ISSN 1343-9499

TOHOKU
MATHEMATICAL
PUBLICATIONS

Number 30

Computing in the Jacobian of a C_{34} curve

by

Soondug Kim

August 2004

Sendai 980-8578, Japan

This series aims to publish material related to the activities of the Mathematical Institute of Tohoku University. This may include:

1. Theses submitted to the Institute by grantees of the degree of Doctor of Science.
2. Proceedings of symposia as well as lecture notes of the Institute.

A primary advantage of the series lies in quick and timely publication. Consequently, some of the material published here may very likely appear elsewhere in final form.

Tohoku Mathematical Publications

Mathematical Institute
Tohoku University
Sendai 980-8578, Japan

TOHOKU
MATHEMATICAL
PUBLICATIONS

Number 30

Computing in the Jacobian of a C_{34} curve

by

Soondug Kim

August 2004

Sendai 980-8578, Japan

Computing in the Jacobian of a C_{34} curve

A thesis presented

by

Soondug Kim

to

The Mathematical Institute

for the degree of

Doctor of Science

Tohoku University

Sendai, Japan

September 2003

Contents

Introduction

In recent years, certain algebraic curves have been drawing much attention for their applications to cryptography ([14], [15], [22]).

To make good use of algebraic curves in cryptography, we need a fast algorithm on addition in their Jacobians. In elliptic curve cryptosystems, a point of their Jacobians can be uniquely represented by a point of the corresponding curve. The problem of solving the discrete logarithm problem for elliptic curves has proven difficult, and therefore elliptic curve cryptosystems have substantial potential for high-security public key schemes of relatively small block size.

As for general algebraic curves of genus greater than 1, hyperelliptic curves provide more secure sources. In hyperelliptic curve cryptosystems, a point of the Jacobian can be uniquely represented by Mumford's form, and the known algorithms to compute in the Jacobian utilize Mumford's form ([3], [9], [10]). It is interesting to study cryptography systems obtained from non-hyperelliptic algebraic curves. Since any algebraic curve of genus 2 is a hyperelliptic curve, and since the cryptography system obtained from an algebraic curve of genus > 3 suffers attacks, we study non-hyperelliptic curves of genus 3 in this thesis. The main difficulty in studying them is in the fact that points on their Jacobians can not be represented by Mumford's forms.

As an important family of algebraic curves, S. Miura ([23]) found a family of algebraic curves, called C_{ab} curves, including elliptic and hyperelliptic curves in the development of algebraic geometry codes, and subsequently S. Arita provided an algorithm on addition in the Jacobian of a C_{ab} curve ([2]).

To be more precise, let K be a perfect field. For relatively prime positive integers a and b, a C_{ab} curve defined over K is a nonsingular plane algebraic curve defined by

$F(X,Y)=0$, where $F(X,Y)$ has the form

$$F(X,Y)=\alpha_{0,a}Y^a+\alpha_{b,0}X^b+\sum_{ai+bj<ab}\alpha_{i,j}X^iY^j\in K[X,Y]$$

with nonzero $\alpha_{0,a},\alpha_{b,0}$. For a C_{ab} curve C, it is known that: (i) the defining polynomial $F(X,Y)$ is absolutely irreducible; (ii) the genus of C is equal to $(a-1)(b-1)/2$; (iii) there exists exactly one rational place at infinity, which is denoted by ∞; (iv) the pole divisors of X and Y are $a\cdot\infty$ and $b\cdot\infty$, respectively; (v) the Jacobian $J_K(C)$ is isomorphic to the ideal class group of the affine coordinate ring $R_K(C)$ with the isomorphism Φ defined as $\Phi([E-n\cdot\infty])=[L(\infty\cdot\infty-E)]$ for any effective divisor E of degree n, where $L(\infty\cdot\infty):=\bigcup_{i=1}^{\infty}L(i\cdot\infty)$. Furthermore, S. Arita defined the notion of normal divisors and proved that every point of the Jacobian is uniquely represented by a normal divisor ([2]).

The genus of a C_{34} curve is 3, which is the smallest genus of non-elliptic, non-hyperelliptic C_{ab} curves. For this reason, we are primarily concerned with C_{34} curves in this thesis. Especially, we study the addition in the Jacobian of a C_{34} curve. In this thesis, we express a normal divisor by the reduced Groebner basis with respect to the C_{ab} order for the corresponding ideal of $K[X,Y]$, which is called a normal ideal. We give a condition of a polynomial subset to be the reduced Groebner basis for a normal ideal. Furthermore, we give an explicit expression of such basis. The main results of this thesis are the followings: (i) For a given normal divisor, we give explicitely the inverse normal divisor D', which is the unique normal divisor D' such that $D+D'$ is linearly equivalent to 0; (ii) For any two normal divisors D_1,D_2, we calculate the normal divisor D such that D is linearly equivalent to D_1+D_2.

This thesis is organized as follows. Let K be a perfect field. In Chapter 1, we summarize relevant known facts on the Jacobian of an algebraic curve and linear systems

$$L(D)=\{f\in K(C)^*\mid (f)+D\geq 0\}\cup\{0\}.$$

We denote by I_D the ideal $L(\infty\cdot\infty-D^+)$ of $R_K(C)$ for a divisor D of the form $D=D^+-n\cdot\infty\in \mathrm{Div}_K^0(C)$, where D^+ denotes the zero divisor of D. We write $D\sim D'$ if two divisors D and D' are linearly equivalent.

In Chapter 2, we recall basic facts on Groebner bases in a polynomial ring $K[X_1, \ldots, X_n]$. A *monomial order* on $K[X_1, \ldots, X_n]$ is a relation $>$ on $\mathbf{Z}_{\geq 0}^n$, or equivalently, a relation on the set of monomials $X^\alpha = \prod_{i=1}^n {X_i}^{\alpha_i}, \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}_{\geq 0}^n$, satisfying

(i) $>$ is a total order on $\mathbf{Z}_{\geq 0}^n$ and $\alpha \geq 0$ for any $\alpha \in \mathbf{Z}_{\geq 0}^n$, and

(ii) if $\alpha > \beta$, then $\alpha + \gamma > \beta + \gamma$ for any $\gamma \in \mathbf{Z}_{\geq 0}^n$.

We denote by $\mathrm{LC}(f)$, $\mathrm{LM}(f)$ and $\mathrm{LT}(f)$ the leading coefficient, the leading monomial and the leading term of a polynomial f, respectively. For an ideal I of $K[X_1, \ldots, X_n]$, we define $\delta(I)$ to be the number of monomials which are not contained in $\mathrm{LM}(I)$. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subset K[X_1, \ldots, X_n]$ is called a *Groebner basis* if it satisfies

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

In particular, a Groebner basis satisfying

(i) $\mathrm{LC}(g) = 1$ for all $g \in G$, and

(ii) for $g \in G$, any term of g is not in $\langle \mathrm{LT}(G - \{g\}) \rangle$

is called a *reduced Groebner basis*. It is known that every ideal of $K[X_1, \ldots, X_n]$ has a *unique* reduced Groebner basis. We quote several criterions determining whether or not a given generating subset is a Groebner basis by using S-polynomials.

In Chapter 3, we introduce the theory of C_{ab} curves. In Section 3.1, we recall some basic properties of C_{ab} curves. In Section 3.2, for a C_{ab} curve C, we define the notion of semi-normal divisors and normal divisors as follows.

Definition 0.0.1 Let $g(C)$ be the genus of C. Then a divisor D on C of the form $D = E - n \cdot \infty$ with an effective divisor E of degree n and prime to ∞ is called a *semi-normal divisor* if n satisfies $0 \leq n \leq g(C)$. Furthermore, a semi-normal divisor $D = E - n \cdot \infty$ is called a *normal divisor* if n is minimal in the set of n' of the semi-normal divisors $E' - n' \cdot \infty$ with $D \sim E' - n' \cdot \infty$.

We show that every divisor $D \in \mathrm{Div}_K^0(C)$ has a unique normal divisor D' such that $D' \sim D$ (cf. Proposition 3.2.2).

Next, we introduce the notion of C_{ab} orders on $K[X, Y]$.

Definition 0.0.2 (C_{ab} order) Let a and b be relatively prime positive integers with

$a < b$. For $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbf{Z}^2_{\geq 0}$, we write $\alpha > \beta$ if

$$a\alpha_1 + b\alpha_2 > a\beta_1 + b\beta_2, \quad \text{or} \quad a\alpha_1 + b\alpha_2 = a\beta_1 + b\beta_2 \text{ and } \alpha_1 < \beta_1.$$

It is easily seen that this monomial order corresponds to the pole degrees of functions in $R_K(C)$. In this thesis, we only use this order.

Let φ be the homomorphism such that $\varphi(f(X,Y)) = f(X,Y) \bmod F(X,Y)$. For a normal divisor D, we call an ideal in $K[X,Y]$ of the form $\varphi^{-1}(I_D)$ a *normal ideal*.

We quote from [2] a proposition which plays a vital roll in this thesis.

Proposition 0.0.3 *For a divisor $D = E - n \cdot \infty \in \mathrm{Div}^0_K(C)$ with an effective divisor E prime to ∞, we have*

$$\deg E = \delta(I),$$

where I is the ideal $\varphi^{-1}(I_D)$ of $K[X,Y]$.

In Section 3.3, we introduce the algorithms due to S. Arita (i) for computing the normal divisor equivalent to a given divisor of the form $D = D^+ - n \cdot \infty \in \mathrm{Div}^0_K(C)$, and (ii) for computing the normal divisor equivalent to the sum of normal divisors. Furthermore, we prove the following proposition.

Proposition 0.0.4 *For a divisor $D \in \mathrm{Div}^0_K(C)$ of the form $D = D^+ - n \cdot \infty$, let G be the reduced Groebner basis for $I = \varphi^{-1}(I_D) \subset K[X,Y]$, and let $g_1(X,Y) \in G$ be the polynomial satisfying $\mathrm{LM}(g_1(X,Y)) = \min(\mathrm{LM}(G) - \{Y^a\})$. Then $D' = -D + (\varphi(g_1(X,Y)))$ is the normal divisor such that $D' \sim -D$.*

The main results of this thesis are given in Chapter 4. Throughout Chapter 4, we assume that C is a C_{34} curve defined by $F(X,Y) = 0$, where $F(X,Y)$ has the form

$$F(X,Y) = Y^3 + \gamma_2(X)Y + \gamma_3(X)$$

with $\gamma_2(X) = s_2X^2 + s_1X + s_0, \gamma_3(X) = X^4 + t_3X^3 + t_2X^2 + t_1X + t_0 \in K[X]$. In Section 4.1, we give a condition for a semi-normal divisor to be a normal divisor in the C_{34} curve C:

Theorem 0.0.5 *Let $D \in \mathrm{Div}_K^0(C)$ be a semi-normal divisor and let $n = \deg D^+$. Then D is a normal divisor if and only if either*

(i) $0 \leq n \leq 2$, *or*

(ii) $n = 3$ *and I_D contains no function of the form $X + a$ or $Y + bX + c$ for $a, b, c \in K$.*

In Section 4.2, we give a condition of a polynomial subset to be the reduced Groebner basis for a normal ideal of C (cf. Theorem 4.2.2). Furthermore, we give an explicit expression of the reduced Groebner basis for the normal ideal $\varphi^{-1}(I_D)$ when a normal divisor D has the form $\sum P_i - n \cdot \infty$ with $P_i = (x_i, y_i) \in C$ (cf. Theorem 4.2.3). In Section 4.3, for any normal divisor D, we give the reduced Groebner basis for $\varphi^{-1}(I_{D'})$, where D' is the normal divisor such that $D' \sim -D$ (cf. Theorem 4.3.1). We prove it by using the fact that, if $g_1(X, Y) \in \varphi^{-1}(I_D)$ has the smallest leading monomial in the reduced Groebner basis for $\varphi^{-1}(I_D)$, then we have $D' = -D + (\varphi(g_1(X, Y)))$, and $g_1(X, Y) \in \varphi^{-1}(I_{D'})$ has the smallest leading monomial in the reduced Groebner basis for $\varphi^{-1}(I_{D'})$. In Section 4.4, we study the sum of normal divisors. In general, many S-operators are needed to construct the normal divisor D that is linearly equivalent to $D_1 + D_2$ from normal divisors D_1, D_2. We discuss which S-operators are really needed to construct D.

In Appendix, we present an alternative way to compute the sum $D_1 + D_2$ for normal divisors D_1, D_2 of a C_{34} curve except the case of $D_1 = D_2 = D$ with $\deg D^+ = 3$. Also, we give a method to compute the sum $D_1 + D_2$ for the general case.

Throughout this thesis, K denotes a perfect field and $\overline{K}$ denotes the algebraic closure of K.

Acknowledgment

I wish to express my sincere gratitude to my thesis advisor Professor Yasuo Morita for his endless help and encouragement in various aspects. I am indebted to the members of the Mathematical Institute of Tohoku University for making my mathematical experience so fruitful. I also wish to thank all my colleagues for making my campus life invaluably enjoyable.

Chapter 1

Algebraic curves

We review the Jacobian group of algebraic curves and the Riemann-Roch Theorem. Standard references are [6], [33] and [35].

1.1 Jacobian of an algebraic curve

Let C be a plane curve defined over K and let $K(C)$ denote the function field of C. Then the divisor group $\mathrm{Div}(C)$ of C is defined to be the free abelian group generated by the points of C. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum

$$D = \sum_{P \in C} n_P P$$

with $n_P \in \mathbf{Z}$ and $n_P = 0$ for all but a finite number of $P \in C$. The degree of a divisor $D = \sum_{P \in C} n_P P$ is defined by $\deg D = \sum_{P \in C} n_P$. The divisors of degree 0 form a subgroup

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \mid \deg D = 0\}$$

of $\mathrm{Div}(C)$. Let the Galois group $G_{\overline{K}/K}$ act on $\mathrm{Div}(C)$ as $D^\sigma = \sum_{P \in C} n_P P^\sigma$. Then D is defined over K if and only if $D^\sigma = D$ for all $\sigma \in G_{\overline{K}/K}$. We denote by $\mathrm{Div}_K(C)$ the group of divisors defined over K and put $\mathrm{Div}^0_K(C) = \mathrm{Div}^0(C) \cap \mathrm{Div}_K(C)$.

For $f \in \overline{K}(C)^*$, we can associate to f the divisor $(f) \in \mathrm{Div}^0(C)$ given by

$$(f) = \sum_{P \in C} \mathrm{ord}_P(f) P,$$

where $\mathrm{ord}_P(f)$ denotes the order of f at $P \in C$. A divisor $D \in \mathrm{Div}(C)$ is principal if it has the form $D = (f)$ for some $f \in \overline{K}(C)^*$. The set of principal divisors of C forms

a subgroup of $\mathrm{Div}^0(C)$. Two divisors D_1 and D_2 are linearly equivalent if $D_1 - D_2$ is principal, and it is denoted as $D_1 \sim D_2$.

Definition 1.1.1 Let C be an algebraic curve defined over K. The *Jacobian group of* C, denoted $J(C)$, is the quotient group of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors. The invariant subgroup $J_K(C)$ of $J(C)$ under the action of $G_{\overline{K}/K}$ is called the *Jacobian group of* C *defined over* K.

1.2 Vector space $L(D)$

Let C be a plane curve defined over K, and $K(C)$ be the function field of C. A divisor $D = \sum_{P \in C} n_P P$ is said to be effective (or positive) if each $n_P \geq 0$. We write

$$\sum_{P \in C} n_P P \geq \sum_{P \in C} m_P P$$

if $n_P \geq m_P$ holds for any P. For a divisor $D = \sum_{P \in C} n_P P$, effective divisors defined by

$$D^+ = \sum_{n_P > 0} n_P P \quad \text{and} \quad D^- = \sum_{n_P < 0} (-n_P) P$$

are the zero divisor and the pole divisor of D, respectively. Therefore every divisor D can be expressed as $D = D^+ - D^-$.

Definition 1.2.1 For a divisor D defined over K, we set

$$L(D) := \{f \in K(C)^* \mid (f) \geq -D\} \cup \{0\}.$$

For any divisor $D \in \mathrm{Div}_K(C)$, the space $L(D)$ is a finite dimensional vector space over K. We denote by $l(D)$ the dimension $\dim_K L(D)$. Then the following hold.

(a) For every divisor D' which is linearly equivalent to D, we have an isomorphism $L(D) \simeq L(D')$, and hence $l(D) = l(D')$.

(b) If D_1 and D_2 satisfy $D_1 \leq D_2$, then $L(D_1) \subset L(D_2)$ and $l(D_1) \leq l(D_2)$.

(c) If $\deg D = 0$, then $l(D) = 1$ if and only if D is a principal divisor.

Now, we quote the following theorem without proof.

Theorem 1.2.2 (Riemann-Roch Theorem) *For any divisor $D \in \mathrm{Div}_K(C)$, we have*

$$l(D) = \deg D + 1 - g(C) + l(\mathbf{K} - D),$$

where $g(C)$ is the genus of C and $\mathbf{K}$ is a canonical divisor on C.

Chapter 2

Groebner bases

We recall basic results on Groebner bases, which play an important role throughout this thesis. A standard reference is [5]. By making use of Groebner bases, we study the ideal description problem and the ideal membership problem in a polynomial ring.

2.1 Monomial orders and Groebner bases

We recall the definition of Groebner bases. For a field K, let $K[X_1, \ldots, X_n]$ denote the polynomial ring with coefficients in K.

Definition 2.1.1 A *monomial order* on $K[X_1, \ldots, X_n]$ is a relation $>$ on $\mathbf{Z}_{\geq 0}^n$, or equivalently, a relation on the set of monomials $X^\alpha = \prod_{i=1}^n {X_i}^{\alpha_i}, \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}_{\geq 0}^n$, satisfying:

(i) $>$ is a total order on $\mathbf{Z}_{\geq 0}^n$ and $\alpha \geq 0$ for any $\alpha \in \mathbf{Z}_{\geq 0}^n$.

(ii) If $\alpha > \beta$, then $\alpha + \gamma > \beta + \gamma$ for any $\gamma \in \mathbf{Z}_{\geq 0}^n$.

For a fixed monomial order, the multidegree $\mathrm{MD}(f)$ of a polynomial $f = \sum_\alpha a_\alpha X^\alpha$ is

$$\max\{\alpha \in \mathbf{Z}_{\geq 0}^n \mid a_\alpha \neq 0\},$$

where the maximum is taken with respect to the monomial order. In addition, we denote by $\mathrm{LC}(f), \mathrm{LM}(f)$ and $\mathrm{LT}(f)$ the leading coefficient, the leading monomial and the leading term of a polynomial f with respect to the monomial order, respectively. For a nonempty polynomial set $G \subset K[X_1, \ldots, X_n]$, we denote by $\mathrm{LT}(G)$ and $\mathrm{LM}(G)$ the set of leading terms and the set of leading monomials of elements of G, respectively.

Definition 2.1.2 Fix a monomial order on $K[X_1, \ldots, X_n]$. Then a finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subset K[X_1, \ldots, X_n]$ is called a *Groebner basis* if it satisfies

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

In particular, a Groebner basis satisfying

(i) $\mathrm{LC}(g) = 1$ for all $g \in G$, and

(ii) for $g \in G$, any term of g is not in $\langle \mathrm{LT}(G - \{g\}) \rangle$

is called a *reduced Groebner basis*.

In this thesis, we will mainly use Groebner bases to study the following ideal description problem and the membership problem:

(a) The Ideal Description Problem: For a given ideal $I \subset K[X_1, \ldots, X_n]$, find a finite set of generators of I.

(b) The Ideal Membership Problem: For a given $f \in K[X_1, \ldots, X_n]$ and an ideal $I = \langle g_1, \ldots, g_s \rangle$ of $K[X_1, \ldots, X_n]$, determine whether or not $f \in I$.

Now, we recall the following.

Theorem 2.1.3 *Fix a monomial order on $K[X_1, \ldots, X_n]$. Then any Groebner basis for an ideal I generates I. Furthermore, every ideal $I \neq \{0\}$ has a unique reduced Groebner basis.*

2.2 Properties of Groebner bases

We quote, without proofs, basic results on the problem determining whether or not a given generating subset is a Groebner basis.

On division by Groebner bases, we have the following.

Proposition 2.2.1 *Let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis for an ideal I of $K[X_1, \ldots, X_n]$ and let $f \in K[X_1, \ldots, X_n]$. Then either $r = 0$, or there is a unique $r \in K[X_1, \ldots, X_n]$ with the following properties*:

(i) *No term of r is divisible by any of* $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t)$.

(ii) *There is* $g \in I$ *such that* $f = g + r$.

In particular, r *is the remainder on division of* f *by* G *no matter how the elements of* G *are listed in the division algorithm.*

We use $\overline{f}^G$ for the remainder on division of f by the ordered set G.

Corollary 2.2.2 *Let* $G = \{g_1, \ldots, g_t\}$ *be a Groebner basis for an ideal* I *of* $K[X_1, \ldots, X_n]$ *and let* $f \in K[X_1, \ldots, X_n]$. *Then* $f \in I$ *if and only if the remainder* $\overline{f}^G$ *on division of* f *by* G *is zero.*

From now on, we consider the problem of determining whether or not a given generating subset is a Groebner basis. Here, we need the notion of an S-polynomial.

Definition 2.2.3 Let $f, g \in K[X_1, \ldots, X_n]$ be nonzero polynomials. The *S-polynomial* of f and g is the polynomial defined by

$$S(f, g) = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g)) \left(\frac{f}{\mathrm{LT}(f)} - \frac{g}{\mathrm{LT}(g)} \right),$$

where lcm denotes the least common multiple.

The following theorem, called Buchberger's S-pair criterion, is one of the key results about Groebner bases.

Theorem 2.2.4 *Let* I *be an ideal of* $K[X_1, \ldots, X_n]$. *Then a finite generating subset* G *for* I *is a Groebner basis for* I *if and only if for all pairs* $g_i \neq g_j$ *of* G, *the remainder* $\overline{S(g_i, g_j)}^G$ *on division of* $S(g_i, g_j)$ *by* G *is zero.*

Definition 2.2.5 Fix a monomial order and let $G = \{g_1, \ldots, g_t\} \subset K[X_1, \ldots, X_n]$. Given $f \in K[X_1, \ldots, X_n]$, we say that f *reduces to zero modulo* G, which is denoted as

$$f \to_G 0,$$

if f can be written in the form $f = q_1 g_1 + \cdots + q_t g_t$ such that whenever $q_i g_i \neq 0$, we have $\mathrm{MD}(f) \geq \mathrm{MD}(q_i g_i)$.

We have the following criterion:

Theorem 2.2.6 *A generating subset $G = \{g_1, \ldots, g_t\}$ for an ideal I is a Groebner basis if and only if $S(g_i, g_j) \to_G 0$ for all $i \neq j$.*

For $f, g \in G \subset K[X_1, \ldots, X_n]$, we have $S(f, g) \to_G 0$ if

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

Let $G = (g_1, \ldots, g_t)$ be an ordered set of polynomials and fix $f \in K[X_1, \ldots, X_n]$. Then, it is easily seen that $\overline{f}^G = 0$ implies $f \to_G 0$, though the converse is false in general.

Before closing this section, we recall the following.

Lemma 2.2.7 *Let $G_1 = \{f_i \mid i = 1, \ldots, m\}$ be a Groebner basis for an ideal I, and let $G_2 = \{g_j \mid j = 1, \ldots, n\}$ be a Groebner basis for an ideal J in $K[X_1, \ldots, X_n]$. Then*

$$S(f_i g_j, f_i g_{j'}) = \frac{f_i}{\mathrm{LC}(f_i)}\ S(g_j, g_{j'}) \longrightarrow_G 0,$$

where $G = \{f_i g_j \mid f_i \in G_1, g_j \in G_2\}$.

Chapter 3

C_{ab} curves

In this chapter, we introduce the notion of C_{ab} curves which constitute a wide class of algebraic curves including elliptic curves, hyperelliptic curves and superelliptic curves ([2], [7], [18], [23], [29]).

3.1 Definition and properties of C_{ab} curves

We introduce the definition and basic properties of C_{ab} curves.

Definition 3.1.1 Let a and b be relatively prime positive integers. Then a C_{ab} *curve* defined over K is a nonsingular plane curve defined by $F(X,Y)=0$, where $F(X,Y)$ has the form

$$F(X,Y)=\alpha_{0,a}Y^a+\alpha_{b,0}X^b+\sum_{ai+bj<ab}\alpha_{i,j}X^iY^j\in K[X,Y]$$

for nonzero $\alpha_{0,a},\alpha_{b,0}\in K$.

Since $\gcd(a,b)=1$, we have $m,n\in\mathbf{Z}$ such that $am+bn=1$. Then, multiplying $F(X,Y)$ by $\alpha_{0,a}^{(a-1)bm}\alpha_{b,0}^{-am}$ and replacing X and Y by $\alpha_{0,a}^{-(a-1)n}\alpha_{b,0}^{-n}X$ and $\alpha_{0,a}^{-(m+bn)}\alpha_{b,0}^{m}Y$, respectively, we have a simplified equation $F_1(X,Y)=0$, where

$$F_1(X,Y):=Y^a+X^b+\sum_{ai+bj<ab}\beta_{i,j}X^iY^j\in K[X,Y].$$

Here, we quote the following proposition without proof.

Proposition 3.1.2 *Let C be a C_{ab} curve defined over K. Then we have the following*:

(a) *C is an absolutely irreducible algebraic curve.*

(b) *There exists exactly one K-rational place ∞ at infinity, which implies that the degree of ∞ is 1. Furthermore, the pole divisors of X and Y are $a \cdot \infty$ and $b \cdot \infty$, respectively.*

Let $R_K(C)$ denote the plane coordinate ring of C. Then we have:

Proposition 3.1.3 *Let C be a C_{ab} curve defined by $F(X,Y) = 0$ with $F(X,Y) \in K[X,Y]$. Then the following hold.*

(a) *$\{X^iY^j \bmod F(X,Y) \mid 0 \leq i, 0 \leq j \leq a-1\}$ is a K-basis of $R_K(C)$ and elements in this basis have pairwise distinct valuation at infinity.*

(b) *$R_K(C) = L(\infty \cdot \infty) := \bigcup_{i=1}^{\infty} L(i \cdot \infty)$.*

(c) *For $m \in \mathbf{Z}_{\geq 0}$, $\{X^iY^j \bmod F(X,Y) \mid 0 \leq i, 0 \leq j \leq a-1, ai+bj \leq m\}$ is a basis of a vector space $L(m \cdot \infty)$ over K.*

Proof. This proposition can be proved easily because C is a nonsingular curve given by the irreducible polynomial $F(X,Y)$ for $\gcd(a,b) = 1$, and the valuation of X^iY^j at infinity is $-(ai+bj)$ for all $0 \leq i, 0 \leq j \leq a-1$. □

3.2 Jacobian of a C_{ab} curve

We investigate representations of the Jacobian of a C_{ab} curve. Let C denote a C_{ab} curve defined by $F(X,Y) = 0$ with $F(X,Y) \in K[X,Y]$. Then the genus of C is $(a-1)(b-1)/2$.

Definition 3.2.1 Let $g(C)$ be the genus of C. Then a divisor D on C of the form $D = E - n \cdot \infty$ with an effective divisor E of degree n and prime to ∞ is called a *semi − normal divisor* if n satisfies $0 \leq n \leq g(C)$. Furthermore, a semi-normal divisor $D = E - n \cdot \infty$ is called a *normal divisor* if n is minimal in the set of n' of the semi-normal divisors $E' - n' \cdot \infty$ with $D \sim E' - n' \cdot \infty$.

It should be remarked that a semi-normal divisor may be linearly equivalent to another semi-normal divisor. However, for normal divisors, we have the following.

Proposition 3.2.2 *Every divisor $D \in \mathrm{Div}_K^0(C)$ has a unique normal divisor D' such that $D \sim D'$.*

Proof. For a principal divisor D, we have a unique normal divisor $D' = 0 - 0 \cdot \infty$ which is linearly equivalent to D.

Now, assume that D is not a principal divisor. For the sequence of divisors

$$D \leq D + \infty \leq \cdots \leq D + n \cdot \infty \leq D + (n+1) \cdot \infty \leq \cdots,$$

we have an ascending sequence

$$0 = l(D) \leq l(D + \infty) \leq \cdots \leq l(D + n \cdot \infty) \leq l(D + (n+1) \cdot \infty) \leq \cdots.$$

Consider the difference

$$l(D + (n+1) \cdot \infty) - l(D + n \cdot \infty).$$

Then the Riemann-Roch Theorem shows that this difference is equal to

$$(n+1) + 1 - g(C) + l(\mathbf{K} - D - (n+1) \cdot \infty) - (n + 1 - g(C) + l(\mathbf{K} - D - n \cdot \infty)),$$

where $g(C)$ is the genus of C and $\mathbf{K}$ is a canonical divisor on C. Hence the difference is equal to

$$1 + l(\mathbf{K} - D - (n+1) \cdot \infty) - l(\mathbf{K} - D - n \cdot \infty),$$

which implies that the difference is 0 or 1.

Let m be the smallest positive integer such that $l(D + m \cdot \infty) = 1$ and let f be a nonzero function $f \in L(D + m \cdot \infty)$. Then we have $0 < m \leq g(C)$, since

$$l(D + g(C) \cdot \infty) = g(C) + 1 - g(C) + l(\mathbf{K} - D - g(C) \cdot \infty) \geq 1.$$

For an effective divisor $E = (f) + D + m \cdot \infty \geq 0$, we have a semi-normal divisor $D' = E - m \cdot \infty$ which is linearly equivalent to D. Furthermore, we contend that this semi-normal divisor D' is a normal divisor. Let $E' - m' \cdot \infty$ with $E' \geq 0$ be a semi-normal divisor linearly equivalent to D. Then $E' - m' \cdot \infty = D + (g)$ for a nonzero function g. Since $g \in L(D + m' \cdot \infty) \neq \{0\}$, we have $m' \geq m$. The uniqueness of D' follows from $l(D + m \cdot \infty) = 1$. □

For a C_{ab} curve C, its coordinate ring $R_K(C)$ is a Dedekind domain because C is a nonsingular curve. Further, the Jacobian group $J_K(C)$ is isomorphic to the ideal class

group $H(R_K(C))$ of $R_K(C)$ by the isomorphism

$$\begin{array}{rccl} \Phi & : & J_K(C) & \longrightarrow & H(R_K(C)) \\ & & [E - \deg E \cdot \infty] & \longmapsto & [L(\infty \cdot \infty - E)], \end{array}$$

where, for any class $[D]$ in $J_K(C)$, we choose an effective divisor E which satisfying $D \sim E - \deg E \cdot \infty$. For a divisor $D \in \mathrm{Div}_K^0(C)$ of the form $D = D^+ - n \cdot \infty$ with $n = \deg D^+$, we denote by I_D the ideal $L(\infty \cdot \infty - D^+)$ of $R_K(C)$.

Next, we consider the homomorphism

$$\begin{array}{rccl} \varphi & : & K[X,Y] & \longrightarrow & R_K(C) \\ & & f(X,Y) & \longmapsto & f(X,Y) \bmod F(X,Y). \end{array}$$

It is well-known that every ideal I of $R_K(C)$ has a one-to-one correspondence with an ideal $\varphi^{-1}(I)$ of $K[X,Y]$ containing $\ker\varphi = \langle F(X,Y)\rangle$. Further, each ideal $\varphi^{-1}(I)$ of $K[X,Y]$ can be uniquely represented by a reduced Groebner basis with respect to a monomial order. For a normal divisor $D \in \mathrm{Div}_K^0(C)$, we call the ideal $\varphi^{-1}(I_D)$ of $K[X,Y]$ a normal ideal of C.

Now, we introduce the C_{ab} order, a monomial order which is of great significance in C_{ab} curves.

Definition 3.2.3 (C_{ab} order) Let a and b be relatively prime positive integers with $a < b$. For $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbf{Z}_{\geq 0}^2$, we write $\alpha > \beta$ if

$$a\alpha_1 + b\alpha_2 > a\beta_1 + b\beta_2, \quad \text{or} \quad a\alpha_1 + b\alpha_2 = a\beta_1 + b\beta_2 \text{ and } \alpha_1 < \beta_1.$$

It is easily seen that this monomial order corresponds to pole degrees of functions in $R_K(C)$. From now on, we only use this order.

Let J be an ideal of $R_K(C)$. Then we have the following:

(a) If $G_1 = \{g_1, \ldots, g_t\}$ generates J, then $\{f_1(X,Y), \ldots, f_t(X,Y), F(X,Y)\}$ generates the ideal $\varphi^{-1}(J)$ of $K[X,Y]$, where $f_i(X,Y) \in \varphi^{-1}(g_i)$ for all i.

(b) If a subset G_2 of $K[X,Y]$ generates $\varphi^{-1}(J)$, then $\varphi(G_2)$ generates J.

For an ideal I of $K[X,Y]$, we define the set $\Delta(I)$ as

$$\Delta(I) = \{(i,j) \in \mathbf{Z}_{\geq 0}^2 \mid X^iY^j \notin \mathrm{LT}(I)\} \text{ or equivalently, } \{X^iY^i \mid (i,j) \in \Delta(I)\}.$$

Let $\delta(I)$ denote the number of elements in $\Delta(I)$. On the other hand, for a polynomial subset $G = \{g_1, \ldots, g_m\}$, we define $\Delta(G)$ to be

$$\Delta(G) = (\mathbf{Z}^2_{\geq 0} - \cup_{i=1}^{m}(\mathrm{MD}(g_i) + \mathbf{Z}^2_{\geq 0})) \text{ or equivalently, } \{X^iY^j \mid (i,j) \in \Delta(G)\},$$

and denote by $\delta(G)$ the number of elements in $\Delta(G)$, where MD denotes the multidegree. Then for a subset $G = \{g_1, \ldots, g_t\}$ of an ideal I satisfying $\delta(I) < \infty$, we have that G is a Groebner basis for I if and only if $\delta(I) = \delta(G)$.

Now, we prove the following.

Proposition 3.2.4 *If $D = E - n \cdot \infty \in \mathrm{Div}^0_K(C)$ is a divisor with an effective divisor E prime to ∞, then*

$$\deg E = \delta(I),$$

where I is the ideal $\varphi^{-1}(I_D)$ of $K[X,Y]$.

Proof. Since the equation to be proved remains unchanged under base field extensions, we can assume that the definition field K is algebraically closed. For a polynomial ideal I of $K[X,Y]$, it is known that $K[X,Y]/I$ is isomorphic to $\mathrm{Span}(\Delta(I))$ as a K-vector space. For an effective divisor $E = \sum n_P P$, the ideal $L(\infty \cdot \infty - E)$ of $R_K(C)$ is $\prod_P M_P^{n_P}$, where M_P is the maximal ideal at P. Thus, we have

$$\begin{aligned}
\delta(I) &= \dim_K K[X,Y]/\varphi^{-1}(L(\infty \cdot \infty - E)) \\
&= \dim_K R_K(C)/L(\infty \cdot \infty - E) \\
&= \dim_K R_K(C)/\prod {M_P}^{n_P} \\
&= \textstyle\sum n_P \dim_K R_K(C)/M_P \\
&= \textstyle\sum n_P \\
&= \deg E.
\end{aligned}$$

□

3.3 Arita's algorithms

We introduce the algorithms due to S. Arita ([2]) on the normal divisors of a C_{ab} curve C.

For a nonzero function $g \in R_K(C)$, we denote by $\tilde{g}(X,Y)$ the polynomial in $\varphi^{-1}(g)$, which has the form

$$\tilde{g}(X,Y) = \sum_{0 \le i,\ 0 \le j \le a-1} k_{i,j} X^i Y^j$$

for $k_{i,j} \in K$. Let $\mathrm{LM}(\tilde{g}(X,Y)) = X^{\alpha_1} Y^{\alpha_2}$. Then $\deg(g)^+ = a\alpha_1 + b\alpha_2$. For a polynomial $q(X,Y) \in K[X,Y]$,

$$\mathrm{LM}(\tilde{g}(X,Y) + q(X,Y)F(X,Y)) = \max(\mathrm{LM}(\tilde{g}(X,Y)), \mathrm{LM}(q(X,Y)F(X,Y))),$$

because $\mathrm{LM}(\tilde{g}(X,Y)) \neq \mathrm{LM}(q(X,Y)F(X,Y))$. Thus, $\mathrm{LM}(\tilde{g}(X,Y)) = \min \mathrm{LM}(\varphi^{-1}(g))$.

Proposition 3.3.1 *For a divisor $D \in \mathrm{Div}_K^0(C)$ of the form $D = D^+ - n \cdot \infty$, let G be the reduced Groebner basis for $I = \varphi^{-1}(I_D) \subset K[X,Y]$, and let $g_1(X,Y) \in G$ be the polynomial satisfying $\mathrm{LM}(g_1(X,Y)) = \min(\mathrm{LM}(G) - \{Y^a\})$. Then $D' = -D + (\varphi(g_1(X,Y)))$ is the normal divisor such that $D' \sim -D$.*

Proof. As shown in Proposition 3.2.2, $D' = -D + (f)$ for a nonzero $f \in L(m \cdot \infty - D)$ with the smallest integer m such that $l(m \cdot \infty - D) = 1$. It follows that $(f)^+ \ge D^+$ and $(f)^- = (m+n) \cdot \infty$. If g is a nonzero function in I_D, then there is an integer $m' \ge m$ such that $g \in L(m' \cdot \infty - D) - L((m'-1) \cdot \infty - D)$. It follows that $(g)^+ \ge D^+$ and $(g)^- = (m'+n) \cdot \infty$. Thus $\deg(g)^- = m' + n \ge m + n$. Therefore, f is a nonzero function such that $(f)^+ \ge D^+$ with the smallest pole degree, which implies that

$$\mathrm{LM}(\tilde{f}(X,Y)) = \min \mathrm{LM}(I \setminus \ker \varphi).$$

If $g(X,Y) \in I \setminus \ker \varphi$ satisfies $\mathrm{LM}(g(X,Y)) = \min \mathrm{LM}(I \setminus \ker \varphi)$, then $\mathrm{LM}(g(X,Y)) = \mathrm{LM}(\tilde{f}(X,Y))$. It then follows that

$$g(X,Y) - \frac{\mathrm{LC}(g(X,Y))}{\mathrm{LC}(\tilde{f}(X,Y))} \tilde{f}(X,Y)$$

is an element of I, whose leading monomial is smaller than $\min \mathrm{LM}(I \setminus \ker \varphi)$. Thus

$$g(X,Y) - \frac{\mathrm{LC}(g(X,Y))}{\mathrm{LC}(\tilde{f}(X,Y))} \tilde{f}(X,Y) \in \ker \varphi.$$

Since $(\varphi(\tilde{f}(X,Y))) = (f)$, we have $(\varphi(g(X,Y))) = (f)$, from which follows that $D' = -D + (\varphi(g(X,Y)))$. Furthermore, since $\min \mathrm{LM}(I \setminus \ker \varphi) = \min(\mathrm{LM}(G) - \{Y^a\})$, we

have $D' = -D + (\varphi(g_1(X,Y)))$ for the polynomial $g_1(X,Y) \in G$ with the smallest leading monomial but Y^a. $\square$

Let $D \in \mathrm{Div}_K^0(C)$ be a divisor of the form $D = D^+ - n\cdot\infty$, and let the reduced Groebner basis for $\varphi^{-1}(I_D)$ be $G = \{f_1(X,Y), \ldots, f_t(X,Y)\}$. Let D_0 be the normal divisor such that $D_0 \sim D$, and D' the normal divisor such that $D' \sim -D$. For a polynomial $f(X,Y)$, we denote by f the function $\varphi(f(X,Y))$. Let $f_1(X,Y)$ be the polynomial with the smallest leading monomial but Y^a in G. Then, $D' = -D + (f_1)$ and $\deg(D')^+ = \deg(f_1)^+ - n$. For $g(X,Y) \in \varphi^{-1}(I_{D'})$, we have

$$\begin{aligned}
g \in I_{D'} &\iff (g)^+ \geq (D')^+ = -D^+ + (f_1)^+ \\
&\iff (g)^+ + D^+ \geq (f_1)^+ \\
&\iff (g)^+ + (f_i)^+ \geq (f_1)^+ \quad \text{for all } f_i(X,Y) \in G \\
&\iff (gf_i)^+ \geq (f_1)^+ \quad \text{for all } f_i(X,Y) \in G \\
&\iff gf_i \in L(\infty\cdot\infty - (f_1)^+) \quad \text{for all } f_i(X,Y) \in G \\
&\iff gf_i \in \langle f_1 \rangle \quad \text{for all } f_i(X,Y) \in G \\
&\iff \varphi^{-1}(gf_i) \subset \varphi^{-1}(\langle f_1 \rangle) = \langle f_1(X,Y), F(X,Y) \rangle \quad \text{for all } f_i(X,Y) \in G \\
&\iff g(X,Y)f_i(X,Y) \in \langle f_1(X,Y), F(X,Y) \rangle \quad \text{for all } f_i(X,Y) \in G.
\end{aligned}$$

It follows that the normal ideal $I' = \varphi^{-1}(I_{D'})$ is

$$\{g(X,Y) \mid g(X,Y)f_i(X,Y) \in \langle f_1(X,Y), F(X,Y) \rangle \text{ for all } f_i(X,Y) \in G\}.$$

Let $g_1(X,Y)$ be a polynomial with the smallest leading monomial in $I' \setminus \ker\varphi$. Then $D_0 = -D' + (g_1)$. Let I_0 be the normal ideal $\varphi^{-1}(I_{D_0})$. If $h \in I_{D_0}$, then

$$(h)^+ \geq (D_0)^+ = -(D')^+ + (g_1)^+ = D^+ - (f_1)^+ + (g_1)^+.$$

If $g_1(X,Y)f_i(X,Y) \in \langle f_1(X,Y), F(X,Y) \rangle$ is written as

$$g_1(X,Y)f_i(X,Y) = q_{i,1}(X,Y)f_1(X,Y) + q_{i,2}(X,Y)F(X,Y)$$

for $q_{i,1}(X,Y), q_{i,2}(X,Y) \in K[X,Y]$, then $q_{i,1}(X,Y) \in I_0$.

Conversely, if $f(X,Y) \in I_0$, then $(f)^+ \geq D_0^+$. It follows that

$$\begin{aligned}
(f)^+ &\geq D^+ - (f_1)^+ + (g_1)^+ \\
&= \min\{(f_i)^+ - (f_1)^+ + (g_1)^+ \mid i = 1, \ldots, t\} \\
&= \min\{(q_{i,1})^+ \mid i = 1, \ldots, t\}.
\end{aligned}$$

It implies that $f \in \langle q_{1,1}, \ldots, q_{t,1} \rangle$. Thus

$$f(X,Y) \in \langle q_{1,1}(X,Y), \ldots, q_{t,1}(X,Y), F(X,Y) \rangle.$$

As a result,

$$I_0 = \langle q_{1,1}(X,Y), \ldots, q_{t,1}(X,Y), F(X,Y) \rangle.$$

Now, we introduce the following algorithms given by S. Arita.

Algorithm 1:

Input : A divisor $D = E - n \cdot \infty \in \mathrm{Div}_K^0(C)$ with an effective divisor E prime to ∞.

Output : A normal divisor D' which is linearly equivalent to $-D$.

Step 1. Find a nonzero function $f \in R_K(C)$ satisfying $(f)^+ \geq E$ with the smallest pole degree.

Step 2. Put $D' \leftarrow -D + (f)$.

Algorithm 2:

Input : Normal divisors $D_1 = E_1 - n_1 \cdot \infty$ and $D_2 = E_2 - n_2 \cdot \infty$.

Output : A normal divisor $D = E - n \cdot \infty$ which is linearly equivalent to $D_1 + D_2$.

Step 1. By applying Algorithm 1 to $D_1 + D_2 = (E_1 + E_2) - (n_1 + n_2) \cdot \infty$, get a normal divisor $D' = E' - n' \cdot \infty$ which is linearly equivalent to $-(D_1 + D_2)$.

Step 2. By applying Algorithm 1 to a normal divisor $D' = E' - n' \cdot \infty$, get a normal divisor $D = E - n \cdot \infty$ which is linearly equivalent to $D_1 + D_2$, and output D.

Chapter 4

C_{34} curves

In this chapter, we consider C_{34} curves. Throughout this chapter, let C be a C_{34} curve defined by

$$F(X, Y) := Y^3 + \gamma_2(X)Y + \gamma_3(X) = 0$$

with $\gamma_2(X) = s_2X^2 + s_1X + s_0, \gamma_3(X) = X^4 + t_3X^3 + t_2X^2 + t_1X + t_0 \in K[X]$. Then the genus of C is equal to 3. In this chapter, we use the notation defined in Chapter 3 with the C_{ab} order.

4.1 Normal divisors

We give a condition for a semi-normal divisor to be a normal divisor of C. The pole divisors of X and Y in $R_K(C)$ are $3 \cdot \infty$ and $4 \cdot \infty$, respectively. It follows that:

Lemma 4.1.1 *Let a, b, c be elements of K. Then the principal divisor $(X + a)$ can be written as $(X + a) = P_1 + P_2 + P_3 - 3 \cdot \infty$ with $P_1, P_2, P_3 \in C$, and the principal divisor $(Y + bX + c)$ can be written as $(Y + bX + c) = Q_1 + Q_2 + Q_3 + Q_4 - 4 \cdot \infty$ with $Q_1, Q_2, Q_3, Q_4 \in C$.*

The following theorem gives a condition for a semi-normal divisor $D \in \mathrm{Div}_K^0(C)$ to be a normal divisor.

Theorem 4.1.2 *Let $D \in \mathrm{Div}_K^0(C)$ be a semi-normal divisor and let $n = \deg D^+$. Then D is a normal divisor if and only if either*

(i) $0 \leq n \leq 2$, *or*

(ii) $n = 3$ *and* I_D *contains no function of the form* $X + a$ *or* $Y + bX + c$ *for* $a, b, c \in K$.

Proof. The semi-normal divisor D is a normal divisor if and only if D is not linearly equivalent to any semi-normal divisor with a pole degree which is smaller than n.

If $n = 0$, then $D = 0$ is a normal divisor.

If $n = 1$ and D is not a normal divisor, then $D \sim 0$. It follows that $D = (f)$ for some $f \in K(C)^*$. Then f is in $L(1 \cdot \infty) - L(0 \cdot \infty)$. But it is a contradiction because $L(1 \cdot \infty) - L(0 \cdot \infty) = \emptyset$ by Proposition 3.1.3.

If $n = 2$ and D is not a normal divisor, then $D \sim 0$ or $D \sim P - \infty$ for a point $P \in C$. First, it is impossible that $D \sim 0$, since $L(2 \cdot \infty) - L(1 \cdot \infty) = \emptyset$. Second, suppose that $D \sim P - \infty$ for $P = (x, y) \in C$. Then $D - P + \infty = (f)$ for some $f \in K(C)^*$. We have $f \cdot (X - x) \in L(4 \cdot \infty) - L(3 \cdot \infty)$ since $(f) + (X - x) = D^+ + P_2 + P_3 - 4 \cdot \infty$ for $P_2, P_3 \in C$ such that $(X - x) = P + P_2 + P_3 - 3 \cdot \infty$. This implies that $(f \cdot (X - x)) = (Y + bX + c)$ for $b, c \in K$. Thus, we have $Y + bX + c, X - x \in L(\infty \cdot \infty - (P_2 + P_3))$. It is a contradiction because there is only one line through with P_1 and P_2, which is the tangent line if $P_1 = P_2$.

If $n = 3$ and D is not a normal divisor, then $D \sim 0$, $D \sim P - \infty$, or $D \sim Q_1 + Q_2 - 2 \cdot \infty$ for $P, Q_1, Q_2 \in C$. First, suppose that $D \sim 0$. Then $D = (f)$ for some $f \in K(C)^*$. It follows that $f \in L(3 \cdot \infty) - L(2 \cdot \infty)$. This implies that $(f) = (X + a)$, i.e. $X + a \in I_D$, for $a \in K$. Second, suppose that $D \sim P - \infty$. Then $D - P + \infty = (f)$ for some $f \in K(C)^*$. For $P = (x, y) \in C$, $(f) + (X - x) = D^+ + P_2 + P_3 - 5 \cdot \infty$ for $P_2, P_3 \in C$ such that $(X - x) = P + P_2 + P_3 - 3 \cdot \infty$. It follows that $f \cdot (X - x) \in L(5 \cdot \infty) - L(4 \cdot \infty) = \emptyset$, which is a contradiction. Last, suppose that $D \sim Q_1 + Q_2 - 2 \cdot \infty$. Then $D - Q_1 - Q_2 + 2 \cdot \infty = (f)$ for some $f \in K(C)^*$. Let g be the defining equation of the line through with Q_1 and Q_2, which is the tangent line if $Q_1 = Q_2$. Then either $g = X + a$ for $a \in K$ or $g = Y + bX + c$ for $b, c \in K$. For $g = Y + bX + c$, we can write $(g) = Q_1 + Q_2 + Q_3 + Q_4 - 4 \cdot \infty$ for $Q_3, Q_4 \in C$. Then $(fg) = D^+ + Q_3 + Q_4 - 5 \cdot \infty$, which is a contradiction since $L(5 \cdot \infty) - L(4 \cdot \infty) = \emptyset$. Thus $g = X + a$. Let $(g) = Q_1 + Q_2 + Q_5 - 3 \cdot \infty$ for $Q_5 \in C$. Then $(fg) = D^+ + Q_5 - 4 \cdot \infty$. It follows that $fg \in L(4 \cdot \infty) - L(3 \cdot \infty)$. Thus $(fg) = (Y + b'X + c')$, i.e. $Y + b'X + c' \in I_D$, for $b', c' \in K$. Therefore, we proved that if D is not a normal divisor, there is a function $f \in I_D$ of the form $X + a$ or $Y + bX + c$ for $a, b, c \in K$.

Conversely, if $n = 3$ and there is a function $f = X + a \in I_D$ for $a \in K$. Then we have $(f)^+ = D^+$, since $(f)^+ \geq D^+$ with $\deg(f)^+ = \deg D^+$. It implies that $(f) = D$, and $D \sim 0$. Thus D is not a normal divisor. If $n = 3$ and there is a function $f = Y + bX + c \in I_D$ for $b, c \in K$, then $(f) = D^+ + P - 4 \cdot \infty$ for $P = (x, y) \in C$. It follows that $D-(f)+(X-x) = P_2+P_3-2\cdot\infty$ for $P_2, P_3 \in C$ such that $(X-x) = P+P_2+P_3-3\cdot\infty$. It implies that $D \sim P_2 + P_3 - 2 \cdot \infty$. Thus D is not a normal divisor. □

4.2 A Groebner basis for a normal ideal

We give a condition of an ideal of $K[X, Y]$ to be a normal ideal of C, and a condition of a polynomial subset of $K[X, Y]$ to be a reduced Groebner basis for a normal ideal of C. Furthermore, we give an expression of the reduced Groebner basis for a normal ideal of a normal divisor $D = \sum P_i - n \cdot \infty \in \mathrm{Div}_K^0(C)$.

The following proposition states a condition for an ideal in $K[X, Y]$ to be a normal ideal of C.

Proposition 4.2.1 *Let $I \neq \{0\}$ be an ideal of $K[X, Y]$ and let G be the reduced Groebner basis for I. Then I is a normal ideal of C if and only if G satisfies the following:*

(a) *The remainder $\overline{F}^G$ of $F(X, Y)$ on division by G is 0.*

(b) *Either $0 \leq \delta(G) \leq 2$, or $\delta(G) = 3$ with $\mathrm{LM}(G) = \{X^2, XY, Y^2\}$.*

Proof. Assume that I is a normal ideal of C. Then $I = \varphi^{-1}(I_D)$ for a normal divisor $D \in \mathrm{Div}_K^0(C)$. Thus $F(X, Y) \in \ker(\varphi) \subset I$. It follows that the remainder $\overline{F}^G$ is equal to 0. Furthermore, $\delta(I) = \deg D^+ < \infty$ and $\delta(I) = \delta(G)$. Since D is normal, either $0 \leq \deg D^+ \leq 2$, or $\deg D^+ = 3$ and I_D contains no function of the form $X+a$ or $Y+bX+c$ for $a, b, c \in K$ by Theorem 4.1.2. This implies that either $0 \leq \delta(G) \leq 2$, or $\delta(G) = 3$ and $I = \varphi^{-1}(I_D)$ cannot contain any polynomial $f(X, Y)$ such that $\mathrm{LM}(f(X, Y)) = X$ or Y. Therefore, if $\delta(G) = 3$, then $X, Y \in \Delta(I) = \Delta(G)$, i.e. $\mathrm{LM}(G) = \{X^2, XY, Y^2\}$.

Assume that G satisfies the conditions (a) and (b). Then $F(X, Y) \in I$. Since $\ker(\varphi) = \langle F(X, Y)\rangle \subset I$, we have $I = \varphi^{-1}(\varphi(I))$. Since $\varphi(I)$ is an ideal of $R_K(C)$, we can write $\varphi(I) = L(\infty\cdot\infty - D^+)$ with a divisor $D = D^+ - n\cdot\infty \in \mathrm{Div}_K^0(C)$. Then $\deg D^+ = \delta(I) = \delta(G)$ by Proposition 3.2.4. By the condition (b), either $0 \leq \deg D^+ \leq 2$, or $\deg D^+ = 3$

and $L(\infty \cdot \infty - D^+)$ contains no function of the form $X + a$ or $Y + bX + c$ for $a, b, c \in K$. This implies that D is a normal divisor. Thus I is a normal ideal. $\square$

It follows that a polynomial subset $G \neq \{0\}$ of $K[X, Y]$ is the reduced Groebner basis for a normal ideal of C if and only if G is the reduced Groebner basis satisfying the conditions (a), (b) of Proposition 4.2.1. Thus we have:

Theorem 4.2.2 *Let $G \neq \{0\}$ be a polynomial subset of $K[X, Y]$. Let a_i, b_i, c_i be elements of K. Then G is a reduced Groebner basis for a normal ideal of C if and only if G is one of the following*:

(a) $G = \{1\}$;

(b) $G = \{g_1(X, Y) = X + c_1, g_2(X, Y) = Y + c_2\}$ *and satisfies* $F(-c_1, -c_2) = 0$;

(c) $G = \{g_1(X, Y) = X + c_1, g_2(X, Y) = Y^2 + a_2Y + c_2\}$ *and satisfies* $g_2(X, Y) \mid F(-c_1, Y)$;

(d) $G = \{g_1(X, Y) = Y + b_1X + c_1, g_2(X, Y) = X^2 + b_2X + c_2\}$ *and satisfies* $g_2(X, Y) \mid F(X, -b_1X - c_1)$;

(e) $G = \{g_1(X, Y), g_2(X, Y), g_3(X, Y)\}$ *for*

$$\begin{aligned} g_1(X, Y) &= X^2 + a_1Y + b_1X + c_1, \\ g_2(X, Y) &= XY + a_2Y + b_2X + c_2, \\ g_3(X, Y) &= Y^2 + a_3Y + b_3X + c_3 \end{aligned}$$

satisfying

$$\begin{aligned} c_1 &= -a_2^2 + a_2b_1 - a_1b_2 + a_1a_3, \\ c_2 &= a_2b_2 - a_1b_3, \\ c_3 &= -a_2b_3 - b_2^2 + a_3b_2 + b_1b_3, \end{aligned}$$

and

$$\begin{aligned} a_1 \neq 0 \quad &\Rightarrow \quad g_2(X, f(X)) \mid F(X, f(X)), \\ b_3 \neq 0 \quad &\Rightarrow \quad g_2(g(Y), Y) \mid F(g(Y), Y), \\ a_1 = b_3 = 0 \quad &\Rightarrow \quad g_1(X, Y) \mid F(X, -b_2),\ g_3(X, Y) \mid F(-a_2, Y), \end{aligned}$$

where $f(X) = -a_1^{-1}(X^2 + b_1X + c_1)$ and $g(Y) = -b_3^{-1}(Y^2 + a_3Y + c_3)$.

Proof. Let $\overline{F}^G$ denote the remainder of $F(X, Y)$ on division by G. Then it is enough to find a reduced Groebner basis G such that $\overline{F}^G$ is equal to 0, and $\mathrm{LM}(G)$ is $\{1\}$, $\{X, Y\}$,

$\{X, Y^2\}$, $\{Y, X^2\}$, or $\{X^2, XY, Y^2\}$ by Proposition 4.2.1. We wish to find a condition that $\overline{F}^G = 0$ is satisfied by a reduced Groebner basis G with a set of leading monomials of the above form. Let r_i denote an element of K.

(a) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{1\}$, then $G = \{1\}$.

(b) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{X, Y\}$, then the elements of G are $g_1(X, Y) = X + c_1, g_2(X, Y) = Y + c_2$ for $c_1, c_2 \in K$. For the remainder $\overline{F}^G = r_0 \in K$, we can write

$$F(X, Y) = q_1(X, Y)g_1(X, Y) + q_2(X, Y)g_2(X, Y) + r_0$$

with $q_1(X, Y), q_2(X, Y) \in K[X, Y]$. Thus $\overline{F}^G = 0$ if and only if $F(-c_1, -c_2) = 0$.

(c) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{X, Y^2\}$, then the elements of G are $g_1(X, Y) = X + c_1, g_2(X, Y) = Y^2 + a_2Y + c_2$ for $a_2, c_1, c_2 \in K$. For the remainder $\overline{F}^G = r_1Y + r_0$, we can write

$$F(X, Y) = q_1(X, Y)g_1(X, Y) + q_2(X, Y)g_2(X, Y) + r_1Y + r_0$$

with $q_1(X, Y), q_2(X, Y) \in K[X, Y]$. Since

$$F(-c_1, Y) = q_2(-c_1, Y)g_2(-c_1, Y) + r_1Y + r_0,$$

the remainder of $F(-c_1, Y)$ on division by $g_2(-c_1, Y)$ is $r_1Y + r_0$. Thus $\overline{F}^G = 0$ if and only if $F(-c_1, Y)$ is divisible by $g_2(-c_1, Y) = g_2(X, Y)$.

(d) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{Y, X^2\}$, then the elements of G are $g_1(X, Y) = Y + b_1X + c_1, g_2(X, Y) = X^2 + b_2X + c_2$ for $b_1, b_2, c_1, c_2 \in K$. For the remainder $\overline{F}^G = r_1X + r_0$, we can write

$$F(X, Y) = q_1(X, Y)g_1(X, , Y) + q_2(X, Y)g_2(X, Y) + r_1X + r_0$$

with $q_1(X, Y), q_2(X, Y) \in K[X, Y]$. Since

$$F(X, -b_1X - c_1) = q_2(X, -b_1X - c_1)g_2(X, -b_1X - c_1) + r_1X + r_0,$$

the remainder of $F(X, -b_1X - c_1)$ on division by $g_2(X, -b_1X - c_1)$ is $r_1X + r_0$. Thus $\overline{F}^G = 0$ if and only if $F(X, -b_1X - c_1)$ is divisible by $g_2(X, -b_1X - c_1) = g_2(X, Y)$.

(e) If G is a reduced Groebner basis with $\mathrm{LM}(G) = \{X^2, XY, Y^2\}$, then G has the elements

$$\begin{aligned} g_1(X,Y) &= X^2 + a_1Y + b_1X + c_1, \\ g_2(X,Y) &= XY + a_2Y + b_2X + c_2, \\ g_3(X,Y) &= Y^2 + a_3Y + b_3X + c_3 \end{aligned}$$

with $a_i, b_i, c_i \in K$ for $i = 1, 2, 3$ satisfying that the remainder of $S(g_j(X,Y), g_k(X,Y))$ on division by G is equal to 0 for all $1 \leq j \neq k \leq 3$. It follows that

$$\begin{aligned} c_1 &= -a_2^2 + a_2b_1 - a_1b_2 + a_1a_3, \\ c_2 &= a_2b_2 - a_1b_3, \\ c_3 &= -a_2b_3 - b_2^2 + a_3b_2 + b_1b_3. \end{aligned} \tag{2.1}$$

For the remainder $\overline{F}^G = r_2Y + r_1X + r_0$, we can write

$$\begin{aligned} F(X,Y) = {} & q_1(X,Y)g_1(X,Y) + q_2(X,Y)g_2(X,Y) + q_3(X,Y)g_3(X,Y) \\ & + r_2Y + r_1X + r_0 \end{aligned} \tag{2.2}$$

with $q_1(X,Y), q_2(X,Y), q_3(X,Y) \in K[X,Y]$.

If $a_1 \neq 0$, (2.2) can be written as

$$F(X,Y) = q_1'(X,Y)g_1(X,Y) + q_2'(X,Y)g_2(X,Y) + r_2Y + r_1X + r_0$$

for $q_1'(X,Y) = q_1(X,Y) + a_1^{-1}(Y + b_2)q_3(X,Y), q_2'(X,Y) = q_2(X,Y) - a_1^{-1}(X - a_2 + b_1)q_3(X,Y) \in K[X,Y]$ since

$$g_3(X,Y) = a_1^{-1}(Y + b_2)g_1(X,Y) - a_1^{-1}(X - a_2 + b_1)g_2(X,Y).$$

If we substitute $f(X) = -a_1^{-1}(X^2 + b_1X + c_1)$ for Y, then

$$F(X, f(X)) = q_2'(X, f(X))g_2(X, f(X)) + r_2f(X) + r_1X + r_0.$$

It follows that the remainder of $F(X, f(X))$ on division by $g_2(X, f(X))$ is $r_2f(X) + r_1X + r_0$. Thus $\overline{F}^G = 0$ if and only if $F(X, f(X))$ is divisible by $g_2(X, f(X))$.

If $b_3 \neq 0$, (2.2) can be written as

$$F(X,Y) = q_2''(X,Y)g_2(X,Y) + q_3''(X,Y)g_3(X,Y) + r_2Y + r_1X + r_0$$

for $q_2''(X,Y) = q_2(X,Y) - b_3^{-1}(Y - b_2 + a_3)q_1(X,Y), q_3''(X,Y) = q_3(X,Y) + b_3^{-1}(X + a_2)q_1(X,Y) \in K[X,Y]$ since

$$g_1(X,Y) = -b_3^{-1}(Y - b_2 + a_3)g_2(X,Y) + b_3^{-1}(X + a_2)g_3(X,Y).$$

If we substitute $g(Y) = -b_3^{-1}(Y^2 + a_3Y + c_3)$ for X, then

$$F(g(Y),Y) = q_2''(g(Y),Y)g_2(g(Y),Y) + r_2Y + r_1g(Y) + r_0.$$

It follows that the remainder of $F(g(Y),Y)$ on division by $g_2(g(Y),Y)$ is $r_2Y + r_1g(Y) + r_0$. Thus $\overline{F}^G = 0$ if and only if $F(g(Y),Y)$ is divisible by $g_2(g(Y),Y)$.

If $a_1 = b_3 = 0$, then

$$\begin{aligned} g_1(X,Y) &= (X + a_2)(X - a_2 + b_1), \\ g_2(X,Y) &= (X + a_2)(Y + b_2), \\ g_3(X,Y) &= (Y + b_2)(Y - b_2 + a_3) \end{aligned}$$

by (2.1). Applying them in (2.2), we have

$$F(-a_2,Y) = q_3(-a_2,Y)g_3(-a_2,Y) + r_2Y - a_2r_1 + r_0$$

and

$$F(X,-b_2) = q_1(X,-b_2)g_1(X,-b_2) + r_1X - b_2r_2 + r_0.$$

Thus $\overline{F}^G = 0$ if and only if $g_3(X,Y) \mid F(-a_2,Y)$ and $g_1(X,Y) \mid F(X,-b_2)$. □

Now, we consider an explicit expression of the reduced Groebner basis for a normal ideal of C. The following is on the reduced Groebner basis for a given normal divisor.

Theorem 4.2.3 *Let $D = \sum_{i=1}^n P_i - n \cdot \infty \in \mathrm{Div}_K^0(C)$ be a normal divisor, where $P_i = (x_i, y_i) \in C$ for $i = 1, \ldots, n$. Let*

$$l(X,Y) = \begin{cases} (x_2 - x_1)(Y - y_1) - (y_2 - y_1)(X - x_1) & \text{if } P_1 \neq P_2; \\ F_Y(x,y)(Y - y) + F_X(x,y)(X - x) & \text{if } P_1 = P_2 = (x,y), \end{cases}$$

where F_X (resp. F_Y) denotes the partial derivative of $F(X,Y)$ with respect to X (resp. Y). Let I be the normal ideal $\varphi^{-1}(I_D)$ and let G be the reduced Groebner basis for I. Then G satisfies the following:

(a) *If* $D = 0$, *then* $G = \{1\}$.

(b) *If* $D = P_1 - \infty$, *then* $G = \{X - x_1, Y - y_1\}$.

(c) *If* $D = P_1 + P_2 - 2 \cdot \infty$, *then*

(i) $\mathrm{LM}(l(X,Y)) = X$*:* $G = \{l_m(X,Y), (Y - y_1)(Y - y_2)\}$*;*

(ii) $\mathrm{LM}(l(X,Y)) = Y$*:* $G = \{l_m(X,Y), (X - x_1)(X - x_2)\}$,

where $l_m(X,Y) = \mathrm{LC}(l(X,Y))^{-1} l(X,Y)$.

(d) *If* $D = P_1 + P_2 + P_3 - 3 \cdot \infty$, *then* $G = \{g_1(X,Y), g_2(X,Y), g_3(X,Y)\}$ *with*

$$\begin{aligned} g_1(X,Y) &= (X - x_1)(X - x_2) + k_1 l(X,Y), \\ g_2(X,Y) &= (X - x_1)(Y - y_2) + k_2 l(X,Y), \\ g_3(X,Y) &= (Y - y_1)(Y - y_2) + k_3 l(X,Y) \end{aligned}$$

for

(i) *if* $\sharp\{P_1, P_2, P_3\} = 2$ *or* 3, *then we can assume that* $P_3 \neq P_1, P_2$ *and we have*

$$\begin{aligned} k_1 &= -l(x_3, y_3)^{-1}(x_3 - x_1)(x_3 - x_2), \\ k_2 &= -l(x_3, y_3)^{-1}(x_3 - x_1)(y_3 - y_2), \\ k_3 &= -l(x_3, y_3)^{-1}(y_3 - y_1)(y_3 - y_2); \end{aligned}$$

(ii) *if* $\sharp\{P_1, P_2, P_3\} = 1$ *and* $(x,y) = (x_1, y_1)$, *then we have*

$$\begin{aligned} k_1 &= (S_0^2 T_2 + 3y T_1^2 - S_0 S_1 T_1)^{-1} S_0^2, \\ k_2 &= -(S_0^2 T_2 + 3y T_1^2 - S_0 S_1 T_1)^{-1} S_0 T_1, \\ k_3 &= (S_0^2 T_2 + 3y T_1^2 - S_0 S_1 T_1)^{-1} T_1^2 \end{aligned}$$

for

$$\begin{aligned} S_0 &= 3y^2 + s_2 x^2 + s_1 x + s_0, \\ S_1 &= 2s_2 x + s_1, \\ T_1 &= 2s_2 xy + s_1 y + 4x^3 + 3t_3 x^2 + 2t_2 x + t_1, \\ T_2 &= s_2 y + 6x^2 + 3t_3 x + t_2, \end{aligned}$$

where $\sharp\{P_1, P_2, P_3\}$ *denotes the number of elements in* $\{P_1, P_2, P_3\}$.

Proof. For the reduced Groebner basis G for I, we have $\delta(G) = \delta(I) = n$.

(a) If $D = 0$, then $\delta(G) = 0$. It follows that $\mathrm{LM}(G) = \{1\}$. Thus $G = \{1\}$.

(b) If $D = P_1 - \infty$, then $\delta(G) = 1$. Thus $\mathrm{LM}(G) = \{X, Y\}$ and

$$G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y + c_2\}$$

for $c_1, c_2 \in K$. Since $(g_1)^+, (g_2)^+ \geq P_1$, we have $c_1 = -x_1$, $c_2 = -y_1$.

(c) If $D = P_1 + P_2 - 2 \cdot \infty$, then $\delta(G) = 2$. Thus $\mathrm{LM}(G) = \{X, Y^2\}$ or $\{Y, X^2\}$. For the linear polynomial $l(X, Y)$, we have $l(X, Y) \in I$ and $(X - x_1)(X - x_2), (Y - y_1)(Y - y_2) \in I$. The set $\{l(X, Y), (X - x_1)(X - x_2), (Y - y_1)(Y - y_2)\}$ is a Groebner basis for I since $\delta(\{l(X, Y), (X - x_1)(X - x_2), (Y - y_1)(Y - y_2)\}) = 2$. Thus we have

$$G = \begin{cases} \{l_m(X, Y), (Y - y_1)(Y - y_2)\} & \text{if } \mathrm{LM}(l(X, Y)) = X; \\ \{l_m(X, Y), (X - x_1)(X - x_2)\} & \text{if } \mathrm{LM}(l(X, Y)) = Y. \end{cases}$$

(d) If $P_1 + P_2 + P_3 - 3 \cdot \infty$, then $\delta(G) = 3$. Thus the elements of G are

$$\begin{aligned} g_1(X, Y) &= X^2 + a_1 Y + b_1 X + c_1, \\ g_2(X, Y) &= XY + a_2 Y + b_2 X + c_2, \\ g_3(X, Y) &= Y^2 + a_3 Y + b_3 X + c_3 \end{aligned}$$

for $a_i, b_i, c_i \in K$ $(i = 1, 2, 3)$ by Theorem 4.2.2. Every linear polynomial in $\varphi^{-1}(L(\infty \cdot \infty - (P_1 + P_2)))$ is $kl(X, Y)$ for $k \in K$.

(i) For every $g_i(X, Y) \in G$, we have $g_i(X, Y) \in \varphi^{-1}(L(\infty \cdot \infty - (P_1 + P_2)))$. Since $(X - x_1)(X - x_2), (X - x_1)(Y - y_2), (Y - y_1)(Y - y_2) \in \varphi^{-1}(L(\infty \cdot \infty - (P_1 + P_2)))$, $g_1(X, Y) - (X - x_1)(X - x_2), g_2(X, Y) - (X - x_1)(Y - y_2), g_3(X, Y) - (Y - y_1)(Y - y_2)$ are in $\varphi^{-1}(L(\infty \cdot \infty - (P_1 + P_2)))$ with the leading monomials $\leq Y$. It follows that

$$\begin{aligned} g_1(X, Y) - (X - x_1)(X - x_2) &= k_1 l(X, Y), \\ g_2(X, Y) - (X - x_1)(Y - y_2) &= k_2 l(X, Y), \\ g_3(X, Y) - (Y - y_1)(Y - y_2) &= k_3 l(X, Y) \end{aligned}$$

for $k_1, k_2, k_3 \in K$. Since $g_i(x_3, y_3) = 0$ and $l(x_3, y_3) \neq 0$ by Theorem 4.1.2, we have

$$\begin{aligned} k_1 &= -l(x_3, y_3)^{-1}(x_3 - x_1)(x_3 - x_2), \\ k_2 &= -l(x_3, y_3)^{-1}(x_3 - x_1)(y_3 - y_2), \\ k_3 &= -l(x_3, y_3)^{-1}(y_3 - y_1)(y_3 - y_2). \end{aligned}$$

(ii) Since $P_1 = P_2$, we have

$$\begin{aligned} l(X, Y) &= F_Y(x, y)(Y - y) + F_X(x, y)(X - x) \\ &= S_0(Y - y) + T_1(X - x). \end{aligned}$$

If $F_Y(x,y) = S_0 \neq 0$, then $(l)^+ \geq 2P$ with $\mathrm{LM}(l(X,Y)) = Y$. It follows that $l(X,Y)(X-x), l(X,Y)(Y-y) \in I$ with the leading monomials XY and Y^2, respectively. For a polynomial $F(X,Y) - F_Y(x,y)^{-1}l(X,Y)(Y-y)Y \in I$, the remainder

$$r(X,Y) = S_0^{-2}(S_0^2T_2 + 3yT_1^2 - S_0S_1T_1)(X-x)^2 + l(X,Y)$$

on division by $\{l(X,Y)(X-x), l(X,Y)(Y-y)\}$ is also in I. Since D is a normal divisor, we have $S_0^2T_2 + 3yT_1^2 - S_0S_1T_1 \neq 0$ by Theorem 4.1.2. Thus $\mathrm{LM}(r(X,Y)) = X^2$. It implies that

$$g_1(X,Y) = (X-x)^2 + (S_0^2T_2 + 3yT_1^2 - S_0S_1T_1)^{-1}S_0^2l(X,Y). \tag{2.3}$$

For the monic polynomial $l_m(X,Y) = \mathrm{LC}(l(X,Y))^{-1}l(X,Y)$, we have a Groebner basis

$$\{g_1(X,Y), l_m(X,Y)(X-x), l_m(X,Y)(Y-y)\},$$

whose elements are monoic polynomials, for I. Thus $g_2(X,Y)$ is the remainder on division of $l_m(X,Y)(X-x)$ by $g_1(X,Y)$ and $g_3(X,Y)$ is the remainder of $l_m(X,Y)(Y-y)$ on division by $\{g_1(X,Y), g_2(X,Y)\}$. It follows that

$$\begin{aligned} g_2(X,Y) &= (X-x)(Y-y) - (S_0^2T_2 + 3yT_1^2 - S_0S_1T_1)^{-1}S_0T_1l(X,Y), \\ g_3(X,Y) &= (Y-y)^2 + (S_0^2T_2 + 3yT_1^2 - S_0S_1T_1)^{-1}T_1^2l(X,Y). \end{aligned} \tag{2.4}$$

If $F_Y(x,y) = S_0 = 0$, then $(l)^+ = (X-x)^+ \geq 2P$. It follows that $g_1(X,Y) = (X-x)^2$ and $g_2(X,Y) = (X-x)(Y-y)$. For a polynomial $F(X,Y) - (Y-y)^3 \in I$, the remainder $r(X,Y) = 3y(Y-y)^2 + T_1(X-x)$ on division by $\{g_1(X,Y), g_2(X,Y)\}$ is also in I. Since D is a normal divisor, we have $y \neq 0$ by Theorem 4.1.2. Thus $\mathrm{LM}(r(X,Y)) = Y^2$. It follows that $g_3(X,Y) = (Y-y)^2 + (3y)^{-1}l(X,Y)$. These $g_1(X,Y), g_2(X,Y), g_3(X,Y)$ are the same as (2.3) and (2.4). □

4.3 Inverse of a normal divisor

We give the inverse of normal divisors of C.

Theorem 4.3.1 *Let $D \in \mathrm{Div}_K^0(C)$ be a normal divisor, and let G be the reduced Groebner basis for the normal ideal $\varphi^{-1}(I_D)$. Let D' be the normal divisor such that $D' \sim -D$. Then the reduced Groebner basis G' for the normal ideal $\varphi^{-1}(I_{D'})$ is as follows*:

(a) *If* $G = \{1\}$, *then* $G' = \{1\}$.

(b) *If* $G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y + c_2\}$, *then*
$G' = \{h_1(X,Y) = X + c_1, h_2(X,Y) = Y^2 - c_2 Y + {c_2}^2 + s_2 c_1^2 - s_1 c_1 + s_0\}$.

(c) *If* $G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y^2 + a_2 Y + c_2\}$, *then*
$G' = \{h_1(X,Y) = X + c_1, h_2(X,Y) = Y - a_2\}$.

(d) *If* $G = \{g_1(X,Y) = Y + b_1 X + c_1, g_2(X,Y) = X^2 + b_2 X + c_2\}$, *then*
$G' = \{h_1(X,Y), h_2(X,Y)\}$ *for*

$$\begin{aligned} h_1(X,Y) &= Y + b_1 X + c_1, \\ h_2(X,Y) &= X^2 + (-b_1^3 - b_2 + t_3 - b_1 s_2)X \\ &\quad + b_1^3 b_2 + b_2^2 - 3b_1^2 c_1 - c_2 + t_2 - b_2 t_3 - b_1 s_1 + b_1 b_2 s_2 - c_1 s_2. \end{aligned}$$

(e) *If* $G = \{g_1(X,Y), g_2(X,Y), g_3(X,Y)\}$ *for*

$$\begin{aligned} g_1(X,Y) &= X^2 + a_1 Y + b_1 X + c_1, \\ g_2(X,Y) &= XY + a_2 Y + b_2 X + c_2, \\ g_3(X,Y) &= Y^2 + a_3 Y + b_3 X + c_3, \end{aligned}$$

then $G' = \{h_1(X,Y), h_2(X,Y), h_3(X,Y)\}$ *for*

$$\begin{aligned} h_1(X,Y) &= X^2 + a_1 Y + b_1 X + c_1, \\ h_2(X,Y) &= XY + (-a_2 + b_1)Y + (a_1^2 - a_3 - a_1 s_2)X \\ &\quad - a_1^2 a_2 + a_2 a_3 - a_1^2 b_1 - a_3 b_1 + a_1 b_3 - a_1 s_1 + a_1 a_2 s_2 + a_1^2 t_3, \\ h_3(X,Y) &= Y^2 + (a_1^2 - b_2 - a_1 s_2)Y + (2a_1 b_1 - b_3 + s_1 - b_1 s_2 - a_1 t_3)X \\ &\quad - 2a_1 a_2^2 + 2a_1^2 a_3 + 2a_1 a_2 b_1 - a_1 b_1^2 - 3a_1^2 b_2 + b_2^2 + a_2 b_3 - b_1 b_3 + s_0 + a_2^2 s_2 \\ &\quad - a_1 a_3 s_2 - a_2 b_1 s_2 + 2a_1 b_2 s_2 - a_1 t_2 + a_1 b_1 t_3. \end{aligned}$$

Proof. By Proposition 3.3.1, we have $D' = -D + (\varphi(g(X,Y)))$ for the polynomial $g(X,Y)$ with the smallest leading monomial but Y^3 in G. Since D is a normal divisor, $Y^3 \notin \mathrm{LM}(G)$. It follows that $D' = -D + (\varphi(g_1(X,Y)))$ for the polynomial $g_1(X,Y)$ with the smallest leading monomial in G. Furthermore, we have

$$\varphi^{-1}(I_{D'}) = \{h(X,Y) \mid h(X,Y) g_i(X,Y) \in \langle g_1(X,Y), F(X,Y)\rangle \text{ for all } g_i(X,Y) \in G\}.$$

Thus $g_1(X,Y) \in \varphi^{-1}(I_{D'})$. Since D is a normal divisor such that $D \sim -D'$, $D = -D' + (g')$ for a nonzero function g' with the smallest pole degree in $I_{D'}$. Then $(g') = D + D' = (g_1)$.

This implies that the polynomial $h_1(X,Y)$ with the smallest leading monomial in G' is equal to $g_1(X,Y)$. Futhermore,

$$\delta(G') = \deg(D')^+ = \deg(g_1)^+ - \deg D^+ = \deg(g_1)^+ - \delta(G).$$

(a) If $G = \{g_1(X,Y) = 1\}$, $\delta(G') = 0$. Thus $G' = \{h_1(X,Y) = 1\}$.

(b) If $G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y + c_2\}$, then $\delta(G') = 2$. Since $g_1(X,Y) = X + c_1 \in G'$, we have $\mathrm{LM}(G') = \{X, Y^2\}$. Thus

$$G' = \{h_1(X,Y) = X + c_1, h_2(X,Y) = Y^2 + A_2Y + C_2\}$$

for $A_2, C_2 \in K$ such that $h_2(X,Y)g_i(X,Y) \in \langle g_1(X,Y), F(X,Y)\rangle$ for all $g_i(X,Y) \in G$. We have a Groebner basis $\{g_1(X,Y), F(X,Y)\}$ for $\langle g_1(X,Y), F(X,Y)\rangle$ since

$$\mathrm{lcm}(\mathrm{LM}(g_1(X,Y)), \mathrm{LM}(F(X,Y))) = \mathrm{LM}(g_1(X,Y))\mathrm{LM}(F(X,Y)).$$

It follows that

$$h_2(X,Y)g_2(X,Y) = q_1(X,Y)g_1(X,Y) + q_2(X,Y)F(X,Y)$$

for $q_1(X,Y), q_2(X,Y) \in K[X,Y]$ with $\mathrm{LM}(q_1(X,Y)) \leq X^3$ and $\mathrm{LM}(q_2(X,Y)) \leq 1$. It implies that $A_2 = -c_2, C_2 = {c_2}^2 + s_2c_1^2 - s_1c_1 + s_0$.

(c) If $G = \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y^2 + a_2Y + c_2\}$, then $\delta(G') = 1$. Thus $\mathrm{LM}(G') = \{X, Y\}$ and

$$G' = \{h_1(X,Y) = X + c_1, h_2(X,Y) = Y + C_2\}$$

for $C_2 \in K$ such that $h_2(X,Y)g_i(X,Y) \in \langle g_1(X,Y), F(X,Y)\rangle$ for all $g_i(X,Y) \in G$. It follows that

$$h_2(X,Y)g_2(X,Y) = q_1(X,Y)g_1(X,Y) + q_2(X,Y)F(X,Y)$$

for $q_1(X,Y), q_2(X,Y) \in K[X,Y]$ with $\mathrm{LM}(q_1(X,Y)) \leq X^3, \mathrm{LM}(q_2(X,Y)) \leq 1$ since $\{g_1(X,Y), F(X,Y)\}$ is a Groebner basis for $\langle g_1(X,Y), F(X,Y)\rangle$. It implies that $C_2 = -a_2$.

(d) If $G = \{g_1(X,Y) = Y + b_1X + c_1, g_2(X,Y) = X^2 + b_2X + c_2\}$, then $\delta(G') = 2$. Since $g_1(X,Y) \in G'$, we have $\mathrm{LM}(G') = \{Y, X^2\}$. Thus

$$G' = \{h_1(X,Y) = Y + b_1X + c_1, h_2(X,Y) = X^2 + B_2X + C_2\}$$

for $B_2, C_2 \in K$ such that $h_2(X,Y)g_i(X,Y) \in \langle g_1(X,Y), F(X,Y)\rangle$ for all $g_i(X,Y) \in G$. Let $S(X,Y) = F(X,Y) - Y^2 g_1(X,Y)$. Then $\{g_1(X,Y), S(X,Y)\}$ is a Groebner basis for $\langle g_1(X,Y), F(X,Y)\rangle$ since $\delta(\{g_1(X,Y), S(X,Y)\}) = \deg(g_1)^+$. Thus

$$h_2(X,Y)g_2(X,Y) = q_1(X,Y)g_1(X,Y) + q_2(X,Y)S(X,Y)$$

for $q_1(X,Y), q_2(X,Y) \in K[X,Y]$ with $\mathrm{LM}(q_1(X,Y)) \leq XY$,$\mathrm{LM}(q_2(X,Y)) \leq 1$. It implies that

$$\begin{aligned} B_2 &= -b_1^3 - b_2 + t_3 - b_1 s_2, \\ C_2 &= b_1^3 b_2 + b_2^2 - 3b_1^2 c_1 - c_2 + t_2 - b_2 t_3 - b_1 s_1 + b_1 b_2 s_2 - c_1 s_2. \end{aligned}$$

(e) If $G = \{g_1(X,Y), g_2(X,Y), g_3(X,Y)\}$ for

$$\begin{aligned} g_1(X,Y) &= X^2 + a_1 Y + b_1 X + c_1, \\ g_2(X,Y) &= XY + a_2 Y + b_2 X + c_2, \\ g_3(X,Y) &= Y^2 + a_3 Y + b_3 X + c_3, \end{aligned}$$

then $\delta(G') = 3$ and

$$\begin{aligned} c_1 &= -a_2^2 + a_2 b_1 - a_1 b_2 + a_1 a_3, \\ c_2 &= a_2 b_2 - a_1 b_3, \\ c_3 &= -a_2 b_3 - b_2^2 + a_3 b_2 + b_1 b_3. \end{aligned} \tag{3.1}$$

Since D' is a normal divisor, $\mathrm{LM}(G') = \{X^2, XY, Y^2\}$. Thus the elements of G' are

$$\begin{aligned} h_1(X,Y) &= X^2 + a_1 Y + b_1 X + c_1, \\ h_2(X,Y) &= XY + A_2 Y + B_2 X + C_2, \\ h_3(X,Y) &= Y^2 + A_3 Y + B_3 X + C_3 \end{aligned}$$

for $A_i, B_i, C_i \in K$ such that $h_j(X,Y)g_k(X,Y) \in \langle g_1(X,Y), F(X,Y)\rangle$ for all $j,k = 1,2,3$. Since $\delta(\{g_1(X,Y), F(X,Y)\}) = \deg(g_1)^+$, $\{g_1(X,Y), F(X,Y)\}$ is a Groebner basis for $\langle g_1(X,Y), F(X,Y)\rangle$.

For $h_2(X,Y) \in G'$,

$$h_2(X,Y)g_2(X,Y) = q_{1,1}(X,Y)g_1(X,Y) + q_{1,2}(X,Y)F(X,Y) \tag{3.2}$$

for $q_{1,1}(X,Y), q_{1,2}(X,Y) \in K[X,Y]$ with $\mathrm{LM}(q_{1,1}(X,Y)) \leq Y^2$, $\mathrm{LM}(q_{1,2}(X,Y)) \leq 1$, and

$$h_2(X,Y)g_3(X,Y) = q_{2,1}(X,Y)g_1(X,Y) + q_{2,2}(X,Y)F(X,Y) \tag{3.3}$$

for $q_{2,1}(X,Y), q_{2,2}(X,Y) \in K[X,Y]$ with $\mathrm{LM}(q_{2,1}(X,Y)) \leq X^3$, $\mathrm{LM}(q_{2,2}(X,Y)) \leq X$. Thus, if $a_1 \neq 0$, then

$$\begin{aligned} A_2 &= -a_2 + b_1, \\ B_2 &= a_1^2 - a_3 - a_1 s_2, \\ C_2 &= -a_1^2 a_2 + a_2 a_3 - a_1^2 b_1 - a_3 b_1 + a_1 b_3 - a_1 s_1 + a_1 a_2 s_2 + a_1^2 t_3 \end{aligned} \tag{3.4}$$

by (3.1) and (3.2). And, if $a_1 = 0$, then $A_2 = -a_2 + b_1$, $B_2 = -a_3$, $C_2 = a_2 a_3 - a_3 b_1$ by (3.1), (3.2) and (3.3). These values are the same as those in (3.4) with $a_1 = 0$.

For $h_3(X,Y) \in G'$,

$$h_3(X,Y) g_2(X,Y) = q_{3,1}(X,Y) g_1(X,Y) + q_{3,2}(X,Y) F(X,Y) \tag{3.5}$$

for $q_{3,1}(X,Y), q_{3,2}(X,Y) \in K[X,Y]$ with $\mathrm{LM}(q_{3,1}(X,Y)) \leq X^3$, $\mathrm{LM}(q_{3,2}(X,Y)) \leq X$, and

$$h_3(X,Y) g_3(X,Y) = q_{4,1}(X,Y) g_1(X,Y) + q_{4,2}(X,Y) F(X,Y) \tag{3.6}$$

for $q_{4,1}(X,Y), q_{4,2}(X,Y) \in K[X,Y]$ with $\mathrm{LM}(q_{4,1}(X,Y)) \leq X^2 Y$, $\mathrm{LM}(q_{4,2}(X,Y)) \leq Y$. Thus, if $a_1 \neq 0$, then

$$\begin{aligned} A_3 &= {a_1}^2 - b_2 - a_1 s_2, \\ B_3 &= 2a_1 b_1 - b_3 + s_1 - b_1 s_2 - a_1 t_3, \\ C_3 &= -2a_1 a_2^2 + 2a_1^2 a_3 + 2a_1 a_2 b_1 - a_1 b_1^2 - 3a_1^2 b_2 + b_2^2 + a_2 b_3 - b_1 b_3 \\ &\quad + s_0 + a_2^2 s_2 - a_1 a_3 s_2 - a_2 b_1 s_2 + 2a_1 b_2 s_2 - a_1 t_2 + a_1 b_1 t_3 \end{aligned} \tag{3.7}$$

by (3.1) and (3.5). And, if $a_1 = 0$, then $A_3 = -b_2$, $B_3 = -b_3 + s_1 - b_1 s_2$ and $C_3 = b_2^2 + a_2 b_3 - b_1 b_3 + s_0 + a_2^2 s_2 - a_2 b_1 s_2$ by (3.1), (3.5) and (3.6). These values are the same as those in (3.7) with $a_1 = 0$.

Hence, we completely proved it. □

4.4 Addition of normal divisors

We consider the addition of normal divisors in $\mathrm{Div}_K^0(C)$. Let $D_1 = E_1 - n_1 \cdot \infty$ and $D_2 = E_2 - n_2 \cdot \infty$ be normal divisors of C. Let $D' = E' - n' \cdot \infty$ be a normal divisor such that $D' \sim -(D_1 + D_2)$, and let $D = E - n \cdot \infty$ be a normal divisor such that $D \sim D_1 + D_2$.

From now on, we use the following notation: For $i = 1, 2$,

$$
\begin{aligned}
I_i &: \text{a normal ideal } \varphi^{-1}(L(\infty \cdot \infty - E_i)),\\
I' &: \text{a normal ideal } \varphi^{-1}(L(\infty \cdot \infty - E')),\\
I &: \text{a normal ideal } \varphi^{-1}(L(\infty \cdot \infty - E)),\\
G_i &: \text{ a reduced Groebner basis for } I_i,\\
G_g &: \text{ a set } \{f_i(X,Y)g_j(X,Y), F(X,Y) \mid f_i(X,Y) \in G_1, g_j(X,Y) \in G_2\},\\
G &: \text{ a reduced Groebner basis for } I,\\
H &: \text{ a reduced Groebner basis for } \varphi^{-1}(I_{D_1+D_2}) = \varphi^{-1}(L(\infty \cdot \infty - (E_1 + E_2))),\\
h_1(X,Y) &: \text{ a polynomial with the smallest leading monomial in } H,\\
v_1(X,Y) &: \text{ a monic polynomial with the smallest leading monomial in } I'.
\end{aligned}
$$

The final purpose of this section is to find G for the given G_1 and G_2.

We first study a way of finding the reduced Groebner basis H for $\varphi^{-1}(I_{D_1+D_2})$ by using the fact that G_g is a generating set of $\varphi^{-1}(I_{D_1+D_2})$. We have $\delta(H) = n_1 + n_2$. Thus, if $\delta(G_g) > n_1 + n_2$, then G_g is not a Groebner basis and it is necessary to do division of S-polynomials by the algorithm due to Buchberger. It is possible to omit the following S-polynomials in G_g:

(a) $S(f_i g_j, f_{i'} g_{j'})$ for $f_i, f_{i'} \in G_1$, $g_j, g_{j'} \in G_2$ with $i = i'$ or $j = j'$;

(b) $S(f, g)$ for $f, g \in G_g$ with $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{LM}(f)\mathrm{LM}(g)$;

(c) $S(f, g)$ for $f, g \in G_g$ with $h \neq f, g$ in G_g such that $S(f, h)$ and $S(g, h)$ are divisible by G_g, and $\mathrm{LT}(h)$ divides $\mathrm{lcm}(\mathrm{LT}(f), \mathrm{LT}(g))$.

Let $S = \{S_1, \ldots, S_m\}$ be the set of S-polynomials in G_g except those S-polynomials. For $i = 1, \ldots, m$, let r_i be the remainder of S_i on division by $G_g \cup \{r_1, \ldots, r_{i-1}\}$. Let $G_{g,1} = G_g \cup \{r_1, \ldots, r_m\}$. Then

$$n_1 + n_2 \leq \delta(G_{g,1}) < \delta(G_g).$$

If $n_1 + n_2 < \delta(G_{g,1})$, it is needed to consider S-polynomials in $G_{g,1}$. For every $r_i \neq 0$, it is enough to consider the S-polynomials $S(r_i, f)$ and $S(r_i, g)$, where f (resp. g) is a nearest element to r_i in the lower right-hand (resp. in the upper left-hand) as considering the leading monomials by the above (c). By iterating this work until the value of δ decreases to $n_1 + n_2$, we get a Groebner basis. Thus the number of divisions to be done for getting a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$ is $m + 2(\delta(G_g) - (n_1 + n_2) - 1)$ at most.

Since we have $\delta(H) = n_1 + n_2 \leq 6$, H contains an element whose leading monomial is smaller than Y^3. Thus, $D' = -(D_1 + D_2) + (h_1)$ for the polynomial $h_1(X, Y)$ with the smallest leading monomial in H by Proposition 3.3.1. Furthermore, we have

$$I' = \{v(X, Y) \mid v(X, Y)h_i(X, Y) \in \langle h_1(X, Y), F(X, Y)\rangle \text{ for all } h_i(X, Y) \in H\}$$

as shown in Section 3.3. Since D' is a normal divisor, $D = -D' + (v_1)$ and $v_1(X, Y) \in G$. It follows that

$$D = D_1 + D_2 - (h_1) + (v_1).$$

Thus

$$E = E_1 + E_2 - (h_1)^+ + (v_1)^+$$

because the divisors D, $D_1 + D_2$, (h_1) and (v_1) have no pole point but at infinity. Since $D' = -(D_1 + D_2) + (h_1)$, we have $n' = \deg(h_1)^+ - (n_1 + n_2)$. Thus $\mathrm{LM}(v_1(X, Y))$ is determined if $\deg(h_1)^+ \neq n_1 + n_2 + 2$. If $\deg(h_1)^+ = n_1 + n_2 + 2$, then $\mathrm{LM}(v_1(X, Y))$ is either X or Y. Further, $\mathrm{LM}(v_1(X, Y))$ is determined by $\mathrm{LM}(v_1(X, Y)h_i(X, Y)) \in \mathrm{LM}(\langle h_1(X, Y), F(X, Y)\rangle)$ for all $h_i(X, Y) \in H$. Let $H = \{h_1(X, Y), \ldots, h_t(X, Y)\}$. Then $\mathrm{LM}(G)$ is determined by $\mathrm{LM}(H)$ and G is obtained by a generating set for I, which is given as follows.

Let $q_{i,1}(X, Y), q_{i,2}(X, Y) \in K[X, Y]$ satisfy

$$v_1(X, Y)h_i(X, Y) = q_{i,1}(X, Y)h_1(X, Y) + q_{i,2}(X, Y)F(X, Y).$$

Then

$$(v_1) + (h_i) = (q_{i,1}) + (h_1).$$

It follows that

$$(v_1)^+ + (h_i)^+ = (q_{i,1})^+ + (h_1)^+.$$

Thus

$$(q_{i,1})^+ = (v_1)^+ + (h_i)^+ - (h_1)^+.$$

Since $(h_i)^+ \geq E_1 + E_2$, we have $q_{i,1} \in L(\infty \cdot \infty - E)$. Thus $q_{i,1}(X, Y) \in I$.

If $f(X, Y) \in I$, then $(f)^+ \geq E$. It follows that

$$\begin{aligned}(f)^+ &\geq E_1 + E_2 - (h_1)^+ + (v_1)^+ \\ &= \min\{(h_i)^+ - (h_1)^+ + (v_1)^+ \mid i = 1, \ldots, t\} \\ &= \min\{(q_{i,1})^+ \mid i = 1, \ldots, t\}.\end{aligned}$$

It implies that $f \in \langle q_{1,1}, \ldots, q_{t,1} \rangle$. Thus

$$\begin{aligned} f(X,Y) &\in \varphi^{-1}(\langle q_{1,1}, \ldots, q_{t,1} \rangle) \\ &= \langle q_{1,1}(X,Y), \ldots, q_{t,1}(X,Y), F(X,Y) \rangle. \end{aligned}$$

Hence $I = \langle q_{1,1}(X,Y), \ldots, q_{t,1}(X,Y), F(X,Y) \rangle$.

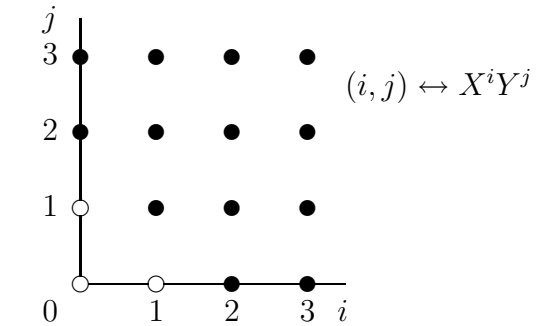
Now, we study the sum $D_1 + D_2$. We assume that coefficients $A_i, B_i, C_i, a_i, b_i, c_i$ of polynomials are elements of K and we assume that S_i, r_i are polynomials in $K[X,Y]$. For a polynomial $f(X,Y)$, we write f instead of $f(X,Y)$.

I. $\mathbf{n_1 = 1, n_2 = 1}$

Since $\deg (D_1 + D_2)^+ = 2$, $D_1 + D_2$ is a normal divisor by Theorem 4.1.2. Thus $D = D_1 + D_2$, and G is equal to H. If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = X + C_1, f_2(X,Y) = Y + C_2\}, \\ G_2 &= \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y + c_2\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$. The point of vacant circle denotes an element in $\Delta(G_g)$, and 'MD $= (i,j) : f(X,Y)$' means $\mathrm{LM}(f(X,Y)) = X^i Y^j$ for a polynomial $f(X,Y) \in G_g$.



$(i,j) \leftrightarrow X^i Y^j$

MD = $(0,3) : F$

$(0,2) : f_2 g_2$

$(1,1) : f_1 g_2, f_2 g_1$

$(2,0) : f_1 g_1$

$\mathrm{LM}(G_g) = \{X^2, XY, Y^2, Y^3\}$

It follows that $S = \{S_1 = S(f_1 g_2, f_2 g_1), S_2 = S(F, f_2 g_2)\}$ with $\deg(G_g) = n_1 + n_2 + 1$. For a nonzero r_i in $\{r_1, r_2\}$, $\mathrm{LM}(r_i)$ is either X or Y. The remainder of S_1 on division by G_g is

$$r_1 = (C_1 - c_1)Y + (-C_2 + c_2)X + C_1 c_2 - C_2 c_1.$$

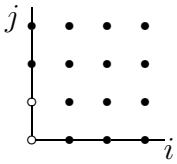
Further, if $r_1 = 0$, i.e. $G_1 = G_2$, the remainder of S_2 on division by G_g is

$$r_2 = F_Y(-C_1, -C_2)(Y + C_2) + F_X(-C_1, -C_2)(X + C_1),$$

where F_X (resp. F_Y) denotes the partial derivative of $F(X, Y)$ with respect to X (resp. Y).

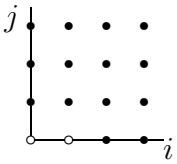
Since $\delta(H) = 2$, we have the following diagrams on $\mathrm{LM}(H) = \mathrm{LM}(G)$.

(1)



$\mathrm{LM}(H) = \mathrm{LM}(G)$
$= \{X, Y^2\}$

(2)



$\mathrm{LM}(H) = \mathrm{LM}(G)$
$= \{Y, X^2\}$

As a result, we have the following:

(i) If $G_1 \neq G_2$ with $C_1 \neq c_1$, then $H = G = \{(C_1 - c_1)^{-1} r_1, f_1 g_1\}$.

(ii) If $G_1 \neq G_2$ with $C_1 = c_1$, then $H = G = \{f_1, f_2 g_2\}$.

(iii) If $G_1 = G_2$ and $F_Y(-C_1, -C_2) \neq 0$, then $H = G = \{F_Y(-C_1, -C_2)^{-1} r_2, f_1 g_1\}$.

(iv) If $G_1 = G_2$ and $F_Y(-C_1, -C_2) = 0$, then $H = G = \{f_1, f_2 g_2\}$.

II. $\mathbf{n_1 = 1, n_2 = 2}$

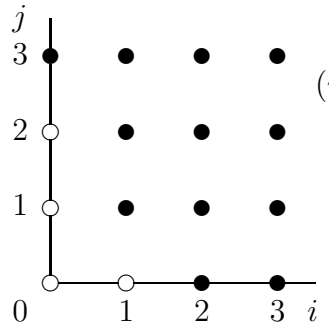
For a normal divisor D_2 of pole degree 2, $\mathrm{LM}(G_2)$ is either $\{X, Y^2\}$ or $\{Y, X^2\}$.

1. $\mathbf{LM(G_2) = \{X, Y^2\}}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X, Y) = X + C_1, f_2(X, Y) = Y + C_2\}, \\ G_2 &= \{g_1(X, Y) = X + c_1, g_2(X, Y) = Y^2 + a_2 Y + c_2\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



$(i,j) \leftrightarrow X^iY^j$

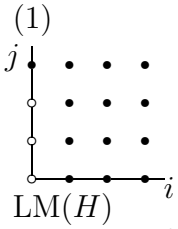
$$\mathrm{MD} = \begin{array}{l} (0,3) : f_2g_2, F \\ (1,2) : f_1g_2 \\ (1,1) : f_2g_1 \\ (2,0) : f_1g_1 \end{array}$$

$\mathrm{LM}(G_g) = \{X^2, XY, XY^2, Y^3\}$

It follows that $S = \{S_1 = S(f_1g_2, f_2g_1), S_2 = S(F, f_2g_2)\}$ with $\delta(G_g) = n_1 + n_2 + 1$. Thus, for $r_i \neq 0$ in $\{r_1, r_2\}$, $\mathrm{LM}(r_i)$ is either X or Y^2. The coefficient of Y^2 in r_1 is $C_1 - c_1$. Further, if $r_1 = 0$, the coefficient of Y^2 in r_2 is $-C_2 - a_2$. It follows that H contains an element whose leading monomial is X if and only if $C_1 = c_1$ and $C_2 = -a_2$.

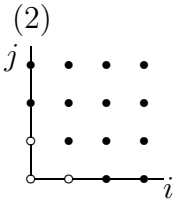
Since $\delta(H) = 3$ with $\Delta(H) \subset \{1, X, Y, Y^2\}$, we have the following diagrams on $\mathrm{LM}(H)$, which are followed by $\mathrm{LM}(G)$.

(1)



$\mathrm{LM}(H) = \{X, Y^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{1\}$

(2)



$\mathrm{LM}(H) = \mathrm{LM}(G) = \{X^2, XY, Y^2\}$

As a result, H and G are as follows:

(i) If $C_1 = c_1$ and $C_2 = -a_2$, then $H = \{f_1, f_2g_2\}$ and $G = \{1\}$.

(ii) If $C_1 = c_1$ and $C_2 \neq -a_2$, then $H = G = \{f_1g_1, f_2g_1, -(C_2 + a_2)^{-1}r_2\}$.

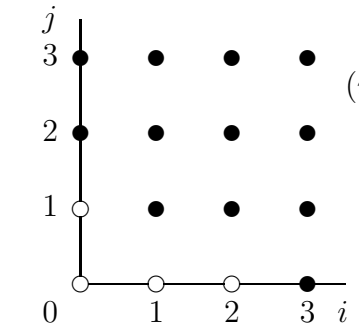
(iii) If $C_1 \neq c_1$, then $H = G = \{f_1g_1, f_2g_1, (C_1 - c_1)^{-1}r_1\}$.

2. $\mathbf{LM(G_2) = \{Y, X^2\}}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = X + C_1, f_2(X,Y) = Y + C_2\}, \\ G_2 &= \{g_1(X,Y) = Y + b_1X + c_1, g_2(X,Y) = X^2 + b_2X + c_2\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



$(i,j) \leftrightarrow X^iY^j$

$\mathrm{LM}(G_g) = \{XY, Y^2, X^3, X^2Y, Y^3\}$

$\mathrm{MD} = \quad (0,3) : F$

$(0,2) : f_2g_1$

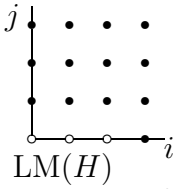
$(1,1) : f_1g_1 \qquad (2,1) : f_2g_2$

$(3,0) : f_1g_2$

It follows that $S = \{S_1 = S(f_1g_1, f_2g_2), S_2 = S(F, f_2g_1)\}$ with $\delta(G_g) = n_1 + n_2 + 1$. For $r_i \neq 0$ in $\{r_1, r_2\}$, $\mathrm{LM}(r_i)$ is either Y or X^2. The coefficient of X^2 in r_1 is $-g_1(-C_1, -C_2)$. Further, if $r_1 = 0$, the coefficient of X^2 in r_2 is the remainder on division of the quotient $F(X, -b_1X - c_1)/g_2$ by f_1.

Since $\delta(H) = 3$ with $\Delta(H) \subset \{1, X, Y, X^2\}$, we have the following diagrams on $\mathrm{LM}(H)$, which are followed by $\mathrm{LM}(G)$.

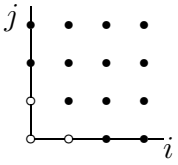
(1)



$\mathrm{LM}(H) = \{Y, X^3\}$

$\Leftrightarrow \mathrm{LM}(G) = \{X, Y^2\}$

(2)



$\mathrm{LM}(H) = \mathrm{LM}(G) = \{X^2, XY, Y^2\}$

As a result, we have H and G as follows:

(i) If $g_1(-C_1, -C_2) = 0$ and $F(X, -b_1X - c_1)$ is divisible by f_1g_2, then $H = \{h_1 = g_1, h_2 = f_1g_2\}$ and $\mathrm{LM}(G) = \{X, Y^2\}$. For the polynomial v_1, we have

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}(F - Y^2h_1)$$

for $q_{2,1}, q_{2,2} \in K[X, Y]$ with $\mathrm{LT}(v_1) = X, \mathrm{LM}(q_{2,1}) \leq XY, q_{2,2} = 1$ since $\{h_1, F - Y^2h_1\}$ is a Groebner basis for $\langle h_1, F\rangle$ and $v_1h_2 \in \langle h_1, F\rangle$. It follows that $\{v_1, Y^2 - q_{2,1}\}$ is a Groebner basis, whose elements are monic polynomials, for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $Y^2 - q_{2,1}$ on division by v_1.

(ii) If $g_1(-C_1, -C_2) = 0$ and $F(X, -b_1X - c_1)$ is not divisible by f_1g_2, then $H = G = \{r_{2,m}, f_1g_1 - b_1r_{2,m}, f_2g_1 - b_1f_1g_1 + b_1^2r_{2,m}\}$.

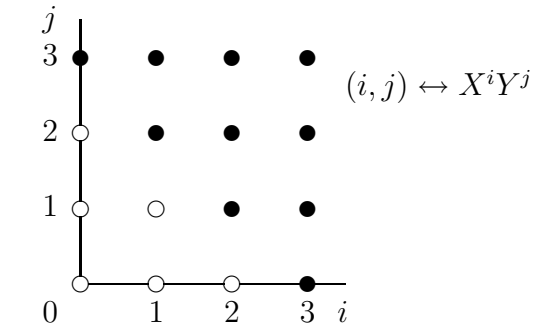
(iii) If $g_1(-C_1, -C_2) \neq 0$, then $H = G = \{r_{1,m}, f_1g_1 - b_1r_{1,m}, f_2g_1 - b_1f_1g_1 + b_1^2r_{1,m}\}$.

III. $\mathbf{n_1 = 1, n_2 = 3}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = X + C_1, f_2(X,Y) = Y + C_2\}, \\ G_2 &= \{g_1(X,Y) = X^2 + a_1Y + b_1X + c_1, g_2(X,Y) = XY + a_2Y + b_2X + c_2, \\ &\quad g_3(X,Y) = Y^2 + a_3Y + b_3X + c_3\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



$\mathrm{LM}(G_g) = \{X^3, X^2Y, XY^2, Y^3\}$

$$\begin{aligned} \mathrm{MD} = \quad & (0,3) : f_2g_3, F \\ & (1,2) : f_1g_3, f_2g_2 \\ & (2,1) : f_1g_2, f_2g_1 \\ & (3,0) : f_1g_1 \end{aligned}$$

It follows that $S = \{S_1 = S(f_1g_2, f_2g_1), S_2 = S(f_1g_3, f_2g_2), S_3 = S(F, f_2g_3)\}$ with $\delta(G_g) = n_1 + n_2 + 2$. For $G_{g,1} = G_g \cup \{r_1, r_2, r_3\}$, $\delta(G_{g,1})$ is either 4 or 5. If $\delta(G_{g,1}) = 4$, then $G_{g,1}$ is a Groebner basis. If $\delta(G_{g,1}) = 5$, then there is exactly one nonzero polynomial in $\{r_1, r_2, r_3\}$. For $r_i \neq 0$, $\mathrm{LM}(r_i)$ is X^2, XY or Y^2 and it is enough to consider the following S-polynomials in $G_{g,1}$:

(i) $S(r_i, f_1g_1)$ and $S(r_i, f_1g_2)$ if $\mathrm{LM}(r_i) = X^2$;

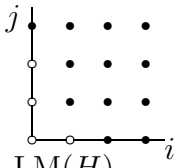
(ii) $S(r_i, f_1g_2)$ and $S(r_i, f_1g_3)$ if $\mathrm{LM}(r_i) = XY$;

(iii) $S(r_i, f_1g_3)$ and $S(r_i, f_2g_3)$ if $\mathrm{LM}(r_i) = Y^2$.

For a nonzero remainder r of these S-polynomials on division by $G_{g,1}$, $G_{g,1} \cup \{r\}$ is a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$ since $\delta(G_{g,1}) = n_1 + n_2 + 1$. Thus, the number of divisions to be done for getting a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$ is 5 at most.

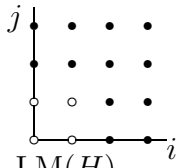
Since $\delta(H) = 4$ with $\Delta(H) \subset \{1, X, Y, X^2, XY, Y^2\}$, we have the following diagrams on $\mathrm{LM}(H)$, which are followed by $\mathrm{LM}(G)$.

(1)



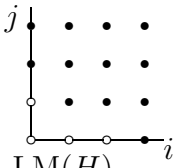
$\mathrm{LM}(H) = \{X^2, XY, Y^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X, Y\}$

(2)



$\mathrm{LM}(H) = \{X^2, Y^2\}$
$\Leftrightarrow \mathrm{LM}(G) = \{Y, X^2\}$

(3)



$\mathrm{LM}(H) = \{XY, Y^2, X^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X^2, XY, Y^2\}$

In the case of (1), $n' = \deg(h_1)^+ - (n_1 + n_2) = 2$. It follows that $\mathrm{LM}(v_1)$ is either X or Y. Let $H = \{h_1, h_2, h_3\}$ with $\mathrm{LM}(h_1) = X^2, \mathrm{LM}(h_2) = XY, \mathrm{LM}(h_3) = Y^3$. Then $\{h_1, F\}$ is a Groebner basis for $\langle h_1, F\rangle$ since $\mathrm{lcm}(\mathrm{LM}(h_1), \mathrm{LM}(F)) = \mathrm{LM}(h_1)\mathrm{LM}(F)$. Thus $\mathrm{LM}(v_1 h_i) \in \langle X^2, Y^3\rangle$ for all $h_i \in H$. It follows that $\mathrm{LM}(v_1) = X$. Further, $n = 1$ and $\mathrm{LM}(G) = \{X, Y\}$. Since $v_1 h_2 \in \langle h_1, F\rangle$, we have

$$v_1 h_2 = q_{2,1} h_1 + q_{2,2} F$$

for $q_{2,1}, q_{2,2} \in K[X, Y]$ with $\mathrm{LT}(q_{2,1}) = Y, q_{2,2} = 0$. It follows that $\{v_1, q_{2,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $q_{2,1}$ on division by v_1.

In the case of (2), $n' = \deg(h_1)^+ - (n_1 + n_2) = 2$. Let $H = \{h_1, h_2\}$ with $\mathrm{LM}(h_1) = X^2, \mathrm{LM}(h_2) = Y^2$. Then $\{h_1, F\}$ is a Groebner basis for $\langle h_1, F\rangle$. Thus $\mathrm{LM}(v_1 h_i) \in \langle X^2, Y^3\rangle$ for all $h_i \in H$. It follows that $\mathrm{LM}(v_1) = Y$. Further, $n = 2$ and $\mathrm{LM}(G) = \{Y, X^2\}$. Since $v_1 h_2 \in \langle h_1, F\rangle$, we have

$$v_1 h_2 = q_{2,1} h_1 + q_{2,2} F$$

for $q_{2,1}, q_{2,2} \in K[X, Y]$ with $\mathrm{LT}(q_{2,1}) = -X^2, q_{2,2} = 1$. It follows that $\{v_1, -q_{2,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $-q_{2,1}$ on division by v_1.

In the case of (3), $n' = \deg(h_1)^+ - (n_1 + n_2) = 3$. Thus $\mathrm{LM}(v_1) = X^2$ and $\mathrm{LM}(G) = \{X^2, XY, Y^2\}$. Let $H = \{h_1, h_2, h_3\}$ with $\mathrm{LM}(h_1) = XY, \mathrm{LM}(h_2) = Y^2, \mathrm{LM}(h_3) = X^3$. Then $\{h_1, F, XF - Y^2 h_1\}$ is a Groebner basis for $\langle h_1, F\rangle$. Since $v_1 h_i \in \langle h_1, F\rangle$ for all $h_i \in H$, we have

$$v_1 h_2 = q_{2,1} h_1 + q_{2,2} F + q_{2,3}(XF - Y^2 h_1)$$

for $q_{2,1}, q_{2,2}, q_{2,3} \in K[X,Y]$ with $\mathrm{LT}(q_{2,1}) = XY, \mathrm{LM}(q_{2,2}) \leq 1, q_{2,3} = 0$, and

$$v_1 h_3 = q_{3,1} h_1 + q_{3,2} F + q_{3,3}(XF - Y^2 h_1)$$

for $q_{3,1}, q_{3,2}, q_{3,3} \in K[X,Y]$ with $\mathrm{LM}(q_{3,1}) \leq XY, \mathrm{LM}(q_{3,2}) \leq 1, q_{3,3} = 1$. It follows that $\{v_1, q_{2,1}, Y^2 - q_{3,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2, v_3\}$ for the remainder v_2 of $q_{2,1}$ on division by v_1 and the remainder v_3 of $Y^2 - q_{3,1}$ on division by $\{v_1, v_2\}$.

Remark. We have another way to find H according to the relation between G_1 and G_2. We give it in Appendix.

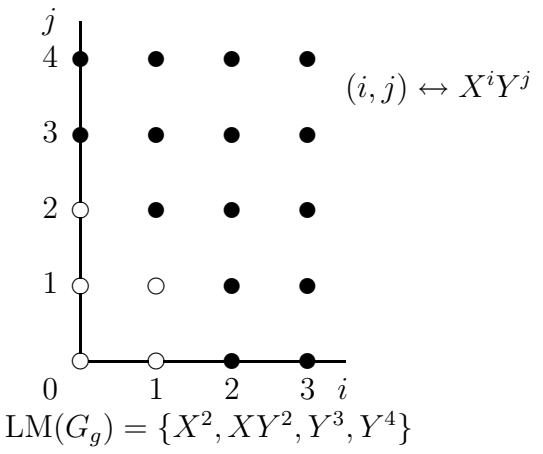
IV. $\mathbf{n_1 = 2, n_2 = 2}$

1. $\mathbf{LM(G_1) = \{X, Y^2\}, LM(G_2) = \{X, Y^2\}}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = X + C_1, f_2(X,Y) = Y^2 + A_2 Y + C_2\}, \\ G_2 &= \{g_1(X,Y) = X + c_1, g_2(X,Y) = Y^2 + a_2 Y + c_2\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



$\mathrm{LM}(G_g) = \{X^2, XY^2, Y^3, Y^4\}$

MD = $(0,4) : f_2 g_2$

$(0,3) : F$

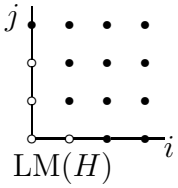
$(1,2) : f_1 g_2, f_2 g_1$

$(2,0) : f_1 g_1$

It follows that $S = \{S_1 = S(f_1 g_2, f_2 g_1), S_2 = S(F, f_1 g_2), S_3 = S(F, f_2 g_2)\}$ with $\delta(G_g) = n_1 + n_2 + 1$. For a nonzero r_i in $\{r_1, r_2, r_3\}$, $G_g \cup \{r_i\}$ is a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$ with $\mathrm{LM}(r_i) = XY$ or Y^2 since $\delta(G_g) = n_1 + n_2 + 1$.

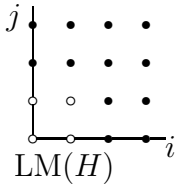
Since $\delta(H) = 4$ with $\Delta(H) \subset \{1, X, Y, XY, Y^2\}$, we have the following diagrams on $\mathrm{LM}(H)$ with the same result on G corresponding to H as that of **III**. $\mathbf{n_1 = 1, n_2 = 3}$.

(1)



$\mathrm{LM}(H) = \{X^2, XY, Y^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X, Y\}$

(2)



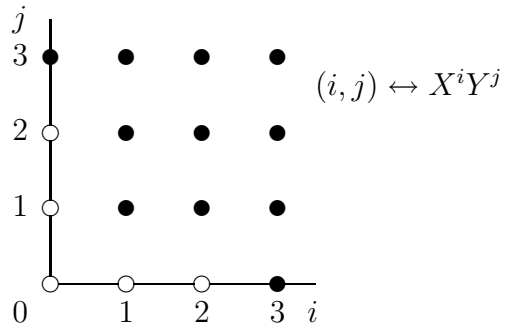
$\mathrm{LM}(H) = \{X^2, Y^2\}$
$\Leftrightarrow \mathrm{LM}(G) = \{Y, X^2\}$

2. $\mathbf{LM(G_1) = \{X, Y^2\}, LM(G_2) = \{Y, X^2\}}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = X + C_1, f_2(X,Y) = Y^2 + A_2Y + C_2\}, \\ G_2 &= \{g_1(X,Y) = Y + b_1X + c_1, g_2(X,Y) = X^2 + b_2X + c_2\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



$\mathrm{LM}(G_g) = \{XY, X^3, Y^3, X^2Y^2\}$

MD = $(0,3) : f_2g_1, F$

$(2,2) : f_2g_2$

$(1,1) : f_1g_1$

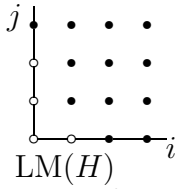
$(3,0) : f_1g_2$

It follows that $S = \{S_1 = S(F, f_2g_1), S_2 = S(f_2g_2, f_1g_1)\}$ with $\delta(G_g) = n_1 + n_2 + 1$. For a nonzero r_i in $\{r_1, r_2\}$, $G_g \cup \{r_i\}$ is a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$.

Since $\delta(H) = 4$ with $\Delta(H) \subset \{1, X, Y, X^2, Y^2\}$, we have the following diagrams on

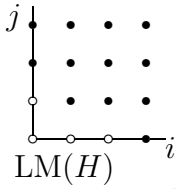
$\mathrm{LM}(H)$ with the same result on G corresponding to H as that of **III**. $\mathbf{n_1 = 1, n_2 = 3}$.

(1)



$\mathrm{LM}(H) = \{X^2, XY, Y^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X, Y\}$

(2)



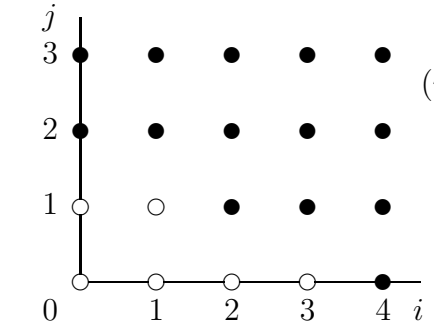
$\mathrm{LM}(H) = \{XY, Y^2, X^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X^2, XY, Y^2\}$

3. $\mathbf{LM(G_1) = \{Y, X^2\}, LM(G_2) = \{Y, X^2\}}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = Y + B_1X + C_1, f_2(X,Y) = X^2 + B_2X + C_2\}, \\ G_2 &= \{g_1(X,Y) = Y + b_1X + c_1, g_2(X,Y) = X^2 + b_2X + c_2\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



$(i,j) \leftrightarrow X^iY^j$

$\mathrm{LM}(G_g) = \{Y^2, X^2Y, X^4, Y^3\}$

$\mathrm{MD} = \quad (0,3) : F$

$(0,2) : f_1g_1$

$(2,1) : f_1g_2, f_2g_1$

$(4,0) : f_2g_2$

It follows that $S = \{S_1 = S(F, f_1g_3), S_2 = S(f_2g_2, f_1g_1), S_3 = S(f_2g_3, f_1g_2)\}$ with $\delta(G_g) = n_1 + n_2 + 2$. For $G_{g,1} = G_g \cup \{r_1, r_2, r_3\}$, $\delta(G_{g,1})$ is either 5 or 6. If $\delta(G_{g,1}) = 5$, then $G_{g,1}$ is a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$. If $\delta(G_{g,1}) = 6$, then there is exactly one nonzero polynomial in $\{r_1, r_2, r_3\}$. For $r_i \neq 0$, $\mathrm{LM}(r_i) = XY$ or X^3, and it is enough to consider the following S-polynomials:

(i) $S(f_1g_1, r_i)$ and $S(f_1g_2, r_i)$ if $\mathrm{LM}(r_i) = XY$;

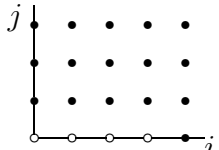
(ii) $S(f_2g_1, r_i)$ and $S(f_2g_2, r_i)$ if $\mathrm{LM}(r_i) = X^3$.

Then, for a nonzero remainder r of these S-polynomials on division by $G_{g,1}$, $G_{g,1} \cup \{r\}$

is a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$ since $\delta(G_{g,1}) = n_1 + n_2 + 1$. Thus, the number of divisions to be done for getting a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$ is 5 at most.

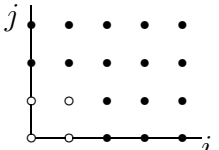
Since $\delta(H) = 4$ with $\Delta(H) \subset \{1, X, Y, X^2, XY, X^3\}$, we have the following diagrams on $\mathrm{LM}(H)$ with the same result on G corresponding to H as that of **III**. $\mathbf{n_1 = 1, n_2 = 3}$.

(1)



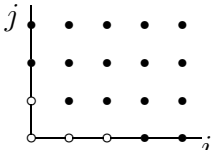
$\mathrm{LM}(H) = \{Y, X^4\}$
$\Leftrightarrow \mathrm{LM}(G) = \{1\}$

(2)



$\mathrm{LM}(H) = \{X^2, Y^2\}$
$\Leftrightarrow \mathrm{LM}(G) = \{Y, X^2\}$

(3)



$\mathrm{LM}(H) = \{XY, Y^2, X^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X^2, XY, Y^2\}$

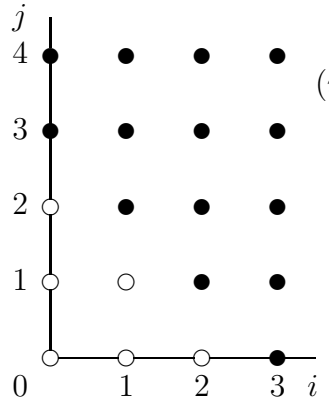
V. $\mathbf{n_1 = 2, n_2 = 3}$

1. $\mathbf{LM(G_1) = \{X, Y^2\}}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = X + C_1, f_2(X,Y) = Y^2 + A_2Y + C_2\}, \\ G_2 &= \{g_1(X,Y) = X^2 + a_1Y + b_1X + c_1, g_2(X,Y) = XY + a_2Y + b_2X + c_2, \\ &\quad g_3(X,Y) = Y^2 + a_3Y + b_3X + c_3\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



$(i,j) \leftrightarrow X^iY^j$

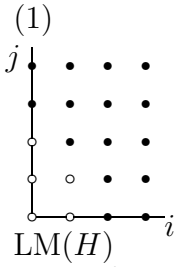
MD = $(0,4) : f_2g_3$
$(0,3) : F$ $\quad (1,3) : f_2g_2$
$(1,2) : f_1g_3$ $\quad (2,2) : f_2g_1$
$(2,1) : f_1g_2$
$(3,0) : f_1g_1$

$\mathrm{LM}(G_g) = \{X^3, X^2Y, XY^2, Y^3, X^2Y^2, XY^3, Y^4\}$

It follows that $S = \{S_1 = S(f_2g_1, f_1g_3), S_2 = S(f_2g_2, f_1g_3), S_3 = S(f_2g_2, F), S_4 = S(f_2g_3, F)\}$ with $\delta(G_g) = n_1 + n_2 + 1$. For $r_i \neq 0$ in $\{r_1, r_2, r_3, r_4\}$, $G_g \cup \{r_i\}$ is a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$.

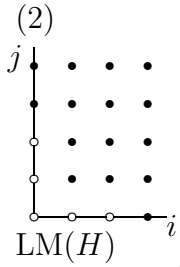
Since $\delta(H) = 5$ with $\Delta(H) \subset \{1, X, Y, X^2, XY, Y^2\}$, we have the following diagrams on $\mathrm{LM}(H)$, which are followed by $\mathrm{LM}(G)$.

(1)



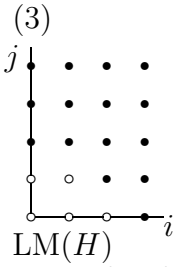
$\mathrm{LM}(H) = \{X^2, XY^2, Y^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X, Y^2\}$

(2)



$\mathrm{LM}(H) = \{XY, X^3, Y^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{Y, X^2\}$

(3)



$\mathrm{LM}(H) = \{Y^2, X^3, X^2Y\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X^2, XY, Y^2\}$

In the case of (1), $n' = 1$ and $\mathrm{LM}(v_1) = X$. Further, $n = 2$ and $\mathrm{LM}(G) = \{X, Y^2\}$. Let $H = \{h_1, h_2, h_3\}$ with $\mathrm{LM}(h_1) = X^2, \mathrm{LM}(h_2) = XY^2, \mathrm{LM}(h_3) = Y^3$. Then $\{h_1, F\}$ is a Groebner basis for $\langle h_1, F\rangle$. Since $v_1h_2 \in \langle h_1, F\rangle$, we have

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}F$$

for $q_{2,1}, q_{2,2} \in K[X, Y]$ with $\mathrm{LT}(q_{2,1}) = Y^2, \mathrm{LM}(q_{2,2}) \leq 1$. It follows that $\{v_1, q_{2,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $q_{2,1}$ on division by v_1.

In the case of (2), $n' = 2$. It follows that $\mathrm{LM}(v_1)$ is either X or Y. Let $H = \{h_1, h_2, h_3\}$ with $\mathrm{LM}(h_1) = XY, \mathrm{LM}(h_2) = X^3, \mathrm{LM}(h_3) = Y^3$. Then $\{h_1, F, XF - Y^2h_1\}$ is a Groebner basis for $\langle h_1, F\rangle$. Since $\mathrm{LM}(v_1h_i) \in \langle XY, X^3, Y^3\rangle$ for all $h_i \in H$, we have $\mathrm{LM}(v_1) = Y$. It follows that $n = 2$ and $\mathrm{LM}(G) = \{Y, X^2\}$. Since $v_1h_2 \in \langle h_1, F\rangle$, we have

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}F + q_{2,3}(XF - Y^2h_1)$$

for $q_{2,1}, q_{2,2}, q_{2,3} \in K[X, Y]$ with $\mathrm{LT}(q_{2,1}) = X^2, \mathrm{LM}(q_{2,2}) \leq 1, q_{2,3} = 0$. It follows that $\{v_1, q_{2,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $q_{2,1}$ on division by v_1.

In the case of (3), $n' = 3$ and $\mathrm{LM}(v_1) = X^2$. Further, $\mathrm{LM}(G) = \{X^2, XY, Y^2\}$. Let $H = \{h_1, h_2, h_3\}$ with $\mathrm{LM}(h_1) = Y^2, \mathrm{LM}(h_2) = X^3, \mathrm{LM}(h_3) = X^2Y$. Then $\{h_1, F - Yh_1\}$

is a Groebner basis for $\langle h_1, F\rangle$. Since $v_1 h_2 \in \langle h_1, F\rangle$, we have

$$v_1 h_2 = q_{2,1} h_1 + q_{2,2}(F - Y h_1)$$

for $q_{2,1}, q_{2,2} \in K[X,Y]$ with $\mathrm{LM}(q_{2,1}) \leq X^2, \mathrm{LT}(q_{2,2}) = X$, and

$$v_1 h_3 = q_{3,1} h_1 + q_{3,2}(F - Y h_1)$$

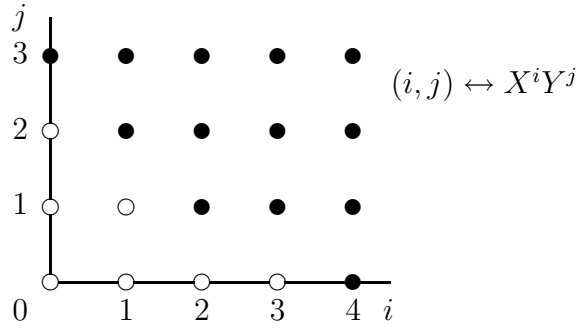
for $q_{3,1}, q_{3,2} \in K[X,Y]$ with $\mathrm{LM}(q_{3,1}) \leq XY, \mathrm{LT}(q_{3,2}) = Y$. It follows that $\{v_1, q_{2,2}Y - q_{2,1}, q_{3,2}Y - q_{3,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2, v_3\}$ for the remainder v_2 of $q_{2,2}Y - q_{2,1}$ on division by v_1 and the remainder v_3 of $q_{3,2}Y - q_{3,1}$ on division by $\{v_1, v_2\}$.

2. $\mathbf{LM(G_1) = \{Y, X^2\}}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = Y + B_1 X + C_1, f_2(X,Y) = X^2 + B_2 X + C_2\}, \\ G_2 &= \{g_1(X,Y) = X^2 + a_1 Y + b_1 X + c_1, g_2(X,Y) = XY + a_2 Y + b_2 X + c_2, \\ &\quad g_3(X,Y) = Y^2 + a_3 Y + b_3 X + c_3\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



$\mathrm{LM}(G_g) = \{X^2Y, XY^2, X^4, Y^3, X^3Y, X^2Y^2\}$

$$\begin{aligned} \mathrm{MD} = \quad & (0,3) : f_1 g_3, F \\ & (1,2) : f_1 g_2 \quad (2,2) : f_2 g_3 \\ & (2,1) : f_1 g_1 \quad (3,1) : f_2 g_2 \\ & (4,0) : f_2 g_1 \end{aligned}$$

It follows that $S = \{S_1 = S(F, f_1 g_3), S_2 = S(f_2 g_2, f_1 g_1), S_3 = S(f_2 g_3, f_1 g_2)\}$ with $\delta(G_g) = n_1 + n_2 + 2$. For $G_{g,1} = G_g \cup \{r_1, r_2, r_3\}$, $\delta(G_{g,1})$ is either 5 or 6. If $\delta(G_{g,1}) = 5$, then $G_{g,1}$ is a Groebner basis. If $\delta(G_{g,1}) = 6$, then there is exactly one nonzero polynomial in $\{r_1, r_2, r_3\}$. For $r_i \neq 0$, $\mathrm{LM}(r_i)$ is XY, Y^2 or X^3 and it is enough to consider of the following S-polynomials:

(i) $S(f_1 g_1, r_i)$ and $S(f_1 g_2, r_i)$ if $\mathrm{LM}(r_i) = XY$;

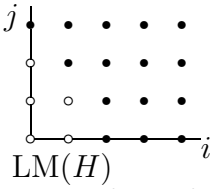
(ii) $S(f_1g_2, r_i)$ and $S(f_1g_3, r_i)$ if $\mathrm{LM}(r_i) = Y^2$;

(iii) $S(f_2g_1, r_i)$ and $S(f_2g_2, r_i)$ if $\mathrm{LM}(r_i) = X^3$.

For a nonzero remainder r of these S-polynomials on division by $G_{g,1}$, $G_{g,1} \cup \{r\}$ is a Groebner basis for $\varphi^{-1}(I_{D_1+D_2})$ since $\delta(G_{g,1}) = n_1 + n_2 + 1$. Thus, the number of divisions to be done for getting a Groebner basis is 5 at most.

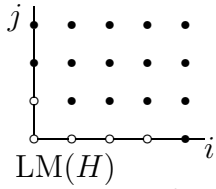
Since $\delta(H) = 5$ with $\Delta(H) \subset \{1, X, Y, X^2, XY, Y^2, X^3\}$, we have the following diagrams on $\mathrm{LM}(H)$ with the same result on G as that of **1.** $\mathbf{LM(G_1) = \{X, Y^2\}}$ in **V.** $\mathbf{n_1 = 2, n_2 = 3}$ except (2).

(1)



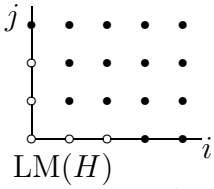
$\mathrm{LM}(H) = \{X^2, XY^2, Y^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X, Y^2\}$

(2)



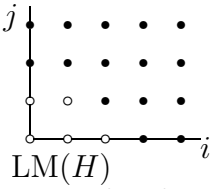
$\mathrm{LM}(H) = \{XY, Y^2, X^4\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X, Y\}$

(3)



$\mathrm{LM}(H) = \{XY, X^3, Y^3\}$
$\Leftrightarrow \mathrm{LM}(G) = \{Y, X^2\}$

(4)



$\mathrm{LM}(H) = \{Y^2, X^3, X^2Y\}$
$\Leftrightarrow \mathrm{LM}(G) = \{X^2, XY, Y^2\}$

In the case of (2), $n' = 2$. Thus $\mathrm{LM}(v_1)$ is either X or Y. Let $H = \{h_1, h_2, h_3\}$ with $\mathrm{LM}(h_1) = XY, \mathrm{LM}(h_2) = Y^2, \mathrm{LM}(h_3) = X^4$. Then $\{h_1, F, XF - Y^2h_1\}$ is a Groebner basis for $\langle h_1, F\rangle$.

Now, consider on $\mathrm{LM}(v_1)$. Suppose that $\mathrm{LM}(v_1) = Y$. Then $\mathrm{LM}(G) = \{Y, X^2\}$. Since $v_1h_2 \in \langle h_1, F\rangle$,

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}F + q_{2,3}(XF - Y^2h_1)$$

for $q_{2,1}, q_{2,2}, q_{2,3} \in K[X, Y]$ with $\mathrm{LM}(q_{2,1}) \leq Y, q_{2,2} = 1, q_{2,3} = 0$. Then $q_{2,1} = kv_1$ for $k \in K$ since $q_{2,1} \in I$ with $\mathrm{LM}(q_{2,1}) \leq Y$. It follows that $v_1(h_2 - kh_1) = F$. It is a contradiction since F is irreducible. Hence we have $\mathrm{LM}(v_1) = X$ and $\mathrm{LM}(G) = \{X, Y\}$.

Since $v_1h_2 \in \langle h_1, F\rangle$, we have

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}F + q_{2,3}(XF - Y^2h_1)$$

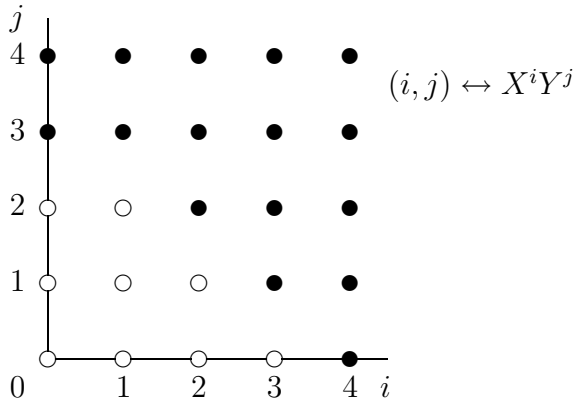
for $q_{2,1}, q_{2,2}, q_{2,3} \in K[X, Y]$ with $\mathrm{LT}(q_{2,1}) = Y, q_{2,2} = q_{2,3} = 0$. It follows that $\{v_1, q_{2,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $q_{2,1}$ on division by v_1.

VI. $\mathbf{n_1 = 3, n_2 = 3}$

If the reduced Groebner bases are

$$\begin{aligned} G_1 &= \{f_1(X,Y) = X^2 + A_1Y + B_1X + C_1, f_2(X,Y) = XY + A_2Y + B_2X + C_2, \\ &\quad f_3(X,Y) = Y^2 + A_3Y + B_3X + C_3\}, \\ G_2 &= \{g_1(X,Y) = X^2 + a_1Y + b_1X + c_1, g_2(X,Y) = XY + a_2Y + b_2X + c_2, \\ &\quad g_3(X,Y) = Y^2 + a_3Y + b_3X + c_3\}, \end{aligned}$$

we have the following diagram on $\mathrm{LM}(G_g)$.



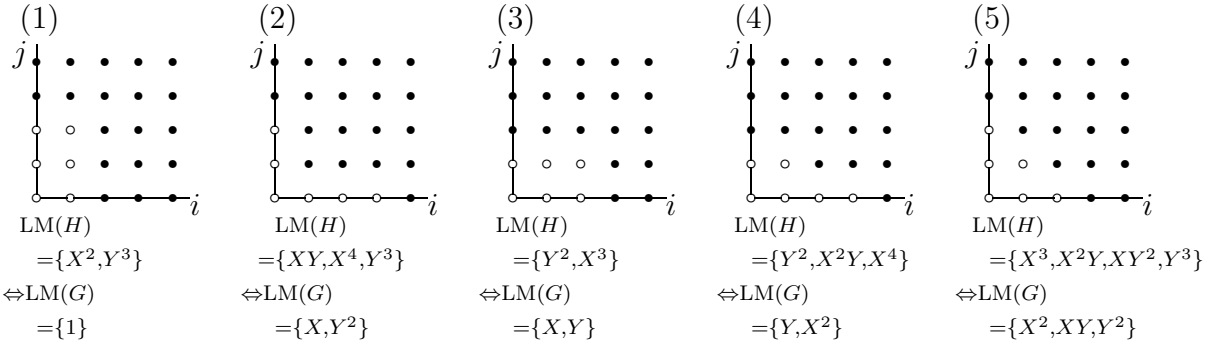
$\mathrm{LM}(G_g) = \{X^4, Y^3, X^3Y, X^2Y^2, XY^3, Y^4\}$

$$\begin{aligned} \mathrm{MD} = \ & (0,4) : f_3g_3 \\ & (0,3) : F \qquad (1,3) : f_2g_3, f_3g_2 \\ & (2,2) : f_1g_3, f_2g_2, f_3g_1 \\ & (3,1) : f_1g_2, f_2g_1 \\ & (4,0) : f_1g_1 \end{aligned}$$

It follows that $S = \{S_1 = S(f_1g_2, f_2g_1), S_2 = S(f_1g_3, f_2g_2), S_3 = S(f_1g_3, f_3g_1), S_4 = S(f_2g_3, f_3g_2), S_5 = S(f_2g_3, F), S_6 = S(f_3g_3, F)\}$ with $\delta(G_g) = n_1 + n_2 + 3$. For $G_{g,1} = G_g \cup \{r_1, r_2, r_3, r_4, r_5, r_6\}$, $\delta(G_{g,1})$ is 6, 7 or 8. If $\delta(G_{g,1}) = 6$, then $G_{g,1}$ is a Groebner basis. If $\delta(G_{g,1}) = 7$, then there are one or two nonzero polynomials in $\{r_1, r_2, r_3, r_4, r_5, r_6\}$. For all $r_i \neq 0$ in $\{r_1, r_2, r_3, r_4, r_5, r_6\}$, we compute the remainders of S-polynomials $S(r_i, f)$ and $S(r_i, g)$ for a nearest polynomial f to r_i in the lower right-hand and a nearest polynomial g to r_i in the upper left-hand of $G_{g,1}$ as considering the leading monomials. Then, for a nonzero remainder r of S-polynomials, $G_{g,1} \cup \{r\}$ is a Groebner basis since $\delta(G_{g,1}) = n_1 + n_2 + 1$. If $\delta(G_{g,1}) = 8$, then there is exactly one nonzero polynomial in $\{r_1, r_2, r_3, r_4, r_5, r_6\}$. For a nonzero r_i in $\{r_1, r_2, r_3, r_4, r_5, r_6\}$, it is enough to consider the S-polynomials $S(r_i, f)$ and $S(r_i, g)$ for a nearest polynomial f to r_i in the lower right-hand and a nearest polynomial g to r_i in the upper left-hand of $G_{g,1}$. Let $r_{i,1}$ be the remainder of $S(r_i, f)$ on division by $G_{g,1}$ and let $r_{i,2}$ be the remainder of $S(r_i, g)$ on division by $G_{g,1} \cup \{r_{i,1}\}$. For $G_{g,2} = G_{g,1} \cup \{r_{i,1}, r_{i,2}\}$, $\deg(G_{g,2})$ is either 6 or 7. If $\delta(G_{g,2}) = 6$, then $G_{g,2}$ is a Groebner basis. If $\delta(G_{g,2}) = 7$, then there is only one nonzero polynomial in $\{r_{i,1}, r_{i,2}\}$. For a nonzero $r_{i,j}$ in $\{r_{i,1}, r_{i,2}\}$, it is enough to consider the

S-polynomials $S(r_{i,j}, f)$ and $S(r_{i,j}, g)$ for a nearest polynomial f to $r_{i,j}$ in the lower right-hand and a nearest polynomial g to $r_{i,j}$ in the upper left-hand of $G_{g,2}$. For a nonzero remainder r of those S-polynomials on division by $G_{g,2}$, $G_{g,2} \cup \{r\}$ is a Groebner basis since $\delta(G_{g,2}) = n_1 + n_2 + 1$. Thus, the number of divisions to be done for getting a Groebner basis is 10 at most. In particular, if $G_1 = G_2$, the number of divisions to be done is 7 at most.

Since $\delta(H) = 6$ with $\Delta(H) \subset \{1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2\}$, we have the following diagrams on $\mathrm{LM}(H)$, which are followed by $\mathrm{LM}(G)$.



In the case of (1), $n' = 0$. Thus $n = 0$ and $G = \{1\}$.

In the case of (2), $n' = 1$. Thus $\mathrm{LM}(v_1) = X$ and $\mathrm{LM}(G) = \{X, Y^2\}$. Let $H = \{h_1, h_2, h_3\}$ with $\mathrm{LM}(h_1) = XY, \mathrm{LM}(h_2) = X^4, \mathrm{LM}(h_3) = Y^3$. Then $\{h_1, F, XF - Y^2h_1\}$ is a Groebner basis for $\langle h_1, F\rangle$. Since $v_1h_2 \in \langle h_1, F\rangle$, we have

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}F + q_{2,3}(XF - Y^2h_1)$$

for $q_{2,1}, q_{2,2}, q_{2,3} \in K[X, Y]$ with $\mathrm{LM}(q_{2,1}) \leq XY, \mathrm{LM}(q_{2,2}) \leq 1, q_{2,3} = 1$. It follows that $\{v_1, Y^2 - q_{2,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $Y^2 - q_{2,1}$ on division by v_1.

In the case of (3), $n' = 2$. Thus $\mathrm{LM}(v_1)$ is either X or Y. Let $H = \{h_1, h_2\}$ with $\mathrm{LM}(h_1) = Y^2, \mathrm{LM}(h_2) = X^3$. Then $\{h_1, F - Yh_1\}$ is a Groebner basis for $\langle h_1, F\rangle$. Since $\mathrm{LM}(v_1h_i) \in \langle Y^2, X^4\rangle$ for all $h_i \in H$, we have $\mathrm{LM}(v_1) = X$. It follows that $\mathrm{LM}(G) = \{X, Y\}$. Since $v_1h_2 \in \langle h_1, F\rangle$, we have

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}(F - Yh_1)$$

for $q_{2,1}, q_{2,2} \in K[X, Y]$ with $\mathrm{LM}(q_{2,1}) \leq X, q_{2,2} = 1$. It follows that $\{v_1, Y - q_{2,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $Y - q_{2,1}$ on division by v_1.

In the case of (4), $n' = 2$. Thus $\mathrm{LM}(v_1)$ is either X or Y. Let $H = \{h_1, h_2, h_3\}$ with $\mathrm{LM}(h_1) = Y^2, \mathrm{LM}(h_2) = X^2Y, \mathrm{LM}(h_3) = X^4$. Then $\{h_1, F - Yh_1\}$ is a Groebner basis for $\langle h_1, F\rangle$. Since $\mathrm{LM}(v_1h_2) \in \langle Y^2, X^4\rangle$, we have $\mathrm{LM}(v_1) = Y$. It follows that $\mathrm{LM}(G) = \{Y, X^2\}$. Since $v_1h_2 \in \langle h_1, F\rangle$, we have

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}(F - Yh_1)$$

for $q_{2,1}, q_{2,2} \in K[X, Y]$ with $\mathrm{LT}(q_{2,1}) = X^2, \mathrm{LM}(q_{2,2}) \leq 1$. It follows that $\{v_1, q_{2,1} - Yq_{2,2}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2\}$ for the remainder v_2 of $q_{2,1} - Yq_{2,2}$ on division by v_1.

In the case of (5), $n' = 3$ and $\mathrm{LM}(v_1) = X^2$. Further, $\mathrm{LM}(G) = \{X^2, XY, Y^2\}$. Let $H = \{h_1, h_2, h_3, h_4\}$ with $\mathrm{LM}(h_1) = X^3, \mathrm{LM}(h_2) = X^2Y, \mathrm{LM}(h_3) = XY^2, \mathrm{LM}(h_4) = Y^3$. Then $\{h_1, F\}$ is a Groebner basis for $\langle h_1, F\rangle$. Since $v_1h_i \in \langle h_1, F\rangle$ for all $h_i \in H$, we have

$$v_1h_2 = q_{2,1}h_1 + q_{2,2}F$$

for $q_{2,1}, q_{2,2} \in K[X, Y]$ with $\mathrm{LT}(q_{2,1}) = XY, \mathrm{LM}(q_{2,2}) \leq X$, and

$$v_1h_3 = q_{3,1}h_1 + q_{3,2}F$$

for $q_{3,1}, q_{3,2} \in K[X, Y]$ with $\mathrm{LT}(q_{3,1}) = Y^2, \mathrm{LM}(q_{3,2}) \leq Y$. It follows that $\{v_1, q_{2,1}, q_{3,1}\}$ is a Groebner basis for I. Thus $G = \{v_1, v_2, v_3\}$ for the remainder v_2 of $q_{2,1}$ on division by v_1 and the remainder v_3 of $q_{3,1}$ on division by $\{v_1, v_2\}$.

Chapter 5

Appendix

In this appendix, we consider on the sum of normal divisors D_1 and D_2 of a C_{34} curve by using the relation between the reduced Groebner basis for $\varphi^{-1}(I_{D_1})$ and the reduced Groebner basis for $\varphi^{-1}(I_{D_2})$. In particular, we consider on the reduced Groebner basis H for $\varphi^{-1}(I_{D_1+D_2})$. Let D be the normal divisor such that $D \sim D_1 + D_2$. For the given H, the computation of the reduced Groebner basis G for $\varphi^{-1}(I_D)$ is presented in Section 4.4. Now that the reduced Groebner basis is easily computed by a Groebner basis ([5]), we compute a Groebner basis. Here, we use the notation in Chapter 4. Sometimes we represent a polynomial $f(X, Y) \in K[X, Y]$ as f.

For the sum $D_1 + D_2$ with $n_1 = 1$ and $n_2 = 1$ or 2, the result on G is given in Section 4.4.

Now, we consider the sum $D_1 + D_2$ with $n_1 = 1$ and $n_2 = 3$. Let $D_1 = P - \infty$ and $D_2 = E_2 - 3 \cdot \infty$ be normal divisors of C with

$$G_1 = \{f_1(X, Y) = X + C_1, f_2(X, Y) = Y + C_2\}$$

and $G_2 = \{g_1(X, Y), g_2(X, Y), g_3(X, Y)\}$, where

$$\begin{aligned} g_1(X, Y) &= X^2 + a_1 Y + b_1 X + c_1, \\ g_2(X, Y) &= XY + a_2 Y + b_2 X + c_2, \\ g_3(X, Y) &= Y^2 + a_3 Y + b_3 X + c_3. \end{aligned}$$

Let

$$\begin{aligned}
g_2'(X,Y) &= XY + (-a_2+b_1)Y + (a_1^2 - a_3 - a_1s_2)X \\
&\quad -a_1^2a_2 + a_2a_3 - a_1^2b_1 - a_3b_1 + a_1b_3 - a_1s_1 + a_1a_2s_2 + a_1^2t_3, \\
g_3'(X,Y) &= Y^2 + (a_1^2 - b_2 - a_1s_2)Y + (2a_1b_1 - b_3 + s_1 - b_1s_2 - a_1t_3)X \\
&\quad -2a_1a_2^2 + 2a_1^2a_3 + 2a_1a_2b_1 - a_1b_1^2 - 3a_1^2b_2 + b_2^2 + a_2b_3 - b_1b_3 + s_0 + a_2^2s_2 \\
&\quad -a_1a_3s_2 - a_2b_1s_2 + 2a_1b_2s_2 - a_1t_2 + a_1b_1t_3.
\end{aligned}$$

Then $\{g_1(X,Y), g_2'(X,Y), g_3'(X,Y)\}$ is the reduced Groebner basis for the normal ideal $\varphi^{-1}(I_{D_2'})$, where D_2' is the normal divisor such that $D_2' \sim -D_2$.

For $S = \{S_1 = S(f_1g_2, f_2g_1), S_2 = S(f_1g_3, f_2g_2), S_3 = (F, f_2g_3)\}$ and the remainder r_3 of S_3 on division by $G_g = \{f_ig_j \mid f_i \in G_1, g_j \in G_2\} \cup \{F\}$, we have

$$\begin{aligned}
S_1 &= -a_1Y^2 + (a_2 - b_1 + C_1)XY + \cdots, \\
S_2 &= (-a_2 + C_1)Y^2 + (a_3 - b_2 - C_2)XY + \cdots, \\
r_3 &= -(a_3 + C_2)Y^2 + (a_1a_2 + a_1b_1 - b_3 + a_1C_1 + s_1 - a_2s_2 - C_1s_2 - a_1t_3)XY + \cdots.
\end{aligned}$$

Here,

$$\begin{aligned}
g_1(-C_1,-C_2) &= (a_2 - b_1 + C_1)(-a_2 + C_1) + a_1(a_3 - b_2 - C_2), \\
g_2'(-C_1,-C_2) &= -a_1(a_1a_2 + a_1b_1 - b_3 + a_1C_1 + s_1 - a_2s_2 - C_1s_2 - a_1t_3) \\
&\quad +(a_2 - b_1 + C_1)(a_3 + C_2)
\end{aligned}$$

by Theorem 4.2.2. It follows that:

(a) $Y^2, XY \in \mathrm{LM}(\langle S_1, S_2\rangle)$ if $g_1(-C_1,-C_2) \neq 0$;

(b) $Y^2, XY \in \mathrm{LM}(\langle S_1, r_3\rangle)$ if $g_2'(-C_1,-C_2) \neq 0$.

Since $\delta(H) = 4$ with $\Delta(H) \subset \{1, X, Y, X^2, XY, Y^2\}$, $\mathrm{LM}(H)$ is one of the following: $\{X^2, XY, Y^3\}$; $\{X^2, Y^2\}$; and $\{XY, Y^2, X^3\}$. For every $h(X,Y) \in H$, $h(X,Y)$ is divisible by G_2 since $\varphi^{-1}(I_{D_1+D_2}) \subset \varphi^{-1}(I_{D_2})$. It implies that $X^2 \in \mathrm{LM}(H)$ if and only if $g_1(X,Y) \in H$. In other words, $X^2 \in \mathrm{LM}(H)$ if and only if $(D_2')^+ \geq P = (-C_1,-C_2)$, i.e. $g_1(-C_1,-C_2) = g_2'(-C_1,-C_2) = g_3'(-C_1,-C_2) = 0$.

As a result, we have the following on the ideal $\varphi^{-1}(I_{D_1+D_2}) \subset K[X,Y]$.

(i) If $g_1(-C_1,-C_2) \neq 0$, then we have a Groebner basis

$$\{g_2 + k_1g_1, g_3 + k_2g_1, f_1g_1\} \text{ with } \mathrm{LM}(H) = \{XY, Y^2, X^3\},$$

where $k_1 = -g_1(-C_1,-C_2)^{-1}g_2(-C_1,-C_2), k_2 = -g_1(-C_1,-C_2)^{-1}g_3(-C_1,-C_2) \in K$.

(ii) If $g_1(-C_1, -C_2) = 0$ and $g_2'(-C_1, -C_2) \neq 0$, then we have a Groebner basis

$$\{S_1, r_3, S(S_1, r_3), f_1 g_1\} \text{ with } \mathrm{LM}(H) = \{XY, Y^2, X^3\}.$$

(iii) If $g_1(-C_1, -C_2) = g_2'(-C_1, -C_2) = 0$ and $g_3'(-C_1, -C_2) \neq 0$, then $a_1 = 0$ and we have a Groebner basis

$$\{S_2, r_3, g_2 + F_Y(-C_1, -C_2)^{-1} F_X(-C_1, -C_2) g_1, f_1 g_1\} \text{ with } \mathrm{LM}(H) = \{XY, Y^2, X^3\}.$$

(iv) If $g_1(-C_1, -C_2) = g_2'(-C_1, -C_2) = g_3'(-C_1, -C_2) = 0$, then we have a Groebner basis

$$\{g_1, g_2, f_2 g_3\} \text{ with } \mathrm{LM}(H) = \{X^2, XY, Y^3\}$$

in the case of $a_1 = -a_2 + C_1 = a_3 + C_2 = 0$, and

$$\{S_1, S_2, r_3, g_1\} \text{ with } \mathrm{LM}(H) = \{X^2, Y^2\}$$

in the other cases.

Hence we have G when $n_1 = 1$.

In the case of $n_1 = 2$ and $n_2 = 2$ or 3, the zero divisor $E_1 = P_1 + P_2$ is obtained by the equations $f_1(X, Y) = 0$ and $f_2(X, Y) = 0$. Thus G can be obtained by the sum of $P_1 - \infty$ and $(P_2 - \infty) + D_2$.

Now, we consider the last case $n_1 = n_2 = 3$. Let $E_1 = P_1 + P_2 + P_3$ with $P_i = (x_i, y_i)$. Then

$$(X + A_2) f_2(X, Y) - A_1 f_1(X, Y) = \prod_{i=1}^{3} (X - x_i). \tag{1}$$

At first, we compute the reduced Groebner basis G_c for

$$\langle f_1, f_2, f_3, f_1 - g_1, f_2 - g_2, f_3 - g_3 \rangle.$$

Then $\mathrm{LM}(G_c) = \{1\}, \{X, Y\}, \{X, Y^2\}, \{Y, X^2\}$ or $\{X^2, XY, Y^2\}$.

If $\mathrm{LM}(G_c) = \{1\}$, then $h(X, Y) \in \varphi^{-1}(L(\infty \cdot \infty - (E_1 + E_2)))$ if and only if $h(X, Y)$ is divisible by G_1 and by G_2. Thus the reduced Groebner basis H is easily computed. For example, if $f_1(X, Y) = g_1(X, Y)$, then $h_1(X, Y) = f_1(X, Y) \in H$.

If $\mathrm{LM}(G_c) = \{X, Y\}, \{X, Y^2\}$ or $\{Y, X^2\}$, then $E_1 = P_1 + P_2 + P_3$ is obtained by G_c and (1). Thus G can be obtained by $(P_1 - \infty) + ((P_2 - \infty) + ((P_3 - \infty) + D_2))$.

If $\mathrm{LM}(G_c) = \{X^2, XY, Y^2\}$, then $D_1 = D_2$. In the case of $A_1 = 0$, $E_1 = (A_2 - B_1, -B_2) + (-A_2, \beta_1) + (-A_2, \beta_2)$ for the roots β_1, β_2 of $Y^2 + A_3 Y - B_3 A_2 + C_3 = 0$. Thus G can be obtained by $(A_2 - B_1, -B_2) - \infty + ((-A_2, \beta_1) - \infty + ((-A_2, \beta_2) - \infty + D_2))$. In the case of $A_1 \neq 0$, to avoid using a cubic equation, we use the method given in Section 4.4 with the S-polynomials whose number is 7 at most.

From now on, we consider the general case $\langle f_1, f_2, f_3, f_1 - g_1, f_2 - g_2, f_3 - g_3 \rangle = \langle 1 \rangle$. Let

$$M(G_1, G_2) = \begin{pmatrix} A_1 - a_1 & A_2 - a_2 & A_3 - a_3 \\ B_1 - b_1 & B_2 - b_2 & B_3 - b_3 \\ C_1 - c_1 & C_2 - c_2 & C_3 - c_3 \end{pmatrix}.$$

Assume that $\det M(G_1, G_2) \neq 0$. Then the elements of H are

$$\begin{aligned} h_1(X, Y) &= (X + k_1) f_1 + k_2 f_2 + k_3 f_3, \\ h_2(X, Y) &= k_4 f_1 + (X + k_5) f_2 + k_6 f_3, \\ h_3(X, Y) &= k_7 f_1 + k_8 f_2 + (X + k_9) f_3 \end{aligned}$$

and the remainder of $F(X, Y)$ on division by $\{h_1(X, Y), h_2(X, Y), h_3(X, Y)\}$ for $k_i \in K$ such that

$$\begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} = M(G_1, G_2)^{-1} \begin{pmatrix} a_2(A_1 - a_1) + a_1(B_1 - b_1) \\ b_2(A_1 - a_1) + b_1(B_1 - b_1) - (C_1 - c_1) \\ c_2(A_1 - a_1) + c_1(B_1 - b_1) \end{pmatrix},$$

$$\begin{pmatrix} k_4 \\ k_5 \\ k_6 \end{pmatrix} = M(G_1, G_2)^{-1} \begin{pmatrix} a_2(A_2 - a_2) + a_1(B_2 - b_2) \\ b_2(A_2 - a_2) + b_1(B_2 - b_2) - (C_2 - c_2) \\ c_2(A_2 - a_2) + c_1(B_2 - b_2) \end{pmatrix},$$

$$\begin{pmatrix} k_7 \\ k_8 \\ k_9 \end{pmatrix} = M(G_1, G_2)^{-1} \begin{pmatrix} a_2(A_3 - a_3) + a_1(B_3 - b_3) \\ b_2(A_3 - a_3) + b_1(B_3 - b_3) - (C_3 - c_3) \\ c_2(A_3 - a_3) + c_1(B_3 - b_3) \end{pmatrix}.$$

Since $D' = (h_1) - (D_1 + D_2)$ is a normal divisor with the pole degree 3, we have a unique polynomial $v_1 \in K[X, Y]$ with $\mathrm{LT}(v_1) = X^2$ such that $v_1 h_i \in \langle h_1, F \rangle$ for all $h_i \in H$.

$\{h_1, F\}$ is a Groebner basis for $\langle h_1, F\rangle$ since $\mathrm{lcm}(\mathrm{LM}(h_1), \mathrm{LM}(F)) = \mathrm{LM}(h_1)\mathrm{LM}(F)$. For the polynomials $v_1, q_{2,1}, q_{2,2}, q_{3,1}, q_{3,2} \in K[X, Y]$ such that

$$\begin{aligned} v_1 h_2 &= q_{2,1} h_1 + q_{2,2} F, \\ v_1 h_3 &= q_{3,1} h_1 + q_{3,2} F \end{aligned}$$

with $\mathrm{LT}(v_1) = X^2, \mathrm{LT}(q_{2,1}) = XY, \mathrm{LM}(q_{2,2}) \leq X, \mathrm{LT}(q_{3,1}) = Y^2, \mathrm{LM}(q_{3,2}) \leq Y$, we have $G = \{v_1, v_2 = q_{2,1} - c_{2,1} v_1, v_3 = q_{3,1} - c_{3,2} v_2 - c_{3,1} v_1\}$, where $c_{2,1}$ is the coefficient of X^2 in $q_{2,1}$ and $c_{3,1}, c_{3,2}$ are the coefficients of X^2, XY in $q_{3,1}$, respectively.

Example

Let C be a C_{34} curve defined over $F_{11} = Z/11Z$ by

$$F(X, Y) = Y^3 + X^4 + 1.$$

Let D_1, D_2 be the normal divisors with the reduced Groebner bases G_1, G_2 for their normal ideals, respectively:

$$\begin{aligned} G_1 &= \{f_1 = X^2 + 8Y + 9X + 9, f_2 = XY + 4Y + 9X + 8, f_3 = Y^2 + 9Y + 9X + 1\}, \\ G_2 &= \{g_1 = X^2 + 10Y + 7X + 7, g_2 = XY + 2Y + 4X + 6, g_3 = Y^2 + 7Y + 9X + 2\}. \end{aligned}$$

Then $\langle f_1, f_2, f_3, f_1 - g_1, f_2 - g_2, f_3 - g_3\rangle = \langle 1\rangle$. For G_1 and G_2, we have

$$M(G_1, G_2) = \begin{pmatrix} 9 & 2 & 2 \\ 2 & 5 & 0 \\ 2 & 2 & 10 \end{pmatrix} \quad \text{with} \quad \det M(G_1, G_2) \neq 0.$$

Thus the elements of H are

$$\begin{aligned} h_1(X, Y) &= (X + k_1) f_1 + k_2 f_2 + k_3 f_3, \\ h_2(X, Y) &= k_4 f_1 + (X + k_5) f_2 + k_6 f_3, \\ h_3(X, Y) &= k_7 f_1 + k_8 f_2 + (X + k_9) f_3 \end{aligned}$$

and the remainder of $F(X, Y)$ on division by $\{h_1(X, Y), h_2(X, Y), h_3(X, Y)\}$ for

$$\begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} = \begin{pmatrix} 6 \\ 5 \\ 9 \end{pmatrix}, \quad \begin{pmatrix} k_4 \\ k_5 \\ k_6 \end{pmatrix} = \begin{pmatrix} 6 \\ 8 \\ 3 \end{pmatrix}, \quad \begin{pmatrix} k_7 \\ k_8 \\ k_9 \end{pmatrix} = \begin{pmatrix} 1 \\ 8 \\ 6 \end{pmatrix}.$$

It follows that

$$\begin{aligned} h_1 &= X^3 + 9Y^2 + 2XY + 4X^2 + 6Y + 2X + 4, \\ h_2 &= X^2Y + 3Y^2 + XY + 4X^2 + 8Y + 7X, \\ h_3 &= XY^2 + 6Y^2 + 6XY + 10X^2 + 6Y + 4X + 2. \end{aligned}$$

From

$$\begin{aligned} v_1 h_2 &= q_{2,1} h_1 + q_{2,2} F, \\ v_1 h_3 &= q_{3,1} h_1 + q_{3,2} F \end{aligned}$$

with $\mathrm{LM}(v_1) = X^2, \mathrm{LT}(q_{2,1}) = XY, \mathrm{LM}(q_{2,2}) \leq X, \mathrm{LT}(q_{3,1}) = Y^2, \mathrm{LM}(q_{3,2}) \leq X$, we have

$$\begin{aligned} v_1 &= X^2 + 3Y + 10X + 10, \\ q_{2,1} &= XY + 9X^2 + 3X + 6, \\ q_{2,2} &= 2X + 9, \\ q_{3,1} &= Y^2 + 9XY + 3X^2 + 8Y + 3X + 9, \\ q_{3,2} &= 2Y + 8X + 6. \end{aligned}$$

It follows that

$$G = \{v_1 = X^2 + 3Y + 10X + 10, v_2 = XY + 6Y + X + 4, v_3 = Y^2 + 8X + 9\}.$$

Bibliography

[1] L. M. Adleman, J. DeMarrais and M. D. Huang, *A subexponential Algorithm for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields,* Algorithmic Number Theory, 28–40, Lecture Notes in Comput. Sci. 877, Springer-Verlag, Berlin, 1994.

[2] S. Arita, *Algorithms for computation in Jacobian group of C_{ab} curve and their application to discrete-log-based public key cryptosystems,* The mathematics of public key cryptography, Fields Institute A. Odlyzko et al (eds.), 1999.

[3] D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve,* Math. Comp. 48 (1987), 95–101.

[4] D. G. Cantor, *On the analogue of the division polynomials for hyperelliptic curves,* J. Reine Angew. Math. 447 (1994), 91–145.

[5] D. Cox, J. Little and D. O'shea, *Ideals, Varieties, and Algorithms,* Springer-Verlag, Berlin, 1997.

[6] W. Fulton, *Algebraic Curves,* Benjamin, New York, 1969.

[7] S. D. Galbraith, S. M. Paulus and N. P. Smart, *Arithmetic on Superelliptic Curves,* Math. Comp. 71 (2002), 393–405.

[8] V. D. Goppa, *Geometry and Codes,* Kluwer Academic Publishers, 1988.

[9] R. Harley, *adding.text,* http://cristal.inria.fr/~harley/hyper/, 2000.

[10] R. Harley, *doubling.c,* http://cristal.inria.fr/~harley/hyper/, 2000.

[11] R. Hartshorne, *Algebraic Geometry,* Springer-Verlag, 1977.

[12] M. -D. Huang and D. Ierardi, *Efficient algorithms for the effective Riemann-Roch problem and for addition in the Jacobian of a curve,* J. Symbolic Comp. 18 (1994), 519–539.

[13] H. Kim, J. Cheon and S. Hahn, *Elliptic curve lifting problem and its applications,* Proc. Japan Acad. 75 Ser. A (1999), 166–168.

[14] N. Koblitz, *Elliptic Curve Cryptosystems,* Math. Comp. 48 (1987), 203–209.

[15] N. Koblitz, *Hyperelliptic cryptosystems,* J. Cryptology 1 (1989), 139–150.

[16] N. Koblitz, *A course in number theory and cryptography,* 2nd ed., Grad. Texts in Math. 114, Springer-Verlag, New York, 1994.

[17] N. Koblitz, *Algebraic Aspects of Cryptograph,* Springer-Verlag, 1998.

[18] R. Matsumoto, *The Cab curve - a generalization of the Weierstrass form to arbitrary plane curves,* http://www.rmatsumoto.org/cab/html.

[19] K. McCurley, *The Discrete Logarithm Problem* (Boulder, CO, 1989), 49–74, Proc. Sympos. Appl. Math. 42, Amer. Math. Soc., Proridence, RI, 1990.

[20] A. Menezes, *Elliptic Curve Public Key Cryptosystems,* Kluwer Acad. Publ., 1993.

[21] A. Menezes, T. Okamoto and S. A. Vanstone, *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field,* IEEE Trans. Inform. Theory 39 (1993), 1639–1646.

[22] V. Miller, *Uses of elliptic curves in cryptography,* Advances in Cryptology-Proc. Crypto '85 (Santa Barbara, Calif., 1985), 417–426, Lecture Notes in Comput. Sci. 218, Springer-Verlag, New York, 1986.

[23] S. Miura, *Algebraic geometric codes on certain plane curves,* Trans. IEICE **J75-A** (1992), 1735–1745 (Japanese).

[24] S. Miura, *Linear codes on affine algebraic curves,* Trans. IEICE **J81-A** (1998), 1398–1421 (Japanese).

[25] Y. Morita, *Seisuron,* Tokyo Univ. Press, 1999 (Japanese).

[26] D. Mumford, *Abelian Varieties,* Oxford Univ. Press, London, 1970.

[27] D. Mumford, *Curves and their Jacobians,* Michigan Univ. Press, Ann Arbor, Mich., 1975.

[28] D. Mumford, *Teta Lectures on Theta II,* Progr. Math. 43, Birkhäuser, Boston, Inc., Boston, MA, 1984.

[29] R. Pellikaan, *On the existence of order functions,* J. Statist. Plann. Inference 94 (2001), 287–301.

[30] H. -G. Ruck, *On the discrete logarithm in the divisor class group of curves,* Math. Comp. 68 (1999), 805–806.

[31] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p,* Math. Comp. 44 (1985), 483–494.

[32] R. Schoof, *Counting points on elliptic curves over finite fields,* J. Théor. Nombres Bordeaux 7 (1995), 219–254.

[33] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Grad. Texts in Math. 106, Springer-Verlag, New York, 1986.

[34] J. H. Silverman, *The xedin calculus and the elliptic curve discrete logarithm problem,* Des. Codes Cryptogr. 20 (2000), 5–40.

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

[36] J. T. Tate, *The Arithmetic of Elliptic Curves,* Invent. Math. 23 (1974), 179–206.

[37] E. J. Volcheck, *Computing in the Jacobian of a plane algebraic curve,* ANTS-I (Ithaca, NY, 1994), 221–233, Lecture Notes in Comput. Sci. 877, Springer-Verlag, Berlin, 1994.

Tohoku Mathematical Publications

No.1 Hitoshi Furuhata: *Isometric pluriharmonic immersions of Kähler manifolds into semi-Euclidean spaces*, 1995.

No.2 Tomokuni Takahashi: *Certain algebraic surfaces of general type with irregularity one and their canonical mappings*, 1996.

No.3 Takeshi Ikeda: *Coset constructions of conformal blocks*, 1996.

No.4 Masami Fujimori: *Integral and rational points on algebraic curves of certain types and their Jacobian varieties over number fields*, 1997.

No.5 Hisatoshi Ikai: *Some prehomogeneous representations defined by cubic forms*, 1997.

No.6 Setsuro Fujiié: *Solutions ramifiées des problèmes de Cauchy caractéristiques et fonctions hypergéométriques à deux variables*, 1997.

No.7 Miho Tanigaki: *Saturation of the approximation by spectral decompositions associated with the Schrödinger operator*, 1998.

No.8 Y. Nishiura, I. Takagi and E. Yanagida: *Proceedings of the International Conference on Asymptotics in Nonlinear Diffusive Systems — towards the Understanding of Singularities in Dissipative Structures —*, 1998.

No.9 Hideaki Izumi: *Non-commutative L^p-spaces constructed by the complex interpolation method*, 1998.

No.10 Youngho Jang: *Non-Archimedean quantum mechanics*, 1998.

No.11 Kazuhiro Horihata: *The evolution of harmonic maps*, 1999.

No.12 Tatsuya Tate: *Asymptotic behavior of eigenfunctions and eigenvalues for ergodic and periodic systems*, 1999.

No.13 Kazuya Matsumi: *Arithmetic of three-dimensional complete regular local rings of positive characteristics*, 1999.

No.14 Tetsuya Taniguchi: *Non-isotropic harmonic tori in complex projective spaces and configurations of points on Riemann surfaces*, 1999.

No.15 Taishi Shimoda: *Hypoellipticity of second order differential operators with sign-changing principal symbols*, 2000.

No.16 Tatsuo Konno: *On the infinitesimal isometries of fiber bundles*, 2000.

No.17 Takeshi Yamazaki: *Model-theoretic studies on subsystems of second order arithmetic*, 2000.

No.18 Daishi Watabe: *Dirichlet problem at infinity for harmonic maps*, 2000.

No.19 Tetsuya Kikuchi: *Studies on commuting difference systems arising from solvable lattice models*, 2000.

No.20 Seiki Nishikawa: *Proceedings of the Fifth Pacific Rim Geometry Conference*, 2001.

No.21 Mizuho Ishizaka: *Monodromies of hyperelliptic families of genus three curves*, 2001.

No.22 Keisuke Ueno: *Constructions of harmonic maps between Hadamard manifolds*, 2001.

No.23 Hiroshi Sato: *Studies on toric Fano varieties*, 2002.

No.24 Hiroyuki Kamada: *Self-dual Kähler metrics of neutral signature on complex surfaces*, 2002.

No.25 Reika Fukuizumi: *Stability and instability of standing waves for nonlinear Schrödinger equations*, 2003.

No.26 Tôru Nakajima: *Stability and singularities of harmonic maps into spheres*, 2003.

No.27 Yasutsugu Fujita: *Torsion of elliptic curves over number fields*, 2003.

No.28 Shin-ichi Ohta: *Harmonic maps and totally geodesic maps between metric spaces*, 2004.

No.29 Satoshi Ishiwata: *Geometric and analytic properties in the behavior of random walks on nilpotent covering graphs*, 2004.

No.30 Soondug Kim: *Computing in the Jacobian of a C_{34} curve*, 2005.

Tohoku Mathematical Publications

Mathematical Institute
Tohoku University
Sendai 980-8578, Japan