2013-09-09

Constructing and Tabulating Dihedral Function Fields

Weir, Colin

UNIVERSITY OF CALGARY

Constructing and Tabulating Dihedral Function Fields

by

Colin Weir

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
AUGUST, 2013

Abstract

We present and implement algorithms for constructing and tabulating odd prime degree ℓ dihedral extensions of a rational function field $k_0(x)$, where k_0 is a perfect field with characteristic not dividing 2ℓ. We begin with a class field theoretic construction algorithm when k_0 is a finite field. We also describe modifications to this algorithm to improve the run time of its implementation.

Subsequently, we introduce a Kummer theoretic algorithm for constructing dihedral function fields with prescribed ramification and fixed quadratic resolvent field, when k_0 is a perfect field and not necessarily finite. We give a detailed description of this Kummer theoretic approach when k_0, or a quadratic extension thereof, contains the ℓ-th roots of unity. Avoiding the case when k_0 is infinite and the quadratic resolvent field is a constant field extension of $k_0(x)$, we show that our Kummer theoretic algorithm constructs *all* degree ℓ dihedral extensions of $k_0(x)$ with prescribed ramification. This algorithm is based on the proof of our main theorem, which gives an exact count of such fields.

When k_0 is a finite field, we implement and experimentally compare the run times of the class field theoretic and Kummer theoretic construction algorithms. We find that the Kummer theoretic approach performs better in all cases, and hence we use it later in our tabulation method.

Lastly, utilizing the automorphism group of $\mathbb{F}_q(x)$, we present a tabulation algorithm to construct all degree ℓ dihedral extensions of $\mathbb{F}_q(x)$ up to a given discriminant bound, and we present tabulation data. This data is then compared to known

asymptotic predictions, and we find that these estimates over-count the number of such fields. We also give a formula for the number of degree ℓ dihedral extensions of $\mathbb{F}_q(x)$ when $q \equiv \pm 1 \bmod 2\ell$, with discriminant divisors of minimum possible degree.

Table of Contents

Abstract ii

Table of Contents iv

1 Introduction 1
- 1.1 Structural Overview . . . 6

2 Background and Preliminary Results 13
- 2.1 Function Fields . . . 13
  - 2.1.1 Algebraic Function Fields . . . 14
  - 2.1.2 Places . . . 15
  - 2.1.3 Extensions of Function Fields . . . 18
  - 2.1.4 Divisors, Genus and Different . . . 20
- 2.2 Galois Representations and L-functions . . . 26
  - 2.2.1 Galois Theory of Function Fields . . . 26
  - 2.2.2 Representation Theory . . . 29
  - 2.2.3 L-functions . . . 34
- 2.3 Dihedral Function Fields . . . 36

3 Construction of Dihedral Function Fields via Class Field Theory 42
- 3.1 Class Fields of Function Fields . . . 43
- 3.2 Class Field Theoretic Construction Algorithms . . . 46

4 Kummer Theoretic Approach with ℓ-th Roots of Unity 58
- 4.1 Constructing and Counting Dihedral Function Fields . . . 59
  - 4.1.1 Kummer Theory . . . 60
  - 4.1.2 Virtual Unit Decomposition . . . 65
  - 4.1.3 The Number of $\mathcal{D}_\ell$ Function Fields . . . 70
  - 4.1.4 Defining equations . . . 73
- 4.2 Construction Algorithms . . . 74

5 Kummer Theoretic Approach without ℓ-th Roots of Unity 84
- 5.1 Construction with Quadratic Resolvent $K_2 = K_0(\zeta_\ell)$ . . . 85
- 5.2 Construction with Quadratic Resolvent K_2 when K_2/K_0 is geometric 92
- 5.3 Construction when K_2/K_0 is geometric and $[k_0(\zeta_\ell) : k_0] = 2$ . . . 96
- 5.4 Construction Algorithms when $[k_0(\zeta_\ell) : k_0] = 2$ . . . 99

6 Numerical Results and Tabulation Techniques **106**
6.1 Tabulation Method 107
6.2 Implementations and Numerical Results 111
6.2.1 Asymptotic Comparison when $\ell = 3$ 113
6.2.2 Explicit Formulas for $B = 2(\ell - 1)$ 116
6.3 Tables of Numerical Data 120

7 Conclusions **125**

Bibliography **132**

Chapter 1

Introduction

Two important problems in algebraic and algorithmic number theory are the construction of global fields of a fixed discriminant or prescribed ramification – with its curve analogue of constructing Galois covers of fixed genus – and the tabulation of global fields with a certain Galois group up to some discriminant or genus bound. The latter problem goes hand in hand with asymptotic estimates for the number of such fields; for example, estimates for cubic number fields were first given in [15] and for quartics in [3]. There is a sizable body of literature on construction, tabulation, and asymptotic counts of number fields; a rather comprehensive survey of known results can be found in [9], and extensive tables of data are available at [26].

Far less is known in the function field setting; only the asymptotic counts for cubic [14] and abelian [43] extensions have been proved. However, there is a general program described by Venkatesh and Ellenberg [40] for formulating these asymptotic estimates for both number fields and function fields. In particular, they point out the "alarming gap between theory and experiment" in asymptotic predictions for number fields. In the case of cubic number fields, this inconsistency led Roberts [29] to conjecture the secondary term in the theorem of Davenport and Heilbronn in [15]. His conjecture was later proved independently by Bhargava, Shankar, and Tsimerman [4] and by Taniguchi and Thorne [39]. In the function field setting,

however, there is practically no experimental data to potentially identify a similar such gap. In fact, the only known algorithms for constructing non-abelian function fields are those which construct non-Galois cubic fields with squarefree discriminant [25]. Recently although, Pohst [28] showed how to construct all non-Galois cubic extensions of $\mathbb{F}_q(x)$ with a given discriminant, which also leads to such an algorithm (though no description of an implementation is provided in [28]). In fact, Pohst's method is a special case of the class field theoretic approach that we will present. Tabulation methods for certain classes of cubic function fields with squarefree discriminants can be found in [31], [33] and [32], though neither can provide complete lists of cubic function fields in general.

This thesis represents the next steps in function field construction and tabulation. We present, implement, and compare new algorithms for constructing all odd prime degree dihedral function fields with prescribed ramification (which includes all non-Galois cubics) over finite fields in all characteristics greater than 3, and over infinite perfect fields under some restrictions. This provides the first example of a method to construct function fields over infinite constant fields with a fixed non-abelian Galois group and given ramification. Via these method we are able to provide the first complete tables of function fields over finite fields whose discriminant divisors have degree below a fixed bound. In particular, only now can the asymptotic estimates for cubic function fields be truly compared to the actual number of cubic fields in characteristics greater than 3. Moreover, via Kummer theory, we obtain a new and fruitful understanding of dihedral function fields. With this view point, we obtain new explicit formulas for the number of dihedral function fields in several cases, generalizing the work of Howe in [42].

Many of the contributions of this thesis are inspired by the work of Cohen [8, 11] in the number field setting, and based upon my work that first appeared in [42]. Let ℓ be an odd prime. In [42] we presented a method for constructing all degree ℓ extensions of $\mathbb{F}_q(x)$ with prescribed ramification and with Galois group isomorphic to the dihedral group of order 2ℓ, when $q \equiv 1 \bmod 2\ell$. Here, and going forward, we make the common abuse of language by saying that a field has Galois group $\mathcal{G}$ when we are in fact referring to the Galois group of its Galois closure.

In [42] we used a Kummer-theoretic approach inspired by the methods of Cohen [8, Ch 5], [11] for number fields. This construction method can be converted into a tabulation algorithm in the usual manner via iteration. However, in [42] we explained how to use the automorphism group $\mathrm{PGL}(2, q)$ of $\mathbb{F}_q(x)$ to effect significant speed-ups in this case. We note that this technique is unique to the function field setting and cannot be utilized in the number field scenario, as there are no nontrivial automorphisms on the rational numbers. Exploiting $\mathbb{F}_q(x)$-automorphisms reduces the number of constructions by a factor of order q^3 compared to the naïve approach. We presented our improved tabulation procedure along with numerical data obtained from an implementation in Magma [5]. It is important to note that in the special case $\ell = 3$, our algorithm generates complete tables of non-Galois cubic function fields over $\mathbb{F}_q(x)$ up to a given discriminant bound when $q \equiv 1 \bmod 3$.

In this thesis we present two general methods for constructing degree ℓ dihedral function fields. First, we explore a class field theoretic technique for constructing dihedral function fields over finite fields with characteristic different from 2 and ℓ. We then show how to improve this algorithm, making it practical for implementation purposes. We note that this method specializes to the one presented in [28] when

$\ell = 3$. We also note that we developed our algorithm before the publication of [28] and were unaware of Pohst's work at the time.

Second, we present the Kummer theoretic approach of [42], but generalized to a wider class of function fields. We extend this approach to construct degree ℓ dihedral function fields over an arbitrary perfect field k_0 of characteristic not dividing 2ℓ, when k_0, or a quadratic extension thereof, contains the ℓ-th roots of unity. When k_0 is a finite field $\mathbb{F}_q$, we thus obtain algorithms for constructing all dihedral function fields with prescribed ramification when $q \equiv \pm 1 \bmod 2\ell$. Notice that when $\ell = 3$, this now allows us to construct (and later tabulate) non-Galois cubic function fields over finite fields of characteristic greater than 3. When k_0 is not finite, but perfect and of characteristic not dividing 2ℓ, we obtain a method for constructing all dihedral function fields with prescribed ramification whose quadratic resolvent field is not a constant field extension of $k_0(x)$. Hence, eventually we make the following assumption:

Assumption: COEFF (*C*onstants are *O*nly *E*xtended over *F*inite *F*ields). When K_2 is a quadratic constant field extension of a rational function field K_0, we assume that the constant field k_0 of K_0 is a finite field. When K_2/K_0 is a geometric field extension, we do not assume that k_0 is finite, only that it is perfect. In both cases we assume that $\mathrm{char}(k_0) \nmid 2\ell$.

The reasons for this restriction are quite natural. All extensions of finite fields are cyclic and thus not dihedral. However, when k_0 is a number field for example, there are infinitely many degree ℓ dihedral extensions of k_0 and hence infinitely many unramified dihedral extensions of $k_0(x)$. The methods to construct and tabulate such extensions are number field theoretic and beyond the scope of this thesis (see

[8, Ch 8,9] and [11] for known methods). Consequently, we will eventually need to invoke Assumption COEFF to avoid this case. However, given a discriminant divisor Δ that is not a multiple of $\ell - 1$, our algorithms construct all geometric degree ℓ dihedral function fields with perfect constant field k_0 and discriminant Δ when the characteristic of k_0 does not divide 2ℓ. Therefore, this thesis contains the first known algorithm for constructing all geometric function fields over an infinite constant field with a fixed non-abelian Galois group and prescribed ramification.

When the constant field k_0 is a finite field $\mathbb{F}_q$, we implement the class field theoretic and Kummer theoretic approaches in Magma [5], and compare the two for several values ℓ and q where $q \equiv \pm 1 \bmod 2\ell$. For the case $\ell = 3$, to the best of my knowledge, this is the first implementation and profiling of the class field theoretic algorithm discussed in [28]. However, we find that our Kummer theoretic algorithm is multiple times faster than the class field theoretic method in all cases considered, and considerably faster still when $q \equiv -1 \bmod 2\ell$. Hence, we later use the Kummer theoretic method in our tabulation algorithms.

To tabulate dihedral fields, we use the technique I first developed in [42]. In this thesis, we show how to use the automorphism group $\mathrm{PGL}(2, q)$ of $\mathbb{F}_q(x)$ to improve tabulation over an arbitrary finite field. We present our improved tabulation procedure and the numerical data obtained from an implementation in Magma [5]. We then compare this data to the asymptotic formula of [14] when $\ell = 3$. This represents the first true comparison of this formula to complete counts of cubic function fields over $\mathbb{F}_q$ when $q \equiv -1 \bmod 3$ (the case $q \equiv 1 \bmod 3$ was originally presented in [42]). As in the number field setting, we find considerable "gaps" between the asymptotic predictions and the actual number of cubic function fields, regardless of the character-

istic. Moreover, like the number field setting, the asymptotic formulas overestimate the actual number of cubic fields.

Lastly, we provide an explicit formula for the number of degree ℓ dihedral function fields over a finite field whose discriminants divisor have smallest possible degree. This formula is originally due to Howe [42] for the case $q \equiv 1 \bmod 2\ell$, and here we extend it to the case when $q \equiv -1 \bmod 2\ell$. An interesting consequence of these two formulas is that the total number of index ℓ subgroups of class groups of genus 1 quadratic extensions of $\mathbb{F}_q(x)$ is a function of ℓ and q which does not vary with the presence of ℓ-th roots of unity in $\mathbb{F}_q$. We find this especially interesting because the expected number of index ℓ subgroups in the class group of any one of these extensions depends on the presence of ℓ-th roots of unity in $\mathbb{F}_q$. These and other consequences are discussed further in the conclusions (Chapter 7).

In summary, we present, implement, and compare new algorithms for constructing all dihedral function fields of odd prime degree with a given discriminant divisor. When the constant field is infinite, this yields the first method to construct function fields with a fixed non-abelian Galois group and given ramification. New and complete tables of function fields over finite fields are produced and compared to the known asymptotic estimates. Moreover, via Kummer theory, we present an in-depth approach to dihedral function fields, giving rise to new explicit formulas for counting the number of these fields in several cases.

1.1 Structural Overview

Throughout this thesis we make a strong effort towards notational consistency and hence use several conventions. For example, K will always denote an arbitrary func-

tion field with constant field k, while K' will denote an extension of K. K_0 is always a rational function field with constant field k_0 and transcendental x. We use K_i to denote a degree i extension of K_0, where K_2 is obtained by adjoining y or z. Note that we nearly always assume that $\mathrm{char}(k_0) \nmid 2\ell$, where ℓ is an odd prime. The letter T is reserved for the transcendental of a polynomial ring. Furthermore, general groups are represented with the calligraphy font ($\mathcal{G}$, $\mathcal{H}$ for example), and their elements are always Greek letters (usually $\varrho, \tau, \sigma, \gamma$); this includes Galois groups and automorphism groups. However, $\alpha, \beta, \kappa, \theta$ are reserved for elements of a function field, with κ typically in K_0, and θ typically a root of $T^\ell - \alpha$. Capital Greek letters are used for maps. Divisors of K are denoted with capital letters such as D, E, while divisors of K' are denoted with D', E'. Constants, including elements of k_0, are represented with lower case letters. The remaining notation is introduced as needed.

In Chapter 2, we present a range of material required to understand and describe dihedral function fields. In the first section, we describe function fields and their extensions, places and their valuations. We then we discuss divisors and Riemann-Roch spaces amoung other topics. This allows us to present definitions for the genus, different and discriminant divisor of a function field, and state the Riemann-Hurwitz genus formula. With this introductory material in hand, the main goal of the rest of this chapter is to introduce the subject matter required to prove Theorem 2.3.2; an explicit formula for the discriminant divisor of a dihedral function field.

In Section 2.2, we recall basic Galois theory and describe the action of the Galois group of a function field on its various structures. This section also contains the definitions of interia and decomposition groups which will become useful later on for presenting Artin L-functions.

As Artin L-functions are associated to representations, Subsection 2.2.2 presents a basic introduction to finite representation theory. The definition of a finite Galois representation is given along with that of its associated character. Moreover, we discuss the representations of the group $\mathcal{D}_\ell$, the dihedral group with 2ℓ elements. It is here that we find a linear relationship between the characters of the induced representations of subgroups of $\mathcal{D}_\ell$.

Subsection 2.2.3 begins with an introduction to zeta function of an algebraic function field, which then leads to an introduction to Artin L-functions. At this point we see that the Artin L-function of an induced representation is the zeta function of its fixed field, and that the Artin L-function of the sum of two representations if the product of the L-functions of these representations. This is a key componenent of the proof of Theorem 2.3.2, which is finally provided in the following section. The chapter concludes with a general description of how we intend to construct dihedral function fields, namely by constructing cyclic degree ℓ extensions of quadratic fields, such that the resulting field is dihedral and has the correct discriminant divisor.

As we wish to construct cyclic extensions of quadratic fields, we proceed to study class field theory. In Chapter 3 we begin with a brief introduction to the main results of class field theory of function fields. In Section 3.2 we see how to use class field theory to construct all dihedral function fields over a finite field with a given discriminant divisor. In particular, we show that one can construct cyclic extensions of quadratic fields by considering index ℓ subgroups of ray class groups. Moreover, we discuss how all dihedral function fields over finite fields can be constructed in this way. These ideas are first presented in Algorithm 3.1, and to the best of my knowledge are new results for $\ell > 3$. We then prove two propositions that allow us to refine Algorithm 3.1

into the more practical version described by Algorithm 3.2. Much later in the thesis, in Chapter 6, we discuss the implementation of Algorithm 3.2 and show that, while it is widely applicable, it computes dihedral fields much slower than the Kummer theoretic algorithms presented in the next two chapters.

In Chapter 4, we present an alternative to Algorithm 3.1 when the underlying rational function field contains the ℓ-th roots of unity. This chapter is based upon my work that first appeared in [42], though generalized to prefect constant fields with ℓ-th roots of untiy under Assumption COEFF. The material of [42] was edited by Everett Howe who made several additinos to the proofs and notation. In particular, in Subsection 4.1.4, we present his method for producing defining equations for dihedral function fields, instead of the one I originally proposed. The remainder of this chapter, however, is primarily my own work.

The construction method of Chapter 4 stems from Kummer theory as presented in Section 4.1.1. Kummer theory states that if a function field K contains the ℓ-th roots of unity, then every cyclic degree ℓ extension K'/K is radical, i.e. $K' = K(\sqrt[\ell]{\alpha})$ for some $\alpha \in K$. The remainder of this chapter is primarily dedicated to constructing elements α in a quadratic field such that the resulting Kummer extension is dihedral with the appropriate discriminant divisor. To that end, in Subsection 4.1.2 we introduce the theory of (ℓ-)virtual units for function fields. This is based upon the ideas of Cohen in the number field setting [11]. Of note is the fact that we present the theory of virtual units independent of the presence of roots of unity. This will become especially useful in the following chapter.

In Subsection 4.1.3, we give a constructive proof of the main result of Chapter 4; an exact count of the number of dihedral degree ℓ extensions of K_0 with a given quadratic

resolvent field K_2 and discriminant divisor Δ. This naturally leads to Algorithm 4.1 in Section 4.2 for constructing degree ℓ dihedral function fields. Here make use of Howe's formula for defining equations [42] which we present in Subsection 4.1.4.

In Chapter 5, we present original work to construct dihedral function fields via Kummer theory when k_0 does not contain the ℓ-th roots of unity. First, in Section 5.1, we consider the case when the quadratic resolvent field $K_2 = K_0(\zeta_\ell)$. Upon making Assuption COEFF, we restrict to the case that k_0 is a finite field. We then apply our Kummer theoretic approach to this case and present Algorithm 5.1 to construct all degree ℓ dihedral function fields with a given discriminant divisor.

In the following section we consider the situation when the quadratic resolvent field K_2 is a geometric extension of K_0. In this case we adjoin the roots of unity to K_2 and apply our Kummer theoretic methods of Chapter 4 to $K_2(\zeta_\ell)$. This results in Algorithm 5.2. The inefficiencies of this generic method motivates our subsequent restriction to the case $[k_0(\zeta_\ell) : k_0] = 2$. While this may seem rather restrictive, when $\ell = 3$, this still allows us to construct all non-Galois cubic function fields over finite fields with characteristic greater than 3, and prescribed ramification.

In Section 5.3, we perform a detailed analysis of the case that K_2/K_0 is a geometric extension and $[k_0(\zeta_\ell) : k_0] = 2$. We show that to apply our Kummer theoretic construction of dihedral function fields, one does not need to perform calculations in the quartic field $K_2(\zeta_\ell)$ but rather in a subfield, namely the quadratic twist of K_2. Indeed, to construct all degree ℓ dihedral function fields with a given discriminant divisor Δ in this case, one need only apply Algorithm 4.1 with input ℓ, Δ, and the twist of K_2. It is this result – that one need only perform calculations in a quadratic extension of K_0 – that leads to significant improvements over the class field theoretic

approach in this case. The details of this new method are discussed in Section 5.4, and presented in Algorithm 5.3.

In Chapter 6 we discuss our findings from tabulating dihedral function fields over finite fields whose discriminant divisors have degree bounded by B. The general technique we use for tabulation is my own work originally presented in [42]. Here, we also compare the implementations of our class field theoretic and Kummer theoretic construction algorithms for various values of ℓ and q when $q \equiv \pm 1 \bmod 2\ell$. In all cases we considered, the Kummer theoretic approach constructs dihedral fields significantly faster than the algorithm involving class field theory. The data from our comparison can be found in Table 6.1, where we also include the ratio of the time it took each these algorithms to perform the various constructions. This speed-up justifies our use of the Kummer theoretic algorithms during tabulation.

In Section 6.1, we introduce how to use the automorphism group of K_0 to tabulate function fields more efficiently than the naïve method of iteration. We implement this approach and summarize our findings for various values of q, ℓ, and B. The data from our findings is presented in Tables 6.2 and 6.3. In these tables we also record the approximate improvement factor of our method over the standard method of iteration with utilizing the automorphism group. In all cases considered our technique is several times faster than the naïve approach.

With this tabulation data in hand, in Subsection 6.2.1 we compare our data counting cubic function fields to the asymptotic predictions of [14]. We note that there are no known explicit asymptotic formulas for degree ℓ dihedral function fields with $\ell > 3$. We present the results of this comparison when $\ell = 3$ in Table 6.4. As in the number field setting, we find that the asymptotic estimates over-count the actual number of

cubic function fields, resulting in a similar "gap between theory and experiment", as pointed out in the number field scenario by Ellenberg and Venkatesh [40].

When $q \equiv 1 \bmod \ell$, Everett Howe in [42] proves an explicit formula for the number of degree ℓ dihedral function fields over a finite field $\mathbb{F}_q$ whose discriminant divisors have the smallest possible degree. In Subsection 6.2.2, we present that result and extend it to the case that $q \equiv -1 \bmod \ell$. We find that the two formulas for these cases are nearly identical; the only difference being when the quadratic resolvent field is a constant field extensions. This leads to some interesting conclusions regarding the ℓ-ranks of genus 1 quadratic function fields. These and other conclusions are discussed further in Chapter 7.

Chapter 2

Background and Preliminary Results

2.1 Function Fields

The goal of this section is to recall basic and relevant facts about algebraic function fields. We begin with the fundamental theory of algebraic function fields by describing places, divisors, discriminants, and the genera of function fields and their extensions. This is followed by recalling basic representation theory, leading to an introduction of Galois representations and their corresponding L-functions. With this material in mind, we conclude with some preliminary results on dihedral function fields.

Throughout, k will denote an arbitrary perfect field, and $k[x]$ the univariate polynomial ring over a field k. Also, q will be a power of a prime p, and $\mathbb{F}_q$ will denote the finite field with q elements. While much of the theory of function fields will be described over any field, we will typically be concerned with function fields over finite fields.

2.1.1 Algebraic Function Fields

We begin by recalling the basic theory of algebraic function fields. Most of this material can be found in [37].

Definition 2.1.1. The *rational function field over* k is the field of fractions of the polynomial ring $k[x]$, denoted as $k(x)$, i.e.

$$k(x) = \left\{ \frac{a(x)}{b(x)} : b(x) \neq 0,\ a(x), b(x) \in k[x] \right\}.$$

The field k is called the *constant field* of $k(x)$.

Definition 2.1.2. An *algebraic function field* $k(x, y)$ is a finite algebraic extension of $k(x)$, i.e. there exists some element y such that

$$k(x, y) = k(x)[y]/(h(x, y)) \text{ for some irreducible } h(x, y) \in k(x)[y].$$

The degree of h in y is called the *degree* of the algebraic function field $k(x, y)$. Often we will use K_i to denote an algebraic function field of degree i, and simply K for an arbitrary algebraic function field. The *characteristic* of an algebraic function field is the characteristic of the field k.

Note 2.1.3. An function field can be represented as an extension of various rational function fields, and hence the degree of an function field is generally not well-defined. We avoid this issue by fixing the rational function field $k(x)$ once and for all.

All function fields throughout will be algebraic function fields and hence we will typically drop the word algebraic when describing them. Moreover, we will assume that every function field is a separable extension of a rational function field.

Definition 2.1.4. The *constant field* of a function field K over k is the field $K \cap \bar{k}$, where $\bar{k}$ denotes the algebraic closure of k.

Throughout, we will typically consider algebraic function fields whose constant field is the same as that of its underlying rational function field; called *geometric* extensions. We will thus use the notation K/k to denote the function field whose constant field is k, or we will simply write K if the particular constant field is of little consequence.

2.1.2 Places

To define the places of a function field we begin by describing the valuations (absolute values) associated with each place.

Definition 2.1.5. A *discrete valuation* of a function field K/k is a function $v : K \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

1. $v(\alpha) = \infty$ if and only if $\alpha = 0$.
2. $v(\alpha\beta) = v(\alpha) + v(\beta)$ for all $\alpha, \beta \in K$.
3. $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$ for all $\alpha, \beta \in K$.
4. $v(c) = 0$ for any $0 \neq c \in k$.

Definition 2.1.6. Let v be a discrete valuation of K/k, and fix a real number $0 < c < 1$. Define the *absolute value* of v as $||_v : K \to \mathbb{R}$ by

$$|\alpha|_v = \begin{cases} c^{v(\alpha)} & z \neq 0, \\ 0 & \alpha = 0. \end{cases}$$

Now, $||_v$ is a metric on K and hence K can be viewed as a metric space and thus a topological space in the natural way. Two valuations (or their absolute values) are

called *equivalent* if they induce the same topology.

We can now give the definition a place of a function field.

Definition 2.1.7. A *place* of a function field K/k is an equivalence class of absolute values. We denote the set of places of K as $\mathbb{P}(K)$.

To each place we can associate a local ring.

Definition 2.1.8. A *valuation ring* of a function field K/k is a ring $O \subset K$ such that

1. $k \subset O \subset K$, and
2. for every $\alpha \in K$ we have $\alpha \in O$ or $\alpha^{-1} \in O$.

Proposition 2.1.9 ([37] Prop 1.1.5-6)**.** *Let O be a valuation ring of a function field K. Then*

1. *O is a local ring; i.e. it has a unique proper maximal ideal P.*
2. *O is a principal ideal domain, thus, $P = \pi O$ for some $\pi \in O$ called a local parameter or uniformizer.*
3. *If $0 \subset I \subset O$ is an ideal then $I = P^n$ for some $n \in \mathbb{Z}^{>0}$.*
4. *If $P = \pi O$ then each $0 \neq \alpha \in K$ has a unique representation of the form $\alpha = \pi^n \epsilon$ for some $n \in \mathbb{Z}$ and $\epsilon \in O^\times$ (the unit group of O).*

A valuation ring satisfying properties 1 and 2 above is called a *discrete valuation ring*. Thus every valuation ring of a function field is in fact a discrete valuation ring. Now to each valuation ring we can associate a discrete valuation.

Definition 2.1.10. Let O be a valuation ring of K with maximal ideal P and local parameter π. Then by Proposition 2.1.9, each $\alpha \in K$ can be written uniquely as $\alpha = \pi^n \epsilon$ for some $\epsilon \in O^\times$. The discrete valuation $v_P : K \to \mathbb{Z}$ is defined such that $v_P(\alpha) = n$.

As we will see, the above function is indeed a discrete valuation. Conversely, to each discrete valuation we can associate a valuation ring. Let v be a discrete valuation. Set $O_v = \{\alpha \in K : v(\alpha) \geq 0\}$, and $P_v = \{\alpha \in K : v(\alpha) > 0\}$. Then we have the following theorem:

Theorem 2.1.11 ([37] Thm 1.1.13)**.** *1. Let v be a discrete valuation. Then O_v is a valuation ring with maximal ideal P_v.*

2. Let O be a valuation ring with maximal ideal P. Then v_P is a discrete valuation.

3. There is a one-to-one correspondence between the equivalence classes of valuations on K and the valuation rings of K (and hence the maximal ideals of the valuation rings of K).

Using the third item above, one may now also define a *place* of a function field K to be (a maximal ideal of) a valuation ring. This definition may be more common; however, we will use the two definitions interchangeably. Moreover, as a place is a maximal ideal of its valuation ring, we will often use the notation $\langle \alpha_1, \ldots, \alpha_r \rangle$ to express the particular place (ideal) generated by $\alpha_1, \ldots, \alpha_r \in O_P$.

Definition 2.1.12. Let O_P be a valuation ring of a function field K corresponding to the place P. Define $F_P = O_P/P$ to be the *residue field* of P. Then F_P is a finite extension of k, the degree of which is called the *degree* of the place P, denoted $\deg(P)$.

Example 2.1.13. Let $K = k(x)$ be the rational function field over k. We will consider two types of places of $k(x)$.

1. Let h be an irreducible polynomial in $k[x]$ and

$$P_h = \langle h(x) \rangle = \left\{ \frac{a(x)}{b(x)} \in k(x) : h(x) \mid a(x), h(x) \nmid b(x) \right\}.$$

Then P_h is a place of $k(x)$ with uniformizer $h(x)$ and $\deg(P) = \deg(h(x))$.

2. Set
$$P_\infty = \langle 1/x \rangle = \left\{ \frac{a(x)}{b(x)} \in k(x) : \deg(a(x)) - \deg(b(x)) < 0 \right\}.$$
Then P_∞ is a place of $k(x)$ of degree 1 with uniformizer $1/x$.

In fact, these constitute all the places of $k(x)$.

2.1.3 Extensions of Function Fields

In this section we discuss extensions of algebraic function fields and their places. Throughout, let K'/K be a finite algebraic extension of function fields of degree $[K' : K]$. Then $k' = K' \cap \bar{k}$ is the constant field of K'.

Definition 2.1.14. Suppose that P and P' are places of K and K', respectively. The place P' is said to *lie over* P, and P is said to *lie under* P', if $P \subseteq P'$. We write this as $P'|P$.

The places of K' lying over those of K are related by the following proposition:

Proposition 2.1.15 ([37] Prop 3.1.4)**.** *Suppose that P and P' are places of K and K' respectively. Then the following are equivalent:*

1. *$P'|P$.*
2. *$O_P \subseteq O_{P'}$.*
3. *There exists an integer $e \geq 1$, such that $v_{P'}(\alpha) = e \cdot v_P(\alpha)$ for all $\alpha \in K$.*

Moreover, if $P'|P$ then $P = P' \cap K$ and $O_P = O_{P'} \cap K$.

Note that as $P \subseteq P'$ and $O_P \subseteq O_{P'}$ we can consider F_P as a subfield of $F_{P'}$. Moreover, as K'/K is a finite extension, so too is $F_{P'}/F_P$. This leads to the following definitions:

Definition 2.1.16. Let K'/K be a finite extension of function fields and let $P'|P$.

1. The *relative degree* of $P'|P$, denoted as $f(P'|P)$, equals $[F'_P : F_P]$.
2. The integer e of Proposition 2.1.15 is called the *ramification index* of $P'|P$, which we denote as $e(P'|P)$.
3. P' is *ramified* if $e(P'|P) > 1$ and *tamely ramified* if $\mathrm{char}(k)$ does not divide $e(P'|P)$. P is called *ramified* if at least one place $P'|P$ is ramified, and *tamely ramified* if every place $P'|P$ is tamely ramified.
4. K'/K is *unramified* if no place of K' is ramified over K, and *tamely ramified* if every ramified place of K' is tamely ramified over K.
5. P is *(totally) inert* if $f(P'|P) = [K' : K]$.
6. P is *(totally) split* if $f(P'|P) = e(P'|P) = 1$ for all P' lying over P.
7. The *norm* of a place $P'|P$ is $\mathrm{N}_{K'/K}(P') = f(P'|P)P$.
8. The *co-norm* of a place $P'|P$ is $\mathrm{Con}_{K'/K}(P) = \sum_{P'|P} e(P'|P)P$.

We now confirm the existence of places in an extension lying above those of the ground field with the following proposition:

Proposition 2.1.17 ([37] Prop 3.1.6-7)**.** *Let K'/K be a finite algebraic extension of function fields.*

1. *For each place P' of K' there is exactly one place P of K such that $P'|P$, namely $P = P' \cap K$.*
2. *Conversely, every place P of K has at least one, but only finitely many, places P' of K' such that $P'|P$.*

Moreover, if $K''/K'/K$ are extensions of function fields with places $P''|P'|P$, respectively, then

$$e(P''|P) = e(P''|P')e(P'|P), \qquad f(P''|P) = f(P''|P')f(P'|P).$$

The number of places lying over a given place, their relative degrees, and ramification indices are strongly related. Indeed, we have the following theorem:

Theorem 2.1.18 ([37] Thm 3.1.11)**.** *Let K'/K be a finite algebraic extension of function fields. Let P be a place of K and let $P'_1, \ldots, P'_r$ be all the places of K' lying over P. Then*

$$\sum_{i=1}^{r} e(P'_i|P) f(P'_i|P) = [K' : K].$$

Example 2.1.19. Consider the rational function field $K_0 = \mathbb{F}_7(x)$. Let K_2 be the quadratic function field defined by $y^2 = x(x+3)(x+1) \in \mathbb{F}_7[x, y]$. Then the place $P_x \in \mathbb{P}(K_0)$ is ramified in K_2, with one place $\langle x, y \rangle \in \mathbb{P}(K_2)$ lying over it. The place $P_{x+4} \in \mathbb{P}(K_0)$ is split in K_2 with two places $\langle x+4, y+3 \rangle$, $\langle x+4, y+4 \rangle \in \mathbb{P}(K_2)$ lying over it. The place $P_{x^2+x+6} \in \mathbb{P}(K_0)$ is inert in K_2 with one place $\langle x^2+x+6 \rangle \in \mathbb{P}(K_2)$ lying over it. By Theorem 2.1.18, these are the only possible cases.

2.1.4 Divisors, Genus and Different

In this section we present the fundamental invariant of a function field - its genus. Moreover, we describe the genus of a function field in terms of a slightly more refined invariant called the discriminant divisor. To do so, we begin with the definition of a divisor.

Definition 2.1.20. The *divisor group* of a function field K is the additive free abelian group generated by the places of K, denoted $\mathrm{Div}(K)$. The elements of this group are called *divisors*. Thus a divisor D can be written as

$$D = \sum_{P \in \mathbb{P}_K} n_P P \text{ where } n_P \in \mathbb{Z} \text{ and all but finitely many } n_P = 0.$$

The *support* of a divisor D, denoted $\mathrm{Supp}(D)$, is defined as

$$\mathrm{Supp}(D) = \{P \in \mathbb{P}(K) : n_P \neq 0\}.$$

Two divisors are *coprime* if they have disjoint support. The *degree* of a divisor D, denoted $\deg(D)$, is

$$\deg(D) = \sum_{P \in \mathbb{P}_K} n_P \deg(P).$$

The subgroup of $\mathrm{Div}(K)$ of degree 0 divisors is denoted $\mathrm{Div}^0(K)$. The norm of a place also extends additively to a divisor.

To each nonzero function in K we can associate a divisor.

Definition 2.1.21. Let $\alpha \in K^\times$. The *divisor of* α, denoted (α) is

$$(\alpha) = \sum_{P \in \mathbb{P}(K)} v_P(\alpha) P.$$

It can be shown that the divisor of a function is an element of $\mathrm{Div}^0(K)$. Consequently, an element $D \in \mathrm{Div}^0(K)$ is called *principal* if there exists an element $\alpha \in K^\times$ such that $(\alpha) = D$. The principal divisors of K form a subgroup of $\mathrm{Div}^0(K)$, which is denoted $\mathrm{Prin}(K)$.

It is a natural question to ask what proportion of degree 0 divisors are in fact principal divisors. To measure this disparity we form the *degree* 0 *divisor class group* of a function field K. The degree 0 divisor class group (also called the degree 0 *Picard group*) is the group $\mathrm{Pic}^0(K) = \mathrm{Div}^0(K)/\mathrm{Prin}(K)$. Notice that this group is trivial exactly when all degree 0 divisors are principal. Moreover, the larger the class group, the 'further' we are from this situation. As we will see in Theorem 2.1.25, in the

event that the constant field of K is finite, $\mathrm{Pic}^0(K)$ is a finite group. First, we begin by associating a vector space to a divisor.

Definition 2.1.22. For a divisor $D \in \mathrm{Div}(K)$, define the *Riemann-Roch space* associated to D by

$$L(D) = \{\alpha \in K : (\alpha) \geq -D\} \cup \{0\},$$

where a divisor $D_1 \geq D_2$ if and only if $v_P(D_1) \geq v_P(D_2)$ for all $P \in \mathbb{P}(K)$.

The Riemann-Roch space is a finite-dimensional k-vector space, as seen in the following proposition:

Proposition 2.1.23 ([37] Prop 1.4.14)**.** *For all divisors $D \in \mathrm{Div}(K)$ we have*

1. $\dim(L(D)) \leq 1 + \deg(D)$.
2. *There is a constant $c \in \mathbb{Z}^{\geq 0}$ independent of D such that*

$$\deg(D) - \dim(L(D)) \leq c + 1.$$

The genus of a function field is the least upper bound for c in the above proposition, and formally defined as follows:

Definition 2.1.24. The *genus* g of a function field K is defined by

$$g = \max\{\deg(D) - \dim(L(D)) + 1 : D \in \mathrm{Div}(K)\}.$$

Setting $D = 0$, one can see that the genus is a nonnegative integer. Moreover, a function field has genus 0 if and only if it is a rational function field (see [37], Prop 1.6.3). When necessary to make the function field explicit, we will write g_K for the genus of a function field K.

In the event that the constant field of K is finite, the size of $\mathrm{Pic}^0(K)$ is bounded by the following theorem:

Theorem 2.1.25 (Hasse-Weil Theorem, [37] Thm 5.2.3)**.** *The order of the divisor class group of a function field K with constant field $\mathbb{F}_q$ is bounded by*

$$(\sqrt{q}-1)^{2g} \leq \left|\mathrm{Pic}^0(K)\right| \leq (\sqrt{q}+1)^{2g}.$$

where g is the genus of K.

The genus is the fundamental invariant of a function field. Not only does it determine the Hasse-Weil bounds of Theorem 2.1.25, but as we will now see, it also bounds the number of ramified places of K.

Theorem 2.1.26 (Riemann-Hurwitz Formula, [37] Thm 3.4.13)**.** *Let K'/K be an extension of function fields with constant fields k' and k, and genera g' and g, respectively. Suppose that K'/K is tamely ramified. Then*

$$2g'-2 = (2g-2)\frac{[K':K]}{[k':k]} + \sum_{P\in\mathbb{P}(K)}\sum_{P'|P}(e(P'|P)-1).$$

To avoid introducing different exponents, we have presented a simplified version of the Riemann-Hurwitz formula by restricting ourselves to only tamely ramified extensions; the reference for the general version is provided. Henceforth, we will typically only be considering tamely ramified extensions. Regardless, we have the following corollaries:

Corollary 2.1.27. *In a finite extension of function fields only finitely many primes ramify.*

Corollary 2.1.28. *Assume that K is a rational function field with the same constant*

field as K', which is tamely ramified over K. Then

$$2g' - 2 = -2[K' : K] + \sum_{P \in \mathbb{P}(K)} \sum_{P'|P} (e(P'|P) - 1)$$

Now, to further describe function fields, we will often use more refined information about the ramification than merely the genus. This information is recorded via the different and discriminant divisors.

Definition 2.1.29. Let K'/K be a tamely ramified extension of function fields with constant fields k' and k, respectively.

1. The *different divisor* of K'/K is

$$\mathrm{Diff}(K'/K) = \sum_{P \in \mathbb{P}(K)} \sum_{P'|P} (e(P'|P) - 1)P'$$

2. The *discriminant divisor* of K'/K is $\Delta(K'/K) = \mathrm{N}_{K'|K}(\mathrm{Diff}(K'|K))$.

Notice that $\mathrm{Diff}(K'/K) \in \mathrm{Div}(K')$, while $\Delta(K'/K) \in \mathrm{Div}(K)$. Thus, we use discriminant divisors when discussing the existence of fields with prescribed ramification.

Example 2.1.30. Note that all finite places P of K_0 correspond to monic irreducible polynomials $f_P(x)$ in $k_0[x]$. Therefore, we can easily construct $K_2 = k(x, y)$ with squarefree discriminant divisor Δ as follows: if $\Delta = 0$, then y is simply the square

root of a nonsquare in k_0. If $\Delta \neq 0$, then there are two possibilities for K_2, either

$$y^2 = \prod_{\substack{P \in \operatorname{Supp} \Delta \\ P \text{ finite}}} f_P(x),$$
$$y^2 = c \prod_{\substack{P \in \operatorname{Supp} \Delta \\ P \text{ finite}}} f_P(x).$$

where c is a nonsquare in k. These quadratic function fields are called *twists* of each other.

The different and discriminant divisors of towers of extensions are related as follows.

Proposition 2.1.31. *Let $K''/K'/K$ be extensions of function fields. Then*

1. $\operatorname{Diff}(K''/K) = \operatorname{Con}_{K''/K'}(\operatorname{Diff}(K'/K)) + \operatorname{Diff}(K''/K')$.

2. $\Delta(K''/K) = [K'' : K'] \cdot \Delta(K'/K) + \mathrm{N}_{K'/K}(\Delta(K''/K'))$.

Notice that a place appears in the support of $\Delta(K'/K)$ (and $\operatorname{Diff}(K'/K)$) if and only if it is ramified.

We now have the background to state the general aims of this work; namely to efficiently construct certain types of function fields with a given discriminant divisor, and to tabulate all such fields whose discriminant divisor's degree is below a fixed bound. Understanding the types of such fields is the first aim of the following section.

2.2 Galois Representations and L-functions

In this section we present the basic concepts from Galois theory and representation theory in order to describe Artin L-functions. A broader treatment of Galois theory can be found in many texts such as [17]. The representation theory is mainly from [34] and the introduction to L-functions of function fields primarily from [37] and [41].

Throughout this section, let K'/K be a finite extension of function fields.

2.2.1 Galois Theory of Function Fields

We begin by recalling some basic facts from Galois theory of finite extensions of fields.

Definition 2.2.1. Consider the automorphism group

$$\mathrm{Aut}(K'/K) = \{\gamma \in \mathrm{Aut}(K') : \gamma(\alpha) = \alpha, \forall \alpha \in K\}.$$

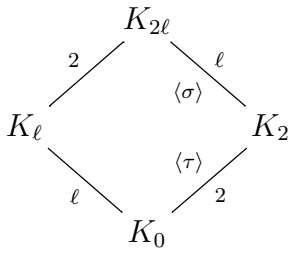
An extension is called *Galois* if $|\mathrm{Aut}(K'/K)| = [K' : K]$, in which case we write $\mathrm{Gal}(K'/K) = \mathrm{Aut}(K'/K)$. The *Galois closure* of K' is the smallest K''/K' such that K''/K is Galois.

Example 2.2.2. All quadratic function fields with $\mathrm{char}(k) \neq 2$ are Galois. Let $K_2 = k(x)[y]/\langle y^2 - h(x)\rangle$ with $\mathrm{char}(k) \neq 2$, then $\mathrm{Gal}(K_2/K(x)) = \{id, \tau\}$ where $\tau(y) = -y \neq y$ and $\tau(\alpha) = \alpha, \forall \alpha \in K(x)$. Here τ is called the *quadratic involution* of $K_2/k(x)$.

When K'/K is not Galois, we will often make the common abuse of language referring to the Galois group of K'/K when in fact we mean the Galois group of its Galois closure. We now recall the fundamental theorem of Galois theory.

Theorem 2.2.3 ([37] Appendix A.12)**.** *Let K''/K be Galois. There is a one-to-one*

Figure 2.1:



correspondence between the subfields K' of K'' containing K and the subgroups of $\mathrm{Gal}(K''/K)$*; namely the subgroup $\mathcal{H}$ of* $\mathrm{Gal}(K''/K)$ *corresponds to the fixed field of $\mathcal{H}$,* $\mathrm{Fix}(\mathcal{H}) = \{\alpha \in K' : \gamma(\alpha) = \alpha, \forall \gamma \in \mathcal{H}\}$*. Moreover, K'/K is Galois if and only if $\mathcal{H}$ is normal in* $\mathrm{Gal}(K''/K)$*.*

Example 2.2.4. Let ℓ be an odd prime. Consider the diagram of function fields presented in Figure 2.1. Here, the field K_0 is a rational function field with constant field k_0 with characteristic different from 2 and ℓ. The field $K_{2\ell}$ is the Galois closure of K_ℓ with Galois group $\mathcal{D}_\ell$, the dihedral group with 2ℓ elements. K_2 is the fixed field of the unique index 2 subgroup $\mathcal{C}_\ell$ of $\mathcal{D}_\ell$ generated by σ. As $\mathcal{C}_\ell$ is normal in $\mathcal{D}_\ell$, K_2 is indeed Galois with $\mathrm{Gal}(K_2/K_0)$ generated by τ. K_ℓ is the fixed field of an element of order 2 in $\mathcal{D}_\ell$. We note that there are ℓ such elements in $\mathcal{D}_\ell$ which give ℓ *conjugate* subfields K_ℓ of $K_{2\ell}$. The field K_2 is called the *quadratic resolvent field* of K_ℓ.

The Galois group of an extension K'/K has a profound effect on the splitting behavior of the places of K'.

Theorem 2.2.5 ([37] Thm 3.7.1)**.** *Let K'/K be a Galois extension of function fields. Let $P'_1, P'_2 \in \mathbb{P}(K')$ lie over a place $P \in \mathbb{P}(K)$. Then there exists an element $\gamma \in$* $\mathrm{Gal}(K'/K)$ *such that $P'_2 = \gamma(P'_1)$. Moreover, $v_{P'_2}(\alpha) = v_{P'_1}(\gamma^{-1}(\alpha))$.*

Corollary 2.2.6 ([37] Cor 3.7.2)**.** *Let K'/K be Galois. Let $P'_1, \ldots, P'_r \in \mathbb{P}(K')$ be all the places of K'/K lying over a place $P \in \mathbb{P}(K)$. Then*

1. *$e(P'_i|P) = e(P'_j|P)$ for all $1 \leq i, j \leq r$.*
2. *$f(P'_i|P) = f(P'_j|P)$ for all $1 \leq i, j \leq r$.*
3. *$e(P'_i|P) \cdot f(P'_i|P) \cdot r = [K' : K]$.*

Now, for each place in a Galois extension we can associate two groups describing the ramification and relative degree.

Definition 2.2.7. Let K'/K be a Galois extension of function fields with Galois group $\mathcal{G}$. Let $P' \in \mathbb{P}(K')$ lie over a place $P \in \mathbb{P}(K)$. Then

1. $\mathcal{Z}(P'|P) = \{\gamma \in \mathcal{G} : \gamma(P') = P'\}$ is called the *decomposition group* of $P'|P$.
2. $\mathcal{I}(P'|P) = \{\gamma \in \mathcal{G} : v_{P'}(\gamma(\alpha) - \alpha) > 0 \text{ for all } \alpha \in O_{P'}\}$ is called the *inertia group* of $P'|P$.

Notice that $\mathcal{I}(P'|P) \subset \mathcal{Z}(P'|P)$ are both subgroups of $\mathcal{G}$. In addition, we have the following theorem:

Theorem 2.2.8 ([37] Thm 3.8.2-5)**.** *With the notation above we have:*

1. *$|\mathcal{Z}(P'|P)| = e(P'|P)f(P'|P)$.*
2. *$|\mathcal{I}(P'|P)| = e(P'|P)$.*
3. *For any $\gamma \in \mathcal{G}$, $Z(\gamma(P')|P) = \gamma Z(P'|P)\gamma^{-1}$ and $I(\gamma(P')|P) = \gamma I(P'|P)\gamma^{-1}$.*
4. *The residue class extension $F_{P'}/F_P$ is a cyclic Galois extension. Moreover, each $\gamma \in \mathcal{Z}(P'|P)$ induces an automorphism $\bar{\gamma} \in \mathrm{Gal}(F_{P'}/F_P)$ by setting $\bar{\gamma}(\alpha + P') = \gamma(\alpha) + P'$ for $\alpha \in O_{P'}$. The mapping*

$$\mathcal{Z}(P'|P) \to \mathrm{Gal}(F_{P'}/F_P).$$

$$\gamma \mapsto \bar{\gamma},$$

is a surjective homomorphism with kernel $\mathcal{I}(P'|P)$.

5. *If* $|\mathcal{G}|$ *is relatively prime to* $\mathrm{char}(K) > 0$, *then* $\mathcal{I}(P'|P)$ *is a cyclic group.*

2.2.2 Representation Theory

The Galois group also plays a crucial role in determining the ramification of all the intermediate fields of K'/K. To make this apparent we use the theory of L-functions together with information gained by examining the representations of the Galois group. Throughout this section, let $\mathcal{G}$ denote a finite group and V a finite-dimensional complex vector space.

Definition 2.2.9. A *representation* of $\mathcal{G}$ is a homomorphism $\rho : \mathcal{G} \to \mathrm{Aut}(V)$. When ρ is given, V is called a *representation space* of $\mathcal{G}$. The dimension of V is called the *degree* of the representation ρ. Two representations ρ, ρ' are *isomorphic* if there exists a linear isomorphism $A : V \to V'$ such that

$$A\rho(\gamma) = \rho'(\gamma)A \quad \forall \gamma \in \mathcal{G}.$$

The following are examples of representations for an arbitrary group $\mathcal{G}$ that will be particularly useful.

Example 2.2.10. Consider the representation $\rho_0 : \mathcal{G} \to \mathbb{C}$ given by $\rho(\gamma) = 1$ for all $\gamma \in \mathcal{G}$. This representation ρ is called the *trivial representation.* Now, consider that exists an embedding $\mathcal{G} \to \mathcal{S}_n$ of $\mathcal{G}$ into the symmetric group on n elements. Consider

the representation $\rho_\pm : \mathcal{G} \to \mathbb{C}$ given by

$$\rho_\pm(\sigma) = \begin{cases} 1 & \sigma \text{ has even parity in } \mathcal{S}_n, \\ -1 & \sigma \text{ has odd parity in } \mathcal{S}_n, \end{cases}$$

This is called a *parity representation* of $\mathcal{G}$. These are two (typically) nonisomorphic 1-dimensional representations of $\mathcal{G}$.

Example 2.2.11. Consider the $|\mathcal{G}|$-dimensional complex vector space V spanned by a set of vectors $B = \{e_\delta : \delta \in \mathcal{G}\}$, a basis indexed by the elements of $\mathcal{G}$. Define the *(left) regular representation* ρ_1 as the homomorphism that linearly extends the action of $\mathcal{G}$ on the basis B given by $\rho_1(\gamma)(e_\delta) = e_{\gamma\delta}$ for all $\gamma \in \mathcal{G}$ and $e_\delta \in B$.

Example 2.2.12. Let $\mathcal{H}$ be a subgroup of $\mathcal{G}$. Consider the $|\mathcal{G}/\mathcal{H}|$-dimensional complex vector space V spanned by a set of vectors $B = \{e_{\delta\mathcal{H}} : \delta\mathcal{H} \in \mathcal{G}/\mathcal{H}\}$, a basis indexed by the (left) cosets of $\mathcal{G}/\mathcal{H}$. Define the *(left) induced representation* (of the trivial representation on $\mathcal{H}$) $\rho_\mathcal{H}$ as the homomorphism that linearly extends the action of $\mathcal{G}$ on the basis B given by $\rho_\mathcal{H}(\gamma)(e_{\delta\mathcal{H}}) = e_{(\gamma\delta)\mathcal{H}}$ for $\gamma \in \mathcal{G}, e_{\delta\mathcal{H}} \in B$. Notice that when $\mathcal{H}$ is $\langle 1 \rangle$, the induced representation is isomorphic to the regular representation and hence the notation is consistent. Also notice that $\rho_\mathcal{G}$ is the trivial representation.

Definition 2.2.13. Let ρ be a representation of $\mathcal{G}$ with representation space V. Let W be a subspace of V. A subspace W of V is said to be $\mathcal{G}$-*stable* if for all $w \in W$, $\rho(\gamma)(w) = w$ for all $\gamma \in \mathcal{G}$. Then the restriction of ρ to W is a representation called a *subrepresentation* of V. A representation is called *irreducible* if it has no $\mathcal{G}$-stable subrepresentations.

Theorem 2.2.14 ([34] Ch 1 Thms 1,2)**.** *Let $\rho : \mathcal{G} \to \mathrm{Aut}(V)$ be a representation*

and let W be a $\mathcal{G}$-stable subspace of V. Then there exists a complement W^o of W in V that is stable under $\mathcal{G}$. Consequently, every representation is a direct sum of irreducible representations.

We will write $\rho_1 \oplus \rho_2$ for the direct sum of two representations $\rho_1 : \mathcal{G} \to V_1$ and $\rho_2 : \mathcal{G} \to V_1$, which acts on the space $V_1 \oplus V_2$ component-wise.

The following example demonstrates a decomposition of a representation.

Example 2.2.15. Let $\mathcal{D}_\ell$ be the dihedral group of 2ℓ elements for an odd prime ℓ. Consider the natural embedding of $\mathcal{D}_\ell$ into $\mathcal{S}_\ell$. Let V be a complex ℓ-dimensional vector space with basis $\{e_i\}$. Then, $\mathcal{D}_\ell$ naturally acts on V by permutation on the basis vectors. Call this representation ρ. Now, ρ has $\mathcal{D}_\ell$-stable subspaces

$$W = \{c_0 e_1 + c_0 e_2 + \cdots + c_0 e_\ell : c_0 \in \mathbb{C}\},$$
$$W^O = \left\{c_1 e_1 + c_2 e_2 + \cdots + c_\ell e_\ell : \textstyle\sum_{i=1}^{\ell} c_i = 0, c_i \in \mathbb{C}\right\}.$$

In fact, $V = W \oplus W^O$, and thus $\rho = \rho|_W \oplus \rho|_{W^O}$. Notice that $\rho|_W$ is the trivial representation and hence irreducible. However, it can be shown that $\rho|_{W^O}$ is reducible when $\ell > 3$ as there are no irreducible representations of $\mathcal{D}_\ell$ of degree greater than 2, so this is not the full decomposition of ρ into irreducible representations.

To each representation we associate a function to characterize that representation.

Definition 2.2.16. Let $\rho : \mathcal{G} \to \mathrm{Aut}(V)$ be a representation. The *character* χ_ρ of ρ is defined to be

$$\chi_\rho(\gamma) = \mathrm{Tr}(\rho(\gamma)) \text{ for all } \gamma \in \mathcal{G},$$

where Tr denotes the trace of $\rho(\gamma)$ (the sum of the eigenvalues of $\rho(\gamma)$, or equivalently, the sum of the diagonal entries).

Throughout, we will let $\chi_{\mathcal{H}}$ denote the character of the induced representation $\rho_{\mathcal{H}}$ corresponding to a subgroup $\mathcal{H}$ of a group $\mathcal{G}$.

Proposition 2.2.17 ([34] Ch 2)**.** *If χ is the character of a representation ρ of degree n, then*

1. $\chi(1) = n$.
2. $\chi(\gamma^{-1}) = \overline{\chi(\gamma)}$, *the complex conjugate of* $\chi(\gamma)$, *for all* $\gamma \in \mathcal{G}$.
3. $\chi(\gamma\delta\gamma^{-1}) = \chi(\delta)$ *for all* $\gamma, \delta \in \mathcal{G}$.

Moreover, if ρ_1, ρ_2 are representations with respective characters χ_1 and χ_2, then the character of $\rho_1 \oplus \rho_2$ is $\chi_{\rho_1} + \chi_{\rho_2}$. Lastly, ρ_1 and ρ_2 are isomorphic if and only if $\chi_1 = \chi_2$.

Through the above proposition, we can see that characters play an important role in classifying representations. In particular, we can use characters to find relationships between induced representations.

Example 2.2.18. Consider the characters of the induced representations of the various subgroups of $\mathcal{D}_\ell$. Write

$$\mathcal{D}_\ell = \left\langle \sigma, \tau : \sigma^\ell = 1, \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \right\rangle.$$

By Proposition 2.2.17 we need only consider the values of these characters on conjugacy classes of elements, i.e. on the set

$$C = \{[1], [\tau]\} \cup \left\{[\sigma^i] = [\sigma^{-i}] : 1 \leq i \leq (\ell - 1)/2\right\}$$

where $[\gamma]$ denotes the conjugacy class of $\gamma \in \mathcal{D}_\ell$.

1. The trivial representation $\rho_{\mathcal{D}_\ell}$ (inducing the entire group) is a 1-dimensional

Table 2.1: Induced Character Table of the Dihedral Group $\mathcal{D}_\ell$

	$\chi_{\mathcal{D}_\ell}$	χ_1	$\chi_{\mathcal{C}_\ell}$	$\chi_{\mathcal{C}_2}$
$[1]$	1	2ℓ	2	ℓ
$[\tau]$	1	0	0	1
$\{[\sigma^i]\}$	1	0	2	0

representation where $\chi_{\mathcal{D}_\ell}(\gamma) = 1$ for all $\gamma \in \mathcal{D}_\ell$.

2. The regular representation ρ_1 (inducing the trivial subgroup) is a 2ℓ-dimensional representation; thus, $\chi_1(1) = 2\ell$. As left multiplication by a nontrivial element in a group has no fixed points, $\chi_1(\gamma) = 0$ for all $1 \neq \gamma \in \mathcal{D}_\ell$.
3. The representation $\rho_{\mathcal{C}_\ell}$ (inducing the order ℓ cyclic subgroup generated by σ) is a 2-dimensional representation; thus, $\chi_{\mathcal{C}_\ell}(1) = 2$. As $\tau \notin \mathcal{C}_\ell$, τ permutes the cosets $\mathcal{C}_\ell, \tau\mathcal{C}_\ell$, and thus $\chi_{\mathcal{C}_\ell}(\tau) = 0$. Lastly, all other classes of elements in $\mathcal{D}_\ell$ are in $\mathcal{C}_\ell$, and thus act trivially. Hence, $\chi([\sigma^i]) = 2$ for all conjugacy classes $[\sigma^i] \in C$.
4. The representation $\rho_{\mathcal{C}_2}$ (inducing the order 2 cyclic subgroup generated by τ) is an ℓ-dimensional representation; thus, $\chi_{\mathcal{C}_2}(1) = \ell$. As $\tau \in \mathcal{C}_2$, τ fixes the coset $\mathcal{C}_2$. Moreover, $\tau\sigma^i\mathcal{C}_2 = \sigma^{-i}\tau\mathcal{C}_2 = \sigma^{-i}\mathcal{C}_2$, and so τ fixes no other cosets of $\mathcal{D}_\ell/\mathcal{C}_2$. Hence $\chi_{\mathcal{C}_2}(\tau) = 1$. Lastly, the other classes $[\sigma^i]$ act on $\mathcal{D}_\ell/\mathcal{C}_2$ like cyclic permutations and thus fix no cosets. Hence, $\chi([\sigma^i]) = 0$ for all conjugacy classes $[\sigma^i] \in \mathcal{C}_2$.

We summarize the above information in Table 2.1.

From Table 2.1 we can see that we have the following relationship between these induced representations:

$$2\chi_{\mathcal{D}_\ell} + \chi_1 = \chi_{\mathcal{C}_\ell} + 2\chi_{\mathcal{C}_2}. \tag{2.1}$$

2.2.3 L-functions

L-functions provide a means for converting information about Galois groups and their representations into information about the underlying function fields. In particular, we will see how to use (2.1) to further understand the ramification of dihedral extensions. We begin by recalling the zeta functions of function fields. These functions have a rich and extensive theory. Only the few results required for the purpose of relating subfields of Galois extensions are presented (for more information, see [37], Chapter 5). Throughout this section, K will be a function field whose field of constants is $k = \mathbb{F}_q$, and $F[[t]]$ will denote the ring of formal power series in t over a field F.

Definition 2.2.19. Define $N(D) = q^{\deg(D)}$ as the *absolute norm* of a divisor D. Then the power series

$$\zeta_K(s) = \sum_{\substack{D \in \mathrm{Div}(K) \\ D \geq 0}} N(D)^{-s} \in \mathbb{Z}[[q^{-s}]]$$

is called the *zeta function* of K. For simplicity, we make the change of variable $t = q^{-s}$ and define $Z_K(t) = \zeta_K(s)$, and also call this the zeta function of K.

Zeta functions have the following remarkable properties:

Proposition 2.2.20 ([37], Sect 5.1)**.** *Let $Z(t)$ denote the zeta function of K. Then*

1. *$Z(t)$ is absolutely convergent for $|t| < q^{-1}$.*

2. *For $|t| < q^{-1}$, $Z(t)$ has a convergent* Euler product*:*

$$Z(t) = \prod_{P \in \mathbb{P}(K)} (1 - t^{\deg(P)})^{-1}.$$

3. $Z(t)$ *satisfies a* functional equation*:*

$$Z(t) = (\sqrt{q}t)^{2g-2} Z\left(\frac{1}{qt}\right).$$

where g *is the genus of* K*.*

Example 2.2.21. Let K be a function field of genus 0, i.e $K = \mathbb{F}_q(x)$. Then

$$Z_K(t) = \frac{1}{(1-t)(1-qt)}.$$

Now, to define a zeta function associated to a Galois representation, we present a Corollary of Theorem 2.2.8 describing the action of Frobenius on a vector space.

Corollary 2.2.22. *Let* ρ *be a representation of* $\mathrm{Gal}(K'/K)$ *on a complex vector space* V*. Let* $P' \in \mathbb{P}(K')$ *be a place lying over* $P \in \mathbb{P}(K)$*. Let* W *denote the subspace of* V *fixed by* $\mathcal{I}(P'|P)$*. As* $F'_P/F_P \cong \mathbb{F}_{q^{f(P'|P)}}$*, let* $\mathrm{fr}_{P'}$ *denote the generator of* $\mathrm{Gal}(F'_P/F_P)$ *that corresponds to the* q*-power Frobenius automorphism of* $\mathbb{F}_{q^{f(P'|P)}}$*. Furthermore, let* $\mathrm{Fr}_{P'}$ *denote a pre-image of* $\mathrm{fr}_{P'}$ *under the map of Theorem 2.2.8, part 3. Then* $\rho|_W(\mathrm{Fr}_{P'}) \in \mathrm{Aut}(W)$ *is well defined up to conjugacy; i.e. its characteristic polynomial is independent of the choice of pre-image* $\mathrm{Fr}_{P'}$*.*

From the corollary above, to each place P' of a function field we can now associate a particular linear transformation $\rho|_W(\mathrm{Fr}_{P'})$. Each of these transformations will give rise to a factor in an Euler product, the combination of which will form an L-function.

Definition 2.2.23. With the notation of Corollary 2.2.22, let 1_W denote the identity automorphism of W. Define the *Euler factor* of P' as

$$L_{P'}(\rho, t) = \det\left(1_W - \rho|_W(\mathrm{Fr}_{P'}) t^{\deg(P')}\right)^{-1},$$

i.e. the inverse of the characteristic polynomial of $\rho(\mathrm{Fr}_{P'})|_W$ evaluated at $t^{\deg(P')}$. Moreover, define the *L-function* of ρ to be

$$L(\rho, t) = \prod_{P' \in \mathbb{P}(K')} L_{P'}(\rho, t).$$

Notice that this is indeed a generalization of $Z(t)$ in the sense that if ρ_0 is the trivial representation, then $Z_{K'}(t) = L(\rho_0, t)$. In fact, $L(\rho, t)$ has some similar properties to $Z(t)$.

Proposition 2.2.24 ([30] Thm 9.25)**.** *Let $L(\rho, t)$ denote the L-function of K associated to the representation ρ. Then*

1. *$L(\rho, t)$ is absolutely convergent for $|t| < q^{-1}$.*
2. *$L(\rho, t)$ can be extended to a meromorphic function on $\mathbb{C}$.*

Furthermore, L-functions can be decomposed with respect to the decomposition of their representation. In particular, we have the following proposition which will be utilized in the next section.

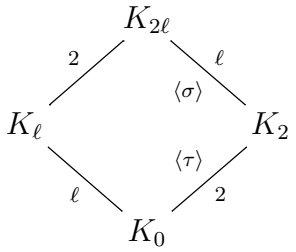
Proposition 2.2.25 ([2])**.** *Let K'/K be a Galois extension with Galois group $\mathcal{G}$, and let $\mathcal{H}$ be a subgroup of $\mathcal{G}$. Let ρ, ρ' be representations of $\mathcal{G}$. Then*

1. *$L(\rho \oplus \rho', t) = L(\rho, t)L(\rho', t)$.*
2. *$L(\rho_{\mathcal{H}}, t) = Z_{\mathrm{Fix}(\mathcal{H})}(t)$.*

2.3 Dihedral Function Fields

The main goal of this section is to compute the discriminant divisor of a degree ℓ dihedral function field. The results of this section are my own work and first appeared in [42].

We begin by recalling the situation in Example 2.2.4. From here on we fix all the following notation. Let ℓ be an odd prime. Recall, the diagram of subfields given in Figure 2.1:



Recall that K_0 is a rational function field, and the field $K_{2\ell}$ is the Galois closure of K_ℓ with Galois group $\mathcal{D}_\ell$, the dihedral group with 2ℓ elements. Recall further that K_2 is the quadratic resolvent, i.e the fixed field of the unique index 2 subgroup $\mathcal{C}_\ell$ of $\mathcal{D}_\ell$ generated by σ. K_ℓ is the fixed field of τ, the generator of $\mathcal{C}_2$ in $\mathcal{D}_\ell$.

To prove the main theorem, we will use the following supporting lemma:

Lemma 2.3.1. *The discriminant divisor $\Delta(K_\ell/K_0)$ satisfies*

$$\deg(\Delta(K_\ell/K_0)) = \frac{\ell-1}{2}\left(\deg(\Delta(K_2/K_0)) + \deg(M)\right),$$

where $M \in \mathrm{Div}(K)$ is defined via $(\ell-1)M = N_{K_2/K_0}(\Delta(K_{2\ell}/K_2))$.

Proof. By (2.1), the induced characters $\chi_1, \chi_{\mathcal{D}_\ell}, \chi_{\mathcal{C}_2}, \chi_{\mathcal{C}_\ell}$ are linearly dependent, and thus by Proposition 2.2.17, the representations $\rho_1, \rho_{\mathcal{D}_\ell}, \rho_{\mathcal{C}_2}, \rho_{\mathcal{C}_\ell}$ satisfy

$$\rho_1 \oplus 2\rho_{\mathcal{D}_\ell} \cong 2\rho_{\mathcal{C}_2} \oplus \rho_{\mathcal{C}_\ell}.$$

By parts 1 and 2 of Proposition 2.2.25, we have

$$Z_{K_{2\ell}}(t)Z_{K_0}(t)^2 = Z_{K_\ell}(t)^2 Z_{K_2}(t).$$

From the functional equation of the zeta function (part 4, Proposition 2.2.20) we obtain

$$(2g_{K_{2\ell}} - 2) + 2(2g_{K_0} - 2) = 2(2g_{K_\ell} - 2) + (2g_{K_2} - 2).$$

Applying Theorem 2.1.26, we have

$$\begin{aligned} \deg(\Delta(K_{2\ell}/K_0)) + 2\deg(\Delta(K_0/K_0)) &= 2\deg(\Delta(K_\ell/K_0)) + \deg(\Delta(K_2/K_0)), \\ \deg(\Delta(K_{2\ell}/K_0)) &= 2\deg(\Delta(K_\ell/K_0)) + \deg(\Delta(K_2/K_0)). \quad (2.2) \end{aligned}$$

By Proposition 2.1.31,

$$\Delta(K_{2\ell}/K_0) = [K_{2\ell} : K_2]\Delta(K_2/K_0) + \mathrm{N}_{K_2/K_0}(\Delta(K_{2\ell}/K_2)).$$

As $K_{2\ell}/K_2$ is a cyclic Galois extension, by Theorem 2.1.18, for all places $P'' \in \mathrm{Supp}(\Delta(K_{2\ell}/K_2))$ lying over a place $P' \in \mathbb{P}(K_2)$, $e(P''|P')$ divides $[K_{2\ell} : K_2] = \ell$ and hence $e(P''|P') = \ell$. Consequently,

$$\Delta(K_{2\ell}/K_2) = (\ell - 1)M',$$

where $M' \in \mathrm{Div}(K_2)$ is the sum of the ramified places of $K_{2\ell}/K_2$. Therefore, $\mathrm{N}_{K_2/K_0}(\Delta_{K_{2\ell}/K_2}) = (\ell - 1)M$ where $M = \mathrm{N}_{K_2/K_0}(M')$. Now, (2.2) can be rewrit-

ten as

$$\ell \deg(\Delta(K_2/K_0)) + (\ell - 1)\deg(M) = 2\deg(\Delta(K_\ell/K_0)) + \deg(\Delta(K_2/K_0)).$$

Thus,

$$\deg(\Delta(K_\ell/K_0)) = \frac{\ell - 1}{2}(\deg(\Delta(K_2/K_0)) + \deg(M)).$$

□

Theorem 2.3.2. *The discriminant divisor $\Delta(K_\ell/K_0)$ satisfies*

$$\Delta(K_\ell/K_0) = \frac{\ell - 1}{2}\left(\Delta(K_2/K_0) + M\right),$$

where $(\ell - 1)M = N_{K_2/K}(\Delta(K_{2\ell}/K_2))$, and M and $\Delta(K_2/K_0)$ are coprime.

Proof. Let $E = \frac{\ell-1}{2}(\Delta(K_2/K_0) + (\ell - 1)M)$. First note that the only places of K_0 ramified in K_ℓ are those lying over places in the support of M and Δ_{K_2}, as $K_{2\ell}/K_2/K_0$ is only ramified at these places. As $\mathcal{D}_\ell$ is not cyclic, by Theorem 2.2.8, there are no places $P'' \in \mathbb{P}(K_{2\ell})$ such that $e(P''|P) = 2\ell$, and hence $\mathrm{Supp}(M)$ and $\mathrm{Supp}(\Delta(K_2/K_0))$ are disjoint. Thus, for all places $P \in \mathrm{Supp}(M)$ and all $P'' \in \mathbb{P}(K_{2\ell})$ lying over P, $e(P''|P) = \ell$. Similarly, for all places $P \in \mathrm{Supp}(\Delta(K_2/K_0))$ and all $P'' \in \mathbb{P}(K_{2\ell})$ lying over P, $e(P''|P) = 2$. As $[K_{2\ell} : K_\ell] = 2 \nmid \ell$, all places $P' \in \mathbb{P}(K_\ell)$ lying over M must have $e(P'|P) = \ell$. Also, for all $P' \in \mathbb{P}(K_\ell)$ lying over Δ_{K_2}, $e(P'|P) \leq 2$. Applying the identity

$$\sum_{P'|P} e(P'|P) f(P'|P) = \ell$$

to any place $P \in \mathrm{Supp}(\Delta(K_2/K_0))$ allows at most $(\ell-1)/2$ places $P'|P$ of K_ℓ to be ramified. Thus, $\Delta(K_\ell/K_0)$ divides E. Since both divisors have the same degree, they must be equal. □

Remark 2.3.3. While we only presented a proof of Theorem 2.3.2 for the case when the coefficient field k_0 of K_0 is a finite field, Theorem 2.3.2 in fact holds when k_0 is an arbitrary perfect field with characteristic not dividing 2ℓ. For brevity we omit the details, but one could prove this by careful examination of the higher ramification groups of $K_{2\ell}/K_0$. When $\mathrm{char}(k_0) \nmid 2\ell$, the inertia groups are cyclic and all higher ramification groups are trivial. Moreover, the only nontrivial cyclic subgroups of $\mathcal{D}_\ell$ are $\mathcal{C}_\ell$ and $\mathcal{C}_2$. As K_ℓ/K_0, is the fixed field of τ, $K_{2\ell}/K_\ell$ is ramified at the places where τ fixes their interia groups, i.e. those places whose interia group is $\mathcal{C}_2$. Proposition 2.1.17 then completes the proof of Theorem 2.3.2. Again, to avoid expounding further upon these topics, we leave the details of this proof to the reader.

In this chapter we defined the fundamental theory required to prove the results of this last section. Having touched upon the theory of function fields, representation theory, Galois theory, and the theory of L-functions, we were able to show the precise relationship between the ramification of a degree ℓ dihedral function field and that of its quadratic resolvent and Galois closure. Using this information, the remaining goal of this thesis is to construct and tabulate all dihedral function fields with prescribed ramification.

The aim of the next three chapters describe different methods for constructing all dihedral extensions of odd prime degree. As we saw in Example 2.2.4, dihedral function fields are uniquely determined (up to Galois conjugacy) by their Galois closures. Thus, our general approach for constructing dihedral function fields will

be to first construct their Galois closures, then compute the degree ℓ subfield by computing the fixed field of an automorphism of order 2. We also saw in Example 2.2.4 that degree 2ℓ dihedral function fields are degree ℓ cyclic extensions of quadratic fields (the quadratic resolvent). From Theorem 2.3.2, the discriminant divisor of a degree ℓ dihedral function field can be computed in terms of the discriminant divisor of its quadratic resolvent and the discriminant divisor of the degree ℓ cyclic extension thereof. Moreover, quadratic function fields are uniquely determined (up to twist) by their discriminant divisors. Hence, to construct degree ℓ dihedral function fields of a given discriminant divisor, we have reduced the problem to constructing all cyclic degree ℓ extensions of a given quadratic function field, with prescribed ramification.

Chapter 3

Construction of Dihedral Function Fields via Class Field Theory

Having introduced the foundations of dihedral function fields, we now proceed by describing our first method for constructing all dihedral extensions of odd prime degree and given ramification; namely via class field theory. In this chapter we will present two algorithms. The first algorithm will construct all degree ℓ dihedral function fields with a given discriminant divisor and fixed quadratic resolvent. Using the first algorithms, we produce another method for constructing all degree ℓ dihedral function fields with a given discriminant divisor (with any possible the quadratic resolvent).

The results of this chapter are similar to those found in [8] (which is based on [19]) for the number field setting; they are however my own work and not mentioned in [42]. We also note that recently (after I had developed this work) this method was presented in [28] for the case $\ell = 3$. To the best of my knowledge, the remaining cases are not covered elsewhere in the literature, though it would not be surprising if others were aware of this technique for other values of ℓ.

Recall that we have reduced the problem of constructing degree ℓ dihedral function fields of a given discriminant divisor to that of constructing all cyclic Galois degree

ℓ extensions of a given quadratic function field with prescribed ramification. Class field theory is the study of abelian extensions, and as such, it is the natural place to begin.

Throughout this chapter, K will be a function field with finite constant field k.

3.1 Class Fields of Function Fields

We begin our introduction to class field theory by returning again to Galois theory.

Definition 3.1.1. Let K'/K be a Galois extension of function fields with Galois group $\mathcal{G}$. Let P_1' and P_2' be two unramified places of K' lying over a place $P \in \mathbb{P}(K)$. Define the *Artin conjugacy class* $(P, K'/K) \subset \mathcal{G}$ to be the set of $Fr_{P'} \in \mathcal{G}$ for all $P'|P$.

Since the above places are assumed to be unramified, their Frobenius elements $Fr_{P'}$ are well defined in $\mathcal{G}$. By Theorem 2.2.8, the two decomposition groups $Z(P_1'|P)$ and $Z(P_2'|P)$ are conjugate subgroups of $\mathcal{G}$. Hence $(P, K'/K)$ is well defined and indeed a conjugacy class of $\mathcal{G}$.

Now, and for the remainder of this section, assume that K'/K is a finite abelian Galois extension of function fields. Then $(P, K'/K)$ is in fact a single automorphism. Hence we can define a map from the unramifield places of K'/K to $\mathcal{G}$.

Definition 3.1.2. Let $S = S(K'/K) \subset \mathbb{P}(K)$ denote the set of places of K ramified in K'. Let $\mathrm{Div}_S(K)$ be the subgroup of $\mathrm{Div}(K)$ consisting of the divisors whose support is disjoint from S. The *Artin map* $(*, K'/K) : \mathrm{Div}_S(K) \to \mathrm{Gal}(K'/K)$ is the homomorphism extending the map defined by $P \mapsto (P, K'/K)$ to $\mathrm{Div}_S(K)$, where $P \in \mathbb{P}(K)$.

The Artin map relates Galois groups to divisor groups in a precise way. This

relationship is made more explicit by the following proposition:

Proposition 3.1.3 ([30] Prop 9.18)**.** *Let* $S' = S'(K'/K)$ *denote the set of* $P'|P$ *where* $P \in S(K'/K)$ *and let* $\mathrm{Div}_{S'}(K')$ *be the subgroup of* $\mathrm{Div}(K')$ *consisting of the divisors whose support is disjoint from* S'*. Then the Artin map is onto and its kernel contains the group* $\mathrm{N}_{K'/K}(\mathrm{Div}_{S'}(K'))$*.*

To understand the kernel of the Artin map, we present ray class groups.

Definition 3.1.4. Let $M = \sum n_P P$ be a divisor of K. The *ray modulo* M is the subgroup of $\mathrm{Prin}(K)$ given by

$$R_M(K) = \{(\alpha) \in \mathrm{Prin}(K) : v_P(\alpha - 1) \geq n_P, \forall P \in \mathrm{Supp}(M)\}.$$

Let $\mathrm{Prin}_M(K)$ denote the principal divisors of K supported away from M. Then $R_M(K)$ is a subgroup of $\mathrm{Prin}_M(K)$, and thus a subgroup of $\mathrm{Div}_S(K)$. The *ray class group modulo* M is the quotient group $Cl_M(K) = \mathrm{Div}_S(K)/R_M(K)$.

We note that every ray class group $Cl_M(K)$ is infinite. There is a natural degree map on $Cl_M(K)$ that induces the following exact sequence:

$$1 \to Cl_M^0(K) \to Cl_M(K) \to \mathbb{Z} \to 1,$$

where $Cl_M^0(K)$ denotes the ray classes of degree 0. We remark that $Cl_M^0(K)$ is finite and thus sometimes called the ray class group in the literature to align with the number field situation in that regard. We will refer to $Cl_M^0(K)$ as the degree zero ray class group modulo M.

We can now describe the kernel of the Artin map.

Theorem 3.1.5 ([7] Ch 7, Sect 5, Thm 5.1)**.** *Let* K'/K*,* $S = S(K'/K)$*, and* $S' =$

$S'(K'/K)$ as above. Then the following hold:

1. *Artin Reciprocity Theorem: The Artin map is onto and there exists an effective divisor M supported on S such that the kernel of the Artin map is $\mathrm{Prin}_M(K)\,\mathrm{N}_{K'/K}(\mathrm{Div}_{S'}(K'))$. Consequently, the Artin Map induces an isomorphism*

$$Cl_M(K)/\langle[\mathrm{N}_{K'/K}(\mathrm{Div}_{S'}(K'))]\rangle \cong \mathrm{Gal}(K'/K).$$

   where $\langle[\mathrm{N}_{K'/K}(\mathrm{Div}_{S'}(K'))]\rangle$ denotes the subgroup of $Cl_M(K)$ generated by the classes of the elements in $\mathrm{N}_{K'/K}(\mathrm{Div}_{S'}(K'))$.

2. *Takagi Existence Theorem: For each subgroup $\mathcal{H}$ of finite index in $Cl_M(K)$ there exists a unique abelian extension K'/K such that $\langle[\mathrm{N}_{K'/K}(\mathrm{Div}_{S'}(K'))]\rangle = \mathcal{H}$.*

Remark 3.1.6. Considering Theorem 3.1.5, we can see that every abelian extension of a function field can be understood via its ray class groups and, more generally, via class field theory. This pursuit is well beyond the scope of this thesis (see [41] and [7] for more details); however, we require further results from class field theory to construct all dihedral function fields of a given discriminant divisor. While we have presented the required background to state these results, the material required to understand their proofs, including that of Theorem 3.1.5, is not covered in this thesis. These results are very deep; their proofs rely on local class field theory, infinite Galois theory, and the theory of Drinfeld modules, to name a few ingredients.

By Theorem 3.1.5, and the universal property of inverse limits, there exists a unique (within a fixed algebraic closure) infinite Galois extension K_M with the property that $\mathrm{Gal}(K_M/K) = Cl_M(K)$. The function field K_M is called the *ray class field* modulo M. Notice that Theorem 3.1.5 says that every abelian extension of K is a subfield of a ray class field of K.

Notice too that the Artin Reciprocity Theorem only claims the existence of an effective divisor M. There are in fact many possible divisors M for which the Artin Reciprocity Theorem holds. In particular, if $M_1 < M_2$ (with "$<$" as in Definition 2.1.22), then $Cl_{M_1}(K) \subset Cl_{M_2}(K)$. However, there is a unique minimal choice of M under this ordering called the *conductor* of K'/K. The conductor of a subgroup $\mathcal{H} \subset R_M$ is defined to be the conductor of the field corresponding to $\mathcal{H}$ in part 2 of Theorem 3.1.5. Putting this together, we see that every field of conductor M is a subfield of the ray class field modulo M, and the ray class field modulo M contains all abelian extensions with conductor less than or equal to M.

From Theorem 3.1.5 we also see that the conductor of K'/K is related to the discriminant divisor of K'/K, as both are supported at the ramified places. We make this relationship explicit for the particular extensions of interest to this thesis with the following proposition:

Proposition 3.1.7 ([41] Thm 12.6.39)**.** *Let ℓ be a prime. Let K'/K be a degree ℓ tamely ramified cyclic Galois extension of function fields. Let $M \in \mathrm{Div}(K)$ be the sum of the places of K ramified in K'. Then the conductor of K'/K is M, and $\Delta(K'/K) = (\ell - 1)M$.*

3.2 Class Field Theoretic Construction Algorithms

In this section we present an algorithm for constructing all degree ℓ dihedral function fields with a given discriminant divisor. As explained before, we do so by constructing cyclic extensions of their quadratic resolvents.

Let K_0/k_0 be a rational function field of characteristic different from 2 and ℓ, with finite constant field k_0. We will use the notation of Example 2.2.4, namely that ℓ is

an odd prime, that K_0 is a rational function field, and that the field $K_{2\ell}$ is the Galois closure of K_ℓ with Galois group $\mathcal{D}_\ell$. Recall further that K_2 is the quadratic resolvent of K_ℓ, i.e. the fixed field of the unique index 2 subgroup $\mathcal{C}_\ell$ of $\mathcal{D}_\ell$ generated by σ. K_ℓ is the fixed field of τ, the generator of $\mathcal{C}_2$ in $\mathcal{D}_\ell$. Also recall from Theorem 2.3.2 that

$$\Delta(K_\ell/K_0) = \frac{\ell-1}{2}\left(\Delta(K_2/K_0) + M\right),$$

where $(\ell-1)M = N_{K_2/K}((\ell-1)M')$, with M' defined by $(\ell-1)M' = \Delta(K_{2\ell}/K_2)$. By Proposition 3.1.7, M' is the conductor of $K_{2\ell}/K_2$.

We saw in the previous section that every abelian extension of a function field is a subfield of a ray class field. Moreover, for the case of tamely ramified cyclic extensions of prime degree, we saw in Proposition 3.1.7 that the discriminant divisor of that extension is determined by its conductor. Consequently, we have a method to compute all degree ℓ dihedral function fields of a given discriminant divisor and fixed quadratic resolvent; namely by computing all degree ℓ subfields of the appropriate ray class field. Thus, Theorem 3.1.5 and Proposition 3.1.7 lead directly to Algorithm 3.1.

This algorithm cannot actually be implemented in Magma as written. While Magma can compute the Galois group of a function field, it does not return the actual Galois automorphisms (the group is returned abstractly). Thus, we cannot compute the fixed field of an element of order 2 in $\mathrm{Gal}(K_{2\ell}/K_0)$ in this manner. One could potentially compute a lift of τ to $K_{2\ell}$ and use Magma's fixed field methods. Using such a lift, we will compute the defining equation for K_ℓ directly from a defining equation of $K_{2\ell}/K_2$ via the following proposition:

Proposition 3.2.1. *With the notation above, let $f(Y)$ be a defining polynomial of*

Algorithm 3.1 (Constructing $\mathcal{D}_\ell$ function fields from their quadratic resolvents via class field theory.)

Input: A quadratic extension K_2 of K_0, an odd prime ℓ, and a squarefree effective divisor M of K_0 coprime to $\Delta(K_2/K_0)$.

Output: The set L of all the dihedral extension K_ℓ of K with $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}(\Delta(K_2/K_0) + M)$ and with quadratic resolvent field K_2.

```
[Compute fundamental information.]
Compute the set S_M of all M' ∈ Div(K_2) such that N_{K_2/K_0}(M') = M.
Initialize the set L to be empty.
[Compute all possible K_ℓ.]
for M' ∈ S_M do
    Compute Cl_{M'}(K_2) and the set S_ℓ of index ℓ subgroups of Cl_{M'}(K_2).
    for H ∈ S_ℓ do
        Compute K_{2ℓ} corresponding to H in part 2 of Theorem 3.1.5.
        Compute the conductor D' of K_{2ℓ}/K_2.
        if D' = M' then
            if K_{2ℓ}/K is Galois and Gal(K_{2ℓ}/K) ≅ D_ℓ then
                Append K_ℓ = Fix(⟨τ⟩) to L
return L
```

$K_{2\ell}/K_2$. *Let* $R(T) = Res_Y(f(Y), \tau(f(T-Y)))$ *be the resultant of* $f(Y)$ *and* $\tau(f(T-Y))$. *Then* $R(T) \in K_0[T]$ *and factors as a product of irreducible polynomials* $Q_j(T) \in K_0[T]$, $0 \le j < \ell$, *each of degree* ℓ. *Moreover, each* $Q_j(T)$ *is a defining equation for the subfield* K_ℓ *of* $K_{2\ell}$.

Proof. Let $\theta_i \in K_{2\ell}$ be the ℓ roots of a defining polynomial for $K_{2\ell}/K_2$. Then the roots of $R(T)$ are exactly the elements $\theta_i + \tau(\theta_j)$, $0 \le i, j \le \ell - 1$, where τ denotes a lift to $K_{2\ell}$ of the nontrivial Galois automorphism of K_2/K_0. Let σ be a generator of $\mathrm{Gal}(K_{2\ell}/K_2)$. Then consider the ℓ polynomials

$$Q_j = \prod_{i=0}^{\ell-1} \big(T - \sigma^i\big(\theta_j + \tau(\theta_j)\big)\big)$$

for $0 \le j < \ell$. Each Q_j is clearly stable under σ. Moreover, as $\tau\sigma\tau = \sigma^{-1}$, each Q_j is

stable under τ as well. Consequently $Q_j \in K_0[T]$ and hence so is $R(x)$.

We claim that Q_j is the minimal polynomial of $\theta_j + \tau(\theta_j)$ which is an element of some index 2 subfield of $K_2(\theta)$. As $\theta_j + \tau(\theta_j)$ is invariant under τ, it lies in its fixed field. However, as it is not invariant under σ, it does not lie in K_0. Thus, as ℓ is prime, $\theta_j + \tau(\theta_j) \in K_\ell$ for some $K_2(\theta)/K_\ell/K_0$ with $[K_2(\theta) : K_\ell] = 2$. Hence, $\theta_j + \tau(\theta_j)$ has a degree ℓ monic irreducible minimal polynomial $m_j \in K_0[T]$. As $\theta_j + \tau(\theta_j)$ is a root of Q_j, m_j divides Q_j. However, Q_j is also a monic polynomial of degree ℓ, and therefore $m_j = Q_j$.

Now, all the index two subfields of $K_{2\ell}$ are Galois conjugate and hence can be defined by the same minimal polynomial. So there are ℓ possible choices of irreducible factors of $R(T)$, not necessarily distinct, each one a defining polynomial for the degree ℓ subfield of $K_{2\ell}$ (up to Galois conjugation). □

We note that each of the statements of Algorithm 3.1 can now be implemented in Magma almost exactly as written (using Proposition 3.2.1 to compute $\mathrm{Fix}(\tau)$).

Example 3.2.2. In this example we perform Algorithm 3.1 for the case $\ell = 3$ and $M = 0$. Consider the rational function field $K_0 = \mathbb{F}_7(x)$. Let $K_2 = \mathbb{F}_7(x, y)$ be the quadratic function field defined by $y^2 = x(x + 3)(x + 1)$. Then

$$Cl_M(K_2) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z} \cong \langle [C_1'] \rangle \oplus \langle [C_2'] \rangle \oplus \langle [C_3'] \rangle,$$

where

$$C_1' = \langle x + 1, y \rangle - \langle x, y \rangle, \qquad C_2' = \langle x + 5, y + 3 \rangle - \langle x, y \rangle, \qquad C_3' = \langle x, y \rangle.$$

There are thus 4 index 3 subgroups of $Cl_M(K_2)$:

$$\mathcal{H}_1 = \langle [C_1'], 3[C_2'], [C_3'] \rangle,$$
$$\mathcal{H}_2 = \langle [C_1'], [C_2'], 3[C_3'] \rangle,$$
$$\mathcal{H}_3 = \langle [C_1'], 3[C_2'], 3[C_3'], [C_1'] + [C_2'] \rangle,$$
$$\mathcal{H}_4 = \langle [C_1'], 3[C_2'], 3[C_3'], [C_1'] + 2[C_2'] \rangle.$$

We compute the fields $K_{6,i}/K_2$ corresponding to $\mathcal{H}_i$ under Theorem 3.1.5. Checking their Galois groups, we find that only $K_{6,1}/K_0$ is dihedral. As the conductor must be less than or equal to $M = 0$, we know $K_{6,1}/K_2$ has conductor 0. We then compute a defining polynomial $Y^3 + 4xy + 6x^3 \in K_2[Y]$ for $K_{6,1}/K_2$. Now, using Proposition 3.2.1, we compute a defining equation for the field K_3/K_0 to be $T^3 + (x^2 + 4x)T + 5x^3$, and find that indeed $\Delta(K_3/K_0) = \Delta(K_2/K_0)$.

Even though Algorithm 3.1 can be implemented in Magma using Proposition 3.2.1, the generic algorithms available to perform the check if $K_{2\ell}$ is Galois, and to compute its Galois group, are very costly. There are however some improvements that can be made via the following propositions:

Proposition 3.2.3. *If $K_{2\ell}/K_2$ is Galois with conductor M', then $\tau(M') = M'$. Let $M = \mathrm{N}_{K_2/K_0}(M')$. Then $M = 2M_0$ for some squarefree effective divisor $M_0 \in \mathrm{Div}(K_0)$, where $\Delta(K_2/K_0)$ and M_0 have disjoint support. Thus $M' = \mathrm{Con}_{K_2/K_0}(M_0)$.*

Proof. If $K_{2\ell}/K_2$ is Galois with conductor M', then a lift of τ fixes $K_{2\ell}$, and hence τ fixes its conductor. Thus, for all P' in $\mathbb{P}(K_2)$, we have $P' \in \mathrm{Supp}(M')$ if and only if $\tau(P')$ in $\mathrm{Supp}(M')$. By Theorem 2.3.2, M and $\Delta(K_2/K_0)$ are disjoint; in particular, no place in $\mathrm{Supp}(M)$ ramifies in K_2. It follows that M' is of the form

$M' = D' + E'$ where D' is the sum of both places P' of K_2 lying above each place P in $\mathrm{Supp}(M)$ that split in K_2, and E' is the sum of the places P' of K_2 lying above the places $P \in \mathrm{Supp}(M)$ that are inert in K_2. Hence, $M = 2M_0$ where $M_0 = N_{K_2/K_0}(D' + E')$. It is now easy to see that M_0 is effective, squarefree, has support disjoint from $\Delta(K_2/K_0)$, and $M' = \mathrm{Con}_{K_2/K_0}(M')$. □

We can now improve Algorithm 3.1 by changing the input to a squarefree effective divisor M_0 instead of a divisor M. Then by the above proposition we need only consider one possibility for M' in step 5, thereby effectively removing the loop. Moreover, we have the following corollary:

Corollary 3.2.4. *There are no dihedral function fields K_ℓ/K_0 with $\deg(\Delta(K_\ell/K_0)) < 2(\ell-1)$ when k_0 is a finite field.*

Proof. Suppose K_ℓ is a $\mathcal{D}_\ell$ extension of K_0 with Galois closure $K_{2\ell}$ and quadratic resolvent K_2. Theorem 2.3.2 and Proposition 3.2.3 give $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}\Delta(K_2/K_0) + (\ell-1)M_0$. Quadratic extensions have discriminants of even degree and so $\deg(\Delta(K_\ell/K_0))$ is divisible by $\ell - 1$. Therefore, it suffices to rule out the three possibilities when $\Delta(K_2/K_0)/2 + \deg(M_0) \leq 1$.

1. $\deg(\Delta(K_2/K_0) = \deg(M_0) = 0$: In this case, K_ℓ/K would be a constant field extension, and would not have Galois group $\mathcal{D}_\ell$.
2. $\deg(\Delta(K_2/K_0)) = 1$, $\deg(M_0) = 0$: In this case K_2 would have genus 0 and $K_{2\ell}/K_2$ would be unramified and hence a constant field extension. So, as K_ℓ is the fixed field of τ, K_ℓ/K_0 would also be a constant field extension, and hence $K_{2\ell}/K_0$ would not be dihedral.
3. $\deg(\Delta(K_2/K_0)) = 0$, $\deg(M_0) = 1$: In this case, K_2/K_0 is a constant field ex-

tension and M_0 is a single place of degree 1; since every place in M_0 must split in K_2 or of degree 2. Now, since the places of K_0 that split in a quadratic constant field extension are the places of even degree, we again have a contradiction.

□

We now show how to verify if $K_{2\ell}/K_0$ is dihedral.

Proposition 3.2.5. *Let M_0 be a squarefree effective divisor of K_0 that is coprime to $\Delta(K_2/K_0)$, and let $M' = \mathrm{Con}_{K_2/K_0}(M_0)$. Let $\mathcal{H} \subset Cl_{M'}(K_2)$ be an index ℓ subgroup of $Cl_{M'}(K_2)$, and let $K_{2\ell}/K_2$ be the extension corresponding to $\mathcal{H}$ via Theorem 3.1.5. Then the following hold:*

1. *$K_{2\ell}/K_0$ is Galois if and only if τ fixes $\mathcal{H}$.*
2. *Additionally, $K_{2\ell}/K_0$ is Galois with Galois group $\mathcal{D}_\ell$ if and only if τ does not fix any generator of $Cl_{M'}(K_2)/\mathcal{H}$.*

Proof. First we show that the ray class field $K_{M'}$ is Galois over K_0. Clearly, $K_{M'}/K_0$ is separable and algebraic, thus it remains to show $K_{M'}/K_0$ is normal. Let K_0^{sep} be a fixed separable closure of K_0 containing $K_{M'}$. Let ω be an element of order 2 in $\mathrm{Gal}(K_0^{\mathrm{sep}}/K_0)$, so that ω is a lift of τ. As $K_{M'}/K_2$ is Galois and thus normal, $K_{M'}/K_0$ is normal if and only if $\omega(K_{M'}) = K_{M'}$ ([17] p. 631).

First, as $K_{M'}/K_2$ is abelian, so too is $\omega(K_{M'})/K_2$. By part 3 of Theorem 2.2.8, $\omega(K_{M'})/K_2$ is ramified only at $\omega(M')$. However, $\omega(M') = \tau(M') = M'$ by Proposition 3.2.3. Now, as $K_{M'}$ is the maximal abelian extension of K_2 ramified at M', we have $\omega(K_{M'}) \subset K_{M'}$, and hence they are equal. Therefore, $K_{M'}/K_0$ is normal and thus Galois.

As K_2/K_0 is Galois, by Theorem 2.2.3, we see that $\mathrm{Gal}(K_{M'}/K_2)$ is a normal

subgroup of $\mathrm{Gal}(K_{M'}/K_0)$ and thus the following sequence is exact and splits canonically:

$$1 \longrightarrow \mathrm{Gal}(K_{M'}/K_2) \longrightarrow \mathrm{Gal}(K_{M'}/K_0) \longrightarrow \mathrm{Gal}(K_2/K_0) \longrightarrow 1.$$

Thus, $\mathrm{Gal}(K_{M'}/K_0)$ is isomorphic to $\mathrm{Gal}(K_{M'}/K_2) \rtimes \langle\tau\rangle$, where τ acts on $\mathrm{Gal}(K_{M'}/K_2)$ by conjugation . Thus, by Theorem 2.2.3, $K_{2\ell}/K_0$ is Galois if and only if $\mathrm{Gal}(K_{2\ell}/K_2) \rtimes \langle\tau\rangle$ is a normal subgroup of $\mathrm{Gal}(K_{M'}/K_2) \rtimes \langle\tau\rangle$.

Investigating the action of τ on $\mathrm{Gal}(K_{M'}/K_2)$ more explicitly via part 3 of Theorem 2.2.8, we see that the Artin map has the property that

$$(\tau(P'), K_{M'}/K_2) = (\omega(P'), K_{M'}/K_2) = \omega(P', K_{M'}/K_2)\omega.$$

for all unramified places $P' \in \mathbb{P}(K_2)$. Now, by Theorem 3.1.5, $\mathrm{Gal}(K_{2\ell}/K_2) \cong Cl_{M'}(K_2)/\mathcal{H}$ via the Artin map. Therefore $K_{2\ell}/K_0$ is Galois if and only if $\mathcal{H} \rtimes \langle\tau\rangle$ is a normal subgroup of $Cl_{M'}(K_2) \rtimes \langle\tau\rangle$, where here, via the Artin map, the action of τ on $Cl_{M'}(K_2)$ is the natural action of τ on divisor classes. As $Cl_{M'}(K_2)$ is abelian, $\mathcal{H} \rtimes \langle\tau\rangle$ is a normal subgroup of $Cl_{M'}(K_2) \rtimes \langle\tau\rangle$ if and only if $\tau(\mathcal{H}) = \mathcal{H}$.

Assuming that $K_{2\ell}/K_0$ is Galois, there are only two possibilities for the group $\mathrm{Gal}(K_{2\ell}/K_0)$; it is either abelian and thus isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, or it is non-abelian, and thus isomorphic to $\mathcal{D}_\ell$. Thus, to prove that the Galois group is $\mathcal{D}_\ell$, we need only show it is not abelian. If we take $[C']$ to be any generator of $Cl_{M'}(K_2)/\mathcal{H}$, then $(\tau(C'), K_{2\ell}/K_2) = \tau(C', K_{2\ell}/K_2)\tau$, and hence $\mathrm{Gal}(K_{2\ell}/K_0)$ is abelian if and only if the action of τ is trivial, i.e. if and only if $\tau([C']) + \mathcal{H} = [C'] + \mathcal{H}$. □

The above proposition gives a simple criterion to effectively check if $K_{2\ell}/K_0$ is Galois and $\mathrm{Gal}(K_{2\ell}/K_0) \cong \mathcal{D}_\ell$ in step 11 of Algorithm 3.1. This removes the need

to use the slower generic algorithms. Combining this with the previously mentioned improvement, we present a practical implementation of Algorithm 3.1 in Algorithm 3.2. This was implemented, and the results are discussed further in Chapter 6.

Algorithm 3.2 (Efficiently constructing $\mathcal{D}_\ell$ function fields from their quadratic resolvents via class field theory.)

Input: A quadratic extension K_2 of K_0, an odd prime ℓ, and an effective squarefree divisor M_0 of K_0 coprime to $\Delta(K_2/K_0)$.

Output: The set L of all the dihedral extension K_ℓ of K with $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}\Delta(K_2/K_0) + (\ell-1)M_0$ and quadratic resolvent K_2.

1: Compute $M' = \mathrm{Con}_{K_2/K_0}(M_0) \in \mathrm{Div}(K_2)$.
2: Initialize the set L to be empty.
3: [Compute all possible K_ℓ.]
4: Compute $Cl_{M'}(K_2)$ and the set S_ℓ of index ℓ subgroups of $Cl_{M'}(K_2)$.
5: **for** $\mathcal{H} \in S_\ell$ **do**
6: Compute the conductor D' of $\mathcal{H}$.
7: **if** $D' = M'$ **then**
8: Compute $[D_\mathcal{H}] + \mathcal{H}$ a generator of $Cl_{M'}/\mathcal{H}$.
9: **if** $\tau(\mathcal{H}) = \mathcal{H}$ and $\tau([D_\mathcal{H}]) + \mathcal{H} \neq [D_\mathcal{H}] + \mathcal{H}$ **then**
10: Compute defining equation $f(Y)$ for $K_{2\ell}/K_2$ corresponding to $\mathcal{H}$ in part 2 of Theorem 3.1.5.
11: Compute the resultant $R(T) = \mathrm{Res}_Y(f(Y), \tau(f(T-Y))$
12: Factor $R(T)$ and let $Q(T)$ be a factor of degree ℓ.
13: Append $Q(T)$ to L_2.
14: **return** L

Example 3.2.6. Using the information of Example 3.2.2, we see that $[C_2'] + \mathcal{H}_1$ is a generator of $Cl_{M'}(K_2)/\mathcal{H}_1$. First we see that $\tau(C_1') = C_1'$ and $\tau(C_3') = C_3'$, and hence

$\tau(\mathcal{H}_1) = \mathcal{H}_1$. We then compute

$$\begin{aligned}\tau(C_2') &= \tau(\langle x+5, y+3\rangle) - \tau(\langle x, y\rangle) \\ &= \langle x+5, y-3\rangle - \langle x, y\rangle \\ &= 5C_2' + 2C_3'\end{aligned}$$

and see that $\tau([C_2]) + \mathcal{H} = 2[C_2'] + \mathcal{H}$. Therefore, $K_{6,1}/K_0$ of Example 3.2.2 is indeed a dihedral Galois extension by Proposition 3.2.5.

Regardless of any remaining inefficiencies, this approach is broad in its applicability and is practical in many cases. Notice that Algorithm 3.2 does not place severe restrictions on the underlying constant field, it only requires the constant field to be finite and of characteristic different from 2 and ℓ. Thus, using Algorithm 3.2, we can produce a reasonable technique to construct all degree ℓ dihedral function fields of a given discriminant divisor. This is presented in Algorithm 3.3.

Algorithm 3.3 takes advantage of the following observation: In order for any degree ℓ dihedral function fields K_ℓ to exist, the discriminant divisor D of its quadratic resolvent must be effective, squarefree, and of even degree. As we saw in Example 2.1.30, if $D = 0$, then this field is the unique quadratic constant field extension of K_0 which we denote $\tilde{K}_0$. If D is nonzero, then there are exactly two quadratic function function fields K_2 and $\widehat{K}_2$ of discriminant divisor D.

Recall that all finite places P of K_0 correspond to monic irreducible polynomials $f_P(x)$ in $k_0[x]$. Therefore, in step 2 of Algorithm 3.3 we can easily construct K_2 and $\widehat{K}_2$ as in Example 2.1.30.

Even with the two improvements resulting from Propositions 3.2.3 and 3.2.5, the

Algorithm 3.3 (Constructing $\mathcal{D}_\ell$ function fields from their divisors via class field theory.)

Input: An odd prime ℓ and squarefree effective divisors D and M_0 of K_0 with disjoint support.

Output: The set L of all the dihedral extension K_ℓ of K_0 with $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}D + (\ell-1)M_0$.

1: **if** $\deg(D)$ is even **then**
2: Construct a quadratic field K_2 with discriminant divisor D.
3: **else**
4: **return** "D IS NOT A QUADRATIC DISCRIMINANT DIVISOR".
5: [Compute possible K_ℓ]
6: Initialize the set L to be empty.
7: **if** $D = 0$ **then**
8: Get L_1 from Algorithm 3.2 with input $\tilde{K}_0, \ell, M_0$.
9: $L \leftarrow L \cup L_1$.
10: **else**
11: Construct K_2 and $\widehat{K}_2$ of discriminant divisor D.
12: Get L_1 from Algorithm 3.2 with input K_2, ℓ, M_0.
13: Get L_2 from Algorithm 3.2 with input $\widehat{K}_2, \ell, M_0$.
14: $L \leftarrow L \cup L_1 \cup L_2$.
15: **return** L.

class field theoretic methods of Algorithm 3.2 (and consequently Algorithm 3.3) are not very efficient. For instance, the built-in function in Magma for computing a defining equation for $K_{2\ell}/K_2$ in step 10 of Algorithm 3.2 is quite costly. Indeed, the method was implemented in Magma by C. Fieker and based upon his number field algorithm in [19], in which he notes that a "rather surprising bottleneck is the computation of the minimal polynomials" for cyclic extensions.

Even if some of these built-in functions could be improved upon by specializing them to computing dihedral extensions, we are still computing more than what is required. We must compute the conductor of every subgroup produced in step 6 of Algorithm 3.2; this includes one for every degree ℓ cyclic field whose conductor divides

M'. While the conductor can be computed group-theoretically without computing the defining equation of $K_{2\ell}$, it still needs to be computed for each subgroup. While not terribly time consuming, this becomes especially inefficient for inputs M_0 with large support, where many irrelevant subgroups are considered.

Example 3.2.7. Consider the rational function field $K_0 = \mathbb{F}_7(x)$. Let $K_2 = \mathbb{F}_7(x, y)$ be the quadratic function field defined by $y^2 = x(x+3)(x+1)$, let $M_0 = \langle x+3 \rangle + \langle x+5 \rangle \in \mathrm{Div}(K_0)$, and let $M' = \mathrm{Con}_{K_2/K_0}(M_0)$. Then

$$Cl_{M'}(K_2) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z},$$

and thus $Cl_{M'}(K_2)/3(Cl_{M'}(K_2)) \cong (\mathbb{Z}/3\mathbb{Z})^4$. Hence, there are 40 distinct index 3 subgroups of $Cl_{M'}(K_2)$, and as we will see in Example 4.2.3, only 3 of these correspond to dihedral function fields with conductor M'.

The above example illustrates the inefficiency of Algorithm 3.2 for a conductor M_0 of degree only 2. As the degree of M_0 grows, so too does the number of extraneous subgroups of $Cl_{M'}(K_2)$ that need to be considered.

The algorithms presented in the next two chapters overcome some of these obstacles. In particular, we will construct all dihedral function fields with the prescribed discriminant divisors without having to verify any conductors (or discriminant divisors) along the way. Furthermore, in this new method we have an explicit formula for the defining equation of K_ℓ/K_0. This avoids the costly computations of finding a defining equation for $K_{2\ell}/K_2$ in step 10 of Algorithm 3.2, and factoring (and computing) a resultant polynomial as in Proposition 3.2.3. A runtime comparison of these approaches will be provided in Chapter 6.

Chapter 4

Kummer Theoretic Approach with ℓ-th Roots of Unity

In this chapter we will present an algorithm to construct all dihedral function fields with a given discriminant divisor when the constant field contains the ℓ-th roots of unity. The construction algorithm is based on the main theorem, which is an exact count for the number of degree ℓ function fields with Galois group $\mathcal{D}_\ell$ and given discriminant divisor Δ. Throughout, let $\zeta_\ell \in \overline{k_0}$ be a primitive ℓ-th root of unity. Again for this chapter we will assume that k_0 is perfect though not necessarily finite, with characteristic not dividing 2ℓ. Let k_2 denote the constant field of a quadratic extension K_2/k_2 of K_0/k_0. Then k_2 is either equal to k_0 or is a quadratic extension thereof. The latter case is equivalent to $K_2 = k_2(x)$ and $\Delta(K_2/K_0) = 0$.

When K_2/K_0 is a constant field extension we are eventually forced to restrict ourselves to the case that k_0 is a finite field. This is essentially due to the fact that all extensions of finite fields are cyclic and thus not dihedral. However, when k_0 is a number field for example, there are infinitely many degree ℓ dihedral extensions of k_0 and hence infinitely many dihedral function fields K_ℓ with $\Delta(K_\ell/K_0) = 0$. The methods to construct and tabulate such fields are beyond the scope of this thesis. Consequently, we will eventually need to make the assumption that when K_2/K_0 is

a constant field extension, K_0 has finite constant field; i.e. we will eventually invoke Assumption COEFF.

Our approach, similar to the last chapter, is to begin with a fixed quadratic resolvent field and construct cyclic degree ℓ extensions of it, such that the resulting field extension $K_{2\ell}/K_0$ is dihedral. In order to perform the Kummer theoretic construction of $K_{2\ell}/K_2$, we will assume that $\zeta_\ell \in k_0$, and hence $\zeta_\ell \in k_2$, for the entirety of this chapter except for Section 4.1.2 where we remove this assumption to present a broader theory of ℓ-virtual units. Thus, outside of Section 4.1.2, when k_0 is a finite field $\mathbb{F}_q$ we assume that $q \equiv 1 \bmod 2\ell$. The case that $\zeta_\ell \in k_2$ but $\zeta_\ell \notin k_0$ is considered in the next chapter.

The contents of this chapter are based upon my work that first appeared in [42], where we only considered the case when k_0 is a finite field $\mathbb{F}_q$ where $q \equiv 1 \bmod 2\ell$. The majority of the results found in this chapter are originally my own work. However, the material in [42] was edited by Everett Howe who made several improvements, clarifying some of the arguments and notation. Moreover, in Subsection 4.1.4, we present his improved method for computing the defining equation of a $\mathcal{D}_\ell$ extension, instead of the method I originally proposed (in Proposition 3.2.1). We will also present his major contribution to [42] in chapter 6, namely a precise count for the number of $\mathcal{D}_\ell$ function fields with the smallest discriminant divisor degree possible, and later extend that result to a wider class of function fields.

4.1 Constructing and Counting Dihedral Function Fields

Since k_2 contains a primitive ℓ-th root of unity, all cyclic ℓ-extensions of K_2 are Kummer extensions — that is, extensions of the form $K_2(\sqrt[\ell]{\alpha})$ for some $\alpha \in K_2^\times \setminus (K_2^\times)^\ell$.

In subsection 4.1.1 we give necessary and sufficient conditions on α for $K_2(\sqrt[\ell]{\alpha})$ to be Galois over K_0 with group $\mathcal{D}_\ell$. In subsection 4.1.2, we use virtual units to decompose $K_2^\times/(K_2^\times)^\ell$ in a way that allows us to determine the elements α that correspond to nonisomorphic dihedral function fields. With this information, in subsection 4.1.3 we give a constructive proof of the main theorem: a parameterization of the number of nonconjugate dihedral degree ℓ extensions of K_0 with a given quadratic resolvent field K_2 and discriminant divisor. We close this section by presenting a method due to Everett Howe [42] for efficiently computing a defining equation for K_ℓ from α.

4.1.1 Kummer Theory

Let ℓ be prime and let K be a function field that contains the ℓ-th roots of unity. A *degree ℓ Kummer extension* of K is an extension of the form $K(\theta)$, where θ^ℓ is an element of $K\backslash K^\ell$. We have the following theorem (see [41, Thm 5.8.5 and Prop 5.8.7]):

Theorem 4.1.1. *Let ℓ be a prime and let K be a field that contains the ℓ-th roots of unity.*

1. *Let $K' = K(\theta)$ be a Kummer extension of K, with $\theta^\ell = \alpha \in K \setminus K^\ell$. Then the minimal polynomial of θ is $T^\ell - \alpha$, and K' is a degree ℓ Galois extension of K.*
2. *Every degree ℓ Galois extension K' of K is a Kummer extension.*
3. *Let $K'_\alpha = K(\sqrt[\ell]{\alpha})$ and $K'_\beta = K(\sqrt[\ell]{\beta})$ be two Kummer extensions of K. Then $K'_\alpha \cong K'_\beta$ if and only if $\alpha = \beta^j\kappa^\ell$ for some $\kappa \in K^\times$ and some $j \in \mathbb{Z}$ with $1 \le j \le \ell - 1$.*
4. *Suppose K is a function field. Let $K' = K(\sqrt[\ell]{\alpha})$ be a Kummer extension, let P*

be a place of K, and let P' be a place of K' lying over P. Then

$$e(P' \mid P) = \frac{\ell}{\gcd(\ell, v_P(\alpha))}.$$

Note in particular that statement (3) gives a bijection between the Kummer extensions of K and the nontrivial cyclic subgroups of $K^\times/(K^\times)^\ell$. Going forwards, we will assume that ℓ is an odd prime.

Let K_2/k_2 be a quadratic extension of K_0/k_0, where k_0 contains a primitive ℓ-th root of unity. We construct dihedral degree ℓ function fields with a given quadratic resolvent field K_2 by starting with the quadratic function field K_2 and constructing, via Kummer's theorem, cyclic degree ℓ extensions of K_2 that are Galois over K_0 with Galois group $\mathcal{D}_\ell$. It remains to classify the degree ℓ Kummer extensions of K_2 that are dihedral extensions of K_0.

Proposition 4.1.2. *Let K_2/K_0 be a quadratic function field and let $K_2(\theta)$ be a Kummer extension of K_2, where $\theta^\ell = \alpha \in K_2 \setminus K_2^\ell$. Then $K_2(\theta)$ is a Galois extension of K_0 with Galois group isomorphic to $\mathcal{D}_\ell$ if and only if $\alpha \notin K_0$ and $\mathrm{N}_{K_2/K_0}(\alpha) = \kappa^\ell$ for some $\kappa \in K_0$.*

Proof. Suppose that $\mathrm{Gal}(K_2(\theta)/K_0) = \mathcal{D}_\ell$. Abusing notation, let τ denote an automorphism of $K_{2\ell}/K_0$ that restricts to the nontrivial Galois automorphism of K_2/K_0. By Theorem 4.1.1, $K_2(\theta)/K_0$ is Galois, so $\tau(\theta) \in K_2(\theta)$ and $\tau(\theta)^\ell = \tau(\alpha)$.

Suppose, towards a contradiction, that $\alpha \in K_0$ and hence that $\tau(\alpha) = \alpha$. Let σ be a generator of $\mathrm{Gal}(K_2(\theta)/K_2)$. Then

$$\tau(\theta)^\ell = \tau(\alpha) = \alpha = \theta^\ell,$$

and thus $\tau(\theta) = \zeta_\ell^i \theta$ for some i. However, as $\sigma(\theta) = \zeta_\ell^j \theta$ for some j, it follows that τ and σ commute, a contradiction. Furthermore, as $\alpha \in K_2$, we have

$$\mathrm{N}_{K_2/K_0}(\alpha) = \alpha\tau(\alpha) = (\theta\tau(\theta))^\ell.$$

Conversely, suppose that $\alpha \notin K_0^\times \cup (K_2^\times)^\ell$ and $\mathrm{N}_{K_2/K_0}(\alpha) = \kappa^\ell$ for some $\kappa \in K_0$. Then $\theta\kappa^{-1} \in K_2(\theta)$. Moreover,

$$(\theta\kappa^{-1})^\ell = \alpha\,\mathrm{N}_{K_2/K_0}(\alpha)^{-1} = \tau(\alpha) \in K_2.$$

As $\alpha \notin (K_2^\times)^\ell$, we see that $K_2(\theta)/K_2$ is a degree ℓ Kummer extension. By Theorem 4.1.1, the minimal polynomial of θ over K_2 is $T^\ell - \alpha$, and by applying τ we find that the minimal polynomial of $\tau(\theta)$ is $T^\ell - \tau(\alpha)$. Therefore, $K_2(\theta)$ is the splitting field of $(T^\ell - \alpha)(T^\ell - \tau(\alpha)) \in K_0[T]$ and is Galois over K_0 with Galois group $\mathcal{D}_\ell$. □

Remark 4.1.3. The norm map from K_2 to K_0 induces a norm map

$$\mathrm{N}\colon K_2^\times/(K_2^\times)^\ell \to K_0^\times/(K_0^\times)^\ell.$$

The above proposition says that a Kummer extension of K_2 is Galois over K_0 with Galois group $\mathcal{D}_\ell$ if and only if the corresponding cyclic subgroup of $K_2^\times/(K_2^\times)^\ell$ is in the kernel of this norm map.

Elements of K_2 whose norms are ℓ-th powers in K_0 have divisors of a specific type, described below.

Proposition 4.1.4. *Let $\alpha \in K_2^\times$. If $\mathrm{N}_{K_2/K_0}(\alpha) = \kappa^\ell$ for some $\kappa \in K_0^\times$, then the*

principal divisor of α takes the form

$$(\alpha) = \ell E' + \sum_{i=1}^{(\ell-1)/2} i(D'_i - D'_{-i}),$$

where $E' \in \mathrm{Div}(K_2)$ and the D'_i are squarefree effective divisors of K_2 with pairwise disjoint support, and where $\tau(D'_i) = D'_{-i}$ for all i. Consequently, every place of K_0 lying under a place in the support of some D'_i splits in K_2.

Proof. Let P' be a place in the support of the principal divisor (α), and set $n_{P'} = v_{P'}((\alpha))$. Then, by the division algorithm, we can uniquely write $n_{P'} = d\ell + r$ for some $d, r \in \mathbb{Z}$ with $|r| \leq (\ell-1)/2$. Repeating this for all places in the support of (α), we see that the divisor of α can be written uniquely as

$$(\alpha) = \ell E' + \sum_{i=1}^{(\ell-1)/2} i(D'_i - D'_{-i}),$$

where the D'_i are squarefree effective divisors with pairwise disjoint support. Applying the norm map N_{K_2/K_0} to (α), we obtain

$$\begin{aligned}(\mathrm{N}_{K_2/K_0}(\alpha)) &= (\alpha) + (\tau(\alpha)) \\ &= \ell(E' + \tau(E')) + \sum_{i=1}^{(\ell-1)/2} i(D'_i - D'_{-i} + \tau(D'_i) - \tau(D'_{-i})).\end{aligned}$$

As $\mathrm{N}_{K_2/K_0}(\alpha) = \kappa^\ell$, we see that

$$i(D'_i - D'_{-i} + \tau(D'_i) - \tau(D'_{-i})) = 0 \quad \text{for } 1 \leq i \leq (\ell-1)/2.$$

This shows that $D'_i = 0$ if and only if $D'_{-i} = 0$. If $D'_i \neq 0$, then D'_i and D'_{-i} are

effective and have disjoint support, forcing $D'_i = \tau(D'_{-i})$. □

The above proposition allows us to precisely determine the discriminant divisor of a dihedral function field.

Corollary 4.1.5. *Let $K_{2\ell} = K_2(\sqrt[\ell]{\alpha})$ be a cyclic degree ℓ extension of K_2 such that $\mathrm{Gal}(K_{2\ell}/K_0) \cong \mathcal{D}_\ell$. Let (α) be as in Proposition 4.1.4. Then $\Delta(K_{2\ell}/K_2) = (\ell-1)M'$ where*

$$M' = \sum_{i=1}^{(\ell-1)/2} D'_i + D'_{-i}. \tag{4.1}$$

Moreover, if K_ℓ is an index 2 subfield of $K_{2\ell}$, then

$$\begin{aligned}\Delta(K_\ell/K_0) &= \frac{\ell-1}{2}\left(\Delta(K_2/K_0) + \mathrm{N}_{K_2/K_0}(M'_0)\right) \\ &= \frac{\ell-1}{2}\left(\Delta(K_2/K_0) + 2M_0\right).\end{aligned} \tag{4.2}$$

where $2M_0 = \mathrm{N}_{K_2/K_0}(M')$.

Proof. This follows directly from Propositions 4.1.4 and 4.1.2, and Theorems 4.1.1, and 2.3.2. □

As the divisors in equations (4.1) and (4.2) are so pertinent to describing $\mathcal{D}_\ell$ function fields, we ascribe them terminology. Let

$$R = \left\{P \in \mathrm{Supp}(\mathrm{N}_{K_2/K_0}((\alpha))) : \ell \nmid v_P(\mathrm{N}_{K_2/K_0}((\alpha))\right\}.$$

We define the *reduced ramification divisor* of α to be the divisor $M_0 = \sum_{P\in R} P$ of K_0 and the *ramification divisor* of α to be its conorm. This terminology stems from our repeated use of Kummer theory; if $K_{2\ell} = K_2(\sqrt[\ell]{\alpha})$, then the ramification divisor

M_0' of α is the conductor of $K_{2\ell}/K_2$ and the reduced ramification divisor of α is M_0 where $2M_0 = \mathrm{N}_{K_2/K_0}(M_0')$.

Remark 4.1.6. From Proposition 3.1.7, we see that M_0' is the conductor of $K_{2\ell}/K_2$. Furthermore, when k_0 has ℓ-th roots of unity, we can refine the results of Proposition 3.2.3 to exclude inert primes from the definition of a valid divisor, as the support of M_0 can only contain primes that are split in K_2 by Corollary 4.1.5.

4.1.2 Virtual Unit Decomposition

Recall that Theorem 4.1.1 states that elements of $K_2^\times$ that generate the same subgroup of $K_2^\times/(K_2^\times)^\ell$ produce the same Kummer extension. We wish to construct distinct dihedral function fields by constructing distinct Kummer extensions of K_2. To that end, we decompose the group $K_2^\times/(K_2^\times)^\ell$ using a function field definition of virtual units, as inspired by H. Cohen's work on number fields [8]. In particular, we show how to construct a basis for the kernel of the norm map $K_2^\times/(K_2^\times)^\ell \to K_0^\times/(K_0^\times)^\ell$. While motivated by constructing nonisomorphic Kummer extensions when $\zeta_\ell \in k_0$, the theory of virtual units we will present is valid for arbitrary fields K_0/k_0 where k_0 is perfect of characteristic not dividing 2ℓ. Hence, for this subsection we only place these assumptions on k_0, and thus do not assume that $\zeta_\ell \in k_0$. This generality will become especially useful in the next chapter.

Analogous to the number field scenario, we define the (ℓ-)*virtual units* of K_2 to be the elements of the set

$$\mathcal{V}_\ell = \{\alpha \in K_2^\times : (\alpha) \in \ell \operatorname{Div}^0(K_2)\}.$$

The map from $\mathcal{V}_\ell$ to $\mathrm{Div}^0(K_2)$ that sends α to $(\alpha)/\ell$ induces a map from $\mathcal{V}_\ell$ to $\mathrm{Pic}^0(K_2)[\ell]$, the ℓ-torsion of the degree 0 divisor class group of K_2; this leads to the exact sequence

$$1 \longrightarrow k_2^\times/(k_2^\times)^\ell \longrightarrow \mathcal{V}_\ell/(K_2^\times)^\ell \longrightarrow \mathrm{Pic}^0(K_2)[\ell] \longrightarrow 0.$$

We also have an exact sequence

$$1 \longrightarrow \mathcal{V}_\ell/(K_2^\times)^\ell \longrightarrow K_2^\times/(K_2^\times)^\ell \longrightarrow K_2^\times/\mathcal{V}_\ell \longrightarrow 1. \tag{4.3}$$

To better understand the second last arrow of this sequence, we set

$$\mathcal{I}_\ell = \mathrm{Prin}(K_2)/(\mathrm{Prin}(K_2) \cap \ell\,\mathrm{Div}^0(K_2)),$$

and define a map $\varphi\colon K_2^\times \to \mathcal{I}_\ell$ by $\varphi(\alpha) = (\alpha) + \mathrm{Prin}(K_2) \cap \ell\,\mathrm{Div}^0(K_2)$. Then φ is surjective, and $\ker\varphi = \mathcal{V}_\ell$, so $K_2^\times/\mathcal{V}_\ell \cong \mathcal{I}_\ell$. All told, we obtain the diagram of exact sequences depicted in Figure 4.1.

The middle vertical sequence in Figure 4.1 shows that the divisor map from $K_2^\times/(K_2^\times)^\ell$ to $\mathrm{Prin}(K_2)/\ell\,\mathrm{Prin}(K_2)$ has kernel $k_2^\times/(k_2^\times)^\ell$. However, by Remark 4.1.3, Kummer extensions of K_2, with $\zeta_\ell \in k_0$, that are Galois over K_0 with group $\mathcal{D}_\ell$ correspond to nontrivial cyclic subgroups of the kernel of the norm map from $K_2^\times/(K_2^\times)^\ell$ to $K_0^\times/(K_0^\times)^\ell$. We now describe how the divisor map behaves on this kernel.

Let $\mathcal{N}_\ell$ be the group

$$\mathcal{N}_\ell = \left\{\alpha \in K_2^\times : \mathrm{N}_{K_2/K_0}(\alpha) \in (K_0^\times)^\ell\right\}, \tag{4.4}$$

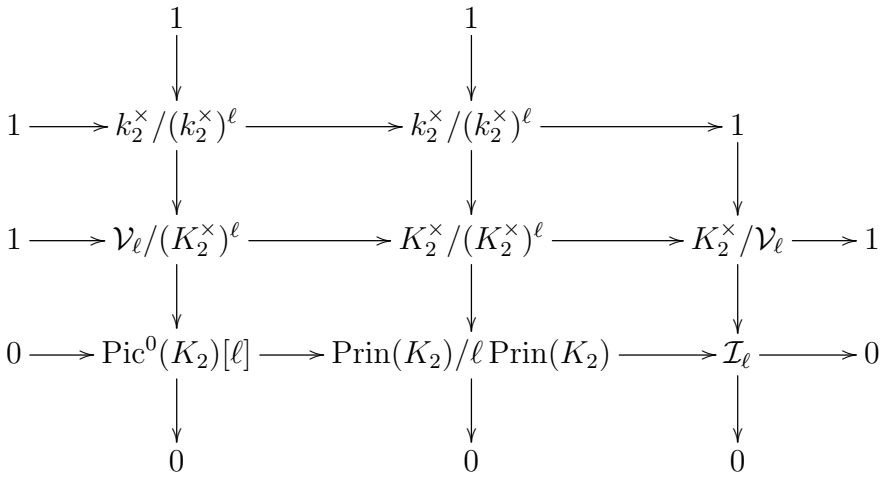


Figure 4.1: Virtual unit decomposition.

so that $\mathcal{N}_\ell/(K_2^\times)^\ell$ is the kernel of the norm map from $K_2^\times/(K_2^\times)^\ell$ to $K_0^\times/(K_0^\times)^\ell$.

Remark 4.1.7. Our combined aim of this chapter and the next is to construct all dihedral degree ℓ function fields with quadratic resolvent K_2 and given discriminant divisor Δ, when $\zeta_\ell \in K_2$. Thus, we need to construct all elements $\alpha \in K_2$ such that $K_{2\ell} = K_2(\sqrt[\ell]{\alpha})$ and $K_{2\ell}/K_0$ is dihedral. We will call such an element α *appropriate*. In order to construct all dihedral function fields with a fixed discriminant divisor, we must be in a situation where there are only finitely many appropriate elements α with a fixed ramification divisor. When this is the case, our approach is to construct such elements α from their divisors.

We have seen in Proposition 4.1.2 that when $\zeta_\ell \in K_0$ the appropriate elements α are the representatives of the group $\mathcal{N}_\ell/(K_2^\times)^\ell$. In Proposition 4.1.8, we will map the elements of this group to their divisors, resulting in the following exact sequence:

$$1 \longrightarrow (k_2^\times \cap \mathcal{N}_\ell)/(k_2^\times)^\ell \longrightarrow \mathcal{N}_\ell/(K_2^\times)^\ell \longrightarrow \mathrm{Prin}(K_2)/\ell\,\mathrm{Prin}(K_2). \tag{4.5}$$

Now, in order to construct all the representatives of $\mathcal{N}_\ell/(K_0^\times)^\ell$ from their divisors, we require the group $(k_0^\times \cap \mathcal{N}_\ell)/(k_0^\times)^\ell$ to be finite. When k_2 is a quadratic extension of $k_0 = \mathbb{Q}(\zeta_3)$ for example, the group $(k_2^\times \cap \mathcal{N}_\ell)/(k_2^\times)^3$ contains all appropriate elements α that result in non-Galois cubic extensions of $\mathbb{Q}(\zeta_3)$ with quadratic resolvent k_2. There are infinitely many of these fields [13], all of which will have trivial discriminant divisor. Thus for $(k_0^\times \cap \mathcal{N}_\ell)/(k_0^\times)^\ell$ to be finite, we must make Assumption COEFF. We will then see in the proof of Proposition 4.1.8 that $(k_0^\times \cap \mathcal{N}_\ell)/(k_0^\times)^\ell$ is in fact trivial under this assumption.

For the remainder of this subsection we make Assumption COEFF.

Proposition 4.1.8. *The map*

$$\mathcal{N}_\ell/(K_2^\times)^\ell \longrightarrow \operatorname{Prin}(K_2)/\ell \operatorname{Prin}(K_2)$$

(*induced from the divisor map*) *is injective, and its image is the group*

$$\mathcal{J}_\ell = \left\{(\beta) + \ell \operatorname{Prin}(K_2) \in \operatorname{Prin}(K_2)/\ell \operatorname{Prin}(K_2) : \mathrm{N}_{K_2/K_0}((\beta)) \in \ell \operatorname{Prin}(K_0)\right\}.$$

Proof. Let $(\mathcal{N}_\ell)$ be the group of divisors of elements in $\mathcal{N}_\ell$. First we claim that the sequence

$$1 \longrightarrow (k_2^\times)^\ell \longrightarrow \mathcal{N}_\ell \longrightarrow (\mathcal{N}_\ell) \longrightarrow 0$$

is exact. To see this, note that the map sending an element of $\mathcal{N}_\ell$ to its divisor is clearly surjective. The kernel of this map is the set $\mathcal{N}_\ell \cap k_2^\times$.

When K_2/K_0 is a geometric extension, let $c \in k_2^\times$ and suppose $\mathrm{N}_{K_2/K_0}(c) \in (K_0^\times)^\ell$. Then $\mathrm{N}_{K_2/K_0}(c) = c\tau(c) = c^2 \in (K_0^\times)^\ell$. As squaring is an isomorphism of $k_2^\times/(k_2^\times)^\ell$,

we have $c \in (k_2^\times)^\ell$.

When K_2/K_0 is a constant extension, let $c \in k_2^\times = \mathbb{F}_{q^2}^\times$, and suppose $\mathrm{N}_{K_2/K_0}(c) \in (K_0^\times)^\ell$. Then $\mathrm{N}_{K_2/K_0}(c) = c\tau(c) = c^{q+1} \in (K_0^\times)^\ell$. However, $c^{q+1} = c^{q-1}c^2$. Now, as $\ell \mid q-1$ and squaring is an isomorphism of $k_2^\times/(k_2^\times)^\ell$, we have $c \in (k_2^\times)^\ell$.

It follows from the exact sequence above that the divisor map

$$\mathcal{N}_\ell/(K_2^\times)^\ell \longrightarrow \mathrm{Prin}(K_2)/\ell\,\mathrm{Prin}(K_2)$$

is injective. Its image is certainly contained in $\mathcal{J}_\ell$. To complete the proof, we must show that every element of $\mathcal{J}_\ell$ lies in the image of $\mathcal{N}_\ell/(K_2^\times)^\ell$.

Let $(\beta) + \ell\,\mathrm{Prin}(K_2)$ be an element of $\mathcal{J}_\ell$, where $\beta \in K_2^\times$ satisfies $\mathrm{N}_{K_2/K_0}((\beta)) \in \ell\,\mathrm{Prin}(K_0)$; say $\mathrm{N}_{K_2/K_0}((\beta)) = \ell(\kappa)$ for some $\kappa \in K_0^\times$. Then $\mathrm{N}_{K_2/K_0}(\beta) = c\kappa^\ell$ for some $c \in k_2^\times$. If we let $d = c^{(\ell-1)/2}$, then $\mathrm{N}_{K_2/K_0}(d\beta) = (c\kappa)^\ell$, so $d\beta$ is an element of $\mathcal{N}_\ell$ whose image in $\mathrm{Prin}(K_2)/\ell\,\mathrm{Prin}(K_2)$ is $(\beta) + \ell\,\mathrm{Prin}(K_2)$. □

Proposition 4.1.9. *Via the bottom row of Figure 2.1, the image of* $\mathrm{Pic}^0(K_2)[\ell]$ *in* $\mathrm{Prin}(K_2)/\ell\,\mathrm{Prin}(K_2)$ *is contained in* $\mathcal{J}_\ell$.

Proof. Suppose $D' \in \mathrm{Div}^0(K_2)$ represents an element of $\mathrm{Pic}^0(K_2)[\ell]$, so that $\ell D'$ is a principal divisor, say equal to (α) for some $\alpha \in K_2^\times$. Then the divisor of $\mathrm{N}_{K_2/K_0}(\alpha)$ is also ℓ-multiple of a principal divisor. □

Let $\mathcal{U}_\ell$ be the image of $\mathcal{N}_\ell/(K_2^\times)^\ell$ when included in $\mathcal{I}_\ell$ via the bottom row of Figure 4.1, so that

$$\mathcal{U}_\ell = \{(\alpha) + \mathrm{Prin}(K_2) \cap \ell\,\mathrm{Div}^0(K_2) : \alpha \in \mathcal{N}_\ell\}.$$

Corollary 4.1.10. *The bottom row of the diagram in Figure 4.1 gives rise to an*

exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(K_2)[\ell] \longrightarrow \mathcal{N}_\ell/(K_2^\times)^\ell \longrightarrow \mathcal{U}_\ell \longrightarrow 0,$$

which splits (noncanonically).

Proof. The sequence is obtained from combining the exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(K_2)[\ell] \longrightarrow \mathcal{J}_\ell \longrightarrow \mathcal{U}_\ell \longrightarrow 0$$

of subgroups of the bottom row of Figure 4.1 with the isomorphism $\mathcal{N}_\ell/(K_2^\times)^\ell \cong \mathcal{J}_\ell$. The sequence splits because all of the groups are ℓ-torsion. □

Notice that Corollary 4.1.10 does not assume the presence of roots of ℓ-th roots of unity in k_0 or k_2; the decomposition it presents is valid regardless. This observation will become useful in the next chapter.

4.1.3 The Number of $\mathcal{D}_\ell$ Function Fields

We now prove the main result of this section, Theorem 4.1.12, which provides a count for the number of nonconjugate degree ℓ dihedral extensions K_ℓ of K_0 with fixed discriminant divisor $\Delta(K_\ell/K_0) = \Delta$ and quadratic resolvent field K_2 when $\zeta_\ell \in k_0$. Thus for the remainder of this chapter we will assume that $\zeta_\ell \in k_0$.

We first prove a correspondence arising from Corollary 4.1.10. Hence, for the remainder of this chapter we also make Assumption COEFF.

Theorem 4.1.11. *Let K_2/k_2 be a quadratic extension of K_0/k_0 such that $\zeta_\ell \in k_0$. Then there is a one-to-one correspondence between Kummer extensions $K_{2\ell}/K_2$ such that $K_{2\ell}$ is Galois over K_0 with Galois group $\mathcal{D}_\ell$ and the set of nontrivial cyclic subgroups of* $\mathrm{Pic}^0(K_2)[\ell] \times \mathcal{U}_\ell$.

This decomposition is the foundation of our method for counting and constructing $\mathcal{D}_\ell$ function fields with a fixed discriminant divisor and quadratic resolvent.

Let $M_0 \in \mathrm{Div}(K_0)$ be a squarefree effective divisor. Set $N_0 = |\mathrm{Supp}(M_0)|$, and suppose that that every place $P_i \in \mathrm{Supp}(M_0)$, $1 \le i \le N_0$, splits in K_2 as $P_i = P_i' + \tau(P_i')$ with $P_i' \neq \tau(P_i')$. We then define a set $Q_\ell(M_0)$ of formal sums by

$$Q_\ell(M_0) = \left\{ \sum_{i=1}^{N_0} n_i(P_i' - \tau(P_i')) : n_i \in (\mathbb{Z}/\ell\mathbb{Z})^* \right\}.$$

We can view $Q_\ell(M_0)$ as a subset of the group

$$\mathcal{Q}_\ell(M_0) = \sum_{i=1}^{N_0} (\mathbb{Z}/\ell\mathbb{Z})(P_i' - \tau(P_i'));$$

note that the natural map $\mathrm{Div}^0(K_2) \to \mathrm{Pic}^0(K_2)$ reduces to a homomorphism

$$\Psi\colon \mathcal{Q}_\ell(M_0) \longrightarrow \mathrm{Pic}^0(K_2)/\ell\,\mathrm{Pic}^0(K_2). \tag{4.6}$$

We set

$$T_\ell(M_0) = \{E' \in Q_\ell(M_0) : \Psi(E') = 0\}. \tag{4.7}$$

Theorem 4.1.12. *Let K_2/k_2 be a quadratic function field over K_0/k_0 of characteristic not dividing 2ℓ, with discriminant divisor $\Delta(K_2/K_0)$, such that k_0 contains the ℓ-th roots of unity. Let r denote the ℓ-rank of $\mathrm{Pic}^0(K_2)$, and let M_0 be a divisor of K_0 that is either zero or a sum of distinct places of K_0 supported away from $\Delta(K_2/K_0)$. Let $\Delta = \frac{\ell-1}{2}\Delta(K_2/K_0) + (\ell-1)M_0$.*

1. *If $M_0 = 0$, then the number of nonconjugate dihedral degree ℓ function fields*

K_ℓ with discriminant divisor $\Delta(K_\ell/K_0) = \Delta$ and quadratic resolvent field K_2 is $(\ell^r - 1)/(\ell - 1)$.

2. *If $M_0 \neq 0$ and some $P \in \mathrm{Supp}(M_0)$ is inert in K_2/K_0, then there are no dihedral degree ℓ function fields K_ℓ with discriminant divisor $\Delta(K_\ell/K_0) = \Delta$ and quadratic resolvent field K_2.*
3. *Suppose $M_0 \neq 0$ and that all $P_i \in \mathrm{Supp}(M_0)$ split in K_2 as $P_i = P_i' + \tau(P')$ with $P_i' \neq \tau(P_i')$. Then the number of nonconjugate dihedral degree ℓ function fields with discriminant divisor $\Delta(K_\ell/K_0) = \Delta$ and quadratic resolvent field K_2 is $|T_\ell(M_0)|\ell^r/(\ell - 1)$, where $T_\ell(M_0)$ is defined by equation (4.7).*

Proof. Let U_{ℓ,M_0} denote the subset of $\mathcal{U}_\ell$ consisting of those classes

$$(\alpha) + \mathrm{Prin}(K_2) \cap \ell\,\mathrm{Div}^0(K_2)$$

such that the reduced ramification divisor of α is equal to M_0. Note that U_{ℓ,M_0} is closed under multiplication by nonzero elements of $\mathbb{Z}/\ell\mathbb{Z}$.

Using the correspondence of Theorem 4.1.11, the conjugacy classes of dihedral degree ℓ function fields with discriminant divisor $\Delta(K_\ell/K_0) = \Delta$ and quadratic resolvent field K_2 are in one-to-one correspondence with the number of nontrivial cyclic subgroups of $\mathrm{Pic}^0(K_2)[\ell] \times \mathcal{U}_\ell$ that can be generated by elements (A, B) with $B \in U_{\ell,M_0}$.

If $M_0 = 0$, then U_{ℓ,M_0} consists only of the identity, so $B = 0$ and A can be any nonzero class in $\mathrm{Pic}^0(K_2)[\ell]$. There are $\ell^r - 1$ such pairs, and they generate $(\ell^r - 1)/(\ell - 1)$ different cyclic subgroups.

If $M_0 \neq 0$, then $|U_{\ell,M_0}| = |T_\ell(M_0)|$. This is because an element α of $\mathcal{N}_\ell$ gives rise

to an element of U_{ℓ,M_0} if and only if its divisor is of the form E' (up to multiples of ℓ) for some E' in $T_\ell(M_0)$. Thus, there are $|T_\ell(M_0)|\ell^r$ pairs (A, B) in $(\mathrm{Pic}^0(K_2))[\ell] \times \mathcal{U}_\ell$ with $B \in U_{\ell,M_0}$, and there are $|T_\ell(M_0)|\ell^r/(\ell-1)$ cyclic subgroups generated by such pairs. □

Notice that the proof of the theorem is constructive. This proof will form the basis of our Kummer theoretic construction technique. Before formalizing this algorithm, we present an efficient method for constructing minimal polynomial for K_ℓ in terms of α. This method is due to Everett Howe [42].

4.1.4 Defining equations

In this section, we will write down explicit defining equations for $\mathcal{D}_\ell$ extensions of K_0 constructed as above.

Definition 4.1.13. Given an integer $n > 0$ and an element κ of K, let $C_{n,\kappa}$ be the polynomial

$$C_{n,\kappa}(X) = \sum_{r=0}^{\lfloor n/2 \rfloor} (-\kappa)^r \frac{n}{n-r} \binom{n-r}{r} X^{n-2r}$$

in $K[X]$. (Note that the coefficient $\frac{n}{n-r}\binom{n-r}{r}$ is in fact an integer, so the definition makes sense in positive characteristic; see [35, Sequence A082985].)

The polynomials $C_{n,\kappa}$ are scaled versions of the Chebyshev polynomials of the first kind, and it follows that if α_1 and α_2 are elements of a field extension K' of K that satisfy $\alpha_1\alpha_2 = \kappa$, then

$$C_{n,\kappa}(\alpha_1 + \alpha_2) = \alpha_1^n + \alpha_2^n.$$

Proposition 4.1.14. *Let ℓ be an odd prime, and let K_2/k_2 be a quadratic extension of K_0/k_0 where $\zeta_\ell \in k_0$. Let α be an element of $K_2 \setminus K_2^\ell$ such that $\mathrm{N}_{K_2/K_0}(\alpha) = \kappa^\ell$*

for some $\kappa \in K_0$, and let $K_{2\ell}$ be the Kummer extension $K_2(\sqrt[\ell]{\alpha})$, so that $K_{2\ell}/K_0$ is Galois with group $\mathcal{D}_\ell$. Then the roots in $K_{2\ell}$ of the polynomial

$$C_{\ell,\kappa}(X) - \mathrm{Tr}_{K_2/K_0}(\alpha)$$

are generators for the index 2 subfields of $K_{2\ell}/K_0$.

Proof. Let θ be a root of $T^\ell - \alpha$ where $\mathrm{N}_{K_2/K_0}(\alpha) = \kappa^\ell$, let σ be a generator of $\mathrm{Gal}(K_{2\ell}/K_2)$, and let τ be an element of $\mathrm{Gal}(K_{2\ell}/K_0)$ that restricts to the nontrivial element of $\mathrm{Gal}(K_2/K_0)$. Then $\tau(\theta)$ and κ/θ are both roots of $T^\ell - \tau(\alpha)$, so there exists an integer i where $\tau' = \sigma^i\tau$ such that $\tau'(\theta) = \kappa/\theta$. Thus, $\theta+\kappa/\theta$ lies in the fixed field of τ' (but does not lie in K_0, for otherwise θ would lie in a quadratic extension of K_0).

It follows that

$$C_{\ell,\kappa}(\theta + \kappa/\theta) = \theta^\ell + (\kappa/\theta)^\ell = \alpha + \tau(\alpha) = \mathrm{Tr}_{K_2/K_0}(\alpha),$$

so one of the roots of $C_{\ell,\kappa}(X) - \mathrm{Tr}_{K_2/K_0}(\alpha)$ generates an index 2 subfield of $K_{2\ell}/K_0$. Since all of these index 2 subfields are conjugate to one another, the other roots of the polynomial generate the other fields. □

4.2 Construction Algorithms

As mentioned, the correspondence of Theorem 4.1.11 can be made explicit, and the proof of Theorem 4.1.12 is constructive; this leads naturally to Algorithm 4.1 below. This algorithm takes as input a quadratic function field K_2 and an effective squarefree

divisor M_0 of K_0, and outputs all nonconjugate degree ℓ dihedral function fields with discriminant divisor $\frac{\ell-1}{2}\Delta(K_2/K_0)+(\ell-1)M_0$ and quadratic resolvent field K_2. Note that K_2 may be the unique degree 2 constant field extension of K_0 when $K_0 = \mathbb{F}_q(x)$, in which case $\Delta(K_2/K_0) = 0$.

Algorithm 4.1 is precisely the construction in the proof of Theorem 4.1.12, and thus computes all elements α such that $K_2(\sqrt[\ell]{\alpha})$ is a Galois dihedral function field. Notice that in Step 14 and Step 20, $\mathrm{N}_{K_2/K_0}(\beta)$ and $\mathrm{N}_{K_2/K_0}(\eta_i)$ can be written as a constant $c \in k_0$ times an ℓ-th power $\kappa^\ell \in K_0$ as in the proof of Proposition 4.1.8, and the resulting redefinitions for β and η_i are elements of $\mathcal{N}_\ell$.

Remarks 4.2.1. There are several ways to perform Algorithm 4.1 more efficiently.

1. The generators $[B_1], \ldots, [B_r]$ of $(\mathrm{Pic}^0(K_2))[\ell]$ in step 2 can be computed from a set of generators $[A_1], \ldots, [A_h]$ of $\mathrm{Pic}^0(K_2)$ chosen so that the order m_i of $[A_i]$ is equal to the i-th invariant factor of the group $\mathrm{Pic}^0(K_2)$. Using the $[A_i]$, it is also easy to check whether an element E' of $Q_\ell(M_0)$ is in the kernel of the map Ψ, and, if so, to obtain an element $\beta \in K_2^\times$ such that $(\beta) - E' \in \ell\,\mathrm{Div}^0(K_2)$, as is required in step 13. We do this as follows: suppose D' is a lift of E' to the degree 0 divisor group of K_2. Write $[D'] = d_1[A_1] + \cdots + d_h[A_h]$. Then E' is in the kernel of Ψ if and only if ℓ divides d_i whenever m_i is divisible by ℓ. If this is the case, set $e_i = d_i/\ell$ when $\ell \mid m_i$ and $e_i \equiv d_i\ell^{-1} \bmod m_i$ when $\ell \nmid m_i$. Then $D' - \ell(e_1A_1 + \cdots e_hA_h)$ is principal, and we can compute $\beta \in K_2^\times$ with this divisor; this is the desired β.

2. When K_2 has positive genus, it is the function field of an elliptic or hyperelliptic curve $y^2 = f(x)$. One could potentially take advantage of faster arithmetic available for the Jacobians of hyperelliptic curves, instead of the slower generic

Algorithm 4.1 (Constructing $\mathcal{D}_\ell$ function fields when $\zeta_\ell \in k_0$)

Input: A quadratic extension K_2/k_2 of K_0/k_0 under Assumption COEFF, an odd prime ℓ, and a squarefree effective divisor M_0 of K_0 coprime to $\Delta(K_2/K_0)$.

Output: The set L_2 of defining equations for all the dihedral extension K_ℓ of K_0 with $\Delta(K_\ell/K_2) = \frac{\ell-1}{2}\Delta(K_2/K_0) + (\ell-1)M_0$ and quadratic resolvent K_2.

[Compute fundamental information.]
Compute a minimal set of generators $\{[B_1], \ldots, [B_r]\}$ of $\mathrm{Pic}^0(K_2)[\ell]$.
Initialize the set L to be empty; eventually, L will contain the pairs of points of K_2 lying over the support of M_0.
for $P \in \mathrm{Supp}(M_0)$ **do**
  Ensure $P = P_0' + P_1'$ in $\mathrm{Div}(K_2)$; upon failure, return the empty set.
  $L \leftarrow L \cup \{(P_0', P_1')\}$.
Use L to compute the set $Q_\ell(M_0)$.
[Compute functions in $\mathcal{N}_\ell$ representing elements of $Q_\ell(M_0)$ that map into $\mathcal{U}_\ell$.]
Initialize the set I to be empty; eventually, I will contain lifts to $\mathcal{N}_\ell$ of all elements of $Q_\ell(M_0)$ (up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$) that can be lifted to $\mathcal{N}_\ell$.
for $E' \in Q_\ell(M_0)$ up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ **do**
  if $\Psi(E') = 0$, where Ψ is from (4.6) **then**
    Compute $F' \in \mathrm{Div}^0(K_2)$ such that $E' - \ell F' \in \mathrm{Prin}(K_2)$.
    Find $\beta \in K_2^\times$ such that $(\beta) = E' - \ell F'$.
    Compute $\mathrm{N}_{K_2/K_0}(\beta) = c\kappa^\ell$ for some $\kappa \in K_0$ and $c \in k_0$.
    Set $\beta \leftarrow c^{\frac{\ell-1}{2}}\beta$ and $I \leftarrow I \cup \{\beta\}$.
[Compute virtual units in $\mathcal{N}_\ell$.]
Initialize the set V to be empty; eventually V will contain elements of $\mathcal{N}_\ell \cap \mathcal{V}_\ell$ whose images in $\mathcal{V}_\ell/(K_2^\times)^\ell$ form a basis for that group.
for $[B_i]$ in the basis of $\mathrm{Pic}^0(K_2)[\ell]$ computed earlier **do**
  Find $\eta_i \in K_2$ such that $(\eta_i) = \ell B_i$.
  Compute $\mathrm{N}_{K_2/K_0}(\eta_i) = c\kappa^\ell$ for some $\kappa \in K_0$ and $c \in k_0$.
  Set $\eta_i \leftarrow c^{\frac{\ell-1}{2}}\eta_i$ and $V \leftarrow V \cup \{\eta_i\}$.
[Create defining equations.]
Initialize the output set L_2 to be empty.
if $M_0 = 0$ **then**
  for nonzero $(z_i) \in (\mathbb{Z}/\ell\mathbb{Z})^r$ up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ **do**
    Compute $\alpha = \prod_i^r \eta_i^{z_i}$ and $\kappa \in K_0$ with $\kappa^\ell = \mathrm{N}_{K_2/K_0}(\alpha)$.
    Let $C(T) = C_{\ell,\kappa}(T) - \mathrm{Tr}_{K_2/K_0}(\alpha)$, as in Proposition 4.1.14.
    $L_2 \leftarrow L_2 \cup \{C(T)\}$.
else
  for $\beta \in I$ **do**
    for $(z_i) \in (\mathbb{Z}/\ell\mathbb{Z})^{\#V}$ **do**
      Compute $\alpha = \beta \prod_{\kappa_i \in V} \eta_i^{z_i}$ and $\kappa \in K_0$ with $\kappa^\ell = \mathrm{N}_{K_2/K_0}(\alpha)$.
      Let $C(T) = C_{\ell,\kappa}(T) - \mathrm{Tr}_{K_2/K_0}(\alpha)$, as in Proposition 4.1.14.
      $L_2 \leftarrow L_2 \cup \{C(T)\}$.
return L_2

arithmetic in $\mathrm{Pic}^0(K_2)$. For example, Magma supports such arithmetic using Mumford representations when k_2 is a finite field, provided the infinite place of K_0 is not inert in K_2. Instead of computing in $\mathrm{Pic}^0(K_2)$, one could compute with Mumford representations and map all calculations to and from the Jacobian $\mathrm{Jac}(K_2)$. Mapping the classes of divisors in $Q_\ell(M_0)$ of step 12 into $\mathrm{Jac}(K_2)$ can also be done quite efficiently, as we know the support of all $E' \in Q_\ell(M_0)$. For example, if the infinite place P_∞ of K is ramified in K_2, say $P_\infty = 2P'_\infty$, then we can rewrite E' as

$$E' = \sum_{P' \in \mathrm{Supp}(E')} n_{P'}(P' - \deg(P')P'_\infty).$$

In our algorithm E' is supported away from P'_∞; thus, all $P' \in \mathrm{Supp}(E')$ are finite. Finding the Mumford representation $J_{P'}$ of $P' - \deg(P')P'_\infty$ is simple, and one could use the faster Jacobian arithmetic to compute $\sum_{P' \in \mathrm{Supp}(E')} n_{P'} J_{P'}$ efficiently.

3. When k_0 is a number field, the largest implementation hurdle to overcome is computing $\mathrm{Pic}^0(K_2)$. Computing this group is notoriously difficult; typically much more intensive than when k_0 is a finite field. In Magma limited functionality exists to do this. Further, when K_2 has genus one, this is equivalent to finding the group of rational points on an elliptic curve. This group could potentially have a large non-torsion subgroup, making this computation completely infeasible. However, in many cases the algorithm can still be implemented as shown in Example 4.2.4

4. Once elements η_i are found in step 19, it is useful to spend a moment finding

a 'smaller' generator of the cyclic subgroup generated by $\eta_i K_2^\times/(K_2^\times)^\ell$ so that the defining equations $\{C(T)\}$ have reasonable coefficients. One suggestion is to replace η_i by an integral ℓ-th power free representative; similarly for the elements β in step 13. This is demonstrated in Example 4.2.2. We note that in our implementation we choose from a set of representatives the one whose norm has the smallest degree to insure the coefficients of the polynomials $\{C(T)\}$ are of reasonable size.

Example 4.2.2. In this example we perform Algorithm 4.1 for the case $\ell = 3$ and $M_0 = 0$. Consider the rational function field $K_0 = \mathbb{F}_7(x)$. Let K_2 be the quadratic function field defined by $y^2 = x(x+3)(x+1)$. Then

$$\mathrm{Pic}^0(K_2) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Hence, $\mathrm{Pic}^0(K_2)[3] = \mathbb{Z}/3\mathbb{Z}$, and is generated by the class of the divisor of

$$B_1 = 2\langle x+5, y+3\rangle - 2\langle x, y\rangle.$$

Consequently, $3B_1$ is principal and it is the divisor of the function

$$\eta_1 = \frac{(x+3)(x+5)^6}{x^3(y+x^2+6x+2)^2}.$$

At this point it is beneficial to find a 'smaller' representative of the cyclic group generated by $\eta_1 K_2^\times/(K_2^\times)^3$. One choice is setting

$$\eta_1 = (x+3)(y+x^2+6x+2).$$

Then $\mathrm{N}_{K_2/K_0}(\eta_1) = (x+3)^3(x+5)^3$ and $\mathrm{Tr}_{K_2/K_0}(\eta_1) = 2(x+3)^3$. Thus, we set $\alpha = \eta_1$ and compute the defining equation of K_3 as

$$C_{3,(x+3)(x+5)}(T) - \mathrm{Tr}_{K_2/K_0}(\eta_1) = T^3 + 4(x+3)(x+5)T - 2(x+3)^3,$$

using Proposition 4.1.14. One can check that the discriminant divisor of K_3 is indeed $\Delta(K_2/K_0)$.

Example 4.2.3. In this example we perform Algorithm 4.1 for the case $\ell = 3$ and $M_0 = \langle x+3\rangle + \langle x+5\rangle$ and K_2 is as in Example 4.2.2. First we notice that both $\langle x+3\rangle$ and $\langle x+5\rangle$ split in K_2. Now, with η_1 from Example 4.2.2, we find the set I described in step 9 of Algorithm 4.1. First, we compute $Q_\ell(M_0) = \{E_1', E_2'\}$ where

$$E_1' = \langle x+5, y+3\rangle + \langle x+4, y+3\rangle - \langle x+5, y+4\rangle - \langle x+4, y+4\rangle,$$
$$E_2' = \langle x+5, y+3\rangle + \langle x+4, y+4\rangle - \langle x+5, y+4\rangle - \langle x+4, y+3\rangle.$$

Next, we find that $[E_1'] \notin 3\,\mathrm{Pic}(K_0)$ and hence $\Psi(E_1') \neq 0$. However, $\Psi([E_2']) = 0$. In fact, E_2' is principal. So, we find $(\beta) = E_2' + 3[0]$ where

$$\beta = \frac{(x+4)(x+5)}{y + 3x^2 + 5x + 3}.$$

Now, $\mathrm{N}_{K_2/K_0}(\beta) = 4 \notin \mathcal{N}_\ell$; thus, we set β to be $4^{(3-1)/2}\beta = 4\beta \in \mathcal{N}_\ell$. Consequently, we find 3 nonisomorphic dihedral function fields $K_{3,0}$, $K_{3,1}$, and $K_{3,2}$ corresponding to

β, $\beta\eta$, and $\beta\eta^2$, respectively. Using Proposition 4.1.14, we compute the polynomials

$$\begin{aligned} C_0 =& T^3 + 4T + \frac{2x^2+x+2}{(x+4)(x+5)}, \\ C_1 =& T^3 + 4(x+3)(x+5)T + \frac{(x+3)^2(x+5)(x+6)}{x+1}, \\ C_2 =& T^3 + 4(x+3)^2(x+5)^2T + \frac{2(x+3)^3(x+5)(x^3+x^2+6x+5)}{x+4}, \end{aligned}$$

which define $K_{3,0}$, $K_{3,1}$, and $K_{3,2}$, respectively. Each of these fields does indeed have discriminant divisor $\Delta(K_2/K_0) + 2M_0$.

Example 4.2.4. In this example we demonstrate the case that k_0 has characteristic zero. Let k_0 be $\mathbb{Q}(\zeta_5)$ and $\ell = 5$. Consider the quadratic extension K_2/k_0 given by $y^2 = x^3 + x^2 + 2$. Then one can check that $\mathrm{Pic}^0(K_2)[5] = 0$. Let $M_0 = \langle x^3 + 2 \rangle$. Then M_0 splits in K_2 into the two places

$$P_1' = \langle x^3 + 2, y - x \rangle \quad \text{and} \quad P_2' = \langle x^3 + 2, y + x \rangle.$$

Consider the divisor $E' = P_1' - P_2'$. Then $E' \in \ell\,\mathrm{Pic}^0(K_2)$ as it is principal; it is equal to the divisor of

$$\beta = \frac{-2xy + x^3 + 2x^2 + 2}{x^3 + 2}.$$

Now, $\mathrm{N}_{K_2/K_0}(\beta) = 1 \in \mathcal{N}_\ell$, and so using Proposition 4.1.14, we compute a defining polynomial for K_5 as

$$C(T) := T^5 - 5T^3 + 5T - \frac{2x^3 + 4x^2 + 4}{x^3 + 2} \in \mathbb{Q}(\zeta_5)[T].$$

Then K_5 is dihedral with discriminant divisor $2(\Delta(K_2/K_0) + 2M_0)$.

Our next algorithm (Algorithm 4.2) takes as input a pair of effective squarefree divisors D and M_0 of K_0 with disjoint support and uses Algorithm 4.1 to generate all nonconjugate degree ℓ dihedral function fields K_ℓ with discriminant divisor $\frac{\ell-1}{2}D + (\ell-1)M_0$. Recall that if $D = 0$, then the quadratic resolvent field K_2 is the unique quadratic constant field extension of $K_0 = \mathbb{F}_q(x)$ which we denote as $\tilde{K}_0$ as before. If D is nonzero, then there are two quadratic function function fields K_2 and $\widehat{K}_2$ of discriminant divisor D; they are in fact twists of one another. Now, any place $P \notin \mathrm{Supp}(D)$ splits in K_2 if and only if it is inert in K_2', and vice versa. Thus, if M_0 is nonzero, only one of K_2 and K_2' needs to be considered in the construction of K_ℓ.

Example 4.2.5. Returning to Examples 4.2.2, and 4.2.3 we find the following:

1. On input $\Delta(K_2/K_0)$ from Example 4.2.2, $M_0 = 0$, and $\ell = 3$, the output of Algorithm 4.2 is the single field K_3 found in Example 4.2.2, as $\widehat{K}_2$ has no nontrivial 3-torsion.

2. On input $\Delta(K_2/K_0)$ from Example 4.2.3, $M_0 = \langle x+3\rangle + \langle x+5\rangle$, and $\ell = 3$, the output of Algorithm 4.2 are the fields $K_{3,0}, K_{3,1}$, and $K_{3,2}$ found in Example 4.2.3 as the places of M_0 are not split in $\widehat{K}_2$.

In conclusion, under Assumption COEFF, and when k_0 contains the ℓ-th roots of unity, we have developed an effective method to count and construct all degree ℓ dihedral function fields of a given discriminant divisor. Notice that this method – like the class field theoretic Algorithm 3.1 – requires the computation of a class group, which is a highly nontrivial task. However, the Kummer theoretic approach computes precisely the desired fields K_ℓ without extraneous conductor or discriminant calculations along the way; there are in fact no explicit calculations of discriminant divisors or conductors whatsoever in Algorithms 4.1 and 4.2. Moreover, using Proposition

Algorithm 4.2 (Constructing all $\mathcal{D}_\ell$ function fields from divisors)

Input: An odd prime ℓ and squarefree effective divisors D and M_0 of K_0 with disjoint support, were $D = 0$ only if $K_0 = \mathbb{F}_q(x)$.

Output: The set L of defining equations for all the degree ℓ dihedral extensions K_ℓ of K_0 with $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}D + (\ell-1)M_0$.

1: **if** $\deg(D)$ is even **then**
2: Construct a quadratic field K_2 with discriminant divisor D.
3: **else**
4: **return** "D IS NOT A QUADRATIC DISCRIMINANT DIVISOR".
5: **if** $D = 0$ **then**
6: Get L from Algorithm 4.1 with input K_2, ℓ, M_0.
7: **else**
8: Construct the quadratic twist $\widehat{K}_2$ of K_2.
9: **if** $M_0 \neq 0$ **then**
10: Pick $P \in \mathrm{Supp}(M_0)$.
11: **if** P is split in K_2 **then**
12: Get L from Algorithm 4.1 with input K_2, ℓ, M_0.
13: **else**
14: Get L from Algorithm 4.1 with input $\widehat{K}_2, \ell, M_0$.
15: **else**
16: Get L_1 from Algorithm 4.1 with input K_2, ℓ, M_0.
17: Get L_2 from Algorithm 4.1 with input $\widehat{K}_2, \ell, M_0$.
18: Set $L \leftarrow L_1 \cup L_2$.
19: **return** L.

4.1.14, we can compute defining equations for the fields K_ℓ in a more straight forward manner than possible with the class field theoretic approach.

The other main benefit of the Kummer theoretic approach is the formulation of the main theorem. Theorem 4.1.12 provides a concrete way to count all the degree ℓ dihedral function fields of a given discriminant divisor. From this result, Everett Howe [42] was able to prove an explicit formula for the number of degree ℓ dihedral function fields over $\mathbb{F}_q$, when $q \equiv 1 \bmod 2\ell$, whose discriminant divisors have degree $2(\ell-1)$. We will discuss this result further in chapter 6, as well as other potential

consequences of this theorem in chapters 6 and 7. In the next chapter, we describe how to use the Kummer theoretic methods above when k_0 does not contain a primitive ℓ-th root of unity.

Chapter 5

Kummer Theoretic Approach without ℓ-th Roots of Unity

The aim of this chapter is to present an algorithm to construct all dihedral function fields with a given discriminant divisor, when the constant field k_0 does not contain the ℓ-th roots of unity. As in the previous chapters we accomplish this by constructing cyclic degree ℓ extensions of a fixed quadratic field. Throughout this chapter, when k_0 is a finite field $\mathbb{F}_q$ of odd characteristic, we assume that $q \not\equiv 1 \bmod \ell$. As usual, we also assume throughout this chapter that k_0 is perfect and the characteristic of k_0 does not divide 2ℓ.

Throughout, let $\zeta_\ell \in \overline{k}_0$ be a primitive ℓ-th root of unity. For a function field K we let $\tilde{K}$ denote $K(\zeta_\ell)$; the function field K with coefficients extended to $\tilde{k}$.

Generally speaking, to construct degree ℓ dihedral extensions when k_0 does not contain the ℓ-th roots of unity, we can adjoin the roots to k_0 and use the results of the last chapter to build the corresponding fields. However, in this chapter we will primarily focus on the case that $[k_0(\zeta_\ell) : k_0] = 2$. The reasons for this are two fold. First, restricting to this case affords us the opportunity to investigate this situation in greater detail. This in turn allows us to develop specialized – and consequently very efficient – algorithms for this case. Second, when $\ell = 3$, this is

sufficient to construct (and later tabulate when $k_0 = \mathbb{F}_q(x)$) all non-Galois cubic function fields with prescribed discriminant divisor when $\mathrm{char}(k_0) \nmid 2\ell$. Explicit asymptotic estimates for the number of $\mathcal{D}_\ell$ fields are only known for the case of $\ell = 3$ and k_0 a finite field. Consequently this is the most interesting situation for tabulation purposes.

As explained in the last chapter, when $K_2 = K_0(\zeta_\ell)$ we are again eventually forced to restrict ourselves to the case that k_0 is a finite field. A more detailed explanation for this is presented in the following section.

5.1 Construction with Quadratic Resolvent $K_2 = K_0(\zeta_\ell)$

Let k_i denote the constant field of K_i. Throughout this section we will assume that $[k_0(\zeta_\ell) : k_0] = 2$ and focus on the case that $K_2 = K_0(\zeta_\ell)$, i.e. when $k_2 = k_0(\zeta_\ell)$. When k_0 is a finite field $\mathbb{F}_q$, we are thus assuming that $q \equiv -1 \bmod \ell$.

Before discussion dihedral extensions, we present the following theorem about the ramification in constant field extensions:

Theorem 5.1.1 ([37] Thm 3.6.3, 3.9.1)**.** *$\tilde{K}/K$ is an unramified extension. Moreover,*

$$\Delta(\tilde{K}'/\tilde{K}) = \mathrm{Con}_{\tilde{K}/K}(\Delta(K'/K)).$$

To apply Kummer theory to the situation when $[k_0(\zeta_\ell) : k_0] = 2$ and $K_2 = K_0(\zeta_\ell)$, we present the following theorem:

Theorem 5.1.2. *Let K/k be a function field such that $[k(\zeta_\ell) : k] = 2$. Let $K' = K(\zeta_\ell)$ be a quadratic extension of K and let ϱ be the nontrivial element of $\mathrm{Gal}(K(\zeta_\ell)/K)$. Let K'' be a degree ℓ cyclic extension of K'. By Theorem 4.1.1, $K'' = K'(\theta)$ where θ*

is a root of $T^\ell - \alpha$ *for some* $\alpha \in K'^\times/(K'^\times)^\ell$. *Then,*

1. K''/K *is Galois if and only if* $\varrho(\alpha)(K'^\times)^\ell = \alpha^{\pm 1}(K'^\times)^\ell$.
2. *Further,* $\mathrm{Gal}(K''/K)$ *is nonabelian (and thus dihedral) if* $\varrho(\alpha)(K'^\times)^\ell = \alpha(K'^\times)^\ell$, *and* $\mathrm{Gal}(K''/K)$ *is abelian if* $\varrho(\alpha)(K'^\times)^\ell = \alpha^{-1}(K'^\times)^\ell$.

To prove this theorem will make use of the following lemma:

Lemma 5.1.3. *If* $[K(\zeta_\ell) : K] = 2$, *and* ϱ *is a generator of* $\mathrm{Gal}(K(\zeta_\ell)/K)$, *then* $\varrho(\zeta_\ell) = \zeta_\ell^{-1}$.

Proof. As ζ_ℓ is a root of $X^\ell - 1$, and this equation is fixed by ϱ, we have $\varrho(\zeta_\ell) = \zeta_\ell^j$ for some $1 \leq j < \ell$. Applying ϱ again to this equation we see that $\zeta_\ell = \varrho^2(\zeta_\ell) = \varrho(\zeta_\ell^j)$, and thus $1 = \zeta_\ell^{j^2-1}$. Hence, $j^2 \equiv 1 \bmod \ell$. But as ϱ is the nontrivial automorphism of $\mathrm{Gal}(K(\zeta_\ell)/K)$, $j \neq 1$, and the results follows. □

We now prove Theorem 5.1.2.

Proof. We prove the statements of Theorem 5.1.2 sequentially.

1. Assume that $K'(\theta)/K$ is Galois. Then $K'(\theta) = K'(\varrho(\theta))$. So by Theorem 4.1.1 there exists an $1 \leq j < \ell$ and an element $\kappa \in K'$ such that $\varrho(\alpha) = \alpha^j \kappa^\ell$. Applying ϱ to this equation we obtain that

$$\alpha = \varrho^2(\alpha) = \varrho(\alpha^j \kappa^\ell) = \varrho(\alpha)^j \varrho(\kappa)^\ell = \alpha^{j^2} \kappa^\ell \varrho(\kappa)^\ell,$$

   Therefore, $(\kappa\varrho(\kappa))^{-\ell} = \alpha^{j^2-1}$ and thus α^{j^2-1} is an ℓ-th power. However, as α is not an ℓ-th power in K', it must be the case that $j^2 = 1 \bmod \ell$. Thus $\varrho(\alpha)(K'^\times)^\ell = \alpha^{\pm 1}(K'^\times)^\ell$.

   Conversely, suppose $\varrho(\alpha)(K'^\times)^\ell = \alpha^{\pm 1}(K'^\times)^\ell$. Abusing notation, let ϱ also

denote a lift of ϱ to $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ of order 2, where K^{sep} is a separable closure of K. To show that $K'(\theta)/K$ is Galois it suffices to show that $K'(\varrho(\theta)) = K'(\theta)$. To this end, notice that $\varrho(\theta)^\ell = \alpha^{\pm 1}\kappa^\ell$ for some $\kappa \in K'$ and thus $\varrho(\theta) = \zeta^j\theta^{\pm 1}\kappa$ for some $1 \leq j \leq \ell$. Therefore, $K' \subsetneq K'(\varrho(\theta)) \subseteq K'(\theta)$. However, as $[K'(\theta) : K']$ is prime, $K'(\varrho(\theta)) = K'(\theta)$ and consequently $K'(\theta)/K$ is Galois.

2. Without loss of generality, let $\sigma \in \mathrm{Gal}(K''/K')$ be such that $\sigma(\theta) = \zeta_\ell\theta$. Suppose that $\varrho(\alpha) = \alpha\kappa^\ell$ for some $\kappa \in K'$. Then $\varrho(\theta)^\ell = \varrho(\alpha) = \alpha\kappa^\ell$, and so $\varrho(\theta) = \zeta_\ell^i\theta\kappa$ for some $1 \leq i < \ell$. Consequently, by Lemma 5.1.3,

$$\varrho(\sigma(\theta)) = \varrho(\zeta_\ell\theta) = \zeta_\ell^{i-1}\theta\kappa.$$
$$\sigma(\varrho(\theta)) = \sigma(\zeta_\ell^i\theta\kappa)) = \zeta_\ell^{i+1}\theta\kappa.$$

Since $i + 1 \not\equiv i - 1 \bmod \ell$, $\mathrm{Gal}(K''/K')$ is not abelian.

Now, suppose that $\varrho(\alpha) = \alpha^{-1}\kappa^\ell$ for some $\kappa \in K'$. Then $\varrho(\theta)^\ell = \varrho(\alpha) = \alpha^{-1}\kappa^\ell$, and so $\varrho(\theta) = \zeta_\ell^i\theta^{-1}\kappa$ for some $1 \leq i < \ell$. Thus, by Lemma 5.1.3,

$$\varrho(\sigma(\theta)) = \varrho(\zeta_\ell\theta) = \zeta_\ell^{i-1}\theta^{-1}\kappa.$$
$$\sigma(\varrho(\theta)) = \sigma(\zeta^i\theta^{-1}\kappa) = \zeta_\ell^{i-1}\theta^{-1}\kappa.$$

Hence, $\mathrm{Gal}(K''/K)$ is abelian in this case.

□

Setting $K = K_0$ in the above theorem, we see that there is a one-to-one correspondence between $\mathcal{D}_\ell$ extensions K_ℓ with quadratic resolvent $K_2 = K_0(\zeta_\ell)$ and the nontrivial cyclic subgroups of $K_0^\times/(K_0^\times)^\ell$. This can be seen as follows: given a

dihedral function field $K_{2\ell} = K_2(\sqrt[\ell]{\alpha})$, it is straight forward to compute a defining equation for $K_\ell = \mathrm{Fix}(\varrho)$. Indeed, as $\varrho(\alpha) = \alpha$ we see that K_ℓ is defined by $T^\ell - \alpha$.

Given a representative $\alpha(K_0^\times)^\ell \in K_0^\times/(K_0^\times)^\ell$ such that $K_{2\ell} = K_2(\sqrt[\ell]{\alpha})$, we have $\Delta(K_{2\ell}/K_2) = (\ell-1)M_0'$ where M_0' is the ramification divisor of α. As $\Delta(K_2/K_0) = 0$, by Theorem 2.3.2 and Proposition 3.2.3, $\Delta(K_\ell/K_0) = (\ell-1)M_0$ where $2M_0 = \mathrm{N}_{K_2/K_0}(\Delta(K_{2\ell}/K_0)) = \mathrm{N}_{K_2/K_0}(M_0')$. Hence M_0 is the reduced ramification divisor of α. Thus, degree ℓ dihedral fields with a given discriminant divisor $\Delta(K_\ell/K_0) = (\ell-1)M_0$ and quadratic resolvent $K_2 = K_0(\zeta_\ell)$, correspond precisely to the cyclic subgroups of $K_0^\times/(K_0^\times)^\ell$ generated by elements $\alpha(K_0^\times)^\ell$ such that the reduced ramification divisor of α is M_0.

For ease of exposition, we define the *support* of a coset

$$D + \ell\,\mathrm{Div}^0(K) \in \mathrm{Div}^0(K)/\ell\,\mathrm{Div}^0(K)$$

to be the set of places $P \in \mathrm{Supp}(D)$ such that $\ell \nmid v_P(D)$. Hence, an element $\alpha \in K_0$ has reduced ramification divisor M_0 if and only if $(\alpha) + \ell\,\mathrm{Div}^0(K_0) \in \mathrm{Div}^0(K_0)/\ell\,\mathrm{Div}^0(K_0)$ has support M_0.

Remark 5.1.4. Recall, our combined aim of this chapter and the last is to construct all dihedral degree ℓ function fields with quadratic resolvent K_2 and given discriminant divisor Δ, when $\zeta_\ell \in K_2$. Further recall from Remark 4.1.7, in order to construct all dihedral function fields with a fixed discriminant divisor, we must be in a situation where there are only finitely many appropriate elements α with a fixed ramification divisor. When this is the case, our approach, like that of the last chapter, is to construct such elements α from their divisors.

Analogous to Remark 4.1.7, in this last chapter we have shown in Theorem 5.1.2 that the appropriate elements α are the representatives of the group $K_0^\times/(K_0^\times)^\ell$. Thus, analogous to Proposition 4.1.8, we have the following exact sequence:

$$1 \longrightarrow k_0^\times/(k_0^\times)^\ell \longrightarrow K_0^\times/(K_0^\times)^\ell \longrightarrow \mathrm{Prin}(K_0)/\ell\,\mathrm{Prin}(K_0) \longrightarrow 0. \tag{5.1}$$

Again, in order to construct all the representatives of $K_0/(K_0^\times)^\ell$ with a given ramification divisor, we require the group $k_0^\times/(k_0^\times)^\ell$ to be finite. When $k_0 = \mathbb{Q}$ and $k_2 = \mathbb{Q}(\zeta_3)$ for example, the group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$ contains all appropriate elements α that result in non-Galois cubic extensions of $\mathbb{Q}$ with quadratic resolvent $\mathbb{Q}(\zeta_3)$. There are infinitely many of these fields [13], all of which will have trivial discriminant divisor. For this reason, we must restrict to the situation when k_0 is a finite field $\mathbb{F}_q$. In this case, we see that not only is $k_0^\times/(k_0^\times)^\ell$ finite, it is also in fact trivial.

For the remainder of this subsection we make Assumption COEFF. Hence, we assume that $k_0 = \mathbb{F}_q$ where $q \equiv -1 \bmod 2\ell$ and $k_2 = \mathbb{F}_{q^2}$.

Proceeding analogously to Subsection 4.1.3, we define a set $\tilde{Q}_\ell(M_0)$ of formal sums by

$$\tilde{Q}_\ell(M_0) = \left\{ \sum_{P \in \mathrm{Supp}(M_0)} n_i P : n_i \in (\mathbb{Z}/\ell\mathbb{Z})^* \text{ and } \sum_{P \in \mathrm{Supp}(M_0)} n_i \deg(P_i) \equiv 0 \bmod \ell \right\}.$$

Proposition 5.1.5. *There is a one-to-one correspondence between the set $\tilde{Q}_\ell(M_0)$ and the cosets $\alpha(K_0^\times)^\ell \in K_0^\times/(K_0^\times)^\ell$ such that the reduced ramification divisor of α is M_0.*

Proof. Suppose $\alpha(K_0^\times)^\ell \in K_0^\times/(K_0^\times)^\ell$ is such that α has reduced ramification divisor

M_0. Then by definition $(\alpha) + \mathrm{Div}^0(K_2) \in \mathrm{Div}^0(K_2)/\ell\,\mathrm{Div}^0(K_2)$ has support M_0. Now, as K_0 is rational, $\mathrm{Div}^0(K_0) = \mathrm{Prin}(K_0)$, and by (4.5), $\mathrm{Prin}^0(K_2)/\ell\,\mathrm{Prin}^0(K_2)$ is isomorphic to $K_0^\times/(K_0^\times)^\ell$. Therefore, via this isomorphism, for any divisor $D \in \mathrm{Div}^0(K_0)/\ell\,\mathrm{Div}^0(K_0)$ supported at M_0, there exists a unique coset $\alpha(K_0^\times)^\ell$ such that $(\alpha) + \ell\,\mathrm{Div}^0(K_0) = D + \ell\,\mathrm{Div}^0(K_0)$.

From the above, we now only need to show that there is a bijection between $\tilde{Q}_\ell(M_0)$ and the subset of $\mathrm{Div}^0(K_2)/\ell\,\mathrm{Div}^0(K_2)$ supported at M_0. To that end, we can view $\tilde{Q}_\ell(M_0)$ as a subset of the group

$$\tilde{\mathcal{Q}}_\ell(M_0) = \sum_{P \in \mathrm{Supp}(M_0)} (\mathbb{Z}/\ell\mathbb{Z})P.$$

Let P_∞ denote the infinite place of K_0 and define the map $\tilde{\Psi}\colon \tilde{\mathcal{Q}}_\ell(M_0) \to \mathrm{Div}^0(K_0)$ by $\tilde{\Psi}(E) = E - \deg(E)P_\infty$. Recall that $\deg(P_\infty) = 1$ and thus the image of $\tilde{\Psi}$ does indeed have degree 0. Notice that $\tilde{\Psi}$ reduces to a homomorphism

$$\tilde{\Psi}\colon \tilde{\mathcal{Q}}_\ell(M_0) \longrightarrow \mathrm{Div}^0(K_0)/\ell\,\mathrm{Div}^0(K_0). \tag{5.2}$$

Thus, it suffices to show that $\tilde{\Psi}$ restricts to a bijection between $\tilde{Q}_\ell(M_0)$ and the subset of the group $\mathrm{Div}^0(K_0)/\ell\,\mathrm{Div}^0(K_0)$ supported at M_0. To that end, we notice that $\tilde{\Psi}$ is clearly injective. To show surjectivity, we note that by the division algorithm, every divisor $D \in \mathrm{Div}^0(K_0)$ supported at M_0 can be written as

$$D = \sum_{P_i \in \mathrm{Supp}(M_0)} z_i P_i - \ell E,$$

for some $1 \le z_i < \ell$, and some divisor $E \in \mathrm{Div}(K_0)$. Moreover, as $\deg(D) = 0$, we see

that $\sum z_i \deg(P_i) \equiv 0 \mod \ell$. Thus, the subset of $\mathrm{Div}^0(K_0)/\ell\,\mathrm{Div}^0(K_0)$ supported at M_0 is precisely the image of $\tilde{Q}_\ell(M_0)$ under $\tilde{\Psi}$. □

Via the proof of Proposition 5.1.5, when $K_0 = \mathbb{F}_q(x)$ with $q \equiv -1 \bmod 2\ell$, we now have a method to construct all dihedral function fields with discriminant divisor $\Delta(K_\ell/K_0) = (\ell-1)M_0$. This is presented in Algorithm 5.1.

Algorithm 5.1 (Constructing $\mathcal{D}_\ell$ function fields with quadratic resolvent field $K_2 = K_0(\zeta_\ell)$ when $K_0 = \mathbb{F}_q(x)$ and $q \equiv -1 \bmod 2\ell$.)

Input: An odd prime ℓ, and a squarefree effective nontrivial divisor M_0 of K_0.
Output: The set L of defining equation for all the dihedral extension K_ℓ of K_0 with $\Delta(K_\ell/K_0) = (\ell-1)(M_0)$ and $K_2 = K_0(\zeta_\ell) = \mathbb{F}_{q^2}(x)$

1: Initialize the output set L to be empty.
2: **if** $M_0 = 0$ **then**
3: **return** L;
4: Write $M_0 = \sum_{i=1}^{r} P_i \in \mathrm{Div}(K_2)$.
5: Set P_∞ to be the infinite place of K_0.
6: [Compute all possible K_ℓ.]
7: **for** $(z_i) \in ((\mathbb{Z}/\ell\mathbb{Z})^*)^r$ up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ such that $\sum_{i=1}^{r} z_i \deg(P_i) \equiv 0 \bmod \ell$ **do**
8: Compute $\alpha \in K_0$ such that $(\alpha) = \sum_{i=1}^{r} z_i\,(P_i - \deg(P_i)P_\infty)$.
9: Let $C(T) = T^\ell - \alpha$.
10: $L \leftarrow L \cup \{C(T)\}$.
11: **return** L

Example 5.1.6. Let $K_0 = \mathbb{F}_{13}(x)$. In this example we construct all degree 7 dihedral function fields with discriminant divisor $\Delta(K_\ell/K_0) = 6M_0$ where $M_0 = \langle x+1\rangle + \langle x+2\rangle + \langle x+3\rangle$. There are 5 elements of $\tilde{Q}_\ell(M_0)$ up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$, namely

the divisors

$$\langle x+1\rangle + \langle x+2\rangle + 5\langle x+3\rangle,$$
$$\langle x+1\rangle + 2\langle x+2\rangle + 4\langle x+3\rangle,$$
$$\langle x+1\rangle + 3\langle x+2\rangle + 3\langle x+3\rangle,$$
$$\langle x+1\rangle + 4\langle x+2\rangle + 2\langle x+3\rangle,$$
$$\langle x+1\rangle + 5\langle x+2\rangle + \langle x+3\rangle.$$

These correspond to 5 dihedral fields with defining polynomials

$$T^7 - (x+1)(x+2)(x+3)^5,$$
$$T^7 - (x+1)(x+2)^2(x+3)^4,$$
$$T^7 - (x+1)(x+2)^3(x+3)^3,$$
$$T^7 - (x+1)(x+2)^4(x+3)^2,$$
$$T^7 - (x+1)(x+2)^5(x+3).$$

5.2 Construction with Quadratic Resolvent K_2 when K_2/K_0 is geometric

In order to construct degree ℓ dihedral extensions with quadratic resolvent field K_2/k_2 when k_2 does not contain the ℓ-th roots of unity, we can adjoin the roots to k_2 and use the results of the last chapter to build the corresponding fields over $K_0(\zeta)$, and compute a fixed field to obtain a dihedral extension of K_0. For the reasons discussed at the beginning of last chapter, in this section we will assume that K_2/K_0 is a

geometric extension, i.e. that $k_2 = k_0$. Under this assumption, we will present a general Kummer theoretic algorithm for this case. The shortcomings of this general algorithm will further motivate the restriction to the case when $[k_0(\zeta_\ell) : k_0] = 2$. In Section 5.3 we will make that restriction and refine this general algorithm, resulting in a much faster Kummer theoretic method for constructing dihedral function fields.

Recall that $\tilde{k}/k$ is a cyclic Galois extension and hence so is $\tilde{K}/K$. Throughout, let ϱ denote a generator of $\mathrm{Gal}(\tilde{K}/K)$ that restricts to a generator of $\tilde{k}/k$. Now, if a geometric extension K'/K is Galois then so is $\tilde{K}'/\tilde{K}$ and $\mathrm{Gal}(\tilde{K}'/\tilde{K}) \cong \mathrm{Gal}(K'/K)$. Furthermore, we have the following proposition:

Proposition 5.2.1. *With the notation above, let K'/K be a Galois extension of function fields such that $K' \cap \tilde{K} = K$. Then $\tilde{K}'/K$ is Galois and*

$$\mathrm{Gal}(\tilde{K}'/K) \cong \mathrm{Gal}(K'/K) \times \mathrm{Gal}(\tilde{k}/k).$$

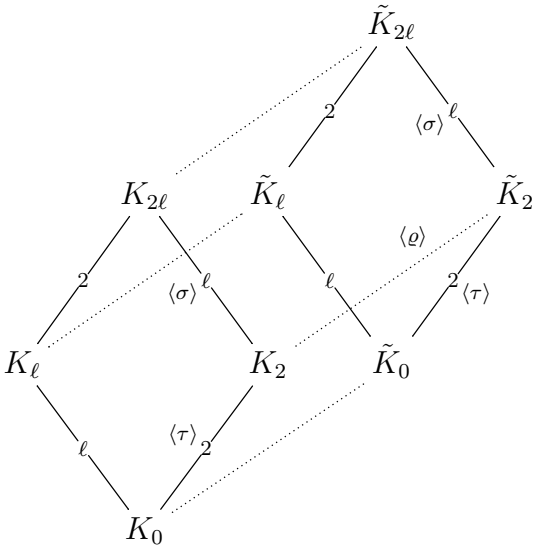
Alternatively, if $\tilde{K}'/K$ is Galois and $\mathrm{Gal}(k'/k)$ is a normal subgroup of $\mathrm{Gal}(\tilde{K}'/K)$ then K'/K is Galois.

Proof. The first statement follows directly from Proposition 14.21 of [17] since the intersection $\tilde{K} \cap K' = K$. The second statement follows directly from Theorem 2.2.3. □

Now, when K_2/K_0 is geometric, we consider the diagram of fields given in Figure 5.1 that depicts the diagram of fields in Figure 2.1 and their constant field extensions when adjoining ζ_ℓ.

Here, $K_{2\ell}/K_0$ is a dihedral Galois extension with quadratic resolvent K_2 which is a geometric extension of K_0. Consequently, $\tilde{K_{2\ell}}/\tilde{K_0}$ is a dihedral Galois extension as

Figure 5.1: Adjoining ℓ-th roots of unity to the diagram of a dihedral extension of function fields.



well. We abuse notation by letting σ and τ denote the generators of $\mathrm{Gal}(\tilde{K_{2\ell}}/\tilde{K}_0)$ that restrict to the generators $\sigma, \tau \in \mathrm{Gal}(K_{2\ell}, K_0)$, respectively.

As $\tilde{K}_0$ contains a primitive ℓ-th root of unity, we can apply Algorithm 4.1 to construct all fields $\tilde{K}_\ell/\tilde{K}_0$ with prescribed ramification. Then, if $\tilde{K}_{2\ell}/K_0$ is Galois with Galois group $\mathcal{D}_\ell \times \langle\varrho\rangle$, we can take the fix field of ϱ to obtain all dihedral fields K_ℓ/K_0 with the same ramification and correct quadratic resolvent. Moreover, by Proposition 5.2.1, all dihedral extensions K_ℓ/K_0 can be constructed in such a manner. This is made precise in Algorithm 5.2.

Notice that the resulting function fields K_ℓ do indeed have discriminant divisor $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}(\Delta(K_2/K_0) + M)$ by Theorem 5.1.1.

This method is quite inefficient. One needs to compute the Galois group for each field $K_{2\ell}$ and potentially a fixed field for each of these afterwards. In fact, when k_0

Algorithm 5.2 (Constructing $\mathcal{D}_\ell$ function fields from their quadratic resolvents without specific roots of unity.)

Input: A quadratic geometric extension K_2 of K_0, an odd prime ℓ, and a squarefree effective divisor M_0 of K_0 with support disjoint from that of $\Delta(K_2/K_0)$.

Output: The set L of all the dihedral extension K_ℓ of K_0 with $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}(\Delta(K_2/K_0) + 2M_0)$ and quadratic resolvent K_2.

1: [Compute all possible K_ℓ.]
2: Obtain the sets I, V from steps $8-21$ of Algorithm 4.1 with input $(\tilde{K}_2/\tilde{K}_0, M', \ell)$ where $M' = \mathrm{Con}_{\tilde{K}_2/K_0}(M_0)$.
3: Initialize the output set L to be empty.
4: **if** $M = 0$ **then**
5: **for** nonzero $(z_i) \in (\mathbb{Z}/\ell\mathbb{Z})^r$ up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ **do**
6: Compute $\alpha = \prod_{i=1}^r \eta_i^{z_i}$ and $\tilde{K}_{2\ell} = \tilde{K}_2(\sqrt[\ell]{\alpha})$
7: **if** $\tilde{K}_{2\ell}/K_0$ is Galois and $\mathrm{Gal}(\tilde{K}_{2\ell}/K_0) \cong \mathcal{D}_\ell \times \langle\varrho\rangle$ **then**
8: Compute $K_\ell = \mathrm{Fix}(\langle\tau\rangle \times \langle\varrho\rangle)$.
9: $L \leftarrow L \cup \{K_\ell\}$.
10: **else**
11: **for** $\beta \in T$ **do**
12: **for** $(z_i) \in (\mathbb{Z}/\ell\mathbb{Z})^{\#V}$ **do**
13: Compute $\alpha = \beta \prod_{\kappa_i \in V} \eta_i^{z_i}$ and $\tilde{K}_{2\ell} = \tilde{K}_2(\sqrt[\ell]{\alpha})$
14: **if** $\tilde{K}_{2\ell}/K_0$ is Galois and $\mathrm{Gal}(\tilde{K}_{2\ell}/K_0) \cong \mathcal{D}_\ell \times \langle\varrho\rangle$ **then**
15: Compute $K_\ell = \mathrm{Fix}(\langle\tau\rangle \times \langle\varrho\rangle)$.
16: $L \leftarrow L \cup \{K_\ell\}$.
17: **return** L

is a finite field, one would probably be better served using the class field theoretic approach of Algorithm 3.2. To improve this algorithm, one would prefer to only compute the elements α such that $\mathrm{Gal}(\tilde{K}_2(\sqrt[\ell]{\alpha})/K_0) \cong \mathcal{D}_\ell \times \langle\varrho\rangle$, without having to check for the correct Galois group afterwards. The aim of the next section is to develop this idea for the simplest nontrivial case, namely when $\tilde{K}_0/K_0$ is a quadratic extension different from K_2. This requirement may seem rather restrictive; however, when $\ell = 3$, this will allow us to efficiently compute non-Galois cubic fields over any perfect field with characteristic not dividing 2ℓ.

5.3 Construction when K_2/K_0 is geometric and $[k_0(\zeta_\ell) : k_0] = 2$

As mentioned, to produce an efficient Kummer theoretic method for constructing dihedral fields, one would like to only compute the elements $\alpha \in \tilde{K}_2$ such that $\mathrm{Gal}(\tilde{K}_2(\sqrt[\ell]{\alpha})/K_0) \cong \mathcal{D}_\ell \times \langle \varrho \rangle$. In this section, we will achieve this when $\tilde{k}_2/k_2$ is a quadratic extension. Thus, throughout this section we will assume that $[k_0(\zeta_\ell) : k_0] = [k_2(\zeta_\ell) : k_2] = 2$, and thus $K_2 \cap K_0(\zeta_\ell) = K_0$. Moreover, for the reasons previously discussed, we will assume that K_2/K_0 is geometric. Recall, the case when $K_2 = K_0(\zeta_\ell)$ was covered in Section 5.1, and so we exclude this case from consideration in this section.

To begin, consider the diagram of fields in Figure 5.2, which corresponds to Figure 5.1 to the case under consideration in this section. Here, we let $\widehat{K}_2$ denote the *twist* of K_2, i.e. the other geometric subfield of $\tilde{K}_2/K_0$ different from K_2. Notice that $\widehat{K}_2$ is the subfield of $\tilde{K}_2$ fixed by $\langle \varrho\tau \rangle = \langle \tau\varrho \rangle$.

As mentioned, the goal of this section is to precisely determine the elements $\alpha \in \tilde{K}_2$ such that $\mathrm{Gal}(\tilde{K}_2(\sqrt[\ell]{\alpha})/K_0) \cong \mathcal{D}_\ell \times \langle \varrho \rangle$. For any field extension K'/K, let

$$\mathcal{N}_\ell(K'/K) = \left\{ \alpha \in K'^\times \setminus K^\times : \mathrm{N}_{K'/K}(\alpha) \in (K^\times)^\ell \right\}.$$

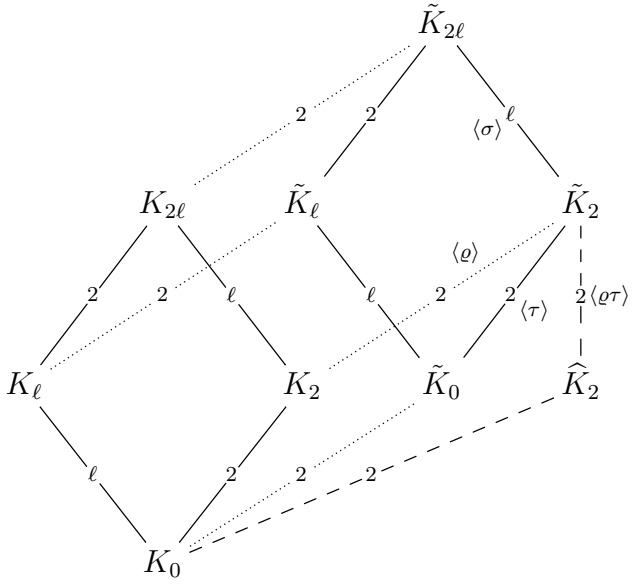
Then, we have the following theorem:

Theorem 5.3.1. *The inclusion*

$$\Phi \colon \mathcal{N}_\ell(\widehat{K}_2/K_0)/(\widehat{K}_2^\times)^\ell \to \mathcal{N}_\ell(\tilde{K}_2/\tilde{K}_0)/(\tilde{K}_2^\times)^\ell$$

is onto the subset of $\alpha(\tilde{K}_2^\times)^\ell \in \mathcal{N}_\ell(\tilde{K}_2/\tilde{K}_0)/(\tilde{K}_2^\times)^\ell$ *such that* $\tilde{K}_2(\sqrt[\ell]{\alpha})/K_0$ *is Galois*

Figure 5.2: Adjoining ℓ-th roots of unity to the diagram of a dihedral extension of function fields when $[K_2(\zeta_\ell) : K_2] = 2$.



with $\mathrm{Gal}(\tilde{K}_2(\sqrt[\ell]{\alpha})/K_0) \cong \mathcal{D}_\ell \times \langle\varrho\rangle$.

Proof. Let $\alpha \in \mathcal{N}_\ell(\tilde{K}_2/\tilde{K}_0)$. First we show that $\alpha(\tilde{K}_2^\times)^\ell$ is in the image of Φ if and only if $\varrho\tau(\alpha)(\tilde{K}_2^\times)^\ell = \alpha(\tilde{K}_2^\times)^\ell$. As $\widehat{K}_2$ is the fixed field of $\varrho\tau$ in $\tilde{K}_2$, $\varrho\tau(\alpha)(\tilde{K}_2^\times)^\ell = \alpha(\tilde{K}_2^\times)^\ell$ if α is the image of Φ. Conversely, suppose $\varrho\tau(\beta)(\tilde{K}_2^\times)^\ell = \beta(\tilde{K}_2^\times)^\ell$ for some $\beta \in \mathcal{N}_\ell(\tilde{K}_2/K_0)$. Then $\varrho\tau(\beta) = \beta\kappa^\ell$ for some $\kappa \in \tilde{K}_2$. Setting $\alpha = \beta/\varrho\tau(\kappa^\ell)$, we find that $\varrho\tau(\alpha) = \alpha$. Now, $\alpha \in \mathcal{N}_\ell(\widehat{K}_2/K_0)$ if and only if $\mathrm{N}_{\widehat{K}_2/K_0}(\alpha) = \kappa_0^\ell$ for some $\kappa_0 \in K_0$. By definition $\mathrm{N}_{\tilde{K}_2/\tilde{K}_0}(\alpha) = \tau(\alpha)\alpha$. However, the restriction of τ to $\widehat{K}_2$ is the nontrivial Galois automorphism of $\widehat{K}_2/K_0$, and thus $\mathrm{N}_{\tilde{K}_2/\tilde{K}_0}(\alpha) \in K_0$. Moreover, as $\alpha \in \mathcal{N}_\ell(\tilde{K}_2/\tilde{K}_0)$, its norm is an ℓ-th power, and thus there exists an element $\kappa_0 \in K_0$ such that $\mathrm{N}_{\tilde{K}_2/\tilde{K}_0}(\alpha) = \mathrm{N}_{\widehat{K}_2/K_0}(\alpha) = \kappa_0^\ell$. Therefore, $\alpha(\tilde{K}_2^\times)^\ell$ is in the image of Φ if and only if $\varrho\tau(\alpha)(\tilde{K}_2^\times)^\ell = \alpha(\tilde{K}_2^\times)^\ell$.

Let $\alpha(\tilde{K}_2^\times)^\ell \in \mathcal{N}_\ell(\tilde{K}_2/\tilde{K}_0)/(\tilde{K}_2^\times)^\ell$ and let θ be a root of $X^\ell - \alpha$. We write $\tilde{K}_{2\ell} = \tilde{K}_2(\theta) = \tilde{K}_2(\sqrt[\ell]{\alpha})$. Now, consider the diagram of fields in Figure 5.2. Without loss of generality, we assume that $\sigma(\theta) = \zeta\theta$.

By Proposition 4.1.2, for all $\alpha(\tilde{K}_2^\times)^\ell \in \mathcal{N}_\ell(\tilde{K}_2/\tilde{K}_0)/(\tilde{K}_2^\times)^\ell$, the extension $\tilde{K}_2(\theta)/\tilde{K}_0$ is Galois and $\mathrm{Gal}(\tilde{K}_2(\theta)/\tilde{K}_0) \cong \mathcal{D}_\ell$. It remains to show that $\tilde{K}_2(\theta)/K_0$ is Galois with Galois group $\mathrm{Gal}(\tilde{K}_2(\theta)/K_0) \cong \mathcal{D}_\ell \times \langle\varrho\rangle$ if and only if $\alpha(\tilde{K}_2^\times)^\ell$ is in the image of $\mathcal{N}_\ell(\widehat{K}_2/K_0)/(\widehat{K}_2^\times)^\ell$, i.e. if and only if $\varrho\tau(\alpha)(\tilde{K}_2^\times)^\ell = \alpha(\tilde{K}_2^\times)^\ell$.

Assume that $\tilde{K}_{2\ell}/K_0$ is Galois with Galois group $\mathrm{Gal}(\tilde{K}_{2\ell}/K_0) \cong \mathcal{D}_\ell \times \langle\varrho\rangle$. Then, by Proposition 4.1.2 there exits an element $\kappa \in \tilde{K}_0$ such that $\alpha\tau(\alpha) = \kappa^\ell$. Hence, $\tau(\alpha) = \alpha^{-1}\kappa^\ell$.

From the assumption that $\tilde{K}_{2\ell}/K_0$ is Galois with Galois group isomorphic to $\mathcal{D}_\ell \times \langle\varrho\rangle$ we see that $\tilde{K}_{2\ell}/K_2$ is Galois and abelian. Therefore, applying Theorem 5.1.2 with $K = K_2$, $K' = \tilde{K}_2$, and $K'' = \tilde{K}_{2\ell}$ we obtain $\varrho(\alpha)(\tilde{K}_2^\times)^\ell = \alpha^{-1}(\tilde{K}_2^\times)^\ell$. Finally,

$$\tau(\varrho(\alpha))(\tilde{K}_2^\times)^\ell = \tau(\alpha^{-1})(\tilde{K}_2^\times)^\ell = \alpha(\tilde{K}_2^\times)^\ell,$$

and therefore, $\alpha(\tilde{K}_2^\times)^\ell$ is in the image of $\mathcal{N}_\ell(\widehat{K}_2/K_0)/(\widehat{K}_2^\times)^\ell$.

Conversely, suppose that $\tilde{K}_{2\ell} = \tilde{K}_2(\theta) = \tilde{K}_2(\sqrt[\ell]{\alpha})$ where $\alpha \in \mathcal{N}_\ell(\widehat{K}_2/K_0)$. To show that $\tilde{K}_2(\theta)/K_0$ is Galois it suffices to show that $\tilde{K}_2(\varrho(\theta)) = \tilde{K}_2(\theta)$, as $\tilde{K}_2/K_0$ is Galois by Proposition 5.2.1. To this end, by Theorem 5.1.2 $\varrho(\alpha) = \alpha^{-1}\kappa^\ell$ and thus $\varrho(\theta) = \zeta^j\theta^{-1}\kappa$ for some $1 \leq j \leq \ell$. Therefore, $\tilde{K}_2(\theta) = \tilde{K}_2(\varrho(\theta))$, and consequently $\tilde{K}_2(\theta)/K_0$ is Galois. Moreover, applying Theorem 5.1.2 with $K = K_2$, $K' = \tilde{K}_2$, and $K'' = \tilde{K}_{2\ell}$, we obtain that ϱ and σ commute. □

Corollary 5.3.2. *Let K_2 be a quadratic geometric extension of K_0/k_0 such that*

$[k_0(\zeta_\ell) : k_0] = 2$. *Then there is a one-to-one correspondence between dihedral function fields* K_ℓ *with quadratic resolvent* K_2 *and the set of nontrivial cyclic subgroups of* $\mathcal{N}_\ell(\widehat{K}_2/K_0)/(\widehat{K}_2^\times)^\ell$.

Recall that the theory of ℓ-virtual units presented in Section 4.1.2 is independent of the presence of roots of unity in k_2. So let

$$\mathcal{U}_\ell(\widehat{K}_2) = \{(\alpha) + \mathrm{Prin}(\widehat{K}_2) \cap \ell \,\mathrm{Div}^0(\widehat{K}_2) : \alpha \in \mathcal{N}_\ell(\widehat{K}_2/K_0)\}.$$

Then we have the following corollary:

Corollary 5.3.3. *Let* K_2 *be a quadratic geometric extension of* K_0/k_0 *such that* $[k_0(\zeta_\ell) : k_0] = 2$. *Then there is a one-to-one correspondence between dihedral function fields* K_ℓ *with quadratic resolvent* K_2 *and the set of nontrivial cyclic subgroups of* $\mathrm{Pic}^0(\widehat{K}_2)[\ell] \times \mathcal{U}_\ell(\widehat{K}_2)$.

From the above corollary, we can obtain an exact count for the number of dihedral fields K_ℓ with quadratic resolvent K_2, by replacing K_2 with $\widehat{K}_2$ in Theorem 4.1.12. We spare the reader the nearly verbatim rewriting of Theorem 4.1.12 in this case. However, as the theorem is constructive, in the next section we will use it to produce an algorithm for constructing dihedral function fields with a given discriminant divisor.

5.4 Construction Algorithms when $[k_0(\zeta_\ell) : k_0] = 2$

In this section we present an algorithm for constructing all degree ℓ dihedral function fields with a given discriminant divisor $\Delta \in \mathrm{Div}(K_0/k_0)$, when $[k_0(\zeta_\ell) : k_0] = 2$. We first justify the use of Algorithm 4.1 to construct dihedral fields with given ramification

and a fixed quadratic resolvent $K_2 \neq K_0(\zeta_\ell)$, when $[k_0(\zeta_\ell) : k_0] = 2$. Then, under Assumption COEFF, we combine this with Algorithm 5.1 to produce an algorithm for constructing all dihedral fields of a given discriminant divisor when $[k_0(\zeta_\ell) : k_0] = 2$. Thus, throughout this section assume that $[k_0(\zeta_\ell) : k_0] = 2$.

When K_2/K_0 is geometric, by Corollary 5.3.3, the function fields $\tilde{K}_{2\ell}$ such that $K_{2\ell}/K_0$ is Galois with Galois group $\mathcal{D}_\ell$ correspond to cyclic subgroups of the group $\mathrm{Pic}^0(\widehat{K}_2)[\ell] \times \mathcal{U}_\ell(\widehat{K}_2)$. Let $\Delta = \frac{\ell-1}{2}\Delta(K_2/K_0) + (\ell-1)M_0$. Let $U_{\ell,M_0}(\widehat{K}_2)$ denote the subset of $\mathcal{U}_\ell(\widehat{K}_2)$ consisting of those classes

$$(\alpha) + \mathrm{Prin}(K_2) \cap \ell\,\mathrm{Div}^0(K_2)$$

such that the reduced ramification divisor of α is equal to M_0. Using the correspondence of Corollary 5.3.3, the conjugacy classes of dihedral degree ℓ function fields with discriminant divisor $\Delta(K_\ell/K_0) = \Delta$ and quadratic resolvent field K_2 are in one-to-one correspondence with the number of nontrivial cyclic subgroups of $\mathrm{Pic}^0(\widehat{K}_2)[\ell] \times \mathcal{U}_\ell(\widehat{K}_2)$ that can be generated by elements (A, B) with $B \in U_{\ell,M_0}(\widehat{K}_2)$. Notice that Algorithm 4.1 computes all such pairs on input $\widehat{K}_2, \ell, M_0$.

Via Φ we can embed the set $\mathcal{N}_\ell(\widehat{K}_2/K_0)/(\widehat{K}_2^\times)^\ell$ into $\mathcal{N}_\ell(\tilde{K}_2/\tilde{K}_0)/(\tilde{K}_2^\times)^\ell$. Then with $C_{\ell,\kappa}(T)$ as defined in Definition 4.1.13, Proposition 4.1.14 says that

$$C(T) = C_{\ell,\kappa}(T) - \mathrm{Tr}_{\widehat{K}_2/K_0}(\alpha) \in \tilde{K}_0[T]$$

is a defining polynomial of $\tilde{K}_\ell/\tilde{K}_0$. However, recall from the proof of Theorem 5.3.1 that if $\alpha(\widehat{K}_2^\times)^\ell \in \mathcal{N}_\ell(\widehat{K}_2/K_0)/(\widehat{K}_2^\times)^\ell$ then $\mathrm{N}_{\widehat{K}_2/K_0}(\alpha) = \kappa^\ell \in (K_0^\times)^\ell$. Moreover, as $\rho_{|\widehat{K}_2}$ is the nontrivial Galois automorphism of $\widehat{K}_2/K_0$, $\mathrm{Tr}_{\widehat{K}_2/K_0}(\alpha) = \mathrm{Tr}_{\tilde{K}_2/\tilde{K}_0}(\alpha)$.

Therefore, $C(T)$ is defined over K_0 and is thus invariant under ρ. Consequently, $C(T)$ is a defining equation for K_ℓ/K_0 as well.

All told, on input $\widehat{K}_2, \ell, M_0$, Algorithm 4.1 produces all dihedral fields K_ℓ such that $\Delta(K_\ell/K_0) = \Delta$ with quadratic resolvent field K_2 when K_2/K_0 is geometric. Combining this with Algorithm 5.1, we obtain Algorithm 5.3 (when $[k_0(\zeta_\ell) : k_0] = 2$ and under Assumption COEFF) which constructs all dihedral function fields K_ℓ/K_0 with quadratic resolvent field K_2 such that $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}D + (\ell-1)M_0$,

---

Algorithm 5.3 (Constructing all $\mathcal{D}_\ell$ function fields with quadratic resolvent field K_2 when $[k_0(\zeta_\ell) : k_0] = 2$)

Input: A quadratic extension K_2/k_2 of K_0/k_0 under Assumption COEFF, an odd prime ℓ, and a squarefree effective divisor M_0 of K_0 coprime to $\Delta(K_2/K_0)$.

Output: The set L of defining equations for all the degree ℓ dihedral extensions K_ℓ of K_0 with $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}D + (\ell-1)M_0$.

1: [Compute all possible K_ℓ.]
2: **if** $\Delta(K_2/K_0) = 0$ **then**
3: Get L from Algorithm 5.1 with input ℓ, M_0.
4: **else**
5: Get L from Algorithm 4.1 with input $\widehat{K}_2, \ell, M_0$.
6: **return** L.

Example 5.4.1. Consider the rational function field $\mathbb{F}_9(x)$ where $\mathbb{F}_9 = \mathbb{F}_3(\omega)$ and ω is a root of $T^2 - T - 1$. One can check that ω generates $\mathbb{F}_9^\times$. In this example, we will construct an degree 5 dihedral extension with $M_0 = 0$. Let K_2 and $\widehat{K}_2$ be defined by the equations

$$z^2 = \omega x(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4),$$
$$y^2 = x(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4),$$

respectively. To construct a dihedral extension with quadratic resolvent K_2 and discriminant divisor $2\Delta(K_2/K_0)$ we proceed as in Algorithm 4.1 with input $\widehat{K}_2, \ell = 5, M_0 = 0$. We find that

$$\mathrm{Pic}^0(\widehat{K}_2) \cong (\mathbb{Z}/2\mathbb{Z})^3 \oplus \mathbb{Z}/10\mathbb{Z},$$

and further that $\mathrm{Pic}^0(\widehat{K}_2)[5] = \langle [C'] \rangle$ where

$$[C'] = 2\langle x + \omega^5, y + \omega \rangle - 2\langle x, y \rangle.$$

Thus, $5C'$ is principal; it is the divisor of

$$\beta = \frac{(x+\omega^5)^{10}}{x^5\left((x^2+2x)y + \omega^5 x^5 + x^4 + \omega^6 x^3 + x^2 + \omega x + \omega^2\right)}.$$

We choose a 'smaller' representative of $\beta(\widehat{K}_2^{\times})^{\ell}$ by resetting β to be βx^5. Then

$$\begin{aligned} \mathrm{N}_{\widehat{K}_2/K_0}(\beta) &= (x-\omega)^{10}, \\ \mathrm{Tr}_{\widehat{K}_2/K_0}(\beta) &= \omega^7 x^5 + \omega^2 x^4 + x^3 + \omega^2 x^2 + \omega^3 x + 2. \end{aligned}$$

Therefore, using Proposition 4.1.14, we find the defining equation

$$T^5 - (x-\omega)^2 T^3 + (x-\omega)^4 T - \mathrm{Tr}_{\widehat{K}_2/K_0}(\beta)$$

for K_5/K_0. One can indeed verify that K_5/K_0 is dihedral with discriminant divisor $2\Delta(K_2/K_0)$.

Example 5.4.2. Consider the rational function field $\mathbb{Q}(x)$. In this example we will

construct a degree 3 dihedral extensions with $M_0 = 0$. Let K_2 and $\widehat{K}_2$ be defined by the equations

$$z^2 = -3(x^6 - 1) \quad \text{and} \quad y^2 = x^6 - 1$$

respectively. Notice that $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. Thus, to construct a dihedral extension with quadratic resolvent K_2 and discriminant divisor $\Delta(K_2/K_0)$ we proceed as in Algorithm 4.1 with input $\widehat{K}_2, \ell = 3, M_0 = 0$. First, we compute

$$\mathrm{Pic}^0(\widehat{K}_2) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z},$$

and further that $\mathrm{Pic}^0(\widehat{K}_2)[3] = \langle [C'] \rangle$ where

$$[C'] = 2\langle x - 1, y \rangle - 2\langle 1/x, y/x^3 + (x+1)/x \rangle.$$

Thus, $3C'$ is principal; it is the divisor of

$$\beta = (x-1)^3(y + x^3)^{-1}.$$

We choose a 'smaller' representative of the cyclic subgroup generated by $\beta(\widehat{K}_2^{\times})^3$ by resetting $\beta = y + x^3$. Then,

$$\mathrm{N}_{\widehat{K}_2/K_0}(\beta) = 1 \quad \text{and} \quad \mathrm{Tr}_{\widehat{K}_2/K_0}(\beta) = 2x^3.$$

Therefore, using Proposition 4.1.14, we find the defining equation $T^3 - 3T - 2x^3$ for K_3/K_0, and one can check that indeed K_3/K_0 is dihedral with discriminant divisor $\Delta(K_2/K_0)$.

Under Assumption COEFF, when $[k_0(\zeta_\ell) : k_0] = 2$, we now combine Algorithms 5.1 and 4.1 to create an algorithm that outputs all dihedral degree ℓ function fields with a given discriminant divisor. This is presented in Algorithm 5.4.

Algorithm 5.4 (Constructing all $\mathcal{D}_\ell$ function fields over K_0/k_0 from their divisors when $[k_0(\zeta_\ell) : k_0] = 2$

Input: An odd prime ℓ and squarefree effective divisors D and M_0 of K_0 with disjoint support, where $K_0 = \mathbb{F}_q(x)$ when $D = 0$.

Output: The set L of defining equations for all the degree ℓ dihedral extensions K_ℓ of K_0 with $\Delta(K_\ell/K_0) = \frac{\ell-1}{2}D + (\ell-1)M_0$.

1: **if** $\deg(D)$ is even **then**
2: Construct a quadratic field K_2 with discriminant divisor D.
3: **else**
4: **return** "D IS NOT A QUADRATIC DISCRIMINANT DIVISOR".
5: **if** $D = 0$ **then**
6: Get L from Algorithm 5.1 with input ℓ, M_0.
7: **else**
8: Construct the quadratic twist $\widehat{K}_2$ of K_2.
9: **if** $M_0 \neq 0$ **then**
10: Pick $P \in \mathrm{Supp}(M_0)$.
11: **if** P splits in K_2 **then**
12: Get L from Algorithm 4.1 with input $\widehat{K}_2, \ell, M_0$.
13: **else**
14: Get L from Algorithm 4.1 with input K_2, ℓ, M_0.
15: **else**
16: Get L_1 from Algorithm 4.1 with input K_2, ℓ, M_0.
17: Get L_2 from Algorithm 4.1 with input $\widehat{K}_2, \ell, M_0$.
18: Set $L \leftarrow L_1 \cup L_2$.
19: **return** L.

Example 5.4.3. Returning to Examples 5.1.6, and 5.4.2 we find the following:

1. On input $D = 0$ and $M_0 = \langle x+1\rangle + \langle x+2\rangle + \langle x+3\rangle$ as in from Example 5.1.6, the output of Algorithm 4.2 is the five fields K_5 found in Example 5.1.6.
2. On input $\Delta(K_2/K_0)$ from Example 5.4.2, $M_0 = 0$, and $\ell = 3$, the output

of Algorithm 4.2 is the field K_3 found in Example 5.4.2 as $\mathrm{Pic}^0(\widehat{K}_2)$ has no nontrivial 3-torsion.

So using the algorithms of the last chapter we are now able to construct dihedral function fields with prescribed ramification when $[k_2(\zeta_\ell) : k_2] = 2$. Notice that this allows us to produce complete tables of cubic fields when k is a finite field of characteristic greater than 3. We will explore this further in the next chapter.

Chapter 6

Numerical Results and Tabulation Techniques

In this chapter, we present a method to efficiently tabulate all degree ℓ dihedral function fields whose discriminant divisors have degree up to a given bound B when k_0 is a finite field $\mathbb{F}_q$ and q is coprime to 2ℓ. Instead of simply iterating one of the construction methods of the previous chapters, we are able to exact improvements from using the automorphism group of the field K_0. After describing this improvement, we discuss the numerical results from this implementation when $q \equiv \pm 1 \mod 2\ell$. We will see that in all the instances we implemented, the Kummer theoretic approach performs better than the one using class field theory. Consequently, we use the Kummer theoretic approach in our tabulation algorithm to construct complete lists of dihedral fields up to various bounds B for several values of ℓ. These lists are then compared to relevant asymptotic formulas and explicit counting results.

The tabulation technique we will present is my own work and was first presented in [42] for the case that $q \equiv 1 \mod 2\ell$. In [42], we also compared the same tabulation results to the relevant asymptotics in this case. Theorem 6.2.3, which provides an explicit count for the number of degree ℓ dihedral function fields of the smallest degree bound when $q \equiv 1 \mod 2\ell$, was also originally presented in [42] and is due to Everett

Howe. However, we will extend that result to include the case when $q \equiv -1 \bmod 2\ell$.

Throughout this chapter k_0 with be a finite field $\mathbb{F}_q$ with odd characteristic different from ℓ.

6.1 Tabulation Method

Algorithms 4.1, 3.2, and 5.3 construct all degree ℓ dihedral function fields with a given discriminant divisor and fixed quadratic resolvent field; by iterating either of these algorithms, we obtain a procedure for tabulating all degree ℓ dihedral function fields whose discriminant divisor has degree up to some fixed input bound $B \geq 0$. However, in this context, we can use the automorphism group of K_0 to significantly reduce the number of quadratic function fields that need to be considered.

As we will see in the next section, Algorithm 4.1 performs better than Algorithm 3.2, and hence we tabulated dihedral function fields primarily using that algorithm. However, we will present our tabulation method in full generality; we will only assume q is odd and not a power of ℓ.

Recall that $\mathrm{Aut}(K_0) = \mathrm{Aut}(\mathbb{F}_q(x))$ is isomorphic to $\mathrm{PGL}(2, q)$, the group of fractional linear transformations of x over $\mathbb{F}_q$. The group $\mathrm{Aut}(K_0)$ also acts on the set of extension fields K_i of K_0, and for every $\phi \in \mathrm{Aut}(K_0)$ we have $\phi(\Delta(K_i/K_0)) = \Delta(\phi(K_i)/K_0)$. Therefore, instead of applying Algorithm 4.1 to all suitable K_2 and M_0, we only need to consider a representative from each orbit of $\mathrm{Aut}(K_0)$ acting on the set of suitable quadratic function fields K_2. Moreover, for each such field K_2 we need only consider representatives of the action of the stabilizer $\mathrm{Stab}(K_2) \subseteq \mathrm{PGL}(2, q)$ on the set of suitable M_0. After constructing all dihedral fields K_ℓ with quadratic resolvent fields K_2 from the set above, we then reapply the group of $\mathrm{PGL}(2, q)$-automorphisms

to the set of fields K_ℓ (modulo their stabilizers) to obtain the complete list of extensions K_ℓ/K_0. These ideas are captured in Algorithms 6.1, 6.2, and 6.3.

We will let $P(q, \ell, B, h)$ denote the set of nonconstant squarefree polynomials $f \in \mathbb{F}_q[x]$ whose degrees satisfy $\lceil \deg(f)/2 \rceil \leq \lfloor 2B/(\ell-1) \rfloor$ and whose leading coefficient is either 1 or a fixed nonsquare h in $\mathbb{F}_q$. Algorithm 6.1 finds orbit representatives for the set of quadratic function fields whose discriminant divisors are of degree at most $2B/(\ell-1)$.

Algorithm 6.1 Constructing a list of $\mathrm{PGL}(2,q)$-orbit representatives for quadratic function fields of bounded discriminant

Input: A nonnegative integer B, an odd prime ℓ, and an odd prime power $q \not\equiv 0 \bmod \ell$ and a primitive element h of $\mathbb{F}_q$.

Output: A set R'_B of all pairs (f, S_f) such that $f \in P(q, \ell, B, h)$, each S_f is the $\mathrm{PGL}(2,q)$-stabilizer of the class of f in $K_0^\times/(K_0^\times)^2$, and such that every quadratic extension K_2 of K_0 with $\deg \Delta(K_2/K_0) \leq 2B/(\ell-1)$ has exactly one $\mathrm{PGL}(2,q)$-orbit representative in the collection of fields defined by the f.

Initialize $R'_B \leftarrow \{(h, \mathrm{PGL}(2,q))\}$.
Set $L(f) \leftarrow 0$ for all $f \in P(q, \ell, B, h)$.
for $f \in P(q, \ell, B, h)$ **do**
  if $L(f) = 0$ **then**
    for $\phi = \frac{ax+b}{cx+d} \in \mathrm{PGL}(2,q)$ **do**
      $f_1(x) \leftarrow (cx+d)^{2\lceil (\deg f)/2 \rceil} f(\phi(x))$.
      if the leading coefficient m of f_1 is a square **then**
        Replace f_1 with f_1/m
      else
        Replace f_1 with hf_1/m.
      $L(f_1) \leftarrow 1$.
      if $f_1 = f$ **then**
        $S_f \leftarrow S_f \cup \{\phi\}$.
      $R'_B \leftarrow R'_B \cup \{(f, S_f)\}$.
      $S \leftarrow \emptyset$.
Return R'_B.

Recall that every quadratic function field K_2 can be expressed as $K_0(y)$, where

y^2 is equal to either a nonsquare in $\mathbb{F}_q$ or a squarefree polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $2g+1$ or $2g+2$, where g is the genus of K_2. In the former case, K_2 is fixed under $\mathrm{PGL}(2,q)$. In the latter case, the action of $\phi \in \mathrm{PGL}(2,q)$ on K_2 does not necessarily preserve the degree of $f(x)$, but $\phi(K_2)$ has the same genus as K_2; in fact, the discriminant divisors of K_2 and $\phi(K_2)$ have the same degree, namely $2g+2$. Thus, fields in the same $\mathrm{PGL}(2,q)$-orbit have discriminant divisors of the same degree.

Algorithm 6.2 constructs minimal polynomials for all dihedral function fields with discriminant divisors $\frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M_0$ for all suitable M_0 for each representative K_2 obtained from Algorithm 6.1.

Finally, Algorithm 6.3 reapplies $\mathrm{Aut}(K)$ to each of the minimal polynomials constructed in Algorithm 6.2 to obtain the full list of degree ℓ dihedral function fields whose discriminant divisor has degree bounded by B.

The technique of utilizing $\mathrm{Aut}(\mathbb{F}_q(x))$ does result in a significant reduction in run time versus the naive method of iteration for tabulation. This can be seen in Tables 6.2 and 6.3. This and other numerical results are discussed in the following section.

Algorithm 6.2 Tabulating $\mathrm{PGL}(2,q)$-orbit representatives of dihedral function fields with bounded discriminant

Input: A nonnegative integer B, an odd prime ℓ, an odd prime power $q \not\equiv 0 \bmod \ell$, and the set R'_B computed by Algorithm 6.1 on input B, ℓ, q, h.

Output: A set R_B of triples (L_2, Δ, S_Δ) such that each Δ is an effective divisor of K of degree at most B, the group S_Δ is the $\mathrm{PGL}(2,q)$-stabilizer of Δ, the set L_2 consists of defining equations for the $\mathrm{PGL}(2,q)$-orbit representatives of $\mathcal{D}_\ell$ extensions of K_0 with discriminant divisor Δ.

1: Initialize $R_B \leftarrow \emptyset$.
2: **for** $(f, S_f) \in R'_B$ **do**
3: Construct $K_2 = K_0(x)[y]/\langle y^2 - f\rangle$ and compute $\Delta(K_2/K_0)$.
4: Compute $B' = \lfloor B/(\ell-1) - (\deg(\Delta(K_2/K_0)))/2 \rfloor$.
5: Initialize $\mathfrak{M} \leftarrow \emptyset$; eventually, $\mathfrak{M}$ will contain all effective squarefree divisors of K_0 with support disjoint from $\Delta(K_2/K_0)$ and degree at most B'.
6: Compute lists $L_j = \{P \in \mathbb{P}(K_0) \setminus \operatorname{Supp} \Delta(K_2/K_0) : \deg P = j\}$ for $1 \le j \le B'$.
7: **for** i from 0 to B' and for every partition $\mathbf{n} = [n_1, .., n_r]$ of i **do**
8: Generate the set $W_{\mathbf{n}} = \{\sum_{k=1}^{r} P_k : P_k \in L_{n_k}\}$.
9: $\mathfrak{M} \leftarrow \mathfrak{M} \cup W_{\mathbf{n}}$.
10: Compute the set $\mathfrak{M}_S$ of all pairs (M_0, S_Δ) where each $M_0 \in \mathfrak{M}$ is a unique orbit representative of S_f acting on $\mathfrak{M}$ and S_Δ is the stabilizer of M_0 in S_f.
11: **for** $(M_0, S_\Delta) \in \mathfrak{M}_S$ **do**
12: Get L_2 from Algorithm 3.2 (or 4.1 if $q \equiv 1 \bmod \ell$ or 5.3 if $q \equiv -1 \bmod \ell$) on input (K_2, ℓ, M_0).
13: Compute $\Delta = \frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M_0$.
14: $R_B \leftarrow R_B \cup \{(L_2, \Delta, S_\Delta)\}$.
15: Return R_B.

Algorithm 6.3 Tabulating the full list of dihedral function fields with bounded discriminant

Input: A nonnegative integer B, an odd prime ℓ, an odd prime power $q \not\equiv 0 \bmod \ell$, and the set R_B computed by Algorithm 6.2 on input B, ℓ, q.

Output: A set L_B of defining equations for all the dihedral extensions K_ℓ of K with $\deg \Delta_{K_\ell} \le B$.

1: Initialize $L_B \leftarrow \emptyset$.
2: **for** $(L, \Delta, S_\Delta) \in R_B$ **do**
3: **for** all distinct coset representatives ϕ of $\mathrm{PGL}(2,q)/S_\Delta$ and all $C(X) \in L$ **do**
4: Set $L_B \leftarrow L_B \cup \{(\phi(C(X)), \phi(\Delta))\}$.
5: Return L_B.

6.2 Implementations and Numerical Results

All computations were carried out using Magma on one core of a 2GHz Intel Xeon X7550, with 64GB of available RAM. For ease of presentation all the tables of data are gathered together at the end of this chapter in Section 6.3. Throughout, the column headed $K_2/\sim$ gives the number of quadratic function fields generated by Algorithm 6.1. The number of function fields constructed by Algorithm 6.2 is given in the column headed $K_\ell/\sim$, and the total number of nonconjugate dihedral degree ℓ function fields whose discriminant divisor has degree at most B is listed in the column headed K_ℓ.

We begin by comparing the Kummer theoretic approach of Algorithm 4.1 to the class field approach of Algorithm 3.2. We ran Algorithm 6.2 with various inputs for the two cases when $q \equiv \pm 1 \bmod 2\ell$ and recorded our findings in Table 6.1. Both methods produced the same number of fields (instilling confidence in our implementation), but Algorithm 4.1 performs this computation in less time than Algorithm 3.2; the ratio R_0 of the two run times is seen in the last column of Table 6.1.

Notice that the improvement factor R_0 of Algorithm 3.2 over Algorithm 4.1 is much more pronounced when $q \equiv -1 \bmod \ell$. In this case, approximately 75% of the run time is spent preforming Magma's built-in algorithms to find defining equations for the fields $K_{2\ell}/K_2$, while only approximaltely 25% of the run time is spent on this process when $q \equiv 1 \mod \ell$. This disparity is due to the fact that Magma's method for finding a defining equation of $K_{2\ell}/K_2$ utilizes Kummer Theory and Theorem 3.1.5 explicitly. Thus, calculations in Algorithm 3.2 are performed in the extension field $K_2(\zeta_\ell)$, while Algorithm 4.2 does not extend the constant field and performs calculations in $\widehat{K}_2$. This also seems to explain why for a fixed B and ℓ the improvement factor R_0 grows

quickly with q when $q \equiv -1 \bmod \ell$. The remainder of the run time for Algorithm 3.2 is dominated by the construction of ray class groups. When $q \equiv 1 \bmod \ell$ the improvement factor tends to decrease with q when we fix ℓ and B. This appears to be due to the fact that class group computations tend to dominate both algorithms in this case, and hence their run times tend to grow closer. All of these findings are consistent with the observations C. Fieker made in [19] concerning the class field theoretic algorithm in the number field setting.

Notice too that the improvement factor R_0 in Table 6.1 seems to decrease with ℓ when $q \equiv -1 \bmod \ell$, and remains rather consistent when $q \equiv 1 \bmod \ell$. It is not clear why this should be the case. Regardless, Algorithm 4.1 is more efficient for the entire range of cases we considered and hence was used for the final tabulations.

Overall, the run time of Algorithm 4.1 is dominated by the construction of class groups, and obtaining functions for the principal divisors in steps 13 and 19. Data suggests that as B grows, the proportion of time spent finding functions for principal divisors tends to increase. Using Jacobian arithmetic as opposed to divisor arithmetic as suggested in part 2 of Remarks 4.2.1 improved the performance of our tabulation only marginally, though we expect it would have a more significant impact for larger parameters.

In Table 6.2, we provide tabulation data for all odd primes ℓ, prime powers $q \equiv 1 \bmod 2\ell$, and multiples $B > \ell - 1$ of $\ell - 1$ such that $q^{2B/(\ell-1)+1} < 2^{29}$. The running times of Algorithms 6.1, 6.2, and 6.3 are listed when Algorithm 4.2 is used for construction. In Table 6.3 we provide the same information for when $q \equiv -1 \bmod 2\ell$ and Algorithm 5.3 was used for construction. For each ℓ, q and B, we also computed the value $R = (q^3 - q)T_2/(T_1 + T_2 + T_3)$, where T_i denotes the running time

of Algorithm 6.i for $i = 1, 2, 3$. The quantity R estimates the improvement factor obtained by our tabulation method relative to simply iterating Algorithm 4.1, or 5.3, respectively, over all possible quadratic function fields without using the $\mathrm{PGL}(2, q)$ action.

Notice that the improvement factor R is highly varied. For fixed ℓ and q, R tends to decrease as B increases although the improvement still remains significant. Why this decrease occurs is unclear; it may be due to the fact that R is not a sufficiently refined estimate for the actual running time improvement.

Examining the asymptotic complexity of our tabulation method, we recall that the asymptotic run time of tabulation is dominated by the repeated computation of the divisor class groups in Algorithm 4.2. The method implemented in Magma for computing the divisor class group of a function field of genus g over $\mathbb{F}_q$ is that of Hess [23]. It is a sub-exponential probabilistic index calculus algorithm with expected run time $\exp(\sqrt{\log q^g \log\log q^g})^{c+o(1)}$ for some explicit positive constant c as $g \to \infty$.

We need to apply Algorithm 6.1 essentially q^{B-3} times to quadratic function fields of genus at most $(B-2)/2$. Combining these results gives an asymptotic complexity of $q^B \exp(\sqrt{\log q^B \log\log q^B})^{c+o(1)}$ as $B \to \infty$. However, as we only ran our algorithm with small values of B, this run time analysis is of limited value. Moreover in terms of asymptotic complexity, performing Algorithms 6.1 and 6.3 have no benefit over the naive tabulation method, even though they are extremely valuable in practice.

6.2.1 Asymptotic Comparison when $\ell = 3$

In the case when $\ell = 3$, our algorithm tabulates all non-Galois cubic function fields up to a given degree bound on the discriminant divisor over any finite field with

characteristic greater than 3. Galois cubics are not difficult to count, so we can find the total number of cubic extensions of K whose discriminant divisors have degree at most some fixed bound. To illustrate the counting of Galois cubic fields, consider the following example:

Example 6.2.1. In this example we compute the number of Galois extension K_3/K_0 with $\deg(\Delta(K_3/K_0)) = 4$ and $\deg(\Delta(K_3/K_0)) = 6$ when $q \equiv 1 \bmod 3$. By Theorem 5.1.2, the number of geometric extensions equals the number of representatives of the cyclic subgroups of $K_0^\times/(K_0^\times)^3$ such that $\sum_{P\in\mathrm{Supp}((\alpha))} \deg(P) = 2$, and 3, respectively. As $|\mathbb{F}_q^\times/\mathbb{F}_q^3| = 3$, and $\mathrm{Pic}^0(K_0) = 0$, for each coset representative D of $\mathrm{Div}^0(K_0)/3\,\mathrm{Div}^0(K_0)$, there are 3 choices of $\alpha \in K_0^\times/(K_0^\times)^3$ such that $(\alpha) = D + 3\,\mathrm{Div}(K_0)$. Moreover, as α and α^2 correspond to isomorphic cyclic subgroups of $K_0^\times/(K_0^\times)^3$, the number of Galois extensions K_3/K_0 with $\deg(\Delta(K_3/K_0)) = 4$ and $\deg(\Delta(K_3/K_0)) = 6$ is 3 times the number of cosets in $\mathrm{Div}^0(K_0)/3\,\mathrm{Div}(K_0)$ up to multiplication by 2, whose support has degree 4, or 6 respectively.

By the division algorithm, can write each coset $D + 3\,\mathrm{Div}^0(K_0)$ uniquely as $D_1 + 2D_2 + 3\,\mathrm{Div}^0(K_0)$ for some effective coprime divisors $D_1, D_2 \in \mathrm{Div}(K_0)$, where $\deg(D_1) + 2\deg(D_2) \equiv 0 \bmod 3$. Thus we need only count the number of possibilities for D_1 and D_2 such that $\deg(D_1 + D_2) = 4$ and 6, respectively, up to multiplication by 2.

$B = 4$: Here the only possibility is $\deg(D_1) = \deg(D_2) = 1$. There are $3(q+1)q/2$ distinct cyclic cubic fields.

$B = 6$: Here the only possibility is $\deg(D_1) = 2$ and $\deg(D_2) = 1$. When D_1 is a place of degree 2 there are $(q+1)(q^2-q)/2$ distinct choices for D, and when when D_1 is the sum of two places of degree 1 there are $q(q+1)(q-1)/6$ distinct choices

for D. Therefore there are $2q(q+1)(q-1)$ cyclic cubic extensions K_3/K_0 with $\deg(\Delta((K_3/K_0)) = 6$.

When $q \equiv -1 \bmod 3$, the number of Galois extensions can be counted with similar formulas to those above. We, however, simply counted such extensions taking 3 times the result of Algorithm 4.2 with input $(\mathbb{F}_{q^2}(x), B, 3)$. Notice that by Theorem 5.1.2, Algorithm 4.2 conveniently produces abelian extensions with this input.

We now compare our total counts to the asymptotic predictions. A result of Datskovsky and Wright [14, Theorem I.1] provides an asymptotic formula for the number of cubic extensions who have discriminant divisors of degree at most B:

$$\lim_{\substack{B\to\infty \\ B \text{ even}}} q^{-B} \sum_{\substack{K_3/K_0 \\ \deg \Delta(K_3/K_0)\leq B}} 1 = \frac{q^3}{(q^2-1)(q-1)\zeta_{K_0}(3)} = \frac{q^2+q+1}{q^2}. \tag{6.1}$$

(Note that the term $2\log q$ in [14, Theorem I.1] should be simply $\log q$.)

In Table 6.4 we compare this asymptotic expression to our actual computations. For each q and B listed in the first two columns, the entry in column 5 gives the total number of cubic extensions of $\mathbb{F}_q(x)$ with discriminant divisor of degree at most B, broken down into the number of non-Galois extensions (column 3) and Galois extensions (column 4). Column 6 gives the estimate from equation (6.1), and column 7 gives the ratio R_3 of the estimate to the actual values.

As in the number field setting, the leading term of the asymptotic expression overestimates the actual number of cubic function fields, which leads us to believe that the secondary term has a negative coefficient. An explicit computation of this secondary term is currently underway by Yongqiang Zhao [44].

Remark 6.2.2. Notice too that in all cases we computed, the ratio R_3 for $B = 8$ is

larger than that for $B = 6$, which in turn is larger than that for $B = 4$. However, the result of [14] says that R_3 should tend to 1 as B tends to infinity. It is interesting to note that when $q = 5$ (the only case were we where able to fully tabulate when $B = 10$) the ratio R_3 is closer to 1 than the case when $B = 8$. One possible explanation for this is that the number of cubic fields with $M_0 \neq 0$ for $B < 10$ is a relatively smaller proportion than when $B \geq 10$.

6.2.2 Explicit Formulas for $B = 2(\ell - 1)$

In this section we give an explicit formula for the number of $\mathcal{D}_\ell$ extensions whose discriminant divisor has degree $2(\ell - 1)$. This result was first presented in [42] and is originally due to to Everett Howe. Here, we will extend his formula to the case $q \equiv -1 \bmod 2\ell$.

Notice that by Corollary 3.2.4 there are no $\mathcal{D}_\ell$ extensions whose discriminant divisor has degree less than $2(\ell - 1)$. On the other hand, there do exist $\mathcal{D}_\ell$ extensions with discriminant divisor of degree $2(\ell - 1)$, as seen in the following theorem:

Theorem 6.2.3 ([42] Thm 5.1)**.** *Let ℓ be an odd prime and let q be a prime power with $q \equiv 1 \bmod 2\ell$. For every nonnegative even integer d, let N_d be the number of $\mathcal{D}_\ell$ extensions of K_0 whose quadratic resolvents have discriminant divisors of degree d and whose discriminant divisors have degree $2(\ell - 1)$. Let X be the modular curve*

$X_1(\ell)$. *Then*

$$\frac{N_d}{q^3-q} = \begin{cases} \dfrac{1}{2q+2} & \text{if } d=0, \\ 1 & \text{if } d=2, \\ -2+\dfrac{2\#X(\mathbb{F}_q)}{\ell-1} & \text{if } d=4, \\ 0 & \text{otherwise.} \end{cases}$$

When $q \equiv -1 \bmod 2\ell$, we obtain a similar result, where only the case $d=0$ is different. Indeed, we have the following theorem:

Theorem 6.2.4. *Let ℓ be an odd prime and let q be a prime power with $q \equiv -1 \bmod 2\ell$. For every nonnegative even integer d, let N_d be the number of $\mathcal{D}_\ell$ extensions of K_0 whose quadratic resolvents have discriminant divisors of degree d and whose discriminant divisors have degree $2(\ell-1)$. Let X be the modular curve $X_1(\ell)$. Then*

$$\frac{N_d}{q^3-q} = \begin{cases} \dfrac{1}{2q-2} & \text{if } d=0, \\ 1 & \text{if } d=2, \\ -2+\dfrac{2\#X(\mathbb{F}_q)}{\ell-1} & \text{if } d=4, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For the case that $d=0$, by Theorem 5.1.2, we see that non-Galois extensions when $q \equiv -1 \bmod 2\ell$ correspond to the coset representatives α of the cyclic subgroups of $K_0^\times/(K_0^\times)^3$ such that $\sum_{P \in \mathrm{Supp}((\alpha))} \deg(P) = 2$. As we saw in Example 6.2.1, there are $q(q+1)/2$ such representatives.

The case that $d = 2$ follows exactly as in [42] replacing K_2 with $\widehat{K}_2$.

In the case that $d = 4$, we obtain from the proof of Theorem 5.1 in [42] that

$$\frac{N_4}{\#\,\mathrm{PGL}(2,q)} = \frac{2}{\ell - 1} \sum_{(E,P)/\cong} \frac{1}{\#\,\mathrm{Aut}(E,P)}. \tag{6.2}$$

where the sum is over isomorphism classes of pairs (E, P), with E an an elliptic curve over $\mathbb{F}_q$ and P a nonzero ℓ-torsion point in $E(\mathbb{F}_q)$; two such pairs (E_1, P_1) and (E_2, P_2) are isomorphic to one another when there is an isomorphism $E_1 \to E_2$ that takes P_1 to P_2. The automorphism group of a pair (E, P) consists of the automorphisms of E (as an elliptic curve) that fix P.

From [24, Prop 3.3, p. 240] and [24, Prop 2.3, p. 233], Howe then shows that

$$\sum_{(E,P)/\cong} \frac{1}{\#\,\mathrm{Aut}(E,P)} = \#X(\mathbb{F}_q) - c,$$

where c is the number of $\mathbb{F}_q$-rational cusps on X. Since $\mathbb{F}_{q^2}$ contains the ℓ-th roots of unity, all of the $\ell - 1$ geometric cusps of X are defined over $\mathbb{F}_q$ [36, Theorem 1.3.1(b), p. 12], so we have $c = \ell - 1$. Combining this with equation (6.2) gives the formula for N_4 stated in the theorem. □

For $\ell = 3$, 5, and 7, the modular curve $X_1(\ell)$ has genus 0, so for these values of ℓ the formula for N_4 simplifies to

$$\frac{N_4}{q^3 - q} = \frac{2(q - \ell + 2)}{\ell - 1}.$$

In these cases, our tabulation data verifies this result, further supporting the correctness of our implementation. We note that equations for $X_1(\ell)$ for larger values of ℓ

are also known [38].

Notice that the values of these formulas agree with the data in Tables 6.2 and 6.3.

Remark 6.2.5. Note that for $B = 4$, Theorems 6.2.3 and 6.2.4 give explicit formulas for the number of cubic extensions when q is odd and $q \equiv \pm 1 \bmod 3$:

1. When $q \equiv 1 \bmod 3$, by Theorem 6.2.3, the number of non-Galois extensions is

$$(q^3 - q)\left(\frac{1}{2q+2} + 1 + (q-1)\right) = q^4 - \frac{q^2+q}{2},$$

and by Example 6.2.1, and including $\mathbb{F}_{q^3}$, the number of Galois extensions is $(3q^2 + 3q + 2)/2$, so the total number of cubic extension is $q^4 + q^2 + q + 1$. It follows that for $B = 4$ the ratio in column 7 of Table 6.4 is equal to

$$1 + \frac{q^3 - q - 1}{q^4 + q^2 + q + 1}.$$

2. When $q \equiv -1 \bmod 3$, by Theorem 6.2.4, the number of non-Galois extensions is

$$(q^3 - q)\left(\frac{1}{2q-2} + 1 + (q-1)\right) = q^4 - \frac{q^2-q}{2},$$

and the number of Galois extensions is $(3q^2 - 3q + 2)/2$, so the total number of cubic extension is $q^4 + q^2 - q + 1$. It follows that for $B = 4$ the ratio in column 7 of Table 6.4 is equal to

$$1 + \frac{q^3 + q - 1}{q^4 + q^2 - q + 1}.$$

Notice that the secondary terms of the above ratios both have degree -1 in q

6.3 Tables of Numerical Data

	ℓ	q	B	$K_2/\sim$	$K_\ell/\sim$	Run time (sec.) Alg 3.2	Run time (sec.) Alg 4.2	R_0
$q \equiv 1 \bmod \ell$:	3	7	4	30	14	2.6	0.7	3.7
			6	779	458	137.6	31.5	4.4
		13	4	58	30	6.4	1.9	3.4
			6	4,647	2,538	1053.9	264.5	4.0
		19	4	78	38	12.0	3.8	3.2
		43	4	174	86	60.7	25.0	2.5
	5	11	8	42	6	3.6	0.7	5.1
			12	2,855	917	537.6	95.2	5.6
	7	29	12	118	16	22.6	6.8	3.3
	11	23	20	90	5	14.6	3.2	4.7
	23	47	44	186	8	152.8	22.1	6.9
$q \equiv -1 \bmod \ell$:	3	5	4	22	6	4.2	0.3	14.0
			6	307	166	151.4	10.6	14.3
		11	4	42	18	27.9	1.3	21.4
			6	2855	1524	4321.4	156.7	27.6
		17	4	70	30	133.5	3.4	39.0
		47	4	186	90	42201.2	33.5	1259.8
		53	4	217	102	78841.5	50.0	1576.8
	5	9	8	37	6	12.4	0.7	17.7
		9	12	1554	506	1420.0	55.7	25.5
		19	8	78	14	101.5	2.5	40.6
	7	13	12	58	6	20.0	1.3	15.4
		27	12	105	10	253.1	5.5	46.0
	19	37	36	157	4	5110.3	10.8	473.2

Table 6.1: A Comparison of the class field theoretic construction method (Algorithm 3.2 and the Kummer theoretic construction method (Algorithms 4.1, 5.3). For each ℓ, q, and B given in the first three columns, we list in column 4 the number of $\mathrm{PGL}(2,q)$-equivalence classes of quadratic extension K_2 whose discriminants $\Delta(K_2/K_0)$ are such that $4 \leq \Delta(K_2/K_0) \leq 2B/(\ell-1)$. In column 5, we list the number of $\mathrm{PGL}(2,q)$-equivalence classes of $\mathcal{D}_\ell$ extensions of K whose discriminants have degree at most B. In the next two columns we give the running times of the algorithms that computed the quantities in column 5, and in the final column we give the ratio of their run times.

						Run time (sec.)			
ℓ	q	B	$K_2/\sim$	$K_\ell/\sim$	K_ℓ	Alg 6.1	Alg 6.2	Alg 6.3	R
3	7	4	33	17	2,373	0.9	1.1	0.8	132.0
		6	782	472	117,285	25.8	35.2	47.1	109.4
		8	35,010	18,149	5,763,093	1,321.5	2,416.9	2,505.1	130.1
	13	4	61	33	28,470	13.7	3.2	9.5	264.7
		6	4,650	2,564	4,824,534	1,379.5	286.1	1,870.2	176.7
	19	4	81	41	130,131	82.8	7.6	44.5	385.4
	25	4	109	57	390,300	726.8	17.6	149.1	307.3
	31	4	129	65	923,025	821.0	31.7	357.2	779.7
	37	4	157	81	1,873,458	1,983.1	56.5	731.7	1,031.9
	43	4	177	89	3,417,855	4,040.5	100.2	1,341.9	1,452.3
	49	4	205	105	5,763,576	20,544.4	189.6	2,376.5	964.8
5	11	8	45	9	6,655	6.1	1.4	2.7	181.2
		12	2,858	949	1,058,695	461.5	102.9	463.5	132.1
	31	8	109	33	446,865	821.0	29.2	191.0	834.6
	41	8	169	45	1,378,420	3,178.2	80.5	602.0	1,436.2
7	29	12	121	19	219,646	546.8	22.6	94.8	828.9
	43	12	177	29	1,086,911	4,000.5	95.2	567.8	1,622.2
11	23	20	93	8	48,829	192.7	10.1	23.8	541.3
13	53	24	217	21	1,340,794	10,935.6	235.8	742.8	2,945.5
23	47	44	189	11	519,961	5,951.6	184.2	364.9	2,940.5

Table 6.2: Function field counts for all ℓ and $q \equiv 1 \bmod 2\ell$ with $q^{\frac{2B}{\ell-1}+1} < 2^{29}$, for $B \geq 4$. For each ℓ, q, and B given in the first three columns, we list in column 4 the number of $\mathrm{PGL}(2,q)$-equivalence classes of quadratic extension of $K = \mathbb{F}_q(x)$ whose discriminants have degree at most $2B/(\ell-1)$. In column 5, we list the number of $\mathrm{PGL}(2,q)$-equivalence classes of $\mathcal{D}_\ell$ extensions of K whose discriminants have degree at most B, and in column 6 we list the total number of such extensions. In the next three columns we give the running times of the algorithms that computed these quantities, and in the final column we give an estimate of the improvement in running time obtained by using the $\mathrm{PGL}(2,q)$ action in our computations.

						Run time (sec.)			
ℓ	q	B	$K_2/\sim$	$K_\ell/\sim$	K_ℓ	Alg 6.1	Alg 6.2	Alg 6.3	R
3	5	4	25	9	615	0 2	0.5	0.3	60.0
		6	310	176	15,575	3 0	10.8	5.8	66.1
		8	6,818	3596	390,125	76 8	383.4	161.0	74.1
		10	163,701	98,124	11,638,385	2,037 4	17,090.5	4,917.1	85.3
	11	4	45	21	14,586	6 1	2.0	5.1	200.0
		6	2,858	1,546	1,770,966	461 5	142.9	653.5	169.3
	17	4	73	33	83,375	51 1	4.6	30.0	262.8
		6	10,222	5,404	24,136,801	8,150 5	665.7	8,703.1	205.6
	23	4	93	45	279,588	192 7	13.4	99.9	531.8
	29	4	121	57	706,875	546 8	26.6	255.2	782.0
	41	4	169	81	2,824,941	3,191 0	83.9	1,023.6	1344.4
	47	4	189	93	4,878,600	5,951 6	144.1	1,845.1	1883.2
	53	4	217	105	7,889,103	10,935 6	221.8	3,047.2	2323.8
5	9	8	43	9	2,925	5 7	1.1	1.2	99.0
		12	1,600	532	330,495	278 3	57.1	148.1	85.0
		16	121,158	38,116	26,469,345	24,063 6	8,603.7	12,971.4	135.7
	19	8	81	17	61,750	82 8	5.8	23.9	352.6
	29	8	121	29	341,475	546 8	21.8	133.4	756.5
	49	8	205	49	2,823,625	20,544 4	167.8	1,106.6	904.4
7	13	12	61	9	8,099	13 7	2.1	2.8	246.6
		18	4,650	1,017	1,993,342	1,379 5	142.5	836.6	132.0
	27	12	111	13	164,178	1,121 2	17.6	64.8	287.4
	41	12	169	23	896,301	3,191 0	78.3	387.8	1474.7
11	43	20	177	17	716,122	4,052 6	91.4	338.8	1620.2
13	25	24	109	3	15,925	726 8	12.8	7.2	267.4
19	37	36	157	7	152,551	1,982 2	52.4	90.5	132.8

Table 6.3: Function field counts for all ℓ and $q \equiv -1 \bmod 2\ell$ with $q^{\frac{2B}{\ell-1}+1} < 2^{29}$, for $B \geq 4$. For each ℓ, q, and B given in the first three columns, we list in column 4 the number of $\mathrm{PGL}(2,q)$-equivalence classes of quadratic extension of $K = \mathbb{F}_q(x)$ whose discriminants have degree at most $2B/(\ell-1)$. In column 5, we list the number of $\mathrm{PGL}(2,q)$-equivalence classes of $\mathcal{D}_\ell$ extensions of K whose discriminants have degree at most B, and in column 6 we list the total number of such extensions. In the next three columns we give the running times of the algorithms that computed these quantities, and in the final column we give an estimate of the improvement in running time obtained by using the $\mathrm{PGL}(2,q)$ action in our computations.

		Number of cubic extensions				
q	B	Non-Galois	Galois	Total	$q^{B-2}(q^2+q+1)$	Ratio R_3
5	4	615	31	646	775	1.200
	6	15,575	31	15,606	19,375	1.242
	8	390,125	751	390,876	484,375	1.239
	10	11,638,385	751	11,639,136	12,109,375	1.040
7	4	2,373	85	2,458	2,793	1.136
	6	117,285	1,093	118,378	136,857	1.156
	8	5,763,093	4,117	5,767,210	6,705,993	1.163
11	4	14,586	166	14,752	16,093	1.091
	6	1,770,966	166	1,771,132	1,947,253	1.099
13	4	28,470	274	28,744	30,927	1.076
	6	4,824,534	6,826	4,831,360	5,226,663	1.082
17	4	83,375	409	83,784	88,723	1.059
	6	24,132,801	409	24,133,210	25,640,947	1.062
19	4	130,131	571	130,702	137,541	1.052
23	4	279,588	760	280,348	292,537	1.043
25	4	390,300	976	391,276	406,875	1.040
29	4	706,875	1,212	708,087	732,511	1.034
31	4	923,025	1,489	924,514	954,273	1.032
37	4	1,873,458	2,110	1,875,568	1,926,183	1.027
41	4	2,824,941	2,461	2,827,402	2,896,363	1.024
43	4	3,417,855	2,839	3,420,694	3,500,157	1.023
47	4	4,878,600	3,244	4,881,844	4,985,713	1.021
49	4	5,763,576	3,676	5,767,252	5,884,851	1.020
53	4	7,889,103	4,153	7,893,256	8,042,167	1.019

Table 6.4: Cubic function field counts compared to asymptotics, for $B \geq 4$ with $q^{B+1} < 2^{29}$. For the q and B values given in the first two columns, we list the number of cubic extensions of $\mathbb{F}_q(x)$ with discriminant divisor of degree at most B, subdivided into the counts of non-Galois and Galois extensions. The sixth column gives an estimate for the total number of cubic extensions derived from the asymptotic formula (6.1), and the seventh column gives the ratio between the estimate and the actual number from column 5.

Chapter 7

Conclusions

As mentioned, this thesis represents the next steps in function field construction and tabulation. We present, implement, and compare new algorithms for constructing all dihedral function fields with prescribed ramification (which includes all non-Galois cubics) over finite fields in all characteristics greater than 3, and under Assumtion COEFF over infinite perfect fields. With these algorithms we are able to provide the first complete tables of function fields over finite fields whose discriminant divisors have degree at most a fixed bound. In particular, only now can the asymptotic estimates for cubic function fields be truly compared to the actual number of cubic fields in characteristics greater than 3. In all cases that we considered the leading term of the asymptotic expression overestimates the actual number of cubic function fields. This leads us to believe that the secondary term has a negative coefficient. An explicit computation of this secondary terms is currently underway by Yongqiang Zhao [44].

It is interesting that the number of degree ℓ dihedral function fields with a given quadratic resolvent K_2 and discriminant divisor $\Delta = \frac{\ell-1}{2}\Delta(K_2/K_0) + (\ell-1)M_0$ behaves quite differently depending on whether or not M is trivial. We see from Theorem 4.1.12 that when $M_0 = 0$, the number of such fields with a given resolvent field K_2 depends exclusively on the ℓ-rank of K_2. The probability that the divisor

class group of K_2 has a certain ℓ-Sylow subgroup is the focus of various Cohen-Lenstra type heuristics. These are discussed further in [1], [20], [21], and [27], and directly relate to the number of $\mathcal{D}_\ell$ function fields with $M_0 = 0$.

When the degree of the discriminant divisor of a degree ℓ extension is minimal, i.e. of degree $2(\ell-1)$, our tabulation counts are verified by the explicit formulas given in Theorems 6.2.3 and 6.2.4. Notice in these theorems that when $d = 4$, the formulas given are the same despite the variability of the presence of ℓ-th roots of unity. As mentioned above, this situation is related to the ℓ-ranks of class groups of genus 1 function fields. One way to interpret the results of Theorems 6.2.3 and 6.2.4 is as follows: When $q \equiv \pm 1 \bmod \ell$,

$$\sum_{\substack{K_2/K_0, \\ Genus(K_2)=1}} \sum_{\substack{\mathcal{H}\subset \mathrm{Pic}^0(K_2), \\ [\mathrm{Pic}^0(K_2):\mathcal{H}]=\ell}} 1 = -2 + \frac{2\#X(\mathbb{F}_q)}{\ell - 1}.$$

Notice that this equation does not vary with the presence of roots of unity. We find this result surprising since the probability that any one of these extensions has an index ℓ subgroup does vary with the presence of roots of unity. Indeed, as these extensions have genus 1, they can either have ℓ-rank 1 or 2. However, when $q \equiv -1 \bmod \ell$, the case of ℓ-rank 2 cannot occur, yet when $q \equiv 1 \bmod \ell$, there do exist ℓ-rank 2 genus 1 extensions. Hence, it is surprising to us that despite the difference in the probabilities of various ℓ-ranks, the total number of index ℓ subgroups remains a fixed function of q, regardless of when $q \equiv 1 \bmod \ell$ or $q \equiv -1 \bmod \ell$.

The data of Tables 6.2 and 6.2 suggest the existence of other explicit formulas like those of Theorems 6.2.3 and 6.2.4. For example, let ℓ be an odd prime and let q be a prime power such that $q \equiv \pm 1 \bmod \ell$. Let $N(B, \ell, q)$ be the total number

of non-Galois degree ℓ dihedral extensions of $\mathbb{F}_q(x)$ whose discriminant divisors have degree at most B. Let $N_0(B, \ell, q)$ be the number of the above fields whose quadratic resolvents have discriminant divisors of degree 0. Based on our data, we make the following conjectures:

Conjectures 1-5.

1. When $B = 6$ and $\ell = 3$ then $N(6, 3, q) - N_0(6, 3, q) = (q^3 - q)(q^3 + q - 1)$.
2. When $B = 8$ and $\ell = 3$ then $N(6, 3, q) - N_0(6, 3, q) = (q^3 - q)(q^5 + q^3 - 1)/2$.
3. When $B = 6$ and $\ell = 5$ then $N(6, 3, q) - N_0(6, 3, q) = (q^3 - q)(q^3 + 2q^2 + 3q - 2)/2$.
4. For all B and ℓ, $2(q^3 - q)$ divides $(\ell - 1)(N(B, \ell, q) - N_0(B, \ell, q))$.
5. For all B and ℓ, $N(B, \ell, q) - N_0(B, \ell, q) \in \mathbb{Q}(q, \ell)$.

We note that the value of $N_0(6, 3, q)$ is easy to calculate as in the proofs of Theorems 6.2.3 and 6.2.4. Namely, it is $(q^2 - q)/2$ when $q \equiv 1 \bmod 3$, and $(q^2 + q)/2$ when $q \equiv -1 \bmod 3$. These conjecture holds for all values of q we computed. For the first conjecture, all 5 examples when $q = 5, 7, 11, 13$, and 17 satisfy this equation. The second and third conjectures only have 2 data points each (when $q = 5, 7$ and $q = 9, 11$, respectively), and hence are mainly speculation. The fourth conjecture is consistent with all the data but most of these are cases when $B = 2(\ell - 1)$ where we know this result to be true, or $B = 4(\ell - 1)$ where we strongly suspect it is true. The fifth conjecture implies our observation about the ℓ-ranks of genus 1 quadratic extensions discussed above, but also similar statements for higher genera.

When $M_0 \neq 0$, the number of degree ℓ dihedral function fields with given quadratic resolvent field K_2 depends additionally on the cardinality of the set $T_\ell(M_0)$ defined in Section 4.1.3. The natural map $\mathrm{Div}^0(K_2) \to \mathrm{Pic}^0(K_2)/\ell \,\mathrm{Pic}^0(K_2)$ is surjective, and when $|\operatorname{Supp}(M_0)|$ is sufficiently large it is reasonable to expect that the map Ψ from

Section 4.1.3 is also surjective, so that a random element of $\mathcal{Q}_\ell(M_0)$ will lie in the kernel of Ψ with probability

$$\frac{1}{\left|(\mathrm{Pic}^0(K_2)/\ell\,\mathrm{Pic}^0(K_2)\right|} = \frac{1}{\ell^r}.$$

Now, an element of $Q_\ell(M_0)$ lies in $T_\ell(M_0)$ if and only if it is in the kernel of Ψ, so we expect $T_\ell(M_0)$ to contain about $|Q_\ell(M_0)|/\ell^r = (\ell-1)^{|\mathrm{Supp}(M_0)|}/\ell^r$ elements. From Theorem 4.1.12, the number of nonconjugate degree ℓ dihedral function fields with quadratic resolvent K_2 and with discriminant divisor $\Delta = \frac{\ell-1}{2}D + (\ell-1)M_0$ is $|T_\ell(M_0)|\,\ell^r/(\ell-1)$, which we expect to be approximately $(\ell-1)^{|\mathrm{Supp}(M_0)|-1}$. Note that this is independent of r. When the size of $\mathrm{Supp}(M_0)$ is sufficiently large, our data seems to support this heuristic.

One obstacle to generating larger amounts of data is the memory intensive nature of Algorithm 6.1 as written. As we implemented our algorithms in Magma, we were also bounded by its memory restrictions – Magma does not allow arrays of more than 2^{29} elements. To avoid this limitation, one could obtain most of the results by instead looking for orbit representatives of $\mathrm{PGL}(2,q)$ acting on elliptic and hyperelliptic curves of genus g by iterating over these curves and computing their invariants. One would then only need to store a representative for each set of invariants. This would largely remove the storage requirements of the algorithm; however, it would also be a slower process as additional time must be spent computing these invariants.

For primes $\ell > 3$, no asymptotic estimates on counts of degree ℓ function fields are known; it may be possible to obtain such estimates by generalizing the work of [13] or adapting the program of [40] to the case $q \equiv \pm 1 \bmod \ell$ by using results in

[18], [21], and [27]. It would be very interesting to see if the "gaps" for the number field setting referred to in Chapter 1 occur here as well. This is research in progress of various people.

We note that our work is readily extendable to the problem of finding $\mathcal{D}_\ell$ extensions of function fields K other than $\mathbb{F}_q(x)$. This should be reasonably straightforward if one restricts to cases where $\mathrm{Pic}^0(K)[\ell]$ is trivial. Having such an algorithm would be beneficial. For example, in [16] the authors construct curves with a large number of $\mathbb{F}_q$-rational points relative to their genus. Their method is to start with the function field of a curve with many points of small genus and to construct cyclic extensions of it using Magma's built-in class field theoretic functions. In this way, they were able to find several new curves with a record number of points relative to their genus. However, due to the long run time, they where only able to carry out this method over $\mathbb{F}_q$ when $q = 2$. Considering the comparison in Table 6.1, we expect that one could use a Kummer theoretic approach to extend their search technique to larger values of q. One can already attempt this search with the algorithms presented in this thesis, though it is unclear if this would result in any new records.

Recall the situation in Figure 5.1. Here, a careful analysis of the action of ϱ on the ℓ-virtual units should also allow one to efficiently extend our methods to other values of q that are not ± 1 modulo ℓ. However, extending our construction methods to characteristics 2 and ℓ would be quite challenging. Firstly, one would now need to consider wildly ramified places. Secondly, in characteristic p, cyclic degree p extensions are not Kummer extensions, but rather are Artin-Schfeier extensions. Thus, a new theory of virtual units for Artin-Schreier extensions would need to be developed. It is not clear how to do this, and as Artin-Schreier extensions do not

occur in number fields, one cannot look there for inspiration.

As mentioned, we provide the first method for constructing function fields over infinite constant fields k_0 with a fixed non-abelian Galois group and given ramification. For curves over number fields, the invariant of interest is typically the conductor (which encodes primes of bad reduction), rather than the discriminant of the curve's function field, though these two invariants are strongly related. Unfortunately, constructing non-hyperelliptic curves with a given conductor is very difficult. It is our hope that upon further study one could turn our Kummer theoretic technique into one that constructs types of curves with given primes of bad reduction, though admittedly this seems to be very challenging.

In the number field situation, there are various methods to construct and tabulate quartic fields with prescribed ramification [6], [12]. Quartic fields with Galois group $\mathcal{A}_4$ and $\mathcal{S}_4$ are related to certain cubic fields; their cubic resolvents [22]. Moreover, in [12], the authors demonstrate how to use the theory of virtual units to construct all quartic function fields with a given Galois group and prescribed ramification from their cubic resolvent fields. Now that we have developed the theory of virtual units for function fields, and have complete tables of cubic fields in characteristic greater than 3, we expect to be able to able to apply the approach of [12] and develop an algorithm to construct all quartic fields with a given discriminant divisor. Moreover, using the tabulation technique described in Chapter 6, we should soon be able to build complete tables of quartic function fields whose discriminant divisors have degree at most a fixed bound. One should be able to extend this further to construct higher degree extensions with solvable Galois groups (like the degree 8 number fields in [10]).

— THE END —

Bibliography

[1] J. D. Achter, *The distribution of class groups of function fields*, J. Pure Appl. Algebra **204** (2006), no. 2, 316–333.

[2] E. Artin, *Über eine neue Art von L-Reihen*, Collect Papers, Springer-Verlag, New York, 1982, Edited by Serge Lang and John T. Tate, Reprint of the 1965 original.

[3] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.

[4] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, 2010.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[6] J. Buchmann, D. Ford, and M. Pohst, *Enumeration of quartic fields of small discriminant*, Math. Comp. **61** (1993), no. 204, 873–879.

[7] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[8] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.

[9] ———, *Constructing and counting number fields*, Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002) (Beijing), Higher Ed. Press, 2002, pp. 129–138.

[10] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Tables of octic fields with a quartic subfield*, Math. Comp. **68** (1999), no. 228, 1701–1716.

[11] ———, *On the density of discriminants of cyclic extensions of prime degree*, J. Reine Angew. Math. **550** (2002), 169–209.

[12] ———, *Constructing complete tables of quartic fields using Kummer theory*, Math. Comp. **72** (2003), no. 242, 941–951.

[13] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478.

[14] B. Datskovsky and D.J. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. **386** (1988), 116–138.

[15] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.

[16] V. Ducet and C. Fieker, *Computing equations of curves with many points*, Proceedings of the Tenth Algorithmic Number Theory Symposium, 2012, to appear.

[17] D. S. Dummit and R. M. Foote, *Abstract Algebra*, third ed., John Wiley & Sons Inc., Hoboken, NJ, 2004.

[18] J. Ellenberg, A. Venkatesh, and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, arxiv.org/abs/0912.0325v2[math.NT].

[19] C. Fieker, *Computing class fields via the Artin map*, Math. Comp. **70** (2001), no. 235, 1293–1303 (electronic).

[20] E. Friedman and L.C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239.

[21] D. Garton, *Random matrices and the Cohen-Lenstra statistics for global fields with roots of unity*, Ph.D. thesis, University of Wisconsin Madison, 2012.

[22] H. Heilbronn, *On the* 2*-classgroup of cubic fields*, pp. 117–119, Academic Press, London, 1971.

[23] F. Hess, *Zur Klassengruppenberechnung in algebraischen Zahlkörpern*, Ph.D. thesis, Technische Universität Berlin, 1996.

[24] E. W. Howe, *On the group orders of elliptic curves over finite fields*, Compositio Math. **85** (1993), no. 2, 229–247.

[25] M.J. Jacobson Jr., Y. Lee, R. Scheidler, and H.C. Williams, *Construction of all cubic function fields of a given square-free discriminant*, Preprint, 2012.

[26] J. Jones, *Number Fields*, 2012, searchable database of number fields, http://hobbes.la.asu.edu/NFDB.

[27] G. Malle, *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), no. 10, 2823–2835.

[28] M. E. Pohst, *On computing non-Galois cubic global function fields of prescribed discriminant in characteristic* > 3, Publ. Math. Debrecen **79** (2011), no. 3-4, 611–621.

[29] D.P. Roberts, *Density of cubic field discriminants*, Math. Comp. **70** (2001), no. 236, 1699–1705).

[30] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[31] P. Rozenhart, *Fast tabulation of cubic function fields*, Ph.D. thesis, University of Calgary, 2009.

[32] P. Rozenhart, M.J. Jacobson, and R. Scheidler, *Tabulation of cubic function fields via polynomial binary cubic forms*, Math. Comp. **81** (2012), no. 280, 2335–2359.

[33] P. Rozenhart and R. Scheidler, *Tabulation of cubic function fields with imaginary and unusual Hessian*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 357–370.

[34] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977, translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[35] N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, 2012, http://oeis.org.

[36] G. Stevens, *Arithmetic on modular curves*, Progress in Mathematics, vol. 20, Birkhäuser Boston Inc., Boston, MA, 1982.

[37] H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, Berlin, 2000.

[38] A. V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147.

[39] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields*, 2011.

[40] A. Venkatesh and J.S. Ellenberg, *Statistics of number fields and function fields*, Proceedings of the International Congress of Mathematicians. Volume II (New

Delhi), Hindustan Book Agency, 2010, pp. 383–402.

[41] G.D. Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Mathematics: Theory & Applications, Birkhäuser Boston Inc., Boston, MA, 2006.

[42] C. Weir, R. Scheidler, and E. Howe, *Constructing and tabulating dihedral function fields*, Proceedings of the Tenth Algorithmic Number Theory Symposium, 2012, to appear.

[43] D.J. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), no. 1, 17–50.

[44] Y. Zhao, *Private correspondence*, 2012.