Université d'Ottawa · University of Ottawa

HYPERELLIPTIC CURVES AND THEIR APPLICATIONS TO CRYPTOGRAPHY

By
Deholo Nali
March 2002

A Thesis
submitted to the School of Graduate Studies and Research
in partial fulfillment of the requirements
for the degree of
Master of Science in Mathematics[1]

[1]The M.Sc. Program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

Cryptosystems based on hyperelliptic curves were first presented by N. Koblitz, in 1989 (c.f. [11]). In 1996, a first attempt was made to give an elementary introduction to hyperelliptic curves (c.f. [3]). This introduction aimed at presenting these curves to readers having knowledge of undergraduate ring theory. The tentative was difficult because many definitions and results had to be ad-hoc and unmotivated.

The aim of this thesis is to present hyperelliptic curves to readers having completed a first graduate course in commutative algebra. The approach is that of Algebraic Number Theory. All necessary definitions are stated and all crucial results proved and explained. In fact, above the mere presentation of hyperelliptic curves lies the objective of introducing cryptosystems constructed using such curves and of addressing practical issues relevant to the implementation of these cryptosystems.

We proceed by describing hyperelliptic function fields and by discussing computational aspects of ideal theory in these algebraic structures. Then we introduce the Jacobian of a hyperelliptic curve and use our previous developments on ideal theory to draw conclusions on the structure and computational laws of the Jacobian. Finally, we present hyperelliptic Jacobian-based cryptosystems and discuss the practical issues of message encoding and divisor compression.

Acknowledgements

Praise be to the everlasting God! My heart is full of praise for His continuous sustenance, inspiration, encouragement, guidance and provision in the lonely and difficult times. Without my personal relationship with Jesus-Christ, this thesis would never have matured.

I am grateful to my parents for their trust in my potential and their continuous prayers on my behalf. I am also thankful to the rest of my family: not only to my dear and lovely wife, Madeleine (for your beauty and your continuous encouragements during my master's), but also to Myra, Aubert, Emmanuel, Josué and Agnès Nali ("On se tient les coudes").

I also would like to wholeheartedly thank my supervisor, professor Damien Roy, for his many precious suggestions, his financial support and his patience towards me. I am also thankful to professor Gary Walsh, whose teaching of cryptography motivated me greatly.

I had the pleasure of studying with Geneviève Labonté and Fabien Roche: thank you both for your encouragements and friendship. My thanks also to Patrick Boily (cher "idéal premier", merci pour tous tes conseils), Alain Lebel and Guy Beaulieu (for organizing the valuable Graduate Student Lecture Series), Catalín and Andrea Rada (for your true friendship), Corina Olah and Adela Comanici (for your friendliness), and Isabella Weinstabel (I told you that your name would appear:).

Finally, I gratefully acknowledge the financial support from an Ontario Graduate Scholarship in Science and Technology.

Ottawa, Ontario
March 25, 2002

Deholo Nali

Table of Contents

Abstract ii

Acknowledgements iii

Table of Contents iv

1 Algebraic and Number Theoretic Foundation 1
- 1.1 Introduction . . . 1
- 1.2 Order of an Ideal in a Dedekind Domain . . . 6

2 Description of a Hyperelliptic Function Field 9
- 2.1 Introduction . . . 9
- 2.2 Description of the Fractional Ideals of B_K . . . 16
- 2.3 Decomposition of Prime Ideals of A in B_K . . . 24
- 2.4 Uniformizing Parameter of Prime Ideals of B_K . . . 28
- 2.5 Computing the order of a principal fractional ideal of B_K . . . 29
- 2.6 Application of Uniformizing Parameters . . . 31
- 2.7 Units of B_K . . . 37
- 2.8 Results over the Algebraic Closure $\overline{K}$ of K . . . 37

3 Construction of a Hyperelliptic Jacobian 39
- 3.1 Introduction . . . 39
- 3.2 Semi-reduced fractional ideals . . . 40
- 3.3 Reduced Fractional Ideals . . . 42
- 3.4 Computation in $\mathbb{I}_K^*/\mathbb{P}_K^*$ . . . 45
- 3.5 Introduction to divisors . . . 49
- 3.6 Correspondence between ideals and divisors . . . 50
- 3.7 Hyperelliptic Jacobian . . . 54

4 Applications to Cryptography **59**
4.1 Introduction 59
4.2 Message Encoding 62
4.2.1 Generating Points on a Hyperelliptic Curve 62
4.2.2 Message Encoding 66
4.3 Divisor Compression 68
4.3.1 Compression Algorithm 69
4.3.2 Decompression Algorithm 70
4.4 Examples 73
4.4.1 A Hyperelliptic Curve defined over $\mathbb{F}_{3^2}$ 73
4.4.2 A Hyperelliptic Curve defined over $\mathbb{F}_{2^3}$ 74
4.4.3 Structure of $\mathbb{J}(\mathbb{F}_2)$ for an given Hyperelliptic Curve 75
4.4.4 Illustration of Divisor Compression 77
4.4.5 Illustration of ElGamal Encryption 78
4.5 Future Work 80

Chapter 1

Algebraic and Number Theoretic Foundation

In this chapter, we introduce the algebraic infrastructure for further developments on Hyperelliptic Curves. We present Dedekind domains and discuss the factorization of ideals in this special type of rings.

Throughout this chapter (and the following ones), rings will always be assumed to be commutative.

1.1 Introduction

In this section, we present fundamental properties of the integral closure of a Dedekind domain in an algebraic separable extension of its quotient field.

Definition 1.1.1. (Integral Closure of a Ring)

Let R_1 be a ring and R_2 be a subring of R_1. The *integral closure* of R_2 in R_1 is the set of elements $r \in R_1$ that are, each, a root of a monic polynomial $p(u) \in R_2[u]$. Such elements of R_1 are said to be *integral* over R_2.

Moreover, an integral domain R is said to be *integrally closed* if the integral closure of R in the field of fractions of R is R itself.

Definition 1.1.2. (Algebraic Elements)

Let $F \subseteq E$ be a field extension. An element $e \in E$ that is integral over F is said to be *algebraic over* F. Moreover, the *integral closure* of F in E is called the *algebraic closure* of F in E. Furthermore, a field extension $F \subseteq E$ such that every element of E is algebraic over F is called an *algebraic extension* of F. Finally, if an element $e \in E$ is algebraic over F, and if $m(u) \in F[u]$ is the monic polynomial of minimal degree such that $m(e) = 0$, then $m(u)$ is called the *minimal polynomial* of e over F.

Definition 1.1.3. (Noetherian Ring)

A ring R is said to be *Noetherian* if any ideal I of R is finitely generated i.e. if there exist $r_1, \cdots, r_n \in I$ such that $I = \langle r_1, \cdots, r_n \rangle_R$.

Definition 1.1.4. (Normal Field Extension)

Let $F \subseteq E$ be an algebraic field extension. The field E is said to be *normal* if the minimal polynomial, over F, of any element of E splits completely over E.

Definition 1.1.5. (Separable Field Extension)

Let $F \subseteq E$ be an algebraic field extension. The field E is said to be *separable* if the minimal polynomial of any element of E has distinct roots.

Definition 1.1.6. (Galois Group)

Let F be a field and E be a finite normal separable extension of F. The *Galois group* $Gal(E/F)$ of E over F consists of the F-automorphisms of E.

Remark 1.1.1. $|Gal(E/F)| = [E : F]$.

Theorem 1.1.1. *Let A be an integral domain, F its field of fractions, E an algebraic field extension of F and B the integral closure of A in E. Then, the field $Frac(B)$ of fractions of B is E. Moreover, if A is an integrally closed Noetherian ring and E is a finite separable extension of F, then B is a Noetherian ring.*

Proof.

- Let $s \in E$. Then, since E is algebraic over F, there exists $\alpha(u) \in F[u]$ such that $\alpha(s) = 0$. Now, multiplying $\alpha(s)$ by an appropriate non-zero element of A, we get $\beta(s) = 0$ with $\beta(u) \in A[u]$. Then, if w is the coefficient of the highest power of u in $\beta(u)$, then ws is integral over A. So $ws = b$ for some $b \in B$. So $s = \frac{b}{w} \in Frac(B)$.

- Assume now that A is Noetherian and integrally closed, and that E is a finite separable extension of F. We will prove that B is contained in a finitely generated A-module.

  By the primitive element theorem for separable extensions, E can be written as $F[s]$ for some $s \in E$ and, if $[E : F] = n$, then $\{1, s, \cdots, s^{n-1}\}$ is an F-basis of E. In fact, one may assume that $E = F[t]$, where $t = rs \in B$ for some appropriate $r \in A$. Then $\{t^i\}_{i=0}^{n-1}$ is an F-basis of E with elements in B.

  Now, let $b \in B$: then $b = \alpha(t)$ for some $\alpha(u) = \sum_{i=0}^{n-1} f_i u^i \in F[u]$.

  Let also $\mu_{t,F}(u) \in F[u]$ be the minimal polynomial of t over F, and L be the splitting field of $\mu_{t,F}(u)$. Then, let $t_0 = t, t_1, \cdots, t_{n-1}$ be the roots of $\mu_{t,F}(u)$. Note that all these roots are distinct since E is a separable extension of F.

  Now, for $j = 0, \cdots, n-1$, define $b_j = \alpha(t_j)$. Then, let T be the $n \times n$ matrix such that $T_{i+1,j+1} = t_j^i$ for all $i, j \in \{0, 1, \cdots, n-1\}$. Finally, let $\mathbf{f} = (f_0, \cdots, f_{n-1})$, and $\mathbf{b} = (b_0, \cdots, b_{n-1})$.

  Then $\mathbf{f}T = \mathbf{b}$. Thus, $\mathbf{f}TAdj(T) = \mathbf{b}Adj(T)$. So $\mathbf{f}det(T) = \mathbf{b}Adj(T)$ and, by the

same reasoning, $\mathbf{f}det(T)^2 = \mathbf{b}Adj(T)det(T)$.

Note that $det(T) \neq 0$ since $det(T)$ is a Vandermonde determinant and $t_0, \cdots, t_{n-1}$ are all distinct.

Now, if we show that $\mathbf{f}det(T)^2 \in A^n$, then we will have shown that $b = \alpha(t) \in \bigoplus_{i=0}^{n-1} A\frac{t^i}{det(T)^2}$, where $det(T)$ is fixed. Thus we will have shown that B is contained in a finitely generated A-module. Hence, since A is Noetherian, we will have proved that B is Noetherian as an A-module and, therefore, as a ring.

So, we need to show that $f_i det(T)^2 \in A$, for $i = 0, \cdots, n-1$. For this, note that, since A is integrally closed, it is sufficient to show that $f_i det(T)^2 \in F$ and $f_i det(T)^2 \in B$, for $i = 0, \cdots, n-1$.

But $Gal(L/F)$ permutes the rows of T. So $det(T)^2 \in F$. So $f_i det(T)^2 \in F$ for $i = 1, \cdots, n-1$. Moreover, note that all entries of T are integral over A, since $t \in B$ is integral over A and so are its conjugates $t_0, \cdots, t_{n-1}$ under $Gal(L/F)$. So, $det(T)$ and all the entries of $Adj(T)$ are integral over A. Hence, all the entries of $\mathbf{f}det(T)^2 = \mathbf{b}Adj(T)det(T)$ belong to B.

Consequently, B is a Noetherian ring.

□

Definition 1.1.7. (Dedekind Domain)

An integral domain R is said to be a *Dedekind domain* if it is Noetherian, integrally closed, and if any non-zero prime ideal of R is maximal.

Theorem 1.1.2. *Let A be a Dedekind domain, F its field of quotients, E a finite separable field extension of F and B the integral closure of A in E. Then B is a Dedekind domain.*

Proof. • B is integrally closed in E by construction since it is the integral closure

of A in E.

- B is Noetherian by Theorem 1.1.1.
- Finally, considering, for any non-zero prime ideal P' of B, the sequence $A \rightarrow B \rightarrow B/P'$ of surjective homomorphisms, we obtain the injection $A/A \cap P' \hookrightarrow B/P'$. But $P' \cap A$ is a prime and, hence, maximal ideal of A. So, $A/P' \cap A$ can be identified to a subfield of B/P' over which B/P' is integral. Consequently, B/P' is a field. (This short argument can also be found on page 59 of [14])

□

Definition 1.1.8. (Fractional Ideal)

Let A be an integral domain and $F = Frac(A)$. A *fractional ideal* of A is an A-submodule I of F such that there exists $d \in A$ satisfying $d \neq 0$ and $dI \subseteq A$.

Theorem 1.1.3. (Factorization of Fractional Ideals in a Dedekind Domain)

Let A be a Dedekind domain and $\mathcal{P}$ be the set of non-zero prime ideals of A. Then, any fractional ideal I of A can be written uniquely as $I = \prod_{P \in \mathcal{P}} P^{n_P(I)}$ where the $n_P(I)$ are integers which are all equal to 0, except for a finite number of prime ideals $P \in \mathcal{P}$.

Proof. See §3.4 of [14]. □

Lemma 1.1.4. (Lying Over)

Let A be a ring and B be an integral extension of A (i.e. any element of B is integral over A). Then for each prime ideal P of A, there is a prime ideal P' of B such that $P' \cap A = P$.

Proof. See Theorem 28.12, on page 459 of [8]. □

Theorem 1.1.5. (Decomposition of prime ideals of a Dedekind domain A in the integral closure of an algebraic separable extension of $Frac(A)$)

Let A be a Dedekind domain, F its field of fractions, E a finite normal separable field extension of F, $n = [E : F]$ its relative degree, B the integral closure of A in E and P a non-zero prime ideal of A. Then the following are true:

(a) BP is an ideal of B which factors as a product $BP = \prod_{i=1}^{q} P_i^e$, where $P_1, \cdots, P_q$ are the prime ideals of B lying over P and e is a positive integer. Moreover, all the P_i's are conjugate with respect to $Gal(E/F)$.

(b) $qer = [B/BP : A/P] = n$, where r denotes the dimension of the vector space B/P_i over A/P, which is independent of i.

(c) $B/BP \cong \prod_{i=1}^{q}(B/P_i)^e$

Proof. See §5.2 of [14]. □

1.2 Order of an Ideal in a Dedekind Domain

Building on the unique factorization of ideals in Dedekind domain, we now introduce the concept of order of an ideal and present a few properties of the order function.

Definition 1.2.1. (Order of an Ideal)

Let $I = \prod_{i=0}^{q} P_i^{e_i}$ be the factorization of a fractional ideal I of a Dedekind domain B. The *order* $ord_P(I)$ of I at a non-zero prime ideal P of B is defined by

$$ord_P(I) = \begin{cases} e_i & \text{if } P = P_i \text{ for some } i \in \{1, \cdots, q\}. \\ 0 & \text{otherwise.} \end{cases}$$

This defines a function ord_P from the set $\mathcal{I}$ of fractional ideals of B to $\mathbb{Z}$.

Lemma 1.2.1. (Homomorphic Property of the Order Function)

Let I_1 and I_2 be two fractional ideals of a Dedekind domain B and P be non-zero prime ideal of B. Then $ord_P(I_1 I_2) = ord_P(I_1) + ord_P(I_2)$.

Proof. For $j = 1, 2$, let $I_j = \prod_{i=1}^{q} P_i^{e_{j,i}}$ be the factorization of I_j as a product of prime ideals of B. Then

$$\begin{aligned} ord_{P_i}(I_1 I_2) &= ord_{P_i}(\prod_{i=1}^{q} P_i^{e_{1,i}} \prod_{i=1}^{q} P_i^{e_{2,i}}) \\ &= ord_{P_i}(\prod_{i=1}^{q} P_i^{e_{1,i}+e_{2,i}}) \\ &= e_{1,i} + e_{2,i} \\ &= ord_{P_i}(I_1) + ord_{P_i}(I_2) \end{aligned}$$

□

Definition 1.2.2. (Gcd of Fractional Ideals)

Let B be a Dedekind domain and $I_1 = \prod_{i=1}^{q} P_i^{e_1}$, $I_2 = \prod_{i=1}^{q} P_i^{e_2}$ be two fractional ideals of B, written as products of non-zero prime ideals of B.

The *greatest common divisor* $gcd(I_1, I_2)$ of I_1 and I_2 is defined as

$$gcd(I_1, I_2) = \prod_{i=1}^{q} P_i^{min\{e_1, e_2\}}.$$

Lemma 1.2.2. *Let B be a Dedekind domain and I_1, I_2 be two fractional ideals of B. Then*

$$I_1 + I_2 = gcd(I_1, I_2).$$

Proof. • Suppose first that I_1 and I_2 are ordinary ideals of B, and let P be a prime ideal of B.

Note that, for any ideal I of B, we have

$$ord_P(I) = max\{e \in \mathbb{N} \mid P^e \supseteq I\} \tag{1.2.1}$$

Note also that, for any positive integer $e \in \mathbb{N}$, we have

$$\begin{aligned} I_1 + I_2 \subseteq P^e &\Leftrightarrow I_j \subseteq P^e \text{ for } j = 1, 2, \\ &\Leftrightarrow ord_P(I_j) \geq e \text{ for } j = 1, 2, \\ &\Leftrightarrow min_{j=1,2}\{ord_P(I_j)\} \geq e. \end{aligned}$$

Hence, equation 1.2.1 implies that

$$min_{j=1,2}\{ord_P(I_j)\} = max\{e \in \mathbb{N} \mid P^e \supseteq I\} = ord_P(I_1 + I_2).$$

But $gcd(I_1, I_2) = \prod_{i=1}^{q} P_i^{min_{j=1,2}\{ord_{P_i}(I_j)\}}$. So $gcd(I_1, I_2) = I_1 + I_2$.

- Suppose now that I_1 and I_2 are fractional ideals of B. Recall that there exists $b \in B$ such that bI_1 and bI_2 are ordinary ideals of B. So, by the above result, $gcd(bI_1, bI_2) = bI_1 + bI_2 = b \cdot (I_1 + I_2)$. But, it is clear that $gcd(bI_1, bI_2) = b \cdot gcd(I_1, I_2)$. So $gcd(I_1, I_2) = I_1 + I_2$.

□

Definition 1.2.3. (Uniformizing parameter)
Let R be a ring and P be a prime ideal of R. A *uniformizing parameter* p for P is an element $p \in P$ such that $p \notin P^2$.

Lemma 1.2.3. (Existence of a uniformizing parameter in a Dedekind domain)
Let B be a Dedekind domain and P be a non-zero prime ideal of B. Then P has a uniformizing parameter.

Proof. Otherwise, $P \subseteq P^2$. But $P^2 \subseteq P$. So $P^2 = P$, which contradicts the unique factorization of ideals in the Dedekind domain B. □

Chapter 2

Description of a Hyperelliptic Function Field

In this chapter, we define hyperelliptic curves and their function fields. We also thoroughly describe the fractional ideals of a hyperelliptic function field and present computational applications to the concept uniformizing parameter of a prime ideal.

2.1 Introduction

In this section, hyperelliptic curves are introduced, along with their corresponding function fields.

Definition 2.1.1. (Hyperelliptic curve)

- A *hyperelliptic curve* C of genus $g \geq 1$ over a field K is the set of points $(u, v) \in \overline{K} \times \overline{K}$ satisfying an equation of the form 2.1.1, along with a point at infinity, denoted ∞.

$$v^2 + h(u)v = f(u). \tag{2.1.1}$$

  where

- $h(u) \in K[u]$ and $deg(h) \leq g$.
- $f(u) \in K[u]$ is monic and $deg(f) = 2g + 1$.
- there are no singular points on C, i.e. no solutions $(u, v) \in \overline{K} \times \overline{K}$ of equation 2.1.1 which simultaneously satisfy the two partial derivative equations

$$\begin{cases} 2v - h(u) & = 0 \\ h'(u)v - f'(u) & = 0 \end{cases}$$

- $C(K)$ denotes the set of points (u, v) of C such that $(u, v) \in K \times K$.

Definition 2.1.2. (Perfect Fields)

A field K is said to be *perfect* if its characteristic is 0 or if every element $x \in K$ verifies $x = y^{char(K)}$ for some $y \in K$.

Example 2.1.1. *Any finite field is a perfect field.*

Remark 2.1.1.
- In cryptography, one is interested in finite fields for implementation reasons. Moreover, note that one may not be able to consider the Galois group of some pathological extensions of non-perfect fields.
- In the remaining of this chapter (and in chapter 3), C will denote a fixed hyperelliptic curve defined using equation 2.1.1 over a fixed perfect field K.

Lemma 2.1.1. *The polynomial $m(u, v) = v^2 + h(u)v - f(u) \in K[u][v]$ (obtained from equation 2.1.1) is irreducible over $\overline{K}[u]$.*

Proof. If $m(u, v)$ were not irreducible over $\overline{K}[u]$, it would factor as $m(u, v) = (v - a(u))(v - b(u))$ with $a(u), b(u) \in \overline{K}[u]$. But then, $deg(ab) = deg(f) = 2g + 1$, which contradicts the fact that $deg(a + b) = deg(h) \leq g$. So, $m(u, v)$ is irreducible over $\overline{K}[u]$. □

Consider now the following construction:

- Let $A = K[u]$, $K(u) = Frac(K[u])$ and $K(C) = K(u)[\overline{v}]$ where $K(u)[\overline{v}] = K(u)[v]/(m(u,v))$ ($K(C)$ is called the *function field* of C).
- Then, let then B_K be the integral closure of $K[u]$ in $K(C)$.

We want to show that B_K is a Dedekind domain and that $K(C)$ is a Galois field extension of $K(u)$. We shall proceed by presenting the two following intermediate results.

Lemma 2.1.2. *$K(C)$ is a separable extension of $K(u)$.*

Proof. It is sufficient to show that the quadratic minimal polynomial $m(u,v)$ of $\overline{v}$ has 2 distinct roots. Knowing that $m(u,\overline{v}) = \overline{v}^2 + h(u)\overline{v} - f(u) = 0$, we see that the roots of $m(u,v)$ are $\overline{v}$ and $-\overline{v} - h(u)$ (so that their sum equals $-h(u)$). We then distinguish two cases:

- If $char(K) \neq 2$, then consider the change of variables $u \mapsto u, v \mapsto v - \frac{h}{2}$. This draws a bijection between C and the hyperelliptic curve C', defined over K by the equation $\mathbf{v}^2 = \mathbf{f}(u)$, where $\mathbf{v} = v - \frac{h}{2}$ and $\mathbf{f} = f + \frac{h^2}{4}$. It also induces an isomorphism between $K(u)[\overline{v}]$ and $K(u)[\overline{\mathbf{v}}] = K(u)[\mathbf{v}]/(\mathbf{m}(u,\mathbf{v}))$, where $\mathbf{m}(u,\mathbf{v}) = \mathbf{v}^2 - \mathbf{f}(u)$. Thus, if $K(u)[\overline{\mathbf{v}}]$ is a separable extension of $K(u)$, then so is $K(C)$ with respect to $K(u)$.

  Now, in order to prove that $K(u)[\overline{\mathbf{v}}]$ is a separable extension of $K(u)$, it suffices to show that the two roots of $\mathbf{m}(u,\mathbf{v}) = \mathbf{v}^2 - \mathbf{f}(u)$ are distinct. But these two roots are $\overline{\mathbf{v}}$ and $-\overline{\mathbf{v}}$. So they are distinct, because $\mathbf{m}(u,0) = \mathbf{f}(u)$ and $\mathbf{f}(u) \neq 0$ (note that $deg(\mathbf{f}) = 2g+1$).

- If $char(K) = 2$, then the two roots of $m(u, v)$ are $\overline{v}$ and $-\overline{v} - h(u) = \overline{v} + h(u)$. But, we know that $h(u) \neq 0$ (otherwise, any solution $x \in \overline{K}$ of the partial derivative equation $h'(u)v - f'(u) = f'(u) = 0$ yields a singular point (x, y) of $\mathcal{C}$ - which is impossible). Thus, $\overline{v} \neq \overline{v} + h(u)$.

□

Lemma 2.1.3. *$K(\mathcal{C})$ is a normal field extension of $K(u)$.*

Proof. The two roots of the minimal polynomial $m(u, v)$ of $\overline{v}$ are $\overline{v}$ and $-\overline{v} - h(u)$, which both belong to $K(\mathcal{C}) = K(u)[\overline{v}]$. So $K(\mathcal{C})$ is a normal extension of $K(u)$. □

Thus, we note that:

- $K[u]$ is clearly a Dedekind domain (it is a P.I.D.).
- B_K is also a Dedekind domain by Theorem 1.1.2, since $K(\mathcal{C})$ is a finite separable field extension of $K(u) = Frac(K[u])$ and $K[u]$ is a Dedekind domain.
- $K(\mathcal{C})$ is a Galois extension of $K(u)$ since it is normal, separable and of finite degree.
- The Galois group $G = Gal(K(\mathcal{C})/K(u))$ consists of the two $K(u)$-automorphisms $Id : u \mapsto u, \overline{v} \mapsto \overline{v}$ and $\sigma : u \mapsto u, \overline{v} \mapsto -\overline{v} - h(u)$.

Let us now finish this section by presenting an explicit description of B_K.

Lemma 2.1.4. *Let $K[u, \overline{v}] = K[u, v]/(m(u, v))$. Then $B_K = K[u, \overline{v}]$.*

Proof. • First, note that B_K contains $K[u]$ and $\overline{v}$ (since $m(u, \overline{v}) = \overline{v}^2 + h(u)\overline{v} - f(u) = 0$). So, B_K contains $K[u, \overline{v}]$.

- Let us now prove that $B_K \subseteq K[u, \overline{v}]$.

  Let $s = \frac{\alpha}{\gamma} - \frac{\beta}{\gamma}\overline{v} \in B_K$, where α, β and γ are elements of $K[u]$ that have no common roots. Then

$$tr(s) = tr_{B_K/K(u)}(s) = s + \sigma(s) = \frac{2\alpha}{\gamma} - \frac{\beta}{\gamma}(-h) = \frac{2\alpha + \beta h}{\gamma}$$

  and

$$N(s) = N_{B/K(u)}(s) = s \cdot \sigma(s) = \left(\frac{\alpha}{\gamma}\right)^2 + \left(\frac{\alpha}{\gamma}\right)\left(\frac{\beta}{\gamma}\right)h - \left(\frac{\beta}{\gamma}\right)^2 f = \frac{\alpha^2 + \alpha\beta h - \beta^2 f}{\gamma^2}.$$

  Now, $tr(s), N(s) \in K(u)$ and $tr(s), N(s) \in B_K$. Since $K[u]$ is integrally closed, this implies that $tr(s), N(s) \in K[u]$. Hence:

$$\gamma | (2\alpha + \beta h). \tag{2.1.2}$$

$$\gamma^2 | (\alpha^2 + \alpha\beta h - \beta^2 f). \tag{2.1.3}$$

  Also, $s\overline{v} \in B_K$: so

$$(-\frac{\beta}{\gamma} f) + (\frac{\alpha}{\gamma} + \frac{\beta h}{\gamma})\overline{v} \in B_K \tag{2.1.4}$$

  Let us break down our analysis into two cases:

  - Suppose $char(K) = 2$:

    Then equation 2.1.2 becomes $\gamma | \beta h$. So equation 2.1.3 implies that $\gamma | (\alpha^2 - \beta^2 f)$, and equation 2.1.4 that $-\frac{\beta}{\gamma} f + \frac{\alpha}{\gamma}\overline{v} \in B_K$.

    Note that, from $-\frac{\beta}{\gamma} f + \frac{\alpha}{\gamma}\overline{v} \in B_K$, it is possible to show that $\gamma | \alpha h$, in the same way that we showed, from $s = \frac{\alpha}{\gamma} - \frac{\beta}{\gamma}\overline{v} \in B_K$, that $\gamma | \beta h$. So $\gamma | gcd(\beta h, \alpha h)$, and, hence, $\gamma | gcd(\beta, \alpha) h$. But $gcd(\gamma, gcd(\beta, \alpha)) = 1$ as α, β and γ have no common roots. So

$$\gamma | h \tag{2.1.5}$$

(and thus, $hI \subseteq K[u, \overline{v}]$).

Now, equation 2.1.3 implies that γ divides $\alpha^2 + \alpha\beta h - \beta^2 f$ and its derivative. So

$$\gamma | (\alpha^2 + \alpha\beta h - \beta^2 f) \tag{2.1.6}$$

$$\gamma | (2\alpha\alpha' + \alpha' \beta h + \alpha\beta' h + \alpha\beta h' - 2\beta\beta' f - \beta^2 f') \tag{2.1.7}$$

Thus, since $\gamma | h$ and $char(K) = 2$, we get, from equation 2.1.7, that

$$\gamma | (\alpha\beta h' - \beta^2 f') \tag{2.1.8}$$

Now, if $\gamma \notin K$, then there exists $\eta \in \overline{K}$ s.t. $\gamma(\eta) = 0$. Then $h(\eta) = 0$. Now, if $\beta(\eta) = 0$, then equation 2.1.6 implies that $\alpha(\eta) = 0$. Then η is a common root of α, β and γ, which is impossible by hypothesis. So $\beta(\eta) \neq 0$. So, using equation 2.1.6, we deduce that $(\eta, \frac{\alpha(\eta)}{\beta(\eta)})$ is a point of $\mathcal{C}$. Then, equation 2.1.8 implies that $\frac{\alpha(\eta)}{\beta(\eta)} h'(\eta) - f'(\eta) = 0$ i.e. that one of the partial derivatives of $m(u, v)$ at $(\eta, \frac{\alpha(\eta)}{\beta(\eta)})$ is 0. But $h(\eta) = 0$ implies that the other partial derivative $2\overline{v} + h = h$ of $m(u, v)$ at $(\eta, \frac{\alpha(\eta)}{\beta(\eta)})$ is also 0. This is then a contradiction since $\mathcal{C}$ has no singular points. Hence, $\gamma \in K$ and, consequently, $s \in K[u, \overline{v}]$.

– Suppose now that $char(K) \neq 2$.

Let us consider the change of variables $u \longmapsto u, v \longmapsto v - \frac{h}{2}$. This draws a bijection between $\mathcal{C}$ and the hyperelliptic curve $\mathcal{C}'$, defined over K by the equation $\mathbf{v}^2 = \mathbf{f}(u)$, where $\mathbf{v} = v - \frac{h}{2}$ and $\mathbf{f} = f + \frac{h^2}{4}$. It also induces an isomorphism λ between $K[u, \overline{v}]$ and $K[u, \overline{\mathbf{v}}]$, which extends to $K(u, \overline{v})$ and $K(u, \overline{\mathbf{v}})$. Assume now that the integral closure $\mathbf{B_K}$ of $K[u]$ in $K(u, \overline{\mathbf{v}})$ is $K[u, \overline{\mathbf{v}}]$. Then, if $\omega \in B_K$, we have $\lambda(\omega) \in \mathbf{B_K} = K[u, \overline{\mathbf{v}}]$ and, therefore,

$\omega \in \lambda^{-1}(K[u,\overline{v}]) = K[u,\overline{v}]$. Hence, for our goal, it is sufficient to assume that $h(u) = 0$ and to prove directly that $B_K = K[u,\overline{v}]$.

Now, note that f has no repeated roots (otherwise, any repeated root x of f would yield the singular point $(x,0)$ of $\mathcal{C}$, which is impossible).

Recall that $tr(s) = \frac{2\alpha - \beta h}{\gamma} = \frac{2\alpha}{\gamma} \in K[u]$ and $N(s) = \frac{\alpha^2 + \alpha\beta h - \beta^2 f}{\gamma^2} = \frac{\alpha^2 - \beta^2 f}{\gamma^2} \in K[u]$. Thus, $X = tr(s)^2 + 4N(s) \in K[u]$. So $X = \frac{4\alpha^2}{\gamma^2} - 4\frac{\alpha^2 - \beta^2 f}{\gamma^2} = 4\frac{\beta^2}{\gamma^2} f \in K[u]$. So $\gamma^2 | \beta^2 f$. But f has no repeated roots. So $\gamma | \beta$. Therefore, equation 2.1.2 implies that $\gamma | \alpha$.

Hence, $s = \frac{\alpha}{\gamma} - \frac{\beta}{\gamma}\overline{v} \in K[u,\overline{v}]$ and, consequently, $B_K \subseteq K[u,\overline{v}]$.

We now have proved that $B_K = K[u,\overline{v}]$.

□

Remark 2.1.2.

- Since $\overline{v}^2 = f(u) - h(u)\overline{v}$, one can always present an element $\omega(u,\overline{v})$ of B_K in the form $\omega(u,\overline{v}) = a(u) - b(u)\overline{v}$, where $a(u), b(u) \in K[u]$. Hence, $B_K = K[u] \oplus K[u]\overline{v}$.

- Note that, since $B_K = K[u,\overline{v}]$, another notation for B_K is $K[\mathcal{C}]$.

$$\begin{array}{ccc} K[\mathcal{C}] = B_K = K[u,\overline{v}] & \overset{Frac}{\hookrightarrow} & K(\mathcal{C}) = K(u)[\overline{v}] \\ | & & |2 \\ A = K[u] & \overset{Frac}{\hookrightarrow} & F = K(u) \end{array}$$

2.2 Description of the Fractional Ideals of B_K

In this section, the fractional ideals of B_K are precisely described. But before dealing with the fractional ideals, the ordinary ideals of B_K are carefully studied.

If $\omega_1, \omega_2 \in B_K$, we will denote by $\langle \omega_1, \omega_2 \rangle_{K[u]}$, the $K[u]$-submodule of B_K generated by ω_1 and ω_2, i.e. the set of all $K[u]$-linear combinations of ω_1 and ω_2.

Lemma 2.2.1. *Let M be a $K[u]$-submodule of B_K that has rank 2.*

Then, there exist unique polynomials $c(u), d_0(u), d_1(u) \in A = K[u]$ such that $d_0(u)$ and $d_1(u)$ are monic, $deg(c(u)) < deg(d_0(u))$ and

$$M = \langle d_0(u), c(u) - d_1(u)\overline{v} \rangle_A.$$

More precisely, $d_1(u)$ is the monic generator of the ideal

$$J_1 = \{q(u) \in K[u] \mid \exists p(u) \in K[u] \text{ s.t. } p(u) - q(u)\overline{v} \in M\}$$

and $d_0(u)$ is the monic generator of

$$J_0 = M \cap K[u].$$

Proof. • Existence:

Note first that $d_1(u) \neq 0$: otherwise $M \subseteq J_0 \subseteq K[u]$, which implies that $rank(M) \leq 1$ and thereby contradicts $rank(M) = 2$. Moreover, note that $d_0(u)$ and $d_1(u)$ can be chosen to be monic as K is a field.

Now, let $p(u) \in K[u]$ s.t. $\delta = p(u) - d_1(u)\overline{v} \in M$. Consider M', the $K[u]$-submodule of B_K defined by $M' = \langle \delta \rangle_A + J_0$. Let us show that $M = M'$.

Clearly, $M' \subseteq M$ as $\delta \in M$ and $J_0 \subseteq M$. Now, for any $\omega = a(u) - b(u)\overline{v} \in M$, note that $b(u) \in J_1 = \langle d_1(u) \rangle_A$. Thus, let $\beta(u) \in K[u]$ such

that $b(u) = \beta(u)d_1(u)$ and note that $\omega' = \omega - \beta\delta = a(u) - \beta p(u) \in J_0$. So $\omega = \beta\delta + (a - \beta p) \in M'$. Hence $M \subseteq M'$ and, therefore, $M = M'$. Consequently, $M = \langle d_0(u), \delta \rangle_A$.

Now, subtracting, from δ, an appropriate multiple $d_0(u)\gamma(u)$ of $d_0(u)$, we obtain $c(u) - d_1(u)\overline{v}$, such that $deg(c(u)) < deg(d_0(u))$.

Then $M = \langle d_0(u), c(u) - d_1(u)\overline{v} \rangle_A$.

- Uniqueness:

  Suppose that, for $i = 1, 2$, there exist polynomials $c_i(u), d_{0,i}(u), d_{1,i}(u) \in K[u]$ such that $d_{0,i}(u)$ and $d_{1,i}(u)$ are monic, $deg(c_i) < deg(d_{0,i})$ and

  $M = \langle d_{0,i}(u), c_i(u) - d_{1,i}(u)\overline{v} \rangle_A$.

  We find that $\langle d_{0,i} \rangle_A = J_0 = M \cap K[u]$ for $i = 1, 2$; hence $d_{0,1} = d_{0,2}$ as $d_{0,1} | d_{0,2}, d_{0,2} | d_{0,1}$ and both $d_{0,1}$ and $d_{0,2}$ are monic. Similarly, $\langle d_{1,i} \rangle_A = J_1$ for $i = 1, 2$, and, therefore, $d_{1,1} = d_{1,2}$. Finally, $c_1 - c_2 = (c_1(u) - d_{1,1}(u)\overline{v}) - (c_2(u) - d_{1,2}(u)\overline{v}) \in M \cap K[u] = J_0 = \langle d_{0,1} \rangle_A$; hence, $d_{0,1} | (c_1 - c_2)$. But $deg(c_i) < deg(d_{0,i})$ for $i = 1, 2$, and $d_{0,1} = d_{0,2}$. So $c_1 - c_2 = 0$ i.e. $c_1 = c_2$.

□

Theorem 2.2.2. *Let I be a non-zero ideal of B_K.*

Then, there exist unique polynomials $a(u), b(u), d(u) \in K[u]$ such that $a(u)$ and $d(u)$ are monic, $deg(b) < deg(a)$ and

$$I = d(u)\langle a(u), b(u) - \overline{v} \rangle_A.$$

Moreover, $a(u) | b(u)^2 + b(u)h(u) - f(u)$.

Proof. • I is a $K[u]$-submodule of B_K of rank 2 since I is non-zero. Thus by, Lemma 2.2.1, there exist unique polynomials $c(u), d_0(u), d_1(u) \in K[u]$ s.t. $d_0(u)$

and $d_1(u)$ are monic, $deg(c(u)) < deg(d_0(u))$ and $I = \langle d_0(u), c(u) - d_1(u)\overline{v}\rangle_A$; moreover, $d_0(u)$ and $d_1(u)$ are monic generators of the ideals $J_0 = I \cap K[u]$ and $J_1 = \{q(u) \in K[u] \mid \exists p(u) \in K[u] \; s.t \; p(u) - q(u)\overline{v} \in I\}$ respectively.

- Now, $d_0(u)\overline{v} \in I$ as $d_0(u) \in I$, $\overline{v} \in B_K$ and I is an ideal of B_K. But $d_1(u)$ is the generator of J_1, that is of the ideal formed by all "coefficients" of $\overline{v}$ in the elements of I. Thus, $d_1(u)|d_0(u)$. Similarly, note that

$$-d_1 f + (c + hd_1)\overline{v} = (c(u) - d_1(u)\overline{v})\overline{v} \in I,$$

as $c(u) - d_1(u)\overline{v} \in I$, $\overline{v} \in B_K$ and I is an ideal of B_K; hence,

$$d_1(u)|(c(u) + d_1(u)h(u))$$

and, therefore, $d_1(u)|c(u)$

- Consequently, $I = \langle d_0(u), c(u) - d_1(u)\overline{v}\rangle_A = d_1(u)\langle \frac{d_0(u)}{d_1(u)}, \frac{c(u)}{d_1(u)} - \overline{v}\rangle_A$. Writing $d(u) = d_1(u), a(u) = \frac{d_0(u)}{d_1(u)}$ and $b(u) = \frac{c(u)}{d_1(u)}$, we obtain $I = d(u)\langle a(u), b(u) - \overline{v}\rangle_A$.

- Note that $deg(b) < deg(a)$ as $deg(c) < deg(d_0), b = \frac{c}{d_1}$ and $a = \frac{d_0}{d_1}$. Note also that the uniqueness of $a(u), b(u)$ and $d(u)$ comes from that of $d_0(u), c(u)$ and $d_1(u) \in K[u]$. Moreover, note that the fact that $a(u)$ and $d(u) \in K[u]$ are monic follows from the fact that $d_0(u)$ and $d_1(u)$ are monic.

- Since $I = d\langle a, b - \overline{v}\rangle_A$, we have $d(b - \overline{v}) \in I$. Consider then $b + h + \overline{v} \in B_K$ and the product $z = d(b - \overline{v})(b + h + \overline{v}) \in I$. Since

$$z = d(b^2 + bh - f) \in I \cap K[u] = J_0 = \langle d_0\rangle_A = \langle da\rangle_A,$$

we have $da|d(b^2 + bh - f)$ and, hence, $a|(b^2 + bh - f)$.

□

Lemma 2.2.3. *Let I be a non-zero ideal of B_K. Write I as $I = d(u)\langle a(u), b(u) - \overline{v}\rangle_A$, where $a(u), b(u), c(u) \in K[u]$, $a(u)$ and $d(u)$ are monic and $deg(b) < deg(a)$. Then the norm of I is*

$$N(I) = (d^2 a).$$

Proof. By definition, $N(I) = I\widetilde{I}$ where $\widetilde{I} = d(u)\langle a(u), b(u) + h(u) + \overline{v}\rangle_A$ is the conjugate $\sigma(I)$ of I. Thus,

$$\begin{aligned}
N(I) &= d^2\langle a^2, a(b-\overline{v}), a(b+h+\overline{v}), (b-\overline{v})(b+h+\overline{v})\rangle_A \\
&= d^2\langle a^2, ab - a\overline{v}, (ab-ah) + a\overline{v}, b^2 - bh - f\rangle_A \\
&\overset{(1)}{=} d^2\langle a^2, ab - a\overline{v}, 2ab - ah, b^2 - bh - f\rangle_A \\
&= d^2\langle a^2, 2ab - ah, b^2 - bh - f, ab - a\overline{v}\rangle_A \\
&\overset{(2)}{=} d^2 a\langle a, 2b - h, \frac{b^2 - bh - f}{a}, b - \overline{v}\rangle_A
\end{aligned}$$

$(1) : 2ab - ah = (ab - a\overline{v}) - (ab - ah - a\overline{v})$

$(2) : a | b^2 - bh - f$, by Theorem 2.2.2

But $N(I)$ is an ideal of B_K; hence, it can be written as $N(I) = \Delta(u)\langle \alpha(u), \beta(u) - \overline{v}\rangle_A$ for unique polynomials $\alpha(u), \beta(u), \Delta(u) \in K[u]$ s.t. $deg(\beta) < deg(\alpha)$, and $\alpha(u)$ and $\Delta(u)$ are monic. In fact, we know that $\Delta(u)$ is the monic generator of the ideal $J_1 = \{q(u) \in K[u] \mid \exists p(u) \in K[u] \; s.t. \; p(u) - q(u)\overline{v} \in N(I)\}$.

But $N(I) = d^2 a\langle a, 2b - h, \frac{b^2 - hb - f}{a}, b - \overline{v}\rangle_A$; so $\Delta(u) = d^2 a$. Now, note that $N(I)$ is a principal ideal generated by a polynomial $\eta(u) \in K[u]$. Thus, from the form $N(I) = \Delta(u)\langle \alpha(u), \beta(u) - \overline{v}\rangle_A$, we see that $N(I) = (\Delta(u))$ i.e. $N(I) = (d^2 a)$. □

Remark 2.2.1. We shall denote by $N(I)$ both the ideal of B_K and its monic generator in $K[u]$.

Definition 2.2.1. $K[u]_{<t}$ is defined to be $\{p(u) \in K[u] \mid deg(p(u)) < t\}$.

Lemma 2.2.4. *Let $I = d(u)\langle a(u), b(u) - \overline{v}\rangle_A$ be a non-zero ideal of B_K. Then*

$$B_K = I \oplus K[u]_{<deg(da)} \oplus K[u]_{<deg(d)}\overline{v}$$

as vector spaces over K.

Proof. Let $\omega = \omega_1(u) - \omega_2(u)\overline{v}$ be any element of B_K. Let $r_2(u)$ and $q_2(u)$ be the polynomials such that $\omega_2 = q_2(u)d(u) + r_2(u)$ and $deg(r_2(u)) < deg(d(u))$. Then $\omega - q_2 d(b - \overline{v}) = (\omega_1 - q_2 db) - r_2\overline{v}$.

Let now $r_1(u)$ and $q_1(u)$ be the polynomials of $K[u]$ such that $\omega_1 - q_2 db = q_1(da) + r_1$ and $deg(r_1) < deg(da)$. Then $(\omega_1 - q_2 db) - q_1(da) = r_1$. Thus,

$$\omega - [q_2(db - d\overline{v}) + q_1(da)] = r_1(u) - r_2(u)\overline{v}$$

with $deg(r_1) < deg(da), deg(r_2) < deg(d)$ and $q_1(da) + q_2(db - d\overline{v}) \in I$. Thus, $B_K = I + K[u]_{<deg(da)} + K[u]_{<deg(d)}\overline{v}$.

Finally:

- We clearly have $K[u]_{<deg(da)} \cap K[u]_{<deg(d)}\overline{v} = \{0\}$: so, the sum $K[u]_{<deg(da)} + K[u]_{<deg(d)}\overline{v}$ is direct.

- Let $\omega = \omega_1(u) - \omega_2(u)\overline{v} \in I \cap (K[u]_{<deg(da)} \oplus K[u]_{<deg(d)}\overline{v})$.
  Then, since $\omega \in I$, there exist $\alpha(u), \beta(u) \in K[u]$ such that $\omega_2 = \beta d$ and $\omega_1 = da\alpha + \beta db$. But ω also belongs to the direct sum $K[u]_{<deg(da)} + K[u]_{<deg(d)}\overline{v}$; so $deg(\omega_2) < deg(d)$ and $deg(\omega_1) < deg(da)$. So $\beta = 0$ and $\alpha = 0$. Hence, $\omega = 0$, which implies that $I + K[u]_{<deg(da)} + K[u]_{<deg(d)}\overline{v}$ is a direct sum.

□

Theorem 2.2.5. *Let I be a non-zero ideal of B_K. Then*

$$dim_K(B_K/I) = deg(N(I)).$$

Proof. By Theorem 2.2.2. I can be written as $I = d\langle a, b - \overline{v}\rangle_A$ for some polynomials $a, b, d \in K[u]$. By Lemma 2.2.4. we know that $B_K/I \cong K[u]_{<deg(da)} \oplus K[u]_{<deg(d)}\overline{v}$. So.

$$\begin{aligned} dim_K(B_K/I) &= dim_K(K[u]_{<deg(da)}) + dim_K(K[u]_{<deg(d)}) \\ &= deg(da) + deg(d) \\ &= deg(d^2a) \\ &\overset{(1)}{=} deg(N(I)) \end{aligned}$$

$(1) : N(I) = (d^2a)$ *by Lemma* 2.2.3 □

Theorem 2.2.6. *Let M be a $K[u]$-submodule of B_K. Suppose that there exist polynomials $a(u), b(u), d(u) \in K[u]$ such that $a|b^2 + bh - f$ and $M = d(u)\langle a(u), b(u) - \overline{v}\rangle_A$. Then, M is an ideal of B_K.*

Proof. Without loss of generality, we may assume that $d(u) = 1$. We will prove that $M\omega \subseteq M$ for all $\omega \in B_K = K[u, \overline{v}]$.

Clearly, $M\eta(u) \subseteq M$ for all $\eta(u) \in K[u]$ as M is a $K[u]$-module. It thus remains to show that $M\overline{v} \subseteq M$, since $B_K = K[u, \overline{v}]$. We shall do so by showing that both $a\overline{v} \in M$ and $(b - \overline{v})\overline{v} \in M$.

1. Note that $(b - \overline{v}) \in M$ and that $a(u) \in K[u]$. Thus, $ab - a\overline{v} = a(b - \overline{v}) \in M$ as M is a $K[u]$-module. But $ab \in M$ as $a \in M$. So $a\overline{v} = -(ab - a\overline{v}) + ab \in M$.

2. Since $a|b^2 + bh - f$, let $\alpha(u) \in K[u]$ such that $a\alpha = b^2 + bh - f$. Then $(b - \overline{v})\overline{v} = -f + (b + h)\overline{v} = a\alpha - (b^2 + bh) + (b + h)\overline{v} = a\alpha - (b + h)(b - \overline{v}) \in M$.

So $M\overline{v} \subseteq M$. Hence, $M\omega \subseteq M$ for all $\omega \in B_K$. Consequently, M is an ideal of B_K. □

Corollary 2.2.7. *The nonzero ideals I of B_K are the $K[u]$-submodules M of B_K such that there exist polynomials $a(u), b(u), d(u) \in K[u]$ satisfying the following conditions:*

(i) $a|b^2 + bh - f$, *and*

(ii) $M = d(u)\langle a(u), b(u) - \overline{v}\rangle_A$.

Moreover, if such polynomials exist, we may choose them such that:

(iii) $a(u)$ *and* $d(u)$ *are monic, and*

(iv) $deg(b) < deg(a)$.

Then, the conditions (i) through (iv) uniquely determine $a(u), b(u)$ and $d(u)$.

Proof.

- Let M be a $K[u]$-submodule of B_K such that there exist polynomials $a(u), b(u), d(u) \in K[u]$ such that $a|b^2 + bh - f$ and $M = d(u)\langle a(u), b(u) - \overline{v}\rangle_A$. Then, by Theorem 2.2.6, M is an ideal of B_K.
- Let I be a non-zero ideal of B_K. Then, by Theorem 2.2.2, there exist $a(u), b(u), d(u)$ satisfying conditions (i) through (iv).

□

Definition 2.2.2. (Monic Rational Functions)

Let $q(u) \in K(u)$ be a rational function. It can be written uniquely as $q(u) = \frac{n(u)}{d(u)}$ where $n(u), d(u) \in K[u]$, $gcd(n(u), d(u)) = 1$ and $d(u)$ is monic.

Then, $q(u)$ is said to be *monic* if $n(u)$ is monic.

Theorem 2.2.8. *Let I be a non-zero fractional ideal of B_K.*

Then, there exist unique polynomials $a(u)$ and $b(u)$ of $K[u]$ and a unique rational function $q(u) \in K(u)$ such that $a(u)$ and $q(u)$ are monic, $deg(b) < deg(a)$, $a|b^2+bh-f$ and

$$I = q(u)\langle a(u), b(u) - \overline{v}\rangle_A.$$

Proof. • Existence:

Since I is fractional ideal of B_K, there exists a monic polynomial $p(u) \in K[u]$ such that $p(u)I$ is an ideal of B_K. Thus, there exist unique polynomials $a(u), b(u), d(u) \in K[u]$ s.t. $a(u)$ and $d(u)$ are monic, $deg(b) < deg(a)$, $a|b^2 + bh - f$ and $p(u)I = d(u)\langle a(u), b(u) - \overline{v}\rangle_A$. Then $I = q(u)\langle a(u), b(u) - \overline{v}\rangle_A$ where $q(u) = \frac{d(u)}{p(u)}$.

• Uniqueness:

Suppose that there exist polynomials $a_1, a_2, b_1, b_2 \in K[u]$ and rational functions $q_1, q_2 \in K(u)$ s.t. a_1, a_2, q_1, q_2 are monic, $deg(b_i) < deg(a_i)$ and $a_i|b_i^2 + b_ih - f$ for $i = 1, 2$ and $q_1\langle a_1, b_1 - \overline{v}\rangle_A = I = q_2\langle a_2, b_2 - \overline{v}\rangle_A$. Let $p(u) \in K[u]$ be a monic polynomial such that pI is an ideal of B_K. Then, for $i = 1, 2$, $pq_i(b_i - \overline{v}) \in B_K$; so, for $i = 1, 2$, $pq_i \in K[u]$ and pq_i is monic. Thus, by the uniqueness of the form $pI = pq_i\langle a_i, b_i - \overline{v}\rangle_A$ (with $a_i|b_i^2 + b_ih - f$, $deg(b_i) < deg(a_i)$, and pq_i and a_i monic polynomials of $K[u]$), we obtain $q_1 = q_2$ (since $pq_1 = pq_2$), $a_1 = a_2$ and $b_1 = b_2$.

□

Definition 2.2.3. (Standard Form of Fractional Ideals of B_K)
Let I be non-zero fractional ideal of B_K. I is said to be written *in standard form* if $I = q(u)\langle a(u), b(u) - \overline{v}\rangle_A$ where $q(u) \in K(u)$, $a(u), b(u) \in K[u]$, $q(u)$ and $a(u)$ are monic and $deg(b) < deg(a)$.

2.3 Decomposition of Prime Ideals of A in B_K

In chapter I, we noted that every ideal J of A generates an ideal JB_K of B_K. We also noted that J and JB_K may have distinct factorizations as products of prime ideals. In this section, we elaborate on this potential difference by showing how the ideal MB_K of B_K, generated by a prime ideal M of A, factors in B_K.

Remark 2.3.1. Recall that $A = K[u]$ is a P.I.D.. Thus any prime ideal M of A has the form $M = (p(u))$ for some monic irreducible polynomial $p(u) \in A$. We shall denote by $\langle p(u)\rangle_{B_K}$ (instead of $(p(u))$) the ideal of B_K generated by M.

Lemma 2.3.1. *Let $p(u)$ be an irreducible polynomial of $K[u]$. If $\langle p(u)\rangle_{B_K}$ is not a prime ideal, then the prime ideals of B_K that divide $\langle p(u)\rangle_{B_K}$ have the form $P = \langle p(u), b(u) - \overline{v}\rangle_A$, where $b(u) \in K[u]$ satisfies the following equation:*

$$v^2 + h(u)v - f(u) \equiv 0 \ mod\ p(u). \tag{2.3.1}$$

Moreover, such prime ideals have residual degree 1 over A.

Proof. Since $\langle p(u)\rangle_{B_K}$ is not prime, there exists a prime ideal P of B_K such that $\langle p(u)\rangle_{B_K} \subsetneq P$. Then, P can be written in standard form as $P = d(u)\langle a(u), b(u) - \overline{v}\rangle_A$. Hence, $d(u)|p(u)$, which implies that either $d(u) = 1$ or $d(u) = p(u)$. On one hand, if $d(u) = 1$, then $a(u)|p(u)$ and, since $a(u) = 1$ contradicts the fact that P is a

proper ideal of B_K, we have $a(u) = p(u)$. On the other hand, if $d(u) = p(u)$, then $P = \langle p(u)\rangle_{B_K}$, which is impossible by hypothesis. So $a(u) = p(u)$ and, consequently, $b(u)$ is a solution of equation 2.3.1.

Let now $b(u) \in K[u]$ be a solution of equation 2.3.1. Then, by Theorem 2.2.6, $P = \langle p(u), b(u) - \overline{v}\rangle_A$ is an ideal of B_K. Then $B_K/P \cong A/(p(u))$ is a field. So P is prime ideal whose residual degree is 1. □

Remark 2.3.2. Note that $\mathcal{B} = \{1, \overline{v}\}$ is a basis of B_K since $B_K = K[u, \overline{v}]$. Thus the corresponding discriminant of B_K is $\Delta = det \begin{pmatrix} 1 & \overline{v} \\ \sigma(1) & \sigma(\overline{v}) \end{pmatrix}^2 = det \begin{pmatrix} 1 & \overline{v} \\ 1 & -\overline{v} - h \end{pmatrix}^2 =$ $(-h - \overline{v} - \overline{v})^2 = (2\overline{v} + h(u))^2 = 4\overline{v}^2 + 4\overline{v}h + h^2 = 4(f - h\overline{v}) + 4h\overline{v} + h^2 = h^2 + 4f$.

Theorem 2.3.2. *Let M be a non-zero prime ideal of A and $p(u)$ be the monic irreducible polynomial of $A = K[u]$ such that $M = (p(u))$. Consider the equation* 2.3.1 *(see Lemma* 2.3.1*). Then, one distinguishes 3 possibilities:*

(i) If equation 2.3.1 *admits two distinct solutions $b_1(u)$ and $b_2(u) \in A$ mod $p(u)$, then $\langle p(u)\rangle_{B_K} = P_1P_2$ where $P_i = \langle p(u), b_i(u) - \overline{v}\rangle_A$ is a prime ideal of B_K for $i = 1, 2$.*

(ii) If equation 2.3.1 *admits only one solution $b(u) \in A$ mod $p(u)$, then $\langle p(u)\rangle_{B_K} = P^2$ where $P = \langle p(u), b(u) - \overline{v}\rangle_A$ is a prime ideal of B_K.*

(iii) If equation 2.3.1 *admits no solution, then $\langle p(u)\rangle_{B_K}$ is a prime ideal of B_K.*

Moreover, the situation (ii) happens if and only if $p(u)|\Delta = h^2 + 4f$.

Proof. As a preliminary remark, recall (from chapter I) that there exist prime ideals $Q_1, \cdots, Q_q$ of B_K such that $\langle p(u)\rangle_{B_K} = \prod_{i=1}^{q} Q_i^e$ and $qer = [K(\mathcal{C}) : K(u)] = 2$ (where

r is the residual degree of the Q_i's over A). Then either $\langle p(u)\rangle_{B_K}$ is a prime ideal of B_K or $\langle p(u)\rangle_{B_K} = Q_1Q_2$ (in which case, $Q_1 = Q_2$ is possible). Let us now prove the three parts of the theorem.

(iii): We prove the contrapositive. Assume then that $\langle p(u)\rangle_{B_K}$ is not prime. Then there exists a prime ideal P of B_K such that $P|\langle p(u)\rangle_{B_K}$ and $P \neq \langle p(u)\rangle_{B_K}$. Now, by Lemma 2.3.1, P has the form $\langle p(u), b(u) - \overline{v}\rangle_A$, where $b(u) \in K[u]$ satisfies equation 2.3.1. So the contrapositive statement has been proved.

Let us now prove parts (i) and (ii). Since the parts (i), (ii) and (iii) are mutually exclusive, we know that, in cases (i) and (ii), $\langle p(u)\rangle_{B_K}$ is not a prime ideal. So $\langle p(u)\rangle_{B_K} = Q_1Q_2$ where both Q_1 and Q_2 are prime ideals of B_K.

(i): Since, $\langle p(u)\rangle_{B_K}$ is not prime, Lemma 2.3.1 implies that both P_1 and P_2 are prime ideals of B_K dividing $\langle p(u)\rangle_{B_K}$. But $\langle p(u)\rangle_{B_K} = Q_1Q_2$. So, by uniqueness of factorization, $\langle p(u)\rangle_{B_K} = P_1P_2$, as desired.

(ii): As above, the fact that $\langle p(u)\rangle_{B_K}$ is not prime implies that P is a prime ideal of B_K that divides $\langle p(u)\rangle_{B_K}$. But, since $b(u)$ is the only solution of equation 2.3.1, we conclude that P is the only prime ideal of B_K dividing $\langle p(u)\rangle_{B_K}$. Consequently, $\langle p(u)\rangle_{B_K} = Q_1Q_2 = P^2$.

Finally, let us prove that the situation (ii) happens iff $p(u)|\Delta = h^2 + 4f$.

- If there exists a unique solution $b(u)$ *mod* $p(u)$ of equation 2.3.1, then $h(u) \equiv -2b(u)$ *mod* $p(u)$ and $f(u) \equiv -b(u)^2$ *mod* $p(u)$. Then $h^2 + 4f \equiv 4b^2 - 4b^2 \equiv 0$ *mod* $p(u)$. Then $p|\Delta = h^2 + 4f$.

- Conversely, suppose that $p|\Delta = 4f + h^2$ i.e. $h^2 \equiv 4f$ *mod* $p(u)$.

- If $char(K) \neq 2$, then $b(u) \equiv -\frac{h}{2} \ mod \ p(u)$ is the only solution of equation 2.3.1 since $(v-b)^2 = (v+\frac{h}{2})^2 = v^2 + vh + \frac{4f}{4} \equiv v^2 + vh - f \ mod \ p(u)$.
- If $char(K) = 2$, then $p|\Delta$ yields $p|h^2$ and, hence, $p|h$. So, equation 2.3.1 becomes $v^2 - f \equiv 0 \ mod \ p(u)$. Now, if we can show that there exists a polynomial $b(u) \in K[u]$ such that $b(u)^2 \equiv f(u) \ mod \ p(u)$, then $v^2 - f \equiv (v-b)^2 \ mod \ p(u)$ and, consequently, $b(u) \ mod \ p(u)$ is the only solution of equation 2.3.1. So, it suffices to show that $f \ mod \ p(u)$ has a square root $mod \ p(u)$.

  For this, recall that any algebraic extension of a perfect field is also perfect (c.f. Corollary 6.12 of Chapter V, on p.252 of [16]). Moreover, recall that the field K of characteristic 2 is perfect. So the algebraic extension $K[u]/(p(u))$ of K is also perfect. Hence, $f \ mod \ p(u)$ must have a square root $mod \ p(u)$.

□

Definition 2.3.1. Below (where implicit reference is made to Theorem 2.3.2) we introduce terms that distinguish the various possible factorizations of $\langle p(u) \rangle_{B_K}$ in B_K.

Case (i): M is said to *split* in B_K.

Case (ii): M is said to *ramify* in B_K.

Case (iii): M is said to be *inert* in B_K.

Remark 2.3.3. We know, from chapter I, that $\langle p(u) \rangle_{B_K}$ factors (in B_K) into prime ideals that are conjugate with respect to $G = Gal(K(C)/K(u))$. Thus, we denote by $\widetilde{P}$ the conjugate $\sigma(P)$ of P, and often write $\langle p(u) \rangle_{B_K} = P\widetilde{P}$.

2.4 Uniformizing Parameter of Prime Ideals of B_K

In chapter I. we noticed the existence of a uniformizing parameter for any non-zero prime ideal of a Dedekind domain. In this section. we describe the choice of a uniformizing parameter for the non-zero prime ideals of B_K.

Theorem 2.4.1. *Let P be a non-zero prime ideal of B_K lying above a prime ideal $(p(u))$ of $A = K[u]$. Then. a uniformizing parameter of P can be chosen as follows:*

(i) If $(p(u))$ splits or is inert in B_K. then $p(u)$ is a uniformizing parameter for P.

(ii) If $(p(u))$ ramifies in B_K. then $b(u) - \overline{v}$ is a uniformizing parameter for P. where $b(u) \in K[u]$ is the polynomial such that. written in standard form. $P = \langle a(u), b(u) - \overline{v} \rangle_A$.

Proof. (i) – If $(p(u))$ splits in B_K. then $\langle p(u) \rangle_{B_K} = P\widetilde{P}$ where $\widetilde{P} \neq P$. So $p(u) \in P$ but $p(u) \notin P^2$: otherwise. $P\widetilde{P} = \langle p(u) \rangle_{B_K} \subseteq P^2$ and. hence. $\widetilde{P} = P$. which is a contradiction. So $p(u)$ is a uniformizing parameter for P.

– If $(p(u))$ is inert in B_K. note that $p(u) \in \langle p(u) \rangle_{B_K} = P$ but $p(u) \notin \langle p(u) \rangle_{B_K}^2 = P^2$ as $p(u)^2 \nmid p(u)$. So $p(u)$ is a uniformizing parameter.

(ii) If $(p(u))$ ramifies in B_K. then $\langle p(u) \rangle_{B_K} = P^2$. So $p(u)$ cannot be a uniformizing parameter for P (since $p(u) \in P^2$). However. write P in the form $P = \langle p(u), b(u) - \overline{v} \rangle$ and consider $b(u) - \overline{v}$. Note that $b(u) - \overline{v} \in P$ but $b(u) - \overline{v} \notin P^2$ (otherwise $p(u) | b(u) - \overline{v}$ and. hence $p(u) | 1$. which is impossible).

□

2.5 Computing the order of a principal fractional ideal of B_K

In this section, we present a procedure to compute the order of a principal fractional ideal I of B_K at a non-zero prime ideal P of B_K. Note that I has the form $I = \langle \frac{\omega}{z} \rangle_{B_K}$, where $\omega, z \in B_K$, $z \neq 0$ and $\langle \frac{\omega}{z} \rangle_{B_K} = \langle \omega \rangle_{B_K} \langle z \rangle_{B_K}^{-1}$. So, $ord_P(I) = ord_P(\omega) - ord_P(z)$ and, hence, it is sufficient to describe a procedure to compute the order of a principal ideal of B_K at a prime ideal of B_K.

Lemma 2.5.1. *Let I be a non-zero ideal of B_K and $\omega_0 = a_0(u) - b_0(u)\overline{v} \in B_K$. Write I as $I = \langle a(u), b(u) - c(u)\overline{v} \rangle_A$ where $a(u), b(u), c(u)$ are polynomials of $K[u]$.*

In order to determine whether $\omega_0 \in I$, proceed as follows:

Step 1: If $c(u) \nmid b_0(u)$, then $\omega_0 \notin I$.

Step 2: If $c|b_0(u)$, then $\omega_0 \in I$ if and only if $a(u)|(a_0(u) - \frac{b_0(u)}{c(u)} b(u))$.

Proof. Assume that $\omega_0 \in I$. Then, there exist polynomials $\alpha(u), \beta(u) \in K[u]$ s.t.

$$\omega_0 = a_0 - b_0\overline{v} = \alpha a - \beta(b - c\overline{v}) = (\alpha a + \beta b) - \beta c\overline{v}.$$

So $b_0 = \beta c$ and, consequently, $c|b_0$. So *Step* 1 is justified. Moreover, $a_0 = \alpha a + \beta b = \alpha a + \frac{b_0}{c} b$, since $b_0 = \beta c$. Hence, $\alpha a = a_0 - \frac{b_0}{c} b$ and, consequently, $a|(a_0 - \frac{b_0}{c} b)$ So one direction of Step 2 is justified.

For the other direction of Step 2, assume now that $c|b_0$ and $a|(a_0 - \frac{b_0}{c} b)$. Then, there exist $\alpha(u), \beta(u) \in K[u]$ s.t. $b_0 = \beta c$ and $a_0 - \frac{b_0}{c} b = a\alpha$. Then

$$\omega_0 = a_0 - b_0\overline{v} = (a\alpha + \frac{b_0}{c} b) - b_0\overline{v} = (a\alpha + \frac{\beta c}{c} b) - \beta c\overline{v} = a\alpha + \beta(b - c\overline{v}) \in I.$$

So the other direction of Step 2 is justified. □

Remark 2.5.1. One can say that $\omega_0 \in I$ iff ($c|b_0$ and $a|(a_0 - \frac{b_0}{c}b)$).

Theorem 2.5.2. *Let $I = \langle \omega(u,\overline{v}) \rangle_{B_K}$ be a non-zero principal ideal of B_K and P be a prime ideal of B_K lying above a non-zero prime ideal $(p(u))$ of $A = K[u]$.*

The following algorithm allows to compute $ord_P(I)$.

Step 1: Write $\omega(u,\overline{v})$ as $\omega = p(u)^r \omega_0(u,\overline{v})$ where $\omega_0(u,\overline{v}) = a_0(u) - b_0(u)\overline{v}$ is such that $p(u)$ does not divide both $a_0(u)$ and $b_0(u)$.

Step 2: Compute $s \in \mathbb{N}$ as follows:

- *If $\omega_0 \notin P$, then $s = 0$ (use Lemma 2.5.1 to verify this condition).*
- *Otherwise, s is the maximal integer j such that*

$$p(u)^j | N(\omega_0) = a_0^2 + a_0 b_0 h - b_0^2 f.$$

Results:

- *If $(p(u))$ is inert in B_K, then $ord_P(I) = r$.*
- *Otherwise, $ord_P(I) = s +$* $\begin{cases} r & \text{if } (p(u)) \text{ splits in } B_K, \\ 2r & \text{if } (p(u)) \text{ ramifies in } B_K. \end{cases}$

Proof.

- If $(p(u))$ is inert in B_K, then $\langle p(u)^r \rangle_{B_K} = P^r$. So $ord_P(\langle p(u)^r \rangle_{B_K}) = r$. Moreover, $p(u) \nmid \omega_0$ and $\langle p(u) \rangle_{B_K} = P$. So $ord_P(\langle \omega_0 \rangle_{B_K}) = 0$. Hence, $ord_P(I) = ord_P(\langle p(u)^r \rangle_{B_K}) + ord_P(\langle \omega_0 \rangle_{B_K}) = r$.

- Assume now that $(p(u))$ is non-inert in B_K. Note that

$$ord_P(\langle p(u)^r \rangle_{B_K}) = ord_P((P\widetilde{P})^r) = ord(P^r \widetilde{P}^r).$$

So,

$$ord(\langle p(u)^r \rangle_{B_K}) = \begin{cases} r & \text{if } P \neq \widetilde{P} \text{ i.e. if } (p(u)) \text{ splits in } B_K, \\ 2r & \text{if } P = \widetilde{P} \text{ i.e. if } (p(u)) \text{ ramifies in } B_K. \end{cases}$$

But $ord_P(I) = ord_P(\langle p(u)^r \rangle_{B_K}) + ord_P(\langle \omega_0 \rangle_{B_K})$. Hence, it remains to show that $ord_P(\langle \omega_0 \rangle_{B_K}) = s$. For this, we distinguish two situations:

- If $\omega_0 \notin P$, then $ord_P(\langle \omega_0 \rangle_{B_K}) = 0 = s$.
- Otherwise, we distinguish again 2 cases:
  - If $(p(u))$ ramifies in B_K, then $ord_P(\langle \omega_0 \rangle_{B_K}) = 1$. Indeed, $ord_P(\langle \omega_0 \rangle_{B_K}) \geq 1$ (as $\omega_0 \in P$) and $ord_P(\langle \omega_0 \rangle_{B_K}) < 2$ (otherwise $\langle p(u) \rangle_{B_K} = P^2 | \langle \omega_0 \rangle_{B_K}$, which contradicts $p(u) \nmid \omega_0$). Then $\langle \omega_0 \rangle_{B_K} = PI_1$ where $P = \widetilde{P} \nmid I_1$. So $\mathcal{N}(\omega_0) = \mathcal{N}(P)\mathcal{N}(I_1) = p(u)\mathcal{N}(I_1)$ where $p(u) \nmid \mathcal{N}(I_1)$. So the maximal integer j s.t. $p(u)^j | \mathcal{N}(\langle \omega_0 \rangle_{B_K})$ is $s = 1 = ord_P(\langle \omega_0 \rangle_{B_K})$.
  - If $(p(u))$ splits in B_K, then $\widetilde{P} \nmid \langle \omega_0 \rangle_{B_K}$, otherwise $p(u) | \omega_0$, which is impossible. Let now $d = ord_P(\langle \omega_0 \rangle_{B_K})$. Then $\langle \omega_0 \rangle_{B_K} = P^d I_1$ where $P \nmid I_1$ and $\widetilde{P} \nmid I_1$. So $\mathcal{N}(\langle \omega_0 \rangle_{B_K}) = \mathcal{N}(P)^d \mathcal{N}(I_1) = p(u)^d \mathcal{N}(I_1)$ where $p(u) \nmid \mathcal{N}(I_1)$ (as $P, \widetilde{P} \nmid I_1$). So the maximal integer j s.t. $p(u)^j | \mathcal{N}(\langle \omega_0 \rangle_{B_K}) = a_0^2 - a_0 b_0 h - b_0^2 f$ is $s = d = ord_P(\langle \omega_0 \rangle_{B_K})$.

□

2.6 Application of Uniformizing Parameters

In this section, we show that, given a uniformizing parameter π of a non-zero prime ideal P of B_K, one can write any element $\omega(u, \overline{v})$ of B_K in the form $\omega = \pi^{ord_P(\langle \omega \rangle_{B_K})} \frac{\omega_1}{\omega_2}$ where $\omega_1, \omega_2 \in B_K \setminus P$. Moreover, we present a procedure to write any $\omega(u, \overline{v}) \in B_K$ in such a form.

Definition 2.6.1. (Local Ring)

Let B be a Dedekind domain. P be non-zero prime ideal of B and $S = B \setminus P$. Then. the domain $S^{-1}B = \{\frac{b}{s} \mid b \in B.\ s \in S\}$ denoted B_P. is called the *local ring* of B at P.

Theorem 2.6.1. *Let B be a Dedekind domain and P be a non-zero prime ideal of B. Then. the local ring B_P is also a Dedekind domain.*

Proof. See proposition 3 of §5.1 in [14]. □

Theorem 2.6.2. *Let B be a Dedekind domain. P be a non-zero prime ideal of B and π be a uniformizing parameter for P. Then B_P is a P.I.D. and the non-zero ideals of B_P have the form $\pi^j B_P$ where $j \in \mathbb{N}$.*

Proof. See proposition 4 of §5.1 in [14]. □

Corollary 2.6.3. *Let P be a non-zero prime ideal of B_K. π be a uniformizing parameter for P and $\omega \in B_K$. Then ω can be written in the form*

$$\omega = \pi^d \frac{\omega_1}{\omega_2}.$$

where $d = ord_P(\langle\omega\rangle_{B_K})$ and $\omega_1, \omega_2 \in B_K \setminus P$.

Proof. By Theorem 2.6.2. there exists $d \in \mathbb{N}$ s.t. $\omega(B_K)_P = \pi^d(B_K)_P$. Hence. $\frac{\omega}{\pi^d}$ is a unit of $(B_K)_P$. So $\frac{\omega}{\pi^d} = \frac{\omega_1}{\omega_2}$ for some $\omega_1, \omega_2 \in B_K \setminus P$. So $\omega = \pi^d \frac{\omega_1}{\omega_2}$ where $\omega_1, \omega_2 \in B_K \setminus P$. Consequently. $ord_P(\langle\omega\rangle_{B_K}) = ord_P(\langle\pi^d\rangle_{B_K}) + ord_P(\langle\omega_1\rangle_{B_K}) - ord_P(\langle\omega_2\rangle_{B_K}) = ord_P(\langle\pi\rangle^d_{B_K}) = d \cdot ord_P(\langle\pi\rangle_{B_K}) = d \cdot 1 = d.$ □

Lemma 2.6.4. *Let $p(u)$ be a monic irreducible polynomial of $A = K[u]$ s.t. $\langle p(u)\rangle_{B_K} = P^2$, where $P = \langle p(u), b(u) - \overline{v}\rangle_A$ is a prime ideal of B_K. Then $p(u)|(b(u)^2 + f(u))$ and $p(u)|(2b(u) + h(u))$. Moreover,*

$$p(u) = (b(u) - \overline{v})^2 \frac{1}{t_2(u, \overline{v})},$$

where

$$t_2(u, \overline{v}) = \frac{b(u)^2 + f(u)}{p(u)} - \frac{2b(u) + h(u)}{p(u)}\overline{v} \in B_K \setminus P.$$

Proof. Note that $\frac{(b(u)-\overline{v})^2}{p(u)} = \frac{b(u)^2+f}{p(u)} - \frac{2b(u)+h}{p(u)}\overline{v}$ and that $ord_P(\langle\frac{(b(u)-\overline{v})^2}{p(u)}\rangle_{B_K}) = ord_P(\langle(b(u)-\overline{v})^2\rangle_{B_K}) - ord_P(\langle p(u)\rangle_{B_K})$. But $(b(u) - \overline{v})$ is a uniformizing parameter for P since $(p(u))$ ramifies in B_K. So $ord_P(\langle(b(u) - \overline{v})^2\rangle_{B_K}) = 2 = ord_P(\langle p(u)\rangle_{B_K})$. Hence, $ord_P(\langle\frac{(b(u)-\overline{v})^2}{p(u)}\rangle_{B_K}) = 0$ and, consequently, $P \nmid \langle t_2(u, \overline{v})\rangle_{B_K} = \langle\frac{b(u)^2+f(u)}{p(u)} - \frac{2b(u)+h(u)}{p(u)}\overline{v}\rangle_{B_K}$. Thus, it remains to show that $t_2(u, \overline{v}) \in B_K$. For this, we suggest two possible independent arguments:

1. Note that $\langle p(u)\rangle_{B_K} = P^2$. Moreover, since $b(u) - \overline{v}$ is a uniformizing parameter for P, we have $\langle b(u)-\overline{v}\rangle_{B_K}^2 = P^2 I$ for some ideal I of B_K. Hence, $\langle t_2(u, \overline{v})\rangle_{B_K} = \langle\frac{b(u)-\overline{v}}{p(u)}\rangle_{B_K} = I$ is an ideal of B_K. So $t_2(u, \overline{v}) \in B_K$, and, therefore, $p(u)|(b(u)^2 + f(u))$ and $p(u)|(2b(u) + h(u))$.

2. Recall that, by Theorem 2.3.2, $b(u)$ *mod* $p(u)$ is the only solution of $\overline{v}^2 + \overline{v}h - f \equiv 0$ *mod* $p(u)$. So $2b \equiv -h$ *mod* $p(u)$ and, hence, $p(u)|(2b(u) + h(u))$. Moreover, $b^2 + bh - f \equiv 0$ *mod* $p(u)$, since P is an ideal of B_K. So, *mod* $p(u)$, $b^2 + f \equiv b^2 - (b^2 + hb) = b(2b + h) \equiv b \cdot 0 \equiv 0$. So $p(u)|(b(u)^2 + f)$. Hence, $\frac{b(u)^2+f}{p(u)} - \frac{2b(u)+h(u)}{p(u)}\overline{v} \in B_K$.

□

Lemma 2.6.5. *Let $p(u)$ be a monic irreducible polynomial of A such that $\langle p(u)\rangle_{B_K} = P^2$, where $P = \langle p(u), b(u)-\overline{v}\rangle_A$ is a prime ideal of B_K. Let $\omega_0 = a_0(u)-b_0(u)\overline{v} \in B_K$ such that $p(u)$ does not divide both $a_0(u)$ and $b_0(u)$. Suppose that $ord_P(\langle\omega_0\rangle_{B_K}) = 1$. Then,*

$$\omega_0 = (b-\overline{v})\frac{z_1(u,\overline{v})}{z_2(u)}.$$

where

$$z_1(u,\overline{v}) = \frac{a_0(u)(b(u)+h(u)) - f(u)b_0(u)}{p(u)} - \frac{b(u)b_0(u)-a_0(u)}{p(u)}\overline{v} \in B_K \setminus P$$

and

$$z_2(u) = \frac{b^2+bh-f}{p} \in K[u] \setminus P.$$

Proof. Note that

$$\begin{aligned}\frac{\omega_0}{(b-\overline{v})} &= \frac{\omega_0(b+h-\overline{v})}{(b-\overline{v})(b+h-\overline{v})} = \frac{[a_0(b+h)-fb_0]-[bb_0-a_0]\overline{v}}{b^2+bh-f} \\ &= \frac{[(a_0(b+h)-fb_0)-(bb_0-a_0)\overline{v}]/p}{[b^2+bh-f]/p} = \frac{z_1(u,\overline{v})}{z_2(u)}\end{aligned}$$

Moreover, $p|(b^2+bh-f)$ since $P = \langle p, b-\overline{v}\rangle_A$ is an ideal of B_K. so $z_2(u) \in K[u]$. Furthermore, $p|\omega_0(b+h+\overline{v})$ as $\langle p\rangle_{B_K} = P^2$ and $ord_P(\langle\omega_0(b+h+\overline{v})\rangle_{B_K}) = ord_P(\langle\omega_0\rangle_{B_K}) + ord_P(\langle(b-h+\overline{v})\rangle_{B_K}) = 1 + ord_P(\langle\widetilde{b-\overline{v}}\rangle_{B_K}) = 1+1 = 2$. So $z_1(u,\overline{v}) \in B_K$. Finally, note that $ord_P(\langle z_1(u,\overline{v})\rangle_{B_K}) = ord_P(\langle\frac{\omega_0(b+h+\overline{v})}{p}\rangle_{B_K}) = ord_P(\langle\omega_0(b+h+\overline{v})\rangle_{B_K}) - ord_P(\langle p\rangle_{B_K}) = 2-2 = 0$ and that $ord_P(\langle z_2(u)\rangle_{B_K}) = ord_P(\langle(b-\overline{v})(b+h+\overline{v})\rangle_{B_K}) - ord_P(\langle p\rangle_{B_K}) = 2-2 = 0$.

So $z_1(u,\overline{v}) \in B_K \setminus P$ and $z_2(u) \in K[u] \setminus (p(u))$. □

Theorem 2.6.6. *Let ω be a non-zero element of B_K and P be a prime ideal of B_K lying above a non-zero prime ideal $(p(u))$ of $A = K[u]$. The following algorithm presents ω in the form $\omega = \pi^d\frac{\omega_1}{\omega_2}$ where π is a uniformizing parameter for P, $d = ord_P(\langle\omega\rangle_{B_K})$ and $\omega_1, \omega_2 \in B_K \setminus P$:*

Step 1: *Compute the uniformizing parameter π of P, given by Theorem 2.4.1.*

Step 2: *Write ω in the form $\omega = p(u)^r\omega_0$ where $\omega_0(u,\overline{v}) = a_0(u) - b_0(u)\overline{v} \in B_K$ is such that $p(u)$ does not divide both $a_0(u)$ and $b_0(u)$.*

Step 3: *Compute $s \in \mathbb{N}$ as follows:*

- *If $\omega_0 \notin P$, then $s = 0$ (use Lemma 2.5.1. to verify this condition)*
- *Otherwise, s is the maximal integer j such that*

$$p(u)^j | N(\omega_0) = a_0(u)^2 + a_0(u)b_0(u)h - b_0(u)^2 f(u).$$

Step 4: *Compute $\omega_1, \omega_2 \in B_K$ as follows:*

- *If $(p(u))$ is inert in B_K, then $\omega_1 = \omega_0$ and $\omega_2 = 1$.*
- *If $(p(u))$ splits in B_K, then there are two cases:*
  - *If $s = 0$, then $\omega_1 = \omega_0$ and $\omega_2 = 1$.*
  - *Otherwise, $\omega_1 = \frac{N(\omega_0)}{p(u)^s}$ and $\omega_2 = \widetilde{\omega_0}$.*
- *If $(p(u))$ ramifies in B_K, then there are two cases:*
  - *If $s = 0$, then $\omega_1 = \omega_0$ and $\omega_2 = (\frac{b^2+f}{p} - \frac{2b+h}{p}\overline{v})^r$.*
  - *Otherwise, $\omega_1 = (\frac{a_0(b+h)-fb_0}{p} - \frac{bb_0-a_0}{p}\overline{v})$ and $\omega_2 = (\frac{b^2+f}{p} - \frac{2b+h}{p})^r(\frac{b^2+bh-f}{p})$.*

Result:

- *If $(p(u))$ ramifies in B_K, then $\omega = (b - \overline{v})^{2r+s}\frac{\omega_1}{\omega_2}$ where $\omega_1, \omega_2 \in B_K \setminus P$.*
- *Otherwise, $\omega = p(u)^{r+s}\frac{\omega_1}{\omega_2}$ where $\omega_1, \omega_2 \in B_K \setminus P$.*

Proof. Using Theorem 2.5.2. we obtain the following:

- If $(p(u))$ is inert in B_K, then $\omega = p(u)^r\omega_0$ where $ord_P(\langle\omega_0\rangle_{B_K}) = 0$. So $\omega = p(u)^r\frac{\omega_1}{\omega_2}$ where $\omega_1 = \omega_0$, $\omega_2 = 1 \in B_K \setminus P$. Moreover, $ord_P(\langle\omega\rangle_{B_K}) = r = r + s$ (since $s = 0$).

- If $(p(u))$ splits in B_K, then there are two cases:
  - If $\omega_0 \notin P$ (i.e. if $s = 0$), then $\omega = p(u)^r\omega_0$ where $ord_P(\langle\omega_0\rangle_{B_K}) = 0$. So $\omega = p(u)^r\frac{\omega_1}{\omega_2}$ where $\omega_1 = \omega_0, \omega_2 = 1 \in B_K \setminus P$. Moreover, $ord_P(\langle\omega\rangle_{B_K}) = r = r + s$.
  - If $\omega_0 \in P$ (i.e. if $s > 0$), then $\omega = p(u)^r\omega_0 = p(u)^r\frac{N(\omega_0)}{\omega_0}$. Now, write $\langle\omega_0\rangle_{B_K}$, as $\langle\omega_0\rangle_{B_K} = P^sI_1$, where I_1 is an ideal of B_K such that $P \nmid I_1$. Then $N(\omega_0) = p(u)^sN(I_1)$ and, hence, $\omega = p(u)^{r+s}\frac{N(I_1)}{\omega_0}$ with $N(I_1) \in B_K \setminus P$. Now, note that $\widetilde{\omega_0} \notin P$ as $\widetilde{P} \nmid \langle\omega_0\rangle_{B_K}$ (otherwise both P and $\widetilde{P}$ would divide $\langle\omega_0\rangle_{B_K}$, which is impossible). So $\omega = p(u)^{r+s}\frac{\omega_1}{\omega_2}$ where $\omega_1 = \frac{N(\omega_0)}{p(u)^s}, \omega_2 = \widetilde{\omega_0} \in B_K \setminus P$. And $ord_P(\langle\omega\rangle_{B_K}) = r + s$.
- If $(p(u))$ ramifies in B_K, then, unlike in the previous cases, $p(u)$ is not a uniformizing parameter for P; instead, $(b - \overline{v})$ is. By Lemma 2.6.4, we also have $p(u) = (b - \overline{v})^2\frac{1}{t_2}$ where $t_2 = \frac{b^2+f}{p} - \frac{2b+h}{p}\overline{v} \in B_K \setminus P$. So $\omega = (b - \overline{v})^{2r}\frac{\omega_0}{t_2^r}$. We now distinguish two cases:
  - If $\omega_0 \notin P$ (i.e. if $s = 0$), then, taking $\omega_1 = \omega_0$ and $\omega_2 = t_2^r$ gives $\omega = (b - \overline{v})^{2r+s}\frac{\omega_1}{\omega_2}$ where $\omega_1, \omega_2 \in B_K \setminus P$. And $ord_P(\langle\omega\rangle_{B_K}) = 2r + s$, by Theorem 2.5.2.
  - If $\omega_0 \in P$, then, by Lemma 2.6.5, $\omega_0 = (b - \overline{v})\frac{z_1}{z_2}$ where $z_1(u, \overline{v}) = \frac{a_0(b+h)-fb_0}{p} - \frac{bb_0-a_0}{p}\overline{v}, z_2(u) = \frac{b^2+bh-f}{p} \in B_K \setminus P$. So $\omega = (b - \overline{v})^{2r+1}\frac{\omega_1}{\omega_2}$ where $\omega_1 = (\frac{a_0(b+h)-fb_0}{p} - \frac{bb_0-a_0}{p}\overline{v}), \omega_2 = (\frac{b^2+f}{p} - \frac{2b+h}{p}\overline{v})^r(\frac{b^2+bh-f}{p}) \in B_K \setminus P$. And $ord_P(\langle\omega\rangle_{B_K}) = 2r - s = 2r + 1$, by Theorem 2.5.2.

□

2.7 Units of B_K

In this section we underline the fact that the units of the ring B_K are simply the non-zero elements of the field K.

Lemma 2.7.1. *The units of the ring B_K are the non-zero elements of the field K.*

Proof. On one hand, it is clear that any non-zero element of K is a unit of B_K, since K is a field and $K \subseteq B_K$. On the other hand, if $\lambda = a(u) - b(u)\overline{v}$ is a unit of B_K, then $N(\lambda)$ is a unit of $K[u]$ i.e. a non-zero element of K. Hence, $deg(N(\lambda)) = deg(a^2 + abh - b^2 f) = max\{deg(a^2), deg(b^2 f)\} = 0$. But $deg(f) = 2g+1$. So $b(u) = 0$ and $a(u) \in K^*$. Consequently, $\lambda \in K^*$ □

2.8 Results over the Algebraic Closure $\overline{K}$ of K

Let us now present a few results arising in the study of $B = B_{\overline{K}} = \overline{K}[u, \overline{v}]$.

- The non-zero prime ideals of $\overline{K}[u]$ have the form $(u - x)$ where $x \in \overline{K}$.
- The non-zero prime ideals of B have the form $P = \langle u - x, y - \overline{v} \rangle_{\overline{K}[u]}$ where $y^2 + yh(x) - f(x) = 0$.
- There are *no inert prime ideals* P in B, since $v^2 + vh(x) = f(x)$ has a solution $v = y \in \overline{K}$, for any $x \in \overline{K}$.
- The conjugate of the prime ideal $P = \langle u - x, y - \overline{v} \rangle_{\overline{K}[u]}$ is $\widetilde{P} = \langle u - x, (-y - h(x)) - \overline{v} \rangle_{\overline{K}[u]}$.

- A uniformizing parameter for $P = \langle u - x, y - \overline{v} \rangle_{\overline{K}[u]}$ is

$$\begin{cases} u - x & \text{if } (u - x) \text{ splits in } B, \\ y - \overline{v} & \text{if } (u - x) \text{ ramifies in } B. \end{cases}$$

- Let $P = \langle u - x, y - \overline{v} \rangle_{\overline{K}[u]}$ be a prime ideal of B, and $\omega \in B_K$. Let r be the integer such that $\omega = (u - x)^r \omega_0(u, \overline{v})$ where $\omega_0(u, \overline{v}) = a_0(u) - b_0(u)\overline{v}$ is such that $(u - x)$ does not divide both $a_0(u)$ and $b_0(u)$. Finally, let s be the maximal integer j such that $(u-x)^j | N(\omega_0) = a_0(u)^2 + a_0(u)b_0(u)h(u) - b_0(u)^2 f(u) \in \overline{K}[u]$. Then

$$ord(\langle \omega \rangle_B) = s + \begin{cases} r & \text{if } (u - x) \text{ splits in } B, \\ 2r & \text{if } (u - x) \text{ ramifies in } B. \end{cases}$$

Chapter 3

Construction of a Hyperelliptic Jacobian

The goal of this chapter is to present the Jacobian $\mathbb{J}$ of a hyperelliptic curve. We proceed by using our knowledge of fractional ideals to construct an Abelian group, denoted $\mathbb{I}^*/\mathbb{P}^*$, which we then prove to be isomorphic to $\mathbb{J}$. Thus, by transfer of structure, the results developed for $\mathbb{I}^*/\mathbb{P}^*$ then apply to $\mathbb{J}$.

3.1 Introduction

Let us, in this introduction, elaborate on the procedure to build $\mathbb{I}^*/\mathbb{P}^*$.

First, we define semi-reduced and reduced fractional ideals of B_K. Then, we introduce principal fractional ideals and use them to construct an Abelian group, denoted $\mathbb{I}_K^*/\mathbb{P}_K^*$. At this point, we use reduced fractional ideals of B_K in order to show how to perform computation in $\mathbb{I}_K^*/\mathbb{P}_K^*$. Then, we define divisors and their degree, and establish an isomorphism between the group of fractional ideals of $B_{\overline{K}}$ and the group of degree-zero divisors. Finally, we define the Jacobian of a hyperelliptic curve, explain that $\mathbb{I}_{\overline{K}}^*/\mathbb{P}_{\overline{K}}^*$ is isomorphic to $\mathbb{J}$ and, hence, by transfer of structure, obtain indications on $\mathbb{J}$.

3.2 Semi-reduced fractional ideals

In this section, we define an equivalence relation on the group of non-zero fractional ideals of B_K. Then, we define semi-reduced fractional ideals and show that they are representatives of each class of equivalence under the above relation.

First, let us establish a few definitions.

Definition 3.2.1. We denote, by $\mathbb{I}_K^*$, the group of non-zero fractional ideals of B_K and, by $\mathbb{P}_K^*$, the group of non-zero principal fractional ideals of B_K. Then, we write $\mathbb{I}^*$ and $\mathbb{P}^*$ to denote $\mathbb{I}_{\overline{K}}^*$ and $\mathbb{P}_{\overline{K}}^*$ respectively.

Definition 3.2.2. Let $\sim$ be the equivalence relation defined on $\mathbb{I}_K^*$ by

$$I_1 \sim I_2 \text{ if and only if } I_1 I_2^{-1} \in \mathbb{P}_K^*.$$

Remark 3.2.1. The commutativity of $\mathbb{I}_K^*$ implies that $\mathbb{P}_K^*$ is a normal subgroup of $\mathbb{I}_K^*$. Thus, we may form the quotient group $\mathbb{I}_K^*/\mathbb{P}_K^*$, where we have

$$\mathbb{P}_K^* I_1 = \mathbb{P}_K^* I_2 \text{ if and only if } I_1 \sim I_2, \text{ for any two } I_1, I_2 \in \mathbb{I}_K^*.$$

For simplicity, we shall denote $\mathbb{P}_K^* I$ by $[I]_K$, for any $I \in \mathbb{I}_K^*$.

Definition 3.2.3. (Semi-reduced fractional ideals)
Let $I = q(u)(a(u), b(u) - \overline{v})_A$ be an element of $\mathbb{I}_K^*$ written in standard form. Then I is said to be semi-reduced if and only if $q(u) = 1$.

Lemma 3.2.1. *Let $I \in \mathbb{I}_K^*$. Then, the following are equivalent:*

(i) *I is semi-reduced*

(ii) *I is an ideal of B_K and there exists no irreducible polynomial $p(u) \in K[u]$ such that $\langle p(u) \rangle_{B_K} | I$.*

(iii) *I is an ideal of B_K and the following are true:*

1. *There exists no non-zero inert prime ideal P of B_K such that $P|I$.*
2. *If P is a non-zero non-inert prime ideal P of B_K such that $P|I$, then $\widetilde{P} \nmid I$, unless $P = \widetilde{P}$, in which case $ord_P(I) = 1$.*

Proof. Without loss of generality, we may assume that I is an ideal of B_K. Thus, we can write I in standard form as $I = d(u)\langle a(u), b(u) - v \rangle_A$. Then :

$(i) \Leftrightarrow (ii)$ is clear since the irreducible polynomials $p(u) \in K[u]$ such that $\langle p(u) \rangle_{B_K} | I$ are those which divide $d(u)$.

$(ii) \Leftrightarrow (iii)$ follows from the factorization of prime ideals of $K[u]$ in B_K (see Theorem 2.3.2).

□

Definition 3.2.4. (The π_K map)

The map $\pi_K : \mathbb{I}_K^* \longrightarrow \mathbb{I}_K^*/\mathbb{P}_K^*$ is defined to be the canonical projection of $\mathbb{I}_K^*$ onto $\mathbb{I}_K^*/\mathbb{P}_K^*$.

Theorem 3.2.2. (Semi-reduced representative of classes in $\mathbb{I}_K^\bullet/\mathbb{P}_K^\bullet$)
Let $I = q(u)\langle a(u), b(u) - \overline{v}\rangle_A$ be a non-zero fractional ideal of $\mathbb{I}_K^\bullet$, written in standard form. Then the ideal

$$J = \langle a(u), b(u) - \overline{v}\rangle_A$$

is a semi-reduced representative of $[I]_K$.

Proof. Note that $\pi_K(I) = [I]_K = [\langle a(u), b(u) - \overline{v}\rangle_A]_K$, since $\langle q(u)\rangle_{B_K} \in \mathbb{P}_K^\bullet$. Moreover, $J = \langle a(u), b(u) - \overline{v}\rangle_A$ belongs to $\mathbb{I}_K^\bullet$ and is semi-reduced, by definition, as $q(u)\langle a(u), b(u) - \overline{v}\rangle_A$ is the standard form of $I \in \mathbb{I}_K^\bullet$. So, J is a semi-reduced representative of $[I]_K$. □

3.3 Reduced Fractional Ideals

In the previous section, we noticed that any equivalence class of $\mathbb{I}_K^\bullet/\mathbb{P}_K^\bullet$ has a semi-reduced representative. Unfortunately, such a representative is not unique. In this section, we introduce the notion of reduced fractional ideals and show that each class of $\mathbb{I}_K^\bullet/\mathbb{P}_K^\bullet$ has a unique reduced representative.

Definition 3.3.1. (Reduced Fractional Ideal)
Let $I \in \mathbb{I}_K^\bullet$ be a semi-reduced fractional ideal. Then I is said to be reduced if $deg(N(I)) \leq g$.

Theorem 3.3.1. *Let $I \in \mathbb{I}_K^\bullet$. Then $[I]_K$ has a unique reduced representative $J \in \mathbb{I}_K^\bullet$. Moreover, if I is a semi-reduced non-reduced fractional ideal of $\mathbb{I}_K^\bullet$, then J can be computed using the following algorithm:*

Input: $I = \langle a(u), b(u) - \overline{v} \rangle_A \in \mathbb{I}_K^*$ *is a non-reduced semi-reduced fractional ideal, written in standard form (except that we do not require* $a(u)$ *to be monic).*

Step 1:
* $\alpha(u) = \frac{f(u) - b(u)h(u) - b(u)^2}{a(u)}$
* $\beta(u) = (-h(u) - b(u)) \bmod \alpha(u)$

Step 2: *If* $deg(\alpha(u)) > g$, *then set* $a(u) = \alpha(u)$ *and* $b(u) = \beta(u)$, *and go to Step* 1.

Step 3: *Let* c *be the leading coefficient of* $\alpha(u)$. *Then set* $\alpha(u) = c^{-1}\alpha(u)$.

Result: $J = \langle \alpha(u), \beta(u) - \overline{v} \rangle_A \in \mathbb{I}_K^*$ *is the reduced representative of* $[I]_K$.

Proof. • Assuming their existence, let us first show the uniqueness of the reduced representatives.

Let $I_1, I_2 \in \mathbb{I}_K^*$ be two reduced fractional ideal representatives of the same class $[I]_K \in \mathbb{I}_K^*/\mathbb{P}_K^*$. We have $1 \sim I_1 I_2^{-1}$. But $I_1 I_2^{-1} \sim I_1 \widetilde{I}_2$ since $I_2 \widetilde{I}_2 = \mathcal{N}(I_2) \sim 1$. So $1 \sim I_1 \widetilde{I}_2$. Hence, there exists $\omega(u, \overline{v}) = a(u) - b(u)\overline{v} \in B_K$ such that $I_1 \widetilde{I}_2 = \langle \omega(u, \overline{v}) \rangle_{B_K}$. Now $deg(\mathcal{N}(\omega)) = deg(\mathcal{N}(I_1)) + deg(\mathcal{N}(I_2)) \leq 2g$. But

$$deg(\mathcal{N}(\omega)) = deg(a^2 + abh - b^2 f) = max\{deg(a^2), deg(b^2 f)\},$$

and $deg(f) = 2g + 1$. So $b(u) = 0$. Hence, $\omega(u, \overline{v}) = a(u)$. Now, $\mathcal{N}(I_2) I_1 = (I_1 \widetilde{I}_2) I_2 = \omega I_2 = a(u) I_2$. So $\mathcal{N}(I_2) I_1 = a(u) I_2$. But I_1 and I_2 are semi-reduced. So $\mathcal{N}(I_2) = a(u)$ and $I_1 = I_2$.

• Let us now prove the existence of a reduced representative of $[I]_K$, where $I = q(u)\langle a(u), b(u) - \overline{v} \rangle_A$ is any element of $\mathbb{I}_K^*$, written in standard form.

Note first that I can be assumed to be semi-reduced (by Theorem 3.2.2). Hence, we assume that $q(u) = 1$. Assuming that I is not reduced, we will show that the

A-module produced by the algorithm, is a reduced ideal of $\mathbb{I}_K^*$ which is equivalent to I. For this, it is sufficient to show that the A-module $J_1 = \langle \alpha(u), \beta(u) - \overline{v} \rangle_A$ produced by one iteration of *Step* 1 verifies the following: (i) $J_1 \in \mathbb{I}_K^*$ and $J_1 \sim I$. (ii) J_1 is semi-reduced. (iii) $deg(N(J_1)) < deg(N(I))$.

(i) Note that

$$\begin{aligned} J_1 &= \left\langle \frac{f - bh - b^2}{a}, (-b - h) - \overline{v} \right\rangle_A \\ &= \left\langle \frac{(b - \overline{v})(-b - h - \overline{v})}{a}, -b - h - \overline{v} \right\rangle_A \\ &= (-b - h - \overline{v}) \left\langle \frac{b - \overline{v}}{a}, 1 \right\rangle_A \\ &= \frac{-b - h - \overline{v}}{a} \langle a, b - \overline{v} \rangle_A \\ &= \frac{-b - h - \overline{v}}{a} \cdot I. \end{aligned}$$

So $J_1 \in \mathbb{I}_K^*$ and $J_1 \sim I$.

(ii) Note that $a|(b^2 + bh - f)$ since $I = \langle a(u), b(u) - \overline{v} \rangle_A$ is an ideal of B_K. So $a|(f - bh - b^2) = -(b^2 + bh - f)$ and, hence, $J_1 = \langle \frac{f - bh - b^2}{a}, -b - h - \overline{v} \rangle_A$ is an ideal of B_K. Now, $J_1 = \langle \alpha(u), \beta(u) - \overline{v} \rangle_A$, where $\alpha(u), \beta(u) \in K[u]$. So $J_1 \in \mathbb{I}_K^*$. Moreover, we have, by definition, that

$$deg(\beta(u)) < deg(\alpha(u)).$$

So, this is the standard form of J_1, except that $\alpha(u)$ may not be monic. In particular, J_1 is semi-reduced.

(iii) Note that, by Lemma 2.2.3, $deg(N(I)) = deg(a)$ and $deg(N(J_1)) = deg(\alpha(u)) = deg(f - bh - b^2) - deg(a) = max\{deg(f), 2deg(b)\} - deg(a)$.

* If $2deg(b) \leq deg(f) = 2g+1$, then $deg(\alpha(u)) = 2g+1-deg(a) \leq (2g+1)-(g+1) = g$ (as $deg(a) \geq g+1$).
* Otherwise, $deg(\alpha(u)) = 2deg(b) - deg(a)$. But $deg(b) < deg(a)$ implies that $2deg(b) \leq 2(deg(a)-1)$. So $deg(\alpha(u)) \leq deg(a) - 2 < deg(a)$.

So $deg(N(J_1)) < deg(N(I))$.

□

Remark 3.3.1. Since, $deg(\alpha(u)) \leq deg(a) - 2$ whenever $deg(a) > g+1$, the algorithm takes, at most, $\lceil \frac{deg(a)-g}{2} \rceil$ steps to complete.

3.4 Computation in $\mathbb{I}^*_K/\mathbb{P}^*_K$

In this section, we describe a method for multiplying, in $\mathbb{I}^*_K/\mathbb{P}^*_K$, two fractional ideals of $\mathbb{I}^*_K$. Since each class of $\mathbb{I}^*_K/\mathbb{P}^*_K$ has a semi-reduced representative, we first present a formula for the product of two ordinary ideals of B_K. Then, we use the reduction algorithm to find the reduced representative of the product ideal class .

Theorem 3.4.1. *Let I_1 and I_2 be two non-zero ideals of B_K.*
For $i = 1, 2$, write I_i in standard form as $I_i = d_i(u)\langle a_i(u), b_i(u) - \overline{v}\rangle_A$.
Let $\Delta(u) = gcd(a_1(u), a_2(u), b_1(u) + b_2(u) + h(u))$ and $e_1(u), e_2(u), e_3(u) \in K[u]$ be polynomials such that $\Delta = e_1a_1 + e_2a_2 + e_3(b_1 + b_2 + h)$.
Then $\Delta \neq 0$, $\Delta | a_i$ for $i = 1, 2$ and $\Delta | (e_1a_1b_2 + e_2a_2b_1 + e_3(b_1b_2 + f))$.
Define

$$a(u) = \frac{a_1(u)a_2(u)}{\Delta(u)^2}$$

and

$$b(u) = \frac{e_1(u)a_1(u)b_2(u) + e_2(u)a_2(u)b_1(u) + e_3(u)(b_1(u)b_2(u) + f(u))}{\Delta(u)} \bmod a(u).$$

Then

$$I_1 I_2 = d_1(u)d_2(u)\Delta(u)\langle a(u), b(u) - \overline{v}\rangle_A.$$

and this expression is in standard form.

Proof. • Let

$$\begin{aligned} I &= I_1 I_2 \\ &= d_1 d_2 \langle a_1 a_2, a_2(b_1 - \overline{v}), a_1(b_2 - \overline{v}), (b_1 - \overline{v})(b_2 - \overline{v})\rangle_A \\ &= d_1 d_2 \langle a_1 a_2, a_2 b_1 - a_2\overline{v}, a_1 b_2 - a_1\overline{v}, b_1 b_2 + f - (b_1 + b_2 + h)\overline{v}\rangle_A. \end{aligned}$$

• Let

$$I_3 = \frac{1}{d_1 d_2} I = \langle a_1 a_2, a_2 b_1 - a_2\overline{v}, a_1 b_2 - a_1\overline{v}, b_1 b_2 + f - (b_1 + b_2 + h)\overline{v}\rangle_A.$$

Let $\Delta_0(u)$ and $\Delta_1(u) \in K[u]$ be the monic generators of the two ideals $J_0 = I_3 \cap K[u]$ and $J_1 = \{q(u) \in K[u] \mid \exists p(u) \in K[u] \ s.t. \ p(u) - q(u)\overline{v} \in I_3\}$ respectively. Then, by Lemma 2.2.1, $I_3 = \langle \Delta_0, \delta\rangle_A$, where $\delta = p(u) - \Delta_1(u)\overline{v}$ for some $p(u) \in K[u]$.

In the remaining of the proof, we shall compute δ and $\Delta_0(u)$, in order to write I_3 in standard form and thus to find Δ, a and b.

• Computation of δ:

- Computation of Δ_1:

Note that J_1 is the ideal formed by the coefficients of $\overline{v}$ in the elements of I_3:

so $J_1 = \langle a_2, a_1, b_1 + b_2 + h \rangle_A$ and, consequently, $\Delta_1 = gcd(a_1, a_2, b_1 + b_2 + h)$. Let then $e_1(u), e_2(u), e_3(u) \in K[u]$ be polynomials such that $\Delta_1 = e_1 a_1 + e_2 a_2 + e_3(b_1 + b_2 + h)$ and note that $\Delta_1 | a_i$ for $i = 1, 2$. Note also that $\Delta_1 \neq 0$, otherwise $a_1 = 0$ and I_1 could not then be written in standard form as $d_1 \langle a_1, b_1 - \overline{v} \rangle_A$.

- Computation of $p(u)$ and δ:

  Consider $\omega = e_1(a_1 b_2 - a_1 \overline{v}) + e_2(a_2 b_1 - a_2 \overline{v}) + e_3(b_1 b_2 + f - (b_1 + b_2 + h)\overline{v}) \in I_3$. Note that

$$\begin{aligned} \omega &= [e_1 a_1 b_2 + e_2 a_2 b_1 + e_3(b_1 b_2 + f)] - [e_1 a_1 + e_2 a_2 + e_3(b_1 + b_2 + h)]\overline{v} \\ &= (e_1 a_1 b_2 + e_2 a_2 b_1 + e_3(b_1 b_2 + f)) - \Delta_1 \overline{v}. \end{aligned}$$

  Let then $p(u) = e_1 a_1 b_2 + e_2 a_2 b_1 + e_3(b_1 b_2 + f)$ and define δ to be ω. Then $\delta = p(u) - \Delta_1(u)\overline{v} \in I_3$.

- Writing I_3 in standard form:

  - Recall that, by Lemma 2.2.3, $N(I_i) = d_i^2 a_i$ for $i = 1, 2$.

    Note that

$$I = d_1 d_2 I_3 = d_1 d_2 \langle \Delta_0, \delta \rangle_A = d_1 d_2 \langle \Delta_0, p - \Delta_1 \overline{v} \rangle_A.$$

    Recall also that, since I is an ideal, $\Delta_1 | p$ and $\Delta_1 | \Delta_0$ (see the proof of Theorem 2.2.2). Thus $I = d_1 d_2 \Delta_1 \langle \frac{\Delta_0}{\Delta_1}, \frac{p}{\Delta_1} - \overline{v} \rangle_A$.

    Hence, $N(I) = (d_1 d_2 \Delta_1)^2 \frac{\Delta_0}{\Delta_1} = d_1^2 d_2^2 \Delta_1 \Delta_0$. But

$$N(I) = N(I_1 I_2) = N(I_1) N(I_2) = (d_1 a_1)^2 (d_2 a_2)^2 = d_1^2 d_2^2 a_1 a_2.$$

    So $d_1^2 d_2^2 \Delta_1 \Delta_0 = d_1^2 d_2^2 a_1 a_2$ and, consequently, $\frac{\Delta_0}{\Delta_1} = \frac{a_1 a_2}{\Delta_1^2}$.

- Define $\Delta = \Delta_1.\ a = \frac{a_1 a_2}{\Delta^2}$ and $b = \frac{p}{\Delta}\ mod\ a\ = \frac{e_1 a_1 b_2 + e_2 a_2 b_1 + e_3(b_1 b_2 - f)}{\Delta}\ mod\ a.$ Then $I_1 I_2 = d_1 d_2 \Delta \langle a, b - \overline{v} \rangle_A$ and this expression is clearly in standard form.

□

Theorem 3.4.2. *Let I_1 and I_2 be two semi-reduced ideals of $\mathbb{I}_K^*$, written in standard form as $I_i = \langle a_i(u), b_i(u) - \overline{v} \rangle_A$, for $i = 1, 2$. Then, the following algorithm produces the reduced representative of $[I_1 I_2]_K$.*

Part I: Define the following:

- $d_1 = gcd(a_1, a_2)$ *and* $s_1(u), s_2(u) \in K[u]$ *are polynomials such that* $d_1 = s_1 a_1 + s_2 a_2$.
- $d = gcd(d_1, b_1 + b_2 + h)$ *and* $t_1(u), t_2(u) \in K[u]$ *are polynomials such that* $d = t_1 d_1 + t_2(b_1 + b_2 + h)$.
- $e_1 = s_1 t_1,\ e_2 = s_2 t_1$ *and* $e_3 = t_2$.
- $a = \frac{a_1 a_2}{d^2}$
- $b = \frac{e_1 a_1 b_2 + e_2 a_2 b_1 + e_3(b_1 b_2 + f)}{d}\ mod\ a.$

Then $I' = \langle a, b - \overline{v} \rangle_A \in \mathbb{I}_K^*$ is a semi-reduced representative of $[I_1 I_2]_K$, written in standard form.

Part II:

- *If $deg(a) \leq g$, then $I'' = I'$ is the reduced representative of $[I_1 I_2]_K$.*
- *Otherwise, proceed as follows:*

Step 1:

- $\alpha(u) = \frac{f(u) - b(u)h(u) - b(u)^2}{a(u)}$
- $\beta(u) = (-h(u) - b(u))\ mod\ \alpha(u)$

Step 2: *If* $deg(\alpha(u)) > g$, *then set* $a(u) = \alpha(u)$ *and* $b(u) = \beta(u)$, *and go to Step 1.*

Step 3: *Let* c *be the leading coefficient of* $\alpha(u)$. *Then set* $\alpha(u) = c^{-1}\alpha(u)$.

Then, $I'' = \langle \alpha(u), \beta(u) - \overline{v} \rangle_A \in \mathbb{I}_K^*$ *is the reduced representative of* $[I_1 I_2]_K$, *written in standard form.*

3.5 Introduction to divisors

In this section, hyperelliptic divisors are introduced.

Briefly, let us say that hyperelliptic divisors are formal sums of points on a hyperelliptic curve C, like ideals of a Dedekind domain are products of prime ideals of this Dedekind domain.

Definition 3.5.1. (Divisor)

- A *divisor* D of C is a finite formal sum $\sum_{i=1}^{m} e_i p_i$ of points p_i of C.
- Then, the *degree* $deg(D)$ of D is the integer defined by $deg(D) = \sum_{i=1}^{m} e_i$.
- Also, the *support* $supp(D)$ of D is then defined by

$$supp(D) = \{p_i \in C \mid i \in \{1, \cdots, m\} \text{ and } e_i \neq 0\}.$$

- The *order* $ord_p(D)$ of D at a point p of C is the integer defined by

$$ord_p(D) = \begin{cases} 0 & \text{. if } p \notin supp(D). \\ e_i & \text{. if } p = p_i \text{ for some } i \in \{1, \cdots, m\}. \end{cases}$$

- D is said to be *defined over* K if $D^\theta = \sum_{i=1}^{m} e_i\theta(p_i) = D$ for all $\theta \in Gal(\overline{K}/K)$ (note that $\theta(\infty) = \infty$ for all $\theta \in Gal(\overline{K}/K)$, by definition).

Remark 3.5.1. The set $\mathbb{D}$ of all divisors forms an Abelian group under the addition rule $D_1 - D_2 = \sum_{i=1}^{m}(e_{i,1} - e_{i,2})p_i$ for any two divisors D_1 and D_2 such that $D_j = \sum_{i=1}^{m} e_{i,j}p_i$ for $j = 1, 2$.

Definition 3.5.2. (Degree zero Divisor)
The set $\mathbb{D}^0$ consists of all *degree zero divisors* i.e. all divisors D of C such that $deg(D) = 0$.
The set $\mathbb{D}^0_K$ consists of all degree zero divisors of C that are defined over K.

Remark 3.5.2. $\mathbb{D}^0$ is a subgroup of D under the addition rule and $\mathbb{D}^0_K$ is a subgroup of $\mathbb{D}^0$.

3.6 Correspondence between ideals and divisors

In this section, we shed light upon the correspondence between the fractional ideals of $B_{\overline{K}}$ and the degree zero divisors.

Definition 3.6.1. Let $\mathbb{M}^*_K$ denote the set of maximal ideals of B_K. Then $\mathbb{M}^*$ denotes $\mathbb{M}^*_{\overline{K}}$.

Remark 3.6.1. Since $B_{\overline{K}}$ is a Dedekind domain, $\mathbb{M}^*$ consists of the non-zero prime ideals of $B_{\overline{K}}$. Thus, if $M \in \mathbb{M}^*$, then $M = \langle u - x, y - \overline{v}\rangle_{\overline{K}[u]}$ for some $x, y \in \overline{K}$.

Lemma 3.6.1. (Correspondence between Prime Ideals and Points)
Let $M = \langle u - x, y - \overline{v}\rangle_{\overline{K}[u]} \in \mathbb{M}^*$. *Then, the point* (x, y) *belongs to* C. *Moreover, the map* $\phi : \mathbb{M}^* \longrightarrow C \setminus \{\infty\}$, *defined by*

$$\phi(\langle u - x, y - \overline{v}\rangle_{\overline{K}[u]}) = (x, y),$$

is a bijection.

Proof.

- Let $M = \langle u - x, y - \overline{v}\rangle_{\overline{K}[u]}$ and $M' = \langle u - x', y' - \overline{v}\rangle_{\overline{K}[u]}$ be two maximal ideals of $B_{\overline{K}}$. If $M = M'$, then $x = x'$ and $y = y'$, by uniqueness of the standard form of ideals in $B_{\overline{K}}$. So $(x, y) = (x', y')$ and, hence, ϕ is well defined. Moreover, $(u - x) \mid y^2 - yh(u) - f(u)$, since M is an ideal of $B_{\overline{K}}$. So $y^2 + h(x)y - f(x) = 0$ and, consequently, $(x, y) \in C \setminus \{\infty\}$.

- Now, let $(x, y) \in C$: then $y^2 + h(x) - f(x) = 0$ and, consequently, $(u - x)|y^2 + yh(u) - f(u)$. So $\langle u - x, y - \overline{v}\rangle_{\overline{K}[u]}$ is an ideal of $B_{\overline{K}}$, by Theorem 2.2.6. But, this is a prime ideal, since $\overline{K}[u, \overline{v}]/\langle u - x, y - \overline{v}\rangle_{\overline{K}[u]} \cong \overline{K}$ is a field. So $\langle u - x, y - \overline{v}\rangle_{\overline{K}[u]} \in \mathbb{M}^*$. Then $\phi(\langle u - x, y - \overline{v}\rangle_{\overline{K}[u]}) = (x, y)$ and, hence, ϕ, is surjective.

- For the injectivity of ϕ, simply note that $(x, y) = (x', y')$ implies that $x = x'$ and $y = y'$, which implies that $\langle u - x, y - \overline{v}\rangle_{\overline{K}[u]} = \langle u - x', y' - \overline{v}\rangle_{\overline{K}[u]}$.

So ϕ is a bijection. □

Theorem 3.6.2. (Injection of $\mathbb{I}^*_K/\mathbb{P}^*_K$ in $\mathbb{I}^*/\mathbb{P}^*$)
Let $\varphi : \mathbb{I}^*_K \longrightarrow \mathbb{I}^*$ *be the map defined by*

$$\varphi(q(u)\langle a(u), b(u) - \overline{v}\rangle_A) = q(u)\langle a(u), b(u) - \overline{v}\rangle_{\overline{K}[u]}.$$

Then φ *is an injective group homomorphism. Moreover,* φ *induces an injective group homomorphism from* $\mathbb{I}^*_K/\mathbb{P}^*_K$ *to* $\mathbb{I}^*/\mathbb{P}^*$.

Proof. The homomorphic property of φ is clear. Now, let $I_1, I_2 \in \mathbb{I}^*_K$ and, for each $i = 1, 2$, write I_i in standard form as $I_i = q_i(u)\langle a_i(u), b_i(u) - \overline{v}\rangle_A$. Suppose now that $\varphi(I_1) = \varphi(I_2)$. Then $q_1\langle a_1, b_1 - \overline{v}\rangle_{\overline{K}[u]} = q_2\langle a_2, b_2 - \overline{v}\rangle_{\overline{K}[u]}$. So, it follows from the uniqueness of the standard form that $q_1 = q_2$, $a_1 = a_2$ and $b_1 = b_2$. Hence, $I_1 = I_2$ and φ is consequently injective.

Thus, φ induces the injection $\mathbb{I}^*_K/(\mathbb{I}^*_K \cap \varphi^{-1}(\mathbb{P}^*)) \hookrightarrow \mathbb{I}^*/\mathbb{P}^*$. If we show that $\mathbb{P}^*_K = \mathbb{I}^*_K \cap \varphi^{-1}(\mathbb{P}^*)$, then we obtain the injection $\mathbb{I}^*_K/\mathbb{P}^*_K \hookrightarrow \mathbb{I}^*/\mathbb{P}^*$, which is clearly a group homomorphism. So it remains to show that $\mathbb{P}^*_K = \mathbb{I}^*_K \cap \varphi^{-1}(\mathbb{P}^*)$. But $\mathbb{I}^*_K \cap \varphi^{-1}(\mathbb{P}^*) \supseteq \mathbb{P}^*_K$ is obvious. So, it remains to prove the reverse inclusion.

For this, let $I \in \mathbb{I}^*_K$ such that $\varphi(I) \in \mathbb{P}^*$. Then, there exists a non-zero element $\omega = \alpha(u) - \beta(u)\overline{v}$ of $B_{\overline{K}}$ such that $\varphi(I) = \langle\omega\rangle_{B_{\overline{K}}}$ and either $\alpha(u)$ or $\beta(u)$ is monic. Note that, since $I \in \mathbb{I}^*_K$, we have $\varphi(I)^\theta = \varphi(I)$, for all $\theta \in Gal(\overline{K}/K)$. Now, let θ be any element of $Gal(\overline{K}/K)$. Then

$$\langle\omega^\theta\rangle_{B_{\overline{K}}} = \langle\omega\rangle_{B_{\overline{K}}}.$$

So, $\lambda_\theta = \frac{\omega^\theta}{\omega}$ is a unit of $B_{\overline{K}}$. Hence, by Lemma 2.7.1, we conclude that $\lambda_\theta \in \overline{K}^*$. But $\alpha(u)^\theta = \lambda_\theta\alpha(u)$ and $\beta(u)^\theta = \lambda_\theta\beta(u)$. Thus, if $\alpha(u)$ is monic, then so is $\alpha(u)^\theta$ and, hence, $\lambda_\theta = 1$. Similarly, $\lambda_\theta = 1$ can be shown if $\beta(u)$ is monic. So $\omega^\theta = \omega$, which implies that $\omega \in B_K$ and, hence, that $\mathbb{I}^*_K \cap \varphi^{-1}(\mathbb{P}^*) \subseteq \mathbb{P}^*_K$. □

Lemma 3.6.3. *Let $I \in \mathbb{I}^*$. Then*

$$I \in \varphi(\mathbb{I}^*_K) \quad \textit{if and only if} \quad I^\theta = I \textit{ for all } \theta \in Gal(\overline{K}/K).$$

Proof.

- If $J \in \mathbb{I}^*_K$, then it is clear that $\varphi(J)^\theta = \varphi(J)$ for all $\theta \in Gal(\overline{K}/K)$.
- Now, let $I \in \mathbb{I}^*$ such that $I^\theta = I$ for all $\theta \in Gal(\overline{K}/K)$. Write I in standard form as $I = q(u)\langle a(u), b(u) - \overline{v}\rangle_{\overline{K}[u]}$, where $q(u) \in \overline{K}(u)$, and $a(u), b(u) \in \overline{K}[u]$.

Then, for all $\theta \in Gal(\overline{K}/K)$, we have

$$I^\theta = q(u)^\theta \langle a(u)^\theta, b(u)^\theta - \overline{v} \rangle_{K[u]},$$

where $q(u)^\theta$ and $a(u)^\theta$ are monic, and $deg(b(u)^\theta) < deg(a(u)^\theta)$. So, by uniqueness of the standard form, we have $q(u)^\theta = q(u)$, $a(u)^\theta = a(u)$ and $b(u)^\theta = b(u)$ for all $\theta \in Gal(\overline{K}/K)$. So $q(u) \in K(u)$ and $a(u), b(u) \in K[u]$. Hence, $I \in \varphi(\mathbb{I}^*_K)$.

□

Definition 3.6.2. (The *div* map)

The map $div : \mathbb{I}^* \longrightarrow \mathbb{D}^0$ is defined as follows:

$$div(I) = \begin{cases} 0 & \text{. if } I = B_K \in \mathbb{I}^*. \\ \sum_{i=1}^m e_i \wp(M_i) - (\sum_{i=1}^m e_i)\infty & \text{. if } I = \prod_{i=1}^m M_i^{e_i} \in \mathbb{I}^*. \end{cases}$$

Theorem 3.6.4. (Correspondence between Ideals and Divisors of degree zero)

The div map defined above is an isomorphism.

Moreover, the fractional ideals of B_K that are generated by non-zero fractional ideals of B_K correspond, via the map div, to the degree-zero divisors of $\mathcal{C}$ that are defined over K.

Proof.

- – The homomorphic property of the *div* map is clear.
- – The injectivity of the *div* map comes from the fact that $ker(div) = \{B_K\}$ and B_K is the unity of $\mathbb{I}^*$.
- – For the surjectivity of *div*, let $D = \sum_{i=1}^m e_i p_i - (\sum_{i=1}^m e_i)\infty \in \mathbb{D}^0$. Then, let $M_i = \wp^{-1}(p_i)$ for $i = 1, \cdots, m$ and note that $div(\prod_{i=1}^m M_i^{e_i}) = D$.

Hence, the *div* map is an isomorphism.

- To prove the second assertion, note that:

$$\begin{aligned} I \in \mathbb{I}^{\bullet} \text{ is generated by an ideal of } \mathbb{I}^{\bullet}_{K} &\overset{(1)}{\Leftrightarrow} I^{\theta} = I \text{ for all } \theta \in Gal(\overline{K}/K) \\ &\Leftrightarrow div(I^{\theta}) = div(I) \text{ for all } \theta \in Gal(\overline{K}/K) \\ &\Leftrightarrow div(I)^{\theta} = div(I) \text{ for all } \theta \in Gal(\overline{K}/K) \\ &\Leftrightarrow div(I) \text{ is defined over } K. \end{aligned}$$

(1): by Lemma 3.6.3.

□

3.7 Hyperelliptic Jacobian

Using the *div* map, we present, in this section, analogous results to those found earlier, for fractional ideals. More specifically, we define an equivalence relation on $\mathbb{D}^{0}_{K}$, introduce the notions of semi-reduced and reduced divisors, and show that any non-trivial degree-zero divisor is equivalent to a unique reduced divisor. Doing so, we define the so-called Jacobian of a hyperelliptic curve.

Definition 3.7.1. (Principal Divisors)
Considering the injective group homomorphism φ going from $\mathbb{I}^{\bullet}_{K}$ to $\mathbb{I}^{\bullet}$, we denote by $\mathcal{P}_{K}$ the image of $\varphi(\mathbb{P}^{\bullet}_{K})$ under the *div* map. Similarly, we denote $div(\mathbb{P}^{\bullet})$ by $\mathcal{P}$.
Then $\mathcal{P}$ is referred to as the set of *principal divisors* and $\mathcal{P}_{K}$ as the set of *principal divisors defined over* K.

Remark 3.7.1. Since the *div* map is a group isomorphism, it carries the group structure of $\mathbb{P}^{\bullet}_{K}$ and $\mathbb{P}^{\bullet}$ to $\mathcal{P}_{K}$ and $\mathcal{P}$ respectively. Thus, both $\mathcal{P}_{K}$ and $\mathcal{P}$ are groups.

Definition 3.7.2. We denote by $\equiv$ the equivalence relation defined on $\mathbb{D}_K^0$ by

$$D_1 \equiv D_2 \text{ if and only if } D_1 - D_2 \in \mathcal{P}_K$$

Definition 3.7.3. (Hyperelliptic Jacobian)

Given a hyperelliptic curve $\mathcal{C}$, we denote by $\mathbb{J}(K)$ the quotient group

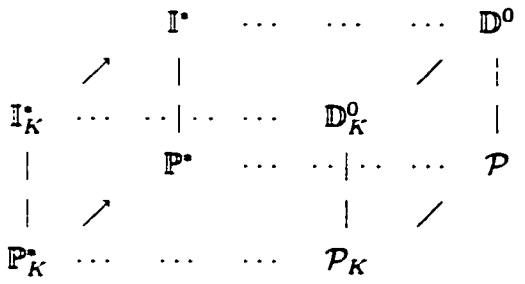
$$\mathbb{J}(K) = \mathbb{D}_K^0/\mathcal{P}_K,$$

where $D_1 + \mathcal{P}_K = D_2 + \mathcal{P}_K$ if and only if $D_1 \equiv D_2$. Moreover, for any $D \in \mathbb{D}_K^0$, we write $[D]_K$ to denote $D + \mathcal{P}_K$.

Then, the Jacobian $\mathbb{J}$ of $\mathcal{C}$ is defined by

$$\mathbb{J} = \mathbb{D}^0/\mathcal{P}.$$

We now have the following figure:



Remark 3.7.2.

- Using Theorem 3.6.4, Definition 3.7.1 and the above figure, we see that the *div* map identifies the group structures of the following:
  - $\mathbb{I}^*$ and $\mathbb{D}^0$.
  - $\varphi(\mathbb{I}_K^*)$ and $\mathbb{D}_K^0$.
  - $\mathbb{P}^*$ and $\mathcal{P}$.
  - $\varphi(\mathbb{P}_K^*)$ and $\mathcal{P}_K$.

- Hence, the *div* map and the injective homomorphism φ induce a group isomorphism between the quotients $\mathbb{I}_K^*/\mathbb{P}_K^*$ and $\mathbb{J}(K) = \mathbb{D}^0/\mathcal{P}$.

- Finally, we know (from Theorem 3.6.2) that $\mathbb{I}_K^*/\mathbb{P}_K^*$ is homomorphically injected into $\mathbb{I}^*/\mathbb{P}^*$. So the quotient group $\mathbb{J}(K) = \mathbb{D}_K^0/\mathcal{P}_K$ is also homomorphically injected into the Jacobian $\mathbb{J} = \mathbb{D}^0/\mathcal{P}$. Thus, $J(K)$ can be identified to a subgroup of $\mathbb{J}$.

Definition 3.7.4. (Semi-reduced divisor)

A *semi-reduced divisor* D is a degree-zero divisor such that $div^{-1}(D)$ is a non-zero semi-reduced fractional ideal of $B_{\overline{K}}$.

Remark 3.7.3. By Lemma 3.2.1, we see that a divisor D is said to be semi-reduced if $D \in \mathbb{D}^0$ and the following are true:

1. $ord_p(D) > 0$ for all $p \in supp(D)$ such that $p \neq \infty$,

2. if $p \in supp(D)$, then $\tilde{p} \notin supp(D)$ [1], unless $p = \tilde{p}$, in which case $ord_p(D) = 1$.

Lemma 3.7.1. (Semi-reduced representatives of classes in $\mathbb{J}(K)$)

Let $D \in \mathbb{D}_K^0$. Then $[D]_K$ has a semi-reduced representative divisor $D' \in \mathbb{D}_K^0$.

Proof. This follows directly from Definition 3.7.4, Theorem 3.6.4 and Theorem 3.2.2. □

Definition 3.7.5. (Reduced Divisor)

A semi-reduced divisor D is said to be *reduced* if $div^{-1}(D)$ is a non-zero reduced fractional ideal of $B_{\overline{K}}$.

[1] We define the conjugate $\tilde{p}$ of the point $p = (x, y) \in C$ to be the point $\sigma(\sigma(\langle u - x, y - \overline{v}\rangle_{\overline{K}[u]})) = (x, -h(x) - y)$, where the conjugation map $\sigma : u \mapsto u, \overline{v} \mapsto -\overline{v} - h \in Gal(K(C)/K(u))$ was defined earlier.

Theorem 3.7.2. (Unique representative of classes of $\mathbb{J}(K)$)

Let $D \in \mathbb{D}_K^0$. Then $[D]_K$ has a unique reduced representative divisor $D' \in \mathbb{D}_K^0$.

Proof. This follows directly from Definition 3.7.5, Theorem 3.6.4 and Theorem 3.3.1.

□

Definition 3.7.6. (Length of a degree zero Divisor)

Let $D = \sum_{i=1}^{m} e_i p_i - (\sum_{i=1}^{m} e_i)\infty$ be a degree zero divisor. The *length* $|D|$ of D is defined by

$$|D| = \sum_{i=1}^{m} |e_i| .$$

Lemma 3.7.3. (Alternative Characterization of Reduced Divisors)

Let $I \in \mathbb{I}_K^*$ be semi-reduced and let $D = div(\varphi(I))$. Then the following are true:

(i) $|D| = deg(N(\varphi(I)))$.

(ii) *D is reduced if* $|D| \leq g$.

Proof. First, note that *(ii)* follows from *(i)* combined with Definition 3.7.5 and Definition 3.3.1. Hence, it suffices to show *(i)*.

For this, let $\varphi(I) = \prod_{i=1}^{q} P_i^{e_i}$ be the factorization of $\varphi(I)$ into prime ideals of $B_{\overline{K}}$. Since I is semi-reduced, note that $e_i > 0$ for $i = 1, \cdots, q$. So

$$|D| = |div(\varphi(I))| = \left| \sum_{i=1}^{q} e_i \phi(P_i) - \left(\sum_{i=1}^{q} e_i \right) \infty \right| = \sum_{i=1}^{q} |e_i| = \sum_{i=1}^{q} e_i .$$

But

$$deg(N(\varphi(I))) = \sum_{i=1}^{q} deg(N(\varphi(P_i^{e_i}))) = \sum_{i=1}^{q} e_i \cdot deg(N(\varphi(P_i))).$$

Now, for each $i = 1, \cdots, q$, note that $deg(N(P_i)) = 1$ since P_i has the form $\langle u - x_i, y_i - \overline{v} \rangle_{\overline{K}[u]}$ for some $x_i, y_i \in \overline{K}$. Hence,

$$deg(N(\varphi(I))) = \sum_{i=1}^{q} e_i = |D|.$$

□

Theorem 3.7.4. *If K is a finite field, then $\mathbb{J}(K)$ is finite.*

Proof. Since $\mathbb{J}(K)$ and $\mathbb{I}_K^*/\mathbb{P}_K^*$ are isomorphic groups, it suffices to show that $\mathbb{I}_K^*/\mathbb{P}_K^*$ is finite, whenever K is finite. Now, to show this, note that every class of $\mathbb{I}_K^*/\mathbb{P}_K^*$ has a reduced representative. Hence, the classes of $\mathbb{I}_K^*/\mathbb{P}_K^*$ can each be represented uniquely by an ideal of the form $\langle a(u), b(u) - \overline{v} \rangle_A$, where $a(u), b(u) \in K[u]$, $a(u)$ is monic and $deg(b(u)) < deg(a(u)) \leq g$. But, since K is finite, there are a finite number of polynomials $a(u), b(u) \in K[u]$ that satisfy these conditions. So $\mathbb{I}_K^*/\mathbb{P}_K^*$ is finite. □

To close this chapter, let us point out that, since $\mathbb{J}(K)$ and $\mathbb{I}_K^*/\mathbb{P}_K^*$ are isomorphic groups, we can use this isomorphism and the computational laws developed earlier for $\mathbb{I}_K^*/\mathbb{P}_K^*$ to obtain the results of computation intended to be carried in $\mathbb{J}(K)$. In fact, the algorithm of Theorem 3.4.2 is computationally equivalent to the so-called Cantor's algorithm for computing in a hyperelliptic Jacobian (see [4] for further information).

Chapter 4

Applications to Cryptography

In this ultimate chapter, we present applications of hyperelliptic curves to cryptography. In particular, we show how hyperelliptic Jacobians can be used to build cryptosystems based on the Discrete Logarithm Problem, and we address the important issues of message encoding and divisor compression.

4.1 Introduction

Whenever a finite Abelian group G is known, one may try to determine whether the discrete logarithm problem (DLP) is difficult to solve in G. If this problem is proved or strongly assumed to be computationally hard on G, then systems allowing proven or assumed secure communication may be built on G.

In the previous chapter, we showed that, if $\mathcal{C}$ is a hyperelliptic curve defined over a finite field K, then $\mathbb{J}(K)$ is a finite Abelian group. Thus, we may formulate the DLP on $\mathbb{J}(K)$ as follows:

> Given two divisors D_0 and D_1 of $\mathbb{J}(K)$, find (if it exists) an integer m such that $D_1 \equiv mD_0$.

When N. Koblitz introduced Hyperelliptic Curve cryptosystems (see [11]), the best attacks to solve the HCDLP were the general ones known for solving the DLP in Abelian groups, namely the "Baby-step Giant-step" algorithm, the Pollard rho method, the Pohlig-Hellman algorithm and the Index Calculus type of attacks. These attacks are all of exponential time complexity, and the best current one for low-genus curves is due to P. Gaudry, who showed that his index calculus type method performs better than Pollard's rho method for curves of genus greater than 4 (see [13]).

In [9], M. Adleman, J. DeMarrais and M.-D. Huang (ADH) presented an attack which has subexponential time complexity for large genus hyperelliptic curves defined over odd characteristic finite fields. In [1], A. Enge improved the result of ADH by presenting a subexponential attack solving the DLP for hyperelliptic curves, defined over arbitrary finite fields, whose genus is greater than a specified lower bound. Enge's attack is the best current one against high-genus hyperelliptic curves.

However, as summarized by N. G. Smart in [10], three special types of curves should be avoided for use in cryptography:

1. Curves with n points over $\mathbb{F}_q$ such that there exists a small integer l satisfying $q^l \equiv 1 \ mod \ n$. This is due to a generalization, by Frey and Rück (see [6]), of the attack of Menezes et al on supersingular elliptic curves.

2. Curves for which $\mathbb{J}(\mathbb{F}_p)$ has a subgroup of order p with small index. This is also due to Rück (see [7]) who generalized, for these curves, the anomalous elliptic curve attack due to Semaev, Satoh, Araki and Smart.

3. Curves of genus g over $\mathbb{F}_p$ for which $3g > log(p)$. These curves are indeed susceptible to an attack due to Flassenberg and Paulus (see [17] and [15]).

Apart from these three avoidable types of curves, the HCDLP is assumed to be computationally hard to solve (especially for curves of genus lower than 4). Hence, $\mathbb{J}(K)$ provides a structure suitable for use in cryptography. In particular, let us present the ElGamal cryptosystem on $\mathbb{J}(K)$.

The ElGamal Cryptosystem :

If a member A (of a community using the ElGammal cryptosystem) wants to send a message m to another member B, then the following must take place:

Step 1: B must generate its public and private keys as follows:

1. Select a finite field K, a hyperelliptic curve C defined over K and a cyclic subgroup G of order n of $\mathbb{J}(K)$ such that the DLP is assumed or proven to be difficult to solve on G. Denote then by eq the defining equation of C
2. Find a generator D of G
3. Select a random integer a such that $1 \leq a \leq n-1$, and compute aD.

   Result: (D, aD, eq, K) and a are, respectively, the public and private keys of B.

Step 2: A must encrypt m as follows:

1. Obtain B's public key (D, aD, eq, K).
2. Encode[1] m onto G as D_m.
3. Select a random integer k such that $1 \leq k \leq n-1$.

[1]The ElGamal encryption scheme assumes the public knowledge of a mechanism which translates messages into divisors belonging to a chosen cyclic subgroup of $\mathbb{J}(K)$. If $\mathbb{J}(K)$ is cyclic, one may then use the encoding/decoding scheme presented in section 4.2.2. Even though other encryption schemes assume the public knowledge of an encoding/decoding mechanism, they do not require that messages are encoded into cyclic groups.

4. Compute $\gamma = kD$ and $\delta = D_m + k(aD)$.

   Result: The ciphertext $c = (\gamma, \delta)$ represents m and is sent to B.

Step 3: B decrypts the cyphertext c as follows:

1. Use the private key a to compute $-a\gamma$.
2. Recover D_m by computing $(-a\gamma) + \delta$.
3. Decode D_m into a message m'.

   Result: m' is the original message m.

4.2 Message Encoding

Message encoding is of crucial importance in cryptography. In the context of hyperelliptic curve cryptography, one would like to define a correspondence between messages (say integers of a given range) and divisors of a Jacobian. In this section, such a message encoding method is presented.

First, we construct a probabilistic method for generating points on a hyperelliptic curve. Then, we generalize the elliptic curve message embedding scheme suggested by N. Koblitz (c.f. p. 179 of [12]) in order to develop a message encoding scheme on the Jacobian of a hyperelliptic curve.

4.2.1 Generating Points on a Hyperelliptic Curve

Theorem 4.2.1. *Let t be a positive integer and C be a hyperelliptic curve defined, over a finite field $K = \mathbb{F}_{p^n}$, by equation 2.1.1. Then it is possible to generate a point (x, y) of C, within t trials, with a success probability of approximately $(1 - \frac{1}{2^t})$.*

Proof. Let us first assume that $char(K) \neq 2$:

Note that C is in bijection with the hyperelliptic curve C' defined over K, by the equation $\mathbf{v}^2 = \mathbf{f}(u)$, where $\mathbf{v} = v - \frac{h}{2}$ and $\mathbf{f} = f + \frac{h^2}{4}$. Thus, we can assume that $h(u) = 0$ and equation 2.1.1 then becomes

$$v^2 = f(u). \tag{4.2.1}$$

Now, given $x \in K$, one seeks a root of $v^2 - f(x)$. Assuming, as N. Koblitz on page 180 of [12], that the probability for $f(x)$ not be a square in K is approximately $\frac{1}{2}$, we conclude that the probability of finding, within t random trials, a value x such $f(x)$ is a square is about $(1 - \frac{1}{2^t})$.

Let us now assume that $char(K) = 2$:

Then $K = \mathbb{F}_{2^n}$ for some positive integer n and, since $h(u) \neq 0$, we can distinguish two situations:

- Assume first that $h(u) \neq 1$.

  If $x \in K$ is a root of $h(u)$, then $v = f(x)$ is the solution of the equation $v^2 + h(x)v + f(x) = 0$, since $f(x)^2 = f(x)$.

  Moreover, note that the map $(u, v) \mapsto (u, \frac{v}{h(u)})$ draws a bijection between the two sets of points $(u, v) \in K \times K$ satisfying conditions C_1 and C_2, respectively.

$$C_1 : \begin{cases} h(u) \neq 0 \text{ and} \\ v^2 + h(u)v + f(u) = 0 \end{cases} \quad \text{and } C_2 : \begin{cases} h(u) \neq 0 \quad \text{and} \\ v^2 + v + \frac{f(u)}{h(u)^2} = 0 \end{cases}$$

  Thus, if x is not a root of $h(u)$, then the probability of finding a solution of $v^2 + h(x)v + f(x) = 0$ is that of solving the equation $v^2 + v + \gamma = 0$, where $\gamma = \frac{f(x)}{h(x)^2} \in K$. Now, as we will show below, the latter equation has a solution

if and only if the trace $tr(\gamma)$ of γ is 0. But the trace $tr : K \longrightarrow \mathbb{F}_2$ is a $\mathbb{F}_2$-linear map, which, consequently, satisfies $|ker(tr)| = \frac{|K|}{2}$. Hence, assuming the randomness of $tr(\frac{f}{h^2})$ outside of h's roots, we see that the probability for $tr(\frac{f}{h^2})$ to be 0 is approximately $\frac{1}{2}$. Therefore, the probability of finding, outside of h's roots, and within t random trials, a value $x \in K$ such that $v^2+h(x)v+f(x) = 0$ has a solution $v \in K$ is about $(1 - \frac{1}{2^t})$.

- Now, let us assume that $h(u) = 1$. Then equation 2.1.1 becomes

$$v^2 + v + f(u) = 0. \tag{4.2.2}$$

When x has been chosen, then we let $\gamma = f(x)$ and seek a solution of

$$v^2 - v - \gamma = 0. \tag{4.2.3}$$

As we will see, the existence of a solution for this equation is guaranteed if and only if the trace $tr(\gamma)$ of γ is equal to 0. This result is in fact a special case of Hilbert's Theorem 90, for which we present the following short proof (c.f. Theorem 6.3, on page 290 of [16]).

First of all, note that the Galois group $Gal(K/\mathbb{F}_2)$ is cyclic and generated by the Frobenius automorphism $\sigma : u \mapsto u^2$.

Thus, if there exists a solution $\alpha \in K$ of equation 4.2.3, then

$$\gamma = -\alpha - \alpha^2 = \alpha - \alpha^\sigma,$$

and, consequently:

$$tr(\gamma) = \sum_{i=1}^{n} \gamma^{\sigma^i} = (\alpha^\sigma - \alpha^{\sigma^2}) + (\alpha^{\sigma^2} - \alpha^{\sigma^3}) + \cdots + (\alpha^{\sigma^n} - \alpha^\sigma) = 0.$$

Conversely, assume that $tr(\gamma) = 0$ and note that, since the trace is a non-zero linear form, there exists an element θ of K such that $tr(\theta) = 1 \neq 0$. Then, considering

$$\alpha = \frac{1}{tr(\theta)}(\gamma\theta^{\sigma} + (\gamma + \gamma^{\sigma})\theta^{\sigma^2} + \cdots + (\gamma + \gamma^{\sigma} + \cdots + \gamma^{\sigma^{n-2}})\theta^{\sigma^{n-1}}).$$

we obtain the following:

$$\begin{aligned}
-\alpha - \alpha^2 &= \alpha - \alpha^{\sigma} \\
&= \frac{1}{tr(\theta)}\Big(\gamma\theta^{\sigma} + (\gamma + \gamma^{\sigma})\theta^{\sigma^2} + \cdots + (\gamma + \gamma^{\sigma} + \cdots + \gamma^{\sigma^{n-2}})\theta^{\sigma^{n-1}} \\
&\qquad -\gamma^{\sigma}\theta^{\sigma^2} - (\gamma^{\sigma} + \gamma^{\sigma^2})\theta^{\sigma^3} - \cdots - (\gamma^{\sigma} + \gamma^{\sigma^2} + \cdots + \gamma^{\sigma^{n-1}})\theta^{\sigma^n}\Big) \\
&= \frac{1}{tr(\theta)}\Big(\gamma\theta^{\sigma} - \gamma\theta^{\sigma^2} + \cdots + \gamma\theta^{\sigma^{n-1}} - (\gamma^{\sigma} + \gamma^{\sigma^2} + \cdots + \gamma^{\sigma^{n-1}})\theta^{\sigma^n}\Big) \\
&= \frac{1}{tr(\theta)}(\gamma(tr(\theta) - \theta) - (tr(\gamma) - \gamma)\theta) \\
&= \frac{1}{tr(\theta)}(\gamma tr(\theta) - \gamma\theta + \gamma\theta) \\
&= \gamma.
\end{aligned}$$

i.e. α is a solution of equation 4.2.3.

Hence, we conclude that equation 4.2.3 has a solution if and only if $tr(\gamma) = 0$. Now, assuming the randomness of $tr(f)$, the probability for $tr(f(x))$ to be 0, when x is randomly chosen, is approximately that of $tr(x)$ to be 0, that is $\frac{1}{2}$. Thus, the probability of finding, within t random trials, a value x such $tr(f(x)) = 0$ is about $(1 - \frac{1}{2^t})$.

□

4.2.2 Message Encoding

Before presenting the message encoding algorithm, we first need to establish a representation of the elements of any given finite field K.

Let then p be the prime and n be the positive integer such that $K = \mathbb{F}_{p^n}$. Then, by the primitive element Theorem, there exists an element x of K such that $\{x^{n-1}, x^{n-2}, \cdots, x, 1\}$ is an $\mathbb{F}_p$-basis of K. Thus, any element α of K can be uniquely written as $\alpha = \sum_{i=0}^{n-1} a_i x^i$, where $a_0, \cdots, a_{n-1}$ are non-negative integers which are smaller than p. Hence, any element $\alpha \in K$ can be represented as an ordered sequence $(a_{n-1}a_{n-1}\cdots a_1 a_0)$ of n non-negative integers which are smaller than p. Moreover, we can associate, to any $\alpha \in K$ represented as $(a_{n-1}\cdots a_0)$, the integer $a = \sum_{i=0}^{n-1} a_i p^i$.

Let us now present the encoding algorithm.

Input:

- A positive integer g.
- A positive integer t such that the desired encoding success probability is approximately $(1 - \frac{1}{2^t})^g$.
- A message range $[0, \Omega)$.
- A prime number p.
- A positive integer n such that $log_p(\Omega \cdot g \cdot t) \leq n$.
- A hyperelliptic curve C, of genus g, defined over the finite $K = \mathbb{F}_{p^n}$, by equation 2.1.1.
- An ordered sequence $m_1, m_2, \cdots, m_g \in [0, \Omega)$ of messages.

Algorithm:

1. Let $l_\Omega = \lfloor log_p(\Omega) \rfloor$ and $l_g = \lfloor log_p(g) \rfloor$ and $l_t = \lfloor log_p(t) \rfloor$.

2. For $i = 1$ to g, proceed as follows:

   Step 1: Set the integer j to 1 and the boolean $Nexti$ to $False$. Then, compute the following:

   * $(\alpha_{l_\Omega - 1} \cdots \alpha_0)_p$ is the l_Ω-digit[2] base-p representation of m_i.
   * $(\beta_{l_g - 1} \cdots \beta_0)_p$ is the l_g-digit base-p representation of the integer i.
   * δ is the sequence $(\beta_{l_g - 1} \cdots \beta_0 \alpha_{l_\Omega - 1} \cdots \alpha_0)$.

   Step 2: While ($j \leq t$ and $Nexti = False$) do the following:

   (a) Compute the l_t-digit base-p representation $(\gamma_{l_t - 1} \cdots \gamma_0)_p$ of the integer j.

   (b) Let x_i be the element of K represented by the padded sequence $(\gamma_{l_t - 1} \cdots \gamma_1 \gamma_0 | \delta)$.

   (c) Determine whether the equation $v^2 + h(u)v - f(u) \equiv 0 \ mod \ (u - x_i)$ has a solution in K.

   * If $y_i \in K$ is a solution of this equation, then $\langle u - x_i, y_i - \overline{v} \rangle_A$ is a prime ideal of B_K. So, set $Nexti$ to $True$.
   * If there is no solution of this equation, then set j to $j + 1$.

3. Let $a(u) = \prod_{i=1}^{g} (u - x_i) \in K[u]$ and $b(u) \in K[u]$ be the solution $(mod \ a(u))$ of the system

$$\varepsilon(u) \equiv y_i \ mod \ (u - x_i), \text{for all } i = 1, \cdots, g.$$

Output: The divisor $D = div(\varphi(\langle a(u), b(u) - \overline{v} \rangle_A)) \in \mathbb{J}(K)$, representing the ordered sequence $m_1, m_2, \cdots, m_g$ of message.

[2]This is just the typical base-p representation with zeros padded at the beginning, if necessary. For example, the 6-digit base-2 representation of the integer 13 is $(001101)_2$.

Remark 4.2.1.

- For all $i = 1, \cdots, g$, note that the base-p representation of m_i can be obtained directly from the l_Ω last digits of the representation of x_i as a sequence of non-negative integers each smaller than p.
- For all $i = 1, \cdots, g$, note that x_i is represented as a sequence of $l_\Omega + l_g + l_t$ integers. Hence, the fact that $log(\Omega \cdot g \cdot t) \leq n$ allows to represent any $x_i \in K = \mathbb{F}_{p^n}$.
- The encoding procedure simply (and judiciously) generates g points of $\mathcal{C}$. Hence, the success probability of $(1 - \frac{1}{2^t})^g$ follows directly from Theorem 4.2.1.
- Note that the encoding scheme maps g-long sequences of messages to reduced divisors of the form $div(\varphi(\langle a(u), b(u) - \overline{v} \rangle_A))$ where $a(u)$ factors completely over K. Moreover, since any message m is mapped to the x component of a point (x, y) of $\mathcal{C}(K)$, then it may happen that the encoding scheme uses only half of the points of $\mathcal{C}(K)$ (in particular, if $\mathcal{C}(K)$ has no finite special points).

  Hence, these limitations should be mitigated with the high success probability of the encoding scheme.

4.3 Divisor Compression

Divisor compression is the hyperelliptic counterpart of elliptic curve point compression, which allows for a 50% bandwidth reduction when transferring or storing information. If $\mathcal{C}$ is a hyperelliptic curve defined, over a finite field K, by equation 2.1.1, then (a priori) it takes $2g$ elements of K to represent a reduced divisor $D = div(\langle a(u), b(u) - \overline{v} \rangle_A)$ (since $deg(b) < deg(a) \leq g$). However, we will show that D can be represented using only g elements of K and a g-long array $\mathcal{B} = [\beta_1 | \beta_2 | \cdots | \beta_g]$

of binary bits. This compression scheme is inspired by a technique presented by F. Hess, G. Seroussi and N. Smart, in [5].

In order to perform the divisor compression, we first need to establish an order on K. This can be done as follows:

> Let a and b be the two integers associated with any two elements α, β of K. Then α is said to be *smaller* than β (and we write $\alpha < \beta$) if $a < b$.

Similarly, we can establish an order on $K[u]$, as follows:

> Let $a_j(u) = \sum_{i=0}^{q} a_{j,i}\, u^i \in K[u]$, for $j = 1, 2$. Let also $a_{j,i}$ be the integer associated with $a_{j,i}$, for all $j = 1, 2$ and $i = 1, \cdots, q$. Then $a_1(u)$ is said to be *smaller* than $a_2(u)$ (and we write $a_1(u) < a_2(u)$) if
>
> $$\left(\sum_{i=0}^{q} a_{1,i} p^{ni}\right) < \left(\sum_{i=0}^{q} a_{2,i} p^{ni}\right).$$

These two orders are examples of *lexicographic* orders of K and $K[u]$, respectively. Let us now present the compression algorithm and its decompression analogue. Then, we will prove that they are sound.

4.3.1 Compression Algorithm

Input:

- The integer n and the prime p characterizing the finite field $K = \mathbb{F}_{p^n}$.
- The equation $v^2 + vh(u) = f(u)$ determining the hyperelliptic curve $\mathcal{C}$ defined over K.
- A reduced divisor $D = div(\varphi(\langle a(u), b(u) - \overline{v} \rangle_A)) \in \mathbb{D}_K^0$.

Compression:

- Step 1: Find the irreducible polynomials $p_1(u), p_2(u), \cdots, p_{m-1}(u)$ and $p_m(u)$ of $K[u]$ such that $a(u) = \prod_{i=1}^{m} p_i(u)$, and order them lexicographically, as $p_1(u), p_2(u), \cdots, p_m(u)$ [3].
- Step 2: For each $i = 1, \cdots, m$ proceed as follows:
  - If $i \geq 2$ and $p_i(u) = p_{i-1}(u)$, then set the binary bit $\mathcal{B}_i$ to equal its predecessor $\mathcal{B}_{i-1}$.
  - Otherwise, proceed as follows:
    1. Compute $s_i(u) = b(u) \ mod \ p_i(u)$ and $\widetilde{s}_i(u) = -b(u) - h(u) \ mod \ p_i(u)$.
    2. · If $s_i(u) \leq \widetilde{s}_i(u)$, then set $\mathcal{B}_i$ to be 1.
       · Otherwise, set $\mathcal{B}_i$ to be 0.
- Step 3: If $m < g$, then set $\mathcal{B}_i$ to be 0, for $i = m + 1, \cdots, g$.

Output: $\{ (p_1(u), p_2(u), \cdots, p_m(u)) : \mathcal{B} \}$ represents the reduced divisor D, where $\mathcal{B} = [\mathcal{B}_1 | \cdots | \mathcal{B}_g]$ is a g-long array of binary bits.

4.3.2 Decompression Algorithm

Input: $\{ (p_1(u), p_2(u), \cdots, p_m(u)) : \mathcal{B} \}$ is the compressed representative of a divisor D, where $\mathcal{B} = [\mathcal{B}_1 | \cdots | \mathcal{B}_g]$ is a g-long array of binary bits.

[3] Note that $1 \leq m \leq g$.

Decompression:

- Step 1: For $i = 1, \cdots, m$ proceed as follows:
  - If $i \geq 2$ and $p_i(u) = p_{i-1}(u)$, then set the polynomial $b_i(u)$ of $K[u]$ to equal its predecessor $b_{i-1}(u)$.
  - Otherwise, proceed as follows:
    1. Compute the two solutions $s_i(u)$ *mod* $p_i(u)$ and $-s_i(u)-h(u)$ *mod* $p_i(u)$ of the equation $v^2 + vh(u) - f(u) \equiv 0$ *mod* $p_i(u)$.
    2. · If $\mathcal{J}_i = 1$, then let $b_i(u)$ be the smallest of $s_i(u)$ *mod* $p_i(u)$ and $-s_i(u) - h(u)$ *mod* $p_i(u)$.
       · Otherwise, let $b_i(u)$ be the greatest of $s_i(u)$ *mod* $p_i(u)$ and $-s_i(u) - h(u)$ *mod* $p_i(u)$.
- Step 2: Using Theorem 3.4.2, compute the polynomials $a(u)$ and $b(u)$ of $K[u]$ such that:

$$\langle a(u), b(u) - \overline{v} \rangle_A = \prod_{i=1}^{m} \langle p_i(u), b_i(u) - \overline{v} \rangle_A.$$

Output: The divisor $D = div(\varphi(\langle a(u), b(u) - \overline{v} \rangle_A))$ is reduced and corresponds to the compressed form $\{ (p_1(u), p_2(u), \cdots, p_m(u)) : \mathcal{J} \}$.

Theorem 4.3.1. *Let $D = div(\langle a(u), b(u) - \overline{v} \rangle_A) \in \mathbb{D}_K^0$ be a reduced divisor. If the compression and decompression algorithms are successively applied to D, then the resulting divisor is D itself.*

Proof. The idea behind the compression algorithm is to decompose the reduced ideal $\langle a(u), b(u) - \overline{v} \rangle_A$ of B_K into a product $\langle p_1(u), b_1(u) - \overline{v} \rangle_A \cdots \langle p_m(u), b_m(u) - \overline{v} \rangle_A$ of prime ideals B_K. Then, remarking that, for each $i = 1, \cdots, m$, the class $b_i(u)$ *mod* $p_i(u)$ is one of the two solutions of the equation

$$v^2 + vh(u) - f(u) \equiv 0 \text{ } mod \text{ } p_i(u), \tag{4.3.1}$$

the trick is to set β_i to be the information bit that specifies which of the two solutions $b_i(u)\ mod\ p_i(u)$ is.

Let us first comment each step of the compression algorithm.

- Step 1: The irreducible factors $p_1(u), \cdots, p_m(u)$ of $a(u)$ can be found using conventional factorization techniques.
- Step 2:
  - If $i \geq 2$ and $p_i(u) = p_{i-1}(u)$, then $b_i(u) = b_{i-1}(u)$ since D is reduced. Hence, $\beta_i = \beta_{i-1}$.
  - Otherwise:
    1. We compute $s_i(u) = b(u)\ mod\ p_i(u)$ and $\widetilde{s}_i(u) = -b(u) - h(u)\ mod\ p_i(u)$. Such modular reduction can be performed in polynomial time complexity.
    2. Then β_i is set to be 1 if and only if $b(u)\ mod\ p_i(u)$ is the smallest of $b(u)\ mod\ p_i(u)$ and $-b(u) - h(u)\ mod\ p_i(u)$.
- Step 3: This is just in case $a(u)$ has at least one non-linear irreducible factor. We then give default values to $\beta_{m+1}, \cdots, \beta_g$.

Let us now comment the decompression algorithm and show that it works.

The idea here is to use the binary bits $\beta_1, \cdots, \beta_m$ in order to recover the polynomials $b_1(u), \cdots, b_m(u)$. Let us then analyze each step of the algorithm and see how the $b_i(u)$'s are recovered.

- Step 1:
  - If $i \geq 2$ and $p_i(u) = p_{i-1}(u)$, then $b_i(u) = b_{i-1}(u)$ since D is reduced.
  - Otherwise:
    1. The two solutions $s_i(u)\ mod\ p_i(u)$ and $-s_i(u) - h(u)\ mod\ p_i(u)$ of equation 4.3.1 can be found in polynomial time complexity. We now need to determine which one of these solutions is $b_i(u)$.
    2. * If $\beta_i = 1$, then, by the compression algorithm, $b_i(u)$ must be the lowest of the two solutions.
       * Otherwise, $b_i(u)$ must be the greatest of the two solutions.

- Step 2: Theorem 3.4.2 may be used to compute

$$\prod_{i=1}^{m} \langle p_i(u), b_i(u) - \overline{v} \rangle_A = \langle a(u), b(u) - \overline{v} \rangle_A.$$

Hence, we see that the compression and decompression schemes do work.

Moreover, note that, since the polynomial $a(u) \in K[u]$ is monic, it takes $deg(a)$ elements of K to represent the sequence $p_1(u), p_2(u), \cdots, p_m(u)$. Consequently, it takes at most g elements of K to represent the sequence $p_1(u), \cdots, p_m(u)$ and g binary bits to represent the polynomial $b(u)$. □

4.4 Examples

In this section, we first present two examples of hyperelliptic curves defined over finite fields of odd and even characteristic. Then, we reveal the structure of the group $\mathbb{J}(K)$ associated with a hyperelliptic curve defined over a finite field K of even characteristic. Using this $\mathbb{J}(K)$, we then illustrate both divisor compression and ElGamal encryption.

4.4.1 A Hyperelliptic Curve defined over $\mathbb{F}_{3^2}$

Let $m(u) = u^2 + 1 \in \mathbb{Z}_3[u]$. Then $m(u)$ is irreducible over $\mathbb{Z}_3$ since it has no root in $\mathbb{Z}_3$. Then $K = \mathbb{F}_{3^2} \cong \mathbb{Z}_3[u]/(m(u))$. Moreover, if $x \in K$ is such that $x^2 + 1 = 0$, then $K = \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}$. Now, the multiplicative group generated by $\alpha = x + 2$ is presented in the following table.

α	α^2	α^3	α^4	α^5	α^6	α^7	α^8
$x+2$	x	$2x+2$	2	$2x+1$	$2x$	$x+1$	1

Hence, we see that α generates K^*.

Now, let $f(u) = u(u^2+1)(u+1)(u+2) = u^5 + 2u$ and note that it has no double

root. Consider then the curve C defined. over K. by $v^2 = f(u)$. Then the following table presents the values of u^2 and $f(u)$ for all $u \in K$.

u	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	0
u^2	x	2	$2x$	1	x	2	$2x$	1	0
$f(u)$	$x+2$	0	$2x+2$	0	$2x+1$	0	$x+1$	0	0

So. the finite points verifying $v^2 = f(u)$ are $(0,0)$. $(\alpha^2,0)$. $(\alpha^4,0)$. $(\alpha^6,0)$ and $(\alpha^8,0)$. Now. the partial derivatives of $v^2 = f(u)$ are $2v$ and $-f'(u) = u^4 + 1$. Moreover. a point (s_1, s_2) of C is a solution of the system $\begin{cases} 2v & = 0 \\ u^4+1 & = 0 \end{cases}$ if and only if s_1 is a double root of $f(u)$. But $f(u)$ has no double root. So C is a hyperelliptic curve of genus $g = 2$ and whose points over K are $(0,0)$. $(\alpha^2,0)$. $(\alpha^4,0)$. $(\alpha^6,0)$. $(\alpha^8,0)$ and ∞. In particular. note that all points of $C(K)$ are special[4].

4.4.2 A Hyperelliptic Curve defined over $\mathbb{F}_{2^3}$

Let $m(u) = u^3 - u - 1 \in \mathbb{Z}_2[u]$. Then $m(u)$ is irreducible over $\mathbb{Z}_2$ since it has no root in $\mathbb{Z}_2$. Then $K = \mathbb{F}_{2^3} \cong \mathbb{Z}_2[u]/(m(u))$. Moreover. if $x \in K$ is such that $x^3 + x + 1 = 0$. then $K = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$. Now. the multiplicative group generated by $\alpha = x$ is presented in the following table.

α	α^2	α^3	α^4	α^5	α^6	α^7
x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1

Hence. we see that α generates K^*.

Now. let $h(u) = u$ and $f(u) = m(u)(u^2 + u + 1) = u^5 + u^4 + 1$. Consider then the curve C defined. over K. by $v^2 + vu = u^5 + u^4 - 1$. Then the following table presents the values of $f(u)$ for all $u \in K$.

[4] A point p of C is said to be *special* if $p = \bar{p}$.

u	α	α^2	α^3	α^4	α^5	α^6	α^7	0
$f(u)$	0	0	x^2	0	x	x^2+x	1	1

Moreover, the value of v^2+uv is given by the following table.

$v \setminus u$	α	α^2	α^3	α^4	α^5	α^6	α^7	0
α	0	x^2+x+1	x	$x+1$	1	x^2+1	x^2+x	x^2
α^2	x^2+1	0	1	$x+1$	x^2+x+1	x^2	x	x^2+x
α^3	$x+1$	x	0	x^2	x^2+x+1	1	x^2+x	x^2+1
α^4	x^2+1	x^2+x+1	$x+1$	0	x^2+x	1	x^2	x
α^5	x^2+x	x	1	x^2+x+1	0	x^2+1	x^2	$x+1$
α^6	x^2-x	x^2+1	$x+1$	x^2	1	0	x	x^2+x+1
α^7	$x+1$	x^2+1	x	x^2+x+1	x^2+x	x^2	0	1
0	0	0	0	0	0	0	0	0

So, the finite points verifying $v^2+uv = f(u)$ are $(0,1)$, $(\alpha,0)$, (α,α), $(\alpha^2,0)$, (α^2,α^2), $(\alpha^4,0)$ and (α^4,α^4).

Now, the partial derivatives of $v^2+uv = f(u)$ are u and $v+u^4$. So the first derivative has non-zero values for all $u \in \overline{K}^*$. Moreover, the partial derivatives at $(0,1)$ have value 0 and 1 respectively. So $\mathcal{C}$ is a hyperelliptic curve of genus $g=2$ and its points over K are $(0,1)$, $(\alpha,0)$, (α,α), $(\alpha^2,0)$, (α^2,α^2), $(\alpha^4,0)$, (α^4,α^4) and ∞. In particular, note that $\mathcal{C}(K)$ has no finite special point over K.

4.4.3 Structure of $\mathbb{J}(\mathbb{F}_2)$ for an given Hyperelliptic Curve

Consider the two polynomials $h(u)=u$ and $f(u)=u^5+u^3+u^2+1$ of $\mathbb{Z}_2[u]$, and the curve $\mathcal{C}$ defined, over $K=\mathbb{F}_2$, by $v^2+vh(u)=f(u)$. Then $f(0)=1$ and $f(1)=0$. Moreover, the value of v^2+uv is given by the following table.

$v \setminus u$	0	1
0	0	0
1	1	0

So, the finite points verifying $v^2 + uv = f(u)$ are $(0,1)$, $(1,0)$ and $(1,1)$.

Now, the derivatives of $v^2 + uv = f(u)$ are u and $v + u^2$. And the only solution of the system $\begin{cases} u & = & 0 \\ v + u^2 & = & 0 \end{cases}$ is $u = v = 0$. But $(0,0)$ does not belong to C. So C is a hyperelliptic curve of genus $g = 2$ and its points over K are $(0,1)$, $(1,0)$, $(1,1)$ and ∞. In particular, note that $(1,0)$ and $(1,1)$ are conjugate, and that $(0,1)$ is special.

Moreover note that the only irreducible quadratic in $\mathbb{Z}_2[u]$ is $a(u) = u^2 + u + 1$, and that $b(u) = u \ mod \ a(u)$ and $b(u) = 0 \ mod \ a(u)$ are the two solutions of $v^2 + vh(u) - f(u) \equiv 0 \ mod \ a(u)$. Hence, the divisors $D_1 = div(\varphi(\langle a(u), u - \overline{v} \rangle_A))$ and $\widetilde{D_1} = div(\varphi(\langle a(u), -\overline{v} \rangle_A))$ both belong to $\mathbb{J}(K)$.

Thus, the reduced elements $\mathbb{J}(K)$ are listed below:

0	$(0,1) - \infty$	$(1,0) - \infty$	$(1,1) - \infty$
$2(0,1) - 2\infty = 0$	$2(1,0) - 2\infty$	$2(1,1) - 2\infty$	$(0,1) + (1,0) - 2\infty$
$(0,1) + (1,1) - 2\infty$	$(1,0) + (1,1) - 2\infty = 0$	D_1	$\widetilde{D_1}$

So $\mathbb{J}(K)$ is an Abelian group consisting of 10 distinct elements. Consequently, $\mathbb{J}(K)$ is isomorphic to either $C_2 \times C_5$ or C_{10}. In order to determine the structure of $\mathbb{J}(K)$, let us first present the reduced elements of $\mathbb{J}(K)$ and their corresponding ideals in $\varphi(B_K)$.

Divisor	Ideal	Divisor	Ideal
0	$\langle 1, -\overline{v} \rangle$	$2(1,1) - 2\infty$	$\langle u^2 + 1, u - \overline{v} \rangle$
$(0,1) - \infty$	$\langle u, 1 - \overline{v} \rangle$	$(0,1) + (1,0) - 2\infty$	$\langle u^2 + u, u + 1 - \overline{v} \rangle$
$(1,0) - \infty$	$\langle u + 1, -\overline{v} \rangle$	$(0,1) + (1,1) - 2\infty$	$\langle u^2 + u, 1 - \overline{v} \rangle$
$(1,1) - \infty$	$\langle u + 1, 1 - \overline{v} \rangle$	D_1	$\langle u^2 + u + 1, u - \overline{v} \rangle$
$2(1,0) - 2\infty$	$\langle u^2 + 1, -\overline{v} \rangle$	$\widetilde{D_1}$	$\langle u^2 + u + 1, -\overline{v} \rangle$

Now, computation using Theorem 3.4.2 shows that the group generated by the element $D = (1,1) - \infty$ of $\mathbb{J}(K)$ is the following:

D	$(1,1) - \infty$	$6D$	$(0,1) + (1,1) - 2\infty$
$2D$	$2(1,1) - 2\infty$	$7D$	D_1
$3D$	$\widetilde{D_1}$	$8D$	$2(1,0) - 2\infty$
$4D$	$(0,1) + (1,0) - 2\infty$	$9D$	$(1,0) - \infty$
$5D$	$(0,1) - \infty$	$10D$	0

So $\mathbb{J}(K)$ is isomorphic to the cyclic group of order 10 and D is a generator of $\mathbb{J}(K)$.

4.4.4 Illustration of Divisor Compression

In order to illustrate divisor compression, we consider the group $\mathbb{J}(K)$ defined in the previous section and the divisor

$$6D = div(\varphi(\langle u^2 + u, 1 - \overline{v}\rangle_A)).$$

- Step 1: Since $a(u) = u^2 + u$, then $p_1(u) = u$ and $p_2(u) = u + 1$.
- Step 2:
  - $i = 1$: Since $s_1(u) = 1 \ mod \ u = 1$, then $\widetilde{s_1}(u) = s_1(u) + h(u) \ mod \ u = u + 1 \ mod \ u = 1$. So $s_1(u) \leq \widetilde{s_1}(u)$ and, hence, $\beta_1 = 1$.
  - $i = 2$: Since $s_2(u) = 1 \ mod \ u+1 = 1$, then $\widetilde{s_2}(u) = s_2(u)+h(u) \ mod \ u+1 = u + 1 \ mod \ u + 1 = 0$. So $s_2(u) > \widetilde{s_2}(u)$ and, hence, $\beta_2 = 0$.

  Output: $\{u, u + 1 : [10]\}$.

4.4.5 Illustration of ElGamal Encryption

Let us now illustrate how a member A (of a community using the ElGamal cryptosystem) can send a message m to another member B.

As underlying structure, we consider the cyclic group $\mathbb{J}(K)$ defined in section 4.4.3.

- Key Generation for B:
  - Private Key: the integer 3 is randomly selected.
  - Public Key: $(D\ ,\ \widetilde{D_1}\ ,\ v^2+uv=u^5+u^3+u^2+1, \mathbb{F}_2\ )$ is generated.

    Note that $\widetilde{D_1}=3D$.
- Encryption of m by A:
  - B's public key is obtained.
  - It is assumed that m is encoded onto $\mathbb{J}(K)$ as

$$D_m = 6D = (0,1)+(1,1)-2\infty.$$

  - The integer 5 is randomly selected.
  - The following divisors are computed

$$\gamma = 5D = (0,1)-\infty,$$

    and

$$\delta = D_m - 5(\widetilde{D_1}) = (6+5*3)D \equiv D = (1,1)-\infty.$$

    Result: The following ciphertext is sent to B:

$$c = (\ (0,1)-\infty\ ,\ (1,1)-\infty\ ).$$

- Decryption of c by B:
  - Using the private key 3. the following divisor is computed

$$-3\gamma = -(3 * 5)D \equiv 5D = (0, 1) - \infty.$$

  - Then. using -3γ. the divisor D_m is recovered as follows:

$$-3\gamma + \delta = (-3 * 5 + 21)D = 6D = (0, 1) + (1, 1) - 2\infty = D_m.$$

  - Finally. D_m is decoded into m.

4.5 Future Work

- *Hyperelliptic Discrete Logarithm Problem (HCDLP)*:

  The algorithms for solving the HCDLP (particularly the recent ones of A. Enge[1] and P. Gaudry[13]) should be carefully studied for potential improvements.

- *Group Structure of Hyperelliptic Jacobians*:

  For encryption schemes such as ElGamal's, cyclic subgroups of the Jacobian are used. The density of these subgroups in any (or even certain types of) hyperelliptic Jacobians ought to receive more attention. Further work also needs to be done in the development of algorithms which give the group structure of a hyperelliptic Jacobian; such algorithms would indeed be useful in the computation of the order a hyperelliptic Jacobian and, hence, in the choice of hyperelliptic curves suitable for cryptography.

- *Message Encoding*:

  As hinted at in remark 4.2.1, research should be carried in the encoding of messages into cyclic subgroups of hyperelliptic Jacobians. Moreover, it would be important to develop encoding schemes that use an optimal number of points on any given hyperelliptic curve.

- *Computation in Hyperelliptic Jacobians*:

  In terms of implementation, work should be done on the choice of hyperelliptic curves that speed up the additive law of the corresponding Jacobians. For this purpose, a precise complexity analysis of the addition in the Jacobian (c.f

[2]) will be of a major importance. Moreover, a complete implementation of a hyperelliptic curve cryptosystem would reveal the exact location of computational bottlenecks, thereby giving rise to specific research on computational refinements. Finally, an alternative representation of divisors should be explored, in the hope of finding a more efficient way to compute in the Jacobian. Such improvements would have major repercussions on the use of hyperelliptic cryptosystems, especially when computation is to be carried on small electronic devices such as smart cards.

Bibliography

[1] A. Enge. *Computing Discrete Logarithms in High-Genus Hyperelliptic Jacobians in Provably Subexponential Time.* www.cacr.math.uwaterloo.ca/techreports/1999/corr99-04.ps (1999).

[2] ———. *The extended Euclidean algorithm on polynomials, and the computational efficiency of hyperelliptic cryptosystems.* Designs, Codes and Cryptography **23** (2001), 53–74.

[3] A. J. Menezes, Y.-H. Wu, R. J. Zuccherato. *An elementary introduction to hyperelliptic curves.* www.cacr.math.uwaterloo.ca/techreports/1997/corr96-19.ps (1996).

[4] D. G. Cantor. *Computing in the Jacobian of a Hyperelliptic Curve,* Mathematics of Computation **48, Issue 177** (1987), 95–101.

[5] F. Hess, G. Seroussi, N. Smart. *Two Topics in Hyperelliptic Cryptography.* www.hpl.hp.com/techreports/2000/HPL-2000-118.pdf (2000).

[6] G. Frey, H.-G. Rück. *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves.* Mathematics of Computation **62** (1994), 865–874.

[7] H.-G. Rück. *On the discrete logarithm problem in the divisor class group of curves.* Preprint (1997).

[8] I. Martin Isaacs. *Algebra. A Graduate Course*, Brooks/Cole Publishing Company. Pacific Grove. CA 93950. 1994.

[9] M. Adleman. J. DeMarrais. M.-D. Huang. *A Subexponential Algorithm for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields.* Lecture Notes in Computer Science **877** (1994). 28–40.

[10] N. G. Smart. *On the performance of Hyperelliptic Cryptosystems.* HP Technical Reports **HP-98-162** (1998).

[11] N. Koblitz. *Hyperelliptic Cryptosystems.* Journal of Cryptology **1** (1989). 139–150.

[12] Neal Koblitz. *A Course in Number Theory and Cryptography.* Springer-Verlag. New York. 1994.

[13] P. Gaudry. *Computing Discrete Logarithms in High-Genus Hyperelliptic Jacobians in Provably Subexponential Time.* Advances in Cryptology. Eurocrypt'2000. Springer-Verlag.LNCS **1807** (2000). 19–34.

[14] P. Samuel. *Théorie algébrique des nombres.* Hermann. Éditeur des sciences et des arts. 293 rue Lecourbe. 75015 Paris. 1971.

[15] R. Flassenberg and S. Paulus. *Sieving in function fields.* Preprint **1997**.

[16] S. Lang. *Algebra.* Addison-Wesley Publishing Company. U.S.A.. 1993.

[17] S. Paulus. *An algorithm of sub-exponential type computing the class group of quadratic orders over principal ideal domains.* ANTS-2: Algorithmic Number Theory. Editor H. Cohen. Springer-Verlag. LNCS **1122** (1996). 243–257.