The University of Osaka
Institutional Knowledge Archive

Title	Jacobian Group Arithmetic on Algebraic Curves
Author(s)	原澤, 隆一
Citation	大阪大学, 2003, 博士論文
Version Type	VoR
URL	https://hdl.handle.net/11094/337
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

Jacobian Group Arithmetic on Algebraic Curves

Ryuichi Harasawa

Osaka University

March 2003

Abstract

This thesis proposes an efficient method for performing Jacobian group arithmetic on nonsingular projective curves defined over a finite field $\mathbf{F}_q$ and evaluates its time complexity. Such arithmetic has been commonly used in cryptosystems based on algebraic curves such as hyperelliptic curves.

For elliptic curves

$$y^2 = x^3 + ax + b,$$

there has been a well-known method which realizes its group arithmetic. Also for hyperelliptic curves

$$y^2 = x^{2g+1} + \cdots ,$$

D. G. Cantor proposed an efficient method. The idea is to consider Jacobian group arithmetic as the arithmetic on the ideal class group of the coordinate ring, since the two groups are isomorphic. Furthermore, the method involves only the operations on $\mathbf{F}_q[x]$, a polynomial ring in one variable, so we can evaluate the time complexity precisely, which is $O(g^2 \log^2 q)$ bit-operations, i.e. the square order of the size of the input.

In this thesis, we consider an algebraic function field $F/\mathbf{F}_q$ of one variable. Without loss of generality, we assume that there exists a place P of degree one, and that the set of pole numbers of P is generated by t elements $\mathbf{A}_t := \{a_1, \cdots, a_t\}$. (Hereafter, without loss of generality, we assume $\gcd(a_1, q) = 1$.) In 1998, S. Miura gave an affine algebraic curve $C/\mathbf{F}_q$ with t variables whose function field $\mathbf{F}_q(C)$ is given by the $F/\mathbf{F}_q$. In this thesis, we call such a curve $C/\mathbf{F}_q$ a $\mathbf{A}_t$-*curve*. If $t = 2$ and $\mathbf{A}_t = \{2, 2g+1\}$, then the $\mathbf{A}_t$-curve is a hyperelliptic curve of genus g. In fact, it turns out that Jacobian group on $\mathbf{A}_t$-curves is isomorphic to the ideal class group of the coordinate ring.

In order to realize the arithmetic on ideal class group of the coordinate ring $\mathbf{F}_q[C]$ of a $\mathbf{A}_t$-curve $C/\mathbf{F}_q$, we need to compute:

1. the inverse ideal I^{-1} for a given ideal I; and
2. the minimal element of a given ideal with respect to the pole order at P.

For the first item, we realize the computation by applying results on number theory, since

1. $\mathbf{F}_q[x]$ is a principal ideal domain (**PID**), where x is such an element in $\mathbf{F}_q(C)$ as $(x)_\infty = a_1 P$;
2. $\mathbf{F}_q(C)/\mathbf{F}_q(x)$ is a finite separable extension of degree a_1; and
3. the integral closure of $\mathbf{F}_q[x]$ in $\mathbf{F}_q(C)$ is the coordinate ring $\mathbf{F}_q[C]$.

For the second, we obtain a minimal element by constructing a $\mathbf{F}_q[x]$-basis $\{w_1, \cdots, w_{a_1}\}$ of a given ideal such that $-v_P(w_i) \not\equiv -v_P(w_j) \bmod a_1$ $(i \neq j)$, where $v_P(\cdot)$ denotes the discrete valuation with respect to P.

In this sense, this thesis gives an extension of Cantor's method to $\mathbf{A}_t$-curves. The arithmetic is realized by the operations on a polynomial ring $\mathbf{F}_q[x]$ in the square order of the size of the input with a_1 fixed:

Theorem (Main Result)

Jacobian group arithmetic on $\mathbf{A}_t$-curves of genus g is performed in

$$O(\max\{a_1^6 g^2,\ a_1^8\} \log^2 q)$$

bit-operations.

Moreover, this thesis includes the implementational results of the proposed method for $\mathbf{A}_t$-curves of an actual scale used in algebraic curve cryptography.

Acknowledgements

I am very grateful to Professor Yoshihiko Yamamoto and Professor Joe Suzuki for many supports and fruitful advices to accomplish this thesis. I also would like to thank Professor Takayuki Hibi, Professor Tomoyoshi Ibukiyama and Professor Akio Fujiwara for valuable and helpful comments.

Furthermore, I would like to thank Professor Steven Galbraith, Professor Junji Shikata, Dr. Shinji Miura and Dr. Kohji Yanagawa for fruitful discussion and detailed comments on this thesis.

Finally, I would like to thank the members of the laboratories of Professor Yoshihiko Yamamoto, Professor Joe Suzuki for many supports, especially concerning the implementation in Appendix.

Contents

1 Introduction **6**

2 Preliminaries **10**
2.1 Complexity Theory 10
2.2 **Z**-modules 12
2.3 Algebraic Number Theory 15

3 Algebraic Function Fields **19**
3.1 Algebraic Function Field 19
3.2 Divisor Class Group 22
3.3 The Riemann-Roch Theorem 26
3.4 Algebraic Extensions of Algebraic Function Field . . 28
3.5 Subrings of Function Fields 31
3.6 The Hesse-Weil Theorem 33
3.7 Affine Varieties 35

4 $\mathbf{A}_t$-curves **38**

5 Jacobian Group Arithmetic on Algebraic Function Fields **43**

6 Realization of Jacobian Group Arithmetic **48**
6.1 Computing Inverse Ideal 48
6.1.1 The First Method 50
6.1.2 The Second Method 50
6.2 Computing Minimal Element 53

7 Complexity **56**
7.1 Inverse ideal 56
7.2 Complexity 57

Chapter 1

Introduction

We consider algebraic curve cryptography based on the intractability of the discrete logarithm problem (DLP) in the Jacobian group on an algebraic curve defined over a finite field. We implement a cryptosystem as follows [6]:

Suppose that G is a finite cyclic group with $n = \#G$. Each user makes his/her own public ciphering key (α, β) and secret decoding key l, where $\alpha, \beta \in G$ and $\alpha^l = \beta$ $(0 \leq l \leq n-1)$ are assumed. When Bob sends a message $m \in G$ to Alice, he randomly generates $0 \leq k \leq n-1$, and send m as the cipher $c = (m\beta_A^k, \alpha_A^k)$. When she receives the cipher c from him, she uses her secret key l_A. She decodes c as the message

$$\frac{m\beta_A^k}{(\alpha_A^k)^{l_A}} = \frac{m\beta_A^k}{(\alpha_A^{l_A})^k} = \frac{m\beta_A^k}{(\beta_A^k)} = m.$$

It is easily found that the security of the above cryptosystem depends on how computationally hard it is to obtain l such that $\alpha^l = \beta$.

Even if n is large, if the largest prime factor of n is small, the Chinese remainder theorem solves the problem easily. Also, if the finite cyclic group is complicated, so is the group arithmetic, i.e. the encryption will not be efficient.

In algebraic curve cryptography, G is the Jacobian group on a curve defined over a finite field $\mathbf{F}_q$. This thesis concerns an efficient Jacobian group arithmetic. Considering Jacobian group arithmetic,

the only problem is to compute a suitably expressed representative of each class. In special cases, the problem had been solved.

For elliptic curves, a method for performing addition among Jacobians has been known since long ago, and its group arithmetic is given as a simple formula [17]. For hyperelliptic curves, an efficient method of Jacobian group arithmetic has been given by D. G. Cantor [3]. (Although Cantor assumed that the characteristic is not two, N. Koblitz excluded the constraint [11].) And the method is realized in $O(g^2 \log^2 q)$ bit-operations, where g denotes the genus of an algebraic curve defined over $\mathbf{F}_q$. So, for Jacobian group arithmetic on algebraic curves, the algorithms realized in $O(g^2 \log^2 q)$ bit-operations are supposed to be the most efficient methods thus far. In other words, efficient Jacobian group arithmetic is performed in the square order of the size of the input. (Usually, we regard the size of the input as the logarithm of the order of the Jacobian group, which is $O(q^g)$.)

In this thesis, we address the problem whether or not there exists a method for performing Jacobian group arithmetic in $O(g^2 \log^2 q)$ bit-operations for more general curves than hyperelliptic curves.

Under certain conditions, the problem has been solved in the affirmative for a class of curves called *superelliptic curves* (Galbraith, Paulus, and Smart [8]):

$$C/\mathbf{F}_q : Y^a = \sum_{i=0}^{b} \alpha_i X^i \ ,$$

where $\alpha_i \in \mathbf{F}_q$, $\alpha_b \neq 0$, $\gcd(a, q) = \gcd(a, b) = 1$. And the curve is assumed to be nonsingular as an affine curve. In particular, $a = 2$ implies a hyperelliptic curve, and $a = 2, b = 3$ implies an elliptic curve.

It is known that superelliptic curves have only one point at infinity, which is a $\mathbf{F}_q$-rational point [8]. Then, the Jacobian group is isomorphic to the ideal class group of the coordinate ring. We utilize this fact to implement the Jacobian group arithmetic efficiently (each divisor being represented as a fractional ideal).

In order to perform the arithmetic on the ideal class group of a coordinate ring, we need to find a representative of each class. To solve the problem, we should compute:

1. the inverse ideal I^{-1} for a given ideal I; and
2. the minimal element of a given ideal with respect to the pole order at the infinity place.

For a superelliptic curve $C/\mathbf{F}_q : Y^a = \sum_{i=0}^{b} \alpha_i X^i$, we can solve the first problem by computing the product of the conjugate ideals over $\mathbf{F}_q(x, y)/\mathbf{F}_q(x)$, where $x \equiv X \pmod{C}$ and $y \equiv Y \pmod{C}$, which can be computed easily, since the conjugate elements of y are $\rho^i y$ $(0 \leq i \leq a-1)$, where ρ is a primitive a-th root of unity [8]. However, we must extend the base field if $\rho^i \notin \mathbf{F}_q$, and it seems unclear how to compute a conjugate element in more general curves. Considering the second problem, we can represent an integral ideal of the coordinate ring as a lattice in $(\mathbf{F}_q[x])^a$ over $\mathbf{F}_q[x]$. Then we can solve the problem by applying Paulus' lattice basis reduction method [15], which is a method for finding a minimal element of a given lattice with respect to the degree of x. As a result, Galbraith et. al's method [8] computes Jacobian group arithmetic on superelliptic curves in $O(g^2 \log^2 q)$ bit-operations when the size of a is fixed.

In this thesis, we describe Jacobian group arithmetic on more general curves than superelliptic curves. More precisely, we consider the Jacobian group (i.e., the group of divisor classes of degree zero) on a class of algebraic function fields that contain function fields associated with superelliptic curves.

We consider the following function field $F/\mathbf{F}_q$:

1. there exists at least one place of degree one, denoted by P;
2. the set of pole numbers of P is generated by t elements $\mathbf{A}_t = \{a_1, \cdots, a_t\}$,

where we choose such an a_1 as $\gcd(a_1, q) = 1$. There exists such an a_1, since the fact that the genus is bounded implies $\gcd(a_1, \cdots, a_t) = 1$.

For such function fields, S. Miura [14] gave a non-singular affine model (definition equations) in t variables with only one point at infinity which is a $\mathbf{F}_q$-rational point and corresponds to the given place P. In this thesis, we call such curves "$\mathbf{A}_t$-*curves* ". And, as in superelliptic curves, it turns out that the Jacobian group is isomorphic to the ideal class group of the coordinate ring . Therefore, we

consider the arithmetic on the Jacobian group as that on the ideal class group of the coordinate ring. Note that, unlike superelliptic curves, there may be more than one definition equation.

This thesis proposes an algorithm for realizing Jacobian group arithmetic on $\mathbf{A}_t$-curves, which gives a generalization of Cantor's algorithm in hyperelliptic curve case.

There are two problems described above for performing arithmetic on ideal class of the coordinate ring. First, we can compute the inverse ideal, given an ideal, by modifying a method in number fields different from Galbraith et. al's method. And for the second, we can apply modified Paulus' lattice basis reduction method same as a superelliptic curve case. This proposed method is performed in $O(g^2 \log^2 q)$ bit-operations when a_1 is fixed. Furthermore, when it is restricted to superelliptic curves, this method is more efficient than Galbraith et. al's method.

Finally, we note that S.Arita [1] proposed a method for performing Jacobian group arithmetic on $\mathbf{A}_t$-curves by using Gröbner basis. However, it requires the so-called Buchberger algorithm that computes the reduced Gröbner basis and operations on a polynomial ring in t variables, which is hard to evaluate the complexity. Even in his heuristic analysis, the method takes $O(g^3 \log^2 q)$ bit-operations. On the other hand, our method involves only operations on a polynomial ring of one variable over the base field.

This thesis is organized as follows: Chapters 2 and 3 summarize the basic materials from complexity theory, $\mathbf{Z}$-modules and algebraic number theory and algebraic function field and affine variety, which will be used in this thesis. In Chapter 4, we introduce the definition and some properties of $\mathbf{A}_t$-curves. In Chapter 5, we describe an algorithm for performing Jacobian group arithmetic on $\mathbf{A}_t$-curves. In Chapter 6, we propose a method for realizing the algorithm. In Chapter 7, we evaluate the complexity of the proposed method.

Finally, in Appendix, several implementational results of the proposed method for $\mathbf{A}_t$-curves and superelliptic curves of an actual scale used in algebraic curve cryptography are shown.

Chapter 2

Preliminaries

In this chapter, we describe some results to which will be referred in this thesis. $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ denote the *natural numbers, the integers, the rational numbers, the real numbers, the complex numbers*, respectively. And $\log x$ denotes the *logarithm of x to the base* 2.

2.1 Complexity Theory

In this section, we describe some definitions and properties from complexity theory, which is needed to evaluate the time complexity of an algorithm.

Definition 1 *An algorithm is a computer program written in some specific programming language for a specific computer that takes a variable input and halts with an output.*

An algorithm may be defined from other terms, such as Turing machines, Boolean circuits, etc. However, we adopt the above definition for algorithms since it is easier to analyze the time complexity and it is often the case in dealing with mathematical computational problems.

It is usually of interest to find the most efficient algorithm for solving a given computational problem. In order to give the precise definition of "efficient algorithm", we first define the size of the input and the unit of time used in analyzing algorithms.

Definition 2 *The size of the input is the total number of bits needed to represent the input in ordinary binary notation using an appropriate encoding scheme.*

Definition 3 *The running time of an algorithm on a particular input is the number of specified "operations" executed. The "operation" is usually taken to mean bit/word operations, but sometimes it will be more convenient to take "operations" to mean something else such as a modular multiplication, a multiplication in a finite field, etc.*

Example 1

1. *The number of bits in the binary representation of a positive integer n is $1 + \lfloor \log n \rfloor$ bits, where $\lfloor \log n \rfloor$ is the largest integer less than or equal to $\log n$. For simplicity, the size of n will be approximated by $\log n$.*

2. *If f is a polynomial of degree k, each coefficient being a non-negative integer at most n, then the size of f is $(k+1)\log n$ bits.*

3. *If A is a matrix with r rows, s columns, and with non-negative integer entries each at most n, then the size of A is $rs \log n$ bits.*

In estimating time complexity of algorithms, the running time is estimated by counting the unit of time, i.e. "operations" which we adopt, and is expressed as functions which take variable input sizes. However, it is often difficult to derive the exact running time of algorithms. Therefore, in complexity theory, one is forced to settle for deriving the asymptotic behavior of the functions which express the running time. This concept explains how the running time of the algorithm increases as the size of the input increases without bound.

Definition 4 (Asymptotic upper bound) *Let $f(n)$, $g(n)$ be functions defined on the positive integers n that take on positive real values.*

Then, we define $f(n) = O(g(n))$ if there exists a positive constant c and a positive integer n_0 such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0$.

Now, we describe several fundamental properties of the above order notation.

Proposition 1 *Let $f(n)$, $g(n)$, $h(n)$ and $l(n)$ be functions defined on the positive integers n that take on positive real values. Then, the following are true.*

1. *If $f(n) = O(h(n))$ and $g(n) = O(h(n))$, then $(f+g)(n) = O(h(n))$.*
2. *If $f(n) = O(h(n))$ and $g(n) = O(l(n))$, then $(f \cdot g)(n) = O(h(n)l(n))$.*
3. *$f(n) = O(f(n))$.*
4. *If $f(n) = O(g(n))$ and $g(n) = O(h(n))$, then $f(n) = O(h(n))$.*

In this thesis, we estimate (time) complexity as a usual method. Namely, we apply the following result.

Proposition 2 *Let $\mathbf{F}_q$ denote a finite field with q elements.*

1. *One operation (addition/subtraction/multiplication/division) on $\mathbf{F}_q$ takes $O(\log^2 q)$ bit-operations.*
2. *Let $f(x),\ g(x) \in \mathbf{F}_q[x]$ be two polynomials of degrees at most n. Then the multiplication of $f(x)$ and $g(x)$ takes $O(n^2 \log^2 q)$ bit-operations.*

2.2 Z-modules

In this section, we describe the Hermite normal form and the Smith normal form, Elementary divisor theorem related to **Z**-modules. And we notice that their results are valid for finitely generated (torsion) free modules over a principal ideal domain (**PID**). Therefore, there are many applications to number theory and algebraic function field, which will play very important roles in this thesis. For more details, see [4].

Definition 5 (Hermite Normal Form (HNF)) *We say that an $m \times n$ matrix $A = (a_{i,j})$ with **Z**-coefficients is in Hermite normal form* (HNF) *if there exists $r \leq n$ and a strictly increasing map g from $[r+1,\ n]$ to $[1,\ m]$ satisfying the following properties:*

1. *for* $r+1 \leq j \leq n$, $a_{g(j),j} > 0$, $a_{i,j} = 0$ *if* $i > g(j)$; *and* $0 \leq a_{g(k),j} < a_{g(k),k}$ *if* $k < j$;

2. *the first* r *columns of* A *are equal to* 0.

Theorem 1 *Let* $A = (a_{i,j})$ *be an* $m \times n$ *matrix with* $\mathbf{Z}$*-coefficients. Then, there exists a unique* $m \times n$ *matrix* B *in* HNF *of the form* $B = AU$ *with* $U \in \mathrm{GL}_n(\mathbf{Z})$, *where* $\mathrm{GL}_n(\mathbf{Z})$ *is the group of* $n \times n$ *matrices with* $\mathbf{Z}$*-coefficients which are invertible, i.e. whose determinant is equal to* ± 1.

In this thesis, we call the matrix consisting of the last $n-r$ columns *the HNF of* A.

When we compute an HNF directly, i.e. the method of performing elementary operations on columns, it is hard to evaluate its complexity since we don't know how large the size of an integer grows during the process. However, in the case of $\mathbf{Z}$-coefficients and $\mathrm{rank}(A) = m$, if we know the value D that is a multiple of the determinant of the $\mathbf{Z}$-module $L(A)$ generated by the columns of A, i.e. the determinant of the HNF of A, then we can compute the HNF of A by using D, which involves only operations modulus D [4]:

Algorithm 1 (HNF Modulo D)

Input: $m \times n$ *matrix* $A = (a_{i,j})$ *with* $\mathbf{Z}$*-coefficients of rank* m,
$D \longleftarrow$ *a multiple of determinant of the* $\mathbf{Z}$*-module generated by the columns of* A, *where* A_i *denotes column of* A.

Output: *The HNF matrix* $W = (w_{i,j})$.

Step 1: *Set* $i \leftarrow m$, $j \leftarrow n$, $k \leftarrow n$, $R \leftarrow D$;

Step 2: *if* $j = 1$ *go to step 4;*
otherwise, set $j \leftarrow j-1$, *and if* $a_{i,j} = 0$ *go to Step 2;*

Step 3: *compute* (u, v, d) *such that* $ua_{i,k} + va_{i,j} = d = \gcd(a_{i,k}, a_{i,j})$, *using Euclid's extended algorithm;*
$B \leftarrow uA_k + vA_j$;
$A_j \leftarrow ((a_{i,k}/d)A_j - (a_{i,j}/d)A_k) \bmod R$;
$A_k \leftarrow B \bmod R$;
and go to Step 2;

Step 4 *compute* (u, v, d) *such that* $ua_{i,k} + vR = d = \gcd(a_{i,k}, R)$*;*
$W_i \leftarrow uA_k \bmod R$ *(if* $w_{i,i} = 0$*, then* $w_{i,i} \leftarrow R$*);*
if $i < m$*, then ,for* $j = i+1, \cdots, m$*, we set*
$q \leftarrow \lfloor w_{i,j}/w_{i,i} \rfloor$*; and*
$W_j \leftarrow W_j - qW_i$*;*

Step 5 *if* $i = 1$*, output* $W = (w_{i,j})$*;*
otherwise,
$R \leftarrow R/d$*;*
$i \leftarrow i-1$*,* $k \leftarrow k-1$*,* $j \leftarrow k$*;*
and if $a_{i,k} = 0$*, then* $a_{i,k} \leftarrow R$*, go to Step 2.*

This algorithm requires $O(m^2 n \log^2 |D|)$-bit operations [4].

Definition 6 (Smith Normal Form (SNF)) *We say that an* $n \times n$ *matrix* $A = (a_{i,j})$ *with* $\mathbf{Z}$*-coefficients is in Smith normal form* (SNF) *if* A *is a diagonal matrix with non-negative integer coefficients such that* $a_{i+1,i+1} | a_{i,i}$ *for all* $i < n$*.*

Theorem 2 (Elementary divisors) *Let* A *be an* $n \times n$ *matrix with* $\mathbf{Z}$*-coefficients and non-zero determinant. Then, there exists a unique matrix in SNF* $B = (b_{i,j})$ *such that* $B = VAU$ *with* U *and* V *elements of* $\mathrm{GL}_n(\mathbf{Z})$*. When we set* $d_i = b_{i,i}$*, the* d_i *are said to be the elementary divisors of* A*.*

The above theorem, stated for matrices, is equivalent to the following theorem for $\mathbf{Z}$-modules.

Theorem 3 (Elementary divisor theorem) *Let* L *be a* $\mathbf{Z}$*-submodule of a free module* L' *and of the same rank, denoted by* n*. Then there exist positive integers* $d_1, \cdots, d_n$ *(called the elementary divisors of* L *in* L'*), uniquely determined by* L *and* L'*, satisfying the following conditions:*

1. *For every* i *such that* $1 \leq i < n$*, we have* $d_{i+1} | d_i$*.*
2. *As* $\mathbf{Z}$*-module, we have the isomorphism*
$$L'/L \simeq \bigoplus (\mathbf{Z}/d_i\mathbf{Z}),$$
and in particular $[L' : L] = \prod d_i$ *and* d_1 *is the exponent of* L'/L*, i.e.* $d_1 L' \subseteq L$*.*

3. *There exsists a* $\mathbf{Z}$*-basis* $\{u_1, \cdots, u_n\}$ *of* L' *such that* $\{d_1u_1, \cdots, d_nu_n\}$ *is a* $\mathbf{Z}$*-basis of* L*.*

Finally, we give some results on a change of bases for $\mathbf{Z}$-module.

Lemma 1 *Let* L' *be a free* $\mathbf{Z}$*-module of rank* n*, and* $\{w_1, \cdots, w_n\}$*,* $\{u_1, \cdots, u_n\}$ *two* $\mathbf{Z}$*-bases of* L'*. Then there exists an* $n \times n$ *matrix* M *in* $\mathrm{GL}_n(\mathbf{Z})$ *such that* $[w_1, \cdots, w_n] = [u_1, \cdots, u_n]M$*.*

Theorem 4 *Let* L *be a* $\mathbf{Z}$*-submodule of a free module* L' *and of the same rank* n*. Let* $[w_1, \cdots, w_n]A$ *be a* $\mathbf{Z}$*-basis of* L*, where* $\{w_1, \cdots, w_n\}$ *is a* $\mathbf{Z}$*-basis of* L' *and* A *is an* $n \times n$ *matrix with* $\mathbf{Z}$*-coefficients. Then there exist a* $\mathbf{Z}$*-basis of* L' $\{u_1, \cdots, u_n\}$ *and* M *in* $\mathrm{GL}_n(\mathbf{Z})$ *such that*

$$[w_1, \cdots, w_n]A = [u_1, \cdots, u_n]MA = [u_1, \cdots, u_n] \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \vdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & d_n \end{bmatrix}$$

with $d_{i+1}|d_i$*. And* $|\det A| = |\prod d_i|$ *holds.*

Remark 1 *The above results are valid for finitely generated (torsion) free modules over a* **PID***.*

2.3 Algebraic Number Theory

There are many analogy between algebraic number fields and algebraic function fields of one variable over finite fields. In this section, we summarize some results needed in this thesis, in particular, the theory concerning the ring of algebraic integers of a number field. For more detail, see [2] [7] [12]. (All results given in this section are cited from the references.)

Let K be a number field, i.e. a finite extension field of the rational numbers $\mathbf{Q}$. And let $\mathbf{Z}_K$ denote the ring of algebraic integers of K, which is finitely generated as $\mathbf{Z}$-module of rank $[K : \mathbf{Q}]$ (the extension degree). If $I \neq (0)$ is an integral ideal of $\mathbf{Z}_K$ in K, i.e. $I \subseteq \mathbf{Z}_K$, then I is of rank $[K : \mathbf{Q}]$ as a $\mathbf{Z}$-module.

$I \subseteq K$ is a *fractional ideal of* $\mathbf{Z}_K$ *in* K if I is a $\mathbf{Z}_K$-module such that there exists a $c(\neq 0) \in \mathbf{Z}_K$ for which $cI \subseteq \mathbf{Z}_K$. For a fractional ideal I of $\mathbf{Z}_K$, when we set $J := \{x \in K \mid xI \subseteq \mathbf{Z}_K\}$, which forms a fractional ideal, we say I is *invertible* if $IJ = \mathbf{Z}_K$. Then J is said to be the *inverse ideal of* I, denoted by I^{-1}.

Definition 7 *An integral domain $\mathcal{O}$ is a Dedekind domain if*

1. *$\mathcal{O}$ is a Noetherian ring;*
2. *$\mathcal{O}$ is integrally closed in its field of fractions; and*
3. *all non-zero prime ideals of $\mathcal{O}$ are maximal ideals.*

It is well known that a **PID** and $\mathbf{Z}_K$, for every number field K, are Dedekind domains. More generally, if F is a finite separable extension of the field of fractions K of a Dedekind domain $\mathcal{O}$, then the integral closure of $\mathcal{O}$ in F is a Dedekind domain.

Now, we summarize some results on a Dedekind domain $\mathcal{O}$ with its field of fractions K.

Theorem 5 *For a Dedekind domain $\mathcal{O}$,*

1. *every non-zero fractional ideal of $\mathcal{O}$ is invertible;*
2. *every non-zero fractional ideal of $\mathcal{O}$ has a unique factorization as a product of prime ideals;*
3. *all non-zero prime ideals of $\mathcal{O}$ are maximal ideals.*

Then, the set of non-zero fractional ideals of $\mathcal{O}$ forms a group with respect to multiplication, which is said to be the *group of ideal of* $\mathcal{O}$, denoted by $I(\mathcal{O})$. And the *group of principal fractional ideals* $\{(u) \mid u \in K^*\}$ of $\mathcal{O}$, denoted by $\mathcal{P}(\mathcal{O})$, forms a subgroup of $I(\mathcal{O})$. We define the *ideal class group of* $\mathcal{O}$, denoted by $Cl(\mathcal{O})$, as the quotient group

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

Next, we define *trace* and *norm*. Now we suppose that F/K is a finite separable extension of degree n.

Definition 8 *Let $F^{(i)}$ $(i = 1, \cdots, n)$ are conjugate fields of F over K, and let $\{w_1, \cdots, w_n\}$ be a basis of F/K. For $\alpha \in F$, we set $\alpha[w_1, \cdots, w_n] = [w_1, \cdots, w_n]A(\alpha)$, where $A(\alpha) = (a_{i,j})$ is an $n \times n$ matrix with F-coefficients.*

Then we define the trace of α, denoted by $\mathrm{Tr}_{F/K}(\alpha)$, and the norm of α, denoted by $\mathrm{N}_{F/K}(\alpha)$, as follows:

$$\mathrm{Tr}_{F/K}(\alpha) := \mathrm{Tr}(A(\alpha)) = \sum a_{i,i}, \quad \mathrm{N}_{F/K}(\alpha) := \mathrm{N}(A(\alpha)) = \det(A(\alpha)).$$

Note that the values of trace and norm do not depend on choice of bases of F/K.

Then, the following theorem holds:

Theorem 6 *For $\alpha \in F$, let $\alpha^{(i)}$ $(i = 1, \cdots, n)$ be the conjugate elements of α over K. Then, we have*

$$\mathrm{Tr}_{F/K}(\alpha) = \sum \alpha^{(i)}, \quad \mathrm{N}_{F/K}(\alpha) = \prod \alpha^{(i)}. \tag{2.1}$$

Definition 9 *Let $I \neq (0)$ be an ideal of $\mathbf{Z}_F$, and $I^{(1)}, \cdots, I^{(n)}$ the conjugate ideals of I over K. We define the relative norm of I, denoted by $N_{F/K}(I)$, as $\prod I^{(i)}$ (product of the conjugate ideals). Then $N_{F/K}(I)$ is an extension of an ideal of $\mathbf{Z}_K$ to $\mathbf{Z}_F$.*

Definition 10 *For $\alpha \in F$, let $\alpha^{(1)}, \cdots, \alpha^{(n)}$ be the conjugate elements over K. We define*

$$d(\alpha_1, \cdots, \alpha_n) := \begin{vmatrix} \alpha_1^{(1)} & \cdots & \alpha_n^{(1)} \\ \vdots & \vdots & \vdots \\ \alpha_1^{(n)} & \cdots & \alpha_n^{(n)} \end{vmatrix}^2$$

for $\alpha_1, \cdots \alpha_n \in F$.

Theorem 7 *Let $I \neq (0)$ be a fractional ideal of $\mathbf{Z}_F$. Then there exist fractional ideals $J_1, \cdots, J_n$ of $\mathbf{Z}_K$ and a basis $\{\gamma_1, \cdots, \gamma_n\}$ of F/K such that*

$$I = J_1\gamma_1 \oplus \cdots \oplus J_n\gamma_n \quad \text{as } \mathbf{Z}_K\text{-module.}$$

Furthermore, $(J_1 \cdots J_n)^2(d(\gamma_1, \cdots, \gamma_n))$, an ideal of $\mathbf{Z}_K$, does not depend on the choice of $\{J_i\}_i$ and $\{\gamma_i\}_i$, and is denoted by $d(I)$.

Theorem 8 *If* $\mathbf{Z}_K$ *is a* **PID**, *then there exists a basis of* F/K $\{\gamma_1, \cdots, \gamma_n\}$ *such that*

$$\mathbf{Z}_F = \mathbf{Z}_K\gamma_1 \oplus \cdots \oplus \mathbf{Z}_K\gamma_n \quad \textit{as } \mathbf{Z}_K\textit{-module.}$$

The following theorem gives a relation between $d(I)$, as in Theorem 7, and a relative norn $N_{F/K}(I)$.

Theorem 9

$$d(I) = (N_{F/K}(I))^2 d(\mathbf{Z}_F)$$

for every ideal I *of* $\mathbf{Z}_F$.

Chapter 3

Algebraic Function Fields

This chapter includes several results on algebraic function fields that will be used in the following chapters. All results given in this chapter, except for Corollary 5, are cited from [10], [17] and [19].

3.1 Algebraic Function Field

In this section, K denotes an arbitrary field.

Definition 11 *An algebraic function field F/K of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K.*

From now on, we simply refer to F/K as a *function field*. The set $\tilde{K} := \{z \in F \mid z \text{ is algebraic over } K\}$, a subfield of F, is said to be the *field of constants* of F/K. And we say that K is the *full constant field of F* if $\tilde{K} = K$.

Definition 12 *A valuation ring of a function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties:*

1. *$K \subseteq \mathcal{O} \subseteq F$ and $\mathcal{O} \neq K,\ F$;*
2. *for any $z \in F$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

We describe some properties of a valuation ring.

Theorem 10 *Let $\mathcal{O}$ be a valuation ring of a function field F/K. Then*

1. *$\mathcal{O}$ is a local ring, i.e. $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O} \backslash \mathcal{O}^*$, where $\mathcal{O}^* := \{z \in \mathcal{O} \mid$ there exists a $w \in \mathcal{O}$ such that $zw = 1\}$ is the group of units of $\mathcal{O}$;*
2. *for $0 \neq x \in F$, $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$;*
3. *for the field of constants $\tilde{K}$, we have $\tilde{K} \subseteq \mathcal{O}$ and $\tilde{K} \cap P = \{0\}$.*

Theorem 11 *Let $\mathcal{O}$ is a valuation ring of a function field F/K and P its unique maximal ideal. Then*

1. *P is a principal ideal;*
2. *if we set $P = t\mathcal{O}$ for some $t \in F$, then any $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbf{Z}$ and $u \in \mathcal{O}^*$. And t is said to be a local parameter (or uniformizing variable) for P;*
3. *$\mathcal{O}$ is a* **PID**. *More precisely, if $P = t\mathcal{O}$ and $\{0\} \neq I \subseteq \mathcal{O}$ is an ideal then $I = t^n\mathcal{O}$ for some $n \in \mathbf{N}$.*

Definition 13
1. *A place P of a function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K.*
2. *$\mathbf{P}_F := \{P \mid P$ is a place of $F/K\}$.*

If $\mathcal{O}$ be a valuation ring of F/K and P its maximal ideal, then $\mathcal{O}$ is uniquely determined by P, i.e. $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$. Hence, $\mathcal{O}_P := \mathcal{O}$ is said to be the *valuation ring of the place P*.

Definition 14 *A discrete valuation of F/K is a function $v: F \to \mathbf{Z} \cup \{\infty\}$ with the following properties:*

1. *$v(x) = \infty \Leftrightarrow x = 0$;*
2. *$v(xy) = v(x) + v(y)$ for any $x, y \in F$;*
3. *(Triangle Inequality) $v(x+y) \geq \min\{v(x),\ v(y)\}$ for any $x, y \in F$;*
4. *there exists an element $z \in F$ with $v(z) = 1$;*

5. *$v(a) = 0$ for any $a \in K \setminus \{0\}$.*

Lemma 2 (Strict Triangle Inequality) *Let v be a discrete valuation of F/K and $x, y \in F$ two elements with $v(x) \neq v(y)$. Then $v(x+y) = \min\{v(x),\ v(y)\}$ holds.*

Now we associate a function $v_P :\ F \to \mathbf{Z} \cup \{\infty\}$ to every place P of F/K as follows: Let t be a local parameter for P. Then every $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ with $n \in \mathbf{Z}$ and $u \in \mathcal{O}^*$. We define $v_P(z) = n$ and $v_P(0) = \infty$.

Theorem 12 1. *For every place $P \in \mathbf{P}_F$, the function v_P defined above is a discrete valuation of F/K. Moreover, we have*

$$\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\},$$

$$\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\},$$

$$P = \{z \in F \mid v_P(z) > 0\}.$$

And $x \in F$ is a local parameter for $P \Leftrightarrow v_P(x) = 1$.

2. *Conversely, suppose that v is a discrete valuation of F/K. Then the set $P := \{z \in F \mid v(z) > 0\}$ is a place of F/K, and $\mathcal{O}_P = \{z \in F \mid v(z) \geq 0\}$ is the corresponding valuation ring.*

Let P be a place of F/K and $\mathcal{O}_P$ its valuation ring. Since P is a maximal ideal, the residue class ring $\mathcal{O}_P/P$ is a field. For $x \in \mathcal{O}_P$, we define $x(P) \in \mathcal{O}_P/P$ to be the residue class of x modulo P, i.e. $x(P) = x + P = \{x + p \mid p \in P\}$, and we set $x(P) := \infty$ for $x \in F \setminus \mathcal{O}_P$. Then the residue class map $\mathcal{O}_P \to \mathcal{O}_P/P$ induces a canonical embedding of K into $\mathcal{O}_P/P$, since we have $K \subseteq \mathcal{O}_P$ and $K \cap P = \{0\}$.

Therefore, we shall always consider K as a subfield of $\mathcal{O}_P/P$ via this embedding. (Note that this argument also applies to $\tilde{K}$ instead of K.)

Definition 15 *Let $P \in \mathbf{P}_F$. Then*

1. *$F_P := \mathcal{O}_P/P$ is the residue class field of P. The map $x \mapsto x(P)$ from F to $F_P \cap \{\infty\}$ is said to be the residue class map with respect to P;*

2. $\deg P := [F_P : K]$ *is said to be the degree of* P.

The degree of a place is always finite; more precisely, the following holds:

Proposition 3 *If* P *is a place of* F/K *and* $0 \neq x \in P$, *then*

$$\deg P \leq [F : K(x)] < \infty.$$

Definition 16 *Let* $z \in F$ *and* $P \in \mathbf{P}_F$. *We say that* P *is a zero of* z *if* $v_P(z) > 0$; P *is a pole of* z *if* $v_P(z) < 0$. *If* $v_P(z) = m > 0$, *then* P *is a zero of* z *of order* m; *if* $v_P(z) = -m < 0$, *then* P *is a pole of* z *of order* m.

Corollary 1 *In a function field* F/K, *any element* $x \in F \setminus \{0\}$ *has only finitely many zeros and poles.*

3.2 Divisor Class Group

In this section, F/K *denotes a function field such that* K *is the full constant field of* F/K.

Definition 17 *The (additively written) free abelian group which is generated by the places of* F/K, *denoted by* $\mathcal{D}_F$, *is said to be the divisor group of* F/K.

The elements of $\mathcal{D}_F$ are said to be *divisors* of F/K. In other words, a divisor is a formal sum

$$D = \sum_{P \in \mathbf{P}_F} n_P P \text{ with } n_P \in \mathbf{Z} \text{ with allmost all } n_P = 0.$$

The *support* of D is defined by

$$\text{supp } D := \{P \in \mathbf{P}_F \mid n_P \neq 0\}.$$

A divisor of the form $D = P$ with $P \in \mathbf{P}_F$ is said to be a *prime divisor*. Two divisors $D = \sum_{P \in \mathbf{P}_F} n_P P$ and $D' = \sum_{P \in \mathbf{P}_F} n'_P P$ are added coefficientwise:

$$D + D' = \sum_{P \in \mathbf{P}_F} (n_P + n'_P) P.$$

The zero element of the divisor group $\mathcal{D}_F$ is the divisor

$$0 := \sum_{P \in \mathbf{P}_F} r_P P, \text{ all } r_P = 0.$$

For $Q \in \mathbf{P}_F$ and $D = \sum_{P \in \mathbf{P}_F} n_P P$, we set $v_Q(D) := n_Q$. Then we have

$$\text{supp } D = \{P \in \mathbf{P}_F \mid v_P(D) \neq 0\} \text{ and } D = \sum_{P \in \text{supp } D} v_P(D) \cdot P.$$

We define a partial ordering on $\mathcal{D}_F$ as follows:

$$D_1 \leq D_2 \Longleftrightarrow v_P(D_1) \leq v_P(D_2) \text{ for any } P \in \mathbf{P}_F.$$

And divisor D is said to be *positive* (or *effective*) if $D \geq 0$.

The *degree* of a divisor D is defined by

$$\deg(D) := \sum_{P \in \mathbf{P}_F} v_P(D) \cdot \deg P,$$

which yields a homomorphism $\deg : \mathcal{D}_F \to \mathbf{Z}$.

Definition 18 *Let $0 \neq x \in F$, and let $Z \subseteq \mathbf{P}_F$ (resp. $N \subseteq \mathbf{P}_F$) be the set of zeros (resp. poles) of x. Then we define*

$$(x)_0 := \sum_{P \in Z} v_P(x) P, \text{ the zero divisor of } x,$$

$$(x)_\infty := \sum_{P \in N} -v_P(x) P, \text{ the pole divisor of } x,$$

$$(x) := (x)_0 - (x)_\infty, \text{ the principal divisor of } x.$$

Clearly $(x)_0 \geq 0$, $(x)_\infty \geq 0$ and

$$(x) = \sum_{P \in \mathbf{P}_F} v_P(x) P.$$

The elements $0 \neq x \in F$ which are constant are characterized by

$$x \in K \Longleftrightarrow (x) = 0.$$

Theorem 13 *Any principal divisor has degree zero. More precisely: For $x \in F \setminus K$,*

$$\deg\ (x)_0 = \deg\ (x)_\infty = [F : K(x)].$$

Definition 19

$$\mathcal{P}_F := \{(x) \mid 0 \neq x \in F\ \}$$

is said to be the group of principal divisors of F/K. Then $\mathcal{P}_F$ forms a subgroup of $\mathcal{D}_F$, since we have $(xy) = (x) + (y)$ for $x, y \in F \setminus \{0\}$. The factor group

$$\mathcal{C}_F := \mathcal{D}_F / \mathcal{P}_F$$

is said to be the divisor class group of F/K.

For a divisor $D \in \mathcal{D}_F$, the corresponding element in the factor group $\mathcal{C}_F$ is denoted by $[D]$, called the *divisor class* of D. Two divisors $D, D' \in \mathcal{D}_F$ are said to be *equivalent*, denoted by $D \sim D'$, if $[D] = [D']$ holds, i.e. $D = D' + (x)$ for some $x \in F \setminus \{0\}$.

Definition 20 *We set $\mathcal{D}_F^0 := \{D \in \mathcal{D}_F \mid \deg(D) = 0\ \}$, which forms a subgroup of $\mathcal{D}_F$. Then $\mathcal{P}_F$ also forms a subgroup of $\mathcal{D}_F^0$. The factor group*

$$\mathcal{C}_F^0 := \mathcal{D}_F^0 / \mathcal{P}_F = \{[D] \in \mathcal{C}_F \mid \deg[D] = 0\ \}$$

is said to be the group of divisor classes of degree zero (or Jacobian group of F in terms of algebraic geometry, denoted by $J_K(F)$).

Definition 21 *For a divisor $A \in \mathcal{D}_F$, we define*

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\ \} \cup \{0\},$$

which is said to be the space of functions associated with the divisor A.

Remark 2 *Let $A \in \mathcal{D}_F$. Then*

$$\mathcal{L}(A) \neq 0 \Leftrightarrow \text{ there exists a divisor } A' \sim A \text{ with } A' \geq 0.$$

Lemma 3 *Let $A \in \mathcal{D}_F$. Then*

1. *$\mathcal{L}(A)$ is a vector space over K.*
2. *If $A \sim A'$, then $\mathcal{L}(A) \sim \mathcal{L}(A')$ (isomorphic as vector space over K).*
3. *$\mathcal{L}(0) = K$.*

4. *If* $A < 0$, *then* $\mathcal{L}(A) = \{0\}$.

For a K-vector space V , $\dim_K V$ denotes the dimension of V over K.

Lemma 4 *Let* A, B *be divisors of* F/K *with* $A \leq B$. *Then we have* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *and*

$$\dim_K \ (\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg \ B - \deg \ A.$$

Definition 22 *For* $A \in \mathcal{D}_F$, *the integer* $\dim \ A := \dim_K \mathcal{L}(A)$ *is said to be the dimension of* A.

Proposition 4 *Let* A, A' *be two divisors with* $A \sim A'$. *Then we have* $\dim \ A = \dim \ A'$ *and* $\deg \ A = \deg \ A'$.

Proposition 5 *There exists a constant* $\gamma \in \mathbf{Z}$ *such that*

$$\deg \ A - \dim \ A \leq \gamma \quad \textit{for all } A \in \mathcal{D}_F.$$

Definition 23 *The genus* g *of* F/K *is defined by*

$$g := \max\{\deg \ A - \dim \ A + 1 \mid A \in \mathcal{D}_F \ \},$$

which is a non-negative integer.

Theorem 14 (Riemann's Theorem) *Let* F/K *be a function field of genus* g.

1. *For any divisor* $A \in \mathcal{D}_F$,

$$\dim \ A \geq \deg \ A + 1 - g.$$

2. *There is an integer* c, *depending on* F/K, *such that*

$$\dim \ A = \deg \ A + 1 - g$$

whenever $\deg \ A \geq c$.

3.3 The Riemann-Roch Theorem

As before, F/K denotes a function field such that K is the full constant field of F/K and g the genus of F/K.

Definition 24 *For $A \in \mathcal{D}_F$,*

$$i(A) := \dim\ A - \deg\ A + g - 1$$

is said to be the index of speciality of A.

Definition 25 *An adele of F/K is a mapping*

$$\alpha : \begin{cases} \mathbf{P}_F & \to & F\ , \\ P & \mapsto & \alpha_P\ , \end{cases}$$

with $\alpha_P \in \mathcal{O}_P$ for almost all $P \in \mathbf{P}_F$.

We regard an adele as an element of the direct product $\prod_{P \in \mathbf{P}_F} F$, so we use the notation $\alpha = (\alpha_P)_{P \in \mathbf{P}_F}$ or, even shorter, $\alpha = (\alpha_P)$. The set

$$\mathcal{A}_F := \{\ \alpha \mid \alpha \text{ is an adele of } F/K\ \}$$

is said to be the *adele space* of F/K, which forms a vector space over K in the obvious manner.

The *principal adele* of an element $x \in F$ is the adele whose all components are equal to x. This gives an embedding $F \hookrightarrow \mathcal{A}_F$. Every discrete valuation v_P of F/K extends naturally to $\mathcal{A}_F$ by setting $v_P(\alpha) := v_P(\alpha_P)$, where α_P is the P-component of an adele α. By definition, we have $v_P(\alpha) \geq 0$ for almost all $P \in \mathbf{P}_F$.

Definition 26 *For $A \in \mathcal{D}_F$, we define*

$$\mathcal{A}_F(A) := \{\ \alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(A) \ \ \textit{for all } P \in \mathbf{P}_F\ \},$$

which forms a K-subspace of $\mathcal{A}_F$.

Definition 27 *A Weil differential of F/K is a K-linear map $\omega : \mathcal{A}_F \to K$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor $A \in \mathcal{D}_F$. We call*

$$\Omega_F := \{\ \omega \mid \omega \textit{ is a Weil differential of } F/K\ \}$$

the module of Weil differentials of F/K. For $A \in \mathcal{D}_F$, we define

$$\Omega_F(A) := \{\ \omega \in \Omega_F \mid \omega \textit{ vanishes on } \mathcal{A}_F(A) + F\ \}.$$

We regard Ω_F as a K-vector space in the obvious manner (indeed, if ω_1 vanishes on $\mathcal{A}_F(A_1)+F$ and ω_2 vanishes on $\mathcal{A}_F(A_2)+F$ then $\omega_1+\omega_2$ vanishes on $\mathcal{A}_F(A_3)+F$ for any divisor A_3 with $A_3 \leq A_1$ and $A_3 \leq A_1$, and $a\omega_1$ vanishes on $\mathcal{A}_F(A_1)+F$ for $a \in K$). Clearly $\Omega_F(A)$ is a subspace of Ω_F.

Definition 28 *For $x \in F$ and $\omega \in \Omega_F$, we define $x\omega : \mathcal{A}_F \to K$ by*

$$(x\omega)(\alpha) := \omega(x\alpha).$$

Then $x\omega$ is also a Weil differential of F/K. Indeed, if ω vanishes on $\mathcal{A}_F(A)+F$ then $x\omega$ vanishes on $\mathcal{A}_F(A+(x))+F$, which implies that Ω_F has the structure of a vector space over F.

Proposition 6 *Ω_F is a one-dimensional vector space over F.*

Now we attach a divisor to any Weil differential $\omega \neq 0$. We consider, fixed a ω, the set of divisors

$$M(\omega) := \{\ A \in \mathcal{D}_F \mid \omega \text{ vanishes on } \mathcal{A}_F(A)+F\ \}.$$

Lemma 5 *Let $0 \neq \omega \in \Omega_F$. Then there is a uniquely determined divisor $W \in M(\omega)$ such that $A \leq W$ for any $A \in M(\omega)$.*

Therefore, the following definition make sense by the above lemma.

Definition 29 *1. The divisor (ω) of a Weil differential $\omega \neq 0$ is the uniquely determined divisor of F/K satisfying*

(a) ω vanishes on $\mathcal{A}_F((\omega))+F$.

(b) If ω vanishes on $\mathcal{A}_F(A)+F$, then $A \leq (\omega)$.

2. For $0 \neq \omega \in \Omega_F$ and $P \in \mathbf{P}_F$, we define $v_P(\omega) := v_P((\omega))$.

3. A place P is said to be a zero (resp. pole) of ω if $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$). ω is said to be regular at P if $v_P(\omega) \geq 0$, and ω is said to be regular (or holomorphic) if it is regular at any $P \in \mathbf{P}_F$.

4. A divisor W is said to be a canonical divisor of F/K if $W = (\omega)$ for some $\omega \in \Omega_F$.

Proposition 7 *1. For $0 \neq x \in F$ and $0 \neq \omega \in \Omega_F$, we have $(x\omega) = (x) + (\omega)$.*

2. Any two canonical divisors of F/K are equivalent.

Theorem 15 (Riemann-Roch Theorem) *Let W be a canonical divisor of F/K. Then, for any $A \in \mathcal{D}_F$, we have*

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

Definition 30 *Let $P \in \mathbf{P}_F$. An integer $n \geq 0$ is said to be a pole number of P if there is an element $x \in F$ with $(x)_\infty = nP$. Otherwise, n is said to be a gap number of P.*

Clearly n is a pole number of P if and only if $\dim\ (nP) > \dim\ ((n-1)P)$. Moreover, the set of pole numbers of P is a sub-semigroup of the additive semigroup $\mathbf{N}$ (indeed, if $(x_1)_\infty = n_1P$ and $(x_2)_\infty = n_2P$, then x_1x_2 has the pole divisor $(x_1x_2)_\infty = (n_1+n_2)P$).

Theorem 16 (Weierstrass Gap Theorem) *Suppose that F/K has genus $g > 0$ and P is a place of degree one. Then there are exactly g gap numbers $i_1 < \cdots < i_g$ of P. Furthermore, we have*

$$i_1 = 1 \text{ and } i_g \leq 2g - 1.$$

3.4 Algebraic Extensions of Algebraic Function Field

In this section, F/K denotes a function field with full constant field K. And the field K is assumed to be perfect. Namely, all algebraic extensions of K are separable.

Definition 31 *1. A function field F'/K' is said to be an algebraic extension of F/K if $F' \supseteq F$ is an algebraic field extension and $K' \supseteq K$.*

2. An algebraic extension F'/K' of F/K is said to be a constant field extension if $F' = FK'$, the composite field of F and K'.

3. An algebraic extension F'/K' of F/K is said to be a finite extension if $[F' : F] < \infty$.

Definition 32 *Let F'/K' be an algebraic extension of F/K. A place $P' \in \mathbf{P}_{F'}$ is said to lie over $P \in \mathbf{P}_F$ if $P \subseteq P'$. We also say that P' is an extension of P or that P lies under P', and we write $P'|P$.*

Proposition 8 *Let F'/K' be an algebraic extension of F/K. Suppose that P (resp. P') is a place of F/K (resp. F'/K'), and let $\mathcal{O}_P \subseteq F$ (resp. $\mathcal{O}_{P'} \subseteq F'$) denote the corresponding valuation ring, v_P (resp. $v_{P'}$) the corresponding discrete valuation. Then the following assertions are equivalent:*

1. *$P'|P$.*
2. *$\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.*
3. *There exists an integer $e \geq 1$ such that $v_{P'}(x) = e \cdot v_P(x)$ for all $x \in F$.*

Moreover, if $P'|P$ then

$$P = P' \cap F \quad \text{and} \quad \mathcal{O}_P = \mathcal{O}_{P'} \cap F.$$

For this reason, P is also called the restriction of P' to F.

Definition 33 *Let F'/K' be an algebraic extension of F/K, and let $P' \in \mathbf{P}_{F'}$ be a place of F'/K' lying over $P \in \mathbf{P}_F$.*

1. *The integer $e(P'|P) := e$ with*

   $$v_{P'}(x) = e \cdot v_P(x) \text{ for any } x \in F$$

   is said to be the ramification index of P' over P. We say that $P'|P$ is ramified if $e(P'|P) > 1$, and $P'|P$ is unramified if $e(P'|P) = 1$.

2. *$f(P'|P) := [F'_{P'} : F_P]$ is said to be the relative degree of P' over P.*

Note that $f(P'|P)$ can be finite or infinite; the ramification index, however, is always a natural number.

Proposition 9 *Let F'/K' be an algebraic extension of F/K.*

1. *For any place $P' \in \mathbf{P}_{F'}$, there is exactly one place $P \in \mathbf{P}_F$ such that $P'|P$, i.e. $P = P' \cap F$.*

2. *Conversely, any place $P \in \mathbf{P}_F$ has at least one, but only finite many, extensions $P' \in \mathbf{P}_{F'}$.*

Definition 34 *Let F'/K' be an algebraic extension of F/K. For a place $P \in \mathbf{P}_F$, we define its conorm (with respect to F'/F) as*

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P',$$

where the sum runs over all places $P' \in \mathbf{P}_{F'}$ lying over P. The conorm map is extended to a homomorphism from $\mathcal{D}_F$ to $\mathcal{D}_{F'}$ by setting

$$\mathrm{Con}_{F'/F}(\sum n_P \cdot P) := \sum n_P \cdot \mathrm{Con}_{F'/F}(P).$$

The following theorem contains a summary of the most important properties of constant field extensions.

Theorem 17 *In an algebraic constant field extension $F' = FK'$ of F/K, the following holds:*

1. *F/F' is unramified (i.e., $e(P'|P) = 1$ for all $P \in \mathbf{P}_F$ and all $P' \in \mathbf{P}_{F'}$ with $P'|P$).*

2. *F'/K' has the same genus as F/K*

3. *For any divisor $A \in \mathcal{D}_F$, we have $\deg\ \mathrm{Con}_{F'/F}(A) = \deg\ A$.*

4. *For any divisor $A \in \mathcal{D}_F$,*

$$\dim\ \mathrm{Con}_{F'/F}(A) = \dim\ A.$$

   More precisely: Any basis of $\mathcal{L}(A)$ is a basis of $\mathcal{L}(\mathrm{Con}_{F'/F}(A))$, too. (Note that $\mathcal{L}(\mathrm{Con}_{F'/F}(A))$ is considered as a K'-vector space whereas $\mathcal{L}(A) \subseteq F$ is a K-vector space.)

5. *The residue class field $F'_{P'}$ of any place $P' \in \mathbf{P}_{F'}$ is the compositum $F_P K'$ of K' and the residue class field F_P, where $P = P' \cap F$.*

Let $\bar{K}$ be an algebraic closure of K. Then for any place $\bar{P} \in \mathbf{P}_{\bar{F}}$, we have deg $\bar{P} = [\bar{F}_{\bar{P}} : \bar{K}] = 1$, since every algebraic extension of $\bar{K}$ is $\bar{K}$. From the fact and the above theorem, we can obtain the following corollary.

Corollary 2 *Let $P \in \mathbf{P}_F$ be a place of F/K of degree r and $\bar{F} = F\bar{K}$ the constant field extension of F/K with an fixed algebraic closure $\bar{K}$ of K. Then*

$$\mathrm{Con}_{\bar{F}/F}(P) = \bar{P}_1 + \cdots + \bar{P}_r$$

with pairwise distinct places $\bar{P}_i \in \mathbf{P}_{\bar{F}}$.

3.5 Subrings of Function Fields

In this section, F/K denotes a function field with constant field K.

Definition 35 *A subring of F/K is a ring R such that $K \subseteq R \subseteq F$, and R is not a field.*

In particular, if R is a subring of F/K then $R \neq K,\ F$. Here are two typical examples:

1. $R = \mathcal{O}_P$ for some $P \in \mathbf{P}_F$.
2. $R = K[x_1, \cdots, x_n]$, where $x_1, \cdots, x_n \in F \setminus K$.

Definition 36 *For $\emptyset \neq S \subseteq \mathbf{P}_F$ with $S \neq \mathbf{P}_F$, let*

$$\mathcal{O}_S := \{\ z \in F \mid v_P(z) \geq 0 \ \ \textit{for all } P \in S\ \}$$

be the intersection of all valuation rings $\mathcal{O}_P$ with $P \in S$. Any ring $R \subseteq F$ which is of the form $R = \mathcal{O}_S$ for some $S \subseteq \mathbf{P}_F$ with $S \neq \emptyset,\ \mathbf{P}_F$ is said to be a holomorphy ring of F/K.

We describe some consequences.

Lemma 6 *1. Any valuation ring $\mathcal{O}_P$ is a holomorphy ring, i.e. $\mathcal{O}_P = \mathcal{O}_S$ with $S = \{P\}$.*

2. Any holomorphy ring $\mathcal{O}_S$ is a subring of F/K.

3. *For $P \in \mathbf{P}_F$ and $\emptyset \neq S \subseteq \mathbf{P}_F$ with $S \neq \mathbf{P}_F$, we have*

$$\mathcal{O}_S \subseteq \mathcal{O}_P \Leftrightarrow P \in S.$$

Consequently, $\mathcal{O}_S = \mathcal{O}_T \Leftrightarrow S = T$.

For a subring R of F/K, we define the *integral closure of R in F*, denoted by $ic_F(R)$, as

$$ic_F(R) := \{z \in F \mid z \text{ is integral over } R\ \}.$$

Proposition 10 *Let $\mathcal{O}_S$ be a holomorphy ring of F/K. Then*

1. *F is the quotient field of $\mathcal{O}_S$.*
2. *$\mathcal{O}_S$ is integrally closed.*

Theorem 18 *Let R be a subring of F/K and*

$$S(R) := \{P \in \mathbf{P}_F \mid R \subseteq \mathcal{O}_P\ \}.$$

Then the following holds:

1. *$\emptyset \neq S(R) \subseteq \mathbf{P}_F$, and $S(R) \neq \mathbf{P}_F$.*
2. *$ic_F(R) = \mathcal{O}_{S(R)}$. In particular, $ic_F(R)$ is an integrally closed subring of F/K with quotient field F.*

Corollary 3 *A subring R of F/K with quotient field F is integrally closed if and only if R is a holomorphy ring.*

Proposition 11 *Let $\mathcal{O}_S$ be a holomorphy ring of F/K. Then there is a 1-1 correspondence between S and the set of maximal ideals of $\mathcal{O}_S$, given by*

$$P \mapsto M_P := P \cap \mathcal{O}_S \text{ (for } P \in S).$$

Moreover, the map

$$\varphi : \begin{cases} \mathcal{O}_S/M_P & \to & F_P = \mathcal{O}_P/P\ , \\ x + M_P & \mapsto & x + P \end{cases}$$

is a K-isomorphism.

Therefore, we have $[\mathcal{O}_S/M_P : K] = [F_P : K] = \deg P$ for each $P \in S$.

Proposition 12 *Any holomorphy ring $\mathcal{O}_S$ is a Dedekind domain.*

3.6 The Hesse-Weil Theorem

Throughout this section, F denotes a function field of genus g whose constant field is a finite field $\mathbf{F}_q$ with q elements.

Proposition 13 *$\mathcal{C}_F^0$ is a finite group, where $\mathcal{C}_F^0 = \mathcal{D}_F^0/\mathcal{P}_F$ is the group of divisor classes of degree zero (Definition 20). Its order $h = h_F$ is said to be the class number of $F/\mathbf{F}_q$, i.e.*

$$h = h_F = \text{ord } \mathcal{C}_F^0.$$

Definition 37 *We set*

$$A_n := |\{ \ A \in \mathcal{D}_F \mid A \geq 0 \text{ and } \deg A = n \ \}|.$$

Then the power series

$$Z(t) := Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbf{C}[[t]]$$

is said to be the Zeta function of $F/\mathbf{F}_q$.

Definition 38 *The polynomial $L(t) := L_F(t) := (1-t)(1-qt)Z(t)$ is said to be the L-polynomial of $F/\mathbf{F}_q$.*

We summarize the properties of L-polynomial, which is important when we will study Jacobian group of $F/\mathbf{F}_q$.

Theorem 19 *1. $L(t) \in \mathbf{Z}[t]$ and $\deg L(t) = 2g$.*

2. (Functional equation) $L(t) = q^g t^{2g} L(1/qt)$.

3. $L(1) = h$, the class number of $F/\mathbf{F}_q$.

4. We set $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$. Then the following holds:

(a) $a_0 = 1$ and $a_{2g} = q^g$.

(b) $a_{2g-i} = q^{g-i} a_i$ for $0 \leq i \leq g$.

(c) $a_1 = N - (q-1)$, where N is the number of places $P \in \mathbf{P}_F$ of degree one.

5. *$L(t)$ factors in $\mathbf{C}[t]$ in the form*

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t). \tag{3.1}$$

Then the complex numbers $\alpha_1, \cdots, \alpha_{2g}$ are algebraic integers, and they can be arranged in such a way that $\alpha_i \alpha_{g+i} = q$ holds for $i = 1, \cdots, g$.

6. *If $L_r(t) := (1-t)(1-q^r t)Z_r(t)$ denotes the L-polynomial of the constant field extension $F_r = F\mathbf{F}_{q^r}$, then*

$$L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t), \tag{3.2}$$

where the α_i are given by (3.1).

For a function field $F/\mathbf{F}_q$ of genus g, we set

$$N := N(F) := |\{\ P \in \mathbf{P}_F \mid \deg\ P = 1\ \}| \ \text{ and}$$

$$N_r := N(F_r) = |\{\ P \in \mathbf{P}_{F_r} \mid \deg\ P = 1\ \}|,$$

where $F_r = F\mathbf{F}_{q^r}$ is the constant field extension of $F/\mathbf{F}_q$ of degree r.

Corollary 4 *For any $r \geq 1$,*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r,$$

where $\alpha_1, \cdots, \alpha_{2g} \in \mathbf{C}$ are the reciprocals of the roots of $L(t)$.

Theorem 20 (Hasse-Weil) *Let $\alpha_1, \cdots, \alpha_{2g} \in \mathbf{C}$ be the reciprocals of the roots of $L(t)$. Then*

$$|\alpha_i| = q^{1/2} \quad \text{for } i = 1, \cdots, 2g.$$

Corollary 5 *Let $F/\mathbf{F}_q$ be a function field of genus g and h_r the class number of $F_r = F\mathbf{F}_{q^r}$. Then we have*

$$(q^{r/2} - 1)^{2g} \leq h_r \leq (q^{r/2} + 1)^{2g}.$$

(**Proof of Corollary 5**)
Let $\alpha_1, \cdots, \alpha_{2g} \in \mathbf{C}$ be the reciprocals of the roots of $L(t)$. Then, we have $L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t)$ from (3.2) , and $|\alpha_i| = q^{1/2}$ for $i = 1, \cdots, 2g$ by Theorem 20. And we have $h_r = L_r(1) = \prod_{i=1}^{2g} |1-\alpha_i^r|$ (3 of Theorem 19). Therefore, the proof is completed, since $|\alpha_i| = q^{1/2}$ implies $q^{r/2} - 1 \leq |1 - \alpha_i^r| \leq q^{r/2} + 1$. $\square$

3.7 Affine Varieties

There are many analogy between function fields and affine varieties. In this section, we summarize some results on affine varieties concerning this thesis.

Let K be a perfect field and $\bar{K}$ a fixed algebraic closure of K.

Definition 39 *Affine n-space (over K) is the set of n-tuples*

$$\mathbf{A}^n = \mathbf{A}^n(\bar{K}) = \{P = (x_1, \cdots, x_n) \mid x_i \in \bar{K}\ \}.$$

Similarly, the set of K-rational points in $\mathbf{A}^n$ is the set

$$\mathbf{A}^n(K) = \{P = (x_1, \cdots, x_n) \mid x_i \in K\ \}.$$

Let $\bar{K}[X] = \bar{K}[X_1, \cdots, X_n]$ be a polynomial ring in n variables, and let $I \subseteq \bar{K}[X]$ be an ideal. To each such I, we associate a subset of $\mathbf{A}^n$

$$V_I := \{P \in \mathbf{A}^n \mid f(P) = 0 \text{ for all } f \in I\ \}.$$

Definition 40 *An (affine) algebraic set is any set of the form V_I. If V is an algebraic set, the ideal of V is given by*

$$I(V) = \{f \in \bar{K}[X] \mid f(P) = 0 \textit{ for all } P \in V\ \}.$$

An algebraic set V is defined over K if its ideal $I(V)$ can be generated by polynomials in $K[X]$. We denote it by V/K. If V is defined over K, the set of K-rational points of V is

$$V(K) = V \cap \mathbf{A}^n(K).$$

Remark 3 *Let V be an algebraic set. We consider the ideal*

$$I(V/K) = \{f \in K[X] \mid f(P) = 0 \text{ for all } P \in V\ \} = I(V) \cap K[X].$$

Then V is defined over K if and only if

$$I(V) = I(V/K)\bar{K}[X].$$

Definition 41 *An affine algebraic set V is said to be an (affine) variety if $I(V)$ is a prime ideal in $\bar{K}[X]$. (Note that if V is defined over K, it is not enough to check that $I(V/K)$ is prime in K[X].) Let V/K be a variety (i.e., V is a variety defined over K). Then the affine coordinate ring, denoted by $K[V]$, is defined by*

$$K[V] := K[X]/I(V/K).$$

It is an integral domain; and its quotient field, denoted by $K(V)$, is said to be the function field of V/K. Similarly $\bar{K}[V]$ and $\bar{K}(V)$ are defined by replacing K with $\bar{K}$.

Definition 42 *Let V be a variety. The dimension of V, denoted by* $\dim V$*, is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.*

Definition 43 *Let $V \subseteq \mathbf{A}^n$ be a variety, and $P \in V$. And let $f_1, \cdots, f_m \in \bar{K}[X]$ be a set of generators for $I(V)$. Then V is non-singular (or smooth) at P if the $m \times n$ matrix*

$$(\partial f_i/\partial X_j(P))_{1 \le i \le m, 1 \le j \le n}$$

has $\operatorname{rank} n - \dim V$*. If V is nonsingular at every point, then we say that V is non-singular (or smooth).*

Theorem 21 *Let V be a variety and $P \in V$. Then we define the ideal M_P of $\bar{K}[V]$ as*

$$M_P = \{f \in \bar{K}[V] \mid f(P) = 0\ \}.$$

Notice that M_P is a maximal ideal, since there exists an isomorphism

$$\bar{K}[V]/M_P \to \bar{K}, \qquad \text{given by } f \mapsto f(P).$$

Moreover, the quotient M_P/M_P^2 is a finite dimensional $\bar{K}$-vector space.

Proposition 14 *Let V be a variety. A point $P \in V$ is non-singular if and only if*

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

Theorem 22 *Let V be a variety. Then*

$$P \mapsto M_P$$

gives a 1-1 *correspondence between the points of V and the maximal ideals of $\bar{K}[V]$.*

Chapter 4

$\mathbf{A}_t$-curves

In this thesis, we consider the following algebraic function fields:

> $F/\mathbf{F}_q$ is an algebraic function field of one variable over a finite field $\mathbf{F}_q$ with a place P of degree one.

In this chapter, we introduce some results on such a function field [14].

From now on, we suppose that a function field $F/\mathbf{F}_q$ has a place P of degree one. And let g denote the genus of $F/\mathbf{F}_q$.

Lemma 7 $\mathbf{F}_q$ *is the full constant field of* $F/\mathbf{F}_q$.

(**Proof of Lemma 7**)
Let $\tilde{\mathbf{F}}_q$ be the field of constants of $F/\mathbf{F}_q$. Then we have $\tilde{\mathbf{F}}_q \subseteq \mathcal{O}_P/P$ from Theorem 10. Therefore, $\tilde{\mathbf{F}}_q = \mathbf{F}_q$ holds, since we have $[\mathcal{O}_P/P : \mathbf{F}_q] = \deg P = 1$. $\square$

Let M_P denote the set of pole numbers of P (Definition 30). We suppose that

> M_P is generated by t natural numbers $\mathbf{A}_t := (a_1, \cdots, a_t)$,
> i.e. $M_P = \langle a_1, \cdots, a_t \rangle = a_1\mathbf{Z}_{\geq 0} + \cdots + a_n\mathbf{Z}_{\geq 0}$,

where $\mathbf{Z}_{\geq 0}$ denotes non-negative integers, and that $(a_1, \cdots, a_t)$ is represented as a minimum generating system
(i.e., $a_i \notin \langle a_1, \cdots, a_{i-1}, a_{i+1}, \cdots, a_t \rangle$ for $1 \leq i \leq t$).

Now we suppose

$$\gcd(a_1, \mathrm{char}\ \mathbf{F}_q) = 1. \tag{4.1}$$

There exists such an a_1, since the fact that the genus g is finite implies $\gcd(a_1, \cdots, a_t) = 1$. Namely, there are exactly g gap numbers of P, which is equal to $\#(\mathbf{Z}_{\geq 0} \setminus M_P)$ (Theorem 16).

Let $x_i \in F$, for $1 \leq i \leq t$, be functions such that $(x_i)_\infty = a_i P$. Then the following result is known:

Lemma 8 *[14]*

$$\mathcal{L}(\infty P) = \mathbf{F}_q[x_1, \cdots, x_n],$$

where $\mathcal{L}(\infty P) := \bigcup_{m=0}^{\infty} \mathcal{L}(mP) = \bigcap_{Q \in \mathbf{P}_F \setminus \{P\}} \mathcal{O}_Q$.

(**Proof of Lemma 8**)
By the definition of x_i, we have $\mathcal{L}(\infty P) \supseteq \mathbf{F}_q[x_1, \cdots, x_n]$.

In order to prove the inclusion in the reverse direction, it is sufficient to show $\mathcal{L}(nP) \subseteq \mathbf{F}_q[x_1, \cdots, x_n]$ for all $n \in \mathbf{Z}_{\geq 0}$. And we can show the claim by induction on n, since we have $\dim_{\mathbf{F}_q}(\mathcal{L}((n+1)P)/\mathcal{L}(nP)) \leq \deg P = 1$ for each $n \geq 0$ (Lemma 4). $\square$

Therefore, for a polynomial ring in t variables $\mathbf{F}_q[X] = \mathbf{F}_q[X_1, \cdots, X_t]$, a mapping

$$\Theta : \left\{ \begin{array}{ccc} \mathbf{F}_q[X] & \rightarrow & \mathbf{F}_q[x_1, \cdots, x_n] = \mathcal{L}(\infty P) \ , \\ f(X_1, \cdots, X_t) & \mapsto & f(x_1, \cdots, x_t) \ , \end{array} \right.$$

gives a surjective homomorphism, which implies $\mathbf{F}_q[X]/\mathrm{Ker}\ \Theta \simeq \mathcal{L}(\infty P)$.

Now we define the following ordering on $(\mathbf{Z}_{\geq 0})^t$ so that we will determine Ker Θ.

Definition 44 ($\mathbf{A}_t$-order [14]) *For* $\mathbf{A}_t = (a_1, \cdots, a_t)$, *we define* $\Psi_{\mathbf{A}_t} : (\mathbf{Z}_{\geq 0})^t \longrightarrow \mathbf{Z}_{\geq 0}$ *as* $\Psi_{\mathbf{A}_t}(n_1, \cdots, n_t) := \sum_{i=1}^{t} a_i n_i$.

Then we say $\alpha >_{\mathbf{A}_t} \beta$ *for* $\alpha = (\alpha_1, \cdots, \alpha_t), \beta = (\beta_1, \cdots, \beta_t) \in (\mathbf{Z}_{\geq 0})^t$ *if one of the following two conditions holds:*

1. $\Psi_{\mathbf{A}_t}(\alpha_1, \cdots, \alpha_t) > \Psi_{\mathbf{A}_t}(\beta_1, \cdots, \beta_t)$ *, or*
2. $\Psi_{\mathbf{A}_t}(\alpha_1, \cdots, \alpha_t) = \Psi_{\mathbf{A}_t}(\beta_1, \cdots, \beta_t)$, $\alpha_1 = \beta_1, \cdots, \alpha_i = \beta_i, \alpha_{i+1} < \beta_{i+1}$ *for some* i $(0 \leq i < t)$. *Namely, the left-most nonzero entry in the vector* $(\alpha_1 - \beta_1, \cdots, \alpha_t - \beta_t)$ *is negative.*

In this thesis, we call the order $>_{\mathbf{A}_t}$ *the* $\mathbf{A}_t$*-order.*

Next, for $\mathbf{A}_t = (a_1, \cdots, a_t)$, we define two sets $\mathbf{B}(\mathbf{A}_t)$ and $\mathbf{V}(\mathbf{A}_t)$ as follows:

$$\begin{aligned}
\mathbf{B}(\mathbf{A}_t) &:= \{\text{the least } M \in (\mathbf{Z}_{\geq 0})^t \text{ with respect to } \mathbf{A}_t\text{-order} \\
&\quad \text{with } \Psi_{\mathbf{A}_t}(\mathrm{M}) = a \mid a \in \langle a_1, \cdots, a_t \rangle\}, \\
\mathbf{V}(\mathbf{A}_t) &:= \{\mathrm{L} \in (\mathbf{Z}_{\geq 0})^t \setminus \mathbf{B}(\mathbf{A}_t) \mid \mathrm{L}{=}\mathrm{M}{+}\mathrm{N}, \\
&\quad \mathrm{M} \in (\mathbf{Z}_{\geq 0})^t \setminus \mathbf{B}(\mathbf{A}_t),\ \mathrm{N} \in (\mathbf{Z}_{\geq 0})^t \Rightarrow \mathrm{N}{=}(0, \cdots, 0)\}.
\end{aligned}$$

Then, the following relation holds [14]:

$$(\mathbf{Z}_{\geq 0})^t \setminus \mathbf{B}(\mathbf{A}_t) = \mathbf{V}(\mathbf{A}_t) + (\mathbf{Z}_{\geq 0})^t. \tag{4.2}$$

Now, since $\Psi_{\mathbf{A}_t} : \mathbf{B}(\mathbf{A}_t) \longrightarrow \langle a_1, \cdots, a_t \rangle$ is bijective and $\dim_{\mathbf{F}_q} (\mathcal{L}((n+1)P)/\mathcal{L}(nP)) \leq \deg P = 1$ for each $n \geq 0$ (Lemma 4), the following lemma holds:

Lemma 9 *We set $x^m := \prod_i x_i^{m_i}$ for $m = (m_1, \cdots, m_t) \in (\mathbf{Z}_{\geq 0})^t$. Then*

$$\{x^m \mid m \in \mathbf{B}(\mathbf{A}_t)\ \}$$

is a $\mathbf{F}_q$-basis of $\mathcal{L}(\infty P)$.

Therefore, for each $\mathbf{M} \in (\mathbf{Z}_{\geq 0})^t \setminus \mathbf{B}(\mathbf{A}_t)$, there exists a relation such that

$$x^{\mathbf{M}} + \alpha_{\mathbf{L}} x^{\mathbf{L}} + \sum_{\mathbf{N} \in \mathbf{B}(\mathbf{A}_t), \Psi_{\mathbf{A}_t}(\mathbf{N}) < \Psi_{\mathbf{A}_t}(\mathbf{L})} \alpha_{\mathbf{N}} x^{\mathbf{N}} = 0, \tag{4.3}$$

where $\mathbf{L}$ is the unique $\mathbf{L} \in \mathbf{B}(\mathbf{A}_t)$ satisfying $\Psi_{\mathbf{A}_t}(\mathbf{M}) = \Psi_{\mathbf{A}_t}(\mathbf{L})$, and $\alpha_{\mathbf{L}}, \alpha_{\mathbf{N}} \in \mathbf{F}_q$ with $\alpha_{\mathbf{L}} \neq 0$.

Here, for such an relation (4.3) with each $\mathbf{M} \in (\mathbf{Z}_{\geq 0})^t \setminus \mathbf{B}(\mathbf{A}_t)$, we define

$$F_{\mathbf{M}} := X^{\mathbf{M}} + \alpha_{\mathbf{L}} X^{\mathbf{L}} + \sum_{\mathbf{N} \in \mathbf{B}(\mathbf{A}_t), \Psi_{\mathbf{A}_t}(\mathbf{N}) < \Psi_{\mathbf{A}_t}(\mathbf{L})} \alpha_{\mathbf{N}} X^{\mathbf{N}}, \tag{4.4}$$

where we denote $\prod_i X_i^{\mathbf{m}_i}$ by $X^{\mathbf{M}}$ for $\mathbf{M} = (\mathbf{m_1}, \cdots, \mathbf{m_t}) \in (\mathbf{Z}_{\geq 0})^t$.

It is obvious that $\{F_{\mathbf{M}} \mid \mathbf{M} \in (\mathbf{Z}_{\geq 0})^t \setminus \mathbf{B}(\mathbf{A}_t)\} \subseteq \mathrm{Ker}\ \Theta$. (For $f_1, \cdots f_n \in \mathbf{F}_q[X]$, $\{f_1, \cdots f_n\}$ denotes the ideal in $\mathbf{F}_q[X]$ generated by $f_1, \cdots f_n$.)

More precisely, we can obtain the following theorem from (4.2):

Theorem 23 ([14]) *With notation as above, we have*

$$\mathrm{Ker}\ \Theta = \{F_{\mathbf{M}} \mid \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\}.$$

Remark 4 *[14]*

In an algebraic constant field extension $\bar{F} = F\bar{\mathbf{F}}_q$, where $\bar{\mathbf{F}}_q$ denotes a fixed algebraic closure of $\mathbf{F}_q$, there are exactly one place $\bar{P}$ lying over P (i.e. $\bar{P}|P$) from Corollary 2. And the pole numbers of $\bar{P}$ coincides with those of P from Theorem 17. Therefore, for the surjective homomorphism $\bar{\Theta}:\ \bar{\mathbf{F}}_q[X] \to \mathcal{L}(\infty\bar{P})$, $\bar{\Theta}:\ \bar{f}(X_1, \cdots, X_t) \mapsto \bar{f}(x_1, \cdots, x_t)$, we have $\mathrm{Ker}\ \bar{\Theta} = (\mathrm{Ker}\ \Theta)\bar{\mathbf{F}}_q[X]$ *as an ideal of $\bar{\mathbf{F}}_q[X]$. And $\mathcal{L}(\infty\bar{P})$ is Dedekind domain, since $\mathcal{L}(\infty\bar{P})$ is a holomorphy ring (Definition 36).*

Therefore, the affine algebraic set $\{F_{\mathbf{M}} = 0 \mid \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\}$, corresponding to $\mathrm{Ker}\ \Theta$*, is a non-singular affine variety. And the coordinate ring is $\mathbf{F}_q[x_1, \cdots, x_t]$.*

In this thesis, we call the affine curve $\{F_{\mathbf{M}} = 0 |\ \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\}$ a *"$\mathbf{A}_t$-curve"* corresponding to $(F/\mathbf{F}_q, P)$. (By *(affine) curves*, we mean (affine) varieties of dimension one.) In particular, for $t = 2$ and $\mathbf{A}_t = (a, b)$, the corresponding curve is also said to be a *"C_{ab} curves"* [1] [9].

And it is known [14] that the genus of a $\mathbf{A}_t$-curve is given by

$$g = \#(\mathbf{Z}_{\geq 0} \setminus \mathbf{A}_t) = \sum_{i=0}^{a_1-1} \lfloor b_i/a_1 \rfloor, \tag{4.5}$$

where $b_i := \min\{b \in \langle a_2, \cdots, a_t\rangle \mid b \equiv i \pmod{a_1}\}$ and $\lfloor b_i/a_1 \rfloor := \max\{s \in \mathbf{Z} \mid s \leq b_i/a_1\}$. (Note that the value of (4.5) does not depend on choice of $a_1 \in \{a_1, \cdots, a_t\}$.)

Remark 5 ([14]) *If we define $\mathbf{T}(\mathbf{A}_t)$ as $\mathbf{T}(\mathbf{A}_t) := \mathbf{B}(\mathbf{A}_t) \cap \{0\} \times (\mathbf{Z}_{\geq 0})^{t-1}$, then we have $\mathbf{T}(\mathbf{A}_t) = \{\mathbf{M}(b_i) |\ 0 \leq i \leq a_1 - 1\}$ and $\#\mathbf{T}(\mathbf{A}_t) = a_1$, where b_i is the same as in (4.5) and $\mathbf{M}(b_i) \in (\mathbf{Z}_{\geq 0})^t$ is the minimal element $\mathbf{M} \in (\mathbf{Z}_{\geq 0})^t$ satisfying $\Psi_{\mathbf{A}_t}(\mathbf{M}) = b_i$ with respect to $\mathbf{A}_t$-order.*

Furthermore, the following relation holds:

$$\mathbf{V}(\mathbf{A}_t) \subseteq \mathbf{B}(\mathbf{A}_t) + \{(0, 1, \cdots, 0),\ (0, 0, 1, 0, \cdots, 0),\ \cdots, (0, \cdots, 0, 1)\}.$$

Remark 6 *[14] Conversely, for a minimum generating system* $\mathbf{A}_t = (a_1, \cdots, a_t)$ *with* $\gcd(a_1, \cdots, a_t) = 1$ *and* $\gcd(a_1, \mathrm{char}\mathbf{F}_q) = 1$*, we construct a polynomial* $F_{\mathbf{M}}$ *in* t *variables satisfying (4.4) for each* $\mathbf{M} \in \mathbf{V}(\mathbf{A}_t)$*. We suppose that* $\{F_{\mathbf{M}} = 0 \mid \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\}$ *is non-singular as an affine curve and is a Gröbner basis of the ideal generated by* $\{F_{\mathbf{M}} \mid \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\}$ *with respect to the* $\mathbf{A}_t$*-order. Then* $\{F_{\mathbf{M}} = 0 \mid \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\}$ *is a* $\mathbf{A}_t$*-curve with only one point at infinity, denoted by* P_∞*. And the function field is an algebraic function field of one variable over* $\mathbf{F}_q$ *with the place* P_∞ *of degree one, where we again denote the place corresponding to* P_∞ *by* P_∞*. Furthermore, we have* $(x_i)_\infty = a_i P_\infty$*,* $M_{P_\infty} = \langle a_1, \cdots, a_t \rangle$*, and* $\mathcal{L}(\infty P) = \mathbf{F}_q[x_1, \cdots, x_t]$ *(the coordinate ring), where we set* $x_i \equiv X_i \pmod{\{\ F_{\mathbf{M}} \mid \mathbf{M} \in \mathbf{V}(\mathbf{A}_t)\ \}}$*.*

Example 2 **($(4,5,6)$-Curve)** *Suppose* $\mathrm{char}\ \mathbf{F}_q \neq 2$*. Let* $C/\mathbf{F}_q$ *be a curve defined by two equations*

$$\begin{cases} Y^2 &= F(X)Z \\ Z^2 &= G(X) \end{cases}$$

with $\deg_X F(X) = 1$*,* $\deg_X G(X) = 3$*.*

If $F(X)$ *and* $G(X)$ *have no square roots and no common roots, then* $C/\mathbf{F}_q$ *has an only one point at infinity, denoted by* P*, and* $C/\mathbf{F}_q$ *is a* $(4,5,6)$*-curve corresponding to* $(\mathbf{F}_q(C), P)$*, where* $\mathbf{F}_q(C)$ *denotes the function field of* $C/\mathbf{F}_q$*.*

Example 3 **(C_{ab} curve)** *Suppose* $\gcd(a,b) = 1$ *and* $\gcd(\mathrm{char}\ \mathbf{F}_q, a) = 1$*. Then* C_{ab} *curve* $C/\mathbf{F}_q$ *is given as follows:*

$$C/\mathbf{F}_q : \sum_{0 \le i \le b, 0 \le j \le a, ai+bj \le ab} \alpha_{i,j} X^i Y^j = 0 \ , \tag{4.6}$$

where $\alpha_{i,j} \in K$*,* $\alpha_{b,0} \neq 0$*,* $\alpha_{0,a} \neq 0$*. Furthermore, the affine curve is non-singular.*

Therefore, $a = 2$ (resp. $a = 2$, $b = 3$) implies a hyperelliptic curve (resp. elliptic curve). And a superelliptic curve given in [8],

$$C/F_q : Y^a = \sum_{i=0}^{b} \alpha_i X^i \ ,$$

is the special case of C_{ab} curves.

Chapter 5

Jacobian Group Arithmetic on Algebraic Function Fields

> By *Jacobian group* $J_{\mathbf{F}_q}(F)$, we mean the group of divisor classes of degree zero $\mathcal{C}_F^0$ for a function field $F/\mathbf{F}_q$ (Definition 20).

In this chapter, we describe an algorithm for performing Jacobian group arithmetic on such an algebraic function field $F/\mathbf{F}_q$ as in Chapter 4. (P denotes the given place of degree one.) And let $C/\mathbf{F}_q$ be the corresponding $\mathbf{A}_t$-curve, and $\mathbf{F}_q(C)$ denotes the function field of $C/\mathbf{F}_q$. From now on, we often use the notation $\mathbf{F}_q(C)$ instead of $F/\mathbf{F}_q$ to describe more simply, since we have $F = \mathbf{F}_q(C)$.

At first, we can obtain a unique representative element in each class of Jacobian group by the following results:

Definition 45 *Let $\mathcal{D}_F^0 = \{D \in \mathcal{D}_F \mid \deg D = 0\}$. If $D \in \mathcal{D}_F^0$ is expressed as $E - nP$ such that $E \geq 0$ and $P \notin \operatorname{supp} E$. Then D is said to be a semi-reduced divisor.*

Lemma 10 ([1, 8]) *For each $j \in J_{\mathbf{F}_q}(F)$, there exists a semi-reduced divisor $D \in \mathcal{D}_F^0$ such that $j = [D]$, where we denote the divisor class which D belongs to by $[D]$.*

Definition 46 *If n is minimized in $D_1 = E - nP$ with $E \geq 0$ and $P \notin \text{supp } E$ (semi-reduced) and $D_1 \sim D \in \mathcal{D}_F^0$, then D_1 is said to be the reduced divisor equivalent to D.*

Lemma 11 ([8]) *For each $D \in \mathcal{D}_F^0$, the reduced divisor $D_1 = E - nP \sim D$ is unique, and we have $\deg(E) \leq g$, where $E \geq 0$ and $P \notin \text{supp } E$.*

(**Proof of Lemma 11**)
If D is principal then obviously $n = 0$ and $E = 0$. If D is not principal, then we have $\dim D = 0$, where we set $\dim D := \dim_{\mathbf{F}_q} \mathcal{L}(D)$. From Lemma 4, we have

$$\dim_{\mathbf{F}_q} (\mathcal{L}(D + (n+1)P)/\mathcal{L}(D + nP)) \leq \deg P = 1 \text{ for each } n \geq 0.$$

Therefore, the values of $\dim(D + nP)$ increase with n by 0 or 1.

Let n be the unique minimum positive integer such that $\dim(D + nP) = 1$, and let f be the unique (up to $\mathbf{F}_q^*$) function $f \in \mathcal{L}(D+nP)$. Then, we have $n \leq g$, since $\dim(D + gP) = \deg(D + gP) + 1 - g + \dim(W - (D+gP)) = 1 + \dim(W - (D+gP)) \geq 1$ from the Riemann-Roch Theorem (Theorem 15), where W denotes a canonical divisor of $F/\mathbf{F}_q$.

Furthermore, for $E := (f) + D + nP \geq 0$, we have $E - nP = D + (f) \sim D$. Since $\dim(D + nP) = 1$ and $\mathcal{L}(D) \cong \mathcal{L}(D')$ (isomorphic as vector space over $\mathbf{F}_q$), if $D \sim D'$ then E is unique. $\square$

From $\deg P = 1$ and $\bigcap_{Q \in \mathbf{P}_F \setminus \{P\}} \mathcal{O}_Q = \mathcal{L}(\infty P) = \mathbf{F}_q[x_1, \cdots, x_n]$ and Proposition 11, the Jacobian group $J_{\mathbf{F}_q}(F)$ is isomorphic to the ideal class group of the coordinate ring of the corresponding $\mathbf{A}_t$-curve. We denote it by $Cl(\mathbf{F}_q[x_1, \cdots, x_n])$.

Here, the isomorphism Φ between $J_{\mathbf{F}_q}(C)$ and $Cl(\mathbf{F}_q[x_1, \cdots, x_n])$ is given as follows [1] [8]:

$$\Phi : J_{\mathbf{F}_q}(C) \to \ Cl(\mathbf{F}_q[x_1, \cdots, x_n]),$$

$$[\textstyle\sum_{Q \in \mathbf{F}_P \setminus \{P\}} n_Q Q - (\sum_{Q \in \mathbf{F}_P \setminus \{P\}} n_Q) P]$$

$$\mapsto \ [\textstyle\prod_{Q \in \mathbf{F}_P \setminus \{P\}} (Q \cap \mathbf{F}_q[x_1, \cdots, x_n])^{n_Q}], \tag{5.1}$$

where we denote the ideal class which an ideal I of $\mathbf{F}_q[x_1, \cdots, x_t]$ belongs to by $[I]$.

We call the ideals corresponding to reduced and semi-reduced divisors the *reduced and semi-reduced ideals*, respectively. Then each semi-reduced ideal I is expressed by an integral ideal I of $\mathbf{F}_q[x_1, \cdots, x_t]$. And, for a semi-reduced ideal I, we define the degree of I by such an n that $\Phi^{-1}(I) = E - nP$. Then, from Proposition 11, we have

$$\deg I = \dim_{\mathbf{F}_q}(\mathbf{F}_q[x_1, \cdots, x_t]/I). \tag{5.2}$$

And if I is a reduced ideal, then we have $n \leq g$ from Lemma 11.

From now on, we consider the arithmetic on the Jacobian group as that on the ideal class group of the coordinate ring of the corresponding $\mathbf{A}_t$-curve. And we regard the reduced ideal in each ideal class as the representative element

Here, we introduce a propety of the coordinate rings $\mathbf{F}_q[x_1, \cdots, x_t]$ of $\mathbf{A}_t$-curves:

Theorem 24 ([14]) $\mathbf{T}(\mathbf{A}_t)$ *and* $\mathbf{M}(b_i)$ *are the same as Remark 5. Then we have* $\mathbf{B}(\mathbf{A}_t) = \mathbf{T}(\mathbf{A}_t) + \mathbf{Z}_{\geq 0} \times \{0\}^{t-1}$.

Therefore, from Lemma 9, $\{x^{\gamma_0} = 1, x^{\gamma_1}, \cdots, x^{\gamma_{a_1-1}}\}$ *is a* $\mathbf{F}_q[x_1]$*-basis of the coordinate ring* $\mathbf{F}_q[x_1, \cdots x_t]$*, where we set* $\gamma_i := \mathbf{M}(b_i)$ $(0 \leq i \leq a_1 - 1)$.

Hence, for each γ_i and a nonzero polynomial $f_i(x_1) \in \mathbf{F}_q[x_1]$, we have $-v_P(f_i(x_1)x^{\gamma_i}) = a_1(\deg_{x_1} f_i(x_1)) + \Psi_{\mathbf{A}_t}(\gamma_i) \equiv i \pmod{a_1}$, where $v_P(\cdot)$ denotes the discrete valuation with respect to P.

From now on, we express each element in $\mathbf{F}_q[x_1, \cdots x_t]$ by using the above $\mathbf{F}_q[x_1]$-basis $\{x^{\gamma_0} = 1, x^{\gamma_1}, \cdots, x^{\gamma_{a_1-1}}\}$.

Now we consider a representation of an integral ideal of $\mathbf{F}_q[x_1, \cdots, x_t]$. For each integral ideal of $\mathbf{F}_q[x_1, \cdots x_t]$, the $\mathbf{F}_q[x_1]$-basis can be uniquely expressed by taking the HNF (Definition 5) of the matrix $[\beta_{i,j}]$, where the $\mathbf{F}_q[x_1]$-basis is given as the matrix $(\beta_0, \cdots, \beta_{a_1-1})$ with $\beta_k = \sum_{l=0}^{a_1-1} \beta_{l,k}(x_1)x^{\gamma_l}$. (Note that $\mathbf{F}_q[x_1]$ is a **PID** and we say an $n \times n$ matrix $[\beta_{i,j}]$ with $\beta_{i,j} \in \mathbf{F}_q[x_1]$ is in HNF matrix if $[\beta_{i,j}]$ is an upper triangle matrix and $\beta_{i,i}$ $(1 \leq i \leq n)$ are monic and $\deg_{x_1}\beta_{i,j} < \deg_{x_1}\beta_{i,i}$ $(1 \leq i < j \leq n)$.)

Therefore, we express the representative element, i.e. reduced ideal, in each ideal class of $\mathbf{F}_q[x_1, \cdots x_t]$ by the HNF of the given $\mathbf{F}_q[x_1]$-basis.

We notice that $\mathbf{F}_q(C)/\mathbf{F}_q(x_1)$ is separable, since $[\mathbf{F}_q(C) : \mathbf{F}_q(x_1)] = \deg(x_1)_\infty = a_1$ and $\gcd(a_1, \mathrm{char}\ \mathbf{F}_q) = 1$, and $\mathbf{F}_q[x_1]$ is a **PID**.

Therefore, from Theorems 3, 4, 9 and (5.2), for an integral ideal I with $[\beta_{i,j}]$ the HNF matrix, we have

$$\deg(I) = \sum_i \deg_{x_1} \beta_{i,i} \quad \text{and}$$

$$N_{F/\mathbf{F}_q(x_1)} = \prod_i I^{\sigma_i} = (\prod_i \beta_{i,i}), \tag{5.3}$$

where $\{\sigma_i\}_i$ is the set of isomorphisms of $\mathbf{F}_q(C)$ onto a subfield of an algebraic closure of $\mathbf{F}_q(C)$ leaving $\mathbf{F}_q(x_1)$ fixed.

Now we consider an algorithm for performing Jacobian group arithmetic on $\mathbf{A}_t$-curves. The main problem is how to compute the reduced ideal.

Here, we can obtain a reduced ideal by using the following algorithm [1], [8]:

Algorithm 2

Input: *Semi-reduced ideal I.*

Output: *The reduced ideal $I' \sim I^{-1}$.*

Step 1: *Find $0 \neq f \in I$ such that the pole order $-v_P(f)$ is minimal;*

Step 2: $I' \leftarrow (f)I^{-1}$.

The verification of Algorithm 2 can be checked from the Riemann-Roch theorem: The method of the proof is the same as that in Lemma 11. Namely, we substitute $D = -\Phi^{-1}(I)$ (see (5.1)) to the proof of Lemma 11.

Therefore, we can describe the Jacobian group arithmetic on $\mathbf{A}_t$-curves as follows:

Algorithm 3 *(Jacobian group arithmetic on $\mathbf{A}_t$-curves)*

Input: *Reduced ideals I_1, I_2 in $\mathbf{F}_q[x_1, \cdots, x_t]$* (HNF).

Output: *The reduced ideal $I_3 \sim I_1 I_2$* (HNF).

Step 1: *$D \leftarrow$ the HNF of $I_1 I_2$;*

Step 2: $J \leftarrow$ *a semi-reduced ideal such that* $D^{-1} = \frac{J}{(e)}$, *where* (e) *is a principal ideal generated by* $e \in \mathbf{F}_q[x_1]$ *(then,* $J \sim D^{-1}$*);*

Step 3: $f \leftarrow$ *a minimal nonzero element of* J *with respect to* $-v_P(\cdot)$*;*

Step 4: $I_3 \leftarrow$ *the* HNF *of* $(f)J^{-1} = \frac{(f)D}{(e)}$.

In order to realize Algorithm 3, we should fix the following procedures:

1. how to compute the inverse ideal I^{-1} for a given ideal I (Step 2); and
2. how to compute the minimal element of an ideal with respect to $-v_P(\cdot)$ (Step 3).

Chapter 6

Realization of Jacobian Group Arithmetic

In this chapter, we propose a method (Algorithm 3) for performing Jacobian group arithmetic on algebraic function fields, i.e. ideal class group of the coordinate ring of the corresponding $\mathbf{A}_t$-curves.

6.1 Computing Inverse Ideal

The idea is based on algebraic number theory [4]:

Let L be a number field, and $\mathbf{Z}_L$ the ring of integers of L, and $n := [L : \mathbf{Q}]$. We first fix a $\mathbf{Z}$-basis $(w_i)_{1 \le i \le n}$ of $\mathbf{Z}_L$. For a square matrix M, let M^t denote the transposed matrix of M.

Definition 47 *The different of L is defined as*

$$\Gamma(L) := \{x \in L \mid \mathrm{Tr}_{L/\mathbf{Q}}(x\mathbf{Z}_L) \subseteq \mathbf{Z}\}^{-1}, \tag{6.1}$$

which is an integral ideal of $\mathbf{Z}_L$.

Then, the following proposition follows ([4], pp. 203):

Proposition 15 *Let $(\omega_i)_{1 \le i \le n}$ be a $\mathbf{Z}$-basis of $\mathbf{Z}_L$ and I an ideal of $\mathbf{Z}_L$ given by a matrix M whose columns give the coordinates of a $\mathbf{Z}$-basis $(\gamma_i)_{1 \le i \le n}$ of I on the chosen $\mathbf{Z}$-basis $(\omega_i)_{1 \le i \le n}$. Let $T = (t_{i,j})$ be the $n \times n$ matrix such that $t_{i,j} = \mathrm{Tr}_{L/\mathbf{Q}}(\omega_i \omega_j)$. Then, the columns of the matrix $(M^t T)^{-1}$ form a $\mathbf{Z}$-basis of the ideal $(I\Gamma(L))^{-1}$.*

Therefore, given an ideal I of $\mathbf{Z}_L$, the ideal product $I\Gamma(L)^{-1}$ can be computed by taking the HNF of the $n \times n^2$ matrix obtained from M and T^{-1}. If N denotes the HNF, then $(N^tT)^{-1}$ forms a $\mathbf{Z}$-basis of $(I\Gamma(L)^{-1})^{-1}\Gamma(L)^{-1} = I^{-1}$ from Proposition 15.

Now we go back to the case of $\mathbf{A}_t$-curves. We consider Theorem 18. If we replace R with $\mathbf{F}_q[x_1]$, then we have $S(\mathbf{F}_q[x_1]) = \mathbf{P}_F \setminus \{P\}$. Therefore, the integral closure of $\mathbf{F}_q[x_1]$ in $\mathbf{F}_q(C)$ is $\bigcap_{Q \in \mathbf{P}_F \setminus \{P\}} \mathcal{O}_Q = \mathcal{L}(\infty P) = \mathbf{F}_q[x_1, \cdots x_t]$ and the integral basis is $\{x^{\gamma_i}\}_{0 \le i \le a_1 - 1}$, and $\mathbf{F}_q[x_1]$ is a **PID**. As a result, we can extend the above method for number fields in a natural manner:

Algorithm 4 *(Computation of inverse ideals for $\mathbf{A}_t$-curves)*

Input: *Semi-reduced ideal I of $\mathbf{F}_q[x_1, \cdots x_t]$ with $[\beta_i]_{0 \le i \le a_1 - 1}$ a $\mathbf{F}_q[x_1]$-basis of I* (HNF)*, where we express $\beta_i = \sum_{0 \le j \le a-1} \beta_j^{(i)}(x_1) x^{\gamma_j}$ by $\beta_i = [\beta_0^{(i)}(x_1), \cdots, \beta_{a_1-1}^{(i)}(x_1)]^t$ (a transposed matrix).*

Output: *The inverse ideal I^{-1}.*

Step 1: $N \leftarrow$ *the* HNF *of the ideal product of two ideals generated by column vectors of $[\beta_i]_{0 \le i \le a_1 - 1}$ and by those of dT^{-1};*

Step 2: $h \leftarrow$ *such an element in $\mathbf{F}_q[x_1]$ that $h(N^t)^{-1}$ is a matrix with $\mathbf{F}_q[x_1]$-coefficients;*
$S \leftarrow dh(N^tT)^{-1} = (dT^{-1})(h(N^t)^{-1})$;
$k \leftarrow \mathrm{GCD}(\mathrm{GCD}(S),\ h)$;
$e \leftarrow \frac{h}{k}$;
$W \leftarrow \frac{1}{k}S$;
$I^{-1} \leftarrow (W, e)$ $(I^{-1} = W(e)^{-1})$,

where $T = [t_{i,j}]_{0 \le i,j \le a_1 - 1}$ is given by $t_{i,j} = \mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i} x^{\gamma_j})$ and d is such an element in $\mathbf{F}_q[x_1]$ that dT^{-1} is a matrix with $\mathbf{F}_q[x_1]$-coefficients, and for a matrix A and $f,\ g \in \mathbf{F}_q[x_1]$, $\mathrm{GCD}(A)$ and $\mathrm{GCD}(f, g)$ denote the GCD of all the elements in A and that of f and g, respectively.

Therefore, we can compute inverse ideals if we obtain the matrix $T = [t_{i,j}]_{0 \le i,j \le a_1 - 1} = [\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i} x^{\gamma_j})]_{0 \le i,j \le a_1 - 1}$. And it is enough to compute the values of $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_k})$ for $0 \le k \le a_1 - 1$. In fact, if we express $x^{\gamma_i} x^{\gamma_j}$ as $x^{\gamma_i} x^{\gamma_j} := \sum_{0 \le k \le a_1 - 1} g_k^{(i,j)}(x_1) x^{\gamma_k}$ for some $g_k^{(i,j)}(x_1)$'s, then we have

$$
\begin{aligned}
& \mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i}x^{\gamma_j}) \\
= \; & \mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(\textstyle\sum_{0\le k\le a_1-1} g_k^{(i,j)}(x_1)x^{\gamma_k}) \\
= \; & \textstyle\sum_{0\le k\le a_1-1} g_k^{(i,j)}(x_1)\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_k}).
\end{aligned}
$$

Now, we describe two methods for computing $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_k})$ $(0 \le k \le a_1 - 1)$.

6.1.1 The First Method

The first idea is based on Definition 8. Namely, for each k, we compute the $a_1 \times a_1$ matrix $A(x^{\gamma_k}) = (a_{i,j})$ with $\mathbf{F}_q[x_1]$-coefficients such that

$$x^{\gamma_k}[x^{\gamma_0}, x^{\gamma_1}, \cdots, x^{\gamma_{a_1-1}}] = [x^{\gamma_0}, x^{\gamma_1}, \cdots, x^{\gamma_{a_1-1}}]A(x^{\gamma_k}).$$

Then we have $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_k}) = \sum a_{i,i}$, which is obtained by $a_{i,i} = g_i^{(k,i)}(x_1)$, where we express $x^{\gamma_k}x^{\gamma_i} = \sum_{0\le l\le a_1-1} g_l^{(k,i)}(x_1)x^{\gamma_l}$.

6.1.2 The Second Method

The second idea is based on Theorem 6. Namely, we can obtain $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_k})$ if we compute the minimal polynomial of x^{γ_k} over $\mathbf{F}_q(x_1)$.

For C_{ab} curves $C/\mathbf{F}_q$ (the case of $t = 2$)

$$\sum_{0\le i\le b, 0\le j\le a, ai+bj\le ab} \alpha_{i,j}x^iy^j = 0,$$

the integral basis is $\{y^i\}_{0\le i\le a-1}$. Then we can compute the values of $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x)}(y^i)$ as follows [9], where $\mathbf{F}_q(C)$ denotes the function field:

1. $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x)}(y)$ can be obtained if the minimal polynomial of y over $\mathbf{F}_q(x)$ is given, which coincides with the definition equation;

2. $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x)}(y^i)$ can be computed by using the minimal polynomial of y over $\mathbf{F}_q(x)$ and the Newton formula ([4], pp. 161).

Remark 7 *Especially, for the so-called superelliptic curve $C/\mathbf{F}_q$*

$$y^a = f(x)$$

with $\deg_x f(x) = b$, $\gcd(a, b) = \gcd(a, \mathrm{char}\mathbf{F}_q) = 1$ *and* $\gcd(f(x), f'(x)) = 1$, *where* $f'(x)$ *denotes the formal derivation of* $f(x)$, *matrices* T *and* dT^{-1} *are given as follows:*

$$T = \begin{bmatrix} a & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & af(x) \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & af(x) & \cdots & 0 \\ 0 & af(x) & 0 & \cdots & 0 \end{bmatrix}, dT^{-1} = \begin{bmatrix} f(x) & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{bmatrix}.$$

Then it turns out that the ideal generated by column vectors of dT^{-1} *is the principal ideal* (y), *which gives more efficient method than the case of* $\mathbf{A}_t$*-curves (see Table* 7.1 *and Table* 8.1*). Furthermore, the degree of* x_1 *in the inverse ideal obtained by this method is smaller than that by obtained by Galbraith et. al' method [8], i.e. the method of computing conjugate ideals. This is the main reason why this proposed method is more efficient than their one.*

However, unlike C_{ab} curves, we cannot apply the method to $\mathbf{A}_t$-curves, since $\mathbf{A}_t$-curve may have more than one definition equation.

Now, we propose a method of computing the minimal polynomial of each x^{γ_i} over $\mathbf{F}_q(x_1)$, which leads to the computation of $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x)}(x^{\gamma_i})$.

At first, for extension degrees of x^{γ_i} over $\mathbf{F}_q(x_1)$, we prove the following proposition.

Proposition 16 *For* $1 \leq i \leq a_1 - 1$, *we have*

$$[\mathbf{F}_q(x_1, x^{\gamma_i}) : \mathbf{F}_q(x_1)] = \frac{a_1}{l},$$

where $l := \gcd(i, a_1) = \gcd(\Psi_{\mathbf{A}_t}(\gamma_i), a_1)$.

(**Proof of Proposition 16**)
It is sufficient to show $[\mathbf{F}_q(C) : \mathbf{F}_q(x_1, x^{\gamma_i})] = l$, since we have $a_1 = \deg(x_1)_\infty = [\mathbf{F}_q(C) : \mathbf{F}_q(x_1)] = [\mathbf{F}_q(C) : \mathbf{F}_q(x_1, x^{\gamma_i})][\mathbf{F}_q(x_1, x^{\gamma_i}) : \mathbf{F}_q(x_1)]$, where $(x_1)_\infty$ is the pole divisor of x_1.

Now, since $\Psi_{\mathbf{A}_t}(\gamma_i) = \deg(x^{\gamma_i})_\infty = [\mathbf{F}_q(C) : \mathbf{F}_q(x^{\gamma_i})] = [\mathbf{F}_q(C) : \mathbf{F}_q(x_1, x^{\gamma_i})][\mathbf{F}_q(x_1, x^{\gamma_i}) : \mathbf{F}_q(x^{\gamma_i})]$ holds, we have $[\mathbf{F}_q(C) : \mathbf{F}_q(x_1, x^{\gamma_i})]$ divides $\gcd(a_1, \Psi_{\mathbf{A}_t}(\gamma_i)) = \gcd(a_1, i) = l$.

Therefore, the proposition holds for $l = 1$.

We consider the case of $l > 1$ (, then $i \neq 1$ holds).

Now we suppose that $m := [\mathbf{F}_q(C) : \mathbf{F}_q(x_1, x^{\gamma_i})] < l$, and that the minimal polynomial $G(x_1, x^{\gamma_i}, x^{\gamma_1}) = 0$ of $x^{\gamma_1} \in \mathbf{F}_q(C)$ over $\mathbf{F}_q(x_1, x^{\gamma_i})$ is expressed by

$$\begin{aligned} & G(x_1, x^{\gamma_i}, x^{\gamma_1}) \\ = & \sum_{0 \leq j \leq m, f_j(x_1, x^{\gamma_i}) \neq 0} f_j(x_1, x^{\gamma_i})(x^{\gamma_1})^j \end{aligned} \tag{6.2}$$

for some $f_j(x_1, x^{\gamma_i}) \in \mathbf{F}_q[x_1, x^{\gamma_i}]$.

Then we have

$$-v_P(f_j(x_1, x^{\gamma_i})(x^{\gamma_1})^j) \equiv j \pmod{l}, \tag{6.3}$$

since $-v_P(x^{\gamma_1}) \equiv 1 \pmod{l}$ and $-v_P(f_j(x_1, x^{\gamma_i}))$ can be divided by l. However, for $0 \leq j \leq m < l$, each value of (6.3) is different $\pmod{l}$, so that

$$\begin{aligned} & -v_P(G(x_1, x^{\gamma_i}, x^{\gamma_1})) \\ = & \max_{j, f_j(x_1, x^{\gamma_i}) \neq 0}\{-v_P(f_j(x_1, x^{\gamma_i})(x^{\gamma_1})^j)\} \\ < & \infty, \end{aligned}$$

This contradicts $v_P(0) = \infty$. Therefore we conclude $[\mathbf{F}_q(C) : \mathbf{F}_q(x_1, x^{\gamma_i})] = l$. $\square$

From Proposition 16, we can compute $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i})$ as follows:

Stage 1 if $i = 0$ then $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i}) \leftarrow a_1$;
otherwise, $\lambda \leftarrow \frac{a_1}{l}$ with $l = \gcd(i, a_1)$;

Stage 2 the computation of $(f_k^j(x_1))$ with

$$\begin{bmatrix} 1 \\ x^{\gamma_i} \\ \vdots \\ (x^{\gamma_i})^{\lambda-1} \\ (x^{\gamma_i})^{\lambda} \end{bmatrix} = \begin{bmatrix} f_0^0(x_1) & \cdots & f_{a_1-1}^0(x_1) \\ f_0^1(x_1) & \cdots & f_{a_1-1}^1(x_1) \\ \vdots & \vdots & \vdots \\ f_0^{\lambda-1}(x_1) & \cdots & f_{a_1-1}^{\lambda-1}(x_1) \\ f_0^{\lambda}(x_1) & \cdots & f_{a_1-1}^{\lambda}(x_1) \end{bmatrix} \begin{bmatrix} 1 \\ x^{\gamma_1} \\ \vdots \\ x^{\gamma_{a_1-2}} \\ x^{\gamma_{a_1-1}} \end{bmatrix};$$

Stage 3 the computation of the minimal polynomial $D(x_1, x^{\gamma_i}) = (x^{\gamma_i})^\lambda + \sum_{0\le j\le \lambda-1} D_j^{(i)}(x_1)(x^{\gamma_i})^j$ with

$$\left[\begin{array}{c|cccc} * & * & \cdots & * & * \\ * & * & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & \cdots & * & * \\ D(x_1, x^{\gamma_i}) & 0 & \cdots & 0 & 0 \end{array}\right]$$

by performing elementary operations on rows from

$$\left[\begin{array}{c|ccc} 1 & f_0^0(x_1) & \cdots & f_{a_1-1}^0(x_1) \\ x^{\gamma_i} & f_0^1(x_1) & \cdots & f_{a_1-1}^1(x_1) \\ \vdots & \vdots & \vdots & \vdots \\ (x^{\gamma_i})^{\lambda-1} & f_0^{\lambda-1}(x_1) & \cdots & f_{a_1-1}^{\lambda-1}(x_1) \\ (x^{\gamma_i})^{\lambda} & f_0^{\lambda}(x_1) & \cdots & f_{a_1-1}^{\lambda}(x_1) \end{array}\right];$$

Stage 4 $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i}) \leftarrow -l(D_{\lambda-1}^{(i)}(x_1))$.

6.2 Computing Minimal Element

We can obtain a minimal element with respect to $-v_P(\cdot)$ by modifying Paulus's lattice basis reduction algorithm [15] in a natural manner:

We embed $\mathbf{F}_q[x_1, \cdots, x_t]$ into $\mathbf{F}_q[x_1]^{a_1}$ with

$$\phi : \mathbf{F}_q[x_1, \cdots, x_t] \to (\mathbf{F}_q[x_1])^{a_1},$$

$$\sum_{0\le i\le a_1-1} c_i(x_1)x^{\gamma_i} \mapsto [c_0(x_1), \cdots, c_{a_1-1}(x_1)]^t,$$

and define a metric of $C = [c_0(x_1), \cdots, c_{a_1-1}(x_1)]^t \in (\mathbf{F}_q[x_1])^{a_1}$ as $|C| := \max_i |C|_i$, where $|C|_i := \deg_{x_1}(c_i(x_1)) + \frac{b_i}{a_1}$. The reason why we consider such a metric is that the relation $a_1 \times -v_P(x^{\gamma_i}) = -v_P(x_1) \times b_i$ implies $-v_P(x^{\gamma_i}) = -v_P(x_1) \times \frac{b_i}{a_1}$.

For an integral ideal I of $\mathbf{F}_q[x_1, \cdots, x_t]$, let $\{f_0, \cdots, f_{a_1-1}\}$ be a $\mathbf{F}_q[x_1]$-basis of I. Then, $\phi(I)$ is a lattice generated by $\{\phi(f_i)\}_i$ over $\mathbf{F}_q[x_1]$, so that minimization over $f \in I$ with respect to $-v_P(f)$ is

equivalent to minimization over $u \in \phi(I)$ with respect to $|u|$, since we have $-v_P(f) = a_1|\phi(f)|$ for $f \in I$. (By *lattice* $L \subseteq (\mathbf{F}_q[x_1])^{a_1}$, we mean $\mathbf{F}_q[x_1]$-module of rank a_1 over $\mathbf{F}_q[x_1]$.)

We define a value OD, called the *orthogonality defect*, to compute a minimal element of a given lattice.

Definition 48 ([15]) *The basis $\{f_0, \cdots, f_{a_1-1}\}$ for a lattice L is said to be the reduced basis if $OD(f_0, \cdots, f_{a_1-1}) = 0$, where*

$$OD(f_0, \cdots, f_{a_1-1}) := \sum_i |f_i| - \deg_{x_1}(d(L))$$

and $d(L) := \det[f_0^*, \cdots, f_{a_1-1}^*]$ with
$f_i^* := [f_0^i(x_1),\ f_1^i(x_1)x_1^{\frac{b_1}{a_1}},\ \cdots, f_{a_1-1}^i(x_1)x_1^{\frac{b_{a_1-1}}{a_1}}]^t$ *for* $f_i = \sum_{j=0}^{a_1-1} f_j^i(x_1)x^{\gamma_j}$.

It is easy to see that $OD(f_0, \cdots, f_{a_1-1}) \geq 0$ by the definition of OD.

In the case of $\mathbf{A}_t$-curves, the fact of $b_i \equiv i \pmod{a_1}$ implies that there exists a unique l such that $|f| = |f|_l$ for a nonzero vector $f = [f_0, \cdots, f_{a_1-1}]^t \in (\mathbf{F}_q[x_1])^{a_1}$. In other words, there exists a unique l such that $-v_P(f) = -v_P(f_l(x_1)x^{\gamma_l})$ for a nonzero element $f = \sum_{i=0}^{a_1-1} f_i(x)x^{\gamma_i}$.

Therefore, for a $\mathbf{F}_q[x_1]$-basis $\{f_0, \cdots, f_{a_1-1}\}$ of a lattice L, it turns out that

$$\begin{aligned} &OD(f_0, \cdots, f_{a_1-1}) = 0 \\ \Leftrightarrow\ &|f_i| - |f_j| \notin \mathbf{Z}\ (0 \leq i < j \leq a_1 - 1). \end{aligned} \tag{6.4}$$

We can obtain the following result from (6.4):

Proposition 17 *Let $\{f_0, \cdots, f_{a_1-1}\}$ be the reduced basis for a lattice L. Then $f \in \{f_0, \cdots, f_{a_1-1}\}$ such that $|f| = \min_i\{|f_i|\}$ is the minimal nonzero element in L with respect to $|\cdot|$.*

(**Proof of Proposition 17**)
For each nonzero element $h \in L$, (6.4) implies that there exists some f_i such that $|h| \geq |f_i|$. Therefore we have $|h| \geq |f_i| \geq \min_i\{|f_i|\} = |f|$. $\square$

Hence, we can find the reduced basis (i.e. the minimal element) by performing elementary operations on columns until the condition

(6.4) is satisfied, which is the same method as the case of C_{ab} curves [9]:

If $|f_i| - |f_j| \in \mathbf{Z}$, there exists a unique l such that $|f_i| = |f_i|_l$, $|f_j| = |f_j|_l$. Now we suppose $|f_i|_l \geq |f_j|_l$. Then we perform an elementary operation on columns by computing $f_i \longleftarrow f_i - rx_1^{\alpha} f_j$, with $r = c_{i,l}/c_{j,l}$, $\alpha = \deg_{x_1} f_{i,l}(x_1) - \deg_{x_1} f_{j,l}(x_1)$, where $c_{i,l}$ and $c_{j,l}$ are the leading coefficients of $f_{i,l}(x_1)$ and $f_{j,l}(x_1)$, respectively.

And we can evaluate the complexity as follows:
(Note that we evaluate time complexity based on the fact that multiplying two elements of bit-length N takes $O(N^2)$ bit-operations.)

Theorem 25 *For a basis $\{f_0, \cdots, f_{a_1-1}\}$ of a lattice L, the reduced basis is computed in $O(a_1(a_1 s + \max_k\{b_k\})^2 \log^2 q)$ bit-operations, if the degree of x_1 in $f_{i,j}$ is bounded by s, where we set $f_i = [f_{i,0}, \cdots, f_{i,a_1-1}]^t$ with $f_i = \sum_{j=0}^{a_1-1} f_{i,j}(x_1) x^{\gamma_j}$.*

(**Proof of Theorem 25**)

Let $h = \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{a_1-1} \end{bmatrix}$ be an intermediate column vector obtained by performing an elementary operation on columns. Since OD (see Definition 48) strictly decreases after the operation, there exists f_i such that $|h| < |f_i|$. Then we have

$$\begin{aligned} a_1 \times \deg_{x_1} h_j + b_j &< a_1 s + \max_k\{b_k\} \\ \deg_{x_1} h_j &< s + \tfrac{\max_k\{b_k\}}{a_1} \qquad (0 \leq j \leq a_1 - 1). \end{aligned}$$

Therefore, the complexity of performing each elementary operation on columns is $O(a_1 \times \{s + \frac{\max_k\{b_k\}}{a_1}\} \times \log^2 q) = O((a_1 s + \max_k\{b_k\}) \log^2 q)$.

Since the number of iterations is bounded by $a_1 \times OD(f_0, \cdots f_{a_1-1}) \leq a_1 \times \sum_{j=0}^{a_1-1}(s + \max_k\{\frac{b_k}{a_1}\}) = a_1(a_1 s + \max_k\{b_k\})$, the reduced basis is computed in

$$\begin{aligned} & O(a_1(a_1 s + \max_k\{b_k\}) \times (a_1 s + \max_k\{b_k\}) \log^2 q) \\ = \; & O(a_1(a_1 s + \max_k\{b_k\})^2 \log^2 q). \quad \square \end{aligned}$$

Chapter 7

Complexity

In Chapter 6, we have seen that Algorithm 3 is practical for $\mathbf{A}_t$-curves.

In this chapter, we evaluate the complexity. We assume that the usual multiplication method is used, so that multiplying two elements of bit-length N takes $O(N^2)$ bit-operations.

7.1 Inverse ideal

In this section, we consider the matrices T and dT^{-1} that we require to compute inverse ideals.

Proposition 18 *Let $T = [t_{i,j}]$ with $t_{i,j} = \mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i}x^{\gamma_j})$. If $t_{ij} \neq 0$, then*

$$\deg_{x_1}(t_{i,j}) \leq \frac{b_i + b_j}{a_1}$$

and the degree of x_1 in each element in dT^{-1} is bounded by $2g+a_1-1$. Therefore, the degree of the ideal generated by column vectors of dT^{-1} is bounded by $2a_1g + a_1^2 - a_1$. (Note that the degree of x_1 in the product of diagonal elements of an HNF is at most a_1 times as that of element of the original matrix.)

(**Proof of Proposition 18**)
We set $x^{\gamma_i}x^{\gamma_j} = \sum_{0\leq k\leq a_1-1} g_k^{(i,j)}(x_1)x^{\gamma_k}$. Then, we have

$$\deg_{x_1} g_k^{(i,j)}(x_1) \leq \frac{b_i + b_j - b_k}{a_1} \tag{7.1}$$

from $-v_P(x^{\gamma_i}x^{\gamma_j}) = \max_{k,g_k^{(i,j)}\neq 0}\{-v_P(g_k^{(i,j)}(x_1)x^{\gamma_k})\}$. Since each $x^{\gamma_k} \in \mathbf{F}_q[x_1,\cdots,x_t]$ is integral over $\mathbf{F}_q[x_1]$, we can denote the minimal polynomial of x^{γ_k} over $\mathbf{F}_q(x_1)$ by
$D(x_1, x^{\gamma_k}) = (x^{\gamma_k})^\lambda + \sum_{0\le j\le \lambda-1} D_j^{(k)}(x_1)(x^{\gamma_k})^j$,
where $\lambda := \frac{a_1}{l}$, $l := \gcd(b_k, a_1)$ (Proposition 16).
Then, $\mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_k}) = -lD_{\lambda-1}^{(k)}(x_1)$ holds. And if $D_{\lambda-1}^{(k)}(x_1) \neq 0$, we have

$$\deg_{x_1} D_{\lambda-1}^{(k)}(x_1) \le \frac{b_k}{a_1}, \tag{7.2}$$

since the fact of $(x^{\gamma_k})^j \not\equiv (x^{\gamma_k})^{j'} \pmod{a_1}$ $(0 \le j < j' \le a_1 - 1)$ implies that $-v_P((x^{\gamma_k})^\lambda) \ge -v_P(D_{\lambda-1}^{(k)}(x_1)(x^{\gamma_k})^{\lambda-1})$.

From (7.1), (7.2),

$$\begin{aligned} & \deg_{x_1} \mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i}x^{\gamma_j}) \\ \le\ & \max_k\{\tfrac{b_i+b_j-b_k}{a_1} + \tfrac{b_k}{a_1}\} \\ =\ & \tfrac{b_i+b_j}{a_1}. \end{aligned}$$

Next, from the definition of the determinant of a matrix T,
$\det T := \sum_{(p_0,\cdots,p_{a_1-1})} \mathrm{sgn}(p_0,\cdots,p_{a_1-1}) t_{0,p_0}\cdots t_{a_1-1,p_{a_1-1}}$,
where $(p_0,\cdots,p_{a_1-1})$ runs over the set of permutations of $\{0,\cdots,a_1-1\}$,

$$\begin{aligned} & \deg_{x_1}(\det T) \\ \le\ & \max_{(p_0,\cdots,p_{a_1-1})}\{\tfrac{b_0+b_{p_0}}{a_1} + \cdots + \tfrac{b_{a_1-1}+b_{p_{a_1-1}}}{a_1}\} \\ =\ & \{\tfrac{b_0+\cdots+b_{a_1-1}}{a_1} + \tfrac{b_{p_0}+\cdots+b_{p_{a_1-1}}}{a_1}\} \\ =\ & 2\times(g+\tfrac{1}{2}(a_1-1)) \\ =\ & 2g+a_1-1, \end{aligned}$$

and this method gives the fact of $\deg_{x_1}(\det T') \le 2g + a_1 - 1$ for each cofactor matrix T' of T (note that we have $\sum_{0\le i\le a_1-1}(\frac{b_i}{a_1}) - g = \sum(\frac{b_i}{a_1} - \lfloor\frac{b_i}{a_1}\rfloor) = \sum\frac{i}{a_1} = \frac{1}{2}(a_1-1)$, since we have $g = \sum_{i=0}^{a_1-1}\lfloor b_i/a_1\rfloor$ (4.5) and $b_i \equiv i \pmod{a_1}$), so is the degree of x_1 in each element of $(\det T)T^{-1}$ from Cramer's formula. □

7.2 Complexity

In this thesis, the evaluation of complexity is based on the following results:

Lemma 12 *[16] Let A, B be two polynomials in one variable over a field, where we suppose* $\deg A \geq \deg B \geq 1$. *Let* $S = \gcd(A, B) = XA + YB$ *with polynomials X, Y computed by the extended Euclidian algorithm.*

1. *The number of operations on the base field to compute S is bounded by*

$$(\deg A + 1)(\deg B + 1) - \deg S - (\deg S)^2.$$

2. *The number of operations on the base field to compute X resp. Y is bounded by*

$$(\deg B - \deg S)(\deg B - \deg S - 1)$$

resp. by

$$(\deg A - \deg S)(\deg A - \deg S - 1).$$

Lemma 13 *Let M be an $m \times n$ matrix whose elements are polynomials of x over a finite field $\mathbf{F}_q$. We suppose that* $\mathrm{rank}(M) = m$, *and that the degree of x in each element of M and the determinant of M are bounded by s and t, respectively, where* $\det(M)$ *denotes the product of diagonal elements of the* HNF *of M. Then*

1-1. *if the determinant of M is known, then the HNF of M is obtained in $O(m^2nt^2 \log^2 q)$;*

1-2. *if $n = m$ and $t < q$, then the* HNF *of M is obtained in* $O(\max\{m^2st,\ m^3t^2\} \log^2 q)$;

2. *if $n = m$ and M is given in the* HNF, *then* $\det(M)M^{-1}$ *is obtained in $O(m^3t^2 \log^2 q)$ (by applying the Gaussian elimination) and the degree of x in each element of* $\det(M)M^{-1}$ *is bounded by t.*

and if the degrees of x in two polynomials f, g are bounded by s,

3. *the GCD of f and g is obtained in $O(s^2 \log^2 q)$.*

(**Proof of Lemma 13**)

1-1, 3. Clear. (See [4] or Algorithm 1 for **1-1** and Lemma 12 for **3**.)

1-2. We consider the same method as in [9]:

Step 1: set $W \subseteq \mathbf{F}_q$ of cardinarity $t+1$ (such W exists by the assumption $t < q$);

Step 2: compute $D \bmod f_\alpha(x)$ ($\alpha \in W$), where we define $D := \det M$ and $f_\alpha(x) := x - \alpha$ (then $\mathbf{F}_q[x]/(f_\alpha(x)) \cong \mathbf{F}_q$ holds);

Step 3: compute $D = D \bmod \prod_{\alpha \in W} f_\alpha(x)$ by using Chinese remainder theorem (CRT) (note that this method gives the correct value,
since $\deg_x(\det M) \leq t < \deg_x(\prod_{\alpha \in W} f_\alpha(x))$);

Step 4: compute the HNF of M modulus D (Algorithm 1).

For Step 2, we obtain $M \bmod f_\alpha(x)$ after m^2 divisions between two polynomials whose degrees are s and 1, which takes $O(m^2 s \log^2 q)$. From $\mathbf{F}_q[x]/(f_\alpha(x)) \cong \mathbf{F}_q$, $D \bmod f_\alpha(x)$ is obtained in $O(m^3 \log^2 q)$ [4]. Therefore, Step 2 takes
$O(\#W \times \max\{m^2 s, m^3\} \log^2 q) = O(\max\{m^2 st, m^3 t\} \log^2 q)$.

For Step 3, we compute $D = D \bmod \prod_{\alpha \in W} f_\alpha(x) = \sum_\alpha g_\alpha(D \bmod f_\alpha(x))$, where $g_\alpha = s_\alpha h_\alpha$ with $h_\alpha = (\prod_{\alpha' \in W} f_{\alpha'})/f_\alpha$ and $r_\alpha f_\alpha + s_\alpha h_\alpha = 1$. The multiplication $\prod_{\alpha \in W} f_\alpha$ is done in $O((\sum_{i=1}^{\#(W)} i \cdot 1) \log^2 q) = O(t^2 \log^2 q)$.

For each $\alpha \in W$, the division between $\prod_{\alpha \in W} f_\alpha$ and f_α is done in $O(t \log^2 q)$, since the degrees of x in the two polynomials are $t+1$ and 1, respectively. s_α is computed in $O(1 \cdot \log^2 q)$ from Lemma 12, and we have $s_\alpha \in \mathbf{F}_q$. And the multiplication $g_\alpha = s_\alpha h_\alpha$ is done in $O(t \log^2 q)$, since the degree of x in h_α is t. Final computation $D = \sum_\alpha g_\alpha(D \bmod f_\alpha(x))$ takes $\#(W) \times O(t \cdot 1 \cdot \log^2 q) = O(t^2 \log^2 q)$, since the degrees of x in h_α is t and $D \bmod f_\alpha(x) \in \mathbf{F}_q$. Therefore, Step 3 takes $O(t^2 \log^2 q)$.

For Step 4, since $\deg_x D \leq t$, the complexity is $O(m^3 t^2 \log^2 q)$ [4].

Therefore, the HNF of M is obtained in
$O(\max\{m^2 st, m^3 t, t^2\} \log^2 q) = O(\max\{m^2 st, m^3 t\} \log^2 q)$,
since $t \leq ms$ holds.

2. Let

$$M = \begin{bmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,m}(x) \\ 0 & f_{2,2}(x) & \cdots & f_{2,m}(x) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f_{m,m}(x) \end{bmatrix}$$ be an HNF matrix with

$\deg_x(\det M) = \deg_x \prod f_{i,i}(x) \leq t$ and $\deg_x(f_{i,i}(x)) > \deg_x(f_{i,j}(x))$ $(1 \leq i < j \leq m)$.

Let $\begin{bmatrix} I_1 \\ \vdots \\ I_m \end{bmatrix}$ be a unit matrix and $\begin{bmatrix} I'_1 \\ \vdots \\ I'_m \end{bmatrix} := \det M \begin{bmatrix} I_1 \\ \vdots \\ I_m \end{bmatrix}$.

Then, from the Gaussian elimination, we can compute $\begin{bmatrix} X_1 \\ \vdots \\ X_m \end{bmatrix} :=$ $(\det M)M^{-1}$ with $\left[\begin{array}{c|c} I_1 & X_1 \\ \vdots & \vdots \\ I_m & X_m \end{array}\right]$ by performing elementary operations on rows from

$$\left[\begin{array}{cccc|c} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,m}(x) & I'_1 \\ 0 & f_{2,2}(x) & \cdots & f_{2,m}(x) & I'_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & f_{m,m}(x) & I'_m \end{array}\right].$$

Here, we can compute X_k as follows:

$$X_m = I'_m / f_{m,m}(x),$$

$$X_k = (I'_k - \sum_{k+1 \leq j \leq m} f_{k,j}(x) X_j) / f_{k,k}(x) \quad (1 \leq k < m).$$

Furthermore, it turns out that the degree of each element in X_k, I'_k, and M is bounded by t, since we have $\deg_x(f_{i,i}(x)) > \deg_x(f_{i,j}(x))$ $(1 \leq i < j \leq m)$. Therefore, $(\det M)M^{-1}$ is obtained in $O(\sum_{1 \leq i \leq m}(i \times mt^2) \log^2 q) = O(m^3 t^2 \log^2 q)$. □

From the above results, we estimate the complexity of the proposed method for performing Jacobian group arithmetic as follows:

Theorem 26 *For $\mathbf{A}_t$-curves of genus g defined over a finite field $\mathbf{F}_q$, we suppose $g < q$. Then, the Jacobian group arithmetic (Algorithm*

3) is performed in

$$O(\max\{a_1^6 g^2,\ a_1^8\}\log^2 q)$$

bit-operations.

Remark 8 *We set* $x^{\gamma_i}x^{\gamma_j} = \sum_{0\le k\le a_1-1} g_k^{(i,j)}(x_1)x^{\gamma_k}$ *and* $T = [t_{i,j}]$ *with* $t_{i,j} = \mathrm{Tr}_{\mathbf{F}_q(C)/\mathbf{F}_q(x_1)}(x^{\gamma_i}x^{\gamma_j})$ *for a fixed* $\mathbf{F}_q[x_1]$*-basis* $\{x^{\gamma_0},\cdots,x^{\gamma_{a_1-1}}\}$*. In this thesis, we do not estimate the complexity of computations of* $g_k^{(i,j)}(x_1)$ *and* $(\det T)T^{-1}$ *(and the HNF), since the values can be determined by only the definition equation.*

At first, we estimate the complexity of multiplication on the coordinate ring $\mathbf{F}_q[x_1,\cdots,x_t]$ as follows:

Lemma 14 *With notation above, let* $h = \sum_i h_i(x_1)x^{\gamma_i}$*,* $h' = \sum_i h_i'(x_1)x^{\gamma_i}$ *be two elements in* $\mathbf{F}_q[x_1,\cdots,x_t]$ *with* $\deg_{x_1} h_i(x_1) \le t$ *and* $\deg_{x_1} h_i'(x_1) \le t'$*. Then the multiplication of* h *and* h' *takes* $O(\max\{a_1^2tt',\ a_1^2(a_1+g)(t+t')\}\log^2 q)$*.*

(**Proof of Lemma 14**)
We set $x^{\gamma_i}x^{\gamma_j} = \sum_{0\le k\le a_1-1} g_k^{(i,j)}(x_1)x^{\gamma_k}$, then we have $\deg_{x_1} g_k^{(i,j)}(x_1) \le \frac{b_i+b_j-b_k}{a_1}$ from (7.1). Therefore, the multiplication takes

$$\begin{aligned}
& O(\textstyle\sum_{0\le i,j\le a_1-1}(tt' + (t+t')(\sum_{0\le k\le a_1-1}\frac{b_i+b_j-b_k}{a_1}))\log^2 q) \\
= \ & O(\textstyle\sum_{0\le i,j\le a_1-1}(tt' + (t+t')(b_i+b_j-(\frac{1}{2}a_1-\frac{1}{2}+g)))\log^2 q) \\
= \ & O(a_1^2tt' + a_1^2(t+t')(\tfrac{1}{2}a_1-\tfrac{1}{2}+g))\log^2 q) \\
= \ & O(\max\{a_1^2tt',\ a_1^2(a_1+g)(t+t')\}\log^2 q),
\end{aligned}$$

where we notice $\sum_{0\le i\le a_1-1}(\frac{b_i}{a_1}) - g = \sum \frac{i}{a_1} = \frac{1}{2}(a_1-1)$ (pp. 57).
□

(**Proof of Theorem 26**)
Let (η_i) and (η_i') be the HNF representations of two reduced ideals I_1 and I_2 , respectively.

Step 1 ($O(\max\{a_1^4g^2,\ a_1^5g\}\log^2 q)$): The assumption that the degree of x_1 in each element in HNF expressing the input ideal is $O(g)$ implies that a_1^2 pairs of $(\eta_i\eta_j')$ are obtained in

$O(\max\{a_1^4 g^2,\ a_1^5 g\}\log^2 q)$ by using Lemma 14 with $t = t' = O(g)$.

Using **1-1** with $m = a_1$, $n = a_1^2$, and $t = O(g)$, the HNF J of the $a_1 \times a_1^2$ matrix is obtained in $O(a_1^4 g^2 \log^2 q)$. Note that $\deg(J) = \deg(I_1) + \deg(I_2) = O(g)$ and the determinant of D, i.e. the norm of D, is equal to the product of those of I_1 and I_2 (5.3).

Step 2 ($O(\max\{a_1^6 g^2,\ a_1^8\}\log^2 q)$): We consider Algorithm 4.

For Step 1, the degrees of x_1 in dT^{-1} and the HNF of dT^{-1} are $O(\max\{g,\ a_1\})$ and $O(\max\{a_1 g,\ a_1^2\})$, respectively from Proposition 18.

On the other hand, by assumption the degree of x_1 in each element in the HNF expressing the input ideal of Algorithm 4 is $O(g)$, i.e. $\deg_{x_1}(\beta_i) = O(g)$. Since there are a_1^2 pairs of $(\beta_i\delta_j)_{i,j}$, they are obtained in $O(\max\{a_1^5 g^2,\ a_1^7\}\log^2 q)$ by using Lemma 14 with $t = O(g)$ and $t' = O(\max\{a_1 g,\ a_1^2\})$, where $(\delta_j)_j$ is the ideal generated by column vectors of dT^{-1}. Using **1-1** with $m = a_1$, $n = a_1^2$, and $t = O(\max\{a_1 g,\ a_1^2\})$, the HNF N of the $a_1 \times a_1^2$ matrix is obtained in $O(\max\{a_1^6 g^2,\ a_1^8\}\log^2 q)$. And the degrees of x_1 of each element in matrix N is $O(\max\{a_1 g,\ a_1^2\})$ (note that the degree of x_1 in each element of an HNF is at most a_1 times as that of the original matrix).

For Step 2, if we apply the Gaussian elimination, $h(N^t)^{-1}$ is computed in $O(\max\{a_1^5 g^2,\ a_1^7\}\log^2 q)$ (use **2** with $m = a_1$ and $t = O(\max\{a_1 g,\ a_1^2\})$. Since the degree of x_1 of each element in matrices dT^{-1} (resp. $h(N^t)^{-1}$) is $O(\max\{g,\ a_1\})$ (resp. $O(\max\{a_1 g,\ a_1^2\})$), the matrix S is obtained in $O(\max\{a_1^4 g^2,\ a_1^6\}\log^2 q)$.

And the degree of x_1 in each element of S is $O(\max\{a_1 g,\ a_1^2\})$. Since the GCD of two polynomials of degree $O(\max\{a_1 g,\ a_1^2\})$ is computed in $O(\max\{a_1^2 g^2,\ a_1^4\}\log^2 q)$ (use **3** with $s = O(\max\{a_1 g,\ a_1^2\})$, $\mathrm{GCD}(\mathrm{GCD}(S), h)$ is computed in $O(\max\{a_1^4 g^2,\ a_1^6\}\log^2 q)$.

Since a_1^2 divisions between polynomials of degree $O(\max\{a_1 g,\ a_1^2\})$ are done (recall that the degree of x_1 in each element of S is

$O(\max\{a_1 g,\ a_1^2\})$, so is the degree of x_1 in k), W is obtained in $O(\max\{a_1^4 g^2,\ a_1^6\}\log^2 q)$.

Hence, Step 2 takes $O(\max\{a_1^6 g^2,\ a_1^8\}\log^2 q)$.

Therefore, Algorithm 4 takes $O(\max\{a_1^6 g^2,\ a_1^8\}\log^2 q)$.

Step 3 ($O(\max\{a_1^5 g^2,\ a_1^7\}\log^2 q)$): Step 3 takes $O(\max\{a_1^5 g^2,\ a_1^7\}\log^2 q)$ by using Theorem 25 with $s = O(\max\{a_1 g,\ a_1^2\})$ (recall that the degree of x_1 in each element of W is $O(\max\{a_1 g,\ a_1^2\})$.

Step 4 ($O(\max\{a_1^4 g^2,\ a_1^6\}\log^2 q)$): For $J := (\beta_i)_i$ in Step 1 and a minimal element f in W, we have $\sum_{0\le j\le a_1} \deg_{x_1}(\beta_j^i(x_1)) = O(g)$ and $\deg_{x_1}(f_j(x_1)) = O(\max\{a_1 g,\ a_1^2\})$ for $f = \sum_j f_j(x_1)x^{\gamma_j}$ and $\beta_i = \sum_j \beta_j^i(x_1)x^{\gamma_j}$.

Hence, ideal product $(f)J = (f\beta_i)_i$ is computed in $O(\max\{a_1^4 g^2,\ a_1^6\}\log^2 q)$ by using Lemma 14 with $t = O(g)$ and $t' = O(\max\{a_1 g,\ a_1^2\})$.

Since $\deg_{x_1} e = O(\max\{a_1 g,\ a_1^2\})$ and a_1^2 divisions between polynomials of degree $O(\max\{a_1 g,\ a_1^2\})$ are done, $(f)J/(e)$ is obtained in $O(\max\{a_1^4 g,\ a_1^6\})$.

Therefore, the HNF I_3 of $(f)J/(e)$ is obtained in $O(\max\{a_1^3 g^2,\ a_1^4 g\}\log^2 q)$ by using **1-2** with $m = a_1$ and $s = O(\max\{a_1 g,\ a_1^2\})$, $t = g$. $\square$

From Theorem 26, we can conclude this thesis as follows: for all algebraic function fields of one variable defined over a finite field with at least one place of degree one ($\mathbf{A}_t$-curves), where we set $\mathbf{A}_t = (a_1, \cdots, a_t)$, the Jaccobian group arithmetic is performed in $O(g^2\log^2 q)$ bit-operations if a_1 is fixed. And the complexity is the square order of the size of the input, which is the same as hyperelliptic curve case. (Note that the input size is the logarithm of the order of the Jacobian group, and the order is $O(q^g)$ from Corollary 5.)

Table 7.1: Complexity of Jacobian Group Arithmetic

	Proposed method	
	$\mathbf{A}_t$-curves	superelliptic
Step 1 (ideal product)	$O(\max\{a_1^4 g^2,\ a_1^5 g\} \log^2 q)$	$O(a^4 g^2 \log^2 q)$
Step 2 (inverse ideal)	$O(\max\{a_1^6 g^2,\ a_1^8\} \log^2 q)$	$O(a^4 g^2 \log^2 q)$
Step 3 (minimal element)	$O(\max\{a_1^5 g^2,\ a_1^7\} \log^2 q)$	$O(a^3 g^2 \log^2 q)$ (substitute $s = O(g)$ to Theorem 25)
Step 4 (ideal product)	$O(\max\{a_1^4 g^2,\ a_1^6\} \log^2 q)$	$O(a^3 g^2 \log^2 q)$
whole process	$O(\max\{a_1^6 g^2,\ a_1^8\} \log^2 q)$	$O(a^4 g^2 \log^2 q)$

Appendix

We list several implementational results (Table 8.1) of this proposed method for $\mathbf{A}_t$-curves and superelliptic curves of an actual scale used in algebraic curve cryptography, i.e. $g \log q \geq 160$.

The CPU is intel pentium III 850MHz, using LiDIA.

Table 7.2: Multiplication by 2^{160}

$\mathbf{A}_t$ $(a_1, \cdots)$	genus	average time (sec)	
		$\mathbf{A}_t$-curves	superelliptic
$(2,7)$	3	2.35	0.52
$(2,9)$	4	2.18	0.60
$(2,13)$	6	3.04	0.47
$(2,19)$	9	4.15	0.76
$(3,4)$	3	11.21	1.83
$(3,5)$	4	12.18	1.89
$(3,7)$	6	10.43	1.62
$(3,8)$	7	13.35	1.91
$(3,10)$	9	12.82	3.22
$(4,3)$	3	19.12	3.78
$(4,5)$	6	25.06	3.85
$(4,7)$	9	44.64	8.44
$(4,5,6)$	4	28.44	

Bibliography

[1] S. Arita, *Algorithms for Computations in Jacobian Group of C_{ab} Curve and Their Application to Discrete-Log Based Public Key Cryptosystems*, Conf. on The Mathematics of Public Key Cryptography, Toronto, 1999.

[2] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Addision-Wesley Publishing Company, 1969.

[3] D. G. Cantor, *Computing in the Jacobian of a hyper-elliptic curves*, Math.Comp, **48** (1987), pp. 95-101.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, GTM 138, 1993.

[5] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.

[6] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete lagarithms*, IEEE Trance. Information Theory **31** (1985), 469-472.

[7] G. Fujisaki, *Introduction to Algebraic Number Theory (Thied Edition)*, Syokabo, 2001, in Japanese.

[8] S. D. Galbraith, S. Paulus, and N. P. Smart, *Arithmetic on Superelliptic Curves*, Mathematics of Computation **71** (2002), 393-405.

[9] R. Harasawa, J. Suzuki, *Fast Jacobian Group Arithmetic on C_{ab} Curves*, in ANTS-4, Algorithmic Number Theory (Lecture Notes in Computer Science, vol 1838), 359-376, 2000.

[10] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, GTM 52, 1977.

[11] N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptography, Vol. 1, 139-150, 1989.

[12] S. Lang, *Algebraic Numbers*, Addision-Wesley Publishing Company, 1964.

[13] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptography CRYPTO '85 (Lecture Notes in Computer Science, vol 218), Springer-Verlag, 1986, pp. 417-426.

[14] S. Miura, *Linear Codes on Affine Algebraic Cuves*, Trans. of IEICE, vol. J81-A, No. 10 (1998), pp. 1398-1421, in Japanese.

[15] S. Paulus, *Lattice basis reduction in function field* in ANTS-3, Algorithmic Number Theory(Lecture Notes in Computer Science, vol 1423), 567-575, 1998.

[16] S. Paulus and A. Stein, *Comparing Real and Imaginary Arithmetics for Divisor Class Groups of Hyperelliptic Curves* in ANTS-3, Algorithmic Number Theory(Lecture Notes in Computer Science, vol 1423), 576-591, 1998.

[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1994.

[18] N. P. Smart, *On the performance of Hyperelliptic Cryptosystems*, Advances in Cryptology EUROCRYPTO'99 (Lecture Notes in Computer Science vol 1592), 165-175, 1998.

[19] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Springer-Verlag, 1993.

[20] E. J. Volcheck, *Computing in the Jacobian of a plane algebraic curve*, ANTS-1, Algorithmic Number Theory (Lecture Notes in Computer Science, vol 877), 221-233, 1994.