}, & D_4 &= \frac{\gcd(s_2/s'_2 s''_2, s''_1)}{\gcd(s_2/s'_2 s''_2, s''_1, v_2 - w_2 u_2)}, \\ D_5 &= \gcd(s'_1/D_4, s''_2/D_1), & D_6 &= \gcd(s'_2/D_3, s''_1/D_2), \\ D_7 &= \gcd\left(\frac{s''_2}{D_1 D_5}, \frac{s''_1}{D_2 D_6}\right) \end{aligned}$$

$$I'_1 = \left[\frac{s_1}{D_2 D_4 D_5 D_6 D_7}, \frac{s'_1}{D_4 D_5} \rho, \frac{s''_1}{D_2 D_6 D_7} (v_1 + w_1 \rho + \omega) \right],$$

$$I'_2 = \left[\frac{s_2}{D_1 D_3 D_5 D_6 D_7}, \frac{s'_2}{D_3 D_6} \rho, \frac{s''_2}{D_1 D_5 D_7} (v_2 + w_2 \rho + \omega) \right], \text{ and}$$

$$J = [D_5 D_6, \rho, \omega][D_7, \rho, \omega + E].$$

Proof. The proof follows in a similar manner as the previous three proofs. Again, we seek only to highlight the differences. We begin by factoring I_1 into three ideals as

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

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, $\mathfrak{p}\mathfrak{q}$). The product of $\mathfrak{q}^2 \mathfrak{p}\mathfrak{q}$ 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 $\mathfrak{p}\mathfrak{q}$ and therefore the product must be of the form $(P)\mathfrak{p}$. We get $(D_7)[D_7, \rho, \omega + E]$. \square

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]. Given an ideal $J = [s, s'(u + \rho), s''(v + w\rho + \omega)]$, we want to find an element in this ideal that has minimal norm. The existence of such an element (up to a constant scalar) is guaranteed by Theorem 6.3. Writing the ideal as a triangular matrix and assigning a weight to each column corresponding to the norm of the associated element, the algorithm proceeds to perform elementary row operations on the matrix to find an element of minimum weight.

$$\begin{array}{ccc} \left[\begin{array}{ccc} s & 0 & 0 \\ s'u & s' & 0 \\ s''v & s''w & s'' \end{array} \right] \\ \begin{array}{ccc} \uparrow & \uparrow & \uparrow \\ 3 * \deg FI^2 & 3 * \deg + \deg FI^2 & 3 * \deg + \deg F^2 I \end{array} \end{array}$$

By Theorem 6.1, the weights of distinct columns lie in distinct residue classes modulo three. If two rows have their weight coming from the same position it is possible to reduce the weight of one of the rows while still maintaining a basis for the ideal. The algorithm below just encodes the order in which to do the minimization.

Algorithm 1: MinElement

Input: Minimal Element Algorithm. Let $I = [s, s'(u + \rho), s''(v + w\rho + \omega)]$.

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

Precomputation: Use the ideal to define $b_1 = (b_{1,1}, b_{1,2}, b_{1,3}) = (s, 0, 0)$, $b_2 = (b_{2,1}, b_{2,2}, b_{2,3}) = (s'u, s', 0)$, and $b_3 = (b_{3,1}, b_{3,2}, b_{3,3}) = (s''v, s''w, s'')$. 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: $a + b\rho + c\omega \in \mathcal{O}_{\mathcal{F}}$

Output: A canonical basis of the ideal $I = \langle \alpha \rangle$.

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 and I_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. EXAMPLE COMPUTATION

We present an example to illustrate the algorithms. The field of constants is $\mathbb{F}_{3^{10}} = \mathbb{F}_3[\alpha]/(\alpha^{10} - \alpha^6 - \alpha^5 - \alpha^4 + \alpha - 1)$ and the cubic function field is $\mathbb{F}_{3^{10}}(x, y)$ where y is a root of $T^3 - T + x^4 + \alpha$. Since $A = 1$, this is an Artin-Schreier extension with no finite ramification. The infinite place is totally ramified and the genus of the function field is 3. We let

$$I_1 = [x, -\alpha^9 - \alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 - \alpha^4 - \alpha^3 + \rho, \alpha^8 - \alpha^6 - \alpha^5 + \alpha^4 - \alpha^3 + \alpha^2 + \omega]$$

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

Step 1. We calculate I_1^2 and I_1^3 followed by I_1^6 invoking Proposition 9.2 each time. We state only the parameters used to define I_1^6 which has the form $[s_2, u_2 + \rho, v_2 + \omega]$, where

$$s_2 = x^6, \quad u_2 = x^4 - \alpha^9 - \alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 - \alpha^4 - \alpha^3, \quad \text{and}$$

$$v_2 = (-\alpha^9 - \alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 - \alpha^4 - \alpha^3)x^4 - \alpha^8 + \alpha^6 + \alpha^5 - \alpha^4 + \alpha^3 - \alpha^2 - 1.$$

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, 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

$$\begin{aligned} a &= (\alpha^8 - \alpha^6 - \alpha^5 + \alpha^4 - \alpha^3 + \alpha^2 - 1)x^2 \\ b &= (\alpha^9 + \alpha^8 - \alpha^7 - \alpha^6 - \alpha^5 + \alpha^4 + \alpha^3)x^2 \\ c &= x^2 \end{aligned}$$

Step 4. Applying Algorithm 2 to the above parameters gives

$$\langle x^2 \rangle [x^4, x^4\rho, (\alpha^8 - \alpha^6 - \alpha^5 + \alpha^4 - \alpha^3 + \alpha^2 - 1) + (\alpha^9 + \alpha^8 - \alpha^7 - \alpha^6 - \alpha^5 + \alpha^4 + \alpha^3)\rho + \omega].$$

Step 5. Finally, we calculate $\langle \alpha \rangle / I_3$ according to Proposition 8.11. This has the form $[s_4, u_4 + \rho, v_4 + \omega]$ where

$$\begin{aligned} s_4 &= x^2, \\ u_4 &= -\alpha^9 - \alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 - \alpha^4 - \alpha^3, \\ v_4 &= \alpha^8 - \alpha^6 - \alpha^5 + \alpha^4 - \alpha^3 + \alpha^2. \end{aligned}$$

Note that this happens to be I_1^2 .

14. CONCLUSION

This work was chiefly motivated by two sources. First we wanted to find comparable results of [6, 10] in the characteristic 3 case. Given the history of the subject, it might have been sensible to attempt to compute fundamental units as in [11]. However, a naive approach with the integral basis given in Section 3 failed to work and we are currently investigating a solution. However, the second motivation was a generalization along the lines of Bauer's [1] computation in the ideal class group assuming the function field has a totally ramified infinite place is available. The material presented here is the subject of the second author's Ph.D. thesis.

REFERENCES

1. Mark L. 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, Universität 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. Helmut 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. Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996. MR 1376367 (97e:14035)
8. Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR 1876657 (2003d:11171)
9. Pieter Rozenhart and Renate 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, *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)
11. 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)
12. Renate Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 2, 609–631. MR 1879675 (2002k:11209)
13. Henning 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.

UNIVERSITY OF CALGARY, CALGARY AB T2L 1N4, CANADA

E-mail address: mbauer@math.ucalgary.ca

BATES COLLEGE, LEWISTON ME 04240, USA

E-mail address: jwebster@bates.edu