UNIVERSITY OF CALGARY

Cubic Function Fields in Characteristic Three

by

Jonathan Webster

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

January, 2010

THE UNIVERSITY OF CALGARY
FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Cubic Function Fields in Characteristic Three" submitted by Jonathan Webster in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY.

See attached Dr Bauer on sabbatical out-of-town

Supervisor, Dr. Mark Bauer
Department of Mathematics and Statistics

Dr. Renate Scheidler
Department of Mathematics and Statistics

Dr. Clifton Cunningham
Department of Mathematics and Statistics

Dr. Payman Mohassel
Department of Electrical and Computer Engineering

Dr. Rachel Pries
Department of Mathematics
(Colorado State University)

December 10th, 2009
Date

THE UNIVERSITY OF CALGARY
FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Cubic Function Fields in Characteristic Three" submitted by Jonathan Webster in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY.

Supervisor, Dr. Mark Bauer
Department of Mathematics and Statistics

Dr. Renate Scheidler
Department of Mathematics and Statistics

Dr. Clifton Cunningham
Department of Mathematics and Statistics

Dr. Payman Mohassel
Department of Electrical and Computer Engineering

Dr. Rachel Pries
Department of Mathematics
(Colorado State University)

December 10th, 2009
Date

Abstract

One of the central problems in computational algebraic number theory is the computation of certain invariants of a field and its maximal order. In this thesis, we consider the field in question to be a cubic function field $\mathcal{F}/\mathbb{F}_q(x)$, with $\mathrm{char}(\mathcal{F}) = 3$. We develop the arithmetic on the ideals of the maximal order $\mathcal{O}$ of K.

In previous work in characteristic greater than three, ideal arithmetic was given only in so far as it aided in infrastructure computations. However, in 2004 Bauer [3] gave algorithms for doing arithmetic in the ideal class group of a purely cubic funtion field with a totally ramified place at infinity. Landquist [21] generalized his results by considering singular curves. This shows that ideal arithmetic in a cubic extension of the rational function field in charactersitic three is similar to the previous work.

Acknowledgments

I am deeply indebted to my advisor, Professor Mark Bauer for his time and effort in reviewing this thesis. Whether it has been the hours spent reviewing this thesis, or advice on professional and technical matters, he has been a phenomenal advisor. I have learned a lot from him and can only hope to emulate him as a mathematician and writer. My thanks go to him and Renate Scheidler for introducing me to the topic contained in this thesis. Further, I thank Andreas Stein for introducing me to the researchers at the University of Calgary.

I thank the members of my committee Mark Bauer, Renate Scheidler, Clifton Cunningham, Payman Mohassel, and Rachel Preis for their review of my work. I am especially grateful for Renate Scheidler's careful reading of my thesis.

Along with the aforementioned professors, I also am grateful for discussions of function fields and number theory with Hugh Williams, Mike Jacobson, Qingquan Wu, Pieter Rozenhart, Felix Fontein, Matt Greenberg, Eric Landquist, Andrew Shallue, and Tim Kilbourn.

I thank my new colleagues at Bates College for supporting and encouraging me. Chip Ross and Meredith Greer both volunteered to take my teaching responsibilities so I could travel to defend.

Thanks also to my parents for their continual support. Most of all, special thanks go to my wife, Karen. I do not know what I would do without her support, love, and encouragement. She is more than I deserve.

Highest thanks and praise to Jesus Christ for without Him nothing is possible. *Soli Deo Gloria.*

Table of Contents

Chapter 1

Introduction

Calculating certain invariants of a field and its maximal order remains one of the central problems in computational algebraic number theory. Henri Cohen wrote two excellent books [6, 7] on computational algebraic number theory that provide a good overview of the tools one needs for this research area. In the second book, Cohen states of the work done for number fields that "it is important and natural to generalize these algorithms. Several generalizations can be considered, but the most important are certainly generalizations to global function fields." This thesis contributes to this theme of generalizations by considering cubic function fields in characteristic three. In particular, we give algorithms to perform arithmetic in the Jacobian of any cubic function field of characteristic three with a totally ramified infinite place. In this introduction we will give a brief history of algebraic curves and the number theory considered in this thesis. We will show how this work fits into the current body of literature and provide an outline of the main results proved.

1.1 History and Motivation

We can trace the study of algebraic curves back to the ancient Greeks. They were the first to study conic sections, i.e. curves of the form $C : a_1y^2 + (a_2x + a_3)y + a_4x^2 + a_5x + a_6 = 0$, where $a_i \in k$ for some field k and at least one of a_1 or a_4 is nonzero. In the 4th century BC, Menaechmus is credited with discovering conic sections. He

used hyperbolas and parabolas to "solve" the problem of doubling the cube and his brother used similar methods to "solve" the problem of doubling the square. The solution methods violate the straight edge and compass rules but this only provided more motivation to find further solutions [4, pg. 93-97]. Later Euclid wrote on conic section in his famous *Elements*. Archimedes found engineering applications to the study of conic sections and also contributed to theoretical results.

During the Renaissance, astronomers, mathematicians, and scientists continued to study conic sections for applications to their fields. Kepler formulated laws of planetary motion and Newton in his *Philosphiae Naturalis Principia Mathematica* gave a geometric derivation of Kepler's laws. In his *Enumeratio linearum tertii ordinis* Newton went on to study *cubic plane curves* [4, pg. 410], which have the form $C : a_1y^3 + (a_2x + 3_3)y^2 + (a_4x^2 + a_5x + a_6)y + a_7x^3 + a_8x^2 + a_9x + a_{10} = 0$ with $a_i \in k$ and at least one of a_1 or a_7 nonzero. *Elliptic curves*, which may be written in *Weierstrass form* as $C : y^2 + (a_1x + a_2)y = x^3 + a_2x^2 + a_4x + a_6$ where $a_k \in k$ and there is no point on the curve for which both partial derivatives simultaneously vanish, are a subset of these curves of particular interest to us. These curves arose from the problem of computing the arc length of an ellipse.

While much could be written about elliptic curves, we will only highlight a few important points that relate to this thesis. In 1936 Hasse considered elliptic curves defined over a finite field $\mathbb{F}_q$. He showed that the number of points, (a, b) with $a, b \in \mathbb{F}_q$, on the curve lies in an interval centered at $q + 1$ of length $4\sqrt{q}$ [14]. The points on this curve, along with a "point at infinity", form a group and the group law is given by the chord-tangent and chord-secant construction.

We can consider a natural generalization of elliptic curves by studying $C : y^2 +$

$h(x)y = f(x)$, where $h(x), f(x) \in \mathbb{F}_q[x]$. With suitable restrictions on $h(x)$ and $f(x)$ these curves are called *hyperelliptic curves* (for a precise definition of a hyperelliptic curve, see [17]) and elliptic curves are just a special case of hyperelliptic curves. There is a group associated to these curves called the *Jacobian* of C, denoted $\mathcal{J}_C$. For elliptic curves the group law was relatively simple. However, for these higher genus curves, the Jacobian does not admit the simple isomorphism between itself and the points on the curve. It will still be possible to perform computations by considering the *divisor class group*, and a related group, the *ideal class group*. Weil was able to generalize Hasse's Thereom and prove $(\sqrt{q}-1)^{2g} \leq h \leq (\sqrt{q}+1)^{2g}$, where $h = |\mathcal{J}_C(\mathbb{F}_q)|$.

We can also consider the *function field* of C,

$$F = \mathbb{F}_q(C) = \mathbb{F}_q(x)[y]/(y^2 + h(x)y - f(x)).$$

For hyperelliptic curves, Cantor [5] was the first to derive explicit arithmetic in $\mathcal{J}_F(\mathbb{F}_q)$, where the subscript denotes dependence upon the function field F. Characteristic two poses some minor problems but these extensions are Artin-Schreier extensions (assuming the extension is separable). Zuccherato [39] was one of the first to provide a comprehensive treatment of hyperelliptic curves in characteristic two. This thesis will attempt to do something comparable by generalizing certain work in cubic function fields to characteristic three.

Applications to cryptography and coding theory drives much of the modern interest in function fields. Goppa was the first to use function fields as an application to error correcting codes [12]. Later, Koblitz and Miller independently proposed that elliptic curves defined over a large finite field could be used for public key cryptography [18, 26]. The fast arithmetic and small key size has made elliptic curves an increasingly popular choice for public key cryptography and the subject of intense scrutiny.

Koblitz also proposed hyperelliptic curves for use in public key cryptography by using the arithmetic in the divisor class group of a hyperelliptic curve [19]. When $g = 2$ these proposed systems appear to be just as secure as elliptic curve based cryptosystems. Unfortunately, their arithmetic is more complex and is typically slower.

While cryptography certainly motivates research in cubic function fields, it is unlikely that these fields will be used in any cryptographic scheme. As above, the arithmetic is expected to be more complex than its elliptic or hyperelliptic counterparts. A bigger concern is that we do not have the same security results if the genus of these curves is greater than two; the underlying problem can almost always be solved faster than the problem on curves of genus one and two [11, 37]. Current methods for solving the discrete log problem exploit the fact that the higher genus provides more structure, so it is reasonable to believe that an attack against low genus curves could be modified to apply to the higher genus curves as well. Also, any cubic function field of genus one (resp. two) corresponds to an elliptic (resp. hyperelliptic) curve and it would be more efficient to use this model.

The primary motivation for work on cubic function fields comes from a more number theoretic perspective. To show this motivation, we will consider some common features of function fields and of number fields, which are finite extensions of the field of fractions of $\mathbb{Z}$, that is of $\mathbb{Q}$. We consider $F = \mathbb{Q}(\alpha)$ where α is the root of some monic irreducible polynomial over $\mathbb{Q}$ and this mirrors the situation with function fields, i.e. we have considered the field of fractions of $\mathbb{F}_q[x]$ and adjoined a root of a monic irreducible polynomial over $\mathbb{F}_q(x)$ (as in the hyperelliptic curve case above). These extension fields are called *global fields* and often their properties can be studied in a unified manner. If F is a global field, then its maximal order is the integral

closure of its base ring ($\mathbb{Z}$ or $\mathbb{F}_q[x]$) in F and is written $\mathcal{O} = \mathcal{O}_F$. We can define an equivalence relation on ideals of $\mathcal{O}_F$ to form the *ideal class group* which is denoted $Cl(\mathcal{O}_F)$. This is a finite Abelian group whose order is called the *ideal class number.* The ideal class group is related to the divisor class group by an exact sequence. In special cases and the case that will be the predominant focus of this thesis we have $Cl(\mathcal{O}_F) \cong \mathcal{J}_F(\mathbb{F}_q)$.

The problem of calculating class numbers originated with Gauss in his famous *Disquistiones Arithmeticae.* He discussed the problem of finding the class number of quadratic extensions using binary quadratic forms. His work continues to motivate number theorists. Günther Frei wrote a nice summary of the possible influence a posthumously published portion of Gauss's work has had on function fields [10]. There are a few natural approaches to generalizing his work. One approach is to consider quadratic extensions of function fields. Artin generalized Gauss' work to quadratic extensions of function fields (ignoring $\mathrm{char}(K) = 2$) [1]. Later, Artin and Schreier handled the case of $\mathrm{char}(K) = 2$ [2]. Having generalized Gauss' work to function fields, another approach would be to examine cubic extensions. Cubic number fields were studied first, and in 1962 Delone and Faddeev published a comprehensive study of cubic number fields [9]. Current research on cubic function fields expands on this work.

1.2 Cubic Function Fields

The first significant work on cubic function fields was that of Mang [25]; it mirrored results from cubic number fields and the primary goal was the calculation of fundamental units. The technique Mang used was based on the Pohst-Zassenhause

method for number fields [27] and, by his own admission, was infeasible. Scheidler and Stein [33] took a different approach. Following the work of Williams, et al. [38], they adapted Voronoi's Algorithm [9] to work in purely cubic function fields. Computationally, this was a significant improvement over Mang. In a later paper [34], Scheidler and Stein improve on their earlier work of [33]. Mang gave explicit criterion to construct a purely cubic function field of unit rank 0, 1, or 2, while [33] provides the signature of the function field. Scheidler gave an explicit treatment of the construction of prime ideals and their powers along with an ideal multiplication algorithm [31]. The paper continued by showing how it is possible to perform computations in the infrastructure. There is still a lot of ongoing work on cubic function fields. Scheidler and Stein gave improved algorithms to find the class number [35]. Scheidler and other authors considered arbitrary (as opposed to purely) cubic function fields [32, 22]. Pieter Rozenhart has tabulated cubic function fields of bounded discriminant [30].

Much of the above work closely mirrors the research on cubic number fields and often even focuses on the unit rank one case. In 2004 Mark Bauer considered a case uniquely dissimilar to number fields by considering purely cubic function fields of unit rank zero [3]. One pragmatic difference is in ideal arithmetic. In the earlier work of Scheidler [31] ideal multiplication can be assumed to operate on ideals whose norms were relatively prime. For the unit rank one case, which was the concern of the paper, this criterion is easily met. However, when turning our attention to the unit rank zero case, it is no longer possible to guarantee this. Inspired by divisor arithmetic for hyperelliptic curves, Bauer gives composition and reduction algorithms and thus a way of doing group operations in the ideal class group. While Bauer's work assumed

that the curve was nonsingular, he knew this was an unnecessary restriction and had an unpublished set of notes outlining arithmetic for singular curves. Landquist [21] proved the results and states algorithms for computations in the ideal class group of any purely cubic function field of unit rank zero.

The previous work on cubic function fields assumes that the underlying finite field has characteristic different from three (and usually different from two). This thesis considers cubic function fields in characteristic three. We follow the lead of Bauer and consider unit rank zero fields and develop arithmetic in the ideal class group. The rationale for this approach is that in order to handle a higher unit rank, one must already be able to do arithmetic on ideals. In the above work on cubic function fields, the authors relied on the analogy between number fields and function fields which is so close that ideal arithmetic and integral basis calculations remained nearly unchanged. Since no work has been done in characteristic three, the development of ideal arithmetic is a necessary pre-requisite to doing computations in arbitrary cubic function fields in characteristic three. We consider $y^3 - A(x)y + B(x) = 0$ and show that this corresponds to an aribrary cubic function field. We show how the places split which allows us to compute the genus and give explicit forms for the ideals in terms of an integral basis for the maximal order. This allows us to do arithmetic in the ideal class group.

Chapter 2

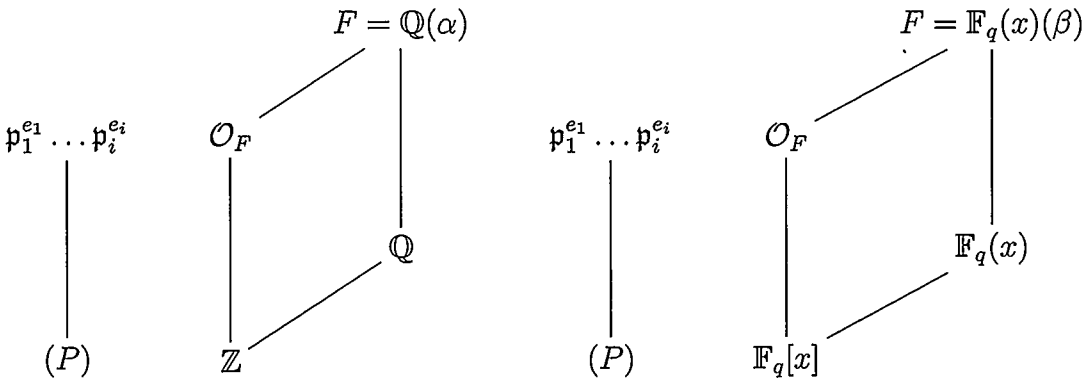
Preliminaries

Chapter one provided historical context and recent research that motivates this thesis. It glossed over much of the mathematical detail in the latter portion to have a more cohesive narrative. This chapter rectifies this by providing the reader with an overview of function fields and establishing the notation that will be used in the remainder of the thesis. We assume the reader is familiar with field theory, Galois theory, and introductory algebraic number theory, which is the typical starting point for introductory texts on function fields. Stichtenoth's *Algebraic Function Fields and Codes* [36] or Rosen's *Number Theory in Function Fields* [28] are both excellent texts to consult. Hasse's treatment [15] of the subject also is very good for seeing the deep connection between function fields and number fields. Lastly, Lorenzini's *An Invitation to Arithmetic Geometry* is a good text to see the connections to algebraic geometry from a classical point of view.

The first section defines an algebraic function field and gives a few examples. Section 2.2 defines places, a key object to study function fields, and the following section quickly reviews properties of the ring of integers. Section 2.4 relates the two previous sections by discussing how the ideal class group is related to the points on the Jacobian. Finally, Section 2.5 discusses two concepts motivated by algebraic geometry: singularity and genus.

2.1 Function Fields

The following diagram provides a better start than a theorem or definition. It compares the typical objects of study in number fields to their analogous counterparts in function fields.



On the left we have $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$. Adjoin to $\mathbb{Q}$ a root, α, of some monic irreducible polynomial over $\mathbb{Q}(x)$ and consider the resulting field extension along with its ring of integers, $\mathcal{O}_F$. The rational primes in $\mathbb{Z}$ all exhibit some sort of splitting behavior in $\mathcal{O}_F$. This picture should be very familiar from an introductory text on number fields and the same picture is true for function fields. This picture serves to highlight the analogy between function fields and number fields. The remainder of the chapter will flesh out this analogy more fully. Special care will be taken in presenting material in which there are key differences between function fields and number fields. Where the mathematics remains unchanged we cover material at a quicker pace.

Definition 2.1.1 (Definition I.1.1 of [36]). *Let k be a field. An* algebraic function field F/k of one variable over k *is an extension field $F \supseteq k$ such that F is a finite*

algebraic extension of $k(x)$ for some element $x \in F$ which is transcendental over k.

The simplest example of an algebraic function field is the rational function field, $K = \mathbb{F}_q(x)$. Other algebraic function fields are finite algebraic extensions of the rational function field, i.e. $F = K(y) = \mathbb{F}_q(x, y)$ where $\phi(y) = 0$ for some monic irreducible polynomial $\phi(T) \in \mathbb{F}_q(x)[T]$. If $\phi(T)$ remains irreducible in $\overline{\mathbb{F}}_q$ then $\phi(T)$ is said to be *absolutely irreducible.* The algebraic closure of $\mathbb{F}_q$ in F is called the *constant field* and is denoted $\tilde{\mathbb{F}}_q$. If $\tilde{\mathbb{F}}_q = \mathbb{F}_q$ then the finite field is called the *full constant field* of F. Here is the first departure from the number field situation because there is no corresponding notion of a constant field extension. It is easy to create examples of extensions that result in constant field extensions.

Example 2.1.1. *Consider $F = \mathbb{F}_3(x, y)$ where y is a root of $T^2 + (x-1)^2 \in \mathbb{F}_3(x)[T]$. Since -1 is not a square in $\mathbb{F}_3$, the quadratic extension given by adjoining y to $\mathbb{F}_3(x)$ is $K = \mathbb{F}_9(x)$.*

We will ignore such extensions by assuming our finite field is the full constant field. We do this because finite field extensions are well understood. It may not be possible to determine whether the base field is the full constant field in general. The following theorem relates the two notions discussed above.

Theorem 2.1.1 (Corollary III.6.7 of [36]). *If $F = \mathbb{F}_q(x, y)$ is a function field and $\phi(x, T) \in \mathbb{F}_q(x)[T]$ is the minimal polynomial of y over $\mathbb{F}_q(x)$, then $\phi(x, T)$ is absolutely irreducible if and only if $\mathbb{F}_q$ is the full constant field of F.*

Since the primary concern of this thesis is cubic function fields in characteristic three, we give two classes of examples of such fields. Both examples are p-extensions in characteristic p and are well understood. The first class of examples are the Artin-Schreier extensions. These are the characteristic p Galois p-extensions. The second

class of examples are purely inseparable extensions. They are described here to illustrate why they are uninteresting from a theoretical perspective.

Example 2.1.2 (Artin-Schreier Extensions, Proposition III.7.8 of [36]). *Let $\mathbb{F}_q$ be a field of characteristic p and $u \in \mathbb{F}_q(x)$ an element such that there is no $\omega \in \mathbb{F}_q(x)$ satisfying $\omega^p - \omega = u$. Then the Artin-Schreier extensions are given by $F = \mathbb{F}_q(x, y)$ with y a root of $T^p - T - u = 0$.*

Any cyclic p-extension in characteristic p is an Artin-Schreier extension. The next chapter considers arbitrary cubic function fields in characteristic three and it will be helpful to know when an extension is an Artin-Schreier extension. In that chapter we will see that a curve of the form $T^3 - A(x)T + B(x) = 0$ gives rise to an Artin-Schreier extension if and only if $A(x)$ is a square.

Example 2.1.3 (Purely Inseparable Extensions, Proposition III.9.2 of [36]). *Let $\phi(T) = T^p - u$ be absolutely irreducible with $u \in \mathbb{F}_q(x)$ and $\mathrm{char}(\mathbb{F}_q) = p$. The purely inseparable extensions are given by $\mathbb{F}_q(x, y)$, where y satisifies $\phi(y) = 0$.*

Such extensions are foreign to number fields since they can only arise in positive characteristic. Unfortunately, that does not make them interesting to study; they are isomorphic to the rational function field. Since these extensions only arise with the stated polynomial, we will exclude these polynomials from our discussion in the next chapter. By doing so, chapter three considers only separable extensions.

2.2 Places

A survey of the literature of function fields and number fields reveals a semantic difference. Studying number fields, we tend to speak of ideals and when studying function fields we tend to speak of places. Accounts that seek to unify the treatment

of function fields and number fields will use the language of places and valuations. We follow this approach.

Definition 2.2.1. *A* place, *P, of a function field $F/\mathbb{F}_q$ is the unique maximal ideal of some discrete valuation ring $\mathcal{O}_P \subset F$.*

The set of places will be denoted $\mathbb{P}_F$. The ring $\mathcal{O}_P$ is a principal ideal domain; therefore, we can write $P = \wp\mathcal{O}_P$ for some $\wp \in \mathcal{O}_P$. The element $\wp$ is a *prime element* (or a *uniformizing element*) and defines the discrete valuation associated to $\mathcal{O}_P$. For any element $\alpha \in F^\times$, it is possible to write $\alpha = \wp^n u$ for some $u \in \mathcal{O}_P^\times$, $n \in \mathbb{Z}$; the valuation of α is $v_P(\alpha) = n$. The *degree* of a place P, denoted $\deg(P)$, is the degree of the extension $[\mathcal{O}_P/P : \mathbb{F}_q]$.

2.2.1 Places of $\mathbb{F}_q(x)$

To harken back to the analogy with number fields, we recall that prime numbers give rise to the prime ideals in $\mathbb{Z}$. The prime numbers are characterized by their divisibility property which is best understood as the property of being irreducible in the ring. It is possible to similarly characterize most of the places of the rational function field $\mathbb{F}_q(x)$. The *finite places* are associated to monic irreducible polynomials $\wp(x) \in \mathbb{F}_q[x]$. Let P be the place associated to $\wp(x)$. The maximal ideal and valuation ring are given by

$$P = \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{F}_q[x], \wp(x) \mid f(x), \wp(x) \nmid g(x) \right\}$$

and

$$\mathcal{O}_P = \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{F}_q[x], \wp(x) \nmid g(x) \right\}.$$

Given these characterizations for P and $\mathcal{O}_P$, it is possible to deduce that $P = \wp(x)\mathcal{O}_P$ and $\deg(P) = \deg(\wp(x))$.

As with the number field case, the finite places do not give all possible valuations. The remaining place to consider is the infinite place of $\mathbb{F}_q(x)$. Unlike the number field case, the infinite place here still gives rise to a discrete valuation ring. The *infinite place* is denoted ∞ and it has uniformizing element $1/x$. Its maximal ideal and valuation ring are given by

$$\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in \mathbb{F}_q[x], \deg f(x) < \deg g(x) \right\}$$

and

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in \mathbb{F}_q[x], \deg f(x) \leq \deg g(x) \right\}.$$

For the infinite place, $\infty = \frac{1}{x}\mathcal{O}_\infty$ and by definition $\deg(\infty) = 1$. Since each place corresponds to a prime element, we will use the terms interchangeably.

2.2.2 Places in Extensions of $\mathbb{F}_q(x)$

Having characterized all the places of the rational function field we recall the analogy with number fields and discuss how these places behave in algebraic extensions. There are typically two separate treatments of how places of $\mathbb{Q}$ behave in a number field. The splitting of prime ideals in number fields is often disjoint from determining the unit rank. Places allow the treatment of these topics to be unified, as the unit rank is associated with the infinite place. The invariants that relates places in $\mathbb{F}_q(x)$ to places in $\mathbb{F}_q(x, y)$ are the same invariants from number fields. We state them briefly, establish the notation, and highlight a few differences.

Definition 2.2.2. *Let* $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q(x,y)}$ *and* $P \in \mathbb{P}_{\mathbb{F}_q(x)}$. *Then* $\mathfrak{p}$ *is said to* lie over P *if*

$P = \mathfrak{p} \cap \mathbb{F}_q[x]$ *and denote this* $\mathfrak{p}|P$.

The *ramification index*, $e(\mathfrak{p}|P)$, is the integer that satisfies $v_{\mathfrak{p}}(\alpha) = e(\mathfrak{p}|P)v_P(\alpha)$ for all $\alpha \in \mathbb{F}_q(x,y)^\times$. The *inertia degree* is $[\mathcal{O}_{\mathfrak{p}}/\mathfrak{p} : \mathcal{O}_P/P]$ and is denoted $f(\mathfrak{p}|P)$.

If $\text{char}(\mathbb{F}_q)$ divides $e(\mathfrak{p}|P)$, then that the place is said to be *wildly ramified.* This definition differs from the definition from number fields. Note that wild ramification is total ramification for p-extensions in characteristic p. An extension is *wildly ramified* if it has a wildly ramified place, otherwise it is a *tame* extension.

In Chapter three, we expect wild ramification to occur and this will play a key role in how the Hurwitz Genus Formula behaves. We will see in Section 2.5 that for tame extensions, different exponents are easily determined from the ramification index. However, the ramification index only serves as a lower bound for the different exponent of a wildly ramified place. One last difference is that some function field extensions can have no ramification and these are called *unramified* extensions. While relative extensions of number fields may be unramfied, any extension of $\mathbb{Q}$ is a ramified extension. An example of an unramified function field extension is an Artin-Schreier extension with $u \in \mathbb{F}_q[x]$.

A famous result for number fields relating ramification degree, inertial degree, and extension degree is also true for function fields.

Theorem 2.2.1 (Theorem III.1.11 of [36]). *Let* $F = \mathbb{F}_q(x)$, $P \in \mathbb{P}_{\mathbb{F}_q(x)}$, $\mathfrak{p}_i \in \mathbb{P}_F$ *for* $1 \leq i \leq n$ *be the places over* P, $e_i = e(\mathfrak{p}_i|P)$, *and* $f_i = f(\mathfrak{p}_i|P)$. *Then*

$$\sum_{i=1}^{n} e_i f_i = [F : \mathbb{F}_q(x)].$$

For each extension degree, this gives a finite number of possibilities for the splitting behavior. The ordered tuple sorted lexicographically $(e_1, f_1; e_2, f_2; \ldots; e_n, f_n)$ is the *P-signature* of a place. There are five possible cases for cubic extensions: $(1,3)$, $(3,1)$,

$(1,2;1,1)$, $(2,1;1,1)$, and $(1,1;1,1;1,1)$. The *signature* of a function field is just the signature of the infinite place. This is another key point that function fields differ from their number field analogue. The place at infinity can have arbitrary splitting type for a function field, but for a number field the infinite places have $e_i = 1$ and $f_i = 1$ or 2.

2.2.3 Determining P-Signatures

The primary tool to determine P-signatures is Kummer's Theorem. For all but a finite number of places, the theorem will completely determine the P-signature.

Theorem 2.2.2 (Kummer's Theorem, Theorem III.3.7 of [36]). *Let $F = \mathbb{F}_q(x,y)$ be a function field where $\phi(y) = 0$, $\phi(T) \in \mathcal{O}_P[T]$ is an absolutely irreducible monic polynomial, and $P \in \mathbb{P}_K$. Let*

$$\phi(T) \equiv \prod_{i=1}^{r} \phi_i(T)^{\epsilon_i} \pmod{P}$$

be the factorization of $\phi(T)$ into irreducible polynomials modulo P. Then the number of places $\mathfrak{p}_i|P$ is at least r, $f(\mathfrak{p}_i|P) \geq \deg \phi_i(T)$, and $e(\mathfrak{p}_i|P) \leq \epsilon_i$.

In many cases the inequalities in Kummer's Theorem may be replaced by equalities. If a place is not associated to a singular point (singularity will be discussed in section 2.5) then Kummer's Theorem gives equalities. For now, it is sufficient to know that almost every place is nonsingular; therefore, Kummer's Theorem will completely determine the P-signature for almost all places. When Kummer's Theorem fails to completely determine the signature, we have a few options. Applying the theorem to a different curve that gives rise to the same extension can often resolve the problem. For background on changing curves and a more geometric view of function fields, see Appendix B of [36], or [24]. Appealing to certain completions can also resolve the

problem. While the following theorem applies to any place, we will only invoke this theorem to determine the signature of the function field.

Theorem 2.2.3. *[Theorem 3.1 of [22]] Let $F = \mathbb{F}_q(x,y)$ be an algebraic function field, where $\phi(x,y) = 0$ and $\phi(T) \in \mathbb{F}_q[x][T]$ is a monic polynomial that is irreducible over $\mathbb{F}_q(x)$. Let P be any place of $\mathbb{F}_q(x)$, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ the places of F lying above P, and write $e_i = e(\mathfrak{p}_i|P)$, $f_i = f(\mathfrak{p}_i|P)$, and $n_i = e_i f_i$ for $1 \leq i \leq r$. Then there exists an enumeration of the roots $y^{(0)}, y^{(1)}, \ldots, y^{(n-1)}$ of $\phi(T)$ as*

$$(y^{(0)}, y^{(1)}, \ldots, y^{(n-1)}) = (y_{1,1}, \ldots, y_{1,n_1}, y_{2,1}, \ldots, y_{2,n_2}, \ldots, y_{r,1}, \ldots, y_{r,n_r})$$

so that $y_{i,j}$ lies in an extension E of $\bar{\mathbb{F}}_q\langle P\rangle$ of degree e_i, but in no proper subfield of E, for $1 \leq j \leq n_i$, and $1 \leq i \leq r$. If $e_i = 1$ for some $i \in \{1,2,\ldots,r\}$, then $y_{i,j} \in \mathbb{F}\langle P\rangle$ for $1 \leq j \leq n_i$, where $\mathbb{F}$ is an extension of degree at most f_i of $\mathbb{F}_{q^{\deg(P)}}$.

2.2.4 Divisor Class Groups and Jacobians

The goal is to develop arithmetic on the points of the Jacobian of a curve. The Jacobian of a curve is a g-dimensional abelian variety, where g is the genus of the curve. For elliptic curves, the Jacobian is isomorphic to the curve itself and thus arithmetic on the Jacobian is equivalent to arithmetic on the points of the elliptic curve. For higher genus curves this description becomes more complex. Having defined places, we are now in a position to define certain groups that will lead to a particular group that is isomorphic to the points on the Jacobian of the curve. Under another assumption, the points of the Jacobian will be isomorphic to the ideal class group of the function field. We will give algorithms to do arithmetic here.

Definition 2.2.3. *The* divisor group of F, *denoted $\mathcal{D}_F$, is the free abelian group generated by the places of F.*

Elements of this group are called *divisors* and are formal sums of places. In other words we can write a divisor D as

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ with } n_P \in \mathbb{Z}, \text{ almost all } n_P = 0.$$

The *support* of D is $supp\ D = \{P \in \mathbb{P}_F | n_P \neq 0\}$. If we let $S \subseteq \mathbb{P}_F$ then we will use the notation $\mathcal{D}_F(S)$ to denote the subgroup of of divisors of $\mathcal{D}_F$ that have support in S:

$$\mathcal{D}_F(S) = \{D \in \mathcal{D}_F \mid supp\ D \in S\} = \{D \in \mathcal{D}_F \mid D = \sum_{P \in S} n_p P\}.$$

If a divisor $D = P$ for some $P \in \mathbb{P}_F$ then the divisor is *prime*. Since prime ideals in $\mathcal{O}_F$ are in one-to-one correspondence with finite places it will often be convenient to consider S as above corresponding only to the finite places. The *finite part* of a divisor is the sub-sum of the divisor with support only in the finite places. The *degree* of a divisor is $\deg D = \sum_{P \in \mathbb{P}_F} n_P \deg(P)$ and this yields a homomorphism $\deg : \mathcal{D}_F \to \mathbb{Z}$. Using the degree map we can define

$$\mathcal{D}_F^0 := \{D \in \mathcal{D}_F \mid \deg D = 0\}$$

which is the divisor group of degree zero. To any $\alpha \in F^\times$ we can associate a *principal divisor* by $(\alpha) = \sum_{P \in \mathbb{P}_F} v_P(\alpha) P$. Every principal divisor has degree zero. The set

$$\mathcal{P}_F := \{(\alpha) \mid \alpha \in F^\times\}$$

forms the group of principal divisors and it is also a subgroup of both $\mathcal{D}_F$ and $\mathcal{D}_F^0$. The *divisor class group of degree zero* which is the quotient $\mathcal{D}_F^0/\mathcal{P}_F$ is a finite Abelian group. The points on the *Jacobian* of F are isomorphic to $\mathcal{D}_F^0/\mathcal{P}_F$.

This should also highlight why this structure might be closely related to the ideal class group. Both look like a particular set modulo a "principal" set. Since the

nonzero prime ideals are in one-to-one correspondence with the finite places, this should help see how the numerators of the quotient groups are going to be related.

2.3 Ring Extensions and Ideals

Given the great similarity between function fields and number fields when viewed from an algebraic perspective, we briefly review familiar topics of integral closure, integral basis, norm, and discriminant. This will serve as preparation for the definition of the ideal class group.

2.3.1 Ring of Integers

The first section discussed function fields qua fields. However, the diagram that we opened with suggests that the underlying ring structure is an important object of study. As before, let $F = \mathbb{F}_q(x, y)$ where y is a root of a monic absolutely irreducible polynomial $\phi[T] \in \mathbb{F}_q[x][T]$ and $n = [F : \mathbb{F}_q(x)]$.

Definition 2.3.1. *The* ring of integers *or* maximal order *of F is the integral closure of $\mathbb{F}_q[x]$ in $F = \mathbb{F}_q(x, y)$ and is denoted $\mathcal{O}_F$.*

It is often helpful to think of $\mathcal{O}_F$ as $\mathbb{F}_q[x][y]$. Much like the number field case there are times when $\mathcal{O}_F = \mathbb{F}_q[x][y]$. In the case that they are not equal then $\mathbb{F}_q[x][y]$ is a proper subset of $\mathcal{O}_F$ and is called a non-maximal order. In Section 2.5 we will see that $\mathcal{O}_F = \mathbb{F}_q[x][y]$ if and only if the affine curve $\phi(x, y) = 0$ has no singular points. An *integral basis* of F is an $\mathbb{F}_q[x]$-basis of $\mathcal{O}_F$.

The discriminant is one of the most important invariants of a function field that is associated to its ring of integers. To define it we first need to recall that any root y of $\phi(x)[T]$ has $n - 1$ conjugates $y^{(1)}, y^{(2)}, \ldots, y^{(n-1)}$ which are the other $n - 1$

roots of the minimal polynomial. This can be extended to an arbitrary element of F to speak of the conjugates of $\alpha \in F$ as $\alpha = \alpha^{(0)}, \alpha^{(1)}, \ldots, \alpha^{(n-1)}$ by realizing that $\alpha = a_0 + a_1 y + a_2 y^2 + \ldots + a_{n-1} y^{n-1}$ with $a_0, \ldots, a_{n-1} \in \mathbb{F}_q(x)$ and applying the conjugate map to each term in the sum.

Definition 2.3.2. *Let $\{\beta_1, \ldots, \beta_n\}$ be an integral basis of F. The* discriminant of F *(or the* field discriminant*) is*

$$\Delta(F) = \Delta(\beta_1, \beta_2, \ldots, \beta_n) = \begin{vmatrix} \beta_1 & \beta_1^{(1)} & \beta_1^{(2)} & \cdots & \beta_1^{(n-1)} \\ \beta_2 & \beta_2^{(1)} & \beta_2^{(2)} & \cdots & \beta_2^{(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_n & \beta_n^{(1)} & \beta_n^{(2)} & \cdots & \beta_n^{(n-1)} \end{vmatrix}^2 .$$

The discriminant of F is an important quantity that encodes information about ramification of ideals. Related to the discriminant of F is the discriminant of $\alpha \in \mathcal{O}_F$ which is

$$\Delta(\alpha) = \Delta(\alpha, \alpha^{(1)}, \ldots, \alpha^{(n-1)}).$$

The discriminant of an element relates to the field discriminant by $\Delta(\alpha) = I_\alpha^2 \Delta(F)$ for some $I_\alpha \in \mathbb{F}_q[x]$ and I_α is called the *index of* α. The discriminant and the index are only unique up to a square factor in $\mathbb{F}_q^\times$. We will often abuse language and speak of "the discriminant" and "the index" when referring to the discriminant of F and the index of y where the extension is generated as $\mathbb{F}_q(x, y)$. Index divisors are the typical primes for which Kummer's theorem will not completely determine the P-signature. In cubic number fields, there exist *common inessential discriminant divisors* which are primes that divide the index of any element. Fortunately, only finitely many primes P can be common inessential discriminant divisors; they have to satisfy $p < [F : K]$. Only the prime 2 can be one in a cubic number fields. The corresponding theorem

for function fields states $q^{\deg P} < [L : K]$ which means that only cubic function fields defined over $\mathbb{F}_2$ can have these primes P. Hence, this phenomenon will not happen in Chapter 3.

We know that $\mathbb{F}_q^\times$ is the set of units of $\mathbb{F}_q[x]$. Calculating the set of units for a generic ring of integers $\mathcal{O}_F$ is often not so easy. However, we can easily tell the structure of the group of units. In 1903, Kuhne proved the function field analogue of Dirchlet's Unit Theorem [20].

Theorem 2.3.1. *Let F and $\mathcal{O}_F$ be as above and let the place at infinity split into $r+1$ places in F. Then $\mathcal{O}_F^\times \cong \mathbb{F}_q^\times \times \mathbb{Z}^r$.*

We call r the *unit rank* of a function field. Our main concern will be field extensions with unit rank zero; therefore, $\mathbb{F}_q^\times$ will be the full unit group.

2.3.2 Ideals and Ideal Class Group of $\mathcal{O}_F$

Both of $\mathbb{F}_q[x]$ and $\mathcal{O}_F$ are Dedekind domains. While there are many salient properties of Dedekind domains (see Theorem VIII.6.10 of [16]), the one that we will use the most is the fact that every proper ideal of a Dedekind domain is uniquely the product of a finite number of prime ideals. Prime ideals are an example of *integral ideals*, which are $\mathcal{O}_F$-submodules of $\mathcal{O}_F$. If $\mathfrak{a}$ is an integral ideal then it is a free $\mathbb{F}_q[x]$-submodule of rank n. Therefore, it has an $\mathbb{F}_q[x]$-basis $\{\lambda_1, \ldots, \lambda_n\}$ and we shall write $\mathfrak{a} = [\lambda_1, \ldots, \lambda_n]$. Every integral ideal has a basis that satisfies $\lambda_i = \sum_{j=1}^{i} m_{i,j}\beta_j$ with $m_{i,j} \in \mathbb{F}_q[x]$ for $1 \leq i \leq n$ and we call such a basis a *triangular basis*. The norm of an ideal is the discriminant of the n x n matrix $(m_{i,j})_{1\leq i,j\leq n}$. The norm is unique up to factors in $\mathbb{F}_q^\times$. The norm of an ideal given in a triangular basis is the product of the $m_{i,i}$. We call an ideal *canonical* if it is in triangular and $m_{i,j}$ are chosen to be of

minimal degree.

Much like we use the integers to form quotients to get the rationals, we use ideals to form *fractional ideals.* We will use these to form the ideal class group.

Definition 2.3.3. *A* fractional ideal *of $\mathcal{O}_F$ is a nonzero $\mathcal{O}_F$-submodule $\mathfrak{f}$ of F such that $d\mathfrak{f} \subset \mathcal{O}_F$ for some $d \in \mathcal{O}_F^\times$.*

A way to interpret the definition is to view a fractional ideal as the set $\mathfrak{f} = \mathfrak{a}/d$ where $d \in \mathbb{F}_q[x]^\times$ and $\mathfrak{a}$ is an integral ideal. The product of two fractional ideals

$$\mathfrak{fg} = \left\{ \sum_i f_i g_i \mid f_i \in \mathfrak{f}, g_i \in \mathfrak{g} \right\}$$

is also a fractional ideal. Thus, the set of all fractional ideals form a group and we denote this group $\mathcal{I}(\mathcal{O}_F)$. The unique monic polynomial d in $\mathbb{F}_q[x]$ of minimal degree such that $\mathfrak{a} = d\mathfrak{f}$ is an integral ideal is called the *denominator* of $\mathfrak{f}$; we also write $d = L(\mathfrak{a})$. The ideal $\mathfrak{f}$ will have an $\mathbb{F}_q[x]$-basis of the form $[\lambda_1/d, \ldots, \lambda_n/d]$, $\lambda_i \in \mathcal{O}_F$. Like integral ideals, $\mathfrak{f}$ can be written in a triangular basis where $\lambda_i = \sum_{j=1}^{i} m_{i,j}\beta_j/L(\mathfrak{a})$ with $m_{i,j} \in \mathbb{F}_q[x]$. Then the norm of a fractional ideal in triangular form is

$$N(\mathfrak{f}) = \frac{1}{d^n} \prod_{i=1}^{n} m_{i,i}.$$

A fractional ideal with $d = 1$ is an integral ideal.

An ideal is *principal* if it is generated by a single element of $F^\times$ and the set of principal ideals forms a subgroup, $\mathcal{P}(\mathcal{O}_F)$, of $\mathcal{I}(\mathcal{O}_F)$.

Definition 2.3.4. *The quotient group*

$$Cl(\mathcal{O}_F) = \mathcal{I}(\mathcal{O}_F)/\mathcal{P}(\mathcal{O}_F)$$

is a finite Abelian group and is called the ideal class group *of $\mathcal{O}_F$.*

Ideal class groups are an object of much study and, as mentioned before, Gauss was the first to study this group in quadratic number fields. In Chapter 3, we will present

an algorithm to do arithmetic in this group for cubic function fields in characteristic three.

To summarize this section in preparation for Chapter three, we have an easy way to write integral ideals. Integral ideals in cubic function fields have the form $[a_1, a_2+a_3\beta_1, a_4+a_5\beta_1+a_6\beta_2]$ where $\{1, \beta_1, \beta_2\}$ is an integral basis of F and $a_i \in \mathbb{F}_q[x]$ for $i = 1, \ldots, 6$. Since polynomial arithmetic in $\mathbb{F}_q[x]$ is understood, that leaves open the issue of finding an integral basis suitable for computation. This will be the subject of Section 3.2. With the integral basis, we will have an easy way to perform arithmetic on ideals and this will give us the ability to do arithmetic on the points of the Jacobian.

2.4 The Jacobian and the Ideal Class Group

The previous two sections defined places, divisors, and ideals. We mentioned that finite places are in one-to-one correspondence with prime ideals. This section defines the relationship between fractional ideals and divisors and is one of the key sections in terms of the computation in the ideal class group. While the theoretical ground work has already been laid by others, it is important to point out how it applies here as well. Representing group elements and explaining exactly how the group operation is done can be difficult in an arbitrary group. The work that follows solves those two problems for the points on the Jacobian. We will be able to represent group elements of the ideal class group with integral ideals and we will be able to perform group operations in the ideal class group. The key obstacle here is the notion of "reduction"; there should only be one accepted representation of a group element. Ideal multiplication is theoretically easy. However, a product of two ideals calculated in a naive way, while

clearly in the group, will not likely be represented using the unique representation we desire. We must find a way to reduce an arbitrary product to the desirable representation (usually defined so that it is the smallest such representation). This section will describe the basic process. Since the particulars of reduction depend on the signature of the specific function field, the details of reduction will be given in the next chapter. The previous two sections defined places, divisors, and ideals. We mentioned that finite places are in one-to-one correspondence with prime ideals. This section defines the relationship between fractional ideals and divisors and is one of the key sections in terms of the computation in the ideal class group. While the theoretical ground work has already been laid by others, it is important to point out how it applies here as well. Representing group elements and explaining exactly how the group operation is done can be difficult in an arbitrary group. The work that follows solves those two problems for the points on the Jacobian. We will be able to represent group elements of the ideal class group with integral ideals and we will be able to perform group operations in the ideal class group. The key obstacle here is the notion of "reduction"; there should only be one accepted representation of a group element. Ideal multiplication is theoretically easy. However, a product of two ideals calculated in a naive way, while clearly in the group, will not likely be represented using the unique representation we desire. We must find a way to reduce an arbitrary product to the desirable representation (usually defined so that it is the smallest such representation). This section will describe the basic process. Since the particulars of reduction depend on the signature of the specific function field, the details of reduction will be given in the next chapter.

Let S be the set of finite places in F. There is an isomorphism between $\mathcal{D}_F(S)$

and $\mathcal{I}(\mathcal{O}_F)$. The *Fundamental theorem of ideal theory in an algebraic function field* [15, p 401] gives the isomorphism as

$$\Phi \ : \ \mathcal{D}_F(S) \to \mathcal{I}(\mathcal{O}_F), \quad D \longmapsto \left\{ \alpha \in F^{\times} \;\middle|\; \sum_{P \in S} v_P(\alpha) P \geq D \right\} \cup \{0\}. \tag{2.1}$$

This may also be defined by

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

In general the ideal class group is related to the Jacobian by the following exact sequence (see Theorem 14.1 of [28])

$$(0) \to \mathcal{D}_F(S^c)/\mathcal{P}_F(S^c) \to \mathcal{J}_F(\mathbb{F}_q) \xrightarrow{\Phi} Cl(\mathcal{O}_F) \to \mathbb{Z}/f\mathbb{Z} \to (0),$$

where S^c is the set of infinite places (the set complement of S in $\mathbb{P}_F$) and f is the greatest common divisor of $\{\deg P \mid P \in S\}$. Specifically, this means for a certain class of function fields, the points on the Jacobian will be isomorphic to the ideal class group.

The latter portion of Chapter three concerns function fields with signature $(3,1)$, that is function fields whose infinite place is totally ramified. In this case the above exact sequence yields an isomorphism between the points on the Jacobian and the ideal class group. Let D be a divisor with support in S, then every degree zero divisor has the form

$$D_0 = D - \deg(D)\infty_0.$$

Since ∞_0 is the only infinite place, D_0 is uniquely determined by D. Our goal will be to flesh out this statement below. We state a hierarchy of divisors and show how to find equivalent divisors for each hierarchy. Arithmetic on divisors in the most selective portion of the hierarchy is equivalent to arithmetic in the ideal class group. For the corresponding curves, working in the ideal class group is equivalent to working with

points on the Jacobian. For purely cubic function fields with signature $(3,1)$, Bauer first used this isomorphism to do arithmetic on nonsingular curves [3] and Landquist generalized to encompass the singular cases [21]. Chapter three aims to extend this work to characteristic three.

2.4.1 Hierarchy of divisors

We want to establish a hierarchy of divisors (and hence ideals) so that there is a way to represent elements of the degree zero divisor class group in a unique way with minimal information. A divisor $D = \sum_{P \in \mathbb{P}_F} n_P P$ is said to be *effective* if $D > 0$ (that is, $n_P \geq 0$ for all $P \in \mathbb{P}_F$). The effective part of any divisor D is denoted 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 divisor is called *finitely effective* if its finite part is effective. This is the first step in the hierarchy.

Theorem 2.4.1 (Lemma 1.6 of [3]). *Every divisor $D \in \mathcal{D}_F^0$ is equivalent to a finitely effective divisor.*

For the details of the proof we refer the reader to the original source [3]. We sketch the outline of the proof: Assuming D is not finitely effective, then some $n_P < 0$. Find an element $\alpha \in \mathcal{O}_F$ such $v_P(\alpha) > -n_P$ and then observe that $v_Q(\alpha) \geq 0$ for all finite places $Q \neq P$. Now $D' = D + (\alpha)$ has $v_P(D') \geq 0$. Iterate for each place with $n_P < 0$ until a finitely effective divisor is found.

A finitely effective divisor is *semi-reduced* if there does not exist a non-empty subsum of the form (α) where $\alpha \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$. With the following theorem we establish the next step in the hierarchy.

Theorem 2.4.2 (Lemma 1.8 of [3]). *Every divisor $D \in \mathcal{D}_F^0$ is equivalent to a semi-*

reduced divisor.

We sketch the proof and leave the reader to consult the original source. By the previous theorem, it suffices to show the result for finitely effective divisors. Let D_1 be a nonempty sub-sum of D that also has degree zero such that $D_1 \sim \overline{(\alpha)}$ for $\alpha \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ and the overline notation indicates the inverse in the divisor group. Then $D - D_1 \sim D$ is finitely effective with $\deg(D - D_1)^+ < \deg D^+$. By repeating as necessary we will find a divisor equivalent to D that is semi-reduced.

Let D be a finitely effective divisor, then D is called *reduced* if $\deg D^+ \leq g$ and D is semi-reduced where g is the genus of the curve. Explicit treatment of the genus will occur in the next section. It is sufficient to know that the genus is a non-negative integer number that is an invariant of the function field.

Theorem 2.4.3 (Lemma 1.10 of [3]). *Every divisor class contains a reduced divisor.*

We return to the proof of this statement in the next section. The proof invokes the Riemann-Roch theorem and would be best delayed until we have stated the theorem. Suffice it to say for now that, like the two previous theorems, finding the reduced divisor is not problematic. The goal has been to work toward a condition that guarantees a unique representation of a given class. Unfortunately, there can exist more than one reduced divisor in a given class. The final restriction is to define a *distinguished* divisor. A distinguished divisor D is a divisor such that for all equivalent finitely effective divisors D_1, $\deg D_1^+ \leq \deg D^+$ implies $D = D_1$. If a divisor is distinguished, it is reduced [3, Lemma 1.12]. Unfortunately, we have no apriori way of knowing if such a divisor exists or of verifying that a divisor is distinguished.

This has established a hierarchy for divisors. Visually the implications follow as:

$$\text{distinguished} \Rightarrow \text{reduced} \Rightarrow \text{semi-reduced} \Rightarrow \text{finitely effective}\ .$$

2.4.2 Divisors as Ideals

At the close of Section 2.3 we stated how we would represent ideals. At the beginning of this section we made note that fractional ideals (which are integral ideals with polynomial denominators) can be used to represent divisors. We exploit this relationship to develop arithmetic. The above definitions applied to divisors can immediately be applied to fractional ideals given the isomorphism (2.1). An integral ideal $\mathfrak{a}$ is *primitive* if and only if $\Phi^{-1}(\mathfrak{a})$ is a semi-reduced divisor. 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 $a(x)\mathcal{O}_F$. We cite Landquist's restatement of Bauer's Lemma 2.7 to relate finitely effective ideals to integral ideals:

Theorem 2.4.4 (Lemma 2.5.6 of [21]). *Let D be a finitely effective divisor and define $\mathfrak{a} = \Phi(D^+)$, then $\mathfrak{a}$ is an integral ideal and* $\deg D^+ = \deg \mathfrak{a}$.

Ideal multiplication in the ideal class group is, in some sense, easy because multiplying ideals is just linear algebra. However, inversion in the ideal class group will be more difficult; we will not be able to make a straight forward appeal to linear algebra as we do with multiplication. We state how we invert an ideal.

Theorem 2.4.5 (Lemma 2.5.7 of [21]). *If $\mathfrak{a}$ is an ideal of $\mathcal{O}_F$, then there is a primitive ideal, which is denoted $\overline{\mathfrak{a}}$, such that $\mathfrak{a}\overline{\mathfrak{a}} = \langle L(\mathfrak{a}) \rangle$.*

Proof. Since $L(\mathfrak{a}) \in \mathfrak{a}$, we have that $\langle L(\mathfrak{a}) \rangle \subseteq \mathfrak{a}$, so there is an integral ideal, $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \langle L(\mathfrak{a}) \rangle$. Suppose $\mathfrak{b}$ is not primitive. Then there is some non-constant polynomial $b(x) \in \mathbb{F}_q[x]$ such that $\langle b(x) \rangle | \mathfrak{b}$. But this implies $b(x) | L(\mathfrak{a})$ with $L(\mathfrak{a})/b(x) \subseteq \mathfrak{a}$, contradicting the minimality of $L(\mathfrak{a})$. Thus $\mathfrak{b}$ is primitive. □

The ideal $\overline{\mathfrak{a}}$ represents the inverse class of $\mathfrak{a}$ in the ideal class group since $\mathfrak{a}\overline{\mathfrak{a}}$ is a

principal ideal. We mentioned the problem of uniqueness with distinguished divisors. In Chapter three we will revisit this and show that the norm of an element of the function field can be used to circumvent this problem. Once we have described the norm, it will become clear how this enables the construction of reduced elements in a given class.

2.5 Singularity and Genus

We have avoided going into great detail about the algebraic geometric point of view on function fields. One of the key reasons is that we fix a minimal polynomial and study the extension that arises from this polynomial. Results from algebraic geometry say that we can change models and still study the same function field. While certain algebraic geometric invariants remain unchanged, we often lose the analogue that we have developed from the number theoretic perspective. For instance, the notion of separability is algebraic and upon changing models we can lose this property (see Example 6.3.8 in [36]). In so far as we change models, our changes will keep the extension degree fixed.

2.5.1 Singularity

An algebraic geometer would view the bivariate equation $\phi(x, T) = 0$ as a curve and study the function field associated to that curve. As a curve, one of its most important properties is singularity.

Definition 2.5.1. *A curve* $\phi(x, y) = 0$ *over* $\mathbb{F}_q$ *is* non-singular *if there is no* $(a, b) \in$

$\overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ *such that*

$$\phi(a,b) = 0, \quad \frac{\partial \phi}{\partial x}(a,b) = 0, \quad \textit{and} \quad \frac{\partial \phi}{\partial y}(a,b) = 0.$$

Such a point (a,b) *is called a* singular point.

A curve is *singular* otherwise. There are ways of removing singularities (see Chapter 1, Example 4.9.1 of [13]) , but in general such methods destroy the specific algebraic properties that we want. Thus we will consider singular curves.

The singular points are closely related to the form of an integral basis. Theorem II.5.10 of [24] states that $[1, y, \ldots, y^n]$ is an integral basis of $\mathcal{O}_F$ if and only if $\phi(x,T)$ is non-singular. While the theorem is stated for an algebraically closed base field, an analogous result holds when the base field is not algebraically closed.

2.5.2 Genus and different exponents

There are two invariants of function fields that are closely related: the genus and the discriminant. Defining the genus will require a few definitions about divisors. Associated to a given divisor D there is a set of functions

$$\mathcal{L}(D) = \{\alpha \in \overline{\mathbb{F}}_q(x,y)^\times \mid (\alpha) \geq -D\} \cup \{0\}.$$

This set of functions is a finite-dimensional vector space over $\overline{\mathbb{F}}_q$ whose dimension is denoted by

$$l(D) = \dim\ \mathcal{L}(D).$$

This allows us to state the Riemann-Roch Theorem.

Theorem 2.5.1 (Riemann-Roch). *There is a natural number* g *and a divisor class* $\mathcal{C}$ *such that for* $W \in \mathcal{C}$ *and* $A \in \mathcal{D}_F$*:*

$$l(A) = \deg A - g + 1 + l(W - A).$$

The invariant g is the *genus* of the function field F, the divisor class C is the *canonical class*, and any divisor $W \in C$ is called a *canonical divisor*. Having stated the Riemann-Roch theorem we return to the proof that every divisor class contains a reduced divisor (Theorem 2.4.3 or Lemma 1.10 of [3]).

Proof. It suffices to prove the result for finitely effective divisors. Let D_1 be a finitely effective divisor with $d = \deg D_1^+$. Let $d > g$ (otherwise D_1 is already reduced), then the Riemann-Roch Theorem gives

$$l(D_1^+ - (d-g)\infty) = \deg(D_1^+ - (d-g)\infty) - g + 1 + l(W - (D^+ - (d-g)\infty)) \geq g - g + 1 \geq 1$$

where W is a canonical divisor. Since $l(D_1^+ - (d-g)\infty) \geq 1$, let $\alpha \in \mathcal{L}(D_1^+ - (d-g)\infty)$ with $\alpha \notin \mathbb{F}_q$. Then $D_2 = D_1 + (\alpha)$ is also finitely effective and $d_2 = \deg D_2^+ \leq g$. Now we may find an equivalent semi-reduced divisor D_3 with $\deg D_3^+ \leq g$ and D_3 will be a reduced divisor equivalent to D. □

Since the genus is an important invariant, we will want to calculate it. The Riemann-Roch theorem will not be used to do this. Instead, the Hurwitz Genus Formula will be used. In general the Hurwitz Genus Formula relies on a quantity called the *different*. This different is a sum of *different exponents* and is denoted $d(\mathfrak{p}|P)$ for each place $\mathfrak{p} \in \mathbb{P}_F$. For finite places, the field discriminant is a quantity that keeps track of ramified places and their different exponent, which is the valuation of the discriminant at that place. While this suffices for the finite places it leaves out the infinite places. We will return to finding the different exponent of the infinite places. Having discussed how places split, we have a tool for computing the genus of a curve that relates the genus to the discriminant.

Theorem 2.5.2 (Hurwitz Genus Formula). *Suppose that F is a finite separable ex-*

tension of the rational function field K. Let g denote the genus of F/K. Then

$$2g - 2 = -2[F : K] + \sum_{P \in \mathbb{P}_F} \sum_{\mathfrak{p} | P} d(\mathfrak{p} \mid P) \deg \mathfrak{p}.$$

Sometimes calculating different exponents can be done without appealing to the discriminant. By appealing to the ramification index we can learn information about the different exponents.

Theorem 2.5.3 (Dedekind's Different Theorem). *Let $d(\mathfrak{p}|P)$ be the different exponent of $\mathfrak{p}|P$. Then for all $\mathfrak{p}|P$*

1. $d(\mathfrak{p}|P) \geq e(\mathfrak{p}|P) - 1$.
2. $d(\mathfrak{p}|P) = e(\mathfrak{p}|P) - 1$ *iff* $\text{char}(K) \nmid e(\mathfrak{p}|P)$.

The easiest way to find different exponents for the wildly ramified finite places is by finding the field discriminant. For the infinite place we will appeal to the following theorem.

Theorem 2.5.4 (Theorem III.5.12 of [36]). *Let F/K be a finite separable extension, $P \in \mathbb{P}_K$ and $\mathfrak{p} \in \mathbb{P}_F$ with $\mathfrak{p}|P$. Suppose that $\mathfrak{p}|P$ is totally ramified and let t be a uniformizer for $\mathfrak{p}$ with $\phi(T) \in K[t]$ its minimal polynomial over K. Then $d(\mathfrak{p}|P) = v_{\mathfrak{p}}(\phi'(t))$ and $\{1, t, \ldots, t^{n-1}\}$ is an integral basis for F/K at P.*

This provides a summary of the necessary background mathematics for the next chapter. We will now focus on cubic function fields in characteristic three.

Chapter 3

Curves of the form $T^3 - A(x)T + B(x) = 0$

Chapter two provided an overview of function fields. The focus now narrows to consider cubic extensions of a rational function field when the base field has characteristic three. The first priority is to assign a standard model to an arbitrary cubic curve. With a standard model in hand we calculate an integral basis, the discriminant, and the genus. Section 3.2 also calculates the norm map for the extension which will allow us to return to the subject of distinguished divisors and ideals. The remainder of the chapter is dedicated to explaining arithmetic in the ideal class group. Section 3.4 states integral bases for the prime ideals and their powers. From these theorems we develop inversion, division, and multiplication, which provides the basics of ideal arithmetic. Finally, properties of the norm can be used to find a minimal element which is then used to construct a distinguished ideal. This is the subject of the last three sections.

3.1 Standard Form

The first priority for the two papers that dealt with arbitrary cubic function fields [22, 32] was to define a *standard form*, which is the specific model that will be used for an arbitrary cubic curve. Since many different curves can give rise to the same function field we want a canonical way of representing function fields. In characteristic greater than three, the standard form is given by an absolutely irreducible curve

$\mathcal{C} : T^3 - AT + B = 0$ with $A, B \in \mathbb{F}_q[x]$ and there exists no $Q \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ such that $Q^2 | A$ and $Q^3 | B$. In characteristic three, the standard model will look analogous, but it will have additional degree and divisibility restrictions on A and B. While the appearance is similar, the manner in which we derive the standard model in characteristic three is quite different. Our only concern will be in finding a birationally equivalent curve.

From this point forward $\text{char}(\mathbb{F}_q) = 3$ unless explicitly stated otherwise. $\mathbb{F}_q$ is typically a finite field; however, we only need that it is a perfect field of characteristic three. An arbitrary, absolutely irreducible, cubic plane curve $H(x, T) = 0$ where $H \in \mathbb{F}_q[x][T]$ is given by a bivariate polynomial of degree 3 in T. We write $H(x, T) = ST^3 + UT^2 + VT + W$ with $S, U, V, W \in \mathbb{F}_q[x], SW \neq 0$. Restricting to separable extensions also requires $U \neq 0$ or $V \neq 0$.

If $U = 0$ the curve has the form $ST^3 + VT + W = 0$. In this case the polynomial can be made monic by multiplying the equation by S^2 and using the substition $ST \rightarrow T$ to get a curve of the form $T^3 - AT + B = 0$ (with $A = -SV$ and $B = S^2W$). On the other hand, if $U \neq 0$ it is possible to eliminate the linear term and consider the reverse polynomial. Using the fact that the linear term is only affected by the quadratic term under a linear transformation, completing the square eliminates the linear term. The transformation $T \rightarrow U^{-1}(T + V)$ leads to

$$SU^{-3}T^3 + U^{-1}T^2 + (SU^{-3} + 2U^{-1}V^2 + W) = 0.$$

Multiplying through by U^3 so that the equation is integral yields

$$ST^3 + U^2T^2 + (S + 2U^2V + U^3W) = 0.$$

Considering the reverse polynomial and renaming the coefficients, the curve is now given by $S_1T^3 + V_1T + W_1 = 0$ with $U_1 = 0$. Applying the transformation used when

$U = 0$, we get a curve in the form $T^3 - AT + B = 0$. For this latter case (which is the expected case), we can write A, B in terms of the original S, U, V, W. If we let

$$N = S + 2U^2V + U^3W \quad \text{then}$$

$$A = -NU^2 \quad \text{and} \quad B = N^2S.$$

In characteristic greater than three, if there is a polynomial Q such that $Q^2|A$ and $Q^3|B$ then it is possible to consider instead the curve given by

$$T^3 - (A/Q^2)T + (B/Q^3) = 0$$

which justifies the additional constraint for the standard form. In characteristic three, a transformation of the form $T \rightarrow T + i(x)$ takes the curve to $T^3 - AT + (i^3 - iA + B) = 0$. This transformation only changes the constant term and does not change the function field under consideration. Thus, if there is a polynomial $Q^2|A$ 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

$$T^3 - \left(\frac{A}{Q^2}\right)T + \left(\frac{i^3 - iA + B}{Q^3}\right) = 0. \tag{3.1}$$

The inspiration for this transformation comes primarily from the integral basis construction. If the standard model were given just by the restriction that no polynomial Q satisfies $Q^2|A$ and $Q^3|B$, then we could construct an integral basis element that has a minimal polynomial given by (3.1). That is how this particular transformation was discovered. In essence, that part of the integral basis calculation is finding removable singularities in the model. By incorporating this as part of the standard model, we simplify the elements involved in the integral basis construction. This also places a restriction on the index of this function field. We state an algorithm that returns A and B such that there is no Q, i satisfying A/Q^2 and $(i^3 - iA + B)/Q^3$. The algorithm is called RemSing because it allows the removal of certain singularities.

Algorithm 1: RemSing

Input: The polynomials A and B.

Output: Polynomials A, B so that the curve $T^3 - AT + B$ is in standard form and isomorphic to the original curve.

Precomputation: Find S the set of irreducible polynomials such that $P^2|A$.

1: **for** $P \in S$ **do**
2: calculate k_0 such that $k_0^3 \equiv -B \pmod{P}$
3: **if** $k_0^3 - k_0 A + B \equiv 0 \pmod{P^3}$ **then**
4: Let $A' = A'/P^2$ and $B' = (k_0^3 - k_0 A + B)/P^3$
5: **Return:** RemSing with inputs A' and B'
6: **end if**
7: **end for**
8: **Return:** A and B

Theorem 3.1.1. *Algorithm 1 is correct.*

Proof. We are trying to find a polynomial $i(x)$ such that $i^3 - iA + B \equiv 0 \pmod{P^3}$. Thus, we write $i(x) = k_0 + k_1 P + k_2 P^2$ to see that we need only consider k_0 in the congruence. Since the congruence is defined moduloP^3, it is certainly defined modulo P. Thus, we let $k_0^3 + B \equiv 0 \pmod{P}$. It is now a matter of checking whether $k_0^3 - k_0 A + B \equiv 0 \pmod{P^3}$. □

While the algorithm checks all polynomials P such that $P^2|A$, it will become clear that p has to correspond to singular points and this limits the expected primes. There are two factors that limit this occurrence for randomly chosen polynomials A and B. First, curves are expected to be nonsingular. Being nonsingular is equivalent to two specific polynomials being relatively prime. If we view these as random polynomials then heuristically we expect them to be relatively prime with probability roughly $1 - 1/q$. Second, we expect A to be square-free with probability $1 - 1/q$. This clearly depends on how the curve is constructed. If a random curve is considered as a random

arbitrary cubic curve (choosing S, U, V, T randomly), then A (by the transformations above) will not be square free.

The end result is a curve that has an analogous form as the previously considered cubic curves in characteristic greater than three. However, much like hyperelliptic curves in characteristic two, it is possible to impose degree requirements on A and B that constitute the standard form.

If $3|\deg B$ and $2\deg B > 3\deg A$, we write $B(x) = b_{3n}x^{3n} + b_{3n-1}x^{3n-1} + \ldots + b_0$. We can consider the linear transformation $T \to T - (b_{3n})^{1/3}x^n$. (Note that $b_{3n}^{1/3} \in \mathbb{F}_q$ because $\mathbb{F}_q$ is perfect.) Under this map we get a new curve

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

where the polynomial $b_{3n-1}x^{3n-1} + \ldots + b_0 + A(x)b_{3n}x^n$ 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:

$$3 \nmid \deg B \quad \text{and} \quad 2\deg B > 3\deg A \tag{3.2}$$

$$\text{or} \quad 2\deg B \leq 3\deg A. \tag{3.3}$$

A curve is a *standard model* for a cubic function field if it is in the form:

$$T^3 - AT + B = 0 \tag{3.4}$$

with no Q, i such that $Q^2|A$ and $Q^3|i^3 - iA + B$ and satisfies either (3.2) or (3.3). A curve satisfying (3.2) has a totally ramified infinite place and if it satisfies (3.3) the infinite place will be tamely ramified or unramified. We will freely use this classification of the infinite place until it is proved in the exposition prior to Theorem 3.3.1.

Singularities correspond to the index of the function field. It will be useful to have

an easy criterion to detect singularities.

Theorem 3.1.2. *The curve* $T^3 - A(x)T + B(x) = 0$ *is nonsingular if and only if*

$$\gcd(A(x), A'(x)^3B(x) + B'(x)^3) = 1. \tag{3.5}$$

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

$$b^3 - A(a)b + B(a) = 0. \tag{3.6}$$

$$A(a) = 0. \tag{3.7}$$

$$-A'(a)b + B'(a) = 0. \tag{3.8}$$

From (3.7), a is a root of $A(x)$, and combined with (3.6) we see that $-b^3 = B(a)$. Cubing (3.8) 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 $A(x)$, (3.7) is satisfied. Since $\mathbb{F}_q$ is perfect, we can find b such that $b^3 = -B(a)$ in order to satisfy (3.6). With (3.6) and (3.7) satisfied, it is clear that (3.8) is also satisfied by the above construction. □

This calculation does not require the curve to be in standard form. It could be used prior to establishing the standard form to see if a prime P such that $P^2|A$ corresponds with singular points. In the case that it does correspond with singular points, then $i(x)$ is constructed as previously described to remove this factor from A. Upon establishing the standard form, we can use Theorem 3.1.1 to calculate the index I as follows. Let $d = \gcd(A(x), A'(x)^3B(x) + B'(x)^3)$. A prime P divides d if and only if P divides I. In the next section, we will see that the index is square-free and I is just the square-free factorization of d. From this point forward every curve will be assumed to be in standard form and we will consider the cubic function field

$\mathcal{F} = \mathbb{F}_q(x, y)$ where y is a root of of the polynomial $T^3 - AT + B$.

The next section will calculate the discriminant of the function field. At this point all we know is the discriminant of y which is $A(x)^3$ (recall that this means the field discriminant is a divisor of $A(x)^3$ and differs from $A(x)^3$ by some square factor). This is sufficient for the last theorem of this section.

Theorem 3.1.3. *$\mathcal{F}$ is an Artin-Schreier extension if and only if $A(x)$ is a square.*

Proof. Cubic extensions are Galois (and therefore Artin-Schreier extensions in characteristic three) 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 $f, g \in \mathbb{F}[x]$ is an Artin-Schreier extension then $T^3 - g^2T = fg^2$ is an integral model for this equation. By renaming, we have $A(x) = g(x)^2$ a square. □

3.2 Integral basis, discriminant and genus

We will follow Chapter 2, Section 17, of [9] to develop an integral basis. The integral basis calculations lead to determining the discriminant of the function field, which in turn gives the different exponents of the finite places. To proceed we write down a basis in triangular form. Assuming the basis is integral will lead to restrictions on the elements of the basis. We find these restrictions by examining the minimal polynomial of each element. Following [9], we choose the product of the latter two of the 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 use of i here is due to the fact that this i can coincide with the i used in the reduction to the standard model. We mentioned that the

integral basis construction was a motivation for the standard form, in particular the minimal polynomial of ρ, which is given by

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

Since the minimal polynomial of ρ has coefficients in $\mathbb{F}_q[x]$, $I_1^2|A$ and $I_1^3|i^3 - iA + B$. However, reduction to the standard form was done to eliminate the possibility of such a polynomial I_1, and hence $I_1 = 1$. 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. As noted below, this criterion means that I_2, which is the index, is square-free. From this point forward the subscript of I_2 will be dropped and the index will be denoted I.

Theorem 3.2.1. *The index of a curve in standard form is square-free.*

Proof. By way of contradiction, assume that there exists an irreducible polynomial P such that $P^2|I$. Then by the above, $P^2|I|A$ and $P^6|I^3|(i^3 - iA + B)^2$. The latter implies $P^3|(i^3 - Ai + B)$. This violates the standard form assumption. □

Having established the index is square-free, we can calculate $i(x)$. Since $i(x)$ is unique modulo I, it suffices to define $i(x)$ modulo each prime P dividing I. The

congruence $(i^3-iA+B)^2 \equiv 0 \pmod{I^3}$ may be considered modulo P^2 as $i^3-iA+B \equiv 0 \pmod{P^2}$. Since $I|A$, It suffices to find $i^3 + B \equiv 0 \pmod{P}$. Thus, $i(x)$ maybe found by computing $(-B)^{1/3} \pmod{P}$ for every $P|I$ and constructing $i(x)$ by the Chinese remainder theorem.

The various products of the integral basis elements will be important:

$$\rho^2 = I\omega + A \quad \omega^2 = -E\omega - F\rho \quad \rho\omega = -FI, \tag{3.9}$$
$$\text{where } A = EI \quad \text{and} \quad i^3 - iA + B = FI^2.$$

For any $\alpha \in \mathcal{F}$ there are $a, b, c \in \mathbb{F}_q(x)$ such that α maybe written as $\alpha = a+b\rho+c\omega$. The norm of this element is given by

$$N(a + b\rho + c\omega) =$$
$$a^3 - a^2cE + abcIF - ab^2A + b^2cAE + bc^2AF - bc^2EFI - c^3F^2I - b^3FI^2. \tag{3.10}$$

It is now possible to calculate the discriminant of the function field. Since I is the index and $\Delta(y) = A^3$, this gives $\Delta = \Delta(\mathcal{F}) = A^3/I^2$. In Section 2.5 we defined the different exponent of a place as the valuation of the discriminant at that place. Since we have now calculated the discriminant of the function field, we now know the different exponent of any finite place. To be more precise, the different exponent for a finite place P is $v_P(A^3/I^2)$. All that remains to calculate the genus is to find the different exponent of the infinite place.

Theorem 3.2.2. *If the place at infinity of $\mathbb{F}_q(x)$ is totally ramified in $\mathcal{O}_\mathcal{F}$ then it has different exponent $d = 2\deg B - 3\deg A + 2$.*

Proof. Let $\mathfrak{p} = 1/x$, the place at infinity. Since the place at infinity is totally ramified $v_\mathfrak{p}(x) = -3$. By examining the equation $y^3 - A(x)y + B(x) = 0$, we can determine

$v_{\mathfrak{p}}(y)$. Thus, $v_{\mathfrak{p}}(y^3 - A(x)y) = v_{\mathfrak{p}}(B(x))$. Using the fact that $2\deg B > 3\deg A$, this reduces to $v_{\mathfrak{p}}(y^3) = v_{\mathfrak{p}}(B(x))$. Since $v_{\mathfrak{p}}(B(x)) = -3\deg B$, $v_{\mathfrak{p}}(y) = -\deg B$. We will apply Theorem 2.5.4 and the uniformizer used in the theorem will depend on which residue class $\deg B$ is in modulo 3.

If $\deg B = 3m - 1$ then a uniformizer of $\mathfrak{p}$ is given by $t = y/x^m$. The minimal polynomial of t is $f(t) = t^3 - Atx^{-2m} + Bx^{-3m}$. Applying theorem 2.5.4 we obtain

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

If $\deg B = 3m + 1$ then a uniformizer of $\mathfrak{p}$ is given by $t = y^2/x^{2m+1}$ and $f(t) = t^3 + Ax^{-2m-1}t^2 + A^2x^{-2(2m+1)}t + B^2x^{-3(2m+1)}$. Thus

$$\begin{aligned} d = v_{\mathfrak{p}}(f'(t)) &= v_{\mathfrak{p}}(2Ax^{-2m-1}t + A^2x^{-2(2m+1)}) \\ &= \min\{-3\deg A + 3(2m+1) + 1, -6\deg A + 6(2m+1)\} \\ &= 2\deg B - 3\deg A + 2. \end{aligned}$$

The penultimate equality follows from the fact that the two terms have different valuation, as they can clearly be seen to lie in different residue classes modulo 3. □

Theorem 3.2.3. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$ the function field obtained by adjoining to $\mathbb{F}_q(x)$ a root y of an absolutely irreducible polynomial $T^3 - AT + B$ in standard form with $A, B \in \mathbb{F}_q[x]$, $3 \nmid \deg B$, and $2\deg B > 3\deg A$. 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. □

Theorem 3.2.4. *Let the assumptions be as in Theorem 3.2.3 except that* $2\deg B \leq 3\deg A$. *Then*

$$g = \frac{3\deg A - 2\deg I + \delta_\infty - 4}{2}$$

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 tamely ramified, 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_∞. □

Assuming that (3.3) classifies the infinite place being unramified or tamely ramified, then the above theorem allows us to distinguish the two cases. The next section will describe how all places of $\mathcal{F}$ split but we close this section with a result about a property of the norm.

In the case of (3.2) the degree of the norm of an element can often be determined without calculating the norm. This might be an interesting computational fact, but it will be a crucial aspect in finding elements of minimal norm in a given ideal. Roughly speaking, the theorem states that the degree of norm can be determined by very specific terms in the norm and that the degrees of these terms lie in distinct residue classes modulo 3. Thus, if we have two elements of the same norm in a given ideal, those two elements can be used to construct another element of smaller norm. This will be made more explicit in Theorem 3.2.7 and Section 3.7.

Theorem 3.2.5. *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* $\deg N(\alpha) = \max\{\deg a^3, \deg b^3FI^2, \deg c^3F^2I\}$.

Proof. Each of $\deg a^3, \deg b^3FI^2, \deg c^3F^2I$ lie in a distinct residue class modulo three.

The criterion that $3 \nmid \deg FI^2$ actually forces $\deg FI^2 = \deg B$ and thus the curve satisifies (3.2). We establish the claim by noting that that since $3 \nmid \deg(i^3 + iA + B)$ that $\deg i^3 \leq \max\{\deg iA, \deg B\}$. In either case, by using $2 \deg B > 3 \deg A$ we get the desired equality.

There are nine terms in the norm. By assuming the maximality of one of the above three terms, we have six other terms to compare to. There are 18 cases to consider.

First we establish an equality that will be used for a number of the cases. We use $\deg F^2 I > \deg E^3$ which follows from $\deg B^2 > \deg A^3$ by using the fact that $\deg A = \deg IE$ and $\deg B = \deg FI^2$. We consider three of the 18 cases; the remaining cases follow in a similar manner.

We suppose $\deg a^3 = \max\{\deg a^3, \deg b^3 FI^2, \deg c^3 F^2 I\}$ and show that $\deg a^3$ is greater than the degree of any other term in the norm. We demonstrate the technique by showing this for $\deg a^2 cE$. Note that

$$\deg a^3 > \deg c^3 F^2 I > \deg c^3 E^3.$$

The first inequality is true by the maximality of $\deg a^3$ while the second inequality is true by $\deg F^2 I > \deg E^3$. By examining the left and right sides of the inequality we see that $\deg a > \deg cE$. Thus $\deg a^3 > \deg a^2 cE$ as desired.

A slightly more complicated case is given by considering $\deg b^3 FI^2$ and $\deg a^2 cE$. Now we suppose $\deg b^3 FI^2 = \max\{\deg a^3, \deg b^3 FI^2, \deg c^3 F^2 I\}$. In this case we note

$$3 \deg b^3 FI^2 > 2 \deg a^3 + \deg c^3 F^2 I > 2 \deg a^3 + \deg c^3 E^3.$$

As before, this first inequality is established by the maximality of $\deg b^3 FI^2$ and the second by $\deg F^2 I > \deg E^3$. By examining the left and right sides of the inequality

we see $3\deg b^3FI^2 > 3\deg a^2cE$ which gives the desired inequality.

If we consider $\deg c^3F^2I = \max\{\deg a^3, \deg b^3FI^2, \deg c^3F^2I\}$ and $\deg ab^2A$, then we can examine

$$3\deg c^3F^2I > \deg a^3 + 2\deg b^3B > \deg a^3 + \deg b^6A^3$$

to get the desired result. The other 15 cases proceed in a similar manner.

□

It is natural to wonder if (3.2) implies that $3 \nmid \deg FI^2$. Unfortunately, a small class of curves exists for which this implication is not true. If $\deg I$ is large enough and $\deg B$ is small enough we can construct a curve such that $3 \nmid \deg B$ and $3|\deg FI^2$. In general we do not expect such curves; it requires a very special sort of singularity. An example of this type of singularity is given in the following contstruction.

Example 3.2.1. *Consider the function field given by*

$$T^3 - (x^2+x-1)(x^2+1)T - x^8 + x^6 + x^5 + x^4 + x^2 + 1 = 0.$$

A calculation shows that both divisors of A are singular, $I = (x^2+x-1)(x^2+1)$, and $i = x^3 + x^2$. Thus

$$\deg(i^3 - iA + B) = 9.$$

It is clear that the curve is in reduced form and that it satisifies (3.2).

Having established this property of the norm, we can now return to the specifics of distinguished ideals. As before, the theoretical groundwork was largely laid by Bauer in [3]. We restate and reprove comparable results as they apply to this setting.

Theorem 3.2.6. *(Theorem 5.1 of [3]) 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 of Bauer's but we sketch the key points. The validity

is established using Theorem 3.2.5. 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. If two elements have the degree of their norm coming from different terms, then they will lie in different residue classes modulo 3, thus one of them will be minimal.

Theorem 3.2.7. *(Corollary 5.2 of [3]) Every ideal class contains a unique distinguished ideal.*

Proof. By the previous theorem, there exists an element $\alpha_1 \in J$ of minimal norm. We consider the primitive integral ideal $J_1 = \langle \alpha_1 \rangle J^{-1}$. Assume there is some integral primitive ideal J_2 that is equivalent to J_1 with $\deg N(J_2) \leq \deg N(J_1)$. Then $J_2 J = \langle \alpha_2 \rangle$ with $\alpha_2 \in J$. This gives $\deg N(J_1) = \deg N(\alpha_1) - \deg N(J) \geq \deg N(J_2) = \deg N(\alpha_2) - \deg N(J)$ and this 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. □

We now have all the theoretical pieces in place to develop arithmetic in the ideal class group. Theorem 2.4.5 is the inspiration for ideal inversion in the ideal class group. Ideal multiplication poses no major theoretical obstacles. Finally, 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.

3.3 Splitting of Places

In order to figure out the exact nature of the splitting of the infinite place we will appeal to completions using Theorem 2.2.3. This theorem says 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 (3.3) allows the construction of a root in $\mathbb{F}\langle x^{-1}\rangle$. After we show this, it will be clear why a curve being in the form (3.2) does not have a root in $\mathbb{F}\langle x^{-1}\rangle$ and is thus wildly ramified. For the former case, the goal will be to count the number of roots or to find $[\mathbb{F} : \mathbb{F}_q]$ to distinguish $(1,3)$, $(1,1;1,2)$, $(1,1;2,1)$, and $(1,3)$.

Assume the curve is in standard form and satisfies (3.3). 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 (thus $n = \lceil (\deg A)/2 \rceil$). If $a_{2n} = 0$ then $b_{3n} = 0$ and $b_{3n-1} = 0$ in order to satisfy (3.3). We can examine the coefficients of the powers of x in the equation $y^3 - A(x)y + B(x) = 0$ to get the following equalities:

$$\begin{aligned} x^{3n} &: & y_n^3 - a_{2n}y_n + b_{3n} &= 0 \\ x^{3n-1} &: & -a_{2n-1}y_n - a_{2n}y_{n-1} + b_{3n-1} &= 0 \end{aligned}$$

$$\begin{aligned}
x^{3n-2} &: \quad a_{2n-2}y_n - a_{2n-1}y_{n-1} - a_{2n}y_{n-2} + b_{3n-2} = 0 \\
x^{3n-3} &: \quad y_{n-1}^3 - a_{2n-3}y_n - a_{2n-2}y_{n-1} - a_{2n-1}y_{n-2} - a_{2n}y_{n-3} + b_{3n-3} = 0 \\
\vdots &: \quad \vdots
\end{aligned}$$

The equation associated with x^{3n} is cubic in y_n. After the initial cubic equation, we have an equation associated to x^{3n-i} that is linear in y_{n-i} for $i > 0$. That is, the values for y_{n-i} are uniquely determined by the initial choice for y_n. Therefore, we examine the solutions to $T^3 - a_{2n}T + b_{3n} = 0$.

If $\deg(A)$ is odd then $a_{2n} = 0$ and $T^3 + b_{3n} = 0$ has exactly one solution and as a computational note the system of equations may having many zero solutions before encountering a nonzero solution. This does not change the fact that there is exactly one solution in $\mathbb{F}_q\langle x^{-1}\rangle$. This occurs in the partially ramified case because the signature is $(1,1;2,1)$ which indicates exactly one root in $\mathbb{F}_q\langle x^{-1}\rangle$ and exactly one 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 signature $(1,1;1,1;1,1)$ corresponds to having three distinct roots in $\mathbb{F}_q\langle x^{-1}\rangle$. In this case $T^3 - a_{2n}T + b_{3n}$ splits completely in $\mathbb{F}_q$. For signature $(1,3)$ there will be a root in $\mathbb{F}_{q^3}\langle x^{-1}\rangle$ and therefore $T^3 - a_{2n}T + b_{3n}$ is irreducible over $\mathbb{F}_q$. The last case corresponds to a single root in $\mathbb{F}_q$ and therefore the place is partially split.

Suppose the curve in standard form satisfies (3.2). If we let b_k be the leading coefficient of $B(x)$ then the first equation is $b_k = 0$, thus it would be impossible to construct a root in $\mathbb{F}\langle x^{-1}\rangle$. The only signature that disallows a root in $\mathbb{F}\langle x^{-1}\rangle$ is $(3,1)$. Therefore a curve in standard form satisfying (3.2) is wildly ramified. We summarize the above discussion in following theorem.

Theorem 3.3.1. *The place at infinity splits as follows.*

1. *If* $\phi(T)$ *satisfies* (3.2) *then* $(\infty) = \mathfrak{p}^3$.
2. *If* $\phi(T)$ *satisfies* (3.3) *and* $\deg(A)$ *is odd then* $(\infty) = \mathfrak{p}\mathfrak{q}^2$.
3. *If* $\phi(T)$ *satisfies* (3.3) *and* $\deg(A)$ *is even then* $d = \gcd(T^q - T, T^3 - a_{2n}T + b_{3n})$ *determines the splitting type.*
   (a) *If* $d = 1$ *then* $(\infty) = \mathfrak{p}$.
   (b) *If* $d = T - \alpha$ *for* $\alpha \in \mathbb{F}_q$ *then* $(\infty) = \mathfrak{p}\mathfrak{q}$.
   (c) *If* $d = T^3 - a_{2n}T + b_{3n}$ *then* $(\infty) = \mathfrak{p}\mathfrak{q}\mathfrak{r}$.

We now turn our attention to the finite places.

Theorem 3.3.2. *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* $\mathcal{O}$ *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* $P \nmid A$ *and we consider three cases:*
   (a) *If* $\gcd(T^{q_1} - T, T^3 - aT + b) = T - \alpha$ *for* $\alpha \in \mathbb{F}_q$ *then* $(P) = \mathfrak{p}\mathfrak{q}$.
   (b) *If* $\gcd(T^{q_1} - T, T^3 - aT + b) = T^3 - aT + b$ *then* $(P) = \mathfrak{p}\mathfrak{q}\mathfrak{r}$.
   (c) *If* $\gcd(T^{q_1} - T, T^3 - aT + b) = 1$ *then* $(P) = \mathfrak{p}$.

Proof. For primes not dividing A, $\{1, y, y^2\}$ is an integral basis of $\mathcal{O}_P[y]/\mathcal{O}_P$ and thus Theorem 2.2.2 may be applied to get the desired result. Ramified primes divide A and the splitting type is distinguished by the different exponent. Fortunately, there are only two types of ramification possible and we have already given the criterion to distinguish them. □

Tame ramification can only happen with a singular model. Since $\Delta(y) = A^3$ we would need $v_P(A) = 1$ and $v_P(I) = 1$ to get tame ramification.

Since we have determined how all places split in the extension, our focus will now turn to arithmetic in the ideal class group. Note that if $\phi(x,T)$ is nonsingular then $I=1$, $a=0$, and $c=A$. This gives an integral basis of the form $[1,y,y^2-A]$, which corresponds exactly with the integral basis for a nonsingular curve in characterisitic greater than three described in [32].

3.4 Prime ideals and their powers

We begin with the ramified primes and move to the unramified ones. The goal for both kinds of prime ideals will be the same. First we write the prime ideal in a canonical basis and then show what powers of the prime ideal look like.

3.4.1 Ramified primes

There are three cases to consider for the ramified primes. When it comes to calculating powers of primes, ramification makes the treatement here a little easier for a given prime. A ramified prime is expected to be totally ramified so $\mathfrak{p}^3=(P)\mathcal{O}_F=(P)[1,\rho,\omega]$. This leaves only the calculation of the basis for $\mathfrak{p}$ and $\mathfrak{p}^2$. The tamely ramified primes will not be quite as easy since there are two places in $\mathcal{F}$ lying over it.

Theorem 3.4.1. *Let $v_P(A)\geq 1$ and $v_P(I)=0$ so that $(P)=\mathfrak{p}^3$. Then*

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

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 that $\rho(f+\rho)=$

$f\rho + I\omega + A \in \mathfrak{p}$. Using the fact that I is relatively prime to P we get the last elment as claimed. □

Since these primes are totally ramified, all that remains is the calculation of $\mathfrak{p}^2$.

Theorem 3.4.2. *Let $v_P(A) \geq 1$ and $v_P(I) = 0$, then*

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

Proof. By considering the fact that $(f+\rho)^2 = f^2 - f\rho + I\omega + A \in \mathfrak{p}^2$ we can see that the third term in the basis has the form claimed. Since $v_{\mathfrak{p}}(P) = 3$, $P \in \mathfrak{p}^2$. Since the ideal has to have norm P^2 this forces the second element of the basis to be as stated. □

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. The presence of this term contributes to the difficulty of doing ideal arithmetic in the arbitrary case.

Theorem 3.4.3. *Let $v_P(A) > 1$ and $v_P(I) = 1$ so that $(P) = \mathfrak{p}^3$. Then*

$$\mathfrak{p} = [P, \rho, \omega].$$

Proof. By applying Kummer's theorem to the minimal polynomials of ρ and ω, we see that both are in $\mathfrak{p}$. □

Theorem 3.4.4. *Let $v_P(A) > 1$ and $v_P(I) = 1$ so that $(P) = \mathfrak{p}^3$. Then*

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

Proof. The proof is done by squaring $\mathfrak{p}$ and eliminating redundant elements until we

have a basis.

$$\begin{aligned}\mathfrak{p}^2 &= \langle P^2, P\rho, P\omega, -FI, A + I\omega, -F\rho - E\omega\rangle \\ &= [P, \rho, P\omega]\end{aligned}$$

This follows because $v_p(E) > 0$, $\gcd(P, E) = P$, and $\gcd(P, F) = 1$. The former greatest common divisor calculation is obvious. The latter equality is less obvious. Since $v_p(FI^2) = 2$ (see Theorem 3.2.1) and $v_p(I) = 1$, $v_p(F) = 0$. □

This concludes the totally ramified primes. The tamely ramified primes are all that remain. A portion of the treatment of its powers will be in this section and some will be in the next section.

Theorem 3.4.5. *Let $v_P(A) = 1$ and $v_P(I) = 1$ so that $(P) = \mathfrak{p}\mathfrak{q}^2$. Then*

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

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

Proof. Apply Kummer's Theorem to the minimal polynomials of ρ and ω to see:

$$\rho^3 - A\rho + FI^2 \equiv \rho^3 \pmod{P},$$

$$\omega^3 + E\omega^2 - F^2I \equiv \omega^2(\omega + E) \pmod{P}.$$

Both prime ideals have ρ in their basis. $\mathfrak{q}$ has ω and $\mathfrak{p}$ has $\omega + E$.

By squaring $\mathfrak{q}$ we get

$$\mathfrak{q}^2 = \langle P^2, P\rho, P\omega, -FI, A + I\omega, -F\rho - E\omega\rangle = [P, P\rho, E^{-1}F\rho + \omega].$$

The last equality follows because $\gcd(P^2, A) = P$ and $\gcd(E, I) = 1$. □

The above primes are especially vexing. They are ramified but because it is not totally ramified, powers of $\mathfrak{p}$ and $\mathfrak{q}^2$ will not be principle when cubed. Another

aspect that makes these primes troublesome is the fact that $\mathfrak{p}$ and $\mathfrak{q}$ are distinguished from each other by the ω term in the basis, while for other primes it is sufficient to consider the term associated to ρ. These primes also exhibit another behavior that we will see with unramified primes in that they allow a polynomial coefficient on ρ as in the case of powers of $\mathfrak{q}$ but also exhibit the behavior of an index divisor by exhibiting a polynomial coefficient on ω in the case of $\mathfrak{pq} = [P, \rho, P\omega]$. When taken into consideration with the totally ramified index divisor this does imply one useful fact: the primes dividing the index will divide the coefficient of ω at most once.

3.4.2 Unramified primes

The unramified primes are the primes that we expect to see 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. Second is the case where $\mathfrak{p}$ has inertia degree 2. This case will also handle the case of the product of two primes of inertia degree 1 and the powers of $\mathfrak{q}^2$ of the split ramified case. The last case will be where $\mathfrak{p}$, $\mathfrak{q}$ both have inertial degree 1 and we need to consider products of the form $\mathfrak{p}^i\mathfrak{q}^j$.

Theorem 3.4.6. *Let $\mathfrak{p}|P$ have inertial degree one and ramification index one. 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. Consider the minimal polynomial of ρ modulo P to see

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

Writing the congruence in this way does not imply that the quadratic factor is

irreducible. The ideal $\mathfrak{p}$ is generated by $\langle P, -\alpha + \rho \rangle$. Therefore $(-\alpha + \rho)^2 = \alpha^2 + \alpha\rho + I\omega + A \in \mathfrak{p}$. We can use the fact that $-\alpha + \rho \in \mathfrak{p}$ to see that

$$(-\alpha + \rho)^2 - \alpha(-\alpha + \rho) = A - \alpha^2 + I\omega \in \mathfrak{p}.$$

Since I is relatively prime to P we can consider its modular inverse I^{-1} so that $-I^{-1}(\alpha^2 - A) + \omega \in \mathfrak{p}$. So the ideal has the form claimed. □

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

Theorem 3.4.7. *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 Theorem 3.4.5 and Theorem 3.4.6.

Proof. From the definitions in this theorem it is important that Z_1 be invertible modulo P. In Theorem 3.4.5, E is invertible modulo P. For Theorem 3.4.6 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 $P^{i+1} \subseteq \mathfrak{p}^i$, implies $\omega - Z_{i+1} = \omega - Z_i + f$ for $f \in \mathfrak{p}^i$, so it must be $Z_{i+1} = Z_i + kP^i$. Using the norm map will allows us to find k. We now describe how

to choose k so that the element is correct for P^{i+1}.

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

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

Theorem 3.4.8. *Let* $\mathfrak{q}$ *be a prime with ramification index 1 and inertia degree 2. Then*

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

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

Proof. Kummer's theorem gives $\mathfrak{q} = \langle P, \rho^2 - M\rho + W \rangle$. Since I is invertible modulo P and $\rho^2 = I\omega + A$, we have $\mathfrak{q} = \langle P, I^{-1}(W + A) - I^{-1}M\rho + \omega \rangle$. To justify the last element, note that since $P\rho \in \mathfrak{q}$, $P\rho$ is the basis element. Since the norm of this ideal is P^2, the above elements form a basis. To take one example, $P^2\rho \in \mathfrak{q}$ but if this were the basis element the ideal would have the wrong norm. □

The next theorem states what the powers of the above primes look like. However, if we consider the product of two distinct unramified primes lying over a completely

split prime, we notice

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

Here the last line is justified by the fact that $(\alpha_1 - \alpha_2)$ is relatively prime to P. Thus, the greatest common divisor of $P(\alpha_1 - \alpha_2)$ and P^2 is P. The below theorem treats the following 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 Theorem 3.4.8,
- $\mathfrak{q}^2 = [P, P\rho, E^{-1}F\rho + \omega]$ from Theorem 3.4.5, and
- $\mathfrak{pq} = [P, P\rho, I^{-1}(A + \alpha_1\alpha_2) - I^{-1}(\alpha_1 + \alpha_2)\rho + \omega]$ from the exposition above.

Theorem 3.4.9. *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.

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

This product clearly contains P^i and $P^i\rho$. We ascertain that the final term is as claimed and show that the ideal does not contain P^{i-1} or $P^{i-1}\rho$. Note that in the 9 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 is $M_1M_iI - N_i - N_1 - E$ and it has to be relatively prime to P. If it were not, the product would not be primitive. Since $M_1M_1I - N_1 - N_1 - E$ is invertible modulo P, $M_i = M_{i-1} + kP^{i-1}$ and $N_i = N_{i-1} + kP^{i-1}$, a solution will will always exist modulo P^i.

In order to show that the ideal does not contain P^{i-1} or $P^{i-1}\rho$ we appeal to the norm of the ideal. Note that $N(\mathfrak{r}^i) = P^{2i}$. Since the term with ω does not contribute any powers of P to this product, they have to come from the other two terms. Suppose $P^{i-1} \in \mathfrak{r}^i$. Then $P^{i+1}\rho \in \mathfrak{r}^i$ and $P^i \notin \mathfrak{r}^i$ so that the norm is correct, which is clearly contradicted by the fact that $P^{i-1}\rho \in \mathfrak{r}^{i-1}$, $P \in \mathfrak{r}$, so $P^i\rho \in \mathfrak{r}^i$. A similar argument unfolds by assuming $P^{i-1}\rho \in \mathfrak{r}^i$. Thus, the ideal has the basis as claimed. □

All that remains is the case $\mathfrak{p}^i\mathfrak{q}^{i+j}$ where $0 \neq j$ and each prime has inertia degree 1. By Theorem 3.4.9 we know

$$(\mathfrak{p}\mathfrak{q})^i = [P^i, P^i\rho, N_i - M_i\rho + \omega] \tag{3.11}$$

and by Theorem 3.4.7

$$\mathfrak{q}^j = [P^j, -X_{\mathfrak{q}_j} + \rho, -Z_{\mathfrak{q}_j} + \omega], \tag{3.12}$$

$$\mathfrak{q}^{i+j} = [P^{i+j}, -X_{\mathfrak{q}_{i+j}} + \rho, -Z_{\mathfrak{q}_{i+j}} + \omega], \quad \text{and} \tag{3.13}$$

$$\mathfrak{p}^i = [P^i, -X_{\mathfrak{p}_i} + \rho, -Z_{\mathfrak{p}_i} + \omega]. \tag{3.14}$$

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

Theorem 3.4.10. *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. Consider the product of (3.11) and (3.12) 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 (3.13) and (3.14) we can see that

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

Write this product as

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

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 desired element. Since the coefficient of ω has to be 1, we have established that the third basis element is, indeed, a basis element. While the other two elements are in the ideal, we appeal to the norm to establish the fact that they are basis elements. The norm of this ideal is P^{2i+j} and the elements stated have this norm. Suppose, by way of contradiction that $P^{i+j-1} \in \mathfrak{p}^i\mathfrak{q}^{i+j}$. Then this means that $P^{i+1}\rho + f_1 \in \mathfrak{p}^i\mathfrak{q}^{i+j}$ and $P^i\rho + f_2 \notin \mathfrak{p}^i\mathfrak{q}^{i+j}$ for some $f_1, f_2 \in \mathbb{F}_q[x]$, which is clearly contradicted by the fact that $P^i \in (\mathfrak{p}\mathfrak{q})^i$, $-X_{\mathfrak{q}_j} + \rho \in \mathfrak{q}^j$, so $P^i(-X_{\mathfrak{q}_j} + \rho) \in \mathfrak{p}^i\mathfrak{q}^{i+j}$. A similar argument unfolds by assuming the second element is of the form $P^{i-1}(\rho + f_3) \in \mathfrak{p}^i\mathfrak{q}^{i+j}$ for some $f_3 \in \mathbb{F}_q[x]$. □

We have dealt with all of the prime ideals and their possible powers and products. We now turn to arbitrary ideal arithmetic. The approach is simple. Any given ideal factors into the product of four ideals:

$$J = [s_1, s_1'(u_1 + \rho), v_1 + w_1\rho + \omega][s_2, s_2(u_2 + \rho), v_2 + w_2\rho + \omega]$$

$$[s_3, \rho, s_3''\omega][s_4, s_4'(u_4 + \rho), s_4''(v_4 + w_4\rho + \omega)] = J_1J_2J_3J_4.$$

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. 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 theorems are easier to state for ideals of a given type. The combined theorem 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 troublesome case. From a computational perspective there are a few reasons for this approach. Two of the four cases involve curves that have singularities and we do not expect singular curves. 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 allowed, we still do not expect to deal with three of the four products in the course of doing arithmetic. Hasse's theorem tells us that the size of the ideal class group is roughly q^g. Assuming a worst case scenario where $\deg B = 3n + 1$ and $\deg A = \deg I = 2n$ we have $g = n$. We can bound the number of ideals with degree less than g that have a ramified prime divisor by $4nq^{n-1}$. The expected chance that

two randomly chosen ideals contain a ramified prime is roughly $4n/q$ which will be small if q is large. Thus from a computational point of view, invoking three of the four cases will be rare even when a curve is singular.

3.5 Inversion and division

Some basic properties of the structure of ideals in cubic function fields developed in [31] remain true even in charactersistic three. We cite without proof the containment criterion for ideals written with a triangular basis.

Theorem 3.5.1. *(Lemma 4.1 of [31]) Let* $I_i = [s_i, s_i'(u_i + \rho), s_i''(v_i + w_i\rho + \omega)]$ *for* $i = 1, 2$ *be two ideals. Then* $I_1 \subseteq I_2$ *if and only if*

$$s_2 | s_1, \quad s_2' | s_1', \quad s_2'' | s_1''$$

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

$$s_1'' w_1 \equiv s_1'' w_2 \pmod{s_2'},$$

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

The rest of this section closely follows Section 6 of Bauer [3]. The first goal is to develop ideal inversion. We do not compute the actual inverse of an ideal because we only work with integral ideals. Instead, we compute the primitive ideal that is in the ideal class of the inverse of a given ideal. As a reminder, the notation for such an inverse will be $\overline{J}$ and the notation for division will be J^{-1}. We label the theorems depending on which of the four cases the theorem covers.

Theorem 3.5.2. *(Inversion for Type I and II primes) If* $I_1 = [s, s'(u+\rho), v+w\rho+\omega]$, *then* $I_2 = \overline{I_1} = \langle s \rangle I_1^{-1}$ *is given by* $I_2 = [S, S'(U + \rho), V + W\rho + \omega]$, *where*

$$S = s, \quad S' = s/s', \quad U \equiv -Iw \pmod{s'},$$

$$W \equiv -uI^{-1} \pmod{s/s'}, \quad \textit{and} \quad V \equiv E - v - WIw \pmod{s}.$$

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:

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

The congruence for W follows by considering the product $s'(u + \rho)(V + W\rho + \omega)$ and the coefficient of ω:

$$s'(u + \rho)(V + W\rho + \omega) \in \langle s \rangle \Rightarrow s \,|\, s'(IW+)u \Rightarrow W \equiv -uI^{-1} \pmod{s/s'}.$$

Lastly, we find the congruence for V by considering $(V + W\rho + \omega)(v + w\rho + \omega)$ and the coefficient of ω:

$$(V+W\rho+\omega)(v+w\rho+\omega) \in \langle s \rangle \Rightarrow s \,|\, V+v+WIw-E \Rightarrow V \equiv E-v-WIw \pmod{s}.$$

□

We note that the above theorem 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 theorem without an appeal to the Chinese Remainder Theorem. We will often be able to deal with these two

types of primes together.

Theorem 3.5.3. *(Inversion for Type III primes) If* $I_1 = [s, \rho, s''\omega]$, *then* $I_2 = \overline{I_1} = \langle s \rangle I_1^{-1}$ *is given by* $I_2 = [s, \rho, (s/s'')\omega]$.

Proof. This follows immediately from Theorem 3.4.3. □

Here the index divisors do not seem too complicated, but the case for Type IV ideals is the most 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. This theorem will be the first of many theorems use this. While many possible ideal factorizations may be considered, our approach is to consider a factorization that most closely resembles some of the basic prime powers of Section 3.4. The treatment of Theorem 3.4.10 is enlightening here. That theorem dealt with products of the form $\mathfrak{p}^i\mathfrak{q}^{i+j}$. In the proof we appeals 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 theorems.

Theorem 3.5.4. *(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*

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

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

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

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 Theorem 3.4.5. The inverse of $[s'', \rho, s''\omega]$ is $[s'', \rho, \omega]$ which gives the congruence modulo s'' for U and V. The inverse of $[s', s'\rho, w\rho + \omega]$ is given by $[s', U + \rho, V + \omega]$. We find the congruences for U and V modulo s' by considering the coefficient of ω in the two products $(U + \rho)(w\rho + \omega) \in \langle s' \rangle$ and $(V + \omega)(w\rho + \omega) \in \langle s' \rangle$ and arguing as in Theorem 3.5.2. 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. Recall that the ramified primes are distinguished from the unramified primes by the term associated with ω and s_I correctly identifies the prime ideals corresponding to ramified primes. 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

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

This gives 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. □

This provides inversion in the ideal class group for an arbitrary ideal. The remaining portion of this section leads to arbitrary ideal division. First a lemma is given which allows us to "split" an ideal. The term "split" here refers to the fact that the ideals under consideration are (usually) products of completely split primes. We consider $\mathfrak{p}, \mathfrak{q}$ two primes lying over a completely split place P. Given $(\mathfrak{pq})^i$ and $\mathfrak{p}^i$,

we find $(\mathfrak{pq})^i\mathfrak{p}^{-i} = \mathfrak{q}^i$. Thus the product $(\mathfrak{pq})^i$ is split into two ideals of equal norm, $\mathfrak{p}^i$ and $\mathfrak{q}^i$. This lemma will be helpful for division of a primitive ideal by another primitive ideal, which is the key theorem of this section. The lemma and inversion theorem are then used for division of a nonprimitive ideal by a primitive ideal. Of course, each of these steps has up to four corresponding sub-steps.

Lemma 3.5.1. *(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*

$$U \equiv Iw_2 - u_1 \pmod{s}, \quad V \equiv v_2 - Iw_2^2 + u_1 w_2 \pmod{s}.$$

Proof. By Theorem 3.5.2, $I_2 = \langle s\rangle[s, Iw_2 + \rho, E - v_2 + \omega]^{-1}$. Therefore we can write

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

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

Lemma 3.5.2. *(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* $J = I_2 I_1^{-1} = [s, \rho, \omega]$.

Proof. This follows immediately from Theorem 3.4.3. □

Lemma 3.5.3. *(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* $J = I_2 I_1^{-1} = [s's'', \rho, V + \omega]$, *where*

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

Proof. There are two portions to this proof. By Theorems 3.4.4 and 3.4.5 $J = [s's'', \rho, V + \omega]$ where we need to determine V. For a given prim P, I_2 has either $\mathfrak{p}\mathfrak{q}$ or $\mathfrak{q}^2$ and no higher powers. The ideal I_1 has either $\mathfrak{p}$ or $\mathfrak{q}$. Thus, we need to determine which ramified primes and unramified primes are in I_1. The quantity d corresponds to the ramified primes in I_1. For these primes the unramified conjugate is the inverse, this justifies the choice for V modulo d. □

Rather than proceed straight to the division theorems, we illustrate the method behind the division in Figure 3.5. 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 does in the case that the dividend is $\mathfrak{p}^8\mathfrak{q}^6$ and the divisor is $\mathfrak{p}^5\mathfrak{q}$.

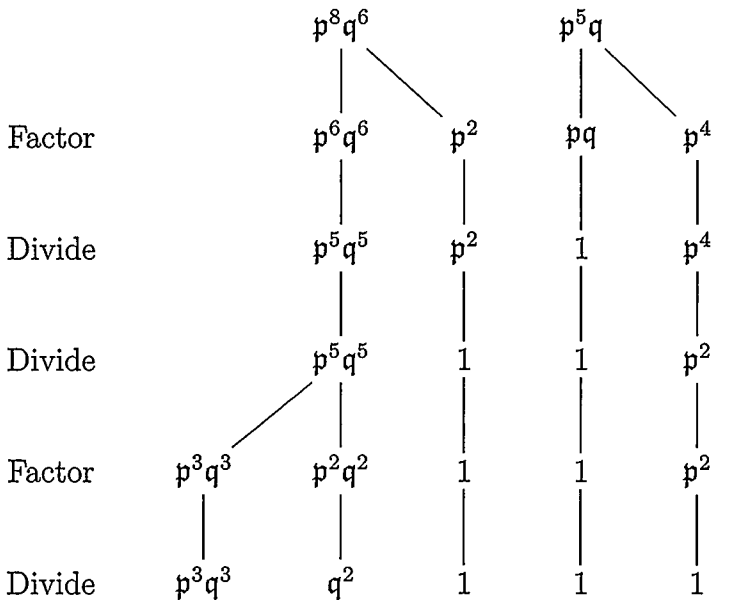


Figure 3.1: Division of $\mathfrak{p}^8\mathfrak{q}^6$ by $\mathfrak{p}^5\mathfrak{q}$

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 be relatively prime.

Theorem 3.5.5. *(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* $J = I_2 I_1^{-1} = [S, S'(U+\rho), V+W\rho+\omega]$, *where*

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

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

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

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

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

The first division is

$$\begin{aligned} &[s_2', s_2'\rho, v_2 + w_2\rho + \omega][s_1', s_1'\rho, v_1 + w_1\rho + \omega]^{-1} \\ &\quad = \left[\frac{s_2'}{s_1'}, \frac{s_2'}{s_1'}\rho, v_2 + w_2\rho + \omega\right]. \end{aligned} \tag{3.15}$$

All that remains of the divisor is

$$\left[\frac{s_1}{s_1'}, u_1 + \rho, v_1 - u_1 w_1 + \omega\right].$$

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 theorem statement. We perform

the following division:

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

This justifies one of the two congruences for U. We factor out of the ideal in (3.15) the part that matches the remaining divisor. That is,

$$\left[\frac{s_2'}{s_1'}, \frac{s_2'}{s_1'}\rho, v_2+w_2\rho+\omega\right] = \left[\frac{s_2'd}{s_1}, \frac{s_2'd}{s_1}\rho, v_2+w_2\rho+\omega\right]\left[\frac{s_1}{s_1'd}, \frac{s_1}{s_1'd}\rho, v_2+w_2\rho+\omega\right]. \tag{3.16}$$

We apply Lemma 3.5.1 to the right hand ideal of (3.16) and the remainder of the divisor to get

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

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

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

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

Theorem 3.5.6. *(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*

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

Proof. This follows by using the same arguments presented in the proof of Theorem 3.5.5. 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. □

Theorem 3.5.7. *(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* $J = I_2 I_1^{-1} = [S, S'(U+\rho), S''(V+W\rho+\omega)]$, *where*

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

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

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

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

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

$$I_i = [s_i' s_i'', s_i'\rho, s_i''(v_i + w_i\rho + \omega)]\left[\frac{s_i}{s_i' s_i''}, u_i + \rho, v_i - u_i w_i + \omega\right].$$

The first division is

$$\begin{aligned}[s_2' s_2'', s_2'\rho, s_2''(v_2 + w_2\rho + \omega)][s_1' s_1'', s_1'\rho, s_1''(v_1 + w_1\rho + \omega)]^{-1} \\ = \left[\frac{s_2' s_2''}{s_1' s_1''}, \frac{s_2'}{s_1'}\rho, \frac{s_2''}{s_1''}(v_2 + w_2\rho + \omega)\right]. \end{aligned} \tag{3.17}$$

All that remains of the divisor is

$$\left[\frac{s_1}{s_1' s_1''}, u_1 + \rho, v_1 - u_1 w_1 + \omega\right].$$

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 theorem statement. Note that unlike the proof of Theorem 3.5.5, we focus on the basis element with ω because these primes are distinguished from one another by this basis element. We perform the following division:

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

This justifies one of the two congruences for U. We factor out of the ideal in (3.17) the part that matches the remaining divisor. That is,

$$\left[\frac{s_2's_2''}{s_1's_1''}, \frac{s_2'}{s_1'}\rho, \frac{s_2''}{s_1''}(v_2+w_2\rho+\omega)\right] = \left[\frac{s_2's_2''d}{s_1}, S'\rho, S''(v_2+w_2\rho+\omega)\right]\left[\frac{s_1}{s_1's_1''d}, s_3'\rho, s_3''(v_2+w_2\rho+\omega)\right], \tag{3.18}$$

where

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

Note that $S'S'' = s_2's_2''d/s_1$ and $s_3's_3'' = s_1/s_1's_1''d$. Apply Lemma 3.5.3 to the right most ideal of (3.18) and the remainder of the divisor to get

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

where v_3 is given in Lemma 3.5.3. 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 (3.18). 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 Theorem 3.5.5 except we have to account for the coefficient of ω. □

Our approach has been very similar to that of Section 6 of Bauer's [3]. He started with inversion. Using inversion he proved a comparable splitting lemma which was used to simplify the division theorem. One key difference is that his division theorem used a certain norm argument that we avoided here. This argument will appear in the section on multiplication. We close this section as Bauer did with a theorem on dividing a nonprimitive ideal by a primitive ideal. The notation is similar, we consider an ideal that is of the form $\langle d \rangle I_2$ where I_2 is primitive and another primitive ideal I_1. The method of the proof is to remove 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 theorems on multiplication can be used calculate the product. A theorem on multiplication will invoke this theorem, but it is invoked under the assumption that I_1 completely divides $\langle d \rangle$ and that there is no corresponding factor I_2.

Theorem 3.5.8. *(Nonprimitive division for Type I and II primes)*
Let $I_2 = [s_2, s_2'(u_2 + \rho), v_2 + w_2\rho + \omega]$ *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 Theorem 3.5.5,

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

is calculated by Theorem 3.5.2,

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

Proof. We note that $\overline{I_m} \subseteq \langle d\rangle$ and $\overline{I_m}[s_1/D_1D_2, s_1'/D_1(u_1+\rho), v_1 + w_1\rho + \omega] = I_1$. Therefore $\langle d\rangle \overline{I_m}^{-1} = I_m$. After this division, the factors that remain in I_1 are $[s_1/D_1D_2, s_1'/D_1(u_1+\rho), v_1 + w_1\rho + \omega]$ and this is contained in I_2. □

The next two theorems 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 theorems.

Theorem 3.5.9. *(Nonprimitive division for Type III primes)*
Let $I_2 = [s_2, \rho, s_2''\omega]$ *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 Theorem 3.5.6,

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

is calculated by Theorem 3.5.3,

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

Theorem 3.5.10. *(Nonprimitive division for Type IV primes)*
Let $I_2 = [s_2, s_2'(u_2+\rho), s_2''(v_2 + w_2\rho + \omega)]$ *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 Theorem 3.5.7,

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

is calculated by Theorem 3.5.4,

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

3.6 Ideal multiplication

Theoretically, ideal multiplication is the easiest operation that will be discussed since it is just linear algebra. This perspective should not be lost upon reading the theorems. The goal for these theorems 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. Treating this problem as a large linear algebra problem entails computational redundancy. The extreme amount of redundancy is obvious for certain products. For example, the product of two relatively prime ideals may be computed quickly by using the Chinese remainder theorem. Computationally, the case of relatively prime operands is the expected case and the product can be calculated as Scheidler did in Theorem 4.4 of [31].

Theorem 3.6.1. *(Theorem 4.4 of [31]) 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*

$$s_3 = s_1 s_2, \quad s_3' = s_1' s_2', \quad s_3'' = s_1'' s_2'',$$

$$u_3 \equiv \begin{cases} u_1 & (\text{mod } s_1/s_1') \\ u_2 & (\text{mod } s_1/s_2') \end{cases}, \quad w_3 \equiv \begin{cases} w_1 & (\text{mod } s_1') \\ w_2 & (\text{mod } s_2') \end{cases}, \quad \textit{and}$$

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

When considering cubic function fields of unit rank one, it is possible to perform a certain operation so that multiplication can always be carried out on relatively prime ideals. The function fields under consideration here have unit rank zero and multiplication can not assume that the two operands will be relatively prime. Thus, we will follow Bauer's Section 7 [3] in developing ideal multiplication. The first set of theorems 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 Theorem 3.5.5 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 $s_2/(s_2'd)$. The theorem would have needed some additional argument if this had happened. This can happen in ideal multiplication and we sketch this additional argument here to prepare the reader. Let u_3 be the polynomial that satisfies the two congruences and is unique up to the least common multiple of their moduli. Using the fact that the norm of $\rho + U$ has to be divisible by S/S', we can write $U = u_3 + kS/S'$. This leads to a congruence for k which finishes the problem.

Theorem 3.6.2. *(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*

$$d = \gcd\left(\frac{s_1}{s_1'}, \frac{s_2}{s_2'}\right), \qquad d_1 = \gcd(d, u_1 - u_2),$$
$$u_3 \equiv u_1 \pmod{s_1 d_1 / s_1' s d}, \qquad u_3 \equiv u_2 \pmod{s_2 d_1 / s_2' d},$$
$$\text{and } k \text{ is chosen such that} \quad d_1 \left| \frac{(u_3^3 - u_3 A - FI^2)S'}{S d_1} + kA, \right.$$

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

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

$$\begin{aligned} &[s_1', s_1'\rho, v_1 + w_1\rho + \omega][s_2', s_2'\rho, v_2 + w_2\rho + \omega] \\ &\quad = [s_1' s_2', s_1' s_2' \rho, V + W\rho + \omega]. \end{aligned}$$

While we still need to find congruences for with V and W, we will return to those

later and focus on the difficult part of the product:

$$\left[\frac{s_1}{s_1'}, u_1+\rho, v_1-w_1u_1+\omega\right]\left[\frac{s_2}{s_2'}, u_2+\rho, v_2-w_2u_2+\omega\right]. \tag{3.19}$$

The goal will be two split this product up into two factors. The quantity d signifies common possible prime factors 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 $S = s_1s_2d/d_1$. It remains to choose U correctly. Combining the two previous statements we see that

$$\left[\frac{S}{S'}, U+\rho, V+\omega\right] = \left[\frac{s_1d_1}{s_1'd}, u_1+\rho, v_1-w_1u_1+\omega\right]\left[\frac{s_2d_1}{s_2'd}, u_2+\rho, v_2-w_2u_2+\omega\right].$$

This justifies the choice for u_3, and we note that u_3 is defined uniquely modulo the least common multiple of $s_1d_1/s_1'd$ and $s_2d_1/s_2'd$. Thus we can write $U = u_3+kS/S'd_1$ and consider

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

By the definition of u_3,

$$\frac{S}{S'd_1} \,\Big|\, u_3 - u_3A - FI^2$$

so we can conclude

$$d_1 \,\Big|\, \frac{(u_3^3 - u_3A - FI^2)S'}{Sd_1} + kA$$

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 the two previously calculated basis

elements to ensure the third element is canonical. □

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 theorem 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.

Theorem 3.6.3. *(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* $I_1 I_2 = I_3$ *is a primitive ideal. Then* $I_3 = [S, S'(U + \rho), V + W\rho + \omega]$, *where*

$$S = s_1 s_2/d, \quad S' = d s_1' s_2', \quad d = \gcd\left(\frac{s_1}{s_1'}, \frac{s_2}{s_2'}\right),$$
$$U \equiv f \pmod{S/S'}, \quad W \equiv I^{-1} f \pmod{S'}, \quad V \equiv f^2 I^{-1} \pmod{S},$$

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

Proof. We invoke Theorem 3.4.1 and Theorem 3.4.2 to calculate U, V, and W. □

Theorem 3.6.4. *(Primitive Multiplication for Type III primes) Let* $I_i = [s_i, \rho, s_i''\omega]$ *for* $i = 1, 2$ *be such that* $I_1 I_2 = I_3$ *is a primitive ideal. Then*

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

Proof. The proof proceeds the same way as above using the factorization as given in Theorem 3.5.6. □

Theorem 3.6.5. *(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* $I_1 I_2 = I_3$ *is a primitive ideal. Then*

$I_3 = [S, S'(U+\rho), S''(V+W\rho+\omega)]$, *where*

$$S = \frac{s_1 s_2}{d d_1 d_2}, \quad S' = s_1' s_2' d, \quad S'' = s_1'' s_2'' d_1 d_2.$$

To define d_1, d_2, *and* d, *let*

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

then

$$d = \gcd(s_{q1}, s_{q2}), \quad d_1 = \gcd\left(s_{q2}, \frac{s_1}{s_1' s_1'' s_{q1}}\right), \text{ and } \quad d_2 = \gcd\left(s_{q1}, \frac{s_2}{s_2' s_2'' s_{q2}}\right).$$

We defined $U = (s_1'' s_2'' d_1 d_2) u_3$ *where* u_3 *satisfies*

$$u_3 \equiv u_1 \pmod{\frac{s_1}{s_1'' s_1'' d d_1 d_2}}, \text{ and } u_3 \equiv u_2 \pmod{\frac{s_2}{s_2'' s_2'' d d_1 d_2}}.$$

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* $i = 1, \ldots, 6$ *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 note the key distinc-

tions. We factor I_i into three distinction factors as

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

Since I_3 is primitive, we have

$$1 = \gcd(s_2'', s_1''), \quad 1 = \gcd(s_2', s_1''), \quad 1 = \gcd(s_2'', s_1').$$

This simplifies the number of possible products we have to consider. We factor $J_{i,1}$ further to distinguish ramified primes (denoted with a subscript $\mathfrak{q}$) from the unramified primes:

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

Now there are three possible type of products these two ideals can form. Products corresponding to a common place of $\mathbb{F}_q(x)$ lying below $\mathfrak{p}$ and $\mathfrak{q}$ indicate the presence of that polynomial being a factor of the coefficent of ω. This justifies the choice of d_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

$$\operatorname{lcm}\left(\frac{s_1}{s_1's_1''d_1d_2d}, \frac{s_2}{s_2's_2''d_1d_2d}\right) = \frac{s_1s_2}{s_1's_2's_1''s_2''(d_1d_2d)^2}.$$

This differs from S/S' by a factor of 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 theorem. 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''. This fact has been accounted for. □

Much like Theorem 3.6.2 the greatest common divisor calculation looks compli-

cated but in general S'' can be found with fewer terms than the necessary 6.

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

Theorem 3.6.6. *(Multiplication for Type I primes) For $i = 1, 2$ let $I_i = [s_i, s_i'(u_1 + \rho), v_i + w_i\rho + \omega]$ be two ideals . Then $I_1 I_2 = (D) I_3$ where $I_3 = I_1' I_2' J$ and $D = D_1 D_2 D_3$ and these quantities are as follows:*

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

$$D_3 = \frac{\gcd(s_1'/D_2, s_2'/D_1)}{\gcd(s_1'/D_2, s_2'/D_1, w_1 - w_2)},$$

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

$$I_2' = \left[\frac{s_2}{D_1 D_2 D_3}, \frac{s_2'}{D_1 D_3}(u_2 + \rho), v_2 + w_2\rho + \omega\right], \text{ and}$$

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

and the last calculation is done by invoking Theorems 3.5.2, 3.5.8, and 3.6.2.

Proof. We factor I_1 and I_2 as follows

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

$$I_2 = I_{2,1} I_{2,2} = \left[\frac{s_2}{s_2'}, u_2 + \rho, v_2 + w_2\rho + \omega\right] [s_2', s_2'\rho, v_2 + w_2\rho + \omega]$$

Of these four factors the non-primitive part of the product does not arise from $I_{1,1} I_{2,1}$. We find the non-primitive part from the product $I_{1,1} I_{2,2}$ (resp. $I_{2,1} I_{1,2}$). 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:

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

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

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 $\mathfrak{pq}$ and $\mathfrak{p}^2$. If $w_1 - w_2 = 0$ then the associated primes correspond to a square and that justifies the choice for the denominator in D_3. We justify the claim for the ideal J by noting the following equalities.

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

The last ideal is the one given in the theorem 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 Theorem 3.6.2. □

The totally ramified primes will be much easier to deal with. For the two different types, appealing to the theorems that govern their powers from Section 3.4 will be sufficient.

Theorem 3.6.7. *(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 $I_1 I_2 = (D)I_3$ with $I_3 = I_1' I_2' J$ and $D = D_1 D_2 D_3$. These quantities are given as follows:*

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

$$I_1' = \left[\frac{s_1}{D_1 D_2 D_3}, \frac{s_1'}{D_2 D_3}(u_1 + \rho), v_1 - w_1 u_1 + \omega\right],$$

$$I_2' = \left[\frac{s_2}{D_1 D_2 D_3}, \frac{s_2'}{D_1 D_3}(u_2 + \rho), v_2 - w_2 u_2 + \omega\right],$$

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

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

Proof. Much like the previous theorem, the key is to factor the ideals and find where the nonprimitive factors arise. Unlike the previous theorem, constructing the equivalent ideal J is trivial. This is because D_3 is squarefree and Theorem 3.4.1 states the form of these ramified primes. □

Theorem 3.6.8. *(Multiplication for Type III primes) For $i = 1, 2$ let $I_i = [s_i, \rho, s_i''\omega]$ be two ideals such then $I_1 I_2 = (D)I_3$. $I_3 = I_1' I_2' J$ and $D = D_1 D_2 D_3$ where these quantities are given as follows:*

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

$$I_1' = \left[\frac{s_1}{D_1 D_2 D_3}, \rho, \frac{s_1''}{D_2 D_3}\omega\right], \quad I_2' = \left[\frac{s_2}{D_1 D_2 D_3}, \rho, \frac{s_2''}{D_1 D_3}\omega\right], \text{ and}$$

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

Proof. This follows in the same manner as the previous proof. □

Theorem 3.6.9. *(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:

$$D_1 = \gcd(s_2'', s_1/s_1' s_1'', v_1 - u_1 w_1), \quad D_2 = \gcd(s_1'', s_2/s_2' s_2'', v_2 - w_2 u_2),$$

$$D_3 = \frac{\gcd(s_1/s_1' s_1'', s_2'')}{\gcd(s_1/s_1' s_1'', s_2'', v_1 - w_1 u_1)}, \quad D_3 = \frac{\gcd(s_2/s_2' s_2'', s_1'')}{\gcd(s_2/s_2' s_2'', s_1'', v_2 - w_2 u_2)},$$

$$D_5 = \gcd(s_1'/D_4, s_2''/D_1), \quad D_6 = \gcd(s_2'/D_3, s_1''/D_2),$$

$$D_7 = \gcd\left(\frac{s_2''}{D_1 D_5}, \frac{s_1''}{D_2 D_6}\right)$$

$$I_1' = \left[\frac{s_1}{D_2 D_4 D_5 D_6 D_7}, \frac{s_1'}{D_4 D_5}\rho, \frac{s_1''}{D_2 D_6 D_7}(v_1 + w_1\rho + \omega)\right],$$

$$I_2' = \left[\frac{s_2}{D_1 D_3 D_5 D_6 D_7}, \frac{s_2'}{D_3 D_6}\rho, \frac{s_2''}{D_1 D_5 D_7}(v_2 + w_2\rho + \omega)\right], \text{ and}$$

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

Proof. The proof follows in a similar manner as the previous three proofs. We highlight only 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, $\mathfrak{pq}$). The product of $\mathfrak{q}^2\mathfrak{pq}$ is $(P)\mathfrak{q}$. Thus we get $(D_5)[D_5, \rho, \omega]$ (resp $(D_6)[D_6, \rho, \omega]$). We remove the factor D_5 (resp. D_6) from $I_{1,2}$ and $I_{2,3}$ (resp. $I_{2,2}$ and $I_{1,3}$) and consider one last product of $I_{1,3}I_{2,3}$. This is a product where each ideal has primes of the form $\mathfrak{pq}$ and therefore the product must be of the form $(P)\mathfrak{p}$. We get $(D_7)[D_7, \rho, \omega + E]$.

□

We have now 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, $\mathcal{F}/K$ has a totally ramified infinite place with $3 \nmid \deg FI^2$. This latter assumption is necessary since we rely on Theorem 3.2.5. These assumptions also ensure that the ideal class group is isomorphic to of the Jacobian of the curve.

3.7 Elements of minimal norm

The content in this section heavily relies on Section 8 of [3]. We will explain how to find the minimal element of an ideal prior to stating the algorithm. Given an ideal $J = [s, s'(u + \rho), s''(v + w\rho + \omega)]$ we want to find the element in this ideal that has minimal norm. Such an element exists by Theorem 3.2.6 and the algorithm to find the element makes use of Theorem 3.2.5. Write the ideal in a triangular matrix and assign a weight of three times its degree to each column, then the algorithm does elementary row operations on the matrix to minimize the weight.

$$\begin{bmatrix} s & 0 & 0 \\ s'u & s' & 0 \\ s''v & s''w & s'' \end{bmatrix}$$
$$\begin{matrix} \uparrow & \uparrow & \uparrow \\ wt & wt + \deg FI^2 & wt + \deg F^2 I \end{matrix}$$

By Theorem 3.2.5 each of wt, $wt + \deg FI^2$, and $wt + \deg F^2 I$ lie in distinct residue classes modulo three or two columns have their weight coming from the same position (the constant term, the term associated with ρ, or the term associated with ω). If two rows have their weight coming from the same position it will be possible to reduce the weight of one of the rows. The algorithm below just encodes the order in which to do the minimization.

Algorithm 2: 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 $b_1 = (b_{1,1}, b_{1,2}, b_{1,2}) = (s, 0, 0)$, $b_2 = (b_{2,1}, b_{2,2}, b_{2,2}) = (s'u, s', 0)$, and $b_3 = (b_{3,1}, b_{3,2}, b_{3,2}) = (s''v, s''w, s'')$. Assign weights $w_{i,1} = 3 \deg b_{i,1}$, $w_{i,2} = 3 \deg b_{i_2} + \deg FI^2$, and, $w_{i,3} = 3 \deg b_{i,3} + \deg F^2 I$ (these weights are the degree of the norm of the respective components of b_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.

We can now calculate an element of minimal norm. The goal will be to construct a canonical basis for the principal ideal generated by this element.

3.8 Canonical basis

The algorithm for finding a canonical basis for the principal ideal generated by an element of $\mathcal{O}_{\mathcal{F}}$ needs little modification from Bauer's work. The key change here is that the products integral basis presented in Section 3.2 does not have the same form as the analogous products of basis in purely cubic function fields. This primarily affects the matrix seen in step 1 of the algorithm.

Algorithm 3: CanBasis

Input: $a + b\rho + c\omega \in \mathcal{O}_F$
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 $d = \gcd(a_1, b_2)$, $s = c_3/d$, $s' = b_2/d$, 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.

3.9 Composition and reduction in the ideal class group

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

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

The proof of correctness has been established in the previous sections. Step 1 invokes the multiplication theorems proved in Section 3.6. Step 2 is ideal inversion. Step 5 is ideal division. While this may seem anticlimactic, "we have plowed, planted, and fertilized; we should not be surprised if, occasionally, something is available for easy picking." [8, p. 77] For nearly any cubic function field in characteristic three with a totally ramified place at infinity, we have given composition and reduction in the ideal class group. Example 3.2.1 represents a function field with a totally ramified place for which we have not given composition and reduction in the ideal class group.

3.10 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 $T^3 - T + x^4 + \alpha$. We let

$$I_1 = [x, \alpha^9+\alpha^8-\alpha^7-\alpha^6-\alpha^5+\alpha^4+\alpha^3-1+\rho, -\alpha^9+\alpha^8+\alpha^7-\alpha^6-\alpha^5+\alpha^4-\alpha^2+1+\omega]$$

and

$$I_2 = [x+\alpha^5, -\alpha^9+\alpha^8-\alpha^6+\alpha^5-\alpha^4-\alpha^3+\alpha-1+\rho, \alpha^9-\alpha^8-\alpha^7+\alpha^5-\alpha^4-\alpha^3+\alpha^2-1+\omega].$$

We compose these two ideals and give their reduction following Algorithm 4.

Step 1. We begin by calculating $I_3 = I_1 I_2$. We know the result will be of the form $I_3 = [s_3, u_3 + \rho, v_3 + \omega]$. Since $x + \alpha^5$ and x are relatively prime we may invoke Theorem 3.6.1 to see

$$\begin{aligned} s_3 &= x^2 + \alpha^5 x, \\ u_3 &= (\alpha^8 - \alpha^7 - \alpha^6 + \alpha^4 - \alpha - 1)x + (\alpha^9 + \alpha^8 - \alpha^7 - \alpha^6 - \alpha^5 + \alpha^4 + \alpha^3 - 1), \text{ and} \\ v_3 &= (\alpha^9 + \alpha^8 - \alpha^6 + \alpha^5 - \alpha^4 - \alpha^2 + \alpha + 1)x - \alpha^9 + \alpha^8 + \alpha^7 - \alpha^6 - \alpha^5 + \alpha^4 - \alpha^2 + 1. \end{aligned}$$

Step 2. We compute $I_4 = \overline{I_3}$. It is clear that this inverse will have the form $[s_4, s_4\rho, v_4 + w_4\rho + \omega]$. By appealing to Theorem 3.5.2, we have

$$\begin{aligned} s_4 &= x^2 + \alpha^5 x, \\ v_4 &= (-\alpha^9 - \alpha^8 + \alpha^6 - \alpha^5 + \alpha^4 + \alpha^2 - \alpha - 1)x + \alpha^9 - \alpha^8 - \alpha^7 + \alpha^6 + \alpha^5 - \alpha^4 + \alpha^2, \text{ and} \\ w_4 &= (-\alpha^8 + \alpha^7 + \alpha^6 - \alpha^4 + \alpha + 1)x - \alpha^9 - \alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 - \alpha^4 - \alpha^3 + 1. \end{aligned}$$

Step 3. The element of minimal norm is $x^2 + \alpha^5 x$. At this point we note that this means that the product found in Step 1 is already distinguished. However, we continue the calculation to verify this fact.

Step 4. The canonical basis for the element of minimal norm is $\langle x^2+\alpha^5 x\rangle[1,\rho,\omega]$.

Step 5. We calculate $\langle x^2+\alpha^5 x\rangle/I_4$ according to Theorem 3.5.8. We see that this inverse is I_3 as given in Step 1.

Chapter 4

Conclusion and Open Problems

This thesis presented a brief history of algebraic curves and number theory associated with function fields. This contributes to the understanding of cubic function fields in characteristic three. This work expands on the current research on cubic function fields [3, 22, 21, 32, 31] by considering the case where the rational function field has characteristic three. We summarize these results and discuss a few questions that have arisen in the course of this work.

4.1 Summary

Previous work on cubic function fields largely ignored characteristics two and three. This thesis sought to remedy this situation by examining cubic function fields in characteristic three. The results are divided into two categories. First, we calculated basic invariants of the function field and then we described arithmetic in the ideal class group for a particular set of curves.

The first goal was to define a standard model for a cubic function field in characteristic three. Motivated by the case for cubic function fields of characteristic greater than three, we showed that $T^3 - AT + B = 0$ can provide a standard model with sufficient restrictions on A and B. These restrictions are motivated by the integral basis calculation and allow us to remove certain types of singular points. Assuming a standard model, we gave an explicit integral basis of this function field that is suit-

able for computations. Following the work of Delone and Faddeev [9] this calculation not only provides the integral basis but also gives the field discriminant. The field discriminant yields the different exponents of the finite places. Appealing to specific completions allowed us to calculate the different exponent of the infinite place. This accounts for all the different exponents and the Hurwitiz Genus formula now gave the genus of any cubic function field in characteristic three. The above provided a near complete picture of the splitting of places; all that remained was distinguishing the three non-ramfied splitting types. This thesis shows how an arbitrary place splits.

The invariants and an integral basis suitable for computations lead to a series of results on arithmetic in the ideal class group. We gave an explicit triangular basis for the prime ideals and their powers. This motivated ideal inversion, division, and multiplication. We followed the work of Bauer in [3] to perform arithmetic in the ideal class group. This was enabled by Theorem 3.2.5 allowing us to find a unique minimal element in a given ideal class. However, for this to work we needed the infinite place to be totally ramified. While this certainly addressed the vast majority of the curves, there were a few remaining curves with a totally ramified place that were unaccounted for. We deal with these in the next section.

4.2 Open problems

Here we list a few open problems encountered during the research. The first problem arose as Example 3.2.1. The second problem is related to calculating fundamental units using Voronoi's algorithm. This technique worked well when applied to cubic function fields of characteristic greater than three and provides the inspiration for the second problem encountered. The next problem comes from recent work in tabulating

function fields and number fields by discriminant. The last problem is motivated by computational concerns.

4.2.1 Norm problems

Example 3.2.1 provides an example of a cubic function field in characteristic three with a totally ramified infinite place but would not satisfying the hypothesis of Theorem 3.2.5. From Chapter 2 we know that there exist elements of minimal norm in a given ideal class. For a complete treatment, we would like to be able to account for these cases. While these cases are exceptionally rare, there is no a priori reason to think that we should not be able to do arithmetic in the ideal class group.

4.2.2 Voronoi's Algorithm

As noted in Chapter 1, the immediate predecessors to this work examined the infrastructure of unit rank one purely cubic function fields of characteristic greater than 3. The reason was primarily historical; that is, this case bears the closest resemblance to purely cubic number fields. The primary motivation came from calculating fundamental units and Voronoi's algorithm was the method used. Unfortunately, a rote application of Voronoi's Algorithm fails in characteristic three.

Section 6 of [31] related properties of elements of a function field if they have the "correct" basis. Let F be a unit rank one cubic function field with $q \equiv -1 \pmod 3$ and $\mathrm{char}F \geq 5$ and consider $\theta = l + m\rho + n\omega \in F$ with $l, m, n \in \mathbb{F}_q[x]$. Then define

$$\begin{aligned} \xi_\theta &= \theta - l &&= m\rho + n\omega \\ \eta_\theta &= (1+2\iota)^{-1}(\theta^{(1)} - \theta^{(2)}) &&= m\rho - n\omega \\ \zeta_\theta &= \theta^{(1)} + \theta^{(2)} &&= 2l - m\rho - n\omega \end{aligned}$$

where ι is a primitive cube root of unity. Then

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

While the above are certainly true for the function fields under consideration in [31], if applied by rote to the function fields considered in Chapter 3 of this thesis it is not true that $\theta^{(1)}\theta^{(2)} = \frac{1}{4}(3\eta_\theta^2 + \zeta_\theta^2)$. The question is, how do we formulate Voronoi's method to work in characteristic three?

4.2.3 Tabulations

Chapter 9 of Cohen's *Advanced Topics in Computational Number Theory* outlines some of the progress made in tabulating number fields by their discriminant. A few authors have already considered some of the generalizations to cubic function fields [29, 30].

There are two obstacles to overcome in tabulating cubic function fields in characteristic three. The first major obstacle is the reliance of [29, 30] on cubic forms to do the tabulating. Cubic forms do have the same arithmetic properties in characteristic three as they do in other characteristics. The second obstacle is more fundamental and it is that enumeration by discriminant seems to be insufficient.

Take a curve of the form $T^3 - T + B = 0$ where $B \in \mathbb{F}_q[x]$ and $3 \nmid \deg B$. Recall that the genus of this function field is $g = \deg B - 1$. We can easily create an infinite family of function fields of discriminant 1 having a different genus (depending solely on the degree of B). This is because the discriminant does not account for the infinite place and we can force the infinite place to have an arbitrary different exponent. Since the previously considered extensions were all tame extensions, bounding the discriminant bounded the different exponent for all places.

4.2.4 Class Number Computations

Following the original motivation given by Gauss, we should be able to compute class numbers of the cubic function fields discussed in this thesis. To do so would require an implementation of the ideal arithmetic. Along with an implementation we could analyze the complexity of the algorithms stated. We could also aim for an efficient implementation of a given class of curves. By choosing nonsingular genus three curves (genus one and two, as mentioned before, would be considered as elliptic and hyperelliptic curves) we could attempt to follow Lange [23] in finding an explicit formula for arithmetic on these genus three curves. If this was done, not only would we have an analysis of the complexity, but we would likely have an explicit operation count in terms of finite field additions, multiplications and inverses.

Bibliography

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen I*, Mathematische Zeitschrift **19** (1924), 153–206.

[2] E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Sem. Hamburg **5** (1927), 225–231.

[3] M. Bauer, *The arithmetic of certain cubic function fields*, Math. Comp. **73** (2004), no. 245, 387–413 (electronic). MR MR2034129 (2004k:11179)

[4] C. Boyer, *A History of Mathematics*, second ed., John Wiley & Sons Inc., New York, 1991. MR MR1094813 (92a:01003)

[5] D. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101. MR MR866101 (88f:11118)

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR MR1228206 (94i:11105)

[7] ———, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR MR1728313 (2000k:11144)

[8] J. Conway, *Functions of One Complex Variable*, Springer-Verlag, New York, 1973, Graduate Texts in Mathematics, 11. MR MR0447532 (56 #5843)

[9] B. Delone and D. Faddeev, *The Theory of Irrationalities of the Third Degree*, Translations of Mathematical Monographs, Vol. 10, American Mathematical Society, Providence, R.I., 1964. MR MR0160744 (28 #3955)

[10] G. Frei, *The unpublished section eight: on the way to function fields over a finite*

field, The Shaping of Arithmetic after C. F. Gauss's *D*isquisitiones arithmeticae, Springer, Berlin, 2007, pp. 159–198. MR MR2308282

[11] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Math. Comp. **76** (2007), no. 257, 475–492 (electronic). MR MR2261032 (2007j:11174)

[12] V. Goppa, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR **259** (1981), no. 6, 1289–1290. MR MR628795 (82k:94017)

[13] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR MR0463157 (57 #3116)

[14] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper II, III*, Journal für die reine und angewandte Mathematik **175** (1936), 69–88, 193–208.

[15] ———, *Number Theory*, German ed., Classics in Mathematics, Springer-Verlag, Berlin, 2002, Reprint of the 1980 English edition [Springer, Berlin; MR0562104 (81c:12001b)], Edited and with a preface by Horst Günter Zimmer. MR MR1885791

[16] T. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 1980, Reprint of the 1974 original. MR MR600654 (82a:00006)

[17] M. Jacobson, R. Scheidler, and A. Stein, *Fast arithmetic on hyperelliptic curves via continued fraction expansions*, Advances in coding theory and cryptography, Ser. Coding Theory Cryptol., vol. 3, World Sci. Publ., Hackensack, NJ, 2007, pp. 200–243. MR MR2454114 (2010a:14054)

[18] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209. MR MR866109 (88b:94017)

[19] ———, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), no. 3, 139–150. MR

MR1007215 (90k:11165)

[20] H. Kühne, *Angenäherte Auflösung von Congruenzen nach Primmodulsystemen in Zusammenhang mit den Einheiten gewisser Körper*, Journal für die reine und angewandte Mathematik **126** (1903), 102–115.

[21] 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.

[22] E. Landquist, P. Rozenhart, R. Scheidler, J. Webster, and Q. Wu, *An explicit treatment of cubic function fields with applications*, To appear in Canadian Journal of Mathematics.

[23] T. Lange, *Formulae for arithmetic on genus 2 hyperelliptic curves*, Appl. Algebra Engrg. Comm. Comput. **15** (2005), no. 5, 295–328. MR MR2122308 (2005j:14082)

[24] D. Lorenzini, *An Invitation to Arithmetic Geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996. MR MR1376367 (97e:14035)

[25] M. Mang, *Berechnung von Fundamentaleinheiten in algebraischen, insbesondere reinkubischen Kongruenzfuktionenkörpern*, Diplomarbeit, Universität des Saarlandes, 1987.

[26] V. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci., vol. 218, Springer, Berlin, 1986, pp. 417–426. MR MR851432 (88b:68040)

[27] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyclopedia of Mathematics and its Applications, vol. 30, Cambridge University

Press, Cambridge, 1997, Revised reprint of the 1989 original. MR MR1483321 (98f:11111)

[28] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR MR1876657 (2003d:11171)

[29] P. Rozenhart, *Fast Tabulation of Cubic Function Fields*, Ph.D. thesis, University of Calgary, 2009.

[30] P. Rozenhart and S. Scheidler, *Tabulation of cubic function fields with imaginary and unusual Hessian*, Proceedings of the Eighth Algorithmic Number Theory Symposium ANTS-VIII, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 357–370.

[31] R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 2, 609–631. MR MR1879675 (2002k:11209)

[32] ———, *Algorithmic aspects of cubic function fields*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 395–410. MR MR2138010 (2006c:11136)

[33] R. Scheidler and A. Stein, *Unit computation in purely cubic function fields of unit rank 1*, Algorithmic Number Theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 592–606. MR MR1726104 (2000k:11145)

[34] ———, *Voronoi's algorithm in purely cubic congruence function fields of unit rank* 1, Math. Comp. **69** (2000), no. 231, 1245–1266. MR MR1653974 (2000j:11177)

[35] ———, *Class number approximation in cubic function fields*, Contrib. Discrete

Math. **2** (2007), no. 2, 107–132 (electronic). MR MR2358265 (2009b:11152)

[36] H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, Berlin, 1993. MR MR1251961 (94k:14016)

[37] E. Thomé and C. Diem, *Index calculus in class groups of non-hyperelliptic curves of genus three*, Journal of Cryptology **21** (2008), 593–611.

[38] H. C. Williams, G. Cormack, and E. Seah, *Calculation of the regulator of a pure cubic field*, Math. Comp. **34** (1980), no. 150, 567–611. MR MR559205 (81d:12003)

[39] R. Zuccherato, *New applications of elliptic curves and function fields in cryptography*, Ph.D. thesis, University of Waterloo, 1997.