UNIVERSITY OF CALGARY

Divisor Class Group Arithmetic on $C_{3,4}$ Curves

by

Evan MacNeil

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF MASTER OF SCIENCE

GRADUATE PROGRAM IN MATHEMATICS AND STATISTICS

CALGARY, ALBERTA
JANUARY, 2020

Abstract

Computing in the divisor class group of an algebraic curve is a non-trivial component in computing L-series. L-series in turn are at the heart of the Sato-Tate conjecture and related conjectures. The Sato-Tate conjecture has been proven for elliptic curves with complex multiplication, but remains open for other families of algebraic curves. In order to test these conjectures against other curve families, it is desirable to have efficient algorithms to perform divisor class group arithmetic.

Fast explicit formulas exist to perform divisor class group arithmetic for genus 1 and genus 2 curves. However, the picture for genus 3 curves is incomplete. Existing explicit formulas for arithmetic on non-hyperelliptic genus 3 curves ($C_{3,4}$ curves) have been developed with cryptographic applications in mind. They make certain genericity assumptions on their inputs that hold with high probability in cryptographic settings, but are unsuited for number theoretic use cases. More general algorithms exist that can perform divisor class arithmetic over any curve, but they are slow.

In this thesis, that gap is bridged. Fast explicit formulae are developed that may be used to add any pair of reduced divisors on any $C_{3,4}$ curve. Formulae optimized for the generic case considered by previous authors are produced, allowing one to add divisors in 1I+111M+3S+99A and double divisors in 1I+135M+3S+116A (inversions, multiplications, squarings, and additions in a field). The formulae are implemented in Sage. Benchmark tests find that these new formulae allow one to add and double 13.2% and 11.1% faster, respectively, that the previous state-of-the-art in $C_{3,4}$ curve arithmetic.

Preface

This thesis is an original work by the author. No part of this thesis has been previously published.

Acknowledgements

Thank you to my family. Your thoughts, prayers, and support were felt 4,500 km away.

Thank you to my supervisors, Dr. Renate Scheidler and Dr. Michael Jacobson. Your expertise in class group computations helped me get this project started. Your expertise in time management helped me finish.

Thank you to my fellow graduate students and officemates. Randy Yee, who poked holes in my proofs like a mathematical awl. Without you, the proofs in this thesis would look awfully stupid. Sumin Leem, who was always happy to help. Your experience with function fields was invaluable to my early understanding of curves. Geoff Vooys, who always had a different perspective on a problem and three references. When I was stuck on something, your take always led somewhere fruitful.

Table of Contents

List of Figures and Illustrations

List of Tables

1 Introduction

This introduction will be light on definitions. Full details of the topics mentioned may be found later in this thesis or in other cited works. For now, it should be enough to know that an **algebraic plane curve** is the set of points (x, y) at which $f(x, y) = 0$, for some field K and polynomial $f \in K[x, y]$, plus possibly some points "at infinity". Examples of algebraic plane curves include elliptic curves, hyperelliptic curves, and the subject of this thesis, $C_{3,4}$ curves. An **elliptic curve** is the set of zeroes of a polynomial [1]

$$y^2 + x^3 + c_4xy + c_3x^2 + c_2y + c_1x + c_0. \tag{1.1}$$

A (ramified genus 3) **hyperelliptic curve** is the set of zeroes of a polynomial

$$y^2 + x^7 + c_{10}x^3y + c_9x^6 + c_8x^2y + c_7x^5 + c_6xy + c_5x^4 + c_4y + c_3x^3 + c_2x^2 + c_1x + c_0, \tag{1.2}$$

though hyperelliptic curves can be of any genus 2 or greater and come in a variety of flavours (ramified, split, inert). A $C_{3,4}$ **curve** is the set of zeroes of a polynomial

$$y^3 + x^4 + c_8xy^2 + c_7x^2y + c_6x^3 + c_5y^2 + c_4xy + c_3x^2 + c_2y + c_1x + c_0. \tag{1.3}$$

For each of these classes of curves, one typically also demands that they be non-singular,[2] as we will do in Chapter 2.

If C is an algebraic plane curve, a **divisor** of C is a formal sum of points on C. If P and Q are points on C, then $2P$ and $P - Q$ are examples of divisors on C. In Chapter 5, we will place an equivalence relation on divisors, partitioning them into **divisor classes**. Together with an addition operation, this forms the **divisor class group** of C.

[1] The order in which the terms appear in Equations 1.1, 1.2, and 1.3 is consistent with the $C_{a,b}$ order (Definition 3.4) used throughout this thesis.

[2] See Section 2.1 for a definition.

1.1 Motivation

Let $\mathbb{F}_q$ be the finite field of order q and suppose E is an elliptic curve defined over $\mathbb{F}_q$, meaning that E is the set of zeroes of a polynomial in $\mathbb{F}_q[x, y]$ of the form in Equation 1.1. The following theorem, due to Helmut Hasse (1898 – 1979), says that the number of rational points (i.e. points in $\mathbb{F}_q \times \mathbb{F}_q$ plus an additional point at infinity) on E lies in some interval that is small compared to the order of $\mathbb{F}_q$.

Theorem 1.4 (Hasse, [20])**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The number of rational points on E differs from $q+1$ by at most $2\sqrt{q}$. That is,*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

In other words, $q+1$ is a good estimate for the number of rational points on E, especially when q is large.

Example 1.5. Let $p = 2^{31} - 1 = 2,147,483,647$, which is prime. The elliptic curve defined by $y^2 + x^3 - 1 = 0$ over $\mathbb{F}_p[x, y]$ has 2,147,391,324 rational points.

Let $a_q = \frac{\#E(\mathbb{F}_q)-(q+1)}{2\sqrt{q}}$. Then Hasse's Theorem says that $a_p \in [-1, 1]$. Letting $\theta_q = \arccos a_q$, then $\theta_q \in [0, \pi]$. Given a subinterval $[\alpha, \beta] \subseteq [0, \pi]$ and a prime p, one can ask what the probabilty is that $\theta_p \in [\alpha, \beta]$. The Sato-Tate Conjecture suggests that, for most elliptic curves, this probability follows a $\sin^2$ distribution.

Conjecture 1.6 (Sato-Tate, [43])**.** *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. For any interval $[\alpha, \beta] \subseteq [0, \pi]$,*

$$\lim_{N\to\infty} \frac{\#\{p \leq N : \alpha \leq \theta_p \leq \beta\}}{\pi(N)} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta \, d\theta,$$

where p is prime and $\pi(N)$ is the prime-counting function.

This conjecture on the number of points on an elliptic curve E can be made into a statement about the L-series of E. The **L-series** of E is defined as

$$L(E/\mathbb{Q}, s) = \prod_{p \text{ is prime}} \frac{1}{L_p\left(\frac{1}{p^s}\right)},$$

where, for each prime p, L_p is a non-zero polynomial in $\mathbb{Q}[t]$ of degree at most 2. For more on L-series, including a precise definition of the polynomials L_p, see [22], [32], or [42].

If $E/\mathbb{Q}$ has "good reduction" at a prime p (see again [22], [32], or [42]), then $L_p(1) = \#E(\mathbb{F}_p)$, which is the value of interest in the Sato-Tate Conjecture.

There are many other important number-theoretic conjectures related to the L-series of an elliptic curve. One of the Clay Mathematics Institute's seven famous Millenium Prize Problems, with a $1,000,000 bounty on its head, is the Birch and Swinnerton-Dyer Conjecture.

Conjecture 1.7 (Birch and Swinnerton-Dyer, [27])**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $L(E/\mathbb{Q}, s)$ has a zero at $s = 1$ of order equal to the rank of $E(\mathbb{Q})$.*

In order to test this conjecture for a given curve $E/\mathbb{Q}$, one may wish to compute $L(E, 1)$, which requires computing $L_p(\frac{1}{p})$ at many primes p, in turn requiring one to count points on many elliptic curves.

Hasse's Theorem has a generalization to higher genus curves (elliptic curves have genus 1) that is easy to state.

Theorem 1.8 (Hasse-Weil, [48])**.** *Let C be an algebraic curve of genus g over a finite field $\mathbb{F}_q$. The number of points on C differs from $q + 1$ by at most $2g\sqrt{q}$. That is,*

$$|\#C(\mathbb{F}_q) - (q + 1)| \leq 2g\sqrt{q}.$$

The Sato-Tate Conjecture and the Birch and Swinnerton-Dyer conjectures (and other L-series-related conjectures not mentioned above, including the Koblitz-Zywina conjecture and

Lang-Trotter conjecture) also have generalizations to higher genus curves [46] [45]. However, on higher-genus curves, $L_p(1)$ is no longer the number of points on the curve, but rather the order of the divisor class group of the curve [24], which is known to be a finite Abelian group. (In the case of elliptic curves, the order of the divisor class group is equal to the number of points on the curve.)

To compute the order of a finite Abelian group, one may first compute the order of an element of that group using an algorithm such as Baby-step/Giant-step or Pollard-Rho. Leveraging Lagrange's Theorem, the order of the element must divide the order of the group. If one has a good estimate in advance for the order of the group, this may be enough to compute this order. The Baby-step/Giant-step and Pollard-Rho algorithms are general algorithms that require that one have another algorithm to perform the group operations in the group whose order one is computing. Thus, in order to compute the order of the divisor class group of a curve, and ultimately to compute terms in the L-series of the curve, we need an algorithm to efficiently carry out addition in the divisor class group.

The above-mentioned conjectures have been studied for genus 1 and genus 2 curves [24]. Attention has turned recently towards studying them on genus 3 curves. Genus 3 algebraic plane curves fall into two categories: hyperelliptic and non-hyperelliptic. Non-hyperelliptic genus 3 curves are also called $C_{3,4}$ curves, a special case of the broader family of $C_{a,b}$ curves. In order to add in the divisor class group of genus 3 curves, we need fast algorithms to compute in the divisor class group of $C_{3,4}$ curves in particular.

The goal of this thesis is find such algorithms. More accurately, the goal of this thesis is to find **explicit formulae** describing arithmetic in a $C_{3,4}$ curve's divisor class group. In brief, a divisor class $[D]$ will typically be represented by a triple of polynomials $\langle f, g, h\rangle$. To find explicit formulae for the sum $[D''] = [D] + [D']$ is to find formulae expressing the coefficients of the polynomials representing $[D'']$ in terms of the coefficients representing $[D]$ and $[D']$. To compare the efficiency of our formulae to earlier works, we will count the number of finite field inversions, multiplications, and additions needed to evaluate these formulae.

1.2 Prior Work

We briefly highlight prior work on genus 3 hyperelliptic curves. For ramified genus 3 hyperelliptic curves, the most efficient published explicit formulae are due to Nyukai [35] [36], who adds divisors in 1I+67M (1 finite field inversion and 67 multiplications) and doubles divisors in 1I+68M. For split genus 3 hyperelliptic curves, Sutherland [45] recently published explicit formulae requiring 1I+79M/1I+82M to add/double. Rezai Rad *et al.* [37] [38] found comparably fast explicit formulae to add/double in the infrastructure of a hyperelliptic curve in 1I+74M+1S/1I+81M (where S denotes squaring in a finite field). The relationship between the divisor class group and the infrastructure is explored in [37] and [38]. Faster hyperelliptic curve arithmetic remains a subject of ongoing research at the University of Calgary.

In [24] and [19], Kedlaya, Harvey, Massierer, and Sutherland use explicit formulae to compute L-series of hyperelliptic curves of genus $g \leq 3$. Sutherland notes in [45] that in earlier attempts at computing L-series using generic divisor arithmetic algorithms (i.e. not using explicit formulae), the majority of the computation time was spent adding and doubling divisors. After moving to optimized, explicit formulae specific to genus 3 hyperelliptic curves, the time spend adding and doubling divisors became "negligible". The benefit of finding explicit formulae describing divisor arithmetic is clear.

Turning now towards the state of $C_{3,4}$ curves, previous work in $C_{3,4}$ curve divisor class group arithmetic has been done with cryptographic applications in mind, as this group may be used in cryptographic primitives based on the Discrete Log Problem. In the cryptographic setting, researchers are interested primarily in $C_{3,4}$ curves defined over very large finite fields of characteristic greater than 3. A $C_{3,4}$ curve over such a field is isomorphic to one given by a short-form equation (see Equation 2.16), yielding faster arithmetic. Moreover, with very high probability, one will only encounter "typical" divisors (see Chapter 7) and many degenerate cases need not be considered. When these assumptions are violated, one may fall back on slower divisor addition algorithms that work on any algebraic curve.

In [25], Khuri-Makdisi describes an algorithm for computing in the divisor class group of

an arbitrary algebraic plane curve, in which divisors are represented by projective embeddings of line bundles. The runtime of this algorithm is polynomial in the genus g of the curve, running in time $O(g^4)$. In [2], Arita gives a $O(g^3)$ algorithm to compute in the divisor class group of an arbitrary $C_{a,b}$ curve, where divisors are identified with polynomial ideals and represented by the Gröbner bases of these ideals. In [18], Harasawa and Suzuki represent divisors by matrices in Hermite normal form, achieving a $O(g^2)$ algorithm.

This is only to highlight the choice of algorithms one might fall back on when the algorithms below fail. The asymptotic runtime of these algorithms are of little interest when we are working with curves of small genus — $C_{3,4}$ curves all have genus 3.

In [3], Arita specializes the algorithm from [2] to the $C_{3,4}$ case. He classifies divisors of $C_{3,4}$ curves into 19 types based on the forms of the Gröbner bases by which they are represented. The algorithm presented allows one to add divisors of any type. This is much more general than the algorithms to follow, requiring 5I+204M/5I+284M. Unlike the algorithms that follow, it allows one to add non-disjoint divisors (e.g. $(P+Q)+(Q+R)$) or double divisors with multiples of a point (e.g. doubling $P+2Q$), although it handles this in a recursive manner that does not terminate over some curves over very small finite fields; Arita was interested in the cryptographic setting over a large finite field.

Other publications are less general but much faster. In [13], Flon *et al.* assume a $C_{3,4}$ curve defined by a short-form polynomial equation (see Equations 2.13 and 2.16). In addition to assuming that divisors are disjoint and have no multiple points, they assume that divisors being added or doubled are typical and mimic techniques from hyperelliptic curve arithmetic — they represent divisors in a manner similar to the Mumford representation used for divisors of hyperelliptic curves, and follow an algorithm similar to Cantor's algorithm (see §10.3 in [15]). The result is an algorithm requiring 2I+148M+15S/2I+165M+20S.

In [40], Abu Salem and Khuri-Makdisi make the same assumptions as in [13]. They represent divisors by a pair of polynomials of minimal degree and compute sums of divisors by computing kernels of maps between vector spaces in 2I+117M/2I+129M. In an

appendix in [26], Khuri-Makdisi gives an improvement bringing the operation count down to 2I+98M/2I+110M.

1.3 Contributions of the Thesis

The goal of this thesis is to marry the methods of Abu Salem and Khuri-Makdisi — who have the fastest explicit formulae to date — with the methods of Arita — whose formulae are the most general — in order to produce fast and fully general explicit formulae describing all cases of $C_{3,4}$ curve arithmetic. More specifically,

- the curve equation may be over a finite field of any size, small or large;
- the curve equation may be over a field of any characteristic, including 0, 2, and 3;
- the curve equation may be in long or short form;
- divisors may be typical or atypical;
- divisors may have multiple points;
- divisors may be non-disjoint;
- and algorithms must provably terminate.

This marriage of methods is facilitated by the fact that Salem/Khuri-Makdisi's representation of typical divisors resembles type 31 divisors from Arita's classification.

All of these goals are attained in this thesis. Fully general algorithms for adding, doubling and reducing divisors are presented in Chapters 8 through 10. These algorithms are used to develop fast explicit formulae in Chapter 11 handling the most typical cases[3] arising in $C_{3,4}$ curve divisor arithmetic. The operation counts of these formulae are summarized in Table 1.1, where I, M, S, A refer to the number of inversions, multiplications, squarings, and additions in a finite field required to evaluate them. The trade-off between inversions and multiplications is discussed in Chapter 11. The algorithms are also used to produce explicit

[3] Specifically, adding/doubling disjoint typical divisors on a curve in short form over a field of characteristic greater than 3.

formulae for all atypical cases[4] as well, though these cases are so numerous that we choose instead to publish them in the form of Sage code on GitHub [30] and present their operation counts in Chapter 12.

Table 1.1: Comparison of operation counts in prior work

	Add				Double			
	I	M	S	A	I	M	S	A
Arita	5	204	–	–	5	284	–	–
Flon et al	2	148	15	–	2	165	20	–
Khuri-Makdisi/Abu Salem	2	98	1	132	2	110	3	155
MacNeil	1	111	3	99	1	135	3	116

By improving upon the typical case and completing the picture for the atypical cases, this thesis will have a significant impact on number theoretic computations heavy on group arithmetic in the divisor class group of a $C_{3,4}$ curve. As is the case in [46], one may wish to take a curve over $\mathbb{Q}$, reduce it modulo all primes up to some bound, and compute the order of the divisor class group of that reduced curve. The improvement in the typical case remains significant over all of the computations, while the completion of the atypical cases becomes more significant over the smaller primes, where one frequently bumps into these atypical cases.

A full implementation in Sage of the arithmetic presented in this thesis is available at [30]. This implementation has been tested by unit tests as well as by adding and doubling a large number of randomly chosen divisors and comparing the results to Sage's own provided ideal arithmetic.

1.4 Thesis Outline

We begin by reviewing some background material necessary for understanding this thesis. Familiarity with common algebraic structures — including monoids, groups, rings, fields, modules, and vector spaces — is assumed. In Chapter 2, we define curves generally and $C_{3,4}$

[4] Including non-disjoint or atypical divisors and curves of arbitrary form and characteristic.

curves specifically, as well as related objects, such as a curve's coordinate ring. In Chapter 3, we review Gröbner bases, which are central to Arita's representation of divisors, which we have adopted here. In Chapter 4, we review differentials, which arise when doubling divisors. In Chapter 5, we introduce divisors and the divisor class group of a $C_{3,4}$ curve.

In Chapters 6 and 7, we continue to present background theory, though we give alternative proofs of known results. This is to avoid invoking the theory of algebraic varieties and schemes or Riemann-Roch spaces, requiring instead only an understanding of more basic algebraic structures. In Chapter 6, we introduce the ideal class group and exhibit an isomorphism between the divisor class group and the ideal class group. We use this isomorphism in Chapter 7 to represent divisors by ideals, in turn represented by reduced Gröbner bases. We then define what it means for a divisor to be reduced or typical and prove several properties of these divisors.

This thesis' original results begin with Chapter 8, where we present a generalization of Khuri-Makdisi and Abu Salem's algorithms [40, 26] to accomplish the goals outlined in the previous section. Chapters 8, 9, and 10 describe algorithms for adding, doubling, and reducing divisors, respectively. In Chapter 11, we examine the most common cases arising when adding and doubling divisors and present fast explicit formulae optimized for these particular cases. The Sage implementations of the formulae presented in Chapter 11 is compared to an implementation of the Abu Salem and Khuri-Makdisi's formulae from [40] and [26] in Chapter 12, where we conclude that this thesis represents a significant improvement over the current state-of-the-art. Operation counts for the atypical cases are also presented in Chapter 12. The results and contributions of this thesis are summarized in the concluding Chapter 13.

2 $C_{3,4}$ Curves

In this chapter, we define the central object of this thesis, $C_{3,4}$ curves. We begin by describing curves more generally, as well as objects related to curves, such as their coordinate rings, function fields, and discrete valuations. In the final section of this chapter, we will define a family of curves called $C_{a,b}$ curves, of which $C_{3,4}$ curves are a special case. The definitions found in this chapter relating to affine and projective space, curves, and coordinate rings may be found in many references on algebraic curves. See, for example, Chapters 5 and 7 in [15], Chapters 1–3 in [28], or Chapter 3 in [47].

All fields will be assumed to be perfect. A field K is called **perfect** if every K-irreducible polynomial in $K[x]$ has distinct roots in $\overline{K}$. There are many other characterizations of perfect fields (see [21]), but this is the definition that will best suit our needs in chapters to come. Every algebraically closed field, every field of characteristic 0 (e.g. $\mathbb{Q}$, $\mathbb{C}$) and every finite field (e.g. $\mathbb{F}_q$) is perfect.

2.1 Algebraic Plane Curves

Let K be a field. The **affine plane over** K, denoted by $\mathbb{A}^2_K$, is the set

$$\mathbb{A}^2_K = K^2.$$

If L/K is an algebraic extension, then $\mathbb{A}^2_K \subseteq \mathbb{A}^2_L$. The **projective plane over** K, denoted by $\mathbb{P}^2_K$, is the set of lines in K^3 through the origin. This may be constructed as the set of points in K^3 other than the origin, modulo an equivalence relation whereby two points are equivalent if and only if they are colinear with the origin. That is,

$$\mathbb{P}^2_K = (K^3 - \{(0,0,0)\})/\sim$$

where

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \iff \exists k \in \overline{K} : (x_1, y_1, z_1) = (kx_2, ky_2, kz_2). \tag{2.1}$$

The equivalence class of a point (x, y, z) is denoted by $(x : y : z)$. If L/K is an algebraic extension, then $\mathbb{P}^2_K \subseteq \mathbb{P}^2_L$.

There is a bijection between $\mathbb{A}^2_L$ and the points in $\mathbb{P}^2_L$ whose third coordinates are non-zero.

$$\phi : \mathbb{A}^2_L \to \mathbb{P}^2_L - \{(x : y : 0) \mid x, y \in L\}$$

$$\phi(x, y) = (x : y : 1)$$
$$\phi^{-1}(x : y : z) = \left(\frac{x}{z}, \frac{y}{z}\right)$$

It is straightforward to show that ϕ^{-1} is well-defined.

Let $f(x, y) \in K[x, y]$ be a polynomial. The **homogenization** of f is the homogeneous polynomial

$$F(X, Y, Z) = Z^{\deg f} f\left(\frac{X}{Z}, \frac{Y}{Z}\right) \in K[X, Y, Z].$$

The homogenization of $0 \in K[x, y]$ is $0 \in K[X, Y, Z]$. For any homogeneous polynomial $F(X, Y, Z) \in K[X, Y, Z]$, the **dehomogenization** of F is the polynomial

$$f(x, y) = F(x, y, 1).$$

The polynomial f might no longer be homogeneous. The homogenization and dehomogenization operations are mutual inverses.

A **projective algebraic plane curve** over K is a set of points

$$C_F : \{(x_0 : y_0 : z_0) \in \mathbb{P}^2_{\overline{K}} \mid F(x_0, y_0, z_0) = 0\},$$

for some homogeneous polynomial $F \in K[X, Y, Z]$. It is the set of points in $\mathbb{P}^2_{\overline{K}}$ at which F

is zero. Notice that this includes points in the algebraic closure of K. The **affine model** of C_F is the set of points $P \in \mathbb{A}^2_{\overline{K}}$ at which f is zero, together with the **points at infinity**, which are in bijection with the intersection of C_F with the projective line $Z = 0$. The points in C_f are in bijection with the points in C_F. An **affine algebraic plane curve** C_f over K is the affine model of a projective algebraic plane curve C_F. The **projective closure** of C_f is C_F.

Because affine and projective algebraic plane curves are so closely related, essentially two representations of the same object, we shall refer to both simply as **curves**. We will define curves by their affine model, i.e. by a polynomial $f \in K[x, y]$. When the defining polynomial is clear in context, we shall omit the subscript and write C rather than C_f.

Although we will define curves by their affine model, we will usually denote points on the curve by their projective coordinates, in the form $(x : y : z)$. By the equivalence relation on projective points, every point in C can be written uniquely in one of the three reduced forms $(x : y : 1)$, $(x : 1 : 0)$ or $(1 : 0 : 0)$. Points of the form $(x : y : 1)$ are **finite points**, while all other points with z-coordinate 0 are **points at infinity**.

If $L \supseteq K$ is an algebraic extension, then the set $C(L)$ of L-rational points on C is

$$C(L) = C \cap \mathbb{P}^2_L.$$

These are the points on C that are equivalent (via the relation in 2.1) to a point with coordinates all in L. Equivalently, these are the points on C whose representations in reduced form have coordinates in L. If C is defined over K, then the K-rational points are simply called **rational**.

A curve $C = C_f$ is **irreducible** if f is $\overline{K}$-irreducible, i.e. if f cannot be written as a product $f = gh$ of lower-degree non-constant polynomials $g, h \in \overline{K}[x, y]$. If P is a point on C, then P is called **singular** if all formal partial derivatives of the homogenization F of f vanish at P. In this case, the tangent line to C at P does not exist.[5] The curve C is

[5] In this case, one might be interested in the Zariski tangent space instead.

called **singular** if it has at least one singular point. Otherwise C is called **non-singular** or **smooth**. Some authors require that algebraic curves be irreducible and sometimes smooth. Our definition of $C_{3,4}$ curves below will require these conditions.

Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ be an automorphism on $\overline{K}$ that fixes K. Then σ also acts on $\mathbb{A}^2_{\overline{K}}$ and $\mathbb{P}^2_{\overline{K}}$ via

$$\begin{aligned} \sigma((x_0, y_0)) &= (\sigma(x_0), \sigma(y_0)) \\ \sigma((X_0 : Y_0 : Z_0)) &= (\sigma(X_0) : \sigma(Y_0) : \sigma(Z_0)). \end{aligned} \tag{2.2}$$

It is easily verified that the action on $\mathbb{P}^2_{\overline{K}}$ is well-defined. If $P \in \mathbb{A}^2_{\overline{K}}$ or $P \in \mathbb{P}^2_{\overline{K}}$, then define the **orbit** of P to be

$$\mathrm{orb}(P) := \{\sigma(P) \mid \sigma \in \mathrm{Gal}(\overline{K}/K)\}.$$

Lemma 2.3. *Let $f \in K[x, y]$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Let $P = (x_0, y_0)$ be a point in $\overline{K} \times \overline{K}$. Then*

$$f(\sigma(x_0), \sigma(y_0)) = \sigma(f(x_0, y_0)).$$

Proof.

$$\begin{aligned} f(\sigma(x_0), \sigma(y_0)) &= \sum a_{i,j}\sigma(x)^i\sigma(y)^j \\ &= \sum \sigma(a_{i,j})\sigma(x)^i\sigma(y)^j && \sigma \text{ fixes } K \\ &= \sum \sigma(a_{i,j}x^iy^j) && \sigma \text{ is multiplicative} \\ &= \sigma\left(\sum a_{i,j}x^iy^j\right) && \sigma \text{ is additive} \\ &= \sigma(f(x_0, y_0)). \end{aligned}$$

□

Corollary 2.4. *Let $f \in K[x, y]$. Then f is zero at P if and only if f is zero at every point in* orb P.

2.2 The Coordinate Ring and Function Field

We will work a lot with the coordinate rings of $C_{3,4}$ curves. After defining divisors of $C_{3,4}$ curves in Chapter 5, we will show in 6 that divisors on a curve are in bijection with non-zero ideals of the curve's coordinate ring. When adding divisors, we will in fact use this bijection to work in the coordinate ring, where the arithmetic is computationally easier.

Let C be a curve over a field K, defined by a polynomial $F \in K[x, y]$. The **coordinate ring** of C, denoted by $K[C]$, is the quotient ring

$$K[C] := \frac{K[x, y]}{\langle F \rangle}.$$

It is the ring of bivariate polynomials over K, modulo the principal ideal generated by the curve's defining polynomial.

It is a well-known fact in algebraic geometry that, if C is given by an irreducible polynomial, its coordinate ring is a Dedekind domain (see §8.2 of [15] or Proposition 8.1 of [34]). Therefore all non-zero ideals of $K[C]$ may be uniquely factored into a product of prime ideals. The coordinate ring has Krull dimension 1, meaning that every non-zero prime ideal is a maximal ideal (Theorem VIII.6.5 in [21]).

The **function field** $K(C)$ of C is the field of fractions of the coordinate ring,

$$K(C) := \text{Frac}(K[C]).$$

We will not work much with the function field itself. We will use it in Chapter 6 in defining the ideal class group, though one of the goals of Chapter 6 is to show that we can work entirely in $K[C]$.

2.3 Local Rings and Valuations

There is a correspondence between closed points[6] on a curve and maximal ideals of its coordinate ring. To each maximal ideal is associated a valuation function that allows one to compute the order of the zero or pole of a function along the curve. In particular, valuations allow one to compute the multiplicity of the intersection of a polynomial with the curve, the geometric notion of contact. When defining divisors in Chapter 5, we will also define the divisor of a function, which records the zeroes and poles of the function along a $C_{3,4}$ curve, along with their orders. We will therefore need to know how to compute these.

Let $K[C]$ be the coordinate ring of an irreducible smooth curve C. Let $\mathfrak{p}$ be a non-zero prime ideal of $K[C]$. We may localize $K[C]$ at the prime ideal $\mathfrak{p}$ to get $K[C]_{\mathfrak{p}}$, the **ring of regular functions at** $\mathfrak{p}$, which is usually denoted by $\mathcal{O}_{\mathfrak{p}}$ instead. This can be defined more explicitly by

$$\mathcal{O}_{\mathfrak{p}} = \left\{ \frac{f}{g} \in K(C) \mid g \notin \mathfrak{p} \right\}.$$

This ring is a local ring, meaning that it has a unique maximal ideal, denoted by $\mathfrak{m}_{\mathfrak{p}}$. Specifically, $\mathfrak{m}_{\mathfrak{p}}$ is

$$\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \left\{ \frac{f}{g} \in K(C) \mid f \in \mathfrak{p},\ g \notin \mathfrak{p} \right\}.$$

Now let P be a finite point on C. Then P induces a prime ideal $\mathfrak{p} = \{f \in K[C] \mid f(P) = 0\}$. Define the **ring of regular functions at** P to be the ring $\mathcal{O}_P := \mathcal{O}_{\mathfrak{p}}$, where $\mathfrak{p}$ is the prime ideal induced by P. Its unique maximal ideal is $\mathfrak{m}_P := \mathfrak{m}_{\mathfrak{p}}$. Explicitly,

$$\mathcal{O}_P = \left\{ \frac{f}{g} \in K(C) \mid g(P) \neq 0 \right\}$$
$$\mathfrak{m}_P = \left\{ \frac{f}{g} \in K(C) \mid f(P) = 0,\ g(P) \neq 0 \right\}.$$

Given a non-zero prime ideal $\mathfrak{p}$, $\mathcal{O}_{\mathfrak{p}}$ is not only a local ring, but also a discrete valuation

[6] The "closed points" are in fact the orbits defined in Section 2.1. This correspondence is shown in Theorem 6.8.

ring, or DVR (Theorem VIII.6.10 in [21]). Rather than define here what discrete valuations and DVRs are in general, we briefly describe the valuation of a function at a prime ideal, For more on DVRs, see Chapter 11 of [11].

Let $f \in K[C]$. The **order** or **valuation** of f at $\mathfrak{p}$, denoted $\nu_{\mathfrak{p}}(f)$, is

$$\nu_{\mathfrak{p}}(f) := \max\{r \in \mathbb{N} \mid f \in \mathfrak{m}_P^r\},$$

if f is not identically 0. The order of 0 at $\mathfrak{p}$ is defined as $\nu_{\mathfrak{p}}(0) = \infty$. Given two polynomials $f, g \in K[C]$, $\nu_{\mathfrak{p}}$ satisfies the relation

$$\nu_{\mathfrak{p}}(fg) = \nu_{\mathfrak{p}}(f) + \nu_{\mathfrak{p}}(g),$$

as long as we define $\infty + \infty = \infty$ and $\infty + n = \infty$ for all $n \in \mathbb{Z}$. We can extend this to polynomials in $K(C)$. Let $f/g \in K(C)$ and define

$$\nu_{\mathfrak{p}}\left(\frac{f}{g}\right) = \nu_{\mathfrak{p}}(f) - \nu_{\mathfrak{p}}(g).$$

This map is well-defined, for if $\frac{f}{g} = \frac{h}{k}$, then

$$\begin{aligned} fk &= gh \\ \nu_{\mathfrak{p}}(fk) &= \nu_P(gh) \\ \nu_{\mathfrak{p}}(f) + \nu_P(k) &= \nu_{\mathfrak{p}}(g) + \nu_{\mathfrak{p}}(h) \\ \nu_{\mathfrak{p}}(f) - \nu_P(g) &= \nu_{\mathfrak{p}}(h) - \nu_{\mathfrak{p}}(k) \\ \nu_{\mathfrak{p}}\left(\frac{f}{g}\right) &= \nu_{\mathfrak{p}}\left(\frac{h}{k}\right). \end{aligned}$$

Analogously for a finite point P on a curve, we may define the order of $f/g \in K(C)$ at P by letting $\mathfrak{p}$ be the prime induced by P and invoking the definition above, i.e. $\nu_P := \nu_{\mathfrak{p}}$, where $\mathfrak{p}$ is the prime ideal induced by P.

There are various ways in which we might go about defining the valuation at a point at infinity of a curve. We will defer defining the valuation there until the end of the chapter. When so doing, we will make use of the following:

Proposition 2.5. *Let $\mathcal{O}_\mathfrak{p}$ be a discrete valuation ring with valuation $\nu_\mathfrak{p}$. For all $f, g \in K(C)$,*

$$\nu_\mathfrak{p}(f+g) \geq \min\{\nu_\mathfrak{p}(f) + \nu_\mathfrak{p}(g)\}.$$

If $\nu_\mathfrak{p}(f) \neq \nu_\mathfrak{p}(g)$, then

$$\nu_\mathfrak{p}(f+g) = \min\{\nu_\mathfrak{p}(f) + \nu_\mathfrak{p}(g)\}.$$

Proof. Lemma 1.1.2 in [16]. □

It is an important fact that the valuation of a function $f \in K(C)$ at a point P agrees with the intersection number of f and C at P. (See property 8 of the intersection number on p.40 of [14].) If $\nu_P(f) = n > 0$, we say that f intersects C at P with multiplicity n, or that f has a zero of order n at P. If $\nu_P(f) = n < 0$, we say that f has a pole of order n at P. The function f passes through P if and only if $\nu_P(f) \geq 1$, and is tangent to C at P if and only if $\nu_P(f) \geq 2$.

Proposition 2.6. *Let $\mathcal{O}_\mathfrak{p}$ be a discrete valuation ring with valuation $\nu_\mathfrak{p}$.*

(i) The maximal ideal of $\mathcal{O}_\mathfrak{p}$ is a principal ideal, $\mathfrak{m}_\mathfrak{p} = \langle u \rangle$ for some $u \in \mathcal{O}_\mathfrak{p}$.

(ii) For any non-zero $f \in K(C)$, $\nu_\mathfrak{p}(f) = n$ if and only if $f = su^n$ for some $s \in \mathcal{O}_\mathfrak{p}^*$.

Proof. Lemmas 7.3.1 and 7.4.7 in [15]. □

The generator u of $\mathfrak{m}_\mathfrak{p}$ is called a **uniformizer** or **local parameter** at $\mathfrak{p}$. Uniformizers are not unique. Any element $u \in \mathfrak{m}_\mathfrak{p} - \mathfrak{m}_\mathfrak{p}^2$, i.e. any element u for which $\nu_\mathfrak{p}(u) = 1$ is a uniformizer. For a point P, this means any function u that passes through but is not tangent to C at P is a uniformizer.

A consequence of Corollary 2.4 from the previous section is that if $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and P is an affine point on C, then P and $\sigma(P)$ induce the same prime ideal $\mathfrak{p}$. Thus we have

Proposition 2.7. *Let P be an affine point on C and let $\mathfrak{p} = \{f \in K[C] \mid f(P) = 0\}$. Then for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $f \in K(C)$,*

$$\nu_P(f) = \nu_{\sigma(P)}(f) = \nu_{\mathfrak{p}}(f).$$

2.4 $C_{3,4}$ Curves

A $C_{3,4}$ curve is a special case of the broader class of $C_{a,b}$ curves. The class of $C_{3,4}$ curves was first described by Miura [33]. One definition is the following (an equivalent characterization will come at the end of this chapter).

Definition 2.8. A $C_{a,b}$ **curve** over a field K is an algebraic projective plane curve C over K that is non-singular everywhere except possibly at its points[7] at infinity, given by a polynomial $F \in K[x, y]$ of the form

$$F = \sum_{\substack{0 \le i \le b \\ 0 \le j \le a \\ ai + bj \le ab}} c_{i,j} x^i y^j \tag{2.9}$$

where $0 < a < b$ are coprime and $c_{b,0}$ and $c_{0,a}$ non-zero.

Here is a useful visualization of Equation 2.9. The monomials in C's defining polynomial F correspond to integer points in or on the boundary of the triangle[8] with corners $(0, 0)$, $(0, a)$, and $(b, 0)$.

Proposition 2.10. *A $C_{a,b}$ curve only has one point at infinity.*

Proof. It is easy to see F has degree b and that $c_{b,0}x^b$ is the only term in F of degree

[7] Although we will see shortly that there is only one point at infinity.
[8] This is the Newton polygon of F.

b. Let $\overline{F}(X, Y, Z)$ be the homogenization of $F(x, y)$ and evaluate $\overline{F}$ at $Z = 0$. We get $\overline{F}(X, Y, 0) = c_{b,0}X^b$.

Now suppose $(u : v : 0)$ is a point at infinity on the curve. Then $\overline{F}(u, v, 0) = c_{b,0}u^b = 0$, so $u = 0$ and $(u : v : 0) = (0 : v : 0) = (0 : 1 : 0)$. □

We will denote the unique point at infinity on a $C_{a,b}$ curve by P_∞.

A few special cases of $C_{a,b}$ curves are worth mentioning. When $a = 2$ and $b = 3$, we get an elliptic curve. When $a = 2$ and $b = 7$, we get a genus 2 ramified hyperelliptic curve. See Equations 1.1 and 1.2. More generally, for $g \geq 2$, when $a = 2$ and $b = 2g+1$, we get a genus g ramified hyperelliptic curve. More importantly in this thesis, when $a = 3$ and $b = 4$, we get a $C_{3,4}$ curve.

Definition 2.11. A $C_{3,4}$ **curve** over a field K is a smooth projective algebraic plane curve given by an affine equation[9]

$$F = c_{10}y^3 + c_9x^4 + c_8xy^2 + c_7x^2y + c_6x^3 + c_5y^2 + c_4xy + c_3x^2 + c_2y + c_1x + c_0,$$

where c_9 and c_{10} are non-zero.

Definition 2.11 may appear to be slightly more restrictive than Definition 2.8 — Definition 2.11 does not allow for the point at infinity to be singular. In fact, the point P_∞ on a $C_{3,4}$ is never singular.

Proposition 2.12. *Let C be a $C_{3,4}$ curve over a field K. The point P_∞ is non-singular.*

Proof. To show that C is non-singular at P_∞, we show that one of the formal partial derivatives of F, the defining polynomial of C, is non-zero at P_∞. Since P_∞ is not a finite point,

[9] The subscripts on the coefficients of C are numbered according to the $C_{3,4}$ monomial order, Definition 3.4.

this requires that we work with the homogenization, $\overline{F}$, of C's defining polynomial,

$$\begin{aligned}\overline{F} = c_{10}Y^3Z + c_9X^4 + c_8XY^2Z + c_7X^2YZ + c_6X^3Z + c_5Y^2Z^2 \\ + c_4XYZ^2 + c_3X^2Z^2 + c_2YZ^3 + c_1XZ^3 + c_0Z^4.\end{aligned}$$

The formal partial derivative of $\overline{F}$ with respect to Z is

$$\begin{aligned}\overline{F}_Z = c_{10}Y^3 + c_8XY^2 + c_7X^2Y + c_6X^3 + 2c_5Y^2Z \\ + 2c_4XYZ + 2c_3X^2Z + 3c_2YZ^2 + 3c_1XZ^2 + 4c_0Z^3.\end{aligned}$$

Evaluated at P_∞, $\overline{F}_Z(0,1,0) = c_{10} \neq 0$. □

We will make some simplifying assumptions on the curve equation. We may assume that both c_9 and c_{10} are 1. Otherwise, multiplying the whole curve equation by $\frac{c_9^3}{c_{10}^4}$ and performing the invertible change of coordinates $X = \frac{c_9}{c_{10}}x$ and $Y = \frac{c_9}{c_{10}}y$ gives a curve equation in which the coefficients of X^4 and Y^3 are 1. In light of this, we now assume the curve equation of C is of the **long form**

$$F = y^3 + x^4 + c_8xy^2 + c_7x^2y + c_6x^3 + c_5y^2 + c_4xy + c_3x^2 + c_2y + c_1x + c_0. \tag{2.13}$$

In fields of sufficiently large characteristic, one may also assume certain coefficients of F are zero. If $\operatorname{char} K \neq 2$, then the invertible change of variables $x = X - \frac{c_6}{4}, y = Y$ gives

$$F(X,Y) = Y^3 + X^4 + d_8XY^2 + d_7X^2Y + d_5Y^2 + d_4XY + d_3X^2 + d_2Y + d_1X + d_0, \tag{2.14}$$

for some new coefficients d_i. Notice that the X^3 term vanishes. If $\operatorname{char} K \neq 3$, then the invertible change of variables $x = X, y = Y - \frac{c_8X + c_5}{3}$ gives

$$F(X,Y) = Y^3 + X^4 + d_7X^2Y + d_6X^3 + d_4XY + d_3X^2 + d_2Y + d_1X + d_0, \tag{2.15}$$

where there is no Y^2 or XY^2 term. If the characteristic of K is neither 2 nor 3, we may perform both substitutions simultaneously. Let

$$a = \frac{27c_6 - 9c_7c_8 + 2c_8^3}{27}$$

and perform the change of variables

$$\begin{aligned} x &= X - \frac{a}{4} \\ y &= Y - \frac{c_8}{3}X + \frac{ac_8 - 4c_5}{12}. \end{aligned}$$

Then this gives C in **short form**

$$F(X,Y) = Y^3 + X^4 + d_7X^2Y + d_4XY + d_3X^2 + d_2Y + d_1X + d_0. \tag{2.16}$$

We now address the valuation at P_∞ on a $C_{3,4}$ curve. We define ν_{P_∞} in terms of a uniformizer. Following §7.3 of [15], a uniformizer of $\mathfrak{m}_{P_\infty}$ is $\frac{x}{y}$. Thus $\nu_{P_\infty}\left(\frac{x}{y}\right) = 1$. From this, we can deduce the pole orders of x and y at P_∞.

Proposition 2.17. *Let P_∞ be the point at infinity of a $C_{3,4}$ curve C over K. The pole orders of $x, y \in K[C]$ are*

$$\nu_{P_\infty}(x) = -3 \quad \textit{and} \quad \nu_{P_\infty}(y) = -4.$$

Proof. First, we note that $\nu_{P_\infty}\left(\frac{x}{y}\right) = 1$ implies $\nu_{P_\infty}(x) = \nu_{P_\infty}(y) + 1$. Next,

$$\begin{aligned}
3\nu_{P_\infty}(y) &= \nu_{P_\infty}(y^3) \\
&= \nu_{P_\infty}(-x^4 - c_8xy^2 - c_7x^2y - \ldots - c_0) \\
&= \min\{\nu_{P_\infty}(-x^4), \nu_{P_\infty}(-c_8xy^2), \nu_{P_\infty}(-c_7x^2y), \ldots, \nu_{P_\infty}(-c_0)\} \qquad \text{Prop. 2.5} \\
&= \min\{\nu_{P_\infty}(x^4), \nu_{P_\infty}(xy^2), \nu_{P_\infty}(x^2y), \ldots, \nu_{P_\infty}(1)\} \\
&= \min\{\nu_{P_\infty}(x^4), \nu_{P_\infty}(xy^2), \nu_{P_\infty}(x^2y)\}
\end{aligned}$$

The minimum of these three is $\nu_{P_\infty}(x^4)$, for assuming otherwise leads to a contradiction. For example, if $3\nu_{P_\infty}(y) = \nu_{P_\infty}(xy^2)$, then $\nu_{P_\infty}(y) = \nu_{P_\infty}(x)$, which contradicts $\nu_{P_\infty}(x) = \nu_{P_\infty}(y) + 1$. So

$$3\nu_{P_\infty}(y) = \nu_{P_\infty}(x^4) = 4\nu_{P_\infty}(x) = 4(\nu_{P_\infty}(y) + 1),$$

which gives $\nu_{P_\infty}(y) = -4$, and

$$\nu_{P_\infty}(x) = \nu_{P_\infty}(y) + 1 = -4 + 1 = -3.$$

□

In general, for a $C_{a,b}$ curve, $\nu_{P_\infty}(x) = -a$ and $\nu_{P_\infty}(y) = -b$. In fact, this is another characterization of $C_{a,b}$ curves.

Theorem 2.18. *Let C be an affine plane curve over K (not necessarily smooth or irreducible). Let $0 < a < b$ be coprime positive integers. The following are equivalent.*

(i) C is a $C_{a,b}$ curve.

(ii) C is irreducible, has exactly one rational point P_∞ at infinity, $\nu_{P_\infty}(x) = -a$, and $\nu_{P_\infty}(y) = -b$.

Proof. Originally proved by Miura in [33]. An English translation of the proof is provided by Matsumoto in [31]. □

3 Gröbner Bases

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K and let I be an R-ideal. A Gröbner basis for I is a set $\{g_1, \ldots, g_m\}$ of generators of I satisfying some additional properties (see Definition 3.12). Every R-ideal has a Gröbner basis and likely has many Gröbner bases. However, once we define the notion of a *reduced* Gröbner basis, every ideal will have a unique reduced Gröbner basis and two ideals will be equal if and only if their reduced Gröbner bases are equal.

Gröbner bases aid us in several ways. For one, reduced Gröbner bases give us a unique representation for ideals of polynomial rings and a way to test equality of ideals. Gröbner bases are always defined in terms of an ordering on monomials of R. One of the elements of the basis will be minimal with respect to that order, and this minimal polynomial will play an important role in the divisor arithmetic described beginning in Chapter 8. The whole basis is minimal, in a sense; the leading monomial of any polynomial in I is divisible by the leading monomial of a basis element, though the notion of a leading monomial depends on an ordering on monomials. Gröbner bases also facilitate computations in R/I and they induce a basis for R/I as a K-vector space.

We begin by describing the monomial orderings underlying Gröbner basis theory.

3.1 Monomial Orderings

As before, we will assume $R = K[x_1, \ldots, x_n]$, but the concepts in this subsection generalize to polynomial rings $R = S[x_1, \ldots, x_n]$ for a ring S, or even to free S-modules with a basis. (See Chapter 15.2 in [11]).

When we write down a polynomial in one variable, we typically write the terms in increasing or decreasing order according to the terms' degrees. One might write $3x^2 + x + 2$ or $2 + x + 3x^2$, for example, but typically not $x + 3x^2 + 3$. It is natural to order terms according to their powers.

In a multivariate polynomial ring, there is no one "natural" way to order terms. One could write an arbitrary bivariate quadratic in the order

$$ax^2 + bxy + cy^2 + dx + ey + f.$$

Here, terms are ordered according to their total degree. Monomials of degree 2 come before those of degree 1, which in turn come before those of degree 0. Within terms of the same degree, we write first the ones with the highest degree in x. This is called a **degree lexicographic order** or **graded lexicographic order**. We could get a different graded lexicographic order by prioritizing y over x among terms having the same degree, e.g.

$$cy^2 + bxy + ax^2 + ey + dx + f.$$

In some contexts, it makes sense to collect powers of y and write instead

$$cy^2 + bxy + ey + ax^2 + dx + f.$$

This occurs in the context of, say, hyperelliptic curves, which are typically defined as the set of solutions to an equation

$$y^2 + h(x)y = f(x) \quad \text{or} \quad y^2 + h(x)y - f(x) = 0.$$

Here, we first write the terms with the highest degree in y. Within the terms having the same degree in y, we write first the terms having the highest degree in x. This is a **lexicographical order**. Prioritizing x over y would yield a different lexicographical order,

$$ax^2 + bxy + dx + cy^2 + ey + f.$$

The two orders described above are examples of monomial orders.

Definition 3.1 (Chapter 15.2 [11])**.** Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring. The **set of (monic) monomials** of R is the set

$$\mathcal{M}_R := \left\{ \prod_{i=1}^{n} x_i^{k_i} \mid k_i \in \mathbb{N} \right\}.$$

A **monomial order** is a total order $\leq$ on $\mathcal{M}_R$ such that for all monomials $a, b, c \in \mathcal{M}_R$:

(i) $1 \leq a$, and

(ii) $a \leq b \implies ac \leq bc$.

Property (i) says that the order has a least element, specifically 1, and property (ii) asserts compatibility with multiplication. Some authors define a monomial order to be a well-order (e.g. Chapter 2.2 in [8]), but well-orderedness is a consequence of properties (i) and (ii).

Proposition 3.2. *Let $(\mathcal{M}_R, \leq)$ be a monomial order. Then $(\mathcal{M}_R, \leq)$ is a well-order.*

Proof. Lemma 15.2 in [11]. □

It was said above that in a univariate polynomial ring $K[x]$, it is "natural" to order monomials by their degree in x. That is because it is the *only* monomial order on $\mathbb{K}[x]$.

Proposition 3.3. *There is only one monomial order on $K[x]$:*

$$1 < x < x^2 < \ldots.$$

Proof. Necessarily, $1 < x$ by property (i) of Definition 3.1. By property (ii), $1 < x$ implies $x < x^2$. The rest follows by induction. □

Thus it is fair to call this order the natural order on monomials of $K[x]$.

In addition to the lexicographic and degree lexicographic orders mentioned already, there is also a monomial order called a **weight order**. Monomials in a polynomial ring $R =$

$K[x_1, \ldots, x_n]$ are in bijection with vectors in $\mathbb{N}^n$, via

$$x_1^{v_1} \ldots x_n^{v_n} \longleftrightarrow (v_1, \ldots, v_n).$$

For a vector $v \in \mathbb{N}^n$, denote its associated monomial by

$$x^v := x_1^{v_1} \ldots x_n^{v_n}.$$

Given a vector $w \in \mathbb{R}^n$, we can define a partial order $<_w$ on $\mathcal{M}_R$ whereby

$$x^u <_w x^v \iff u \cdot w < v \cdot w.$$

Here, the $\cdot$ denotes the dot product in $\mathbb{R}^n$ and the vector w is called a **weight vector**. It is straightforward to show that this order satisfies properties (i) and (ii) of a monomial order, though it is not necessarily total. In the event that $x^u = x^v$, we can break the tie by refining by a second weight vector, w':

$$x^u <_{w,w'} x^v \iff u \cdot w < v \cdot w \text{ or } (u \cdot w = v \cdot w \text{ and } u \cdot w' < v \cdot w').$$

Having n $\mathbb{R}$-linearly independent weight vectors is sufficient (but not necessary) to break all ties, yielding a total monomial order. A single weight vector $w = (w_1, \ldots, w_n) \in \mathbb{R}^n$ alone yields a total order when the w_i's are $\mathbb{Q}$-linearly independent.

Every monomial order on $R[x_1, \ldots, x_n]$ is a weight order given by at most n $\mathbb{R}$-linearly independent weight vectors in $\mathbb{R}^n$ (see [39] and Exercises 2.4.11 and 2.4.12 in [8]). For example, the lexicographic ordering on $R = K[x_1, \ldots, x_n]$ with $x_n < \cdots < x_1$ is given by the rows of the $n \times n$ identity matrix I_n. The graded lexicographic ordering with $x_n < \cdots < x_1$

is given by the rows of

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

In [2], [4], and [18], the authors perform arithmetic in the divisor class group of $C_{a,b}$ curves by associating divisors with polynomial ideals and computing their reduced Gröbner bases. Their chosen monomial order on $K[x, y]$ is one they define as the $C_{a,b}$ **order**,

Definition 3.4. Let $R = K[x, y]$. The $C_{a,b}$ **order** on R is the monomial order on R determined by the rows of the matrix

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

The $C_{a,b}$ order may also be seen as ordering monomials according to their pole orders at infinity on a $C_{a,b}$ curve, with ties broken according to their degrees in y.

$$m < m' \iff \begin{array}{l} -\nu_{P_\infty}(m) < -\nu_{P_\infty}(m') \text{ or} \\ (-\nu_{P_\infty}(m) = -\nu_{P_\infty}(m') \text{ and } \deg_y(m) < \deg_y(m')). \end{array}$$

Example 3.5. The first few monomials of the $C_{2,3}$ order are

$$1 < x < y < x^2 < xy < x^3 < y^2 < x^2y < x^4 < xy^2 < \dots.$$

On monomials less than x^3 and y^2, this order agrees with the degree lexicographic order with $x < y$.

Example 3.6. The first few monomials of the $C_{3,4}$ order are

$$1 < x < y < x^2 < xy < y^2 < x^3 < x^2y < xy^2 < x^4 < y^3 < x^3y < x^2y^2 < \dots.$$

On monomials less than x^4 and y^3, this order agrees with the degree lexicographic order with $x < y$.

In equations 1.1 and 1.2, the monomials are ordered by the $C_{2,3}$ and $C_{2,7}$ orders, respectively. In [3], Arita uses the $C_{3,4}$ **order**, given by the rows of

$$\begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix}.$$

We will make regular use of the $C_{3,4}$ order in this thesis.

3.2 Ideal of Leading Terms

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $f \in R$ be a polynomial, and let $m \in \mathcal{M}_R$ be a monomial. Denote the **coefficient of** m **in** f by $\text{coeff}(f, m)$. For example, if $f = 2x + 3y + 5x + 8$, then $\text{coeff}(f, 1) = 8$, $\text{coeff}(f, x) = 2 + 5 = 7$, $\text{coeff}(f, y) = 3$, and $\text{coeff}(f, x^2) = 0$.

Now let $\leq$ be a monomial order on R. Define also

$$\text{LM}_{\leq}(f) = \max\{m \in (\mathcal{M}_R, \leq) \mid \text{coeff}(f, m) \neq 0\}$$
$$\text{LT}_{\leq}(f) = \text{coeff}(f, \text{LM}_{\leq}(f)) \cdot \text{LM}_{\leq}(f).$$

These are, respectively, the **leading monomial** of f and the **leading term** of f (or **largest monomial** and **largest term**) with respect to the order $\leq$. If $f = 0$, then define $\text{LM}_{\leq}(f) = 0$. It should always be clear what monomial order is being used in any given context, hence we will omit the subscript and simply write $\text{LM}(f)$ and $\text{LT}(f)$.

Example 3.7. Let $R = \mathbb{Q}[x, y]$ with the lexicographic order $x < y$. Let $f = 3x^3+2y^2+1 \in R$. Then $\text{LM}(f) = y^2$ and $\text{LT}(f) = 2y^2$.

Example 3.8. Let $R = \mathbb{Q}[x, y]$ with the graded lexicographic order $x < y$. Let $f = 3x^3 + 2y^2 + 1 \in R$. Then $\text{LM}(f) = x^3$ and $\text{LT}(f) = 3x^3$.

A **monomial ideal** of R is an ideal of R generated by a subset of the monomials of R.

Example 3.9. For any polynomial ring R, R and 0 are monomial ideals, since $R = \langle 1 \rangle$ and 0 is generated by the empty set.

Example 3.10. Let $R = K[x, y]$. Some monomial ideals of R are $\langle x \rangle$, $\langle x, y \rangle$, and $\langle x^2, xy, y^2 \rangle$. While $\langle x + y \rangle$ is not a monomial ideal, $\langle x + y, x \rangle$ and $\langle 2x \rangle$ are, since $\langle x + y, x \rangle = \langle x, y \rangle$ and $\langle 2x \rangle = \langle x \rangle$.

Definition 3.11. Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring with a monomial order $\leq$. Let I be an ideal of R. The **ideal of leading terms** of I, denoted $\mathrm{LT}_{\leq}(I)$, is

$$\mathrm{LT}_{\leq}(I) := \langle \mathrm{LT}_{\leq}(f) \mid f \in I \rangle \,,$$

the ideal generated by the leading terms of all polynomials in I with respect to the order $\leq$. When it is clear what monomial order is being used, we will simply write $\mathrm{LT}(I)$ instead of $\mathrm{LT}_{\leq}(I)$.

For any ideal I, the ideal of leading terms is always a monomial ideal, since

$$\langle \mathrm{LT}(f) \mid f \in I \rangle = \langle \mathrm{LM}(f) \mid f \in I \rangle \,.$$

3.3 Gröbner Bases

As before, let $R = K[x_1, \ldots, x_n]$ be a multivariate polynomial ring over a field K.

Definition 3.12. Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring with a monomial order $\leq$. Let I be an ideal of R. A **Gröbner basis** for I is a finite set $G = \{g_1, \ldots, g_m\}$ such that

$$I = \langle g_1, \ldots, g_m \rangle$$

and

$$\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m) \rangle \,.$$

That is, a Gröbner basis for I is a finite set of generators for I whose leading terms generate $\mathrm{LT}(I)$. We say G is a Gröbner basis if G is a Gröbner basis for $\langle G\rangle = \langle g_1, \ldots, g_m\rangle$. It is known that every polynomial ideal has a Gröbner basis (§2.8 of [6]), and if generators of $I = \langle f_1, \ldots, f_k\rangle$ are given, an algorithm exists to produce a Gröbner basis $\{g_1, \ldots, g_m\}$ for I. See **Buchberger's Algorithm** in §2.11 of [6].

In the examples below, let $R = K[x, y]$ with the $C_{3,4}$ order.

Example 3.13. A somewhat trivial example. Let $I = \langle x^2, xy\rangle$. Then $\{x^2, xy\}$ is a Gröbner basis for I. In general, if $I = \langle g_1, \ldots, g_m\rangle$ and each g_i is a monomial, then $\{g_1, \ldots, g_m\}$ is a Gröbner basis.

Example 3.14. Let $I = \langle x^2 + x, xy\rangle$. Then $\{x^2 + x, xy\}$ is a Gröbner basis for I. In light of the example to follow, this example is not as trivial as it appears.

Example 3.15. Let $I = \langle x^2 + y, xy\rangle$. Then $\{x^2 + y, xy\}$ is *not* a Gröbner basis for I. The polynomial y^2 is in I, since $y^2 = (x^2 + y)y - (xy)x$, hence $y^2 \in \mathrm{LT}(I)$. However, $y^2 \notin \langle \mathrm{LT}(x^2 + y), \mathrm{LT}(xy)\rangle = \langle x^2, xy\rangle$, hence $\mathrm{LT}(I) \neq \langle \mathrm{LT}(x^2 + y), \mathrm{LT}(xy)\rangle$.

It may not be clear why $\{x^2 + x, xy\}$ is a Gröbner basis for an ideal, but $\{x^2 + y, xy\}$ is not. Worse, no justification for the former was given. We will give another characterization of Gröbner bases so as to better recognize them. This characterization is called Buchberger's Criterion, though this characterization requries that we first define reductions and S-polynomials.

Definition 3.16. Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring with a monomial order $\leq$. Let $f, h \in R$ be polynomials and let $G \subseteq R$ be a finite set of polynomials. We say

- f is **reduced modulo** h if no term in f is divisible by $\mathrm{LT}(h)$ — that is, h cannot be used to eliminate a term from f;
- f is **reduced modulo** G if for all $g \in G$, f is reduced modulo g; and

- $\overline{f}$ is **a reduction of** f **modulo** G if $\overline{f}$ is reduced modulo G, and $f = g + \overline{f}$ for some $g \in \langle G \rangle$, the R-ideal generated by G.

There exists a straightforward algorithm to produce a reduction of f modulo G. See the division algorithm[10] in Chapter 2 §3 of [8]. It amounts to eliminating terms in f by repeatedly iterating over G in some order and subtracting from f multiples of the iterand. However, the remainder of this division algorithm is not necessarily unique [11]. Thus, we call $\overline{f}$ *a* reduction, not *the* reduction, of f modulo G. The remainder depends on the chosen monomial order $\leq$ on R, as well as an ordering on G, by which we mean if we consider G an ordered set, then running the division algorithm on different permutations of G may result in different remainders. The division algorithm is deterministic, therefore if we fix an ordering on G, we may speak of ***the*** **reduction of** f **modulo** G with respect to that order.

Definition 3.17. Let $f, g \in K[x_1, \ldots, x_n]$. The S**-polynomial**[12] of f and g is

$$S(f, g) = f\frac{m}{\mathrm{LT}(f)} - g\frac{m}{\mathrm{LT}(g)},$$

where $m = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.

The S-polynomial is constructed such that the leading terms of $fm/\mathrm{LT}(f)$ and $gm/\mathrm{LT}(g)$ cancel.

Let us revisit the ideals from Examples 3.14 and 3.15. Recall that $R = K[x, y]$ with the $C_{3,4}$ order.

Example 3.18. Let $I = \langle x^2 + x, xy \rangle$. The S-polynomial of $x^2 + x$ and xy is

$$S(x^2 + y, xy) = (x^2 + x)\frac{x^2y}{x^2} - (xy)\frac{x^2y}{xy} = xy.$$

[10] Also called multivariate division or generalized polynomial long division.

[11] But see Theorem 3.29. The remainder is unique when G is a Gröbner basis, perhaps the strongest motivation for their invention.

[12] S for "syzygy".

Note that xy is not reduced modulo $\{x^2+x, xy\}$. The reduction of xy modulo $\{x^2+x, xy\}$ is 0.

Example 3.19. Let $I = \langle x^2+y, xy\rangle$. The S-polynomial of x^2+y and xy is

$$S(x^2+y, xy) = (x^2+y)\frac{x^2y}{x^2} - (xy)\frac{x^2y}{xy} = y^2.$$

Note that y^2 *is* reduced modulo $\{x^2+x, xy\}$, but is non-zero.

Theorem 3.20 (Buchberger's Criterion [6])**.** *Let $G = \{g_1, \ldots, g_m\}$ be a finite subset of R. Then G is a Gröbner basis if and only if for all pairs $i \neq j$, the reduction of $S(g_i, g_j)$ modulo G is 0.*

Using Buchberger's Criterion and in light of Example 3.18, one may now see why $\{x^2+y, xy\}$ is not a Gröbner basis in Example 3.14. However, $\{x^2+y, xy, y^2\}$ *is* a Gröbner basis.

Definition 3.21. Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring with a monomial order $\leq$. Let I be an ideal of R and let G be a Gröbner basis of I. The **minimum polynomial** of I (with respect to $\leq$) is the element of G with the smallest leading monomial (with respect to $\leq$).

Recall that every ideal I has a Gröbner basis, hence every ideal has a minimum polynomial. The minimum polynomial of I is unique. Were there two distinct minimum polynomials, their S-polynomial would violate Buchberger's Criterion.

It was mentioned in the introduction to this chapter that reduced Gröbner bases allow for unique representations of ideals. We define reduced Gröbner bases now.

Definition 3.22. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis. Then G is called **reduced** if for all $g \in G$, g is monic and reduced modulo $G - \{g\}$.

In other words G is reduced if for every $g_i \in G$, no term in g_i is divisible by the leading monomial of any other generator in G.

Example 3.23. Still using $R = K[x, y]$ with the $C_{3,4}$ order, consider the ideal

$$I = \left\langle y^2 + xy + x^2,\ y^2 + xy,\ y^2 \right\rangle.$$

The sets $\{x^2, xy + x^2, y^2 + xy + x^2\}$ and $\{x^2, xy, y^2\}$ are both Gröbner bases of I. Only the latter is reduced.

Theorem 3.24. *If G_1, G_2 are reduced Gröbner bases of an ideal I, then $G_1 = G_2$.*

Proof. §2.11 in [6]. □

Thus, we may define $\mathrm{RGB}(I)$ to be the unique reduced Gröbner basis of I. In §2.11 of [6], it is mentioned that Buchberger's Algorithm is easily modified to output $\mathrm{RGB}(I)$, given generators of I. This gives a way of testing equality of ideals. Given two ideals and their generators $I = \langle f_1, \ldots, f_k \rangle$ and $J = \langle g_1, \ldots, g_m \rangle$, then $I = J$ if and only if $\mathrm{RGB}(f_1, \ldots, f_k) = \mathrm{RGB}(g_1, \ldots, g_m)$.

For the remainder of this section, we state several theorems related to Gröbner bases that will get use in later sections.

Theorem 3.25. *Let I be an ideal of R with Gröbner basis $\{g_1, \ldots, g_m\}$. Let B be the set of monomials in R not divisible by the leading term of any g_i,*

$$B := \mathcal{M}_R - \mathrm{LT}(I).$$

Then B is a K-vector space basis for R/I.

Proof. Theorem 15.2 in [11]. □

Corollary 3.26.

$$\dim_K R/I = \#\{m \in \mathcal{M}_R \mid m \notin \mathrm{LT}(I)\}.$$

Theorem 3.27. *Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis and consider the system of polynomial equations*

$$g_1 = \ldots = g_m = 0.$$

This system has finitely many solutions if and only if for every indeterminate $x_i \in K[x_1, \ldots, x_n]$, there is a power x_i^k and element $g \in G$ such that $\mathrm{LM}(g) = x_i^k$.

Proof. §3.6 of [6]. □

Theorem 3.28. *Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis and suppose the system of polynomial equations*

$$g_1 = \ldots = g_m = 0$$

has finitely many solutions. Let N be the number of solutions.

(i) $N = \#\{m \in \mathcal{M}_R \mid m \notin \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)\rangle\}$.

(ii) If I is the R-ideal generated by G, then $N = \dim_K R/I$.

Proof. For part (i), see §3.6 of [6]. Part (ii) follows from Corollary 3.26. □

Theorem 3.29. *Let I be an ideal of R, generated by the Gröbner basis $G = \{g_1, \ldots, g_m\}$. Then,*

(i) Every polynomial $f \in R$ can be written uniquely in the form

$$f = g + r$$

where $g \in I$, $r \in R$, and r is reduced modulo G.

(ii) For any polynomial $f \in R$, $f \in I$ if and only if $r = 0$.

Proof. Chapter 2, §6, Proposition 1 and Corollary 2 in [8]. □

3.4 Gröbner Bases in Coordinate Rings

While the theory of Gröbner bases always takes place in polynomial rings, the theory may be extended to the coordinate ring of a $C_{3,4}$ curve C, though the equivalence relation leads to a complication. Take, for example, the ring $K[x, y]$ for some field K with the $C_{3,4}$ monomial order. Then $x^4 < y^3$ in $K[x, y]$. Now consider the coordinate ring $K[C] := K[x, y]/\langle y^3 + x^4 + 1\rangle$ (supposing this curve is non-singular). This places a relation on 1, x^4, and y^3. How can we compare the monomials y^3 and x^4 in $K[C]$ if $y^3 \equiv -x^4 - 1$? Given that y divides $x^4 + 1$ in $K[C]$, is $\langle y, x^4 + 1\rangle$ a reduced Gröbner basis in $K[C]$ or not? We must therefore make clear what we mean by a Gröbner basis in a coordinate ring.

Let C be a $C_{3,4}$ curve given by a polynomial F. Then the ideals of $K[x, y]$ containing F are in bijection with the ideals of $K[C]$ (Theorem III.2.13 in [21]). Let $G = \langle g_1, \ldots, g_m\rangle$ be a finite subset of $K[C]$ and let $I = \langle G\rangle$ be the $K[C]$-ideal generated by G. Let $\overline{F} \in K[x, y]$ be the reduction of F modulo G, in the sense of Definition 3.16, and treating G as a subset of $K[x, y]$. We will say that G is a Gröbner basis for I if the set $G \cup \{\overline{F}\}$ is a Gröbner basis in $K[x, y]$ with respect to the $C_{3,4}$ order.

In each of the examples below, let $K = \mathbb{F}_{11}$, and let C be the curve given by $F = y^3 + x^4 + 1 \in K[x, y]$.

Example 3.30. Consider the ideal $I = \langle x^2 + x, xy\rangle \subset K[C]$. The set $G = \{x^2 + x, xy\}$ is *not* a Gröbner basis for I.

The reduction of F modulo G is

$$\begin{aligned}
\overline{F} &= y^3 + x^4 + 1 \\
&\equiv y^3 - x^3 + 1 && \text{reduce modulo } x^2 + x \\
&\equiv y^3 + x^2 + 1 && \text{reduce modulo } x^2 + x \\
&\equiv y^3 - x + 1 && \text{reduce modulo } x^2 + x.
\end{aligned}$$

Now we lift I to $I^* = \langle x^2 + x, xy, y^3 - x + 1\rangle \subset K[x, y]$. However, one of the S-polynomials

of the generators of I^* does not reduce to 0 modulo G.

$$\begin{aligned} S(x^2+x, y^3-x+1) &= (x^2+x)\frac{x^2y^3}{x^2} - (y^3-x+1)\frac{x^2y^3}{y^3} \\ &= xy^3 + x^3 - x^2 \\ &\equiv x^3 - x^2 && \text{reduce modulo } xy \\ &\equiv -2x^2 && \text{reduce modulo } x^2+x \\ &\equiv 2x \pmod{G} && \text{reduce modulo } x^2+x. \end{aligned}$$

In fact, $I = \langle x \rangle$ and $\{x\}$ is a Gröbner basis in $K[C]$.

By contrast, $\{x^2+x, xy\}$ *is* a Gröbner basis of $K[x,y]$, as per Example 3.14.

Example 3.31. Consider instead $I = \langle y^2 \rangle \subset K[C]$. The reduction of F modulo y^2 is $\overline{F} = x^4+1$. Lift I to $I^* = \langle y^2, x^4+1 \rangle \subset K[x,y]$. There is only one S-polynomial to consider on the generators of I^*,

$$S(y^2, x^4+1) = (y^2)\frac{x^4y^2}{y^2} - (x^4+1)\frac{x^4y^2}{x^4} = y^2.$$

This S-polynomial reduces to 0 modulo $\{y^2, x^4+1\}$, hence $\{y^2, x^4+1\}$ is a Gröbner basis in $K[x,y]$ and $\{y^2\}$ is a Gröbner basis in $K[C]$.

This example illustrates the need to compute the reduction $\overline{F}$ of F modulo G, since $\{y^2, x^4+1\}$ is a Gröbner basis in $K[x,y]$, but $\{y^2, y^3+x^4+1\}$ is not.

4 Differential Forms

In a typical undergraduate mathematics curriculum, derivatives and differential forms appear in the study of real- or complex-valued functions. In real and complex analysis courses, it is seen that $\mathbb{R}$ and $\mathbb{C}$ are complete with respect to their standard metrics. Concepts such as limits, convergence, and derivatives are defined with respect to these metrics. In this thesis, we wish to speak of derivatives and differentials of functions that are not real-valued, but rather members of a polynomial ring $K[x, y]$ over a finite field or a quotient of that polynomial ring. It is not so clear anymore what is meant by the differential of a polynomial in these discrete spaces.

Differentials arise when doubling divisors (or tripling, etc.). Doubling a divisor typically requires finding polynomials that are tangent to the curve at some prescribed points. This amounts to finding polynomials that pass through the given points and whose differentials also vanish at these points.

In this chapter, we define (Kähler) differentials of functions purely algebraically in a sufficient generality as to cover differentials of polynomials in $A = R[x_1, \ldots, x_n]$, multivariate polynomials with coefficients in a commutative ring with identity R. We will see how to extend this definition to differentials on functions in other spaces constructed from A, such as its field of fractions, quotients, and localizations. Along the way, we give a natural definition of the formal derivative and formal partial derivative.

The contents of this chapter come mostly from a combination of the books [11], [12], [16], and [44].

4.1 Derivations

Definition 4.1. Let R be a commutative ring, A an R-algebra, and M an A-module. A map $\delta : A \to M$ is called a **derivation** (from A to M) if it is R-linear and satisfies the

product rule (also called the Leibniz rule):

$$\delta(ab) = \delta(a)b + a\delta(b).$$

Some authors do not require a derivation to be R-linear, and they distinguish between derivations and R-linear derivations. We will assume all derivations are R-linear.

As the name suggests, many familiar properties of the derivative from calculus are an immediate consequence of this definition. The following are easily verified.

Proposition 4.2. *Let R be a commutative ring, A an R-algebra, and M an A-module. Let $\delta : A \to M$ be a derivation. Then*

(i) If A is unital, then $\delta(1) = 0$.

(ii) If A is unital, then $\delta(r) = 0$ for all $r \in R$.

For all $x, y \in A$,

(iii) If A is commutative, then $\delta(x^2) = 2x\delta(x)$.

(iv) If A is commutative, then for all integers $n > 0$, $\delta(x^n) = nx^{n-1}\delta(x)$.

(v) If x is a unit, then $\delta(x^{-1}) = -x^{-2}\delta(x)$.

(vi) If x is a unit, then for all $n \in \mathbb{Z}$, $\delta(x^n) = nx^{n-1}\delta(x)$.

(vii) If y is a unit, then $\delta(xy^{-1}) = (\delta(x)y - x\delta(y))y^{-2}$.

We can define the sum of two derivations δ_1 and δ_2 by

$$(\delta_1 + \delta_2)(x) = \delta_1(x) + \delta_2(x)$$

and scalar multiplication of a derivation δ by a ring element r by

$$(r\delta)(x) = r\delta(x).$$

Under these operations, the set of derivations from A to M becomes an R-module, denoted by $\mathrm{Der}_R(A, M)$. This is the **module of derivations from A to M**. In the case where $M = A$, this may be denoted by $\mathrm{Der}_R(A)$.

Property (v) of Proposition 4.2 shows that if x is a unit, then $\delta(x^{-1})$ is determined by $\delta(x)$. This suggests that there is a relationship between derivations on an algebra A and derivations on the field of fractions of A, although note that A must not have any zero divisors in order for its field of fractions to be constructed.

Proposition 4.3. *Let A be an R-algebra with no zero divisors and let $\delta \in \mathrm{Der}_R(A, M)$. Let $B = \mathrm{Frac}\, A$, the field of fractions of A. There is a unique $\delta' \in \mathrm{Der}_R(B, M)$ whose restriction to A is $\delta'|_A = \delta$.*

That is to say that if δ is a derivation from A to M, it extends uniquely to a derivation from $\mathrm{Frac}\, A$ to M.

Proof. If $A = B$, we are done. So suppose instead there is a $b \in B$ such that $b \in A$ but $b^{-1} \notin A$. Suppose $\delta_1, \delta_2 \in \mathrm{Der}_R(B, M)$ are such that $\delta_1|_A = \delta = \delta_2|_A$. Then $\delta_1(b) = \delta(b) = \delta_2(b)$ and

$$\delta_1(b^{-1}) = -b^{-2}\delta_1(b) = -b^{-2}\delta_2(b) = \delta_2(b^{-1}).$$

It follows that $\delta_1(ab^{-1}) = \delta_2(ab^{-1})$ for all $ab^{-1} \in B$. □

In order to understand how a derivation acts on $\mathrm{Frac}\, A$, it is enough to know how it acts on A. In the case of a derivation over the field $R(x_1, \ldots, x_n)$, it is enough to know how it acts on the polynomial ring $R[x_1, \ldots, x_n]$. In the univariate case, we can say even more. The behaviour of a derivation $\delta : R(x) \to M$ is entirely determined by the value of $\delta(x)$.

Proposition 4.4. *Let $R(x)$ be the ring of rational functions over a ring R in a single variable x. Let $\delta_1, \delta_2 \in \mathrm{Der}_R(R(x))$. If $\delta_1(x) = \delta_2(x)$, then $\delta_1 = \delta_2$.*

Proof. For all $r \in R$, we have $\delta_1(r) = \delta_2(r) = 0$. For all $f \in R[x]$, we have $\delta_1(f) = \delta_2(f)$ by R-linearity. Now δ_1 and δ_2 agree on all of $R[x]$. By Proposition 4.3, they must agree on all

of $R(x)$. $\square$

For a (unital) ring R, the **formal derivative** on $R(x)$ is the unique derivation $D_x \in \mathrm{Der}_R(R(x))$ satisfying $D_x(x) = 1$. The formal derivative of a function f is often denoted $f' := D_x(f)$, although this convention will not be adopted here — beyond this paragraph, this thesis has no use for derivations on univariate polynomials. The formal derivative behaves exactly as one might expect.

Example 4.5. Let $f = 3x^3 + 6x^2 + 1 \in \mathbb{Z}[x]$. Then

$$\begin{aligned} D_x(f) &= 3D_x(x^3) + 6D_x(x^2) + D_x(1) && R\text{-linearity} \\ &= 3 \cdot 3x^2 D_x(x) + 6 \cdot 2x D_x(x) + 0 && \text{Proposition 4.2} \\ &= 9x^2 + 12x && D_x(x) = 1. \end{aligned}$$

Now consider the R-algebra $A = R(x_1, \ldots, x_n)$, rational functions in n variables. For each $1 \leq i \leq r$, we can set $S_i = R(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$, so that $A = S_i(x_i)$. We have merely realized A as the algebra of rational functions in one variable x_i and coefficients in S_i, which is the algebra of rational functions in the other $n-1$ variables. Then Proposition 4.4 says that there is a unique derivation $D_{x_i} \in \mathrm{Der}_{S_i}(A)$ satisfying $D_{x_i}(x_i) = 1$. This derivation D_{x_i} is also a member of $\mathrm{Der}_R(A)$ and its action on the other indeterminates of A is

$$D_{x_i}(x_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

The requirement that $D_{x_i}(x_j) = 0$ when $i \neq j$ is a consequence of S_i-linearity by D_{x_i}'s membership in $\mathrm{Der}_{S_i}(A)$. If $f \in A$, then $f_{x_i} := D_{x_i}(f)$ is the **formal partial derivative** with respect to x_i.

Example 4.6. In the case of $A = \mathbb{Z}[x, y]$, we have derivations D_x and D_y with $D_x(x) = 1 = D_y(y)$ and $D_x(y) = 0 = D_y(x)$. Let $f = x^2 + xy + y^3 \in A$. Then $f_x = D_x(f) = 2x + y$ and

$f_y = D_y(f) = x + 3y^2$.

We may compose derivations with a morphisms of algebras to obtain new derivations.

Proposition 4.7. *Let $f \in \mathrm{Hom}_R(A, B)$ be a morphism of R-algebras and let $\delta \in \mathrm{Der}_R(B, M)$ be an R-linear derivation.*

$$A \xrightarrow{f} B \xrightarrow{\delta} M$$

Then $\delta \circ f \in \mathrm{Der}_R(A, M)$.

Proof. While M is a B-module, it becomes an A-module under the A-action

$$A \times M \to M : (a, m) \mapsto f(a)m.$$

Both f and δ are R-linear, so $\delta \circ f$ is also R-linear. As for the product rule, let $a, b \in A$. Then

$$\begin{aligned}
(\delta \circ f)(ab) &= \delta(f(ab)) \\
&= \delta(f(a)f(b)) \\
&= \delta(f(a))f(b) + f(a)\delta(f(b)) \\
&= (\delta \circ f(a))f(b) + f(a)(\delta \circ f(b)) \\
&= (b, \delta \circ f(a)) + (a, \delta \circ f(b)).
\end{aligned}$$

□

4.2 Kähler Differentials

In this section, we briefly present a construction of Kähler differentials and some important properties. We will use Kähler differentials in Chapter 9 to solve the problem of doubling divisors. For more details of Kähler differentials, as well as alternative constructions, see [11], [12], [16], or [44].

Let A be an R-algebra. The **module of Kähler differentials** of A over R, denoted by $\Omega_{A/R}$, is the A-module generated by the set $\{d(a) \mid a \in A\}$, where $d(a)$ is merely a symbol,

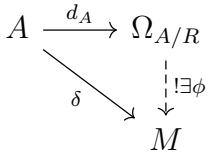
modulo the relations

$$d(ab) = d(a)b + ad(b)$$
$$d(ra + sb) = rd(a) + sd(b)$$

for all $r, s \in R$ and $a, b \in A$. The elements of $\Omega_{A/R}$ are called **differential forms** or **Kähler differentials**. We will write $d(a)$ as simply da, though we will not write $d(ab)$ as dab, as this may be confused with $d(a)b$. The map

$$d_A : A \to \Omega_{A/R} : a \mapsto d(a)$$

is an R-linear derivation, called the **universal derivation**. It is universal in the following sense. If $\delta : A \to M$ is another R-linear derivation from A, then there is a unique morphism of R-modules $\phi : \Omega_{A/R} \to M$ such that



commutes. This map is defined by $\phi : da \mapsto \delta(a)$. We will omit the subscript and write d in place of d_A, except in contexts where there are multiple d's and we need to distinguish them by their domains.

Of particular interest to us in this thesis is the case where $A = R[x_1, \ldots, x_n]$ is a polynomial ring. In this case, $\Omega_{A/R}$ is the free A-module generated by the symbols $dx_1, \ldots, dx_n$.

Proposition 4.8. *Let $A = R[x_1, \ldots, x_n]$. Then*

$$\Omega_{A/R} \cong \bigoplus_{i=1}^{n} A dx_i.$$

4.3 Differential Forms in $K[C]$

In Section 4.2, we defined $\Omega_{A/R}$, the module of Kähler differentials on an R-algebra A. The coordinate ring $K[C]$ of a curve C is a K-algebra, so let us describe the structure of $\Omega_{K[C]/K}$. To do so, we will make use of the following proposition.

Proposition 4.9. *Let $\pi : A \to B$ be an epimorphism of R-algebras. Let $I = \ker \pi$. There is an exact sequence of B-modules*

$$I/I^2 \xrightarrow{d} B \underset{A}{\otimes} \Omega_{A/R} \xrightarrow{D\pi} \Omega_{B/R} \to 0$$

where $d : [f] \mapsto 1 \otimes df$ and $D\pi : b \otimes da \mapsto b(da)$.

Proof. Proposition 16.3 in [11]. □

This proposition makes use of the tensor product of modules. The tensor product will not be defined or discussed in this thesis; one may consult [10], [11], or [21] for more on that topic. We will take advantage of other results to turn the tensor product into a direct sum of modules.

To understand the structure of $\Omega_{K[C]/K}$, we begin by noting that the canonical quotient map $q : K[x,y] \to K[C]$ is an epimorphism of K-algebras whose kernel is $\ker q = \langle F \rangle$, the $K[x,y]$-ideal generated by the defining polynomial F of the curve C. Proposition 4.9 therefore applies, telling us that there is an exact sequence

$$\frac{\langle F \rangle}{\langle F^2 \rangle} \xrightarrow{d} K[C] \underset{K[x,y]}{\otimes} \Omega_{K[x,y]/K} \xrightarrow{Dq} \Omega_{K[C]/K} \longrightarrow 0.$$

Using a property of exact sequences (see remarks on page 176 of [21]),

$$\Omega_{K[C]/K} \cong \frac{K[C] \underset{K[x,y]}{\otimes} \Omega_{K[x,y]/K}}{\operatorname{im} d}.$$

Next applying Proposition 4.8,

$$\Omega_{K[C]/K} \cong \frac{K[C] \underset{K[x,y]}{\otimes} \Omega_{K[x,y]/K}}{\operatorname{im} d} \cong \frac{K[C] \underset{K[x,y]}{\otimes} (K[x,y]dx \oplus K[x,y]dy)}{\operatorname{im} d}.$$

The tensor product distributes over addition (Theorem IV.5.9 [21]), giving

$$\Omega_{K[C]/K} \cong \frac{\left(K[C] \underset{K[x,y]}{\otimes} K[x,y]dx\right) \oplus \left(K[C] \underset{K[x,y]}{\otimes} K[x,y]dy\right)}{\operatorname{im} d}.$$

A basic property of the tensor product is that an R-module A tensored with its ring R is isomorphic to itself, i.e. $A \underset{R}{\otimes} R \cong A$ (Theorem IV.5.7 [21]), hence

$$\Omega_{K[C]/K} \cong \frac{K[C]dx \oplus K[C]dy}{\operatorname{im} d}.$$

To determine the image of d, it is enough to know the image of the element $F \in \langle F \rangle / \langle F^2 \rangle$. The element $F \in \langle F \rangle / \langle F^2 \rangle$ maps to $1 \otimes dF \in K[C] \otimes \Omega_{K[x,y]/K}$. Following the chain of isomorphisms we just produced, this then maps to $F_x dx + F_y dy \in K[C]dx \oplus K[C]dy$. Thus,

$$\Omega_{K[C]/K} \cong \frac{K[C]dx \oplus K[C]dy}{\langle F_x dx + F_y dy \rangle}.$$

The module $\Omega_{K[C]/K}$ of differentials on $K[C]$ is generated by dx and dy, modulo the equivalence relation $F_x dx \equiv -F y dy$. This relation between dx and dy means that it is therefore a rank 1 $K[C]$-module, generated by a single element.

Proposition 4.10. *There is a generator dz for $\Omega_{K[C]/K}$ with the properties*

$$dx \equiv F_y dz$$
$$dy \equiv -F_x dz.$$

Proof. See Lemma 5.1 in [40]. □

In fact, there are many possible generators for $\Omega_{K[C]/K}$. Another choice of generator allowing for more efficient doubling of typical divisors will be presented in Chapter 9. The generator in Proposition 4.10 is a natural choice that is useful for some proofs, and will be used in some atypical cases of divisor doubling.

The differential of a function $f \in K[C]$ with respect to this generator dz is

$$df = (f_x F_y - f_y F_x)dz.$$

If I is an ideal of $K[C]$, we will say by abuse of notation that $df \in I$ if $f_x F_y - f_y F_x \in I$. Equivalently, we will say that $df \in I$ if df vanishes modulo I.

Now let $\mathcal{O}_\mathfrak{p}$ be the local ring at a prime ideal $\mathfrak{p}$ of $K[C]$. Then there is a map $d_{\mathcal{O}_\mathfrak{p}} : \mathcal{O}_\mathfrak{p} \to \Omega_{\mathcal{O}_\mathfrak{p}/K}$. The action of this map is inherited from the map $d_{K[C]} : K[C] \to \Omega_{K[C]/K}$. That is, the differential of a function $f/g \in \mathcal{O}_\mathfrak{p}$ is

$$d_{\mathcal{O}_\mathfrak{p}}\left(\frac{f}{g}\right) = \frac{d_{K[C]}(f)g - f d_{K[C]}(g)}{g^2} = \frac{(f_x F_y - f_y F_x)g - f(g_x F_y - g_y F_x)}{g^2}dz.$$

As noted earlier in this chapter, for readability, we will omit the subscripts on d when it is clear in context which differential map is meant.

Lemma 4.11. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\overline{K}[C]$. Let u be a uniformizer for $\mathfrak{m}_\mathfrak{p}$, the maximal ideal of $\mathcal{O}_\mathfrak{p}$. Then $du \notin \mathfrak{m}_\mathfrak{p}$.*

Proof. Let $\mathfrak{p} = \langle x - x_0, y - y_0 \rangle$. Since C is non-singular, the partial derivatives of F are not simultaneously zero at $P = (x_0, y_0)$, so suppose without loss of generality that $F_y(x_0, y_0) \neq 0$. Then the tangent line to C at P is non-vertical and $u = x - x_0$ is a uniformizer for $\mathfrak{m}_\mathfrak{p}$. Then $du = dx = F_y \notin \mathfrak{m}_\mathfrak{p}$. □

Theorem 4.12. *Let $\mathfrak{p}$ be a non-zero prime ideal of $K[C]$ and f a polynomial in $K[C]$.*

Suppose $\nu_{\mathfrak{p}}(f) \geq n$ for some non-negative integer n. Then

$$\nu_{\mathfrak{p}}(f) \geq n+1 \iff \nu_{\mathfrak{p}}(df) \geq n.$$

Proof. Let u be a uniformizer for $\mathfrak{m}_{\mathfrak{p}}$. Then $f = au^n$ for some $a \in K(C)^*$, and

$$df = d(au^n) = u^n da + nau^{n-1}du.$$

Now $u^n da \in \mathfrak{m}_{\mathfrak{p}}^n$, so $df \in \mathfrak{m}_{\mathfrak{p}}^n$ if and only if $nau^{n-1}du \in \mathfrak{m}_{\mathfrak{p}}^n$. But $n, du \notin \mathfrak{m}_{\mathfrak{p}}$, so this is true if and only if $au^{n-1} \in \mathfrak{m}_{\mathfrak{p}}^n$. Hence

$$df \in \mathfrak{m}_{\mathfrak{p}}^n \iff au^{n-1} \in \mathfrak{m}_{\mathfrak{p}}^n \iff au^n \in \mathfrak{m}_{\mathfrak{p}}^{n+1} \iff f \in \mathfrak{m}_{\mathfrak{p}}^{n+1}. \qquad \square$$

5 The Divisor Class Group

The main matter of this thesis is to describe efficient arithmetic in the divisor class group of a $C_{3,4}$ curve, so we come now to defining that group. We begin with a description of divisors on a curve. Divisors on a curve C form an Abelian group, $\mathrm{Div}(C)$, of which we will describe several subgroups, most notably the subgroups $\mathrm{Div}_K^0(C)$ and $\mathrm{Princ}(C)$. The divisor class group is the quotient of these two subgroups.

We will assume that C is a $C_{3,4}$ curve, though the definitions given in this chapter up to and including the divisor class group work equally well for any curve. Some facts towards the end of the chapter related to a partial order $(\mathrm{Div}_K^0(C), \leq)$, including a characterization of prime divisors, depend on the fact that a $C_{3,4}$ curve has a unique point at infinity, P_∞.

5.1 Divisors

Let C be a $C_{3,4}$ curve. A **divisor** D of C is a formal sum of points in $C(\overline{K})$, including possibly the point at infinity, P_∞. If P, Q, and R are points on the curve C, then examples of divisors include

$$P + Q + R - 3P_\infty,$$
$$P + 3Q - 2R,$$
$$Q,$$
$$0.$$

More generally, a divisor has the form

$$D = \sum_{P \in C(\overline{K})} n_P P,$$

where only finitely many n_P's are non-zero.

A divisor is an element of the free Abelian group generated by the set of points $C(\overline{K})$. This Abelian group is denoted by $\mathrm{Div}(C)$. Addition and negation are defined in the obvious

way:

$$\left(\sum_{P\in C(\overline{K})} n_P P\right) + \left(\sum_{P\in C(\overline{K})} m_P P\right) = \sum_{P\in C(\overline{K})} (n_P + m_P)P$$

$$-\left(\sum_{P\in C(\overline{K})} n_P P\right) = \sum_{P\in C(\overline{K})} (-n_P)P.$$

The coefficient n_P of P is the **order** of the divisor D at P, denoted by $\mathrm{ord}_P(D)$. For example, if $D = P + 3Q - 2R$, then $\mathrm{ord}_Q(D) = 3$ and $\mathrm{ord}_R(D) = -2$. The **degree** of a divisor D, denoted by $\deg(D)$, is the sum of its orders at each point on the curve:

$$\deg(D) = \sum_{P\in C(\overline{K})} \mathrm{ord}_P(D).$$

For example, $\deg(P + 3Q - 2R) = 1 + 3 - 2 = 2$. Beginning with Chapter 7, to simplify discussion, we will use a different notion of degree that ignores the order of the point at infinity. We will make clear what we mean by that in Chapter 7.

The **support** of a divisor, denoted $\mathrm{supp}(D)$, is the set of points P with $\mathrm{ord}_P(D) \neq 0$,

$$\mathrm{supp}(D) := \{P \in C(\overline{K}) \mid \mathrm{ord}_P(D) \neq 0\}.$$

It is easily verified that the map deg and the family of maps ord_P have the additive properties

$$\mathrm{ord}_P(A + B) = \mathrm{ord}_P(A) + \mathrm{ord}_P(B)$$

$$\deg(A + B) = \deg(A) + \deg(B).$$

In fact, ord_P and deg are group homomorphisms $\mathrm{Div}(C) \to \mathbb{Z}$.

There is a partial order $\preceq$ on divisors. For two divisors $D, D' \in \mathrm{Div}(C)$, we order them

$$D \preceq D' \iff \forall P \in C(\overline{K}) : \mathrm{ord}_P(D) \leq \mathrm{ord}_P(D').$$

The divisor D precedes or is equal to D' if its order is no greater than that of D' at every point. This partial order is compatible with addition, in the sense that for any divisors A, B, and D,

$$A \preceq B \implies A + D \preceq B + D.$$

If $D \succeq 0$, then D is called an **effective** divisor.

Divisors of a curve, together with this partial order, form a lattice – every pair of divisors have a unique join and meet, which we call their **least common multiple** and **greatest common divisor**, respectively. Given two divisors D and D', their least common multiple is the unique, smallest divisor L such that $D \preceq L$ and $D' \preceq L$. Their greatest common divisor is the unique, largest divisor G such that $G \preceq D$ and $G \preceq D'$. Defined explicitly,

$$\begin{aligned}\operatorname{lcm}(D, D') &= \sum_{P \in C(\overline{K})} \max\{\operatorname{ord}_P(D), \operatorname{ord}_P(D')\}P \\ \gcd(D, D') &= \sum_{P \in C(\overline{K})} \min\{\operatorname{ord}_P(D), \operatorname{ord}_P(D')\}P.\end{aligned}$$

Just as integers a and b satisfy the law

$$|ab| = \operatorname{lcm}(a, b) \gcd(a, b),$$

divisors satisfy the law

$$D + D' = \operatorname{lcm}(D, D') + \gcd(D, D').$$

This property will play a prominent role when adding divisors in Chapter 8.

There is a short chain of subgroups of $\operatorname{Div}(C)$,

$$\operatorname{Princ}(D) \subset \operatorname{Div}^0_K(C) \subset \operatorname{Div}^0(C) \subset \operatorname{Div}(C),$$

which we will now describe.

Since $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ is a group homomorphism, its kernel is a subgroup of $\mathrm{Div}(C)$. The kernel, of course, is the subgroup of divisors of degree zero, which we denote by $\mathrm{Div}^0(C) := \ker \deg$.

Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. In Chapter 2, we defined the action of σ on a point (Equation 2.2). This may be extended to an action on $\mathrm{Div}(C)$ in a natural way. If $D = \sum n_P P$, then define

$$\sigma(D) = \sum_{P \in C(\overline{K})} n_P \sigma(P).$$

Just as σ permutes points in $C(\overline{K})$, so too does it permute divisors in $\mathrm{Div}(C)$. In this way, an automorphism in $\mathrm{Gal}(\overline{K}/K)$ is also an automorphism of $\mathrm{Div}(C)$.

Given an automorphism f on a group G, the **fixed-point subgroup** of f is

$$G^f := \{g \in G \mid f(g) = g\}.$$

Given a set S of automorphisms on G, this may be generalized even further:

$$G^S := \{g \in G \mid \forall f \in S : f(g) = g\}.$$

So G^S is the set of group elements in G fixed by every automorphism in S.

We say that a divisor D is **defined over** K if D is fixed by every automorphism in $\mathrm{Gal}(\overline{K}/K)$. Divisors defined over K therefore form a subgroup $\mathrm{Div}_K(C) \subset \mathrm{Div}(C)$.

$$\mathrm{Div}_K(C) := \mathrm{Div}(C)^{\mathrm{Gal}(\overline{K}/K)}$$

Example 5.1. Let K be any field, L/K any algebraic extension and $\sigma \in \mathrm{Gal}(\overline{K}/L)$. By definition, σ fixes L. If P is any point with coordinates in L, then $\sigma(P) = P$. If D is any divisor consisting only of points with coordinates in L, then $\sigma(D) = D$ and D is defined over L.

Example 5.2. Let $K = \mathbb{F}_2$ and let $L = K(\alpha)$ be an algebraic extension with $\alpha^2 + \alpha = 1$. Let C be the $C_{3,4}$ curve over K defined by the polynomial $F = y^3 + x^4 + x + 1$. Let P be the point $(\alpha : 1 : 1)$ on C and let D be the divisor $D = P$. There is an automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$ that maps $\alpha \mapsto \alpha + 1$, and

$$\sigma(D) = \sigma(P) = (\sigma(\alpha) : \sigma(1) : \sigma(1)) = (\alpha + 1 : 1 : 1) \neq D.$$

Hence D is not defined over K.

Example 5.3. Let K, L, C, and P be as in the previous example. Let $Q = (\alpha + 1 : 1 : 1)$, which is also a point on C. Let D be the divisor $D = P + Q$. Every automorphism σ in $\mathrm{Gal}(\overline{K}/K)$ maps α to itself or to $\alpha + 1$. Consequently, either

- $\sigma(P) = P$ and $\sigma(Q) = Q$, or
- $\sigma(P) = Q$ and $\sigma(Q) = P$.

In either case

$$\sigma(D) = \sigma(P) + \sigma(Q) = P + Q = D,$$

So D is defined over K.

The intersection of subgroups is again a subgroup, so define

$$\mathrm{Div}_K^0(C) := \mathrm{Div}_K(C) \cap \mathrm{Div}^0(C).$$

These are the divisors defined over K of degree zero.

If $f \in K(C)$ is a rational function on C, define the **divisor of** f as

$$\mathrm{div}(f) = \sum_{P \in C(\overline{K})} \nu_P(f) P.$$

Recall that $\nu_P(f)$ was defined in Section 2.3 for finite points P, and at the end of Section

2.4 for P_∞. The divisor $\mathrm{div}(f)$ is the sum of the zeros of f along C minus its poles, counting multiplicity. If $D = \mathrm{div}(f)$ for some rational function C, then D is called a **principal divisor**.

Proposition 5.4. *Let $f \in K(C)$ be a rational function on C. Then* $\mathrm{div}\, f \in \mathrm{Div}^0_K(C)$.

Proof. By Theorem 7.7.1 in [15], f has finitely many poles and zeroes, so that the formal sum

$$\mathrm{div}(f) = \sum_{P \in C(\overline{K})} \nu_P(f) P$$

is finite. By Theorem 8.3.14 in [15], f has as many poles as it has zeroes, so that $\mathrm{div}(f)$ has degree zero. By Proposition 2.7, $\mathrm{div}(f)$ is defined over K. □

Observe also that

$$\begin{aligned}
\mathrm{div}(f) + \mathrm{div}(g) &= \sum_{P \in C(\overline{K})} \nu_P(f) P + \sum_{P \in C(\overline{K})} \nu_P(g) P \\
&= \sum_{P \in C(\overline{K})} (\nu_P(f) + \nu_P(g)) P \\
&= \sum_{P \in C(\overline{K})} \nu_P(fg) P \\
&= \mathrm{div}(fg).
\end{aligned}$$

We have also $\mathrm{div}(f) - \mathrm{div}(g) = \mathrm{div}(f/g)$, so that principal divisors form a subgroup $\mathrm{Princ}(C) \subset \mathrm{Div}^0_K(C)$. Finally, we have described the subsets

$$\mathrm{Princ}(D) \subset \mathrm{Div}^0_K(C) \subset \mathrm{Div}^0(C) \subset \mathrm{Div}(C).$$

The **divisor class group**[13] of C is the quotient group

$$\mathrm{Cl}(C) = \frac{\mathrm{Div}_K^0(C)}{\mathrm{Princ}(C)}.$$

In the literature, the divisor class group is usually called the **Jacobian**, $\mathrm{Jac}(C)$, of C, e.g. [3], [5], [13], [18], [40]. Other authors call it the divisor class group while giving it the notation $\mathrm{Pic}_K^0(C)$, as it is isomorphic to the **Picard group** of C, e.g. [11] [15] [46]. In this thesis, we will use the term divisor class group, as the Picard group is usually defined in terms of line bundles and the Jacobian implies a relationship to a Jacobian variety, neither perspective being adopted here.

The **affine part** or **finite part** of a divisor D is

$$D_{\mathrm{aff}} = \sum_{\substack{P \in C(\overline{K}) \\ P \neq P_\infty}} n_P P.$$

In the divisor class group, every divisor is equivalent to one whose finite part is effective. To illustrate this, let D be a divisor and suppose $\mathrm{ord}_P(D) = n < 0$ for some finite point $P = (x_0 : y_0 : 1)$. Consider the vertical line through P. This line is given by the polynomial $f = x - x_0$ and intersects C at three points P, Q, and R, not necessarily distinct, but counting multiplicity. Then $\mathrm{div}\, f = P + Q + R - 3P_\infty$, and in the divisor class group, $\mathrm{div}\, f \equiv 0$. Let $D' = D + n\,\mathrm{div}\, f$. Then $D' \equiv D$ in the divisor class group and $\mathrm{ord}_P(D') \geq 0$. At no finite point does D' have lesser order than D. Hence, we can repeatedly add principal divisors to a divisor D to eliminate the points in D with negative order, resulting in an effective divisor equivalent to D.

[13] Technically, the group of degree 0 divisor classes defined over K. In some contexts, one may not demand that divisors by of degree 0 or defined over K, construct analogous quotient groups, and refer to it as the divisor class group.

Every divisor class therefore has a representative[14] of the form

$$D = P_1 + \ldots + P_n - nP_\infty,$$

where the P_i's are finite points, but not necessarily distinct. In other words, in the divisor class group, every divisor D may be written in the form (i.e. is equivalent to a divisor of the form)

$$D \equiv D_+ - D_\infty$$

where D_+ is an effective divisor and $D_\infty = \deg(D_+)P_\infty$ (also effective).

5.2 Prime Divisors

We have a partial order on divisors, with the property that $A \preceq B \implies \deg A \leq \deg B$. On the subgroup $\mathrm{Div}^0_K(C)$, this partial order is uninteresting, since there are no two distinct degree zero divisors with $A \preceq B$.

If D is a degree zero divisor, then we can separate out the point at infinity and write $D = D_{\text{aff}} - D_\infty$, where $P_\infty \notin \mathrm{supp}(D_{\text{aff}})$ and $D_\infty = (\deg D_{\text{aff}})P_\infty$. The divisor D_∞ is uniquely determined by the D_{aff}. This leads to a more useful partial order on degree zero divisors. For $A, B \in \mathrm{Div}^0_K(C)$, define the partial order $\leq$ by

$$A \leq B \iff A_{\text{aff}} \preceq B_{\text{aff}}.$$

Define also the set[15]

$$\mathrm{Div}^{\geq 0}_K(C) := \{D \in \mathrm{Div}^0_K(C) \mid D \geq 0\}.$$

The set $\mathrm{Div}^{\geq 0}_K(C)$ forms a monoid under addition, and $(\mathrm{Div}^{\geq 0}_K(C), \leq)$ forms a lattice with a minimum element, 0.

[14] It may have many representatives of this form. Reduced divisors, introduced in Chapter 7, are meant to be minimal unique representative of this form.

[15] To clear up any possible confusion, that's a K and $\geq$ in $\mathrm{Div}^{\geq 0}_K(C)$, not a $\overline{K}$ and $>$.

With this partial order, we may define prime divisors in a manner that echoes the definition of prime ideals[16] and Euclid's Lemma.[17]

Definition 5.5. A divisor $D \in \mathrm{Div}_K^{\geq 0}(C)$ is **prime** if $D > 0$ and for all $A, B \in \mathrm{Div}_K^{\geq 0}(C)$,

$$D = A + B \implies D \leq A \text{ or } D \leq B.$$

The prime divisors are the least non-zero divisors in the lattice $(\mathrm{Div}_K^{\geq 0}(C), \leq)$. Another characterization of prime divisors is that they are orbits of points on C, which we will show now. If $P \in C(\overline{K})$ is a finite point, define

$$[P] := \sum_{Q \in \mathrm{orb}(P)} (Q - P_\infty).$$

Proposition 5.6. *Let $D \in \mathrm{Div}_K^0(C)$. The following are equivalent.*

(i) D is prime;

(ii) There is a finite point $P \in C(\overline{K})$ such that $D = [P]$.

Proof. Let $D \in \mathrm{Div}_K^0(C)$.

(i) $\implies$ (ii): Suppose D is prime. Then $D > 0$, so let P be a finite point in $\mathrm{supp}(D)$. Since D is defined over K, every point in the orbit of P is also in $\mathrm{supp}\, D$. So $[P] \leq D$, and $D = [P] + D'$ for some divisor $D' \in \mathrm{Div}_K^{\geq 0}(C)$. Since D is prime, either $D \leq [P]$ or $D \leq D'$. Suppose $D \leq D'$. Then $D + [P] \leq D' + [P] = D$, hence $[P] \leq 0$, which is impossible. Therefore $D \leq [P]$. Since we have both $D \leq [P]$ and $[P] \leq D$, the result follows.

(ii) $\implies$ (i): Suppose $D = [P]$ for some finite point P. Let $A, B \in \mathrm{Div}_K^{\geq 0}(C)$ be effective divisors such that $D = A + B$. Then $P \in \mathrm{supp}\, A$ or $P \in \mathrm{supp}\, B$. Suppose, without

[16] A proper R-ideal $\mathfrak{p}$ is prime if for all R-ideals $\mathfrak{a}, \mathfrak{b}$, $\mathfrak{ab} \subseteq \mathfrak{p} \implies \mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.
[17] An integer $p > 1$ is prime if for all $a, b \in \mathbb{Z}$, $p|ab \implies p|a$ or $p|b$.

loss of generality, that $P \in \operatorname{supp} A$. Since A is defined over K, every other point in $\operatorname{orb} P$ is in $\operatorname{supp} A$, hence $[P] \leq A$. Since $D = [P]$, $D \leq A$.

□

Just as non-zero ideals in a Dedekind domain can be uniquely factored into products of prime ideals, non-zero divisors in $\operatorname{Div}_K^0(C)$ can be uniquely partitioned into sums of prime divisors. This relationship is explored in the next chapter.

6 The Ideal Class Group

Performing arithmetic on divisors themselves is cumbersome. As shown in Example 5.3, even if a divisor is defined over a field K, the coordinates of its points may live in an algebraic extension L/K. Performing arithmetic on the points therefore requires operations in L, which is computationally slower than working in K.

In this chapter, we will see that the divisor class group of a curve is isomorphic to the ideal class group of the curve's coordinate ring, $K[C]$. Every divisor may therefore be represented by polynomials with coefficients in K, rather than by points in $\overline{K} \times \overline{K}$. By interpreting divisors as ideals, we may perform our divisor arithmetic over the base field K.

We will demonstrate the existence of this isomorphism between the groups by explicitly constructing an isomorphism and its inverse. As the coordinate ring of a curve is a Dedekind domain, we first describe how this isomorphism acts on non-zero prime ideals of $K[C]$. We then extend this isomorphism to act on non-prime ideals, fractional ideals, and then ideal classes.

6.1 Prime Ideals, Prime Divisors

There is a relationship between prime ideals in $K[C]$ and prime divisors in $\mathrm{Div}_K^{\geq 0}$. In fact, the relationship is a bijection, and the goal of this section is to explicitly describe that bijection. We will define a map $I_{(-)}$ sending prime divisors to non-zero prime ideals and a map $\mathrm{div}(-)$ sending non-zero prime ideals to prime divisors, then show that these are mutual inverses. We begin by defining the former map and showing that it does in fact map primes to primes.

Definition 6.1. Let $[P]$ be a prime divisor on C, as per Proposition 5.6. The **ideal of** $[P]$ is

$$I_{[P]} = \{f \in K[C] \mid f(P) = 0\}.$$

This is the set of polynomials in $K[C]$ that vanish on the support of $[P]$. By Lemma 2.3, $I_{[P]} = I_{[Q]}$ for all $Q \in \mathrm{orb}(P)$. In Section 2.3, we claimed that a point P induces a prime

ideal. That prime ideal is $I_{[P]}$, and any other point in $\mathrm{orb}(P)$ induces the same prime ideal. The proof that $I_{[P]}$ is prime is straightforward:

Proposition 6.2. *Let P be an affine point on C and let $\mathfrak{p} = I_{[P]}$. Then*

(i) $\mathfrak{p}$ is a $K[C]$-ideal;

(ii) $\mathfrak{p}$ is non-zero;

(iii) $\mathfrak{p}$ is prime;

(iv) $\mathfrak{p}$ is maximal;

Proof. (i) Suppose $f, g \in \mathfrak{p}$. Then

$$(f-g)(P) = f(P) - g(P) = 0 + 0 = 0,$$

so $f - g \in \mathfrak{p}$. Suppose $f \in \mathfrak{p}$ and $h \in K[C]$. Then

$$(hf)(P) = h(P)f(P) = h(P) \cdot 0 = 0,$$

so $hf \in \mathfrak{p}$.

(ii) Let $P = (x_0, y_0)$. Let $m(x) \in K[x]$ be the minimum polynomial[18] of x_0. We may view m as a polynomial in $K[C]$. Then m is non-zero but is zero at P, so $m \in \mathfrak{p}$.

(iii) Suppose $fg \in \mathfrak{p}$ for some $f, g \in K[C]$. Then $(fg)(P) = 0 = f(P)g(P)$. Since $f(P)$ and $g(P)$ are field elements, one of them must be zero. Therefore one of f and g is in $\mathfrak{p}$.

(iv) In a Dedekind domain, all non-zero prime ideals are maximal. □

The next proposition gives another characterization of the ideal $I_{[P]}$ in terms of a prime ideal $\mathfrak{q}$ of $\overline{K}[C]$ that lies over $I_{[P]}$.

[18] In the usual algebraic number theory sense of a unique monic polynomial in $K[x]$ of minimal degree such that $m(x_0) = 0$.

Proposition 6.3. *Let $P = (x_0, y_0)$ be an affine point on C. Let $\mathfrak{q} = \langle x - x_0, y - y_0 \rangle$ as a $\overline{K}[C]$-ideal. Then*

$$I_{[P]} = \mathfrak{q} \cap K[C].$$

Proof.

$$\begin{aligned} I_{[P]} &= \langle f \in K[C] \mid f(P) = 0 \rangle \\ &= \langle f \mid f \in K[C], f(P) = 0 \rangle \\ &= \langle f \mid f \in K[C], f \in \mathfrak{q} \rangle \\ &= \langle f \mid f \in K[C] \rangle \cap \langle f \mid f \in \mathfrak{q} \rangle \\ &= K[C] \cap \mathfrak{q}. \end{aligned}$$

□

Intuitively, while $I_{[P]}$ is prime as a $K[C]$-ideal, it might be non-prime as a $\overline{K}[C]$-ideal. In $\overline{K}[C]$, $I_{[P]}$ factors into a product of primes, $\prod_{i=1}^{n} \mathfrak{q}_i$, possibly with $n > 1$. For any of those factors $\mathfrak{q}_i$, we may restrict back down to $K[C]$ to get $I_{[P]} = \mathfrak{q}_i \cap K[C]$.

We have shown that $I_{[-]}$ defines a map from prime divisors to prime ideals. We now show that it maps distinct prime divisors to distinct prime ideals.

Lemma 6.4. *Let P and Q be affine points on C. Then $I_{[P]} = I_{[Q]}$ if and only if $[P] = [Q]$.*

Proof. Certainly if $[P] = [Q]$, then $I_{[P]} = I_{[Q]}$. Suppose that $[P] \neq [Q]$. Write $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$. Let m_x be the minimum polynomial[19] of x_P and m_y the minimum polynomial of y_P.

If $m_x(x_Q) \neq 0$ or $m_y(y_Q) \neq 0$, then we have found a polynomial in $I_{[P]} - I_{[Q]}$ and we are done. Suppose $m_x(x_Q) = m_y(y_Q) = 0$. Then there are automorphisms $\sigma_x, \sigma_y \in \mathrm{Gal}(\overline{K}/K)$ such that $\sigma_x(x_P) = x_Q$ and $\sigma_y(y_P) = y_Q$. These automorphisms must be distinct, since $P \neq Q$. Let $\sigma = \sigma_x^{-1} \circ \sigma_y$ and $R = (x_P, \sigma(y_P))$. Then $R \in \mathrm{orb}(Q)$ and $I_{[R]} = I_{[Q]}$.

[19] Again, in the usual algebraic number theory sense.

Let $\mathfrak{p} = \langle x - x_P, y - y_P \rangle$ and $\mathfrak{r} = \langle x - x_P, y - \sigma(y_P) \rangle$. Then

$$I_{[P]} = \mathfrak{p} \cap K[C],$$
$$I_{[R]} = \mathfrak{r} \cap K[C],$$

$$\mathfrak{p} + \mathfrak{r} = \overline{K}[C],$$

and

$$\begin{aligned} I_{[P]} + I_{[Q]} &= I_{[P]} + I_{[R]} \\ &= (\mathfrak{p} \cap K[C]) + (\mathfrak{r} \cap K[C]) \\ &= (\mathfrak{p} + \mathfrak{r}) \cap K[C] \\ &= \overline{K}[C] \cap K[C] \\ &= K[C] \neq I_{[P]}. \end{aligned}$$

Hence $I_{[P]} \neq I_{[Q]}$. □

In the other direction, we define a map sending non-zero prime ideals to prime divisors.

Definition 6.5. Let $\mathfrak{p}$ be a non-zero prime ideal of $K[C]$. Define the **divisor of $\mathfrak{p}$** to be

$$\operatorname{div} \mathfrak{p} = \sum_{P \in C - P_\infty} \min_{f \in \mathfrak{p} - \{0\}} \{\nu_P(f)\}(P - P_\infty).$$

The affine support of this divisor consists of those points at which *every* polynomial in $\mathfrak{p}$ is zero. It is balanced by a negative multiple of the point at infinity, so that this divisor is of degree zero by construction. To show that $\operatorname{div} \mathfrak{p}$ is a prime divisor, we show $\operatorname{div} \mathfrak{p} = [P]$ for some finite point P on C. First, we establish a lemma.

Lemma 6.6. *Let P be a finite point on C and let $\mathfrak{p} = I_{[P]}$. Then* $\operatorname{ord}_P(\operatorname{div} \mathfrak{p}) = 1$.

Proof. Since every polynomial in $I_{[P]}$ passes through P,

$$1 \geq \min_{f \in I_{[P]} - \{0\}} \{\nu_P(f)\} = \min_{f \in \mathfrak{p} - \{0\}} \{\nu_P(f)\} = \operatorname{ord}_P(\operatorname{div} \mathfrak{p}).$$

To show that $\operatorname{ord}_P(\operatorname{div} \mathfrak{p}) = 1$, we must show that there is a polynomial in $\mathfrak{p}$ whose valuation at P is exactly 1.

Let $P = (x_0, y_0)$ and consider the lines determined by $x - x_0$ and $y - y_0$. Since C is non-singular, at most one of these lines is tangent to C at P. Without loss of generality, suppose $x - x_0$ is not tangent to C at P. Let $m(x)$ be the minimum polynomial of x_0, seen as an element of $K[C]$. Then

$$\begin{aligned}
\nu_P(m) &= \nu_P\left(\prod_{i=0}^{\deg m - 1} (x - x_i)\right) \\
&= \sum_{i=0}^{\deg m - 1} \nu_P(x - x_i) \\
&= \nu_P(x - x_0) && \nu_P(x - x_i) = 0 \text{ for } i \neq 0 \\
&= 1.
\end{aligned}$$

Moreover, m is zero on the orbit of P, so $m \in I_{[P]} = \mathfrak{p}$. □

Proposition 6.7. *Let $\mathfrak{p}$ be a non-zero prime ideal and let P be an affine point on C. The following are equivalent*

(i) $P \in \operatorname{supp}(\operatorname{div} \mathfrak{p})$;

(ii) $\mathfrak{p} = I_{[P]}$.

(iii) $\operatorname{div} \mathfrak{p} = [P]$.

Proof. **(i) $\implies$ (ii):** Suppose P is in the support of $\operatorname{div} \mathfrak{p}$. By Definition 6.5, every polynomial in $\mathfrak{p}$ has a positive valuation at P. Therefore every polynomial in $\mathfrak{p}$ is zero at P,

so $\mathfrak{p} \subseteq I_{[P]}$. Since $\mathfrak{p}$ and $I_{[P]}$ are both prime ideals and therefore maximal, this implies that they are equal.

(ii) $\implies$ (i): Suppose $\mathfrak{p} = I_{[P]}$. For every non-zero polynomial $f \in \mathfrak{p}$, $f(P) = 0$, hence $\nu_P(f) > 0$. Now the order of $\operatorname{div} \mathfrak{p}$ at P is

$$\operatorname{ord}_P(\operatorname{div} \mathfrak{p}) = \min_{0 \neq f \in \mathfrak{p}} \{\nu_P(f)\} > 0$$

therefore $P \in \operatorname{supp}(\operatorname{div} \mathfrak{p})$.

(i) $\implies$ (iii): Suppose $P \in \operatorname{supp}(\operatorname{div} \mathfrak{p})$. We must show that for all finite points $Q \in C$, $\operatorname{ord}_Q(\operatorname{div} \mathfrak{p}) = \operatorname{ord}_Q([P])$.

Let $Q \in C$ be a finite point and suppose $Q \in \operatorname{supp}(\operatorname{div} \mathfrak{p})$. Since (i) implies (ii), $\mathfrak{p} = I_{[Q]}$. Then by Lemma 6.6, $\operatorname{ord}_Q(\operatorname{div} \mathfrak{p}) = 1$. By Lemma 6.4, $[P] = [Q]$, so $\operatorname{ord}_Q([P]) = 1$.

Suppose instead $Q \notin \operatorname{supp}(\operatorname{div} \mathfrak{p})$. Then $\operatorname{ord}_Q(\operatorname{div} \mathfrak{p}) = 0$. By Lemma 6.4, $[P] \neq [Q]$, so $\operatorname{ord}_Q([P]) = 0$.

(iii) $\implies$ (i): Immediate from the definitions. □

Proposition 6.7 has two important consequences. It shows that every non-zero prime ideal $\mathfrak{p}$ of $K[C]$ arises from a prime divisor $[P]$, and every prime divisor $[P]$ arises from a non-zero prime ideal $\mathfrak{p}$. This is summarized in the following theorem, the main result of this section. It shows that prime ideals and prime divisors are in bijection via the maps $I_{(-)}$ and $\operatorname{div}(-)$, which are mutual inverses.

Theorem 6.8. *Let P be an affine point in $C(\overline{K})$ and let $\mathfrak{p}$ be a non-zero prime ideal of $K[C]$. Then*

(i) $I_{\operatorname{div} \mathfrak{p}} = \mathfrak{p}$;

(ii) $\operatorname{div} I_{[P]} = [P]$.

Proof. (i) Let $\mathfrak{p}$ be a non-zero prime ideal of $K[C]$. Then there is an affine point $P \in \operatorname{supp}(\operatorname{div}\mathfrak{p})$. Applying Proposition 6.7 twice,

$$\operatorname{div} I_{[P]} = \operatorname{div}\mathfrak{p} = [P].$$

(ii) Let P be an affine point in $C(\overline{K})$ and let $\mathfrak{p} = I_{[P]}$. Applying Proposition 6.7 twice,

$$I_{\operatorname{div}\mathfrak{p}} = I_{[P]} = \mathfrak{p}.$$

□

6.2 Ideals and Divisors

The coordinate ring $K[C]$ is a Dedekind domain. The non-zero ideals of $K[C]$ may be factored into a product of prime ideals, and this factorization is unique. Our isomorphism between prime ideals and prime divisors can now be extended to an isomorphism between the monoid of non-zero $K[C]$-ideals and the monoid $\operatorname{Div}_K^{\geq 0}$ of divisors $D \geq 0$. In the sections to follow, we extend it even further to an isomorphism between the ideal and divisor class groups.

Let $\mathfrak{a}$ be a non-zero ideal of $K[C]$. Let its factorization into prime ideals be $\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_n^{k_n}$. Then define the divisor of $\mathfrak{a}$ to be

$$\operatorname{div}\mathfrak{a} = \sum_{i=1}^{n} k_i \operatorname{div}\mathfrak{p}_i.$$

The divisor of $\mathfrak{a}$ is the sum of the divisors of its prime factors. As for the whole ring $K[C]$ itself, its prime factorization is the empty product which maps to the empty sum:

$$\operatorname{div}(K[C]) = 0.$$

Note that the divisor of $\mathfrak{a}$ is of degree zero and defined over K, by virtue of it being a sum of prime divisors in $\mathrm{Div}^0_K(C)$.

In the other direction, let D be a non-zero divisor in $\mathrm{Div}^{\geq 0}_K(C)$. Then it factors into a sum of prime divisors, say $D = k_1[P_1] + \cdots + k_n[P_n]$. Define the ideal of D to be

$$I_D = \prod_{i=1}^{n} I_{[P_i]}^{k_i}.$$

The divisor 0 is the empty sum. Let it map to the empty product, which is the whole ring $K[C]$:

$$I_0 = K[C].$$

Let $\mathcal{I}_C$ be the monoid of non-zero ideals of $K[C]$. We now have maps $\mathrm{div}(-) : \mathcal{I}_C \to \mathrm{Div}^0_K(C)$ and $I_{(-)} : \mathrm{Div}^0_K(C) \to \mathcal{I}_C$.

Theorem 6.9. *The maps* $\mathrm{div}(-)$ *and* $I_{(-)}$ *are isomorphisms of monoids and mutual inverses.*

Proof. That these maps are monoid homomorphisms is clear from their definitions. We show that they are mutual inverses.

Let $I \in \mathcal{I}_C$. Let its prime factorization be $\prod \mathfrak{p}_i^{k^i}$. Then

$$\begin{aligned}
I &= \prod_{i=1}^{n} \mathfrak{p}_i^{k_i} \\
\mathrm{div}\, I &= \sum_{i=1}^{n} k_i[P_i] && \text{where } P_i \in \mathrm{supp}(\mathrm{div}\, \mathfrak{p}_i) \\
I_{\mathrm{div}\, I} &= \prod_{i=1}^{n} I_{[P_i]}^{k_i} \\
&= \prod_{i=1}^{n} \mathfrak{p}_i^{k_i} \\
&= I.
\end{aligned}$$

Let $D \in \mathrm{Div}_K^0(C)$. Let its prime factorization be $\sum k_i[P_i]$. Then

$$\begin{aligned} D &= \sum_{i=1}^{n} k_i[P_i] \\ I_D &= \prod_{i=1}^{n} I_{[P_i]}^{k_i} \\ \mathrm{div}(I_D) &= \sum_{i=1}^{n} k_i[P_i] \\ &= D. \end{aligned}$$

□

6.3 Fractional Ideals and $\mathrm{Div}_K^0(C)$

We may extend the maps even further to fractional ideals and the entirety of $\mathrm{Div}_K^0(C)$.

Let $\mathcal{J}_C$ denote the Abelian group of fractional ideals of $K[C]$. Let $\mathfrak{a} \in \mathcal{J}_C$. Then $\mathfrak{a}$ is of the form $\left\langle \frac{1}{f} \right\rangle \mathfrak{b}$ for some non-zero polynomial $f \in K[C]$ and some integral ideal $\mathfrak{b}$ of $K[C]$. Define

$$\mathrm{div}\, \mathfrak{a} = \mathrm{div}\, \mathfrak{b} - \mathrm{div}\, f.$$

Let $D \in \mathrm{Div}_K^0(C)$. Then D can be written in the form $D = A - \mathrm{div}(f)$ where $A \in \mathrm{Div}_K^{\geq 0}(C)$. Define

$$I_D = \left\langle \frac{1}{f} \right\rangle I_A.$$

We show that these two maps are well-defined. Afterwards, we show that they are group homomorphisms. Then, in similar fashion to the previous section, we end by showing they are isomorphisms and mutual inverses.

Proposition 6.10. *The map* $\mathrm{div}(-) : \mathcal{J}_C \to \mathrm{Div}_K^0(C)$ *is well defined.*

Proof. Suppose that $\mathfrak{a}$ is a fractional ideal, $\mathfrak{b}$ and $\mathfrak{c}$ are integral ideals, f and g are non-zero

polynomials, and

$$\mathfrak{a} = \frac{1}{f}\mathfrak{b} = \frac{1}{g}\mathfrak{c}.$$

Then $g\mathfrak{b} = f\mathfrak{c}$ are integral ideals and

$$g\mathfrak{b} = f\mathfrak{c}$$

$$\operatorname{div}(g\mathfrak{b}) = \operatorname{div}(f\mathfrak{c})$$

$$\operatorname{div}(g) + \operatorname{div}\mathfrak{b} = \operatorname{div}(f) + \operatorname{div}\mathfrak{c}$$

$$\operatorname{div}\mathfrak{b} - \operatorname{div}(f) = \operatorname{div}\mathfrak{c} - \operatorname{div}(g)$$

□

Proposition 6.11. *The map* $I_{(-)} : \operatorname{Div}_K^0(C) \to \mathcal{J}_C$ *is well defined.*

Proof. Suppose that $D, A, B \in \operatorname{Div}_K^0(C)$, $A, B \geq 0$, $f, g \in K[C]$ are non-zero, and

$$D = A - \operatorname{div}(f) = B - \operatorname{div}(g).$$

Then

$$A + \operatorname{div}(g) = B + \operatorname{div}(f)$$

$$I_{A+\operatorname{div}(g)} = I_{B+\operatorname{div}(f)}$$

$$I_A I_{\operatorname{div}(g)} = I_B I_{\operatorname{div}(f)}$$

$$gI_A = fI_B$$

$$\frac{1}{f}I_A = \frac{1}{g}I_B.$$

□

Proposition 6.12. *The map* $\operatorname{div}(-) : \mathcal{J}_C \to \operatorname{Div}_K^0(C)$ *is a group homomorphism.*

Proof. Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals, and let

$$\mathfrak{a} = \frac{1}{f}\mathfrak{a}', \quad \mathfrak{b} = \frac{1}{g}\mathfrak{b}',$$

where $\mathfrak{a}'$ and $\mathfrak{b}'$ are integral ideals. Then

$$\begin{aligned}
\operatorname{div}(\mathfrak{a}\mathfrak{b}) &= \operatorname{div}\left(\frac{1}{fg}\mathfrak{a}'\mathfrak{b}'\right) \\
&= \operatorname{div}(\mathfrak{a}'\mathfrak{b}') - \operatorname{div}(fg) \\
&= \operatorname{div}\mathfrak{a}' + \operatorname{div}\mathfrak{b}' - \operatorname{div} f - \operatorname{div} g \\
&= (\operatorname{div}\mathfrak{a}' - \operatorname{div} f) + (\operatorname{div}\mathfrak{b}' - \operatorname{div} g) \\
&= \operatorname{div}\mathfrak{a} + \operatorname{div}\mathfrak{b}.
\end{aligned}$$

□

Proposition 6.13. *The map $I_{(-)} : \operatorname{Div}_K^0(C) \to \mathcal{J}_C$ is a group homomorphism.*

Proof. Let $A, B \in \operatorname{Div}_K^0(C)$ and let

$$A = A' - \operatorname{div} f, \quad B = B' - \operatorname{div} g,$$

where $A', B' \geq 0$. Then

$$\begin{aligned}
I_{A+B} &= I_{A'+B'-\operatorname{div}(fg)} \\
&= \frac{1}{fg} I_{A'+B'} \\
&= \frac{1}{fg} I_{A'} I_{B'} \\
&= \left(\frac{1}{f} I_{A'}\right)\left(\frac{1}{g} I_{B'}\right) \\
&= I_A I_B.
\end{aligned}$$

□

Theorem 6.14. *The maps* $\operatorname{div}(-) : \mathcal{J}_C \to \operatorname{Div}_K^0(C)$ *and* $I_{(-)} : \operatorname{Div}_K^0(C) \to \mathcal{J}_C$ *are group isomorphisms and mutual inverses.*

Proof. Let $\mathfrak{a}$ be a fractional ideal with $\mathfrak{a} = \frac{1}{f}\mathfrak{a}'$, where $\mathfrak{a}'$ is integral. Then

$$\begin{aligned} I_{\operatorname{div}\mathfrak{a}} &= I_{\operatorname{div}\mathfrak{a}' - \operatorname{div} f} \\ &= \frac{1}{f} I_{\operatorname{div}\mathfrak{a}'} \\ &= \frac{1}{f}\mathfrak{a}' \\ &= \mathfrak{a}. \end{aligned}$$

Let D be a degree zero divisor defined over K with $D = D' - \operatorname{div} f$, where $D' \geq 0$. Then

$$\begin{aligned} \operatorname{div} I_D &= \operatorname{div}\left(\frac{1}{f} I_{D'}\right) \\ &= \operatorname{div} I_{D'} - \operatorname{div} f \\ &= D' - \operatorname{div} f \\ &= D. \end{aligned}$$

□

6.4 The Ideal Class Group

Let $\mathcal{J}_C$ be the group of fractional ideals of $K[C]$ and let $\mathcal{P}_C$ denote its subgroup of principal ideals. The **ideal class group** of $K[C]$ is

$$\mathcal{H}_C = \frac{\mathcal{J}_C}{\mathcal{P}_C}.$$

Since $\mathcal{J}_C$ is isomorphic to $\mathrm{Div}_K^0(C)$ and $\mathcal{P}_C$ to $\mathrm{Princ}_K(C)$, we have

$$\mathcal{H}_C \simeq \mathrm{Cl}_K^0(C).$$

In the ideal class group, two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if there is a rational function $\frac{f}{g} \in K(C)$ such that $\mathfrak{a} = \frac{f}{g}\mathfrak{b}$. Under this relation, every fractional ideal is equivalent to an integral ideal. Thus every ideal class has an integral representative. In particular, given an ideal class $[\mathfrak{a}]$, the inverse class $[\mathfrak{a}^{-1}]$ has an integral representative, given by a colon ideal (see Appendix A).

Proposition 6.15. *Let $\mathfrak{a}$ be a non-zero ideal of $K[C]$, and $[\mathfrak{a}]$ its image in the ideal class group. Let $\alpha \in \mathfrak{a}$. Then*

$$[\mathfrak{a}]^{-1} = [\alpha : \mathfrak{a}].$$

Proof. By Corollary A.4,

$$\mathfrak{a}(\alpha : \mathfrak{a}) = (\alpha)$$

as ideals. In the ideal class group,

$$[\mathfrak{a}][\alpha : \mathfrak{a}] = [\alpha] \equiv [1],$$

so that $\mathfrak{a}$ and $\alpha : \mathfrak{a}$ are inverses of one another. □

Since the divisor and ideal class groups are isomorphic, and every ideal class has an integral representative, we may now represent divisor classes by integral ideals, i.e. ideals generated by polynomials. There is no need to work with fractional ideals and rational functions. In the next chapter, we discuss this representation by polynomials in greater detail.

7 Representation

In Chapter 5, we defined the divisor class group of a curve C, and in Chapter 6, we showed that this group is isomorphic to the ideal class group of the curve's coordinate ring, $K[C]$. This forms the foundation of our representation of divisors. We will represent an effective divisor by its associated integral ideal, or more specifically, by the unique reduced Gröbner basis of that ideal. These bases come in many forms, but if we place a bound on the degree of the divisors under consideration, these forms are only finite in number.

In this chapter, we will categorize all the different types of divisors of degree 6 or less. When adding divisors in Chapter 8, we will always assume our summands are of degree 3 or less, thus it is unnecessary to tabulate divisors of degree 7 and higher. We will see which of these types are reduced (not equivalent to a divisor of lesser degree) and which are typical (the statistically most likely to be encountered).

At the end of Section 5.1, we established that every divisor class has a representative D of the form

$$D = P_i + \ldots + P_n - nP_\infty,$$

where the P_i's are finite points, not necessarily distinct. That is, D is equal to an effective divisor minus a multiple of the point P_∞ at infinity. Henceforth, in light of this observation, we will assume that all divisors we work with are of this form. Since the order of P_∞ is determined by the number of finite points in D (counting multiplicities), we will refer to D only by its finite part. For example, when we say D is the degree 3 divisor $D = P + Q + R$, we really mean the degree 0 divisor $D = P + Q + R - 3P_\infty$.

7.1 Divisor Types

In [3], Arita classifies divisors of degree 6 and less into 19 types based on the forms of the reduced Gröbner bases of their ideals. This classification is reproduced in Table 7.1, along with a 20th type representing the divisor 0. Divisors are listed by degree (D), then by type

(T).

Table 7.1: Classification of divisors into types

D	T	Gröbner Basis
0	0	1
1	11	$x + f_0$ $y + g_0$
2	21	$y + f_1x + f_0$, $x^2 + g_1x + g_0$
	22	$x + f_0$, $y^2 + g_2y + g_0$
3	31	$x^2 + f_2y + f_1x + f_0$, $xy + g_2y + g_1x + g_0$, $y^2 + h_2y + h_1x + h_0$
	32	$y + f_1x + f_0$, $x^3 + g_3x^2 + g_1x + g_0$
	33	$x + f_0$
4	41	$xy + f_3x^2 + f_2y + f_1x + f_0$, $y^2 + g_3x^2 + g_2y + g_1x + g_0$, $x^3 + h_3x^2 + h_2y + h_1x + h_0$
	42	$x^2 + f_1x + f_0$, $xy + g_2y + g_1x + g_0$
	43	$x^2 + f_2y + f_1x + f_0$, $y^2 + g_4xy + g_2y + g_1x + g_0$
	44	$y + f_1x + f_0$

D	T	Gröbner Basis
5	51	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0$, $x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0$, $x^2y + h_4xy + h_3x^2 + h_2y + h_1x + h_0$
	52	$xy + f_3x^2 + f_2y + f_1x + f_0$, $y^2 + g_3x^2 + g_2y + g_1x + g_0$
	53	$xy + f_3x^2 + f_2y + f_1x + f_0$, $x^3 + g_5y^2 + g_3x^2 + g_2y + g_1x + g_0$
	54	$x^2 + f_2y + f_1x + f_0$, $xy^2 + g_5y^2 + g_4xy + g_2y + g_1x + g_0$
6	61	$x^3 + f_5y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0$, $x^2y + g_5y^2 + g_4xy + g_3x^2 + g_2y + g_1x + g_0$, $xy^2 + h_5y^2 + h_4xy + h_3x^2 + h_2y + h_1x + h_0$
	62	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0$, $x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0$
	63	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0$, $x^2y + g_6x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0$
	64	$xy + f_3x^2 + f_2y + f_1x + f_0$, $x^4 + g_6x^3 + g_5y^2 + g_3x^2 + g_2y + g_1x + g_0$
	65	$x^2 + f_2y + f_1x + f_0$

So, for example, divisors of degree 2 come in two types: type 21 and type 22. If D is a type 21 divisor, then the unique reduced Gröbner basis of I_D is of the form $\langle y + f_1x + f_0, x^2 + g_1x + g_0\rangle$, where f_0, f_1, g_0, and g_1 lie in the base field K over which the curve is defined. If D is instead a type 22 divisor, then the unique reduced Gröbner basis of I_D is of the form $\langle x + f_0, y^2 + g_2y + g_0\rangle$.

The type 42 divisor in this table differs slightly from the type 42 divisor as presented by Arita in [3]. In [3], a type 42 divisor has a generator of the form $x^2 + a_3y + a_2x + a_1$, though in the table above, the coefficient of y is assumed to be 0. One can show that, were the coefficient of y non-zero, the divisor would be of type 31 instead. (See Theorem 7.16, below).

This table hides the fact that there are many dependencies between the coefficients. For

instance, it can be shown that type 11 divisors are in bijection with type 22 divisors. Type 22 divisors, in a sense, carry only as much information as type 11 divisors. Where the latter are specified uniquely by two field elements, one would hope that type 22 divisors could also be represented by only two elements. Indeed, one can show that if $\langle x + f_0, y^2 + g_2 y + g_0 \rangle$ is in bijection with some type 11 divisor $\langle x + f_0, y + g_0' \rangle$, then

$$g = y^2 + g_2 y + g_0 = \frac{F(-f_0, y)}{y - g_0'},$$

where F is the curve's defining polynomial. Hence f_0, g_0, g_2 can be written in terms of f_0, g_0' and the curve coefficients, so that there is some dependency between the three.

As another example, a type 31 divisor is generated by three polynomials f, g, and h, but typically $h \in \langle f, g \rangle$. (See Definition 7.14 and Theorem 7.16.) This implies that the coefficients of h depend on the coefficients of f, g, and the curve equation C.

7.2 Operations

Chapter 6 established the correspondence between divisors and ideals. Addition of divisors is equivalent to multiplication of ideals. What's more, for divisors A, B, $A \leq B \iff I_B \subseteq I_A$. Divisors form a lattice $(\mathrm{Div}_{\overline{K}}^{\geq 0}(C), \leq)$, as do ideals $(\mathcal{I}_C, \subseteq)$. The map between the two is order-reversing. The meet of two divisors (their gcd) corresponds to the join of two ideals (their ideal sum). The join of two divisors (their lcm) corresponds to the meet of two ideals (their ideal intersection). We have the following equivalences of operations.

Divisors	Ideals
$A + B$	$I_A I_B$
$\mathrm{lcm}(A, B)$	$I_A \cap I_B$
$\gcd(A, B)$	$I_A + I_B$
$\overline{A}$	$f : I_A$

where f is the minimum polynomial[20] in I_A. This last operation we define now.

[20] As in Definition 3.21.

Definition 7.1. Let D be a divisor, with corresponding ideal I_D in the ideal class group. Let f be the minimum polynomial of I_D. The **flip of** D is the divisor

$$\overline{D} := \mathrm{div}(f : I_D).$$

By Proposition 6.15, $f : I_D \equiv I_D^{-1}$ in the ideal class group, so $\overline{D} \equiv -D$ in the divisor class group.

Of course, one may choose some non-minimum polynomial $g \in I_D$ and compute $\mathrm{div}(g : I_D)$ to get some other divisor, which is also equivalent to $-D$ by Proposition 6.15. Once we have defined what a reduced divisor is, we can show that, if f is chosen to be the minimum polynomial in I_D, then $\overline{D}$ is reduced.

Geometrically, to flip a divisor D is to find the polynomial f of least degree interpolating the points of D, then taking the zeroes of f along C that are not in D, properly accounting for multiplicity.

Example 7.2. See Figure 7.1. The three black points form a degree 3, type 31 divisor D. The minimum polynomial $f = x^2 + f_2 y + f_1 x + f_0 \in I_D$ is a parabola which interpolates these points. This parabola intersects C at six points – the points of D plus three other points. The flip $\overline{D}$ consists of the three white points not in D.

7.3 Reduced Divisors

Definition 7.3. Let $D \geq 0$ be a divisor in $\mathrm{Div}_K^0(C)$. Then D is called **reduced** if $\overline{\overline{D}} = D$.

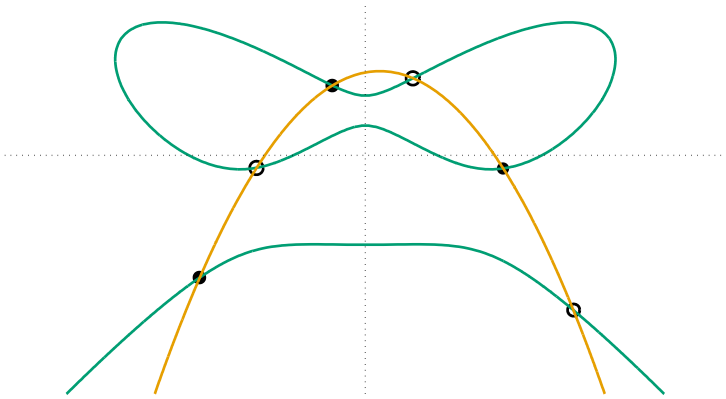
Proposition 7.4. *Let* $A, B \in \mathrm{Div}_K^{\geq 0}(C)$.

(i) $\overline{A} \equiv -A$;

(ii) $\overline{\overline{A}} \equiv A$;

(iii) $A \equiv B \iff \overline{A} = \overline{B}$;

Figure 7.1: A degree 3 divisor and its flip.



(iv) $\overline{\overline{\overline{A}}} = \overline{A}$;

(v) $\overline{A}$ *is reduced.*

Proof. (i) This is simply Proposition 6.15 translated into the language of divisors.

(ii) Immediate by part (i).

(iii) ($\implies$) Suppose $A \equiv B$. Then in the ideal class group, $I_A \equiv I_B$, so that there are polynomials $f, g \in K[C]$ such that $gI_A = fI_B$. Without loss of generality, we may assume f and g are monic. Let a and b be the minimal polynomials in I_A and I_B, respectively. Then the minimum polynomials in gI_A and fI_B are ga and fb, respectively. Since $gI_A = fI_B$, we have $ga = fb$.

Suppose $h \in a : I_A$. Then

$$hI_A \subseteq \langle a \rangle$$
$$hgI_A \subseteq \langle ga \rangle$$
$$hfI_B \subseteq \langle fb \rangle$$
$$hI_B \subseteq \langle b \rangle ,$$

so $h \in b : I_B$. Likewise, if $h \in b : I_B$, then $h \in a : I_A$. Hence $a : I_A = b : I_B$ and $\overline{A} = \overline{B}$.

($\Longleftarrow$) If $\overline{A} = \overline{B}$, then

$$A \equiv -\overline{A} = -\overline{B} \equiv B.$$

(iv) By part (ii), $\overline{\overline{A}} \equiv A$. By part (iii), $\overline{\overline{\overline{A}}} = \overline{A}$.

(v) After part (iv), immediate by Definition 7.3.

□

This proposition is central to the divisor class arithmetic described in this thesis and the unique representation of divisor classes. Given any divisor class $[D]$, we can find a reduced member of that class by flipping D twice, computing $\overline{\overline{D}}$. As the next theorem shows, this reduced representative is *unique*.

Theorem 7.5. *Every divisor class $[D]$ has a unique reduced representative.*

Proof. If $[D]$ is a divisor class, then by parts (ii) and (v) of Proposition 7.4, $\overline{\overline{D}}$ is a reduced divisor in the same class, establishing existence.

For uniqueness, suppose A and B are equivalent reduced divisors. Applying Proposition 7.4.(iii) twice, we have $\overline{A} = \overline{B}$ and $\overline{\overline{A}} = \overline{\overline{B}}$. By Definition 7.3,

$$A = \overline{\overline{A}} = \overline{\overline{B}} = B.$$

□

Another consequence of Proposition 7.4 is the following, which we will make use of many times later in this chapter.

Proposition 7.6. *Let I_A and I_B be ideals with $I_A \equiv I_B$. Let a and b be the minimum polynomials in I_A and I_B, respectively. Then $aI_B = bI_A$.*

Proof. Since the divisor and ideal class groups are isomorphic, we may move between the groups.

$$
\begin{aligned}
I_A &\equiv I_B && \\
A &\equiv B && \text{Thm. 6.14} \\
\overline{A} &= \overline{B} && \text{Prop. 7.4.(iii)} \\
a : I_A &= b : I_B && \text{Def. 7.1} \\
(a : I_A) I_A I_B &= (b : I_B) I_B I_A && \\
aI_B &= bI_A && \text{Prop. 6.15.}
\end{aligned}
$$

□

If D is a divisor, then the degree and type of $\overline{D}$ are determined by the type of D. We may use the formula

$$\deg \overline{D} = \deg(\operatorname{div} f) - \deg D, \tag{7.7}$$

where f is the minimum polynomial in I_D. The degree of $\operatorname{div} f$ is determined by $\mathrm{LM}(f)$, which is determined in turn by the type of D.

Example 7.8. Suppose D is a type 51 divisor. The minimum polynomial f of I_D is

$$f = y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0.$$

Then

$$\begin{aligned}
\deg \overline{D} &= \deg(\operatorname{div} f) - \deg D \\
&= -\nu_{P_\infty}(f) - \deg D \\
&= -\nu_{P_\infty}(y^2) - \deg D \\
&= 8 - 5 = 3 \qquad \text{By Prop. 2.17, } -\nu_{P_\infty}(y^2) = 8.
\end{aligned}$$

By applying Equation 7.7, we can compute the degree of $\overline{D}$ for D of any divisor type.

Table 7.2: Divisor types and the degrees of their flips

type(D)	0	11	21	22	31	32	33	41	42	43
$\deg \overline{D}$	0	2	2	1	3	1	0	3	2	2
type(D)	44	51	52	53	54	61	62	63	64	65
$\deg \overline{D}$	0	3	2	2	1	3	2	2	1	0

We can do even better. Not only can we determine the degree of $\overline{D}$, but also its type. We begin by giving an example of this determination for a divisor of small degree.

Example 7.9. Let D be a type 11 divisor. Then the minimum polynomial of I_D is $f = x + f_0$ for some $f_0 \in K$. By Equation 7.7, $\deg(\overline{D}) = 2$, so $\overline{D}$ is of type 21 or 22. Since $f \in f : I_D = I_{\overline{D}}$, $\overline{D}$ must be of type 22 — were $\overline{D}$ of type 21, its reduced Gröbner basis would have the form $\langle y + \ldots, x^2 + \ldots \rangle$, but an ideal with such a basis cannot contain a polynomial with leading monomial x.

Applying the same reasoning as in Example 7.9, we can determine the type of $\overline{D}$ for all D of degree 3 or less. These are given Table 7.3. To calculate the type of the flip of a divisor of degree greater than 3, it will be helpful to first classify reduced divisors. Table 7.3 will also help us in making that classification. First, we must show that all reduced divisors are of degree 3 or less. It is a well-known fact that reduced divisors on an algebraic curve are of degree g or less, where g is the genus of the curve, 3 in the $C_{3,4}$ curve case. This fact is

a consequence of the Riemann-Roch Theorem, however in this thesis, reduced divisors have been defined in a non-standard way. Rather than a diversion into Riemann-Roch theory, we relegate to Appendix B a proof that reduced divisors have degree 3 or less using the theory of Gröbner bases.

Table 7.3: (Small) Divisor types and the type of their flips

type(D)	0	11	21	22	31	32	33
type($\overline{D}$)	0	22	21	11	31	11	0
type($\overline{\overline{D}}$)	0	11	21	22	31	22	0

Theorem 7.10. *A divisor is reduced if and only if it is of type 0, 11, 21, 22, or 31.*

Proof. By Theorem B.6, a reduced divisor has degree 3 or less, therefore it must be of type 0, 11, 21, 22, 31, 32, or 33. On examination of the above table, if D is of type 32 or 33, then $\overline{\overline{D}}$ is of a different type. Hence $D \neq \overline{\overline{D}}$ and D is not reduced.

Clearly, the divisor of type 0 is reduced, since $\overline{\overline{0}} = 0$.

Suppose D is of type 31. (The argument to follow applies to types 11, 21, and 22, *mutatis mutandis*.) Let f be the minimum polynomial in I_D. Then $f \in I_{\overline{D}}$, and since $\overline{D}$ is also of type 31, f must be the minimum polynomial in $I_{\overline{D}}$. So, too, is f the minimum polynomial in $I_{\overline{\overline{D}}}$. By 7.6, $fI_{\overline{\overline{D}}} = fI_D$, and

$$fI_{\overline{\overline{D}}} = fI_D$$
$$fI_{\overline{\overline{D}}} : f = fI_D : f$$
$$I_{\overline{\overline{D}}} = I_D,$$

hence $\overline{\overline{D}} = D$ and D is reduced. □

We now give a couple more examples of determining types for flips of divisors and fill in Table 7.3 for all remaining divisor types.

Example 7.11. Let D be a type 61 divisor. By equation 7.7, $\deg \overline{D} = 3$. By Proposition 7.4, $\overline{D}$ is reduced. By Theorem 7.10, $\overline{D}$ must be of type 31.

Example 7.12. Let D be a type 62 divisor. By equation 7.7, $\deg \overline{D} = 2$, so $\overline{D}$ must be of type 21 or 22. The ideal of D is $I_D = \langle f, g \rangle$, where $\mathrm{LM}(f) = y^2$ and $\mathrm{LM}(g) = x^3$. There is no polynomial $r \in f : g$ with leading monomial y. If there were, then there would be a polynomial $s \in K[C]$ such that $rg \equiv sf$. Then

$$\begin{aligned} -\nu_{P_\infty}(rg) &= -\nu_{P_\infty}(sf) \\ -\nu_{P_\infty}(r) - \nu_{P_\infty}(g) &= -\nu_{P_\infty}(s) - \nu_{P_\infty}(f) \\ 4 + 9 &= -\nu_{P_\infty}(s) + 8 \\ -\nu_{P_\infty}(s) &= 5. \end{aligned}$$

However, there is no polynomial in $K[C]$ with pole order 5 at infinity.

Since no polynomial with leading monomial y can exist in $f : g = I_{\overline{D}}$, $\overline{D}$ cannot be of type 21 and must therefore be of type 22.

Table 7.4: Divisor types and the type of their flips

type(D)	0	11	21	22	31	32	33	41	42	43
type($\overline{D}$)	0	22	21	11	31	11	0	31	22	21
type($\overline{\overline{D}}$)	0	11	21	22	31	22	0	31	11	21
type(D)	44	51	52	53	54	61	62	63	64	65
type($\overline{D}$)	0	31	22	21	11	31	22	21	11	0
type($\overline{\overline{D}}$)	0	31	11	21	22	31	11	21	22	0

7.4 Typical Divisors

While some publications on $C_{3,4}$ curve divisor arithmetic have described algorithms for adding general divisors [3, 18], the most efficient algorithms have been from those publications that have focused only on "typical" divisors [40, 26, 13]. These divisors are typical

in the sense that, as $q \to \infty$, over a finite field of order q, the probability that a divisor chosen uniformly at random is atypical is $O\left(\frac{1}{q}\right)$ (see Theorem 2.10 in [26]); the chance of encountering an atypical divisor becomes vanishingly small over large finite fields.

In [26], Khuri-Makdisi defines semi-typical and typical divisors of arbitrary curves and in Proposition 2.12 of the same article gives a characterization of degree 3 semi-typical and typical divisors on $C_{3,4}$ curves. We adopt the same definitions here, as they apply to the $C_{3,4}$ case.

Definition 7.13. A divisor D is called **semi-typical** if $I_D = \langle f, g, h\rangle$ where

(i) $\{f, g, h\}$ is a reduced Gröbner basis for I_D;

(ii) $-\nu_{P_\infty}(f) = \deg D + 3$;

(iii) $-\nu_{P_\infty}(g) = \deg D + 4$; and

(iv) $-\nu_{P_\infty}(h) = \deg D + 5$.

Divisors of types 31, 41, 51, and 61 are semi-typical. There exist also semi-typical divisors of degrees 7 and greater.

Definition 7.14. A divisor D is called **typical** if D is semi-typical and $I_D = \langle f, g\rangle$.

That is, while $\{f, g\}$ alone are not a Gröbner basis for I_D, they are still enough to generate I_D if D is typical.

This definition of typicality differs from other authors' definitions. Of note is this definition due to Flon et al.

Definition 7.15 (Flon et al [13])**.** A degree 3 divisor is **typical** if it is the sum of three non-collinear points with pairwise distinct x-coordinates.

This definition more restrictive than Definition 7.14. This definition does not apply to divisors of degree other than 3. In the degree 3 case, Definition 7.14 allows for points to

appear with multiplicity greater than one, as long as the interpolation polynomial through the three points is not a line. Double and triple points are barred by Definition 7.15's requirement that points have pairwise distinct x-coordinates. Going forward, we adopt Definition 7.14.

A reduced divisor may be of type 0, 11, 21, 22, or 31, but a reduced *typical* divisor may only be of type 31. However, not all type 31 divisors are typical (though they are all semi-typical). Here we give a characterization of typical type 31 divisors.

Theorem 7.16 (Khuri-Makdisi [26])**.** *Let D be a type 31 divisor, with minimum polynomial $x^2 + f_2y + f_1x + f_0 \in I_D$. Then D is typical if and only if $f_2 \neq 0$.*

Proof. ($\Longrightarrow$) Suppose $f_2 = 0$. Then $I_D = \langle f, g, h \rangle$ with

$$f = x^2 + f_1x + f_0$$
$$g = xy + g_2y + g_1x + g_0$$
$$h = y^2 + h_2y + h_1x + h_0.$$

The polynomial f factors into $(x - x_0)(x - x_1)$ for some $x_0, x_1 \in \overline{K}$. The divisor D is the sum of three points, say $D = P + Q + R$. By the pigeonhole principle, at least two of these points fall on the same vertical line, $x - x_0$ or $x - x_1$. Without loss of generality, suppose P and Q fall on $x - x_0$.

Geometrically, g is a hyperbola through P, Q and R. Either g passes through two distinct points on the same vertical line, or if $P = Q$, g is tangent to C at P and the tangent line to C at P is $x - x_0$. In either case, g is a degenerate hyperbola and factors into a product of two lines, $g = (x - x_0)(y - y_0)$.

Now suppose there are polynomials r, s such that $h = rf + sg$.

$$\begin{aligned} y^2 &= \mathrm{LM}(h) \\ &= \mathrm{LM}(rf + sg) \\ &= \mathrm{LM}(r(x - x_0)(x - x_1) + s(x - x_0)(y - y_0)) \\ &= \mathrm{LM}(x - x_0)\,\mathrm{LM}(r(x - x_1) + s(y - y_0)) \\ &= x\,\mathrm{LM}(r(x - x_1) + s(y - y_0)). \end{aligned}$$

However, x does not divide y^2, so no such polynomials r and s can exist. Therefore D must be atypical.

($\Longleftarrow$) Suppose $f_2 \neq 0$. Then I_D is generated by three polynomials

$$\begin{aligned} f &= x^2 + f_2 y + f_1 x + f_0 \\ g &= xy + g_2 y + g_1 x + g_0 \\ h &= y^2 + h_2 y + h_1 x + h_0. \end{aligned}$$

Let

$$k = \frac{(y + g_1)f - (x + f_1 - g_2)g}{f_2}.$$

One can verify that k is monic, has leading monomial y^2, and has no xy or x^2 terms. Thus

$$k = y^2 + k_2 y + k_1 x + k_0$$

for some coefficients $k_0, k_1, k_2 \in K$. Since $\{f, g, h\}$ is a reduced Gröbner basis, h is the unique polynomial of this form, so $k = h$. As k was generated by f and h, so too must be h. Hence $I_D = \langle f, g, h \rangle = \langle f, g \rangle$. □

In [26], it is shown that typicality and semi-typicality are preserved by the flip operation.

Theorem 7.17. *A divisor D is semi-typical if and only if its flip $\overline{D}$ is semi-typical.*

Proof. ($\Longrightarrow$) Suppose D is semi-typical. Let f be the minimum polynomial in I_D. Then $-\nu_{P_\infty}(f) = \deg D + 3$. By Equation 7.7, $\deg \overline{D} = 3$. Since $\overline{D}$ is reduced and of degree 3, $\overline{D}$ is of type 31, hence semi-typical.

($\Longleftarrow$) Suppose $\overline{D}$ is semi-typical. Then $\overline{D}$ is of type 31. So, too, is $\overline{\overline{D}}$ of type 31, and $\overline{\overline{D}} \equiv D$. Let $I_{\overline{\overline{D}}} = \langle u, v, w \rangle$. Then u is the minimum polynomial in $I_{\overline{\overline{D}}}$, $-\nu_{P_\infty}(u) = 6$, $-\nu_{P_\infty}(v) = 7$, and $-\nu_{P_\infty}(w) = 8$. Now let f be the minimum polynomial in I_D. By Equation 7.7, $-\nu_{P_\infty}(f) = \deg D + 3$. By Proposition 7.6,

$$fI_{\overline{\overline{D}}} = uI_D,$$

hence $\langle fu, fv, fw \rangle = \langle fu, gu, hu \rangle$, and $fv = gu$ and $fw = hu$. Then

$$\begin{aligned} -\nu_{P_\infty}(fv) &= -\nu_{P_\infty}(gu) \\ -\nu_{P_\infty}(v) + \nu_{P_\infty}(u) &= -\nu_{P_\infty}(g) + \nu_{P_\infty}(f) \\ 7 - 6 &= -\nu_{P_\infty}(g) - \deg D - 3 \\ -\nu_{P_\infty}(g) &= \deg D + 4. \end{aligned}$$

Likewise, $-\nu_{P_\infty}(h) = \deg D + 5$. □

Theorem 7.18. *A divisor D is typical if and only if its reduction $\overline{\overline{D}}$ is typical.*

Proof. ($\Longrightarrow$) Let $I_D = \langle f, g, h \rangle$. Let $I_{\overline{\overline{D}}} = \langle u, v, w \rangle$. Since D is typical, $h \in \langle f, g \rangle$, so there

are polynomials $r, s \in K[C]$ such that $h = rf + sg$. Then

$$\begin{aligned} uI_D &= fI_{\overline{\overline{D}}} \\ \langle fu, gu, hu \rangle &= \langle fu, fv, fw \rangle \\ fw &= hu \\ &= (rf + sg)u \\ &= rfu + sfv \\ w &= ru + sv, \end{aligned}$$

hence $w \in \langle u, v \rangle$.

($\Longleftarrow$) Let $I_D = \langle f, g, h \rangle$. Let $I_{\overline{\overline{D}}} = \langle u, v, w \rangle$. Since $\overline{\overline{D}}$ is typical, $w \in \langle u, v \rangle$, so there are polynomials r and s such that $w = ru + sv$. Then, as above,

$$\begin{aligned} hu &= fw \\ &= f(ru + sv) \\ &= rfu + sgu \\ h &= rf + sg. \end{aligned}$$

□

Theorem 7.19. *A divisor D is typical if and only if its flip $\overline{D}$ is typical.*

Proof. We make use of many of the above theorems.

($\Longrightarrow$) Suppose D is typical. By Theorem 7.18, $\overline{\overline{D}}$ is typical. By Proposition 7.4, $\overline{\overline{D}}$ is reduced. By Theorem 7.10 and Definition 7.14, $\overline{\overline{D}}$ is of type 31. Referring to Table 7.1, the minimum polynomial of $I_{\overline{\overline{D}}}$ is $f = x^2 + f_2 y + f_1 x + f_0$, and by Theorem 7.16, $f_2 \neq 0$. The flip $\overline{\overline{\overline{D}}}$ of $\overline{\overline{D}}$ is also of type 31 (Table 7.3), and since $f \in f : I_{\overline{\overline{D}}} = I_{\overline{\overline{\overline{D}}}}$, $I_{\overline{\overline{\overline{D}}}}$ shares the same minimum polynomial f with $f_2 \neq 0$. Hence by Theorem 7.16, $\overline{\overline{\overline{D}}}$ is also typical. Since $\overline{D}$ is

reduced (Proposition 7.4), $\overline{\overline{\overline{D}}} = \overline{D}$ and the result follows.

($\Longleftarrow$) Suppose D is atypical. Then $\overline{\overline{D}}$ is atypical.

If $\overline{\overline{D}}$ is of type 31, then by Theorem 7.16, the minimum polynomial of $I_{\overline{\overline{D}}}$ is $f = x^2 + f_1 x + f_0$. As in the previous part of this proof, $\overline{D}$ is also of type 31 with the same minimum polynomial f, hence $\overline{D}$ is atypical by Theorem 7.16.

If $\overline{\overline{D}}$ is not of type 31, then $\overline{D}$ is of degree less than 3 (see Table 7.2) and cannot be typical. □

7.5 Semi-typical Divisors

A divisor D of type 31, 41, 51, or 61 may be typical or merely semi-typical. The ideal I_D of such a divisor is always generated by a Gröbner basis of three elements, $I_D = \langle f, g, h \rangle$. Typically, the first two polynomials f and g are enough to generate the ideal, and $I_D = \langle f, g \rangle$. That is, $h \in \langle f, g \rangle$, so there exist polynomials $r, s \in K[C]$ and a constant $t \in K$ such that

$$rf + sg + th \equiv 0 \pmod{F}. \tag{7.20}$$

Lemma 7.21. *Let $I_D = \langle f, g, h \rangle$ be a type 31 divisor. Then a solution to Equation 7.20 is given by*

$$\begin{aligned} r &= y + g_1 \\ s &= -(x + f_1 - g_2) \\ t &= -f_2, \end{aligned}$$

and $h \in \langle f, g \rangle$ if and only if $t \neq 0$.

Proof. The S-polynomial $S(f, g) = yf - xg = f_2 y^2 + \ldots$ reduces to 0 modulo $\langle f, g, h \rangle$ (in

the sense of Definition 3.16). So there exist constants $r_0, s_0, t_0 \in K$ such that

$$yf - xg - t_0 h - s_0 g - r_0 f = 0.$$

Solving for these constants gives $t_0 = f_2$, $s_0 = f_1 - g_2$, $r_0 = -g_1$.

If $t = -f_2 \neq 0$, this gives h in terms of f and g. Conversely, if $h \in \langle f, g \rangle$, then f and g generate I_D, but are not a Gröbner basis. Following Buchberger's Algorithm produces h by reducing $S(f, g)$ modulo $\{f, g\}$, but this implies $t_0 \neq 0$ above. □

Lemma 7.22. *Let $I_D = \langle f, g, h \rangle$ be a type 61 divisor. Then a solution to Equation 7.20 is given by*

$$\begin{aligned} r &= y + f_5 x + (g_3 - f_5(f_3 - c_6)) \\ s &= -(x + f_5(f_4 - c_7) + f_3 - g_4) \\ t &= -(f_5(f_5 - c_8) + f_4 - g_5), \end{aligned}$$

and $h \in \langle f, g \rangle$ if and only if $t \neq 0$.

Just as a type 31 divisor is typical if and only if $f_2 \neq 0$, a type 61 divisor is typical if and only if $f_5(f_5 - c_8) + f_4 - g_5 \neq 0$. The proof of Lemma 7.22 is almost identical to that of 7.21, so we omit it.

If D is semi-typical but not typical, it may still be the case that $\langle f, h \rangle = \langle f, g, h \rangle$. In this case, $g \in \langle f, h \rangle$ and there exist polynomials $r', t' \in K[C]$ and a constant $s' \in K$ such that

$$r'f + s'g + t'h \equiv 0 \pmod{F}. \tag{7.23}$$

Lemma 7.24. *Let $I_D = \langle f, g, h \rangle$ be a type 31 divisor. Then a solution to Equation 7.23 is*

given by

$$r' = x^2 + r'_2 y + r'_1 x + r'_0$$
$$s' = s'_0$$
$$t' = y + t'_1 x + t'_0$$

where

$$t'_1 = c_8$$
$$r'_2 = c_7 - f_2$$
$$r'_1 = c_6 - f_1$$
$$t'_0 = -f_2 r'_2 + c_5 - h_2$$
$$s'_0 = -f_2 r'_1 - f_1 r'_2 - h_2 t'_1 + c_4 - h_1$$
$$r'_0 = -f_1 r'_1 - h_1 t'_1 + c_3 - f_0,$$

and $g \in \langle f, h \rangle$ *if and only if* $s' \neq 0$.

Lemma 7.25. *Let* $I_D = \langle f, g, h \rangle$ *be a type 61 divisor. Then a solution to Equation 7.23 is given by*

$$r' = x^2 + r'_2 y + r'_1 x + r'_0$$
$$s' = s'_0$$
$$t' = y + t'_1 x + t'_0$$

where

$$
\begin{aligned}
t'_1 &= c_8 - f_5 \\
r'_2 &= c_7 - f_4 \\
r'_1 &= f_5 r'_2 + c_6 - f_3 + h_5 \\
t'_0 &= c_8 f_5 r'_2 + c_8 h_5 - f_5 r'_1 - f_4 r'_2 - h_5 t'_1 + c_5 - h_4 \\
s'_0 &= c_7 f_5 r'_2 + c_7 h_5 - f_4 r'_1 - f_3 r'_2 - h_4 t'_1 + c_4 - f_2 - h_4 \\
r'_0 &= c_6 f_5 r'_2 + c_6 h_5 - f_3 r'_1 - h_3 t_1 + c_3 - f_1,
\end{aligned}
$$

and $g \in \langle f, h \rangle$ *if and only if* $s' \neq 0$.

7.6 Geometric Interpretations

Here, we ascribe some geometric meaning to each divisor type of degree 3 or less.

Type 11

If D is of type 11, then $I_D = \langle x - x_0, y - y_0 \rangle$, and $D = P$ where P is the point (x_0, y_0). Since $x - x_0$ and $y - y_0$ have K-rational coefficients, P is a K-rational point. If C is defined over a finite field $\mathbb{F}_q$, by the Hasse-Weil Bound (Theorem 1.8), there are approximately q type 11 divisors on C.

Type 21

Either $D = P + Q$ for distinct points $P \neq Q$, or $D = 2P$.

The former case $D = P + Q$ occurs if and only if $f = x^2 + f_1 x + f_0$ has two distinct roots, x_0 and x_1. Then $P = (x_0, y_0)$ and $Q = (x_1, y_1)$, where $y_i = -g_1 x_i - g_0$ are obtained by solving $g(x_i, y_i) = 0$.

The latter case $D = 2P$ occurs if and only if f has a double root. In this case, g is the tangent line to C at P, necessarily non-vertical.

Type 22

Either $D = P + Q$ for distinct points $P \neq Q$, or $D = 2P$.

The former case $D = P + Q$ occurs if and only if $g = y^2 + g_2 y + g_0$ has two distinct roots, y_0 and y_1. Then $P = (-f_0, y_0)$ and $Q = (-f_0, y_1)$.

The latter case $D = 2P$ occurs if and only if g has a double root. In this case, f is the vertical tangent line to C at P.

Type 31

If D is of type 31, then $I_D = \langle f, g, h \rangle$, where f is the vertically-opening parabola $x^2 + f_2 y + f_1 x + f_0$, g is the hyperbola $xy + g_2 y + g_1 x + g_0$, and h is the horizontally-opening parabola $y^2 + h_2 y + h_1 x + h_0$.

Either D is the sum of three distinct points, the sum of a double point with a second distinct point, or a triple point.

If $D = P + Q + R$ is the sum of three distinct points, then these points are non-collinear. If $D = 2P + Q$ is the sum of a double point with a second distinct point, then the tangent line at P does not pass through Q. If $D = 3P$ is a triple point, then P is not an inflection point.

Type 32

If D is of type 32, then $I_D = \langle f, g \rangle$, where f is the non-vertical line $y + f_1 x + f_0$ and g is the univariate polynomial $x^3 + g_3 x^2 + g_1 x + g_0$. Thus all points in D must be collinear, falling on the line f.

If $D = P + Q + R$ is the sum of three distinct points, then their x-coordinates are the roots of g. If $D = 2P + Q$ for distinct P and Q, then the tangent line at P is f, which also passes through Q, and the x-coordinate of P is a double root of g. If $D = 3P$ is a triple point, then P is an inflection point, f is the tangent line at P, and g has a triple root, the x-coordinate of P.

Type 33

If D is of type 32, then $I_D = \langle f \rangle$ is a principal ideal and f is the vertical line $x + f_0$. The points in D necessarily have the same x-coordinate, $-f_0$. If $D = P + Q + R$ is the sum of three distinct points, then these points have pairwise distinct y-coordinates. If $D = 2P + Q$, for distinct P and Q, then P and Q have distinct y-coordinates and f is the tangent line at P, which passes also through Q. If $D = 3P$ is a triple point, then P is an inflection point and f is the tangent line at P.

8 Addition

We present in this chapter a general algorithm for adding reduced divisors in the divisor class group of a $C_{3,4}$ curve C. Given two reduced divisors D and D', we wish to find a divisor $D'' \equiv D + D'$. More accurately, we wish to find a reduced Gröbner basis for an ideal $I_{D''} \equiv I_D I_{D'}$. The divisor D'' produced by this algorithm will usually not be reduced. We will see in Chapter 10 how to reduce D'', and in Chapter 11 how to combine addition and reduction into a single add-reduce operation.

We will make the following assumptions on D and D':

(i) D and D' are reduced;

(ii) $D \neq D'$;

(iii) $\deg D \geq \deg D'$.

When one of D or D' is unreduced, it can be reduced using algorithms presented in Chapter 10. When $D = D'$, their sum is $2D$, which may be computed using algorithms in Chapter 9. As for the third assumption, the addition algorithm described in this chapter boils down to constructing and row-reducing a matrix. The dimensions of this matrix depends on the degree of D'. By assuming D' is of lesser degree, we may work with a smaller matrix, resulting in faster computations. Should D' be of greater degree than D, we may swap them before adding, as divisor addition is commutative.

The addition algorithm presented in this chapter is based on the algorithm presented by Abu Salem and Khuri-Makdisi in [40], but extended to operate on divisors not considered in [40]. The authors in [40] only considered adding disjoint typical degree 3 divisors, and their algorithm would only return a meaningful value when the sum of the divisors was also typical — otherwise it would return a value indicating an error has occurred. They also assumed that C is defined over a large finite field by an equation of the short form 2.16.

Their algorithm may be briefly described as follows. To add two disjoint typical degree 3 divisors D and D', they first identify these divisors with the vector spaces $W_D^{x^2y}$ and $W_{D'}^{x^2y}$.

These vector spaces will be defined properly below. The sum $D + D'$ is also identified with the vector space $W^{x^2y}_{D+D'}$ and is related to $W^{x^2y}_D$ and $W^{x^2y}_{D'}$ via

$$W^{x^2y}_{D+D'} = W^{x^2y}_D \cap W^{x^2y}_{D'}.$$

The intersection of vector spaces is computed by computing the kernel of the quotient

$$W^{x^2y}_{D+D'} \xhookrightarrow{\ker M_{\text{add}}} W^{x^2y}_D \xhookrightarrow{\iota} W^{x^2y} \xrightarrow{\pi} \frac{W^{x^2y}}{W^{x^2y}_{D'}} \ ,$$

where ι and π indicate the canonical inclusion and quotient maps, and $M_{\text{add}} = \pi \circ \iota$ is their composition.

In this chapter, we will generalize this algorithm to cover all cases of divisor addition by making three key observations.

(i) When D and D' are non-disjoint, the kernel does not give $D + D'$, but rather $L = \text{lcm}(D, D')$.

(ii) $G = \gcd(D, D')$ may be computed by computing the image of the quotient.

(iii) The monomial x^2y indicates an upper bound on a search space — by choosing a larger monomial $m > x^2y$, one can account for the case where $D + D'$ is atypical.

The generalization of Abu Salem and Khuri-Makdisi's addition therefore requires selecting an appropriate bounding monomial m and computing the kernel and image of M_{add} in

$$W^m_L \xhookrightarrow{\ker M_{\text{add}}} W^m_D \xhookrightarrow{\iota} W^m \xrightarrow{\pi} \frac{W^m}{W^m_{D'}} \xrightarrow{\text{im } M_{\text{add}}} \frac{W^m_G}{W^m_{D'}} \ .$$

In the sections to follow, we explain the steps in detail. We will define the space W^m_D and how it relates to D and I_D. We will see how to compute W^m_L and W^m_G. By using the relation

$$D + D' = L + G \tag{8.1}$$

and the fact that, typically, $G = 0$, we give an algorithm for general divisor addition. The atypical case where $G \neq 0$ is handled recursively, so we must also demonstrate that this algorithm terminates.

8.1 The Vector Space W_D^m

For any divisor D, the ideal I_D has structure as an infinite-dimensional K-vector space, which we will denote by W_D. This is merely the vector space where addition of polynomials and scalar multiplication are as in I_D, but we forget multiplication between polynomials. Any K-basis for W_D also generates I_D as an ideal. However, the infinitely large basis for W_D is difficult to compute with. We may restrict to a finite subspace without losing any information. Let $\mathcal{M}$ be the set of monomials of $K[x, y]$ and let $m \in \mathcal{M}$. Define the K-vector spaces

$$W^m := \{f \in K[C] \mid \mathrm{LM}(f) \leq m\}$$

and

$$\begin{aligned} W_D^m &:= W_D \cap W^m \\ &= \{f \in I_D \mid \mathrm{LM}(f) \leq m\}. \end{aligned}$$

Proposition 8.2. *Let $G = \{g_1, \ldots, g_k\}$ be a reduced Gröbner basis for I_D. Let $m = \mathrm{LM}(g_k) > \cdots > \mathrm{LM}(g_1)$. Let B be a K-basis for W_D^m. Then $I_D = \langle B \rangle$.*

Proof. Certainly $\langle B \rangle \subseteq I_D$, since $B \subseteq W_D^m \subseteq I_D$. To show $I_D \subseteq \langle B \rangle$, it suffices to show $G \subseteq \langle B \rangle$, whence $I_D = \langle G \rangle \subseteq \langle B \rangle$.

Let $g_i \in G$. Then $\mathrm{LM}(g_i) \leq m$, so $g_i \in W_D^m$. Therefore g_i is a K-linear combination of elements of B, implying that $g_i \in \langle B \rangle$. □

An echelon basis for W_D^m is a basis B where no two distinct $b, b' \in B$ have the same

leading monomial.

Proposition 8.3. *Let I_D, G, and m be as in Proposition 8.2. If B is an echelon basis for W_D^m, then B is a Gröbner basis for I_D.*

Proof. It suffices to show that for all $f \in I_D$, there is a $b \in B$ such that $\mathrm{LM}(b) | \mathrm{LM}(f)$. This is easy to demonstrate, since there is a $g_i \in G$ such that $\mathrm{LM}(g_i) | \mathrm{LM}(f)$, and there is a $b \in B$ such that $\mathrm{LM}(b) = \mathrm{LM}(g_i)$. □

Corollary 8.4. *Let I_D, G, and m be as in Proposition 8.2. If B is a reduced echelon basis for W_D^m, then there is a subset of B that is a reduced Gröbner basis for I_D.*

Proof. Take the set

$$S = \{b \in B \mid \nexists b' \in B - \{b\} : \mathrm{LM}(b') | \mathrm{LM}(b)\}. \tag{8.5}$$

For any $s \in S$, by construction, $\mathrm{LM}(s)$ is not divisible by the leading term of any other $s' \in S$. Moreover, no term in s is divible by the leading term of any other s' by virtue of B being a reduced echelon basis. □

Given an ideal I_D, we may produce the vector space W_D^m. By Corollary 8.4, given a vector space W_D^m, we may reproduce the ideal I_D, as long as m was chosen to be sufficiently large. In particular, m must be at least as large as the largest leading monomial appearing in the reduced Gröbner basis for I_D.

The space W_D^m is simply a Riemann-Roch space under a different notation.[21] It is a well-known fact in algebraic geometry that Riemann-Roch spaces are finite-dimensional (Proposition 1.4.9 in [44]). We give the dimensions explicitly:

Theorem 8.6. *For a divisor D and monomial m, W^m and W_D^m are finite-dimensional. In*

[21] Namely, $W_D^m = \mathcal{L}(-D - \nu_{P_\infty}(m)P_\infty)$.

particular,

$$\dim W^m = \begin{cases} 1 & m = 1 \\ 2 & m = x \\ 3 & m = y \\ 3i + 4j - 2 & m = x^i y^j > y \end{cases}.$$

$$\dim W_D^m = \#\{\mu \in \mathcal{M} \ : \ \mu \leq m, \ \mu \in \mathrm{LT}(I_D)\}.$$

For sufficiently large m,

$$\dim W_D^m = \dim W^m - \deg D.$$

Proof. The dimension of W^m is the number of monomials in $K[C]$ less than or equal to m. For readability, define $f(i,j) = \dim W^{x^i y^j}$. Recalling the $C_{3,4}$ order on monomials in $K[C]$,

$$1 < x < y < x^2 < xy < y^2 < x^3 < x^2 y < xy^2 < x^4 < x^3 y < x^2 y^2 < \ldots,$$

it is clear that

$$f(0,0) = 1 \qquad f(2,0) = 4$$
$$f(1,0) = 2 \qquad f(1,1) = 5$$
$$f(0,1) = 3 \qquad f(0,2) = 6,$$

that for $i \geq 0$, $f(2+i,0) = 3i + f(2,0)$, and that for $0 \leq j \leq 2$, $f(i,j) = j + f(i+j,0)$. By

the curve equation, for $k \geq 0$, $f(i, 3k + j) = f(4k + i, j)$. Putting these all together.

$$\begin{aligned} f(i,j) &= f(i, 3k + \ell) \\ &= f(4k + i, \ell) \\ &= \ell + f(4k + i + \ell, 0) \\ &= \ell + f(2 + 4k + i + \ell - 2, 0) \\ &= \ell + 3(4k + i + \ell - 2) + f(2, 0) \\ &= 12k + 3i + 4\ell - 2 \\ &= 3i + 4j - 2. \end{aligned}$$

For the second claim, let B be a reduced echelon basis for W_D^m. Then

$$\mu \leq m \text{ and } \mu \in \mathrm{LT}(I_D) \iff \exists b \in B \ : \ \mathrm{LT}(b) = \mu.$$

To see this, suppose $\mu \leq m$ and $\mu \in \mathrm{LT}(I_D)$. Then there is a monic $f \in I_D$ such that $\mathrm{LT}(f) = \mu$. Then $f \in W_D^m$, so f is a K-linear combination on B, so there is a $b \in B$ with $\mathrm{LT}(b) = \mathrm{LT}(f) = \mu$. The converse is trivial, since $\mathrm{LT}(b) \leq m$ and $\mathrm{LT}(b) \in \mathrm{LT}(I_D)$.

For the final claim, the set $\{\mu \in \mathcal{M} \ : \ \mu \notin \mathrm{LT}(I_D)\}$ has a maximum m'. Hence for $m \geq m'$,

$$\begin{aligned} \dim W_D^m &= \#\{\mu \in \mathcal{M} \ : \ \mu \leq m, \ \mu \in \mathrm{LT}(I_D)\} \\ &= \#\{\mu \in \mathcal{M} \ : \ \mu \leq m\} - \#\{\mu \in \mathcal{M} \ : \ \mu \leq m, \ \mu \notin \mathrm{LT}(I_D)\} \\ &= \dim W^m - \deg D. \end{aligned}$$

The last equality holds by Corollary 3.26. □

8.2 Computing W_L^m and W_G^m

Let $L = \operatorname{lcm}(D, D')$ and $G = \gcd(D, D')$. Just as $I_L = I_D \cap I_{D'}$ and $I_G = I_D + I_{D'}$, so too are $W_L^m = W_D^m \cap W_{D'}^m$ and $W_G^m = W_D^m + W_{D'}^m$ (without restriction on the size of m). We now address the question of how to compute W_L^m and W_G^m.

Ultimately, the purpose of computing W_L^m and W_G^m is to recover I_L and I_G. For that, we must first choose a sufficiently large monomial m to bound our vector spaces. The monomial m must be at least as large as the largest leading monomial in the Gröbner bases of I_L and I_G. We do not know *a priori* what those Gröbner bases are, but we may place an upper bound on the degrees of L and G, then refer to Table 7.1 to place a bound on m. For example, if D and D' are both of degree 3, then $D + D'$ is of degree 6, and L and G are no larger than degree 6. Referring to Table 7.1, no divisor of degree 6 (or smaller) has a monomial larger than x^4, so $m = x^4$ is sufficiently large for our purposes.

After choosing m, the following theorem tells us how to compute W_L^m and W_G^m. Strictly speaking, it gives us a quotient of W_G^m, but we will see later that we have enough information to get W_G^m itself.

Theorem 8.7. *Let D and D' be divisors, let m be a monomial, and let M_{add} be the composed map*

$$W_D^m \xhookrightarrow{\iota} W^m \xrightarrow{\pi} \frac{W^m}{W_{D'}^m} \quad .$$

where ι is the canonical inclusion map and π is the canonical quotient map. Then $\ker M_{add} = W_L^m$ *and* $\operatorname{im} M_{add} = W_G^m / W_{D'}^m$,

$$W_L^m \xhookrightarrow{\ker M_{add}} W_D^m \xhookrightarrow{\iota} W^m \xrightarrow{\pi} \frac{W^m}{W_{D'}^m} \xrightarrow{\operatorname{im} M_{add}} \frac{W_G^m}{W_{D'}^m} \quad .$$

Proof. The kernel of M_{add} consists precisely of those elements in W_D^m that vanish modulo $W_{D'}^m$. An element vanishes modulo $W_{D'}^m$ if and only if it is a member of $W_{D'}^m$, so

$$\ker M_{\text{add}} = W_D^m \cap W_{D'}^m = W_L^m.$$

As for the image, it is enough to show that $\operatorname{im} M_{\text{add}}$ is isomorphic to and contained in $W_G^m/W_{D'}^m$. By the first and second isomorphism theorems for vector spaces (see Theorems IV.1.7 and IV.1.9 in [21], or many other algebra and linear algebra texts),

$$\operatorname{im} M_{\text{add}} \overset{\text{(1st)}}{\cong} \frac{W_D^m}{W_L^m} = \frac{W_D^m}{W_D^m \cap W_{D'}^m} \overset{\text{(2nd)}}{\cong} \frac{W_D^m + W_{D'}^m}{W_{D'}^m} = \frac{W_G^m}{W_{D'}^m}.$$

Let $f \in W_D^m$. Then $M_{\text{add}}(f) = [f] \in \frac{W^m}{W_{D'}^m}$. However f is also in $W_D^m + W_{D'}^m = W_G^m$, therefore $[f]$ is also in $\frac{W_G^m}{W_{D'}^m}$. □

Proposition 8.8. *The dimensions of W_L^m and $W_G^{m'}$ are*

(i) $\dim W_L^m = \operatorname{null} M_{add}$;

(ii) $\dim \frac{W_G^m}{W_{D'}^m} = \operatorname{rank} M_{add}$.

For a sufficiently large monomial m,

(iii) $\deg L = \deg D + \operatorname{rank} M_{add}$;

(iv) $\deg G = \deg D' - \operatorname{rank} M_{add}$;

(v) $D + D' = L \iff G = 0 \iff \operatorname{rank} M_{add} = \deg D'$.

Proof. Parts (i) and (ii) are immediate from the Rank-nullity Theorem. For part (iii),

$$\begin{aligned}
\deg L &= \dim W^m - \dim W_L^m && \text{Theorem 8.6} \\
&= \dim W^m - \operatorname{null} M_{\text{add}} && \text{part (i)} \\
&= \dim W^m - \dim W_D^m + \operatorname{rank} M_{\text{add}} && \text{rank-nullity} \\
&= \deg D + \operatorname{rank} M_{\text{add}} && \text{Theorem 8.6.}
\end{aligned}$$

For part (iv),

$$\begin{aligned} \deg G &= \deg G + \deg L - \deg L \\ &= \deg D' + \deg D - \deg L && L + G = D + D' \\ &= \deg D' - \operatorname{rank} M_{\text{add}} && \text{part (iii).} \end{aligned}$$

Finally, for part (v), it is clear that $D + D' = L \iff G = 0$ by equation 8.1, and by part (iv), $G = 0 \iff \operatorname{rank} M_{\text{add}} = \deg D'$. □

In the following subsections, we work out some extended examples of computing L and G.

8.3 The Addition Algorithm

We are now able to compute $L = \operatorname{lcm}(D, D')$ and $G = \gcd(D, D')$. The goal of this chapter is to compute a divisor D'' equivalent to $D + D'$. By Proposition 8.8, if M_{add} has full rank, then $D'' = L$. This occurs if and only if D and D' are disjoint ($G = 0$).

When D and D' are non-disjoint, we compute $D + D'$ by computing L and G, reducing L ($\deg G \leq 2$, so G is already reduced), then adding $\overline{\overline{L}} + G$, introducing an element of recursion to our addition. If not handled properly, this can lead to infinite recursion. For example, suppose $D = P + 2Q$ and $D' = P + Q$. Then $L = P + 2Q = D$ (and is already reduced) and $G = P + Q = D'$. Attempting to compute $D + D'$ by $\overline{\overline{L}} + G$ brings us full circle. In this section, we will identify three cases arising in divisor addition. We will handle each case in such a way that any time we recursively add, the smaller of the two divisors in the next iteration is strictly smaller than in the previous iteration, forcing our algorithm to eventually terminate.

We begin with a proposition characterizing the case $\operatorname{rank} M_{\text{add}} = 0$.

Proposition 8.9. *The following are equivalent:*

(i) $L = D$;

(ii) $G = D'$;

(iii) $D' \leq D$;

(iv) $\operatorname{rank} M_{add} = 0$.

Proof. **(i)** $\iff$ **(ii):** Immediate from the relation $D + D' = L + G$.

(i) $\implies$ **(iii):** $D' \leq L$ and $L = D$, hence $D' \leq D$.

(iii) $\implies$ **(iv):** If $D' \leq D$, then $I_D \subseteq I_{D'}$ and $W_D^m \subseteq W_{D'}^m$. Every element in W_D^m vanishes under M_{add}, $\operatorname{null} M_{\text{add}} = \dim W_D^m$ and $\operatorname{rank} M_{\text{add}} = 0$.

(iv) $\implies$ **(i):** Suppose $\operatorname{rank} M_{\text{add}} = 0$. By Proposition 8.8, $\deg L = \deg D$. Since $D \leq L$ and D and L have the same degree, $L = D$.

□

Corollary 8.10.

$$G < D' \iff \operatorname{rank} M_{add} > 0.$$

We may now identify three cases:

(i) $\operatorname{rank} M_{\text{add}} = \deg D'$;

(ii) $0 < \operatorname{rank} M_{\text{add}} < \deg D'$; or

(iii) $\operatorname{rank} M_{\text{add}} = 0$.

In the first case, we return L and our algorithm terminates. In the second case, we recursively compute $\overline{\overline{L}} + G$; the degree of G is strictly smaller than the degree of D'. In the third case, $\overline{\overline{L}} = D$ and $G = D'$, so recursively adding $\overline{\overline{L}} + G$ leads to an infinite loop. We must treat this case separately.

By Proposition 8.9, if $\operatorname{rank} M_{\text{add}} = 0$, then $D' \leq D$. Since we are assuming $D' \neq D$, we have $D' < D$. Since D is reduced and of degree at most 3, $\deg D'$ is either 1 or 2. We consider each of these cases separately, beginning with the latter.

If D' is of degree 2, then $D = D' + A$ for some degree 1 divisor A, which we must find. Once we have A, we compute

$$D + D' = \overline{\overline{2D'}} + A.$$

Now $\deg A < \deg D'$, so our algorithm is one step closer towards termination. Finding A amounts to finding $x_0, y_0 \in K$ such that

$$I_D = I_{D'} \langle x + x_0, y + y_0 \rangle .$$

To do this, we note that $I_{D'} = \langle f', g' \rangle$ has a Gröbner basis of two elements. To find x_0, y_0, we note that $f'(x + x_0)$ and $f'(y + y_0)$ must be in I_D. So reducing $f'(x + x_0)$ and $f'(y + y_0)$ modulo f, g, h must give 0. This gives us a simple system of linear equations to solve for x_0 and y_0. Formulae solving this system are available at [30].

If D' is of degree 1, then $D = nD' + A$ for some A disjoint from D' (possibly $A = 0$) and some $1 \leq n \leq 3$. We must find A and n and compute

$$D + D' = \overline{\overline{(n+1)D'}} + A.$$

To find A and n, one repeats the process from the previous case. Find a divisor A of degree $\deg D - \deg D'$ such that $D = D' + A$ by reducing $f'(x + x_0)$ and $f'(y + y_0)$ modulo I_D and solving a system of linear equations. It is then easy to check[22] if $D' \leq A$. If not, $n = 1$ and we have the divisor A we need. Otherwise, increment n and repeat the process by finding A' such that $A = D' + A'$, and so on.

Now A is disjoint[23] from $\overline{\overline{(n+1)D'}}$, so that the algorithm will terminate in the next

[22] D consists of one point. Check if the generators of I_A are zero at that point.

[23] Except for an exceptional case where $(n+1)D'$ is type 32 or 33, in which case $\overline{\overline{(n+1)D'}}$ is degree 0 or

recursive step. Computing $(n+1)D'$ requires us to be able to double, triple, or quadruple a point. Doubling is the topic of Chapter 9 and quadrupling is accomplished by doubling twice. In Chapter 9, two doubling algorithms are presented. When the addition algorithm is required to double, it uses Algorithm 9.2, which provably terminates. Formulae for tripling a point are available at [30].

We summarize the addition algorithm in Algorithm 8.3. By "return L", we mean return a reduced Gröbner basis for I_L, which is the subset of the reduced echelon basis for $\ker M_{\text{add}}$ satisfying Equation 8.5. In line 5, we compute the reduced row echelong form (RREF) of M_{add}. The rank and kernel of M_{add} are easily found after computing the RREF, as shown in the example to follow.

8.4 Example – Computing $\ker M_{\text{add}}$

Let C be the $C_{3,4}$ curve over $\mathbb{F}_{11}$ defined by the polynomial $y^3 + x^4 + 1$. Let D and D' be type 31 divisors with

$$\begin{aligned} D &= \langle f, g, h\rangle & D' &= \langle f', g', h'\rangle \\ f &= x^2 + 3y + 7x + 5 & f' &= x^2 + 6y + 3x - 2 \\ g &= xy + 2y + 2x + 9 & g' &= xy + 5y + 5x + 9 \\ h &= y^2 + 4y + 2x + 3 & h' &= y^2 - y - x + 5. \end{aligned}$$

These divisors are disjoint, with

$$\begin{aligned} D &= 2 \cdot (7:6:1) + (10:4:1) \\ D' &= (5:1:1) + (2\alpha + 6 : 7\alpha : 1) + (9\alpha + 3 : 4\alpha + 6 : 1) \end{aligned}$$

where $\alpha \in \mathbb{F}_{11^2}$ is a root of $x^2 + 7x + 2$.

1. In this case, the algorithm will still terminate.

Algorithm 8.1 Divisor Addition

Input: Two reduced divisors D and D' satisfying $D \neq D'$ and $\deg D \geq \deg D'$, represented by the reduced Gröbner bases of their ideals I_D and $I_{D'}$

Output: A divisor D'' equivalent to $D + D'$, represented by its ideal $I_{D''}$

if $D' = 0$ **then**
    return D
end if
Compute $M_{\text{add}} : W_D^m \to W_{D'}^m$
Compute $\text{RREF}(M_{\text{add}})$ and $\operatorname{rank} M_{\text{add}}$ and $\ker M_{\text{add}}$
if $\operatorname{rank} M_{\text{add}} = \deg D'$ **then**
    Compute $L = \operatorname{lcm}(D, D')$
    return L
end if
if $\operatorname{rank} M_{\text{add}} > 0$ **then**
    Compute $L = \operatorname{lcm}(D, D')$
    Compute $G = \gcd(D, D')$
    return $\overline{\overline{L}} + G$
end if
if $\operatorname{rank} M_{\text{add}} = 0$ **then**
    if $\deg D' = 2$ **then**
        Compute A such that $D = A + D'$
        return $\overline{\overline{2D'}} + A$
    end if
    if $\deg D' = 1$ **then**
        Compute A and largest n such that $D = A + nD'$
        return $\overline{\overline{(n+1)D'}} + A$
    end if
end if

The sum $D + D'$ is a degree 6 divisor. Referring to Table 7.1, we see that no generator of any reduced Gröbner basis of a degree 6 divisor has a monomial larger than x^4. Therefore W^{x^4} will be a sufficiently large space in which to perform our computations. We proceed by computing the matrix M_{add} in

$$\begin{array}{ccccccc} & & & \overset{M_{\text{add}}}{\frown} & & & \\ W_L^{x^4} & \overset{\ker M_{\text{add}}}{\hookrightarrow} & W_D^{x^4} & \overset{\iota}{\hookrightarrow} & W^{x^4} & \overset{\pi}{\twoheadrightarrow} & \frac{W^{x^4}}{W_{D'}^{x^4}} \overset{\text{im } M_{\text{add}}}{\twoheadrightarrow} \frac{W_G^{x^4}}{W_{D'}^{x^4}} \\ & & \wr\downarrow & & \wr\downarrow & & \wr\downarrow \\ & & K^7 & \hookrightarrow & K^{10} & \twoheadrightarrow & K^3 \end{array},$$

where the bottom row serves to show the dimensions of these spaces. The dimensions of $\ker M_{\text{add}}$ and $\text{im } M_{\text{add}}$ are not yet known until we do some more calculations.

The spaces $W_D^{x^4}$ and $W_{D'}^{x^4}$ are 7-dimensional. Any seven polynomials from one of these spaces with different valuations at P_∞ will form an echelon basis for that space. Choosing polynomials with different valuations at infinity amounts to choosing polynomials with different leading monomials while also taking into account the linear dependence on the monomials $1, x, \ldots, x^4, y^3$. The most obvious choice for bases of $W_D^{x^4}$ and $W_{D'}^{x^4}$, then, are

$$\begin{aligned} W_D^{x^4} &= \text{Span}_K\{f, g, h, xf, xg, xh, x^2 f\} \\ W_{D'}^{x^4} &= \text{Span}_K\{f', g', h', xf', xg', xh', x^2 f'\}. \end{aligned}$$

We reduce the basis of $W_D^{x^4}$ modulo $W_{D'}^{x^4}$ to get the matrix

$$M_{\text{add}} = \begin{pmatrix} 7 & 0 & 9 & 2 & 10 & 5 & 2 \\ 4 & 8 & 3 & 10 & 2 & 8 & 6 \\ 8 & 8 & 5 & 2 & 0 & 1 & 7 \end{pmatrix},$$

where, e.g., the reduction of f is $\overline{f} = 8y + 4x + 7$, the reduction of g is $\overline{g} = 8y + 8x$, etc.

This matrix M_{add} has the reduced row echelon form and kernel

$$\operatorname{RREF}(M_{\text{add}}) = \begin{pmatrix} 1 & 0 & 6 & 0 & 6 & 9 & 2 \\ 0 & 1 & 7 & 0 & 9 & 8 & 10 \\ 0 & 0 & 0 & 1 & 6 & 4 & 5 \end{pmatrix} \qquad \ker M_{\text{add}} = \begin{pmatrix} -6 & -6 & -9 & -2 \\ -7 & -9 & -8 & -10 \\ 1 & 0 & 0 & 0 \\ 0 & -6 & -4 & -5 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The kernel is 4-dimensional, spanned by the vectors

$$\begin{aligned} \ker M_{\text{add}} &= \operatorname{Span}_K \left\{ \begin{array}{l} h - 7g - 6f, \\ xg - 6xf - 9g - 6f, \\ xh - 4xf - 8g - 9f, \\ x^2 f - 5xf - 10g - 2f \end{array} \right\} \\ &= \operatorname{Span}_K \left\{ \begin{array}{l} y^2 + 4xy + 5x^2 + 5y + x - 2, \\ x^2 y + 5x^3 - 3xy - 2x^2 - 3y - 4x - 1, \\ xy^2 - 4x^3 - 5xy - 2x^2 + y + 3x + 4, \\ x^4 + 3x^2 y + 2x^3 - 3xy + x^2 - 4y - 4x - 1 \end{array} \right\}. \end{aligned}$$

These four polynomials form a basis for $W_L^{x^4}$ and a Gröbner basis for I_L, but not a *reduced* Gröbner basis. By Proposition 8.8, $\deg L = 6$ and $\deg G = 0$. We have just determined that I_L contains polynomials with leading monomials y^2 and $x^2 y$, so by Arita's classification of divisors, L must be of type 63 and the first two polynomials alone form a reduced Gröbner basis,

$$I_L = \left\langle y^2 + 4xy + 5x^2 + 5y + x - 2,\ x^2 y + 5x^3 - 3xy - 2x^2 - 3y - 4x - 1 \right\rangle.$$

Remark 8.11. In this example, we computed the kernel of M_{add} to get four polynomials, though two were not needed. Consequently, two columns of the matrix M_{add} were not needed. An efficient implementation of divisor arithmetic will avoid computing unnecessary columns

of M_{add} by computing them only as they become necessary.

8.5 Example – Computing $\operatorname{im} M_{\text{add}}$

Consider again the $C_{3,4}$ curve C defined by the polynomial $y^3 + x^4 + 1$ over $\mathbb{F}_{11}$. Let D and D' be type 31 divisors with

$$\begin{aligned} D &= \langle f, g, h\rangle & D' &= \langle f', g', h'\rangle \\ f &= x^2 + y + 5x + 1 & f' &= x^2 - 3y - 5x - 3 \\ g &= xy + 2y - 3x + 2 & g' &= xy - 4y + 4x - 4 \\ h &= y^2 + 3y + 3x + 2 & h' &= y^2 - y + 4x - 2. \end{aligned}$$

These divisors are non-disjoint, with

$$\begin{aligned} D &= (0:10:1) + (3:8:1) + (1:4:1) \\ D' &= (0:10:1) + (3:8:1) + (6:1:1). \end{aligned}$$

As in the previous example, we reduce the basis of $W_D^{x^4}$ modulo the basis for $W_{D'}^{x^4}$ to get the matrix

$$M_{\text{add}} = \begin{pmatrix} 4 & 6 & 4 & 2 & 3 & 2 & 1 \\ 10 & 4 & 2 & 5 & 2 & 5 & 8 \\ 4 & 6 & 4 & 2 & 3 & 2 & 1 \end{pmatrix}.$$

This matrix has the reduced row echelon form

$$\operatorname{RREF}(M_{\text{add}}) = \begin{pmatrix} 1 & 7 & 1 & 6 & 9 & 6 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We can see the M_{add} does not have full rank. In this case, $\operatorname{rank} M_{\text{add}} = 1$. By Proposition 8.8, $\deg L = 4$, and G is non-zero with $\deg G = 2$. We have a non-trivial image to compute.

The image of M_{add} is determined by its pivot columns. In this case, there is only one pivot column — the first. The image of M_{add} is therefore given by the column basis

$$\operatorname{im} M_{\text{add}} = \operatorname{Span}_K \begin{pmatrix} 4 \\ 10 \\ 4 \end{pmatrix} = \operatorname{Span}_K \begin{pmatrix} 1 \\ -3 \\ 1 \end{pmatrix}.$$

That is, $\operatorname{im} M_{\text{add}} = \frac{W_G^m}{W_{D'}^m}$ is spanned by the polynomial $u = y - 3x + 1$. Since G has degree 2 and contains a polynomial with leading monomial y, G must be of type 21 and we must find its other generator v with leading monomial x^2. Since $I_D \subseteq I_G$, f must be an element of I_G, and we may reduce f modulo u to obtain v. This gives

$$I_G = \langle u, v \rangle = \left\langle y - 3x + 1,\ x^2 - 3x \right\rangle.$$

Note that u and v intersect at the points $(0 : 10 : 1)$ and $(3 : 8 : 1)$, as expected.

9 Doubling

Abu Salem and Khuri-Makdisi, in [40], present an algorithm for doubling a divisor D. Their algorithm assumes that D is a reduced typical divisor, and that no point in the support of D has order greater than 1. In this chapter, we generalize their algorithm to apply to reduced divisors of any type, typical or atypical, and without regard to the multiplicities of points appearing in the divisor.

As usual, let C be a $C_{3,4}$ curve over a field K, defined by a polynomial F. Given a divisor D on C, analogously to Chapter 8, we wish compute a divisor equivalent to $2D$ in the divisor class group. More precisely, we want to compute a reduced Gröbner basis for an ideal equivalent to I_D^2 in the ideal class group.

The doubling algorithm for divisors on C is very similar to the addition algorithm from the previous chapter. The only significant change is that the map $M_{\text{add}} = \pi \circ \iota$ is instead $M_{\text{doub}} = \pi \circ d$; the canonical inclusion map ι is replaced with the map sending a polynomial f to its differential df. The picture is now this:

$$W_{D_1}^m \xhookrightarrow{\ker M_{\text{doub}}} W_D^m \xrightarrow{d} W^{m'} \xrightarrow{\pi} \frac{W^{m'}}{W_D^{m'}} \xrightarrow{\operatorname{im} M_{\text{doub}}} \frac{W_{D_0}^{m'}}{W_D^{m'}} \quad .$$

Theorem 4.12 tells us that if a polynomial f and its differential df both vanish modulo W_D, then f must have higher order than D at every finite point in its support. Rather than returning the least common multiple and greatest common divisor, computing the kernel and image now yields divisors D_1 and D_0 satisfying

$$0 \leq D_0 < D < D_1 \leq 2D.$$

Typically, $D_1 = 2D$ and $D_0 = 0$.

Notice the presence of a monomial m' in the above diagram. Given a polynomial $f \in K[C]$, the monomials appearing in df will be larger than the monomials appearing in f. Therefore we will need a larger monomial m' to bound some spaces.

The module of Kähler differentials, $\Omega_{K[C]/K}$, is generated as a $K[C]$-module by a single element, but there is more than one choice of generator. The map d, and therefore the computation of the composed map M_{doub}, depends on this choice of generator. In [3], Arita uses the generator seen in Proposition 4.10. In [40], Abu Salem and Khuri-Makdisi make a different choice of generator that allows for more efficient computations. The latter choice of generator was used in [40] to double typical reduced divisors. We will generalize the method to apply to atypical divisors as well, although there is one case for which we will use the former choice of generator (but see Section 13.1, Future Work). We discuss these two choices and the resulting algorithms in the two sections to follow.

9.1 A General Method

Recall from Proposition 4.10 that the module of Kähler differentials $\Omega_{K[C]/K}$ has a generator dz and a derivation d defined by

$$\begin{aligned} d : K[C] &\to \Omega_{K[C]/K} \\ f &\mapsto (f_x F_y - f_y F_x) dz. \end{aligned}$$

The derivation d is K-linear. We may view $K[C]$ and $\Omega_{K[C]/K}$ as K-vector spaces and d a linear transformation between them. However, just like in the previous chapter, we will restrict ourselves to finite-dimensional vector subspaces of these. Let m be the largest leading monomial appearing in a reduced Gröbner basis of a divisor of degree $\deg(2D)$. Let B be an echelon basis for W_D^m, and let m' be the monomial

$$m' := \max\{\text{LM}(f_x F_y - f_y F_x) \mid f \in B\}.$$

We may now restrict the domain of d and view it as a map

$$\begin{aligned} d : W_D^m &\to W^{m'} \\ f &\mapsto f_x F_y - f_y F_x. \end{aligned}$$

Now consider the diagram from earlier,

$$W_{D_1}^m \xhookrightarrow{\ker M_{\text{doub}}} W_D^m \xrightarrow{d} W^{m'} \xrightarrow{\pi} \frac{W^{m'}}{W_D^{m'}} \xrightarrow{\operatorname{im} M_{\text{doub}}} \frac{W_{D_0}^{m'}}{W_D^{m'}} \quad .$$

The kernel of M_{doub} is exactly the set of polynomials in W_D^m whose differentials vanish modulo I_D. Recall from Corollary 8.4, a subset of the reduced echelon basis for $\ker M_{\text{doub}}$ gives the reduced Gröbner basis for D_1, and the subset is given explicitly by Equation 8.5. By Theorem 4.12,

$$D_1 = \sum_{P \in \operatorname{supp}(D)} (\operatorname{ord}_P(D) + 1)P,$$

where the sum is taken only over finite P.

Example 9.1. Let P, Q, R be distinct points. If $D = P + Q + R$, then $D_1 = 2P + 2Q + 2R$. If $D = P + 2Q$, then $D_1 = 2P + 3Q$. If $D = 3P$, then $D_1 = 4P$.

If all points in D appear with order 1, then $D_1 = 2D$. If, however, D has a point appearing with order greater than 1, then $D_1 < 2D$. The difference between D_1 and $2D$ is recovered by D_0. We have

$$D_0 = \sum_{P \in \operatorname{supp}(D)} (\operatorname{ord}_P(D) - 1)P,$$

and

$$D_0 + D_1 = 2D.$$

This gives us a doubling algorithm similar to the addition algorithm. We construct the matrix M_{doub}, then compute $\ker M_{\text{doub}}$, and if necessary (when $\operatorname{rank} M_{\text{doub}} < \deg D$) compute

im M_{doub}, thereby giving us D_0 and D_1. If M_{doub} has full rank, then $D_1 = 2D$, so we return D_1. Otherwise, use the addition algorithm to compute $\overline{\overline{D_1}} + D_0$. This is summarized in Algorithm 9.1. As was noted before Algorithm 8.3, By "return D_1", we mean return a reduced Gröbner basis for I_{D_1}, which is the subset of the reduced echelon basis for $\ker M_{\text{doub}}$ satisfying Equation 8.5. The addition in line 11 is performed by Algorithm 8.3.

Algorithm 9.1 Divisor Doubling

Input: A reduced divisor D, represented by the reduced Gröbner basis of its ideal I_D
Output: A divisor D' equivalent to $2D$, represented by the reduced Gröbner basis of its ideal $I_{D'}$

1: **if** $D = 0$ **then**
2: **return** D
3: **end if**
4: Compute M_{doub}
5: Compute $\text{RREF}(M_{\text{doub}})$, $\operatorname{rank} M_{\text{doub}}$, and $\ker M_{\text{doub}}$
6: Compute D_1
7: **if** $\operatorname{rank} M_{\text{doub}} = \deg D'$ **then**
8: **return** D_1
9: **end if**
10: Compute D_0
11: **return** $\overline{\overline{D_1}} + D_0$

This algorithm either returns a divisor, or else calls upon the addition algorithm, Algorithm 8.3, which terminates.

This algorithm has two significant drawbacks. Firstly, the difference between the leading monomials of f and df can be relatively large. The larger the gap, the longer it takes to reduce df modulo I_D. In the next section, we present a faster alternative, Algorithm 9.2, that minimizes that gap between $\text{LM}(f)$ and $\text{LM}(df)$ and never requires computing a second divisor D_0. Secondly, were the addition algorithm to call Algorithm 9.1 to do its doubling rather than Algorithm 9.2, it would lead to an infinite loop on some inputs. Thus we require Algorithm 9.2 in the next section, which provably terminates, but does not handle one rare case. If D is a type 31 divisor with ideal and reduced Gröbner basis $I_D = \langle f, g, h\rangle$, then there is a small possibility that $\langle f, g\rangle \neq I_D \neq \langle f, h\rangle$. This case is handled by Algorithm 9.1, but not by Algorithm 9.2. Thus, we will use Algorithm 9.1 to double type 31 divisors

satisfying this rare condition. All other cases will be doubled by Algorithm 9.2.

9.2 A Faster Method

Let D be a typical type 31 divisor, with ideal $I_D = \langle f, g, h\rangle$, where $\{f, g, h\}$ is a reduced Gröbner basis. Since D is typical, $I_D = \langle f, g\rangle$. Suppose also that D is the sum of three distinct points. The flip $\overline{D}$ of D has the ideal $I_{\overline{D}} = \langle f, g'\rangle$ for some g'. Define

$$\mathcal{A}_D := \frac{\Omega_{K[C]/K}}{\langle f, g\rangle\, \Omega_{K[C]/K}}.$$

In [40], rather than consider a generator dz for $\Omega_{K[C]/K}$, Abu Salem and Khuri Makdisi instead consider a generator ω for $\mathcal{A}_D$. They show that there exists such a generator with the properties that

$$df = g'\omega \quad \text{and} \quad dg = -h'\omega,$$

where h' satisfies $fh' \equiv -gg'$. This choice of generator and the resulting map d yielded the most efficient arithmetic at the time.

Their proof of existance of ω relied on the fact that D consists of distinct points, a reasonable assumption for the cryptographic applications they were exploring. We will show that their idea applies in greater generality than was considered in [40], to include most atypical divisors as well.[24] The next two lemmas and the theorem following them are a generalization of the three-part Lemma 5.3 in [40]. We change notation from f, g, g', h' to f, r, r', s' to avoid confusion; $\langle f, g, h\rangle$ indicates a Gröbner basis for a I_D, while $\langle f, r\rangle$ does not.

Lemma 9.2. *Let D be a non-zero reduced divisor and suppose $I_D = \langle f, r\rangle$, where f is the minimum polynomial in I_D. Then $I_{\overline{D}} = \langle f, r'\rangle$ for some $r' \in K[C]$ and there is a polynomial $s' \in K[C]$ such that $fs' \equiv -rr' \pmod F$. Let $A = \operatorname{div}(r', s')$. Then $\gcd(D, A) = 0$ and $A + \overline{D} = \operatorname{div} r'$.*

[24] Again, see Section 13.1, Future Work. This can likely be extended to all divisors.

Proof. The existance of s' comes from the definition of the colon ideal[25] and the fact that $\langle f, r' \rangle = f : r$. Since $D + \overline{D} = \operatorname{div} f$,

$$\begin{aligned}
\langle f \rangle &= I_D I_{\overline{D}} \\
&= \langle f, r \rangle \langle f, r' \rangle \\
&= \left\langle f^2, fr, fr', rr' \right\rangle \\
&= \left\langle f^2, fr, fr', fs' \right\rangle \\
&= \langle f \rangle \langle f, r, r', s' \rangle ,
\end{aligned}$$

which implies

$$\langle 1 \rangle = \langle f, r, r', s' \rangle = \langle f, r \rangle + \langle r', s' \rangle = I_D + I_A.$$

In the divisor class group, this translates to

$$0 = \gcd(D, A).$$

As for the claim regarding $\operatorname{div} r'$,

$$\begin{aligned}
I_A I_{\overline{D}} &= \langle r', s' \rangle \langle f, r' \rangle \\
&= \left\langle fr', (r')^2, fs', r's' \right\rangle \\
&= \left\langle fr', (r')^2, rr', r's' \right\rangle \\
&= \langle r' \rangle \langle f, r', r, s' \rangle = \langle r' \rangle ,
\end{aligned}$$

hence $A + \overline{D} = \operatorname{div} r'$. □

Lemma 9.3. *Let I_D, r', and s' be as in Lemma 9.2. Let $\mathfrak{p}$ be a prime factor of I_D. At least one of r' and s' is a unit in $K[C]/\mathfrak{p}$.*

[25] See Appendix A for properties of the colon ideal. The notation $f : r$ is short for $\langle f \rangle : \langle r \rangle$, the colon ideal of $\langle f \rangle$ by $\langle r \rangle$.

Proof. Since $\mathfrak{p}$ is a maximal ideal, to say that r' is a unit in $K[C]/\mathfrak{p}$ is equivalent to saying $r' \notin \mathfrak{p}$. If r' and s' are both in $\mathfrak{p}$, then $I_A = \langle r', s' \rangle \subseteq \mathfrak{p}$. Then $I_D + I_A \subseteq \mathfrak{p}$, a contradiction since $I_D + I_A = \langle 1 \rangle$. □

Theorem 9.4. *Let I_D, f, r, r', and s' be as in Lemma 9.2. Let $a, b \in K[C]$. Then*

$$af + br \in I_D^2 \iff ar' - bs' \in I_D.$$

Proof. ($\Longrightarrow$) Suppose $af + br \in I_D^2$. Using the fact that $\operatorname{div} f = D + \overline{D}$ and $\operatorname{div} r' = A + \overline{D}$ (Lemma 9.2),

$$\begin{aligned}
\langle af + br \rangle &\subseteq I_D^2 \\
\operatorname{div} I_D^2 &\leq \operatorname{div}(af + br) \\
2D &\leq \operatorname{div}(af + br) \\
2D + \operatorname{div} r' &\leq \operatorname{div}(afr' + brr') \\
&= \operatorname{div}(afr' - bfs') \\
&= \operatorname{div} f + \operatorname{div}(ar' - bs') \\
2D + \overline{D} + A &\leq D + \overline{D} + \operatorname{div}(ar' - bs') \\
D + A &\leq \operatorname{div}(ar' - bs') \\
D &\leq \operatorname{div}(ar' - bs') \\
\langle ar' - bs' \rangle &\subseteq I_D.
\end{aligned}$$

($\Longleftarrow$) Suppose $ar' - bs' \in I_D$. Let $\mathfrak{p}^k$ be a prime power factor of I_D. We will show instead that if $ar' - bs' \in \mathfrak{p}^k$, then $af + br \in \mathfrak{p}^{2k}$.

By Lemma 9.3, at least one of r' and s' is a unit modulo $\mathfrak{p}$. Without loss of generality,

suppose r' is a unit. Then r' is a unit modulo $\mathfrak{p}^{2k}$. Because $fs' \equiv -rr'$,

$$\begin{aligned} f(ar' - bs') &\equiv (af + br)r' \pmod{\mathfrak{p}^{2k}} \\ 0 &\equiv (af + br)r' \pmod{\mathfrak{p}^{2k}} && f, ar' - bs' \in \mathfrak{p}^k \\ 0 &\equiv (af + br) \pmod{\mathfrak{p}^{2k}} && r' \text{ a unit.} \end{aligned}$$

□

Now suppose D is a reduced divisor, with ideal I_D generated by two polynomials $\langle f, r\rangle$, one of which, f, is the minimum polynomial in I_D. Let $d' : W_D^m \to W^{m'}$ be the map defined by

$$\begin{aligned} d' : W_D^m &\to W^{m'} \\ af + bg &\mapsto ar' - bs'. \end{aligned}$$

We have a new diagram

$$W_{2D}^m \xhookrightarrow{\ker M'_{\text{doub}}} W_D^m \xrightarrow{d'} W^{m'} \xrightarrow{\pi} \frac{W^{m'}}{W_D^{m'}} \quad \text{with} \quad W_D^m \xrightarrow{M'_{\text{doub}}} \frac{W^{m'}}{W_D^{m'}} .$$

The kernel of M'_{doub} consists exactly of the polynomials $af+br \in W_D^m$ for which $ar'-bs' \in I_D$. By Theorem 9.4, this is exactly W_{2D}^m. There is never a need to compute a basis for the image of M'_{doub} or to compute a second divisor such as D_0 from Section 9.1.

An advantage to this method is that the difference between $\mathrm{LM}(f)$ and $\mathrm{LM}(r')$ is smaller than the difference between $\mathrm{LM}(f)$ and $\mathrm{LM}(f_xF_y - f_yF_x)$. Consequently, reducing r' modulo $\langle f, g, h\rangle$ is faster than reducing $f_xF_y - f_yF_x$.

This results in Algorithm 9.2. We will use this algorithm to double D when we have a pair of polynomials that generate I_D. When D is type 11, 21, or 22, the reduced Gröbner basis for I_D is such a pair. When D is a typical type 31 divisor, then $\langle f, g, h\rangle$ is a Gröbner basis and the pair (f, g) has the desired properties. Recall that this case is characterized by

$f_2 \neq 0$. If D is an atypical type 31 divisor, then $I_D \neq \langle f, g \rangle$, but it may be the case that $I_D = \langle f, h \rangle$. This case is characterized by $h_2 c_8 + f_1 c_7 - c_4 + h_1 = 0$. (Recall that c_i are the coefficient of F. See Equation 2.13.) In the remaining case where $\langle f, g \rangle \neq I_D \neq \langle f, h \rangle$, we may use Algorithm 9.1.

Algorithm 9.2 Fast Divisor Doubling

Input: A reduced divisor D, represented by the reduced Gröbner basis of its ideal I_D. This Gröbner basis is $\{f, g, h\}$ if D is of type 31, otherwise $\{f, g\}$

Output: A divisor D' equivalent to $2D$, represented by the reduced Gröbner basis of its ideal $I_{D'}$

if $D = 0$ **then**
    return D
else if $0 < \deg D < 3$ **then**
    $r \leftarrow g$
else if $\deg D = 3$ **then**
    if $I_D = \langle f, g \rangle$ **then**
        $r \leftarrow g$
    else if $I_D = \langle f, h \rangle$ **then**
        $r \leftarrow h$
    else
        Compute D' via Algorithm 9.1 on input D
        return D'
    end if
end if
Find r', s' such that $fs' \equiv -rr'$
Compute M'_{doub}
Compute $\text{RREF}(M'_{\text{doub}})$ and $\ker M'_{\text{doub}}$.
return $2D$

9.3 Example of General Doubling

Consider the $C_{3,4}$ curve $C : F(x, y) = 0$ over $K = \mathbb{F}_{31}$, given by $F(x, y) = y^3 + x^4 + 1$. Let $I_D = \langle f, g, h \rangle$, where

$$f = x^2 - 10$$

$$g = xy + 14y + 10x - 15$$

$$h = y^2 + 12y - 11$$

is a reduced Gröbner basis. Then $\langle f, g\rangle \neq I_D \neq \langle f, h\rangle$.

The divisor $2D$ has degree 6. Referring to Table 7.1, no degree 6 divisor has a Gröbner basis containing a monomial larger than x^4. Thus, we take $m = x^4$ as a bound and construct the space W_D^m. This space W_D^m is 7-dimensional, with an echelon basis

$$W_D^m = \mathrm{Span}_K\{f, g, h, xf, xg, xh, x^2f\}.$$

We compute the differentials of these basis elements,

$$\begin{aligned}
df &= 6xy^2 \\
dg &= -7x^4 + 6x^3 - y^2 - 3 \\
dh &= -8x^3y + 14x^3 \\
d(xf) &= 9x^2y^2 + y^2 \\
d(xg) &= -10x^5 - 5x^4 - 2xy^2 - 14y^2 - 6x - 11 \\
d(xh) &= -11x^4y + 9x^4 - 2y^2 - 3y - 5 \\
d(x^2f) &= 12x^3y^2 + 2xy^2
\end{aligned}$$

The largest monomial appearing in the differentials is x^3y^2, so d is a map $W_D^{x^4} \to W^{x^3y^2}$.

We reduce the differentials modulo $W_D^{x^3y^2}$ (equivalently, we reduce modulo I_D), to get

$$\begin{aligned}
\overline{df} &= -15y + 11x + 5 \\
\overline{dg} &= 12y - 2x - 1 \\
\overline{dh} &= 4y + 10x + 9 \\
\overline{d(xf)} &= -7y + 9 \\
\overline{d(xg)} &= -13y + 3x + 5 \\
\overline{d(xh)} &= 6y + 5 \\
\overline{d(x^2f)} &= 5y - 14x - 12.
\end{aligned}$$

Therefore M_{doub} is the matrix

$$M_{\text{doub}} = \begin{pmatrix} 5 & -1 & 9 & 9 & 5 & 5 & -12 \\ 11 & -2 & 10 & 0 & 3 & 0 & -14 \\ -15 & 12 & 4 & -7 & -13 & 6 & 5 \end{pmatrix}.$$

It has reduced row echelon form and kernel

$$\text{RREF}(M_{\text{doub}}) = \begin{pmatrix} 1 & 0 & 0 & 9 & -14 & 4 & 10 \\ 0 & 1 & 0 & -15 & 14 & -8 & 0 \\ 0 & 0 & 1 & 15 & 3 & -6 & 0 \end{pmatrix}, \quad \ker M_{\text{doub}} = \begin{pmatrix} -9 & 14 & -4 & -10 \\ 15 & -14 & 8 & 0 \\ -15 & -3 & 6 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Therefore $W^m_{D_1}$ is

$$W^m_{D_1} = \mathrm{Span}_K \left\{ \begin{array}{l} xf - 15h + 15g - 9f, \\ xg - 3h - 14g + 14f, \\ xh + 6h + 8g - 4f, \\ x^2 f - 10f \end{array} \right\}$$

$$= \mathrm{Span}_K \left\{ \begin{array}{l} x^3 - 15y^2 + 15xy - 9x^2 - y - 15x - 1, \\ x^2 y - 3y^2 - 7x^2 - 15y + 10, \\ xy^2 + 6y^2 - 11xy - 4x^2 - 2y + 7x + 9, \\ x^4 + 11x^2 + 7 \end{array} \right\}.$$

Since M_{doub} had full rank, $I_{D_1} = I_{2D}$. So $2D$ is of type 61 and the first three polynomials in the computed basis for $W^m_{D_1}$ form a reduced Gröbner basis for I_{2D}.

9.4 Example of Faster Doubling

Consider again the $C_{3,4}$ curve $C : F(x, y) = 0$ over $K = \mathbb{F}_{31}$, given by $F(x, y) = y^3 + x^4 + 1$. Let $I_D = \langle f, g, h \rangle$ be the typical type 31 divisor given by

$$f = x^2 + 4y + 4x + 6$$

$$g = xy + y + 5x - 10$$

$$h = y^2 - 2y - 4x + 15.$$

Then $I_D = \langle f, r \rangle$, where $r = g$.

There exist polynomials

$$r' = xy + r'_2 y + r'_1 x + r'_0$$

$$s' = y^2 + s'_3 x^2 + s'_2 y + s'_1 x + s'_0$$

such that $fs' \equiv rr' \pmod{F}$. The coefficients of r' and s' may be found by equating

coefficients in $fs' - rr' - f_2F = 0$ and solving the resulting system of linear equations:

$$\begin{aligned}
s'_3 - 4 &= 0 \\
-r'_2 + 4 - r_2 &= 0 \\
4s'_3 - s'_1 + s'_2 - r_1 &= 0 \\
4s'_3 + s'_1 &= 0 \\
4s'_2 - s'_2 r_2 + 6 &= 0 \\
4s'_2 + 4s'_1 - s'_2 r_1 - r'_1 r_2 - r'_0 - r_0 &= 0 \\
6s'_3 + 4s'_1 - r'_1 r_1 + s'_0 &= 0.
\end{aligned}$$

This gives $r' = xy + 3y - 13x + 3$ and $s' = y^2 + 4x^2 + 7y + 15x + 6$.

An echelon basis for W_D^m is given by

$$W_D^m = \mathrm{Span}_K\{f, g, h, xf, xg, xh, x^2 f\}.$$

We must compute the image under M'_{doub} of each of these basis elements. $M'_{\mathrm{doub}}(f)$ and $M'_{\mathrm{doub}}(g)$ are, respectively, the reductions of r' and s' modulo I_D,

$$\begin{aligned}
M'_{\mathrm{doub}}(f) &= 2y + 13x + 13 \\
M'_{\mathrm{doub}}(g) &= -7y + 3x - 2.
\end{aligned}$$

We have $h = ((y+5)f - (x+3)r)/4$, so compute $M'_{\mathrm{doub}}(h)$ by reducing $((y+5)r' - (x+3)s')/4$ modulo I_D.

$$M'_{\mathrm{doub}}(h) = 10y + 10x - 5.$$

The first three columns of M'_{doub} are

$$M'_{\text{doub}} = \begin{pmatrix} 13 & -2 & -5 & * & * & * & * \\ 13 & 3 & 10 & * & * & * & * \\ 2 & -7 & 10 & * & * & * & * \end{pmatrix}.$$

Following suit for xf, xg, xh and x^2f,

$$M'_{\text{doub}} = \begin{pmatrix} 13 & -2 & -5 & 4 & 5 & 9 & 2 \\ 13 & 3 & 10 & 13 & -10 & -2 & 5 \\ 2 & -7 & 10 & 8 & -5 & 12 & 2 \end{pmatrix}$$

with reduced row echelon form and kernel

$$\text{RREF}(M'_{\text{doub}}) = \begin{pmatrix} 1 & 0 & 0 & 1 & -13 & -11 & 0 \\ 0 & 1 & 0 & -13 & -11 & -11 & -9 \\ 0 & 0 & 1 & 7 & 13 & 5 & -3 \end{pmatrix}, \quad \ker M'_{\text{doub}} = \begin{pmatrix} -1 & 13 & 11 & 0 \\ 13 & 11 & 11 & 9 \\ -7 & -13 & -5 & 3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Therefore W^m_{2D} is

$$\begin{aligned} W^m_{2D} &= \text{Span}_K \left\{ \begin{array}{l} xf - 7h + 13g - f, \\ xg - 13h + 11g + 13f, \\ xh - 5h + 11g + 11f, \\ x^2f - 3h - 9g \end{array} \right\} \\ &= \text{Span}_K \left\{ \begin{array}{l} x^3 - 7y^2 - 14xy + 3x^2 - 8y + 2x + 7, \\ x^2y - 13y^2 + 12xy - 13x^2 - 4y - 6x - 10, \\ xy^2 - 5y^2 + 9xy + 7x^2 + 3y + 10x + 5, \\ x^4 + 4x^2y + 4x^3 + 3y^2 + 9xy + 6x^2 + 3y + 2x - 14 \end{array} \right\}. \end{aligned}$$

So $2D$ is of type 61 and the first three polynomials form a reduced Gröbner basis for I_{2D}.

10 Reduction

In the previous two chapters, we were concerned with adding and doubling reduced divisors, thereby producing (likely) unreduced divisors. Given an unreduced divisor D, we now wish to find the unique reduced divisor $\overline{\overline{D}}$ to which it is equivalent in the divisor class group. We will use the letters u, v, w to refer to elements of the reduced Gröbner basis of the ideal of the possibly unreduced divisor D. We will use the letters f, g, h for elements of a Gröbner basis of the reduced equivalent $\overline{\overline{D}}$.

Arita and Abu Salem/Khuri-Makdisi recognized that flipping a divisor twice would reduce it (though Arita did not use the term "flipping"), and that flipping in the divisor class group is analogous to computing quotient ideals in the ideal class group.

In [3], Arita reduces divisors by flipping twice. Given D, one computes $\overline{D}$ followed by $\overline{\overline{D}}$ in two separate steps. Each flip operation requires one inversion in the finite field, and several multiplications. For instance, if D is a type 61 divisor, it costs 1I+54M (1 finite field inversion and 54 finite field multiplications) to compute $\overline{D}$ and 1I+16M to compute $\overline{\overline{D}}$.

In [40], Abu Salem and Khuri-Makdisi recognize that the field inversions performed when computing $\overline{D}$ and $\overline{\overline{D}}$ are in fact the same values. When flipping $I_D = \langle u, v\rangle$ to get $I_{\overline{D}} = \langle f, g'\rangle$, they must compute f_2^{-1}, where f_2 is the coefficient of y in f_2. When computing $I_{\overline{\overline{D}}} = \langle f, g\rangle$, they must again compute f_2^{-1}. They therefore save an expensive inversion operation by passing f_2^{-1} as an input to the second flip operation. They are able to compute $\overline{D}$ in 1I+31M and $\overline{\overline{D}}$ in 0I+7M, a total of 1I+38M.

In [26], Khuri-Makdisi gives an improvement over the cost of reducing in [40] by viewing reduction in a single step rather than as two flip operations. The cost of reduction is decreased to 1I+19M, which is, remarkably, cheaper than even a single flip operation. In this chapter, we will show that the reduction method presented in [26] may be applied to divisors of all types, with one small exception — the same exception encountered in Chapter 9.

In Chapter 9, we had to fall back on slower methods to double type 31 divisors with $\langle f, g\rangle \neq \langle f, g, h\rangle \neq \langle f, h\rangle$. Type 31, 41, 51, and 61 divisors with the same property $\langle u, v\rangle \neq$

$\langle u, v, w\rangle \neq \langle u, w\rangle$ present an obstacle for us again here (though see Section 13.1, Future Work) and we will reduce those divisors via two discrete flip steps.

We will first present in Section 10.1 a method to compute the flip of a divisor, which is a generalization of the method in [40] to include atypical divisors. Afterwards, in Section 10.2, we will see how to reduce a divisor in a single reduction operation, a generalization of [26] to include almost all atypical divisors.

This chapter makes frequent use of colon ideals. The reader is reminded that notation and basic properties of the colon ideal are given in Appendix A.

10.1 Flipping

When flipping a divisor D, we have three cases to consider: the reduced Gröbner basis of I_D consists of 1, 2, or 3 elements.

In the first case, suppose the reduced Gröbner basis of I_D consists of 1 element. That is $I_D = \langle u\rangle$ is principal. In this case, flipping D could not be easier. By Proposition A.1.(vi),

$$I_{\overline{D}} = u : I_D = \langle 1\rangle .$$

When asked to flip a principal divisor, we return $\overline{D} = 0$ or equivalently $I_{\overline{D}} = \langle 1\rangle$.

Suppose instead the reduced Gröbner basis for I_D has 2 elements, $I_D = \langle u, v\rangle$. Then

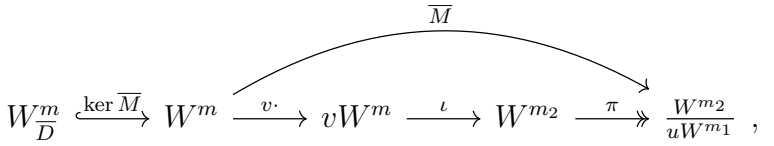
$$I_{\overline{D}} = u : I_D = u : \langle u, v\rangle = u : v.$$

Therefore

$$I_{\overline{D}} = \{p \in K[C] \mid pv \in \langle u\rangle\}.$$

To compute $I_{\overline{D}}$ is to find polynomials p for which $pv \in \langle u\rangle$. As was the case for addition and doubling, we will restrict our search space by choosing a bounding monomial m. We know *a priori* what the type of $\overline{\overline{D}}$ is (Table 7.4), so we let m be the largest monomial appearing in

the reduced Gröbner basis of an ideal of that type. We then look for polynomials $p \in W^m$ for which pv vanishes modulo u. Those polynomials arise as the kernel of the map $\overline{M}$ in



$$W^m_{\overline{D}} \xhookrightarrow{\ker \overline{M}} W^m \xrightarrow{v\cdot} vW^m \xrightarrow{\iota} W^{m_2} \xrightarrow{\pi} \frac{W^{m_2}}{uW^{m_1}} \ ,$$

where $v\cdot$ is the multiplication by v map and m_1 and m_2 are chosen such that

$$-\nu_{P_\infty}(m_2) = -\nu_{P_\infty}(m \operatorname{LM}(v)) = -\nu_{P_\infty}(m_1 \operatorname{LM}(u)). \tag{10.1}$$

Now suppose that $\langle u, v, w\rangle$ is a Gröbner basis for I_D. Typically, the first two polynomials alone are enough to generate I_D. That is, $\langle u, v, w\rangle = \langle u, v\rangle$. In that case, we may flip D by computing the kernel of the map $\overline{M}$ above.

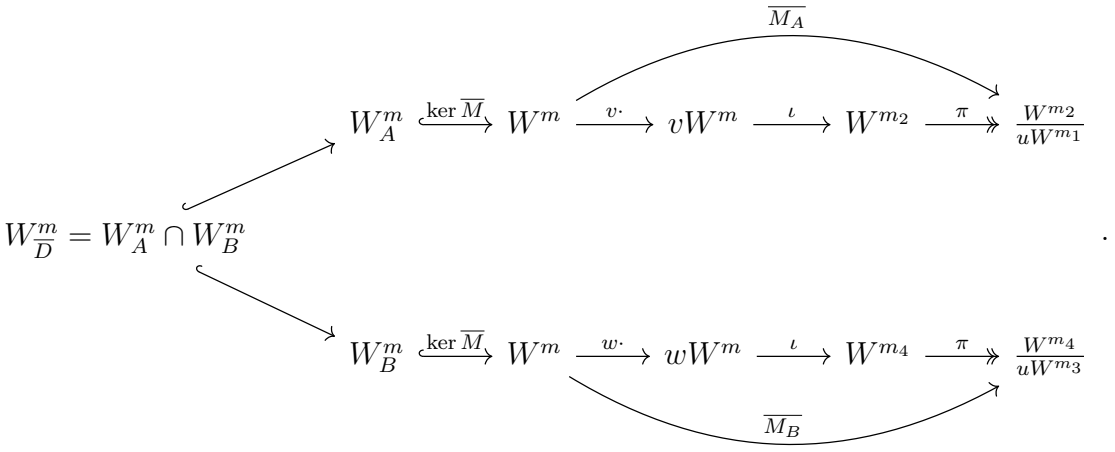
Sometimes, $\langle u, v, w\rangle \neq \langle u, v\rangle$, but it may still be that $\langle u, v, w\rangle = \langle u, w\rangle$. In this case, too, we may flip D by computing the kernel of the map $\overline{M}$ above, though replace v with w in the diagram.

The more difficult case is when $\langle u, v\rangle \neq \langle u, v, w\rangle \neq \langle u, w\rangle$. In this case, we observe that

$$I_{\overline{D}} = u : \langle u, v, w\rangle = u : \langle v, w\rangle = (u : v) \cap (u : w).$$

Let $A = \operatorname{div}(u : v) = \operatorname{div} v - D$ and $B = \operatorname{div}(u : w) = \operatorname{div} w - D$. Then $\overline{D} = \operatorname{lcm}(A, B)$. We may compute each of A and B individually using method outlined above, then compute

their least common multiple using methods from Chapter 8.



10.2 Reduction without Flipping

In the appendix of [26], Khuri-Makdisi presents an improvement over his previous joint work with Abu Salem in [40]. The improvement lies entirely in the reduction step.

Let D be a typical degree 6 divisor, with ideal $I_D = \langle u, v, w\rangle$. Since D is typical, the first two polynomials alone are enough to generate I_D, so $I_D = \langle u, v\rangle$. In prior work [40], D was reduced by flipping twice, computing $\overline{D}$ and then $\overline{\overline{D}}$. In [26], it is observed that this is more work than is necessary. It is known *a priori* that $\overline{\overline{D}}$ is a typical degree 3 divisor. The minimum polynomial $f \in I_{\overline{\overline{D}}}$ is therefore known to be of the form $f = x^2 + f_2 y + f_1 x + f_0$. It is shown in the appendix of [26] that to compute $\overline{\overline{D}}$, it is enough to find a polynomial $g \in K[C]$ such that $fv \equiv gu \pmod F$. Then

$$I_{\overline{\overline{D}}} = \langle f, \overline{g}\rangle\,,$$

where $\overline{g}$ is the reduction of g modulo f.

This statement holds in greater generality than was considered in [26]. It applies to any divisor D whose ideal I_D is generated by two polynomials u, v, where u is the minimum polynomial in I_D. We will prove that the methods outlined in the appendix of [26] may be applied to this wider class of divisors. First, we will establish a lemma that relates generators

of $u : v$ and $v : u$.

Lemma 10.2. *Let $I_D = \langle u, v \rangle$ and let $\langle f, r \rangle = u : v$. Then there exist polynomials $g, s \in K[C]$ such that*

$$fv \equiv gu \pmod{F}$$
$$rv \equiv su \pmod{F}$$

and $\langle g, s \rangle = v : u$.

Proof. The existence of g and s satisfying the two congruence relations comes from the fact that $\langle f, r \rangle = u : v$ and the definition of the colon ideal. Now $(u : v) \langle u, v \rangle = \langle u \rangle$, so

$$\begin{aligned} \langle u \rangle &= \langle f, r \rangle \langle u, v \rangle \\ &= \langle fu, fv, ru, rv \rangle \\ &= \langle fu, gu, ru, su \rangle \\ &= \langle f, g, r, s \rangle \langle u \rangle , \end{aligned}$$

hence

$$\langle f, g, r, s \rangle = \langle 1 \rangle , \tag{10.3}$$

and

$$\begin{aligned} \langle v \rangle &= \langle fv, gv, rv, sv \rangle \\ &= \langle gu, gv, su, sv \rangle \\ &= \langle g, s \rangle \langle u, v \rangle . \end{aligned}$$

Therefore $\langle g, s \rangle = v : u$. □

Theorem 10.4. *Let $I_D = \langle u, v \rangle$, where u is the minimum polynomial in I_D. Let $I_{\overline{D}} = \langle f, r \rangle$,*

where f is the minimum polynomial in $I_{\overline{D}}$. Then there is a polynomial g such that $fv \equiv gu \pmod{F}$ and $I_{\overline{\overline{D}}} = \langle f, g \rangle$.

Proof. By Lemma 10.2, there are polynomials $g, s \in K[C]$ such that $fv \equiv gu$, $rv \equiv su$, and $\langle g, s \rangle = v : u$. The polynomial g is the minimum polynomial in $\langle g, s \rangle$, otherwise f would not be the minimum in $u : v$.

Let $A = \operatorname{div}(g, s)$. Then $I_{\overline{A}} = g : s$. By Proposition 7.4, $\overline{A} = \overline{\overline{D}}$, so $g : s = f : r = I_{\overline{\overline{D}}}$.

Now certainly $\langle f, g \rangle \subseteq I_{\overline{\overline{D}}}$, since $f \in f : r = I_{\overline{\overline{D}}}$ and $g \in g : s = I_{\overline{\overline{D}}}$.

Let $t \in I_{\overline{\overline{D}}}$. Then $t \in f : r$ and $t \in g : s$, therefore $rt \in \langle f \rangle$ and $st \in \langle g \rangle$, so $\langle rt, st \rangle \subseteq \langle f, g \rangle$. By Equation 10.3,

$$\langle t \rangle = \langle ft, gt, rt, st \rangle = \langle ft, gt \rangle + \langle rt, st \rangle .$$

Now $\langle ft, gt \rangle$ and $\langle rt, st \rangle$ are both contained in $\langle f, g \rangle$, while their sum $\langle ft, gt \rangle + \langle rt, st \rangle = \langle t \rangle$ is the smallest ideal containing them. Therefore $\langle t \rangle \subseteq \langle f, g \rangle$ and we conclude $t \in \langle f, g \rangle$. □

Remark 10.5. It is required that u and f be the minimum polynomials in their respective ideals. Recall that the definition of D is $\overline{D} = \operatorname{div} u - D$ (or in the ideal class group, $I_{\overline{D}} = u : I_D$) where u is the minimum polynomial. If u is not the minimum, then $I_{\overline{D}} \neq u : v$.

In Section 10.4, we will see how Theorem 10.4 is applied. It can be used to quickly reduce divisors of all types, except for atypical divisors of types 31, 41, 51, and 61 where $\langle u, v \rangle \neq \langle u, v, w \rangle \neq \langle u, w \rangle$. In that case, we flip twice using the method in Section 10.1. On a curve over a finite field of order q, heuristically, we expect this troublesome case to arise with probability approximately $\frac{1}{q^2}$ for large q.

10.3 Flipping Example

Let C be the $C_{3,4}$ curve over $\mathbb{F}_{31}$ given by the polynomial equation $F(x,y) = y^3 + x^4 + 1 = 0$. Let D be the type 61 divisor given by the ideal $I_D = \langle u, v, w \rangle$, where

$$\begin{aligned} u &= x^3 - 12y^2 + 2xy - 13x^2 - 10y + 7x + 10, \\ v &= x^2y - 9y^2 - 5xy + 2x^2 - 2x + 9, \\ w &= xy^2 - 4y^2 - 9xy - 5x^2 - 3y - 5x + 11. \end{aligned}$$

In this particular example, we have $\langle u, v \rangle \neq \langle u, v, w \rangle \neq \langle u, w \rangle$. (See Lemmas 7.22 and 7.25.) Therefore we compute $I_{\overline{D}} = (u : v) \cap (u : w)$. Let $A = \operatorname{div}(u : v)$ and $B = \operatorname{div}(u : w)$. We will compute A and B.

We know from Table 7.4 that $\overline{D}$ is a type 31 divisor. From Table 7.1, we also know that no monomial in the reduced Gröbner basis of $I_{\overline{D}}$ is larger than $m = y^2$. The monomial x^6 is chosen as x^6 has the same pole order as $m \operatorname{LM}(v) = x^2y^3$. The other monomial x^3 is chosen as $x^3 \cdot \operatorname{LM}(u) = x^6$. (See Equation 10.1.)

To find A, we must compute the kernel of the map M_{flip} in the diagram

$$W_A^{y^2} \xhookrightarrow{\ker M_{\text{flip}}} W^{y^2} \xrightarrow{v\cdot} vW^{y^2} \xrightarrow{\iota} W^{x^6} \xrightarrow{\pi} \frac{W^{x^6}}{uW^{x^3}}, \qquad W^{y^2} \xrightarrow{M_{\text{flip}}} \frac{W^{x^6}}{uW^{x^3}}.$$

We will need bases for W^{y^2} and uW^{x^3}

$$\begin{aligned} W^{y^2} &= \operatorname{Span}_K\{1, x, y, x^2, xy, y^2\} \\ uW^{x^3} &= \operatorname{Span}_K\{u, xu, yu, x^2u, xyu, y^2u, x^3u\}. \end{aligned}$$

We must compute the image of the monomial basis of W^{y^2} under the map M_{flip}, so we must multiply each monomial in the basis of W^{y^2} by v and reduce modulo u. In the matrix below,

we encode all the coefficients of $u, xu, \ldots, x^3u$ and $v, xv, \ldots, y^2v$. All y^3 terms are reduced modulo F.

	u	xu	yu	x^2u	xyu	y^2u	x^3u	v	xv	yv	x^2v	xyv	y^2v
1	10	0	12	0	0	10	0	9	0	9	0	0	0
x	7	10	0	0	12	29	0	29	9	0	0	9	5
y	21	0	10	0	0	12	0	0	0	9	0	0	9
x^2	18	7	0	10	0	0	0	2	29	0	9	0	30
xy	2	21	7	0	10	0	0	26	0	29	0	9	0
y^2	19	0	21	0	0	10	0	22	0	0	0	0	9
x^3	1	18	0	7	0	0	10	0	2	0	29	0	0
x^2y	0	2	18	21	7	0	0	1	26	2	0	29	0
xy^2	0	19	2	0	21	7	0	0	22	26	0	0	29
x^4	0	1	12	18	0	10	7	0	0	9	2	0	0
x^3y	0	0	1	2	18	0	21	0	1	0	26	2	0
x^2y^2	0	0	0	19	2	18	0	0	0	1	22	26	2
x^5	0	0	0	1	12	29	18	0	0	0	0	9	5
x^4y	0	0	0	0	1	12	2	0	0	0	1	0	9
x^3y^2	0	0	0	0	0	1	19	0	0	0	0	1	0
x^6	0	0	0	0	0	0	1	0	0	0	0	0	30

Now we reduce the columns of the right-hand side of the matrix modulo the columns of

the left-hand side.

	u	xu	yu	x^2u	xyu	y^2u	x^3u	v	xv	yv	x^2v	xyv	y^2v
1	10	0	12	0	0	10	0	9	9	17	9	17	26
x	7	10	0	0	12	29	0	29	29	21	29	21	11
y	21	0	10	0	0	12	0	0	0	1	0	1	20
x^2	18	7	0	10	0	0	0	2	2	1	2	1	26
xy	2	21	7	0	10	0	0	26	26	9	26	9	10
y^2	19	0	21	0	0	10	0	22	22	9	22	9	29
x^3	1	18	0	7	0	0	10	0	0	0	0	0	0
x^2y	0	2	18	21	7	0	0	1	1	15	1	15	24
xy^2	0	19	2	0	21	7	0	0	0	10	0	10	14
x^4	0	1	12	18	0	10	7	0	0	0	0	0	0
x^3y	0	0	1	2	18	0	21	0	0	0	0	0	0
x^2y^2	0	0	0	19	2	18	0	0	0	1	0	1	20
x^5	0	0	0	1	12	29	18	0	0	0	0	0	0
x^4y	0	0	0	0	1	12	2	0	0	0	0	0	0
x^3y^2	0	0	0	0	0	1	19	0	0	0	0	0	0
x^6	0	0	0	0	0	0	1	0	0	0	0	0	0

The non-zero rows on the right describe the matrix M_{flip}.

$$M_{\text{flip}} = \begin{pmatrix} 9 & 9 & 17 & 9 & 17 & 26 \\ 29 & 29 & 21 & 29 & 21 & 11 \\ 0 & 0 & 1 & 0 & 1 & 20 \\ 2 & 2 & 1 & 2 & 1 & 26 \\ 26 & 26 & 9 & 26 & 9 & 10 \\ 22 & 22 & 9 & 22 & 9 & 29 \\ 1 & 1 & 15 & 1 & 15 & 24 \\ 0 & 0 & 10 & 0 & 10 & 14 \\ 0 & 0 & 1 & 0 & 1 & 20 \end{pmatrix}.$$

It is clear at a glance that most of the rows in this matrix are linearly dependent. Its reduced

row echelon form and kernel are

$$\mathrm{RREF}(M_{\text{flip}}) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 0 & 1 & 20 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \ker(M_{\text{flip}}) = \begin{pmatrix} -1 & -1 & 0 & -3 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -20 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Therefore $W_A^{y^2}$ is spanned by

$$W_A^{y^2} = \mathrm{Span}_K\{x-1,\ x^2-1,\ xy-y,\ y^2-20y-3\}$$

and A is the type 22 divisor given by

$$I_A = \left\langle x-1,\ y^2-20y-3 \right\rangle.$$

To find B, we follow the same process, computing the kernel of M_{flip} in

$$W_B^{y^2} \xhookrightarrow{\ker M_{\text{flip}}} W^{y^2} \xrightarrow{w\cdot} vW^{y^2} \xrightarrow{\iota} W^{x^5y} \xrightarrow{\pi} \frac{W^{x^5y}}{uW^{x^2y}}\ .$$

We find that $W_B^{y^2}$ is spanned by

$$W_B^{y^2} = \mathrm{Span}_K\{y+12x-8, x^2+13x-14, xy-9x+13, y^2-13x-3\}$$

and B is the type 21 divisor given by

$$I_A = \left\langle y + 12x - 8, x^2 + 13x - 14 \right\rangle.$$

Now given $W_A^{y^2}$ and $W_B^{y^2}$ one may compute $W_{\overline{D}}^{y^2} = W_A^{y^2} \cap W_B^{y^2}$ using standard linear algebra techniques. Alternatively, given I_A and I_B, one may compute $I_{\overline{D}} = I_{\mathrm{lcm}(A,B)}$ using methods from Chapter 8.

Remark 10.6. The matrices above were rather large, and a lot of unnecessary computational effort goes into filling them completely. The first eight rows of the large matrix were linearly dependent, and this will always be the case. One may safely ignore all rows above the line representing coefficients of the monomial x^2y.

The vector spaces $W_A^{y^2}$ and $W_B^{y^2}$ were 4-dimensional, while the reduced Gröbner bases they produced consisted only of two elements each. Therefore two columns in the kernel we computed were unnecessary. One can save time by ignoring the two columns corresponding to the unnecessary kernel basis vectors. It is cheaper to derive those two vectors from the other two.

Considerably less computation time needs to be spent on a flip operation than may appear.

10.4 Reduction Example

Let C be the $C_{3,4}$ curve over $\mathbb{F}_{31}$ given by the polynomial equation $F(x, y) = y^3 + x^4 + 1 = 0$. In Section 9.4, we doubled a type 31 divisor to produce a type 61 divisor. Let D be that type 61 divisor, given by the ideal $I_D = \langle u, v, w \rangle$, where

$$\begin{aligned} u &= x^3 - 7y^2 - 14xy + 3x^2 - 8y + 2x + 7, \\ v &= x^2y - 13y^2 + 12xy - 13x^2 - 4y - 6x - 10, \\ w &= xy^2 - 5y^2 + 9xy + 7x^2 + 3y + 10x + 5. \end{aligned}$$

In that example, we could have saved some effort by not computing w at all, for we will not need it in this example. By Lemma 7.22, this divisor is typical, so that $I_D = \langle u, v \rangle$. We may ignore w and compute $\overline{\overline{D}}$ by applying Theorem 10.4.

By Theorem 10.4, there exist polynomials $f, g \in K[C]$ such that $fv \equiv gu$ and $I_{\overline{\overline{D}}} = \langle f, g \rangle$. We know *a priori* that $\overline{\overline{D}}$ is a typical type 31 divisor, and we may deduce that f and g are of the forms

$$f = x^2 + f_2 y + f_1 x + f_0$$
$$g = xy + g_3 x^2 + g_2 y + g_1 x + g_0.$$

Notice the x^2 term in g; g is not assumed to be reduced modulo f. We will have to reduce it later.

Now we use the relation $fv \equiv gu \pmod{F}$ to solve for the coefficients of f and g. We observe that the polynomial $fv - gu$ (as a member of $K[x, y]$) contains the terms $(-13f_2 + 7g_2)y^3$ and $7xy^3$. Thus we equate coefficients in

$$fv - gu - (7x - 13f_2 + 7g_2)F = 0$$

to get a system of linear equations

$$\begin{aligned}
-g_3 - 7 &= 0 \\
f_2 + 7g_3 + 1 &= 0 \\
f_1 - g_2 + 14g_3 + 9 &= 0 \\
13f_2 - g_1 - 7g_2 - 3g_3 - 13 &= 0 \\
-13f_1 + 12f_2 + 7g_1 + 14g_2 + 8 &= 0 \\
f_0 + 12f_1 - 13f_2 + 14g_1 - 3g_2 + 8g_3 - 6 &= 0 \\
-13f_1 - g_0 - 3g_1 - 2g_3 - 6 &= 0.
\end{aligned}$$

Solving this system gives $f = x^2 - 14y + 11x + 10$ and $g = xy - 7x^2 + 15y - 11$. We then reduce g modulo f to get

$$I_{\overline{\overline{D}}} = \left\langle x^2 - 14y + 11x + 10,\ xy + 10y + 15x - 3 \right\rangle.$$

These two polynomials alone do not form a Gröbner basis for $I_{\overline{\overline{D}}}$. For that we need the third polynomial

$$\begin{aligned} h &= \frac{(y+15)f - (x+1)g}{-14} \\ &= y^2 + 15y + 9x + 9. \end{aligned}$$

Note that $y + 15$, $x + 1$ and 14 are the solutions r, s, and t, respectively, from Lemma 7.21.

11 Explicit Formulae

The three previous chapters discuss adding, doubling, and reducing arbitrary divisors. With the methods described in those chapters, we may add any two reduced divisors, double any reduced divisor, and reduce any unreduced divisor.

Suppose C is a $C_{3,4}$ curve over the finite field $\mathbb{F}_q$. As $q \to \infty$, the chance that a divisor of C chosen uniformly at random is atypical tends toward $\frac{1}{q}$ (Theorem 2.10 in [26]). Consequently, if we are adding or doubling divisors, we will spend most of our time — almost all of it if q is very large — adding and doubling typical type 31 divisors and reducing typical type 61 divisors. Any algorithm which requires adding and doubling divisors will benefit greatly from having the arithmetic in those cases highly optimized. In this chapter, we will apply the methods described in Chapters 8, 9, and 10 and derive explicit formulae to efficiently handle the typical cases arising in divisor class group arithmetic: adding and reducing two disjoint typical type 31 divisors, and doubling and reducing a typical type 31 divisor.

We saw in Chapter 8 that in order to add two divisors, we must first compute the kernel of a matrix M_{add}. Likewise, to double a divisor, we must first compute the kernel of a matrix M_{doub}. In the following two sections, we will see explicit formulae describing the entries of these matrices. After computing the elements of the matrices, the rest of the algorithm — row-reducing the matrices, computing their kernel, then reducing the resulting divisor — proceeds identically.

The formulae we derive in this chapter are more efficient than the current state-of-the-art published in [26]. The savings come primarily from two places. Firstly, after computing polynomials u, v for the basis of $\ker M_{\text{add}}$ (or $\ker M_{\text{doub}}$), the constant coefficients of u and v are not needed in the rest of the calculations. Therefore, we do not compute their constant coefficients, saving several multiplications. Secondly, computing the reduced row echelon form of M_{add} or M_{doub} requires one inversion operation, while reducing a divisor requires another inversion. It is possible to compute the inverses of two finite field elements while performing only one inversion operation, with a technique called Montgomery's Trick, a

mathematical case of killing two birds with one stone.

Example 11.1. Let a, b be non-zero elements of some finite field. Rather than inverting a and b separately, compute

$$c := ab, \quad d := \frac{1}{c}, \quad \alpha := bd, \quad \beta := ad.$$

Then $\alpha = a^{-1}$ and $\beta = b^{-1}$, while only one inversion operation was performed. One inversion is saved at the cost of 3 multipiclations.

Inversions in a finite field are expensive operations; it is worth eliminating one inversion even at the cost of many multiplications, although the exact number of multiplications one should be willing to trade is dependent on the software/hardware implementation of the finite field arithmetic and the size of the finite field. The formulae we find for adding and doubling cost, respectively, 1I+111M+3S+99A and 1I+135M+3S+116A, where I, M, S, A refer to the number of inversion, multiplications, squares, and additions in a finite field. We require more multiplications, but fewer inversions than [26] (which required 2I+98M+1S+132A and 2I+110M+3S+155A to add and double, respectively), so we compared Sage implementations of the formulae below and the formulae in [26] and found that the trade-off is worthwhile, at least in Sage. We refer later to literature that suggests that our formulae should be more efficient in other implementations, hardware or software.

For the remainder of this chapter, we will assume that C is a $C_{3,4}$ curve over a field K with $\operatorname{char} K = 0$ or $\operatorname{char} K > 3$, defined by a polynomial F. The curve C will be assumed to be given by an equation in short form (Equation 2.16), i.e. with coefficients c_5, c_6, and c_8 all equal to 0. Recall that over a field of characteristic other than 2 or 3, a $C_{3,4}$ curve may always be transformed to one in short form. The resulting formulae are collected and reproduced in one place at the end of Section 11.4.

11.1 Constructing the Matrix M_{add}.

We wish to add two type 31 divisors D and D', given by ideals $I_D = \langle f, g, h\rangle$ and $I_{D'} = \langle f', g', h'\rangle$, where

$$\begin{aligned} f &= x^2 + f_2y + f_1x + f_0 & f' &= x^2 + f'_2y + f'_1x + f'_0 \\ g &= xy + g_2y + g_1x + g_0 & g' &= xy + g'_2y + g'_1x + g'_0 \\ h &= y^2 + h_2y + h_1x + h_0 & h' &= y^2 + h'_2y + h'_1x + h'_0. \end{aligned}$$

We will assume that D and D' are disjoint and that $D + D'$ is a typical type 61 divisor. We will be able to detect whether these assumptions are violated,[26] and if so, we may fall back on the addition algorithm from Chapter 8. We need not assume that D or D' are typical; it is possible for $D + D'$ to be typical even if one or both of D and D' is not, and the formulae will still be correct.

We consider the map M_{add} in

$$W_{D+D'}^{x^2y} \xhookrightarrow{\ker M_{\text{add}}} W_D^{x^2y} \xhookrightarrow{\ \iota\ } W^{x^2y} \xrightarrow{\ \pi\ } \frac{W^{x^2y}}{W_{D'}^{x^2y}}\ .$$

Since we are assuming D and D' are disjoint, the kernel gives their sum $D + D'$ rather than merely $\operatorname{lcm}(D, D')$. We are assuming that $D + D'$ is typical, hence the third polynomial in the Gröbner basis of $I_{D+D'}$ is not needed, and the other two polynomials in the basis contain no monomial larger than x^2y.

We construct the matrix

$$M_{\text{add}} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}.$$

[26] Non-disjointedness is detected when M_{add} does not have full rank, and $D + D'$ can be confirmed to be typical via Lemma 7.22.

The space $W_D^{x^2y}$ is spanned by the basis $\{f, g, h, xf, xg\}$. The columns of M_{add}, from left to right, are the reductions of f, g, h, xf, xg modulo f', g', h'. Therefore, the first three columns are given by

$$\begin{aligned} a_1 &= f_0 - f_0' & a_2 &= g_0 - g_0' & a_3 &= h_0 - h_0' \\ a_6 &= f_1 - f_1' & a_7 &= g_1 - g_1' & a_8 &= h_1 - h_1' \\ a_{11} &= f_2 - f_2' & a_{12} &= g_2 - g_2' & a_{13} &= h_2 - h_2'. \end{aligned}$$

We may view multiplication by x as an endomorphism on $\frac{W^{x^2y}}{W_{D'}^{x^2y}}$, given by the matrix

$$T_x = \begin{pmatrix} 0 & -f_0' & -g_0' \\ 1 & -f_1' & -g_1' \\ 0 & -f_2' & -g_2' \end{pmatrix}.$$

We use this matrix to compute the reductions of xf and xg modulo f', g', h'. This gives the last two columns of M_{add}, via

$$\begin{pmatrix} a_4 & a_5 \\ a_9 & a_{10} \\ a_{14} & a_{15} \end{pmatrix} = \begin{pmatrix} 0 & -f_0' & -g_0' \\ 1 & -f_1' & -g_1' \\ 0 & -f_2' & -g_2' \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_6 & a_7 \\ a_{11} & a_{12} \end{pmatrix}.$$

This results in

$$\begin{aligned} a_4 &= -f_0' a_6 - g_0' a_{11} & a_5 &= -f_0' a_7 - g_0' a_{12} \\ a_9 &= a_1 - f_1' a_6 - g_1' a_{11} & a_{10} &= a_2 - f_1' a_7 - g_1' a_{12} \\ a_{14} &= -f_2' a_6 - g_2' a_{11} & a_{15} &= -f_2' a_7 - g_2' a_{12}. \end{aligned}$$

Lemma 11.2. *The matrix M_{add} may be computed in 12M+17A.*

11.2 Constructing the Matrix $M_{\mathbf{doub}}$.

We wish to double a type 31 divisor D, given by the ideal $I_D = \langle f, g, h \rangle$, where

$$f = x^2 + f_2 y + f_1 x + f_0$$
$$g = xy + g_2 y + g_1 x + g_0$$
$$h = y^2 + h_2 y + h_1 x + h_0.$$

We will assume that D is typical, so that $f_2 \neq 0$. Let the inverse of f_2 be $\phi = \frac{1}{f_2}$. We will assume that ϕ is given as an input to the doubling algorithm. This same assumption is made by [40] and [26], justified by the fact that ϕ may be included in the outputs of the reduction algorithm, and that typically one is adding or doubling divisors that were previously reduced by the reduction algorithm.

We must find $g', h' \in K[C]$ such that $fh' \equiv gg' \pmod{F}$. The polynomials g' and h' are of the forms

$$g' = xy + g'_2 y + g'_1 x + g'_0$$
$$h' = y^2 + h'_3 x^2 + h'_2 y + h'_1 x + h'_0.$$

Equating coefficients of g' and h' in the equation $fh' - gg' - f_2F = 0$ gives the solution

$$\begin{aligned}
h'_3 &= f_2 \\
g'_2 &= f_1 - g_2 \\
h'_2 &= \phi(g'_2 g_2 - f_0) \\
g'_1 &= f_2(f_2 - c_7) + h'_2 - g_1 \\
h'_1 &= -f_1 f_2 \\
g'_0 &= h'_2 f_1 + f_2(h'_1 - c_4) - g'_2 g_1 - g'_1 g_2 - g_0 \\
h'_0 &= f_2(c_3 - f_0) - h'_1 f_1 + g'_1 g_1.
\end{aligned}$$

We consider the map M_{doub} in

$$W_{2D}^{x^2y} \xhookrightarrow{\ker M_{\text{doub}}} W_D^{x^2y} \xhookrightarrow{d} W^{x^2y} \xrightarrow{\pi} \frac{W^{x^2y}}{W_{D'}^{x^2y}} \ ,$$

where $d(f) = g'$ and $d(g) = h'$. The space $W_D^{x^2y}$ is spanned by the basis

$$W_D^{x^2y} = \{f, g, h, xf, xg\} = \left\{ f, g, \frac{(y+g_1)f - (x + f_1 - g_2)g}{f_2}, xf, xg \right\}.$$

We construct the matrix

$$M_{\text{doub}} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}.$$

The columns of M_{add}, from left to right, are the reductions of $g', h', \phi((y+g_1)g' - (x + f_1 -$

$g_2)h'), xg', xh'$ modulo f', g', h'. The first two columns are therefore given by

$$a_1 = g'_0 - g_0 \qquad a_2 = h'_0 - h_0 - f_0 f_2$$
$$a_6 = g'_1 - g_1 \qquad a_7 = h'_1 - h_1 - f_1 f_2$$
$$a_{11} = g'_2 - g_2 \qquad a_{12} = h'_2 - h_2 - f_2 f_2.$$

However, observe that $h'_1 = -f_1 f_2$, so $a_7 = 2h'_1 - h_1$. The last two columns, like in the previous section, may be computed by

$$\begin{pmatrix} a_4 & a_5 \\ a_9 & a_{10} \\ a_{14} & a_{15} \end{pmatrix} = \begin{pmatrix} 0 & -f'_0 & -g'_0 \\ 1 & -f'_1 & -g'_1 \\ 0 & -f'_2 & -g'_2 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_6 & a_7 \\ a_{11} & a_{12} \end{pmatrix},$$

giving

$$a_4 = -f_0 a_6 - g_0 a_{11} \qquad a_5 = -f_0 a_7 - g_0 a_{12}$$
$$a_9 = a_1 - f_1 a_6 - g_1 a_{11} \qquad a_{10} = a_2 - f_1 a_7 - g_1 a_{12}$$
$$a_{14} = -f_2 a_6 - g_2 a_{11} \qquad a_{15} = -f_2 a_7 - g_2 a_{12}.$$

Just as multiplication by x may be seen as an endomorphism on $\frac{W^{x^2 y}}{W_D^{x^2 y}}$, so too may multiplication by y. The matrix of this endomorphism is

$$T_y = \begin{pmatrix} 0 & -g'_0 & -h'_0 \\ 0 & -g'_1 & -h'_1 \\ 1 & -g'_2 & -h'_2 \end{pmatrix}.$$

Column 3 is then computed by

$$\begin{aligned} C_3 &= \phi\left(T_y(C_1) + g_1 C_1 - T_x(C_2) - (f_1 - g_2)C_2\right) \\ &= \phi\left(T_y(C_1) + g_1 C_1 - C_5 - (f_1 - g_2)C_2\right) \end{aligned}$$

Noting that $f_1 - g_2 = g_2'$,

$$\begin{aligned} a_3 &= \phi\left(-g_0 a_6 - h_0 a_{11} + g_1 a_1 - a_5 - g_2' a_2\right) \\ a_8 &= \phi\left(-h_1 a_{11} - a_{10} - g_2' a_7\right) \\ a_{13} &= \phi\left(a_1 - g_2 a_6 - (h_2 - g_1) a_{11} - a_{15} - g_2' a_{12}\right). \end{aligned}$$

Lemma 11.3. *The matrix M_{doub} may be computed in 36M+44A.*

Proof. The coefficients of g' and h' require 11M+13A to compute as written, however, the terms $g_1' g_1$, $g_1' g_2 + g_2' g_1$, and $g_2' g_2$ all appear. Given $g_1' g_1$ and $g_2' g_2$, rather than compute $g_1' g_2 + g_2' g_1$ in 2M+1A, we may compute it in 1M+4A via Karatsuba multiplication:

$$g_1' g_2 + g_2' g_1 = (g_1' + g_2')(g_1 + g_2) - g_1' g_1 - g_1' g_2.$$

Thus the coefficients of g' and h' are obtained in 10M+16A.

The first column of M_{doub} costs 3A to compute. The second column costs 2M+6A to compute, counting doubling h_1' as 1 addition. Columns 4 and 5 each cost 6M+4A, while column 3 costs 12M+11A. □

11.3 Computing the Kernel

After computing the matrix M_{add} or M_{doub}, the addition and doubling algorithms proceed identically, so let M be one of the above matrices. If we are adding, let $M = M_{\text{add}}$ and $A = D + D'$. If we are doubling, let $M = M_{\text{doub}}$ and $A = 2D$ instead.

In Chapters 8 and 9, we found a reduced Gröbner basis for A by finding a reduced echelon basis for $\ker M$. Reducing M to its reduced row echelon form typically requires an inversion in $\mathbb{F}_q$ and this ensures that the resulting Gröbner basis for A is monic. In the following, we delay inversion until the next section. Instead, we compute a multiple of $\text{RREF}(M)$. Consequently, we obtain a pair $\{U, V\}$ of non-monic polynomials that generate I_A.

Recall that the elements of M are

$$M = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}.$$

If the first column of M is zero, then A is not a type 61 divisor, so we must abort and fall back on other methods described in this thesis. If the first column is non-zero, but $a_1 = 0$, then swap rows and relabel the elements so that $a_1 \neq 0$. We now put M into echelon form,

$$M' = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & b_1 & b_2 & b_3 & b_4 \\ 0 & 0 & b_5 & b_6 & b_7 \end{pmatrix},$$

via

$$\begin{aligned} d_1 &= a_1a_{12} - a_2a_{11} & b_1 &= a_1a_7 - a_2a_6 & b_5 &= b_1a_{13} - d_1a_8 + d_2a_3 \\ d_2 &= a_6a_{12} - a_7a_{11} & b_2 &= a_1a_8 - a_3a_6 & b_6 &= b_1a_{14} - d_1a_9 + d_2a_4 \\ & & b_3 &= a_1a_9 - a_4a_6 & b_7 &= b_1a_{15} - d_1a_{10} + d_2a_5 \\ & & b_4 &= a_1a_{10} - a_5a_6. & & \end{aligned}$$

If $b_1 = 0$ or $b_5 = 0$, then A is not of type 61, so we must abort. Otherwise, we reduce M' further to

$$M'' = \begin{pmatrix} Z & 0 & 0 & A_1 & A_2 \\ 0 & Z & 0 & B_1 & B_2 \\ 0 & 0 & Z & C_1 & C_2 \end{pmatrix},$$

where

$$\begin{aligned} Y &= a_1b_1 & e_1 &= b_3b_5 - b_2b_6 \\ Z &= Yb_5 & e_2 &= b_4b_5 - b_2b_7 \end{aligned}$$

$$A_1 = b_1(a_4b_5 - b_6a_3) - a_2e_1 \qquad B_1 = a_1e_1 \qquad C_1 = Yb_6$$
$$A_2 = b_1(a_5b_5 - b_7a_3) - a_2e_2 \qquad B_2 = a_1e_2 \qquad C_2 = Yb_7$$

This matrix M'' is $Z \cdot \mathrm{RREF}(M)$. If we have made it this far without aborting, then a_1, b_1, and b_5 are non-zero, so Z is non-zero too.

The kernel of M is $\mathrm{Span}_K\{U, V\}$, where

$$U = Zxf - C_1h - B_1g - A_1f$$
$$V = Zxg - C_2h - B_2g - A_2f.$$

Let $U_1, \ldots, U_5$ be the coefficients of x, y, x^2, xy, y^2 in U and let $V_1, \ldots, V_5$ be the coefficients of $x, \ldots, y^2$ in V. These are given explicitly by

$$U_1 = Zf_0 - C_1h_1 - B_1g_1 - A_1f_1 \qquad V_1 = Zg_0 - C_2h_1 - B_2g_1 - A_2f_1$$
$$U_2 = -C_1h_2 - B_1g_2 - A_1f_2 \qquad V_2 = -C_2h_2 - B_2g_2 - A_2f_2$$
$$U_3 = Zf_1 - A_1 \qquad V_3 = Zg_1 - A_2$$
$$U_4 = Zf_2 - B_1 \qquad V_4 = Zg_2 - B_2$$
$$U_5 = -C_1 \qquad V_5 = -C_2.$$

Note that in the computations to follow in the next section, we will not need the constant coefficients of U and V.

Lemma 11.4. *Given M, the non-constant coefficients of the polynomials U and V may be computed in 57M+32A.*

Proof. The elements b_i of the matrix M' are computed in a total of 21M+12A. The matrix M'' is then computed in an additional 18M+6A. Given M'', the coefficients U_i, V_i for $1 \leq i \leq 5$ cost a total of 18M+14A. □

11.4 Reducing

We now have two (non-monic) polynomials U and V. Let $u = \frac{U}{Z}$ and $v = \frac{V}{Z}$. The type 61 divisor A has the ideal $I_A = \langle u, v \rangle$, where u and v are the first two of three polynomials needed for the reduced Gröbner basis of I_A. We will not need the third polynomial w of I_A's Gröbner basis, but we note that by Lemma 7.22, there are polynomials $r, s \in K[C]$ and a constant $t \in K$ such that $ru + sv + tw \equiv 0 \pmod{F}$. The divisor A is typical if and only if $t \neq 0$. Moreover, $-t$ will become the coefficient of y in f'' in the ideal of the reduced divisor $I_{\overline{A}} = \langle f'', g'', h'' \rangle$.

The inverse of $-t$ will be needed, as will the inverse of Z. Let their inverses be $\zeta = \frac{1}{Z}$ and $\tau = -\frac{1}{t}$. As alluded to in the introduction to this chapter, we will compute ζ and τ using only a single inversion. However, it is more complicated than in Example 11.1. We know Z but we do not yet know $-t$. We compute

$$\begin{aligned} z_0 &= U_5^2 + Z(u_4 - v_5) & z_1 &= Z z_0 \\ z_2 &= \frac{1}{z_1} & z_3 &= Z z_2 \\ \zeta &= z_0 z_2 & \tau &= Z^2 z_3. \end{aligned}$$

Compare the value of t in Lemma 7.22 to the value of z_0 above. We confirm that $-t$ and τ are inverses:

$$\frac{1}{\tau} = \frac{1}{Z^2 z_3} = \frac{1}{Z^3 z_2} = \frac{z_1}{Z^3} = \frac{z_0}{Z^2} = \frac{U_5^2 + Z(U_4 - V_5)}{Z^2} = u_5^2 + u_4 - v_5 = -t.$$

Now let $u_1, \ldots, u_5$ and $v_1, \ldots, v_5$ be the coefficients of $x, y, \ldots, y^2$ in u and v. Compute them by

$$u_i = \zeta U_i, \quad v_i = \zeta V_i, \quad 1 \leq i \leq 5.$$

Now $I_A = \langle u, v \rangle$. Following Theorem 10.4, in order to reduce A, we find polynomials $f'' = x^2 + f_2'' y + f_1'' x + f_0''$ and $G = xy + G_3 x^2 + G_2 y + G_1 x + G_0$ such that $f''v \equiv Gu \pmod{F}$.

We would find that $G_3 = u_5$ and we would then compute the reduction of G modulo f'' by $g'' = G - G_3 f''$. We do both at once by instead computing f'' and $g'' = xy + g''_2 y + g''_1 x + g''_0$ such that $f''v \equiv (g'' + u_5 f'')u \pmod{F}$. Equating coefficients in the equation[27]

$$f''v - (g'' + u_5 f'')u - (f_2 v_5 - u_5(x + f'_2 u_5 + g_2))F = 0$$

gives

$$\begin{aligned}
f''_2 &= u_5^2 + u_4 - v_5 \\
r_0 &= u_5(f''_2 + u_4 - c_7) + u_3 - v_4 \\
r_1 &= f''_2(f''_2 - u_4) \\
g''_1 &= r_1 - u_5(u_3 + r_0) + v_3 \\
g''_2 &= -u_4 u_5 + v_4 - r_0 + \tau(u_4 r_0 - u_5 g''_1 - u_2) \\
f''_1 &= r_0 + g''_2 \\
f''_0 &= -c_7(r_1 + g''_2 u_5) + u_5(f''_2 u_3 + f''_1 u_4 - c_4 + u_2) + g''_2 u_3 + g''_1 u_4 - f''_2 v_3 - f''_1 v_4 + u_1 - v_2 \\
g''_0 &= u_5(c_3 - f''_0 - u_1 - f''_1 u_3) - g''_1 u_3 + f''_1 v_3 + v_1.
\end{aligned}$$

In deriving these formulae, it can be shown that $r_0 = f''_1 - g''_2$.

Finally, we compute $h'' = y^2 + h''_2 y + h''_1 x + h''_0$, the third polynomial in the reduced Gröbner basis of $I_{\overline{\overline{A}}} = \langle f'', g'', h'' \rangle$. Since $\overline{\overline{A}}$ is typical, h'' is given by

$$h'' = \frac{(y + g''_1)f'' - (x + f''_1 - g''_2)g''}{f''_2},$$

[27] $f_2 v_5 - u_5(x + f'_2 u_5 + g_2)$ is chosen so that the left-hand side contains no y^3 term.

though we note that $f_1'' - g_2'' = r_0$. The coefficients of h'' are given by

$$h_0'' = \tau(f_0'' g_1'' - g_0'' r_0)$$
$$h_1'' = \tau(g_1'' g_2'' - g_0'')$$
$$h_2'' = g_1'' + \tau(f_0'' - g_2'' r_0).$$

Lemma 11.5. *Given $Z, U_1, \ldots, U_5, V_1, \ldots, V_5$, the reduced Gröbner basis $\{f'', g'', h''\}$ for $I_{\overline{\overline{A}}}$ can be computed in 1I+42M+3S+40A.*

Proof. It costs 1I+5M+2S+3A to compute τ and ζ; 10M to compute $u_1, \ldots, u_5, v_1, \ldots, v_5$; 20M+1S+33A to compute f'' and g''; and 7M+4A to compute h''. □

11.5 Explicit Formulae

We collect the lemmas from the previous sections to get a statement about the total cost of adding divisors, in the typical case.

Theorem 11.6. *Let D and D' be type 31 divisors, represented by reduced Gröbner bases of their ideals I_D and $I_{D'}$.*

(i) Let $D'' = \overline{\overline{D + D'}}$. If D'' is typical, then a reduced Gröbner basis for $I_{D''}$ can be computed in 1I+111M+3S+99A.

(ii) Let $D'' = \overline{\overline{2D}}$. If D and D'' are typical, then a reduced Gröbner basis for $I_{D''}$ can be computed in 1I+135M+3S+116A.

Proof. For part (i), add the operation counts in Lemmas 11.2, 11.4, and 11.5. For part (ii), add the operation counts in Lemmas 11.3, 11.4, and 11.5. □

The formulae presented in the previous sections are also collected in Tables 11.1 and 11.2.

Table 11.1: Explicit Formulae for adding two type 31 divisors (typical case)

Addition	1I+111M+3S+99A
Input: $I_D = \langle f, g, h\rangle$, $I_{D'} = \langle f', g', h'\rangle$ $f = x^2 + f_2y + f_1x + f_0 \quad f' = x^2 + f'_2y + f'_1x + f'_0$ $g = xy + g_2y + g_1x + g_0 \quad g' = xy + g'_2y + g'_1x + g'_0$ $h = y^2 + h_2y + h_1x + h_0 \quad h' = y^2 + h'_2y + h'_1x + h'_0$ Output: $I_{\overline{D+D'}} = \langle f'', g'', h''\rangle$, $(f''_2)^{-1}$ $f'' = x^2 + f''_2y + f''_1x + f''_0$ $g'' = xy + g''_2y + g''_1x + g''_0$ $h'' = y^2 + h''_2y + h''_1x + h''_0$	
Compute elements a_i of M_{add}	12M+17A
$a_1 = f_0 - f'_0 \quad a_2 = g_0 - g'_0 \quad a_3 = h_0 - h'_0$ $a_6 = f_1 - f'_1 \quad a_7 = g_1 - g'_1 \quad a_8 = h_1 - h'_1$ $a_{11} = f_2 - f'_2 \quad a_{12} = g_2 - g'_2 \quad a_{13} = h_2 - h'_2$ $a_4 = -f'_0a_6 - g'_0a_{11} \qquad a_5 = -f'_0a_7 - g'_0a_{12}$ $a_9 = a_1 - f'_1a_6 - g'_1a_{11} \quad a_{10} = a_2 - f'_1a_7 - g'_1a_{12}$ $a_{14} = -f'_2a_6 - g'_2a_{11} \qquad a_{15} = -f'_2a_7 - g'_2a_{12}$ If a_1, a_6, a_{11} are all zero, then abort. If $a_1 = 0$ but a_6 or a_{11} is non-zero, then swap rows so that $a_1 \neq 0$.	
Compute row echelon form M'_{add} of M_{add}	21M+12A
$d_1 = a_1a_{12} - a_2a_{11} \quad d_2 = a_6a_{12} - a_7a_{11}$ $b_1 = a_1a_7 - a_2a_6 \quad b_5 = b_1a_{13} - d_1a_8 + d_2a_3$ $b_2 = a_1a_8 - a_3a_6 \quad b_6 = b_1a_{14} - d_1a_9 + d_2a_4$ $b_3 = a_1a_9 - a_4a_6 \quad b_7 = b_1a_{15} - d_1a_{10} + d_2a_5$ $b_4 = a_1a_{10} - a_5a_6$	

If $b_1 = 0$ or $b_5 = 0$, then abort.	

Compute $Z \cdot \mathrm{RREF}\,(M_{\mathrm{add}})$	18M+6A
$Y = a_1 b_1 \quad e_1 = b_3 b_5 - b_2 b_6$ $Z = Y b_5 \quad e_2 = b_4 b_5 - b_2 b_7$ $A_1 = b_1(a_4 b_5 - b_6 a_3) - a_2 e_1 \quad B_1 = a_1 e_1 \quad C_1 = Y b_6$ $A_2 = b_1(a_5 b_5 - b_7 a_3) - a_2 e_2 \quad B_2 = a_1 e_2 \quad C_2 = Y b_7$	

Compute $\ker M_{\mathrm{add}}$	18M+14A
$U1 = Z f_0 - C_1 h_1 - B_1 g_1 - A_1 f_1 \quad V1 = Z g_0 - C_2 h_1 - B_2 g_1 - A_2 f_1$ $U2 = -C_1 h_2 - B_1 g_2 - A_1 f_2 \quad V2 = -C_2 h_2 - B_2 g_2 - A_2 f_2$ $U3 = Z f_1 - A_1 \quad V3 = Z g_1 - A_2$ $U4 = Z f_2 - B_1 \quad V4 = Z g_2 - B_2$ $U5 = -C_1 \quad V5 = -C_2.$	

Compute ζ, τ	1I+5M+2S+3A
$z_0 = U_5^2 + Z(u_4 - v_5) \quad z_1 = Z z_0$ $z_2 = \dfrac{1}{z_1} \quad z_3 = Z z_2$ $\zeta = z_0 z_2 \quad \tau = Z^2 z_3$ If $z_0 = 0$, then abort.	

Compute $u_1, \ldots, u_5, v_1, \ldots, v_5$	10M
$u_1 = \zeta U_1 \quad u_4 = \zeta U_4 \quad v_1 = \zeta V_1 \quad v_4 = \zeta V_4$ $u_2 = \zeta U_2 \quad u_5 = \zeta U_5 \quad v_2 = \zeta V_2 \quad v_5 = \zeta V_5$ $u_3 = \zeta U_3 \quad v_3 = \zeta V_3$	

Compute f'', g'', h''	27M+1S+37A
$f_2'' = u_5^2 + u_4 - v_5$ $r_0 = u_5(f_2'' + u_4 - c_7) + u_3 - v_4$ $r_1 = f_2''(f_2'' - u_4)$ $g_1'' = r_1 - u_5(u_3 + r_0) + v_3$ $g_2'' = -u_4 u_5 + v_4 - r_0 + \tau(u_4 r_0 - u_5 g_1'' - u_2)$	

$f_1'' = r_0 + g_2''$ $f_0'' = -c_7(r_1 + g_2''u_5) + u_5(f_2''u_3 + f_1''u_4 - c_4 + u_2)$ $\quad + g_2''u_3 + g_1''u_4 - f_2''v_3 - f_1''v_4 + u_1 - v_2$ $g_0'' = u_5(c_3 - f_0'' - u_1 - f_1''u_3) - g_1''u_3 + f_1''v_3 + v_1$ $h_0'' = \tau(f_0''g_1'' - g_0''r_0)$ $h_1'' = \tau(g_1''g_2'' - g_0'')$ $h_2'' = g_1'' + \tau(f_0'' - g_2''r_0)$	
Output $f_0'', f_1'', f_2'', g_0'', g_1'', g_2'', h_0'', h_1'', h_2''$, and $(f_2'')^{-1} = \tau$	

Table 11.2: Explicit Formulae for doubling type 31 divisors (typical case)

Doubling Input: $I_D = \langle f, g, h\rangle$, ϕ $f = x^2 + f_2y + f_1x + f_0 \quad f_2 \neq 0$ $g = xy + g_2y + g_1x + g_0 \quad \phi = \frac{1}{f_2}$ $h = y^2 + h_2y + h_1x + h_0$ Output: $I_{\overline{2D}} = \langle f'', g'', h''\rangle$, $(f_2'')^{-1}$ $f'' = x^2 + f_2''y + f_1''x + f_0''$ $g'' = xy + g_2''y + g_1''x + g_0''$ $h'' = y^2 + h_2''y + h_1''x + h_0''$	1I+135M+3S+116A
Compute polynomials g' and h' such that $fh' \equiv gg' \pmod F$	10M+16A
$h_3' = f_2$ $g_2' = f_1 - g_2$ $k_0 = g_2g_2'$ $h_2' = \phi(k_0 - f_0)$ $g_1' = f_2(f_2 - c_7) + h_2' - g_1$ $k_1 = g_1g_1'$ $h_1' = -f_1f_2$	

$g'_0 = h'_2 f_1 + f_2(h'_1 - c_4)$ $\quad - (g_1 + g_2)(g'_1 + g'_2) + k_0 + k_1 - g_0$ $h'_0 = f_2(c_3 - f_0) - h'_1 f_1 + k_1$	
Compute elements a_i of M_{doub}	26M+28A
$a_1 = g'_0 - g_0 \quad a_2 = h'_0 - h_0 - f_0 f_2$ $a_6 = g'_1 - g_1 \quad a_7 = h'_1 - h_1 - f_1 f_2$ $a_{11} = g'_2 - g_2 \quad a_{12} = h'_2 - h_2 - f_2 f_2$ $a_4 = -f_0 a_6 - g_0 a_{11} \qquad a_5 = -f_0 a_7 - g_0 a_{12}$ $a_9 = a_1 - f_1 a_6 - g_1 a_{11} \quad a_{10} = a_2 - f_1 a_7 - g_1 a_{12}$ $a_{14} = -f_2 a_6 - g_2 a_{11} \qquad a_{15} = -f_2 a_7 - g_2 a_{12}$ $a_3 = \phi\,(-g_0 a_6 - h_0 a_{11} + g_1 a_1 - a_5 - g'_2 a_2)$ $a_8 = \phi\,(-h_1 a_{11} - a_{10} - g'_2 a_7)$ $a_{13} = \phi\,(a_1 - g_2 a_6 - (h_2 - g_1) a_{11} - a_{15} - g'_2 a_{12})$ If a_1, a_6, a_{11} are all zero, then abort. If $a_1 = 0$ but a_6 or a_{11} is non-zero, then swap rows so that $a_1 \neq 0$.	
Compute row echelon form M'_{doub} of M_{doub}	21M+12A
$d_1 = a_1 a_{12} - a_2 a_{11} \quad d_2 = a_6 a_{12} - a_7 a_{11}$ $b_1 = a_1 a_7 - a_2 a_6 \quad b_5 = b_1 a_{13} - d_1 a_8 + d_2 a_3$ $b_2 = a_1 a_8 - a_3 a_6 \quad b_6 = b_1 a_{14} - d_1 a_9 + d_2 a_4$ $b_3 = a_1 a_9 - a_4 a_6 \quad b_7 = b_1 a_{15} - d_1 a_{10} + d_2 a_5$ $b_4 = a_1 a_{10} - a_5 a_6$ If $b_1 = 0$ or $b_5 = 0$, then abort.	
Compute $Z \cdot \text{RREF}\,(M_{\text{doub}})$	18M+6A
$Y = a_1 b_1 \quad e_1 = b_3 b_5 - b_2 b_6$ $Z = Y b_5 \quad e_2 = b_4 b_5 - b_2 b_7$	

$A_1 = b_1(a_4b_5 - b_6a_3) - a_2e_1 \quad B_1 = a_1e_1 \quad C_1 = Yb_6$ $A_2 = b_1(a_5b_5 - b_7a_3) - a_2e_2 \quad B_2 = a_1e_2 \quad C_2 = Yb_7$	

Compute $\ker M_{\text{doub}}$	18M+14A
$U1 = Zf_0 - C_1h_1 - B_1g_1 - A_1f_1 \quad V1 = Zg_0 - C_2h_1 - B_2g_1 - A_2f_1$ $U2 = -C_1h_2 - B_1g_2 - A_1f_2 \quad V2 = -C_2h_2 - B_2g_2 - A_2f_2$ $U3 = Zf_1 - A_1 \quad V3 = Zg_1 - A_2$ $U4 = Zf_2 - B_1 \quad V4 = Zg_2 - B_2$ $U5 = -C_1 \quad V5 = -C_2.$	

Compute ζ, τ	1I+5M+2S+3A
$z_0 = U_5^2 + Z(u_4 - v_5) \quad z_1 = Zz_0$ $z_2 = \dfrac{1}{z_1} \quad z_3 = Zz_2$ $\zeta = z_0z_2 \quad \tau = Z^2z_3$ If $z_0 = 0$, then abort.	

Compute $u_1, \ldots, u_5, v_1, \ldots, v_5$	10M
$u_1 = \zeta U_1 \quad u_4 = \zeta U_4 \quad v_1 = \zeta V_1 \quad v_4 = \zeta V_4$ $u_2 = \zeta U_2 \quad u_5 = \zeta U_5 \quad v_2 = \zeta V_2 \quad v_5 = \zeta V_5$ $u_3 = \zeta U_3 \quad v_3 = \zeta V_3$	

Compute f'', g'', h''	27M+1S+37A
$f_2'' = u_5^2 + u_4 - v_5$ $r_0 = u_5(f_2'' + u_4 - c_7) + u_3 - v_4$ $r_1 = f_2''(f_2'' - u_4)$ $g_1'' = r_1 - u_5(u_3 + r_0) + v_3$ $g_2'' = -u_4u_5 + v_4 - r_0 + \tau(u_4r_0 - u_5g_1'' - u_2)$ $f_1'' = r_0 + g_2''$ $f_0'' = -c_7(r_1 + g_2''u_5) + u_5(f_2''u_3 + f_1''u_4 - c_4 + u_2)$ $\quad + g_2''u_3 + g_1''u_4 - f_2''v_3 - f_1''v_4 + u_1 - v_2$ $g_0'' = u_5(c_3 - f_0'' - u_1 - f_1''u_3) - g_1''u_3 + f_1''v_3 + v_1$ $h_0'' = \tau(f_0''g_1'' - g_0''r_0)$	

$h_1'' = \tau(g_1''g_2'' - g_0'')$ $h_2'' = g_1'' + \tau(f_0'' - g_2''r_0)$	
Output $f_0'', f_1'', f_2'', g_0'', g_1'', g_2'', h_0'', h_1'', h_2''$, and $(f_2'')^{-1} = \tau$	

12 Implementation and Testing

An implementation in Sage of $C_{3,4}$ curve divisor class group arithmetic is available at `https://github.com/emmacneil/c34-curves` [30]. This implementation uses the optimized explicit formulae in Tables 11.1 and 11.2 to add and double divisors in the typical cases, as described in Chapter 11. It also uses explicit formulae derived from the algorithms in Chapters 8, 9, and 10 to handle the other cases. Specifically, it implements the following:

- An optimized addition subroutine `fast_add_31_31_high_char` implementing the formulae in Table 11.1.
- An optimized addition subroutine `fast_add_31_31` similar to the above, but does not assume the curve coefficients c_5, c_6, and c_8 are zero.
- Addition subroutines for every non-zero pair of reduced divisor types (11, 21, 22, 31). For example, `add_11_11`, `add_21_11`, etc.
- An optimized doubling subroutine `fast_double_31_high_char` implementing the formulae in Table 11.2.
- An optimized doubling subroutine `fast_double_31` similar to the above, but does not assume the curve coefficients c_5, c_6, and c_8 are zero.
- Doubling subroutines for every non-zero reduced divisor type (11, 21, 22, 31). For example, `double_11`, `double_21`, etc.
- A subroutine `triple_11` for tripling type 11 divisors.
- Reduction subroutines for every unreduced divisor type (all types other than 0, 11, 21, 22, 31). For example, `reduce_32`, `reduce_33`, etc.
- Flipping subroutines for every non-zero divisor type in Table 7.1, e.g. `flip_11`, `flip_21`, etc.

When adding two divisors, the addition code checks whether the two input divisors are both of type 31. If so, it attempts to add them with the `fast_add_31_31_high_char` or `fast_add_31_31` subroutine, depending on the curve coefficients. If the input divisors are not of type 31, are non-disjoint, or their sum would be atypical, the optimized subroutine raises and error and the calling code falls back on a slower subroutine instead. The doubling code follows an analogous sequence of steps.

In addition to the above subroutines, there is also implemented code to:

- Generate random $C_{3,4}$ curves.
- Generate random divisors of any type in Table 7.1.
- Compute the formal sum of points making up a divisor.

These methods are implemented using Sage's provided polynomial arithmetic, ideal arithmetic, and geometry libraries.

The implementation defines `C34Curve` and `C34CurveDivisor` classes from which to instantiate objects. A `C34Curve` may be constructed by specifying a base field and the curve coefficients $c_0, \ldots, c_8$, as in Equation 2.13. Divisors may be instantiated via methods of the `C34Curve` class either randomly or by specifying its points or its ideal's reduced Gröbner basis. Operators `+` and `-` are overloaded to allow for addition, negation, and subtraction of divisors. The `*` operator is overloaded to allow for scalar multiplication of divisors by integers.

```
sage: C = C34Curve(GF(41), [1,2,3,4,5,6,7,8,9]); C
C34 curve defined by y^3 + x^4 + 9*x*y^2 + 8*x^2*y + 7*x^3 + 6*y^2
+ 5*x*y + 4*x^2 + 3*y + 2*x + 1 over Finite Field of size 41
sage: C = C.short_form(); C
C34 curve defined by y^3 + x^4 - 19*x^2*y + 13*x*y - 7*x^2 - 18*y
+ 4*x - 20 over Finite Field of size 41
```

```
sage: D1 = C.random_divisor(); D1
<x^2 - 8*y - 2*x - 18, x*y - 19*y + 15*x - 14, y^2 - 18*y - 2*x + 4>
sage: D2 = C.random_divisor(); D2
<x^2 - 13*y + 16*x - 19, x*y + 19*y - 9*x + 5, y^2 + 7*y - 18*x - 8>
sage: D1 + D2
<x^2 + 11*y - 7*x - 10, x*y + 19*y + 17*x + 14, y^2 + 20*y + 2*x - 1>
sage: D1 - D2
<x^2 + 14*x + 4, x*y + 5*y - 3*x - 15, y^2 + 5*y + 6*x - 11>
sage: 777*D1
<x^2 + 20*y - 16*x + 4, x*y + 4*y + 8*x + 10, y^2 + 4*y - 3*x - 13>
```

All of the divisors in the above example are typical type 31 divisors. The arithmetic is also fully implemented for reduced atypical divisors as well.

```
sage: D1 = C.random_divisor_of_type(21); D1
<y - 5, x^2 - 13*x - 8>
sage: D2 = C.random_divisor_of_type(22); D2
<x - 4, y^2 - 20*y + 7>
sage: D1 + D2
<x^2 + 9*y + 13*x - 11, x*y + 17*y - 9*x - 7, y^2 + 11*y + 2*x + 17>
sage: -D2
<x - 4, y + 20>
```

More complete documentation is available at [30].

12.1 Testing

The formulae describing the typical cases in Chapter 11 and the remaining formulae for the atypical cases found at [30] were tested via unit testing and random testing. Producing

test cases requires generating random divisors on curves. We describe below the testing methodology, and in Section 12.2 we describe how random divisors were generated.

Unit Testing

The code implementing the $C_{3,4}$ curve divisor arithmetic is divided up into several subroutines. For every pair of non-zero reduced divisor types (11, 21, 22, and 31), there is one subroutine, e.g. `add_11_11`, `add_21_11`, `add_21_21`, etc. For every non-zero reduced divisor type, there is a doubling subroutine, e.g. `double_11`, `double_21`, etc. There are also flipping subroutines for every non-zero divisor type, reduced or not, and reduction subroutines for every unreduced divisor type.

Addition subroutines consist of several conditional branches. For each possible type that the input divisors' least common mulitple may take on, there is a conditional branch. These branches also correspond to the different possiblities for the form (i.e. positions of the pivot elements) of the reduced row echelon form of M_{add}, the matrix whose construction was described in Chapter 8. For example, when adding a type 21 divisor D_1 to a type 11 divisor D_2, their least common multiple $L = \text{lcm}(D_1, D_2)$ may be of type 31, 32, or 21. Consequently, there are 3 branches in `add_21_11` corresponding to each of these possibilities. The case where L is of type 21 (this happens when $D_2 < D_1$) further breaks down into the case where $D_1 = 2D_2$, in which case a tripling subroutine must be called, and the case where $D_1 \neq 2D_2$, in which case doubling is necessary.

Doubling subroutines also consist of several different conditional branches. As was the case with addition, these branches correspond to the different possible positions of the pivot elements in $\text{RREF}(M_{\text{doub}})$.

Unit tests were written to test every branch of each addition and doubling subroutine. For each subroutine, the most commonly executed branch is tested several times using curves over each of the finite fields $\mathbb{F}_2$, $\mathbb{F}_{2^4}$, $\mathbb{F}_3$, $\mathbb{F}_{3^3}$, $\mathbb{F}_{31}$, $\mathbb{F}_{31^2}$, and $\mathbb{F}_{1009}$. The other branches are tested once, usually over $\mathbb{F}_{997}$ or $\mathbb{F}_{1009}$. The reason for only testing once is due to the difficulty

in constructing instances of the atypical cases. These rare cases get tested further during random testing, discussed in the next subsection.

These particular finite fields were chosen to test the code's correctness over fields of small order, where degenerate cases are more likely to be encountered; in characteristics 2 and 3, which were ignored by previous authors; and over finite fields of non-prime order. Over a very small field such as $\mathbb{F}_2$, it is possible that unit tests might accidentally pass even if the formulae being tested are incorrect. The fields $\mathbb{F}_{31^2}$, $\mathbb{F}_{997}$, and $\mathbb{F}_{1009}$ were chosen as they are large enough that this is unlikely to happen.

Unit tests were also written for each reduction and flipping subroutine. These subroutines are tested on curves over each of the fields $\mathbb{F}_2$, $\mathbb{F}_{2^4}$, $\mathbb{F}_3$, $\mathbb{F}_{3^3}$, $\mathbb{F}_{31}$, $\mathbb{F}_{31^2}$, and $\mathbb{F}_{1009}$. Flipping subroutines for semitypical divisors (types 31, 41, 51, and 61, i.e. those divisors whose ideals are generated by three polynomials $\langle f, g, h\rangle$), have three branches, one for each of the cases $\langle f, g\rangle = \langle f, g, h\rangle$, $\langle f, g\rangle \neq \langle f, g, h\rangle = \langle f, h\rangle$, and $\langle f, g\rangle \neq \langle f, g, h\rangle \neq \langle f, h\rangle$. Each of these cases are tested over each of the above fields.

Random Testing

Unit testing was useful in detecting errors while putting the explicit formulae into code or when making modifications to that code. However, unit testing alone is not sufficient to test the correctness of the formulae. It is not enough to test subroutines over a few select fields and curves. Random testing was also done to ensure correctness. That is, many hundreds of thousands of random divisors were added, on random curves over many base fields of small order. The results of the additions were compared against the results produced by Sage's (slower) provided ideal arithmetic.

More specifically, for every prime power $2 \leq q \leq 31$, 100 random $C_{3,4}$ curves were generated. For each such curve C, 100 pairs of random reduced divisors (D_1, D_2) were generated. These divisors may be of any type representing a reduced divisor (types 0, 11, 21, 22, and 31). See Section 12.2 for details on how these were generated. For each pair, we

add $D_3 := D_1 + D_2$. To test whether the addition was correctly computed, we construct the ideals I_{D_1} and I_{D_2} using Sage's built-in ring ideal classes. We multiply $J := I_{D_1} I_{D_2}$. The test passes if the reduced Gröbner basis of J computed by Sage matches the reduced Gröbner basis we computed for D_3.

Doubling is tested analogously. It proceeds as above, except for each trial we need only generate a single random reduced divisor, D_1, rather than a pair. Then we compute $D_2 := 2D_1$, $J := I_{D_1}^2$, and compare the reduced Gröbner bases of J and D_2.

12.2 Random divisor generation

In order to generate test cases, it is necessary to be able to generate random divisors on curves. Once one is able to generate reduced divisors, it is straightforward to extend the method to generate unreduced divisors of any desired type as well. We describe here how these divisors were generated. Let C be a $C_{3,4}$ curve, defined by a polynomial F. Recall that if D is a reduced divisor, then the minimal polynomial in I_D has leading monomial x^2 or smaller (see Theorem 7.10 and Table 7.1). The general idea is to randomly choose a polynomial f with $\mathrm{LM}(f) \leq x^2$, then construct a divisor D for which the minimal polynomial of I_D is f.

The details are as follows. Choose random coefficients $f_0, f_1, f_2, f_3 \in K$ and set $f := f_3x^2 + f_2y + f_1x + f_0$. If f is constant, then return the zero divisor. Otherwise, the rest proceeds differently depending on whether the leading monomial of f is x^2, y, or x. We will describe the most difficult case, when $\mathrm{LM}(f) = x^2$. In this case, we are about to construct a type 31 divisor, D. the other cases are handled similarly, but are greatly simplified by not needing to consider whether the divisor will be typical or atypical nor needing to generate a third polynomial.

Suppose $f_2 \neq 0$. Then D will be a typical type 31 divisor. We will find polynomials $g, h \in K[C]$ such that $I_D = \langle f, g, h \rangle$ is the ideal of a type 31 divisor. Since $\langle f, g, h \rangle = \langle kf, g, h \rangle$ for any scalar $k \in K$, we simply set $f_2 := 1$, so that $f := f_3x^2 + y + f_1x + f_0$. Set

$\overline{F}(x) = F(x, -f_3x^2 - f_1x - f_0) \in K[x]$. Geometrically, f is a parabola that intersects C at 6 finite points. The x-coordinates of these points are the roots of $\overline{F}$.

We now construct a degree 3 polynomial $g \in K[x]$ that divides $\overline{F}$. This is done by factoring $\overline{F}$ and choosing a random subset of its divisors whose product is of degree 3. If no such g exists (perhaps $\overline{F}$ is irreducible or has only quadratic factors), then we must restart and generate a new polynomial f.

Finally, we make f monic by setting $f := -\frac{1}{f_3}f$, reduce g modulo f by setting $g := g \pmod f$, then compute h via

$$h = \frac{(y + g_1)f - (x + f_1 - g_2)g}{f_2}$$

and return $I_D = \langle f, g, h\rangle$.

Suppose instead $f_2 = 0$. Set $f_3 := 1$, so that $f = x^2 + f_1x + f_0$. Then D will be an atypical type 31 divisor. Every atypical type 31 divisor arises as the sum of a type 11 with a type 22 divisor. Thus, we must check if f factors into linear terms $f = (x + x_1)(x + x_2)$. If not, restart and generate a new polynomial f. Otherwise, generate a type 11 divisor with minimal polynomial $f = x + x_1$ and a type 22 divisor with minimal polynomial $f = x + x_2$.

If $\mathrm{LM}(f) = y$, then D will be of type 21. If $\mathrm{LM}(f) = x$, then D will be of type 11 or 22. Since type 11 and type 22 divisors are in bijection with one another, simply generate a type 11 divisor, then randomly decide whether to flip it afterwards. Generating type 11 and type 21 divisors is similar to generating type 31 divisors: Reduce the curve equation F modulo f to get a univariate polynomial $\overline{F}$, randomly generate a degree $\deg D$ factor g of $\overline{F}$, and return $I_D = \langle f, g \pmod f\rangle$.

Following this method allows one to generate random reduced divisors in such a way that no reduced divisor is left out. Every reduced divisor will occur with probability greater than 0. However, reduced divisors will not occur with uniform probability. If there are many divisors with the same minimal polynomial, each one will occur with lesser frequency than

a divisor that shares a minimal polynomial only with its flip.

The method above allows one to randomly generate a reduced divisor. One can generate a random reduced divisor of a chosen type (0, 11, 21, 22, or 31) by forcing certain coefficients of the random polynomial f to be 0 or 1. It is then possible to generate a random unreduced divisor of any desired type, including unreduced divisors, by first generating a *reduced* divisor A, then finding a divisor D of the desired type whose flip is $\overline{D} = A$.

Briefly, it may be done as follows. To generate a random divisor of type T:

- Let T_A be the type of the flip of a divisor of type T (see Table 7.4).
- Generate a reduced divisor A of type T_A.
- Let m be the leading monomial of the minimum polynomial in the ideal of a divisor of type T_D (see Table 7.1).
- Choose a random polynomial u in I_A with $\mathrm{LM}(u) = m$.
- Compute $I_D = u : I_A$. In a Sage implementation, this can be done using Sage's built-in ideal arithmetic, for example.
- Return D.

12.3 Comparison to State-of-the-art

We now compare the operation counts in the explicit formulae derived in Chapter 11 to the counts of Abu Salem and Khuri-Makdisi in [40] and [26]. These counts are given in Table 12.1. Abu Salem and Khuri-Makdisi reported only the number of inversion and multiplications needed by their formulae, counting squarings as multiplications, and reporting 2I+98M/2I+110M for addition/doubling. In Table 12.1, squarings have been separated out from multiplications and addition counts for [26] have been provided by me.

The explicit formulae produced by this thesis use considerably fewer additions, but considerably more multiplications. More importantly, they use one fewer inversion. Whether or

Table 12.1: Comparison to state-of-the-art

	Addition				Doubling			
Author	I	M	S	A	I	M	S	A
Abu Salem/Khuri-Makdisi [26, 40]	2	97	1	132	2	107	3	151
This thesis	1	111	3	99	1	135	3	116

not the formulae in this thesis are an improvement over the state-of-the-art depends on the cost of computing an inverse versus a product. While it is claimed in [40] that an inversion costs approximately as much as 3 to 10 multiplications, [9] claims that the cost may range anywhere from 4 to 80 multiplications, or higher on embedded devices, while [17] assumes a cost of 80 multiplications. I have elected to create Sage implementations of both sets of formulae, those from Chapter 11 and those from [40] and [26], to compare the number of additions and doublings each can compute in a unit of time. These implementations are available at [30].

In order to do the fairest comparison between the two, the following steps were taken. Let p be the prime number $p = 2^{28} - 57 = 268,435,399$ and let C be the $C_{3,4}$ curve over $\mathbb{F}_p$ defined by

$$y^3 + x^4 - 114167898x^2y - 126472665xy - 20302892x^2 + 56254855y + 63973501x + 65135542.$$

The coefficients of this curve were chosen at random. The prime p was chosen as it is the largest prime number less than 2^{28}, a choice of prime corresponding to a real application where this $C_{3,4}$ curve arithmetic might be used. (In [46], Sutherland computes Sato-Tate distributions on genus 3 ramified hyperelliptic curves over primes $p < 2^{28}$.) Let D_1 and D_2

be the divisors

$$D_1 = \left\langle \begin{array}{r} x^2 - 58199944y + 26531881x - 32437186 \\ xy - 121857018y + 87572390x - 13153072 \\ y^2 + 9642394y - 58287154x + 13450942 \end{array} \right\rangle$$

$$D_2 = \left\langle \begin{array}{r} x^2 - 91512999y - 67449632x + 64403020 \\ xy - 92024952y - 121602716x + 97210118 \\ y^2 + 43402044y - 11043566x - 21890587 \end{array} \right\rangle$$

chosen at random, and compute the Fibonacci-like sequence

$$D_{i+2} = D_{i+1} + D_i, \quad i > 0.$$

Running a Sage script to compute this sequence on a server, the implementation of the formulae from Chapter 11 was able to compute the first 6,532,301 elements of this sequence in 10 minutes. The implementation of the formulae of Abu Salem and Khuri-Makdisi was able to compute the first 5,514,964 in the same period of time. This represents a speed-up of approximately 18.4%. None of the divisors encountered in this sequence were atypical, nor was there ever a case where $D_{i+1} = D_i$ (in which case we would be doubling, not adding).

To compare doubling, let D_1 be as above, and repeatedly double D_1, computing the sequence

$$D_{i+1} = 2D_i, \quad i > 0.$$

Note that the D_2 produced by this sequence is not the same as the D_2 from above. The implementation of the formulae from Chapter 11 was able to compute the first 6,156,174 elements of this sequence in 10 minutes. The implementation of the formulae of Abu Salem and Khuri-Makdisi was able to compute the first 5,249,322 in the same period of time. This represents a speed-up of approximately 17.3%. None of the divisors encountered in this sequence were atypical.

These tests were run on a server with an 80 core 2.8GHz Intel Xeon E7-8891 and 256GB of

RAM, running the operating system Red Hat Enterprise Linux 7. The initial results suggest an approximate speed-up of 17%–18%. However, there has been some variability in the results. Re-running the same tests (same sequences, curves, initial divisors, and computer) at different times has produced varying results, recording speed-ups anywhere between 15% and 27%. The variability may be a result of other users on the server.

The tests were repeated in a more controlled environment, on an Aspire E 15 laptop computer with a 4 core 2.5GHz Intel i5-7200U processor and 8GB of RAM, running the operating system Ubuntu 18.04.3 LTS. This time, the tests were performed over several curves over finite fields of order approximately 2^{28}. The results are recorded in Table 12.2. In each trial, a different prime number p is chosen; a curve C over the field $\mathbb{F}_p$ and divisors D and D' on C are chosen; and the sequences described above are computed. Table 12.2 records how many terms in the sequence each algorithm was able to compute in 10 minutes. Since random curve and divisor generation is slow, timing began only after the initial curve and divisors were generated. The result of the benchmarking suggests a speed-up factor of approximately 13.1% for addition and 11.1% for doubling over the previous state-of-the-art.

12.4 Summary of Operation Costs

Here we list all divisor arithmetic subroutines implemented in Sage at [30], beginning with addition subroutines. There is one addition subroutine for every pair of non-zero reduced divisor types (11, 21, 21, and 31), as well as the two optimized subroutines, `fast_add_31_31_high_char` and `fast_add_31_31`, mentioned earlier. The unoptimized subroutines branch conditionally on the type of the divisor $L = \operatorname{lcm}(D, D')$, where D and D' are the input divisors. Operation counts are given in Table 12.3 only for those branches where D and D' are disjoint (when $\deg L = \deg D + \deg D'$ and $\gcd(D, D') = 0$). Due to the complexity involved in performing operation counts for non-disjoint cases, this analysis has not been done — these cases involve possibly several recursive addition calls, leading to a small combinatorial explosion in the number of cases requiring consideration.

Table 12.2: Efficiency gains over several curves and finite fields

Trial	p	Additions			Doublings		
		MacNeil	AS/K-M	Adv.	MacNeil	AS/K-M	Adv.
1	$2^{28}+3$	5534670	4935428	12.1%	5325050	4788638	11.2%
2	$2^{28}+7$	5530075	4876185	13.4%	5294165	4735269	11.8%
3	$2^{28}+37$	5577575	4910233	13.6%	5323416	4790268	11.1%
4	$2^{28}+67$	5565365	4928041	12.9%	5367155	4817074	11.4%
5	$2^{28}+81$	5584512	4975821	12.2%	5341898	4815965	10.9%
6	$2^{28}+105$	5596761	4984413	12.3%	5382306	4834865	11.3%
7	$2^{28}+121$	5558259	4938502	12.5%	5344099	4793423	11.5%
8	$2^{28}+123$	5569422	4946311	12.6%	5337804	4801917	11.2%
9	$2^{28}+141$	5526751	4846004	14.0%	5255001	4724906	11.2%
10	$2^{28}+175$	5570109	4934148	12.9%	5346967	4801362	11.4%
11	$2^{28}+183$	5578262	4936982	13.0%	5307731	4790802	10.8%
12	$2^{28}+193$	5577656	4859805	14.8%	5273625	4743333	11.2%
13	$2^{28}+213$	5449639	4824727	13.0%	5214041	4675573	11.5%
14	$2^{28}+241$	5546722	4925567	12.6%	5302578	4793662	10.6%
15	$2^{28}+255$	5590669	4939578	13.2%	5287018	4811569	9.9%
16	$2^{28}+267$	5541137	4896662	13.2%	5296219	4753907	11.4%
17	$2^{28}+291$	5543591	4935222	12.3%	5320722	4783549	11.2%
18	$2^{28}+295$	5590081	4938668	13.2%	5358327	4833331	10.9%
19	$2^{28}+301$	5558373	4796069	15.9%	5332765	4801876	11.1%
20	$2^{28}+357$	5560988	4939542	12.6%	5321792	4805944	10.7%
	Total:	111150617	98267908	13.1%	106332679	95697233	11.1%

It is important to note that all counts in Table 12.3 also include the cost of reducing $D + D'$ afterwards. When $D + D'$ is semi-typical, the operation count differs depending on whether $D + D'$ is typical or not. In the right-most column 't' denotes the typical case, and 'a' denotes the atypical case. When $D + D'$ is atypical, the sum is reduced by flipping twice using the appropriate flip subroutines, rather than calling a reduction subroutine. As such, those atypical cases are more costly than the typical ones.

The computational cost of adding two divisors

Table 12.3: Operation counts for addition subroutines

Subroutine	Operation count				Type(L)
	I	M	S	A	
`add_11_11`	1	3	0	4	21
`add_11_11`	0	1	0	3	22

add_21_11	1	13	0	14	31
add_21_11	0	12	0	17	32
add_21_21	2	68	1	58	41-t
add_21_21	2	77	1	68	41-a
add_21_21	1	27	0	19	42
add_21_21	1	39	0	32	43
add_21_21	0	12	0	9	44
add_21_22	2	40	1	41	41-t
add_21_22	2	61	1	71	41-a
add_21_22	0	2	0	2	42
add_22_11	1	5	0	5	31
add_22_11	0	1	0	3	33
add_22_22	1	11	0	17	43
add_31_11	2	43	1	49	41-t
add_31_11	2	64	1	79	41-a
add_31_11	0	6	0	10	42
add_31_11	1	16	0	32	43
add_31_21	2	80	1	77	51-t
add_31_21	2	89	1	96	51-a
add_31_21	1	35	1	33	52
add_31_21	1	57	1	51	53
add_31_21	1	43	1	41	54
add_31_22	2	69	0	64	51-t
add_31_22	2	78	0	83	51-a
add_31_22	1	24	0	20	52
add_31_22	1	46	0	38	53
add_31_22	1	36	0	29	54
fast_add_31_31_high_char	1	111	3	99	61-t
fast_add_31_31	1	114	2	102	61-t
add_31_31	2	154	0	171	61-a
add_31_31	1	69	0	54	62
add_31_31	1	85	0	67	63
add_31_31	1	92	0	79	64

`add_31_31`	0	32	0	28	65

There are fewer cases to consider when doubling divisors. We give operation counts in Table 12.4 for each doubling subroutine, including the optimized subroutines `fast_double_31_high_char` and `fast_double_31`. As before, the cost of reducing the doubled divisor is also included in the table. For `double_31`, the operation counts assume an unfavorable case where $\langle f, g\rangle \neq \langle f, g, h\rangle$.

Table 12.4: Operation counts for addition subroutines

Subroutine	Operation count I	M	S	A	Type(D_1)
`double_11`	1	15	1	20	21
`double_11`	0	8	1	13	22
`double_21`	2	86	1	85	41-t
`double_21`	2	107	1	115	41-a
`double_21`	1	50	0	47	42
`double_21`	1	60	0	60	43
`double_21`	0	7	0	12	44
`double_22`	1	22	0	22	42
`double_22`	1	25	0	29	43
`fast_double_31_high_char`	1	135	3	116	61
`fast_double_31`	1	145	2	126	61
`double_31`	2	188	0	164	61-t
`double_31`	2	209	0	218	61-a
`double_31`	1	124	0	101	62
`double_31`	1	140	0	114	63
`double_31`	1	120	0	116	64
`double_31`	0	69	0	66	65

Operation counts for reduction subroutines are given in Table 12.5. Reduction subroutines are not implemented for atypical semi-typical divisors. Reducing those divisors is handled instead by flipping twice using the flip subroutines.

Table 12.5: Operation counts for reduction subroutines

Subroutine	Operation count I	M	S	A
`reduce_32`	0	8	0	11
`reduce_33`	0	0	0	0
`reduce_41t`	1	23	1	28
`reduce_42`	0	0	0	1
`reduce_43`	0	6	0	11
`reduce_44`	0	0	0	0
`reduce_51t`	1	24	0	32
`reduce_52`	0	1	0	3
`reduce_53`	0	12	0	14
`reduce_54`	0	7	0	10
`reduce_61t`	1	35	0	46
`reduce_62`	0	2	0	5
`reduce_63`	0	8	0	13
`reduce_64`	0	12	0	21
`reduce_65`	0	0	0	0

Finally, we give operation counts for flipping subroutines in Table 12.6. Flipping a principal divisor (type 0, 33, 44, or 65) is free, so their costs are not listed.

Table 12.6: Operation counts for flipping subroutines

Subroutine	Operation count I	M	S	A	Case
`flip_11`	0	4	0	5	
`flip_21`	0	7	0	12	
`flip_22`	0	1	0	2	
`flip_31`	1	15	0	18	$\langle f, g\rangle = \langle f, g, h\rangle$
`flip_31`	0	12	0	20	$\langle f, g\rangle \neq \langle f, g, h\rangle$
`flip_32`	0	3	0	6	
`flip_41`	1	23	1	26	$\langle f, g\rangle = \langle f, g, h\rangle$
`flip_41`	1	32	1	38	$\langle f, g\rangle \neq \langle f, g, h\rangle = \langle f, h\rangle$
`flip_41`	0	28	2	46	$\langle f, g\rangle \neq \langle f, g, h\rangle \neq \langle f, h\rangle$
`flip_42`	0	8	0	9	
`flip_43`	0	5	0	7	
`flip_51`	1	24	0	28	$\langle f, g\rangle = \langle f, g, h\rangle$
`flip_51`	1	21	0	31	$\langle f, g\rangle \neq \langle f, g, h\rangle = \langle f, h\rangle$
`flip_51`	0	33	0	52	$\langle f, g\rangle \neq \langle f, g, h\rangle \neq \langle f, h\rangle$
`flip_52`	0	22	1	27	
`flip_53`	0	26	1	31	
`flip_54`	0	3	1	6	
`flip_61`	1	24	0	41	$\langle f, g\rangle = \langle f, g, h\rangle$
`flip_61`	0	25	0	45	$\langle f, g\rangle \neq \langle f, g, h\rangle = \langle f, h\rangle$
`flip_61`	0	44	0	80	$\langle f, g\rangle \neq \langle f, g, h\rangle \neq \langle f, h\rangle$
`flip_62`	0	4	0	6	
`flip_63`	0	18	0	28	
`flip_64`	0	3	0	9	

13 Conclusion

We have been able to accomplish the two main goals of this thesis: to generalize the techniques of Abu Salem and Khuri-Makdisi to apply to atypical divisors as classified by Arita, and to find an improvement in the typical case as well.

With regards to the generalization to atypical divisors, nowhere in Chapters 8, 9, and 10 did we impose any requirements on the characteristic of the field over which the curve is defined or the curve equation being of long or short form. Moreover, the algorithms described in those chapters terminate with correct outputs even when the divisors involved are non-disjoint or contain points with order greater than 1. Explicit formulae for each of the possible atypical cases[28] have been derived, but due to the sheer number of these cases,[29] these formulae may be found at [30]; to include them all in this thesis would likely add another 100 or more pages, and anyone who needs those formulae would probably prefer raw code over a pdf file or ink on paper.

With regards to the improvement in the typical case, preliminary testing shows that we are able compute divisors faster than the previous state-of-the-art. This was accomplished primarily by avoiding computing some unnecessary polynomial coefficients, and by collecting addition/doubling and reduction into a single step to eliminate a finite field inversion operation. The representation of a typical divisor by a three-polynomial Gröbner basis $\langle f, g, h\rangle$, rather than by a two-polynomial generating set $\langle f, g\rangle$ as in [40], allows for the matrix M_{add} to be computed especially fast. We require many more multiplications than the previous state-of-the-art, but many fewer additions and one fewer inversion. Likely, the trade-off of an inversion for several multiplications contributed the largest portion of the speed-up, while lowering the number of additions likely contributed a non-trivial amount as well.

Sage code for the typical addition and doubling case is also available at [30]. Anyone wishing to perform computations in the divisor class group of a $C_{3,4}$ curve, or wishing to

[28] Either adding one or more atypical divisors, or adding divisors whose sum turns out to be atypical.

[29] There are 13 cases arising from adding two type 31 divisors alone, corresponding to $\text{type}(\text{lcm}(D, D')) = 41, 42, \ldots, 65$.

translate that code into another language such as Magma, may begin by downloading the implementation there.

13.1 Future Work

There are four avenues for possible improvements to $C_{3,4}$ curve arithmetic. Let us end the thesis on a high note by listing them from least to most promising.

There is room for improvement in the arithmetic in the atypical cases. In Chapter 11, we eliminated an expensive inversion operation by combining addition/doubling and reduction into a single step. The formulae in [30] for handling the atypical cases perform addition/doubling and reduction discretely. An inversion could also be eliminated from these cases in much the same way as was done in Chapter 11 for the typical case. However, this is a lot of work for very little gain, considering that any application of this arithmetic will likely spend very little time computing these atypical cases.

Representating divisors by Gröbner bases means carrying around some redundant information. Typically, we represent a divisor by an ideal $\langle f, g, h\rangle$ where h may be computed from f and g. This is a time-space trade-off.[30] In computational applications where memory is a factor, a smaller representation may be desirable. It was known to me at the beginning of this project that any ideal in a Dedekind domain is generated by two or fewer elements. It was not known to me that an even stronger statement is true: given any $f \in I_D$, there is a $g \in I_D$ such that $I_D = \langle f, g\rangle$ — one may choose one of the generators arbitrarily.[31] One of the motivations for using Gröbner bases was that one of its generators is always the minimum polynomial in the ideal. I suspect that every type 31 divisor can be represented instead by one of three forms: $\langle x^2 + \ldots, xy + \ldots\rangle$, $\langle x^2 + \ldots, y^2 + \ldots\rangle$, or $\langle x^2 + \ldots, xy^2 + \ldots\rangle$, where the polynomial $x^2 + \ldots$ is the minimum with respect to the $C_{3,4}$ order. Thus, one

[30] A careful reading of the formulae in [40], where the authors represent a divisor D by only $\langle f, g\rangle$, shows that the authors are computing h every time they add another divisor to D.

[31] See Theorem 8.5.1 in [1]. It is proven that every ideal I in a Dedekind domain is generated by two elements, but the proof is constructive. An element $\alpha \in I$ is chosen arbitrarily and another element β is found such that $I = \langle \alpha, \beta\rangle$.

may reclassify type 31 divisors into 3 subtypes and similarly reclassify type 41, 51, and 61 divisors. I do not know that one will gain any runtime improvements this way, but it would allow for semi-typical divisors to be represented more compactly.

In the typical case, we are able to quickly compute M_{add}, but computing M_{doub} is slow in comparison. Our calculation of M_{doub} does not make much use of the third polynomial h in the representation of a type 31 divisor, though it may be possible to leverage it some more. Presently, to compute M_{doub}, we find g' and h' such that $fh' \equiv gg'$, and make use of a map d that maps $f \mapsto g'$ and $g \mapsto h'$. One promising improvement is to instead let d be the map

$$d : \begin{array}{l} f \mapsto s't - st' \\ g \mapsto t'r - tr' \\ h \mapsto r's - rs' \end{array}$$

where r, s, t, r', s', t' are as in Lemmas 7.21 and 7.24. Each of these six polynomials are very fast to compute. Whereas we currently need 36M+44A to compute g', h', and M_{doub}, it would only require about 30M+41A to compute $r, s, t, r', s', t', M_{\text{doub}}$. Preliminary testing has shown that using this map for d produces correct results. However, this discovery was made late in the writing of this thesis and lacks a proof of correctness and thorough testing.

The current state of $C_{3,4}$ curve arithmetic is that it is still significantly more expensive that arithmetic for genus 3 hyperelliptic curves. Colleagues at the University of Calgary have applied Shanks' NUCOMP algorithm [41] to genus 3 hyperelliptic curve divisor arithmetic [23]. Upcoming results [29] have the cost of addition down to approximately 1I+52M (ramified curves) and 1I+67M (split curves), half as many multiplications as are currently required for $C_{3,4}$ curves. One may wonder whether NUCOMP may be applied to $C_{3,4}$ curve arithmetic as well.

Bibliography

[1] Saban Alaca and Kenneth S. Williams. *Introductory Algebraic Number Theory*. New York: Cambridge University Press, 2004.

[2] Seigo Arita. Algorithms for computations in Jacobian group of $C_{a,b}$ curve and their application to discrete-log-based public key cryptosystems. in Japanese. *IEICE TRANS. FOUND.* J82-A, NO.8 (1999), pp. 1291–1299.

[3] Seigo Arita. An Addition Algorithm in Jacobian of $C_{3,4}$ Curve. *IEICE TRANS. FOUND.* E88-A, NO.6 (2005), pp. 1589–1598.

[4] Seigo Arita. An Addition Algorithm in Jacobian of $C_{a,b}$ Curves. *Discrete Applied Mathematics* 130 (2003), pp. 13–31.

[5] Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, and Nicolas Gürel. Implementing the Arithmetic of $C_{3,4}$ Curves. In: *Sixth Algorithmic Number Theory Symposium (ANTS-VI)*. (University of Vermont, Burlington, VT). Springer, 2004, pp. 87–101.

[6] Bruno Buchberger. Introduction to Gröbner Bases. In: *Gröbner Bases and Applications*. Ed. by Bruno Buchberger and Franz Winkler. London Mathematical Society Lecture Note Series 251. Cambridge: Cambridge University Press, 1998, pp. 3–31.

[7] Keith Conrad. Ideal Factorization. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf.

[8] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. 3rd ed.* 2007.

[9] Erik Dahmen, Katsuyuki Okeya, and Daniel Schepers. Affine Precomputation with Sole Inversion in Elliptic Curve Cryptography. In: *Information Security and Privacy*. Ed. by Josef Pieprzyk, Hossein Ghodosi, and Ed Dawson. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 245–258.

[10] David S. Dummit and Richard M. Foote. *Abstract Algebra*. 3rd edition. Hoboken, NJ: John Wiley and Sons, Inc, 2004.

[11] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. New York: Springer-Verlag, Jan. 1995.

[12] David Eisenbud and Joe Harris. *The Geometry of Schemes*. Vol. 197. New York: Springer-Verlag, 2000.

[13] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler. Fast Addition on Non-Hyperelliptic Genus 3 Curves. In: *Algebraic geometry and its applications, Proceedings of the first SAGA conference, Ser. Number theory and its applications*. Vol. 4. Hackensack, NJ: World Sci. Publ., 2008, pp. 1–28.

[14] William Fulton. *Algebraic Curves: an Introduction to Algebraic Geometry*. 2008. URL: http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf (visited on 01/29/2020).

[15] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. New York: Cambridge University Press, 2012.

[16] David M. Goldschmidt. *Algebraic Functions and Projective Curves*. Vol. 215. New York: Springer-Verlag, 2003.

[17] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. New York: Springer-Verlag, 2004.

[18] Ryuichi Harasawa and Joe Suzuki. Fast Jacobian Group Arithmetic on C_{ab} Curves. In: *Fourth Algorithmic Number Theory Symposium (ANTS-IV)*. (Universiteit Leiden, Leiden, NL). Springer, 2000, pp. 359–376.

[19] David Harvey, Maike Massierer, and Andrew V. Sutherland. Computing L-series of Geometrically Hyperelliptic Curves of Genus Three. In: *Twelfth Algorithmic Number Theory Symposium (ANTS-XII)*. (University of Kaiserslautern, Germany). Springer, Aug. 2016, pp. 220–234.

[20] Helmut Hasse. Zur Theorie der abstrakten elliptischen Funktionkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1936 (175 1936), pp. 193–208.

[21] Thomas W. Hungerford. *Algebra*. Vol. 73. New York: Springer-Verlag, 1974.

[22] Dale Husemöller. *Elliptic Curves*. Vol. 111. New York: Springer-Verlag, 1987.

[23] Michael J. Jacobson Jr., Renate Scheidler, and Andreas Stein. Fast arithmetic on hyperelliptic curves via continued fraction expansions. In: *Series on Coding Theory and Cryptology*. WORLD SCIENTIFIC, July 2007, pp. 200–243.

[24] Kiran S. Kedlaya and Andrew V. Sutherland. Computing L-series of Hyperelliptic Curves. In: *Eighth Algorithmic Number Theory Symposium (ANTS-VIII)*. (Banff, Alberta, Canada). Springer, May 2008, pp. 312–326.

[25] Kamal Khuri-Makdisi. Linear Algebra Algorithms for Divisors on an Algebraic Curve. *Mathematics of Computation* 73 (2004), pp. 333–357.

[26] Kamal Khuri-Makdisi. On Jacobian Group Arithmetic for Typical Divisors on Curves. *Research in Number Theory* 4, no. 1, article 3 (2018).

[27] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. 2nd ed. Vol. 97. New York: Springer-Verlag, 1993.

[28] Ernst Kunz. *Introduction to Plane Algebraic Curves*. Trans. by Richard D. Belshoff. Boston: Birkhäuser, 2005.

[29] Sebastian Lindner. personal communication. Oct. 24, 2019.

[30] Evan MacNeil. *c34-curves*. https://github.com/emmacneil/c34-curves. 2019.

[31] Ryutaroh Matsumoto. The $C_{a,b}$ Curve. 1998. URL: http://www.rmatsumoto.org/cab.pdf.

[32] James S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006, pp. 238+viii. ISBN: 1-4196-5257-5.

[33] Shinji Miura. Research on Error Correcting Codes Based on Algebraic Geometry. japanese. PhD thesis. University of Tokyo, 1997.

[34] Jürgen Neukirch. *Algebraic Number Theory*. Trans. by Norbert Schappacher. Vol. 322. Germany: Springer-Verlag Berlin Heidelberg, 1999.

[35] Jun Nyukai. *A Fast Addition Algorithm on Hyperelliptic Curves*. Tech. rep. 2006. URL: http://ir.c.chuo-u.ac.jp/repository/search/binary/p/3114/s/1893/,.

[36] Jun Nyukai, Kazuto Matsuo, Jinhui Chao, and Shigeo Tujii. *On the Resultant Computation in the Harley Algorithm on Hyperelliptic Curves*. Tech. rep. ISEC2006-5. IEICE Japan, 2006.

[37] Monir Rezai Rad. A Complete Evaluation of Arithmetic in Real Hyperelliptic Curves. PhD thesis. University of Calgary, 2016.

[38] Monir Rezai Rad, Michael J. Jacobson Jr., and Renate Scheidler. Jacobian versus Infrastructure in Split Hyperelliptic Curves. *First International Conference on Algebra, Codes and Cryptography, A2C 2019, Communications in Computer and Information Science* (2019), pp. 183–203.

[39] Lorenzo Robbiano. On the theory of graded structures. *Journal of Symbolic Computation* 2 (June 1986), pp. 139–170.

[40] Fatima Abu Salem and Kamal Khuri-Makdisi. Fast Jacobian group operations for $C_{3,4}$ curves over a large finite field. *LMS Journal of Computation and Mathematics* 10 (Nov. 2007), pp. 307–328.

[41] Daniel Shanks. On Gauss and composition. I, II. In: *Number theory and applications (Banff, AB, 1988)*. Vol. 265. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. Kluwer Academic Publishers, Dordrecht, 1989, pp. 163–178, 179–204.

[42] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009.

[43] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. New York: Springer-Verlag, 1992.

[44] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Vol. 254. New York: Springer-Verlag, 2009.

[45] Andrew V. Sutherland. Fast Jacobian Arithmetic for Hyperelliptic Curves of Genus 3. In: *Thirteenth Algorithmic Number Theory Symposium (ANTS-XIII)*. (University of Wisconsin, Madison). Open Book Series, July 2018, pp. 425–442.

[46] Andrew V. Sutherland. *Sato-Tate Distributions*. 2016. arXiv: 1604.01256 [math.NT].

[47] Robert J. Walker. *Algebraic Curves*. New York: Springer-Verlag, 1978.

[48] André Weil. Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society* 55 (5 1949).

A The Colon Ideal

Let $\mathfrak{a}$ and $\mathfrak{b}$ be *integral* ideals of a commutative ring with identity R. The **ideal quotient** of $\mathfrak{a}$ by $\mathfrak{b}$, also called the **colon ideal**, is

$$\mathfrak{a} : \mathfrak{b} = \{r \in R \mid r\mathfrak{b} \subseteq \mathfrak{a}\}.$$

When an ideal quotient involves principal ideals $\langle a \rangle$ or $\langle b \rangle$, we may write $a : \mathfrak{b}$, $\mathfrak{a} : b$, and $a : b$ for brevity, rather than $\langle a \rangle : \mathfrak{b}$, $\mathfrak{a} : \langle b \rangle$, and $\langle a \rangle : \langle b \rangle$.

The following proposition sums up several useful, well-known properties of the colon ideal.

Proposition A.1. *Let R be a commutative ring with identity. Let $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ be R-ideals. Then*

(i) $\mathfrak{a} : \mathfrak{b}$ *is an R-ideal;*

(ii) $\mathfrak{a} \subseteq \mathfrak{a} : \mathfrak{b}$*;*

(iii) $\mathfrak{a} : R = \mathfrak{a}$*;*

(iv) $R : \mathfrak{a} = R$*;*

(v) $\mathfrak{ab} \subseteq \mathfrak{c} \iff \mathfrak{a} \subseteq \mathfrak{c} : \mathfrak{b}$*;*

(vi) $\mathfrak{a} : \mathfrak{b} = R \iff \mathfrak{b} \subseteq \mathfrak{a}$*;*

(vii) $\mathfrak{a} : (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{a} : \mathfrak{c})$*;*

(viii) $(\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) \cap (\mathfrak{b} : \mathfrak{c})$*;*

(ix) $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : \mathfrak{bc}$.

These properties are given as propositions in [8], though the statements are given for a multivariate polynomial ring over a field, $K[x_1, \ldots, x_n]$ rather than for an arbitrary commutative ring with identity, and most of the proofs are left as exercises. Proofs, in slightly greater generality, are given here.

Proof. (i) Let $a, b \in \mathfrak{a} : \mathfrak{b}$. Then $a\mathfrak{b}, b\mathfrak{b} \subseteq \mathfrak{a}$. Then $(a+b)\mathfrak{b} = a\mathfrak{b} + b\mathfrak{b} \subseteq \mathfrak{a}$ (since $a\mathfrak{b} + b\mathfrak{b}$ is the join of $a\mathfrak{b}$ and $b\mathfrak{b}$ in the lattice of R-ideals). So $a + b \in \mathfrak{a} : \mathfrak{b}$.

Let $a \in \mathfrak{a} : \mathfrak{b}$, $r \in R$. Then $a\mathfrak{b} \subseteq \mathfrak{a}$ and $ra\mathfrak{b} \subseteq a\mathfrak{b}$, so $ra\mathfrak{b} \subseteq \mathfrak{a}$ and $ra \in \mathfrak{a} : \mathfrak{b}$.

(ii) We have

$$\begin{aligned} & \mathfrak{a} \subseteq \mathfrak{a} : b \\ \iff & \forall a \in \mathfrak{a} : a\mathfrak{b} \subseteq \mathfrak{a} \\ \iff & \forall a \in \mathfrak{a} : \forall b \in \mathfrak{b} : ab \in \mathfrak{a}. \end{aligned}$$

The last statement is true since ideals are closed under multiplication by R.

(iii) By part (ii), we have $\mathfrak{a} \subseteq \mathfrak{a} : R$. Suppose $a \in \mathfrak{a} : R$. Then $aR \subseteq \mathfrak{a}$. In particular, $a = a \cdot 1_R \in \mathfrak{a}$, so $\mathfrak{a} : R \subseteq \mathfrak{a}$.

(iv) By definition, $R : \mathfrak{a} \subseteq R$. By part (ii), $R \subseteq R : \mathfrak{a}$.

(v) ($\implies$) Let $a \in \mathfrak{a}$. Then $a\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$, and by hypothesis, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{c}$, so $a\mathfrak{b} \subseteq \mathfrak{c}$, and $a \in \mathfrak{c} : \mathfrak{b}$.

($\impliedby$) Let $a \in \mathfrak{a}$. By hypothesis, $a \in \mathfrak{c} : \mathfrak{b}$, so $a\mathfrak{b} \subseteq \mathfrak{c}$. Since the choice of a was arbitrary, this means $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{c}$.

(vi) ($\implies$) Suppose $\mathfrak{a} : \mathfrak{b} = R$. Then $\mathfrak{b} = 1_R\mathfrak{b} \subseteq \mathfrak{a}$.

($\impliedby$) Suppose $b \subseteq \mathfrak{a}$. For all $r \in R$, $r\mathfrak{b} \subseteq \mathfrak{b}$. So $r\mathfrak{b} \subseteq \mathfrak{a}$ and $\mathfrak{a} : \mathfrak{b} = R$.

(vii) Let $r \in R$. We have

$$\begin{aligned} & r(\mathfrak{b}+\mathfrak{c}) \subseteq \mathfrak{a} \\ \iff & r\mathfrak{b}+r\mathfrak{c} \subseteq \mathfrak{a} \\ \iff & r\mathfrak{b} \subseteq \mathfrak{a} \text{ and } r\mathfrak{c} \subseteq \mathfrak{a}. \end{aligned}$$

So

$$\begin{aligned} \mathfrak{a} : (\mathfrak{b}+\mathfrak{c}) &= \{r \in R \mid r(\mathfrak{b}+\mathfrak{c}) \subseteq \mathfrak{a}\} \\ &= \{r \in R \mid r\mathfrak{b} \subseteq \mathfrak{a} \text{ and } r\mathfrak{c} \subseteq \mathfrak{a}\} \\ &= \{r \in R \mid r\mathfrak{b} \subseteq \mathfrak{a}\} \cap \{r \in R \mid r\mathfrak{c} \subseteq \mathfrak{a}\} \\ &= (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{a} : \mathfrak{c}). \end{aligned}$$

(viii) Similarly to part (vii),

$$\begin{aligned} (\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{c} &= \{r \in R \mid r\mathfrak{c} \subseteq \mathfrak{a} \cap \mathfrak{b}\} \\ &= \{r \in R \mid r\mathfrak{c} \subseteq \mathfrak{a} \text{ and } r\mathfrak{c} \subseteq \mathfrak{b}\} \\ &= \{r \in R \mid r\mathfrak{c} \subseteq \mathfrak{a}\} \cap \{r \in R \mid r\mathfrak{c} \subseteq \mathfrak{b}\} \\ &= (\mathfrak{a} : \mathfrak{c}) \cap (\mathfrak{b} : \mathfrak{c}). \end{aligned}$$

(ix) Let $r \in R$. We have

$$\begin{aligned} & r\mathfrak{c} \subseteq \mathfrak{a} : \mathfrak{b} \\ \iff & r\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a} && \text{by (v)} \\ \iff & r \in \mathfrak{a} : \mathfrak{b}\mathfrak{c}, \end{aligned}$$

so

$$\begin{aligned}(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} &= \{r \in R \mid r\mathfrak{c} \subseteq \mathfrak{a} : \mathfrak{b}\} \\ &= \{r \in R \mid r \in \mathfrak{a} : \mathfrak{b}\mathfrak{c}\} \\ &= \mathfrak{a} : \mathfrak{b}\mathfrak{c}.\end{aligned}$$

□

The following proposition and its corollary illustrate why this ideal is called the ideal quotient. In a Dedekind domain, we have $\mathfrak{a}\mathfrak{b} : \mathfrak{b} = \frac{\mathfrak{a}\mathfrak{b}}{\mathfrak{b}} = \mathfrak{a}$.

Proposition A.2. *Let R be a Dedekind domain. Let $\mathfrak{a}$ be a non-zero ideal and $\mathfrak{p}$ a non-zero prime ideal of R. Then*

$$\mathfrak{a}\mathfrak{p} : \mathfrak{p} = \mathfrak{a}.$$

Proof. Clearly, $\mathfrak{a}\mathfrak{p} \subseteq \mathfrak{a}\mathfrak{p}$. Using Proposition A.1.(v), this gives $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p} : \mathfrak{p}$.

Suppose $\alpha \in \mathfrak{a}\mathfrak{p} : \mathfrak{p}$. Then $(\alpha)\mathfrak{p} \subseteq \mathfrak{a}\mathfrak{p}$ and there exists a non-zero ideal $\mathfrak{b}$ such that $(\alpha)\mathfrak{p} = \mathfrak{a}\mathfrak{b}\mathfrak{p}$. By Corollary 3.3 in [7], $(\alpha) = \mathfrak{a}\mathfrak{b}$, so $(\alpha) \subseteq \mathfrak{a}$ and $\alpha \in \mathfrak{a}$. □

Corollary A.3. *Let R be a Dedekind domain. Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero ideals of R. Then*

$$\mathfrak{a}\mathfrak{b} : \mathfrak{b} = \mathfrak{a}.$$

Proof. Let $\mathfrak{b}$ factor into $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, where the $\mathfrak{p}_i$'s are not necessarily distinct. Then

$$\begin{aligned}\mathfrak{a}\mathfrak{b} : \mathfrak{b} &= (\mathfrak{a}\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n) : (\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n) \\ &= (((\mathfrak{a}\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n : \mathfrak{p}_1) : \mathfrak{p}_2) : \dots) : \mathfrak{p}_n && \text{by Prop A.1.ix} \\ &= ((\mathfrak{a}\mathfrak{p}_2 \dots \mathfrak{p}_n : \mathfrak{p}_2) : \dots) : \mathfrak{p}_n && \text{by Prop A.2} \\ &= \dots && \text{induction} \\ &= \mathfrak{a}.\end{aligned}$$

□

Corollary A.4. *Let R be a Dedekind domain and let $\mathfrak{a}$ be a non-zero R-ideal. Let $a \in \mathfrak{a}$. Then*

$$\mathfrak{a}(a : \mathfrak{a}) = \langle a \rangle .$$

Proof. We have $\mathfrak{a} \subseteq \langle a \rangle$, so there is an R-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \langle a \rangle$. Then by Corollary A.3,

$$a : \mathfrak{a} = (\mathfrak{ab}) : \mathfrak{a} = \mathfrak{b},$$

and

$$\mathfrak{a}(a : \mathfrak{a}) = \mathfrak{ab} = \langle a \rangle .$$

□

B Reduced Divisors Have Degree at Most 3

Let D be a degree 0 divisor on a $C_{3,4}$ curve (as defined in Section 5.1). In keeping with the convention adopted in Chapter 7, we assume that D is of the form $D = D_+ - D_\infty$, where D_+ is effective and D_∞ is a multiple of the point at infinity. The degree of D_∞ is determined by the degree of D_+. In this appendix, we prove that if D is a reduced divisor, then the degree of its finite part D_+ is at most 3. Also in keeping with the convention adopted in Chapter 7, whenever we refer to $\deg D$ below, we really mean the degree of its finite part D_+.

Lemma B.1. *Let D be a divisor with ideal I_D. Fix $b \in \mathbb{N}$. There is a minimal non-zero monic polynomial in the set $\{f \in I_D \mid y^b \text{ divides } \mathrm{LT}(f)\}$.*

This polynomial is minimal in the sense that, if g is any other polynomial such that $y^b | \mathrm{LT}(g)$, then $\mathrm{LT}(f) | \mathrm{LT}(g)$. This polynomial f is not necessarily unique.

Proof. Follows from a monomial order being a well-order. □

Lemma B.2. *Let D be a divisor with ideal I_D. There exist polynomials f, g, h such that $I_D = \langle f, g, h\rangle$, $\mathrm{LT}(f) = x^c$, $\mathrm{LT}(g) = x^b y$, $\mathrm{LT}(h) = x^a y^2$, f, g, and h are minimal in the sense of the previous lemma, and $a \leq b \leq c$.*

Proof. Everything but the relation $a \leq b \leq c$ is immediate from the previous lemma. To prove this relation, suppose $b < a$. Then y^2 divides $\mathrm{LT}(gy)$ and $\mathrm{LT}(gy)$ divides $\mathrm{LT}(h)$, but $\mathrm{LT}(h)$ does not divide $\mathrm{LT}(gy)$, so h was not minimal. Hence $a \leq b$. The same argument can be used to show $b \leq c$. □

Lemma B.3. *Let D be a divisor with ideal I_D. Let $I_D = \langle f, g, h\rangle$ as in the previous lemma. Then $\langle f, g, h\rangle$ is a Gröbner basis for I_D.*

Proof. We must show that for any $r \in I_D$, $\mathrm{LT}(r) \in \mathrm{LT}(I_D)$.

Let $r \in I_D$. Then $\mathrm{LT}(r) = x^m y^n$ for some $0 \leq n \leq 2$. However, by the minimality criterion by which f, g, and h were chosen, one of $\mathrm{LT}(f)$, $\mathrm{LT}(g)$, or $\mathrm{LT}(h)$ divides $\mathrm{LT}(r)$, hence $\mathrm{LT}(r) \in \mathrm{LT}(I_D)$. □

Lemma B.4. *Let D be a divisor with ideal I_D. Let $I_D = \langle f, g, h\rangle$ as in the previous lemma. Then $a + b + c = \deg D$.*

Proof.

$$\begin{aligned}\deg D &= \dim \frac{K[C]}{I_D} = \dim \frac{K[C]}{\langle f, g, h\rangle} = \dim \frac{K[C]}{\langle x^c, x^b y, x^a y^2\rangle} \\ &= a + b + c.\end{aligned}$$

The final equality follows from Corollary 3.26. □

Theorem B.5. *Let D be a divisor with ideal I_D. Let f be minimal in I_D. Then*

$$-\nu_{P_\infty}(f) - \deg D \leq 3.$$

Proof. Let $I_D = \langle f, g, h\rangle$ as in the previous lemma. The minimal polynomial of I_D is either f, g, or h. Consider each case separately.

f is minimal in I_D: Then $\nu_{P_\infty}(f)$ is less than both $\nu_{P_\infty}(g)$ and $\nu_{P_\infty}(h)$. So $3c \leq 3b+4$ and $3c \leq 3a + 8$, which implies $c - b \leq 1$ and $c - a \leq 2$. Then

$$\begin{aligned}-\nu_{P_\infty}(f) - \deg D &= 3c - (a + b + c) \\ &= (c - a) + (c - b) \\ &\leq 2 + 1 = 3.\end{aligned}$$

g is minimal in I_D: Then $3b + 4 < 3c$ and $3b + 4 < 3a + 8$, which implies $b - c \leq -2$ and $b - a \leq 1$, so

$$\begin{aligned}-\nu_{P_\infty}(f) - \deg D &= 3b + 4 - (a + b + c) \\ &= 4 + (b - a) + (b - c) \\ &\leq 4 + 1 - 2 = 3.\end{aligned}$$

h **is minimal in** I_D**:** Then $3a + 8 < 3c$ and $3a + 8 < 3b + 4$, which implies $a - c \leq -3$ and $a - b \leq -2$, so

$$\begin{aligned} -\nu_{P_\infty}(f) - \deg D &= 3a + 8 - (a + b + c) \\ &= 8 + (a - b) + (a - c) \\ &\leq 8 - 2 - 3 = 3. \end{aligned}$$

□

Theorem B.6. *Every reduced divisor on C has degree at most 3.*

Proof. Theorem B.5 and Equation 7.7. □