GROEBNER BASIS AND ITS APPLICATIONS

By

Solomon Belete

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
AT
ADDIS ABABA UNIVERSITY
ADDIS ABABA, ETHIOPIA
JUNE 2012

ADDIS ABABA UNIVERSITY
DEPARTMENT OF MATHEMATICS

The undersigned hereby certify that they have read and recommend to the School of Graduate Studies for acceptance a thesis entitled "**Groebner Basis and its Applications**" by **Solomon Belete** in partial fulfillment of the requirements for the degree of **Master of Science**.

Dated: June 2012

Advisor: _____
Berhanu Bekele(PhD)

Examiners: _____
Seyoum Getu(PhD)

_____
Tilahun Abebaw(PhD)

ADDIS ABABA UNIVERSITY

Date: **June 2012**

Author: **Solomon Belete**

Title: **Groebner Basis and its Applications**

Department: **Department of Mathematics**

Degree: **M.Sc.** Convocation: **June** Year: **2012**

Signature of Author

To Mam and Dad.

Table of Contents

Table of Contents **v**

Abstract **vii**

Acknowledgements **viii**

Introduction **1**

1 Basic Theory Of Groebner Basis **3**
1.1 Preliminaries 3
1.2 Monomial orderings and Division Algorithm 6
1.3 Groebner Basis 9
1.4 S-polynomials and Bucheberger's Algorithm 11
1.5 Reduced Groebner basis 17
1.6 Improvements on Buchberger's Algorithm 20

2 Groebner basis over a Ring **25**
2.1 Basic concepts of Module 25
2.2 Groebner basis and Syzygies 32
2.3 Computation of the Syzygy module 37
2.4 Improvement on Buchberger's Algorithms by using Syzygies 42
2.5 Groebner basis over ring 53
2.6 Computing Groebner basis over a ring 56

3 Application of Groebner Basis **64**
3.1 Elementary Applications of Groebner Basis 64
3.1.1 Ideal Membership Problem 64
3.1.2 Quotients of Polynomial Rings 65

3.1.3 Algorithmic computations in $K[x_1, \ldots, x_n]/I$ 66
3.2 Basic Algorithms In Ideal Theory 70
3.2.1 Elimination Theorem 70
3.2.2 Intersection of Ideals 71
3.2.3 Colon Ideals 74
3.2.4 Saturation Ideals 75
3.3 Hilbert Nullstellensatz 77
3.4 Polynomial Maps 87
3.5 Some Application to Algebraic Geometry 96
3.5.1 Zariski Closure 96
3.5.2 Implicitization 97
3.6 Minimal Polynomials Of Elements In Field Extensions 103
3.7 Radicals of Zero-Dimensional Ideals 107
3.8 The k-Color Problem 112

Bibliography **117**

Abstract

In this thesis we present the basic concepts and results of Groebner basis for a polynomial ideal over a field and introduce an algorithm for computing and then present an improvement of Buchberger's algorithms for computing Groebner basis by reducing number of S-polynomials without computing them. This paper deals with Groebner basis for a polynomial ideal over a ring by defining the module of a solution of a homogenous linear equation with polynomial coefficients (called the syzygy module).

And finally, we will see the application of Groebner basis in detail.

Acknowledgements

First of all, I am grateful to my thesis advisor Dr.Birhanu Bekele for giving the opportunity to do this thesis and his invaluable assistance,suggestion and comment during this work.

Special thanks go to my best friend Getachew Muhabie,he is like brother for me, for his support and encouragement in this work.

My special gratitude to my father and mother for their end less support through out my life.

I would like to express my special gratitude and love for my sister Hana and my girl friend Fetlework for their support and encouragement through out my two year study.

I wish to thank the following: Ayenew, Daniel, Hannibal, , Solomon and Yonas for their support and for all of them whom i did not mention here.

Addis Ababa, Ethiopia Solomon Belete
June 11, 2012

Introduction

This MSc in Mathematics thesis deals with concepts related to Groebner bases theory and its application in commutative algebra and algebraic geometry.
The algorithmic theory of Groebner bases was introduced in 1965 by Bruno Buchberger in his PhD thesis. He named the basis after his PhD advisor, Wolfgang Groebner (1899-1980).A problem of particular interest was the development of algorithms for computing Groebner bases.
This report is structured into three main chapters, i.e.:

- Chapter 1, *Basic theory of Groebner basis*: we first recall the concepts of polynomials, ideals, monomial orders and polynomial division. Next we introduce Groebner basis and the way how to compute by using S-polynomials ,Buchberger's algorithm and the improved buchberger's algorithm.

- Chapter 2, *Groebner basis over a ring*: this chapter deals about Groebner basis over a Noetherian ring. In particular,we use the theory of "syzygy" for computing Groebner basis and also use this syzygy concept for the improvement of Buchberger's algorithm.

- Chapter 3,*Application of Groebner basis*:this chapter present the basic applications to commutative algebra and elementary algebraic geometry and at last we present special topic in graph theory which is vertex coloring.

The main aim of this paper is to introduce Basic theory of Groebner basis over a field and Noetherian ring . And since Groebner basis has vast application in many disciplines, we restrict the scope to commutative algebra and algebraic geometry.

Chapter 1

Basic Theory Of Groebner Basis

In this chapter, we will first recall some concepts on polynomials, ideals.We will then discuss monomial orders and polynomial division, and we will conclude the chapter dealing with basic theory on Groebner bases and Buchberger's algorithm and its improvement.

1.1 Preliminaries

Let us first define monomials and polynomials

Definition 1.1.1. [6] *A monomials in $x_1, x_2, \ldots, x_n$ is a product of the form*

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ non-negative integers. The total degree of this monomial is the sum $\alpha_1 + \alpha_2 + \cdots + \alpha_n$.

We can simplify the notation for monomials as follows Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be n-tuples of non-negative integers then ,we set

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

We let $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ denote the total degree of the monomial x^α.

Definition 1.1.2. [6] *A polynomial f in $x_1, \ldots, x_n$ with coefficient in a field K is a finite linear combination (with coefficients in K) of monomials. We will write polynomials in the form*

$$f = \sum_{\alpha} a_\alpha x^\alpha$$

where $a_\alpha \in K$, where the sum is over a finite number of n- tuples $\alpha = (\alpha_1, \ldots, \alpha_n) \in Z_{n_{\geq 0}}$.

The set of all polynomials in $x_1, \ldots, x_n$ with coefficients is K is denoted in $K[x_1, \ldots, x_n]$.

In the following definition, we introduce a terminology which we use when dealing with polynomials.

Definition 1.1.3. [6] *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $K[x_1, \ldots, x_n]$*

1. *We call a_α the coefficient of the monomial x^α.*
2. *If a_α is non zero, then we call $a_\alpha x^\alpha$ a term of f.*
3. *The total degree of f, denoted deg (f), is the maximum $|\alpha|$ such that the coefficient of x^α is non-zero.*

Example 1.1.4. *$x^3y + x^2 + y$ is a polynomial in $\mathbb{F}_2[x, y]$ with three terms and total degree of four.*

One can show that ,under addition and multiplication $K[x_1, \ldots, x_n]$ satisfies all the field axioms ,except for the existence of multiplicative inverse,for example there is no multiplicative inverse for x_1,as $\dfrac{1}{x_1}$ is not polynomial , such a mathematical structure is called a commutative ring ,and that is why we usually refer to $K[x_1, \ldots, x_n]$ as polynomial ring.

Let us define the following algebraic objects,

Definition 1.1.5. [6] *A subset I of $K[x_1, \ldots, x_n]$ is an ideal if it satisfies*

1. $0 \in I$.
2. *If $f, g \in I$,then $f + g \in I$.*
3. *If $f \in I$ and $h \in K[x_1, \ldots, x_n]$,then $hf \in I$.*

Let us introduce a first example of an ideal.

Definition 1.1.6. [6] *Let $f_1, \ldots, f_s$ be polynomials in $K[x_1, \ldots, x_n]$, we set*

$$\langle f_1, \ldots, f_s \rangle = \{\sum_{i=1}^{s} h_i f_i, | h_1, ...h_s \in K[x_1, \ldots, x_n]\}$$

Let us introduce the concept of ideal generated by $f_1, \ldots, f_s$.

Lemma 1.1.7. [6] *If $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, then $\langle f_1, \ldots, f_s \rangle$ is an ideal of $K[x_1, \ldots, x_n]$. We call $\langle f_1, \ldots, f_s \rangle$ the ideal generated by $f_1, \ldots, f_s$.*

Now we turn our attention to the **Hilbert's basis theorem**, this result is crucial in everything we will be doing throughout this work.It guarantees the termination of our algorithms we have seen in the future.

Theorem 1.1.8. ***(Hilbert's basis theorem)*** [1] *In the ring $K[x_1, \ldots, x_n]$ we have the following*

1. *If I is any ideal of $K[x_1, \ldots, x_n]$,then there exist a polynomial $f_1, \ldots, f_s$ in $K[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \rangle$*
2. *Let $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_s \subseteq \cdots$ is an ascending chain of ideal of in $K[x_1, \ldots, x_n]$ then there exist N such that $I_N = I_{N+1} = I_{N+2} = \cdots$*

1.2 Monomial orderings and Division Algorithm

Let us first note that we can reconstruct the monomial $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ from the n-tuples of exponents $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq}^n 0$. We then have a one-to-one correspondence between the monomial in $K[x_1, \ldots, x_n]$ and $\mathbb{Z}_{\geq 0}^n$.

Moreover any ordering $>$ we establish on the space will give us an ordering on monomials: If $\alpha > \beta$ according to this ordering we will also say that $x^\alpha > x^\beta$.

Since a polynomial is a sum of monomials ,we would like to able to arrange the terms in a polynomials in certain order either in ascending or descending order in unambiguous way. In order to do this ,we must be able to compare every pair of monomials to establish their proper relative position,by doing so,we require our ordering to to be linear or total ordering, i.e for every pair of monomials x^α and x^β, just one of the following statements should be true $x^\alpha > x^\beta, x^\alpha = x^\beta, x^\beta > x^\alpha$.

Concerning the ordering,the sum operation on polynomials presents no problems while the multiplication is a bit more tricky ,as the leading term in the product could be different from the product of the monomials and the leading term of the orginal polynomial(**Remark**:we will introduce formally the concept of the leading term in a while ,basically we will define it as the biggest monomial with associated cofficients according to a certain ordering we assume).

We will then require that all the monomial orderings have the following additional property: If $x^\alpha > x^\beta$ and x^γ is any monomial where $\gamma \in \mathbb{Z}_{\geq}^n 0$,then $x^\alpha + x^\gamma > x^\beta + x^\gamma$.

with the above in mind ,we introduce the following

Definition 1.2.1. [6] *A monomial ordering $>$ on $K[x_1, \ldots, x_n]$ is any relation $>$ on $\mathbb{Z}_{\geq 0}^n$ or equivalently,any relation on the set of monomials $x^\alpha, \alpha \in \mathbb{Z}_{\geq 0}^n$,satisfying :*

1. *$>$ is total ordering on $\mathbb{Z}_{\geq 0}^n$*
2. *If $\alpha > \beta$ and $\gamma \in \mathbb{Z}_{\geq 0}^n$ then $\alpha + \gamma > \beta + \gamma$*

3. $>$ *is a well ordering on* $\mathbb{Z}^n_{\geq 0}$*.this means that every non-empty subset of* $\mathbb{Z}^n_{\geq 0}$ *has a smallest element under* $>$*.*

We will now introduce three examples of monomial orderings namely the lexicographic order,the graded lexicographic order and the graded reverse lexicographic order.

Definition 1.2.2. *(**Lexicographic order**)* [6] *Let* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$ *,we say* $\alpha >_{lex} \beta$ *if ,in the vector difference* $\alpha - \beta \in \mathbb{Z}^n$ *the left most non zero entry is positive ,we will write* $x^\alpha >_{lex} x^\beta$ *if* $\alpha >_{lex} \beta$

In practice ,when we work with polynomials in up to three variables ,we will call the variables x, y, z instead x_1, x_2, x_3. We will again assume,unless differently stated that the alphabetical order $x > y > z$ on the variables is used to define the lexicographic ordering as consequence when dealing with n variables ,we have that $x_1 > x_2 > \cdots > x_n$.

Example 1.2.3. 1. $\alpha = (1, 2, 0) >_{lex} \beta = (0, 3, 4)$ *since* $\alpha - \beta = (1, -1, 4)$

2. $\alpha = (3, 2, 4) >_{lex} \beta = (3, 2, 1)$ *since* $\alpha - \beta = (0, 0, 3)$.

Definition 1.2.4. *(**Graded lexicographic order**)* [6] *Let* $\alpha, \beta \in \mathbb{Z}^n_{\geq_0}$*,We say* $\alpha >_{grlex} \beta$ *if* $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ *or* $|\alpha| = |\beta|$ *and* $\alpha >_{lex} \beta$*.*

We see that grlex order by total degree first ,then "break ties" using lex order.

Example 1.2.5. 1. $(1, 2, 3) >_{grlex} (3, 2, 0)$ *since* $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$

2. $(1, 2, 4) >_{grlex} (1, 1, 5)$ *since* $|(1, 2, 4)| = |(1, 1, 5)|$ *and*
   $(1, 2, 4) >_{lex} (1, 1, 5)$

Definition 1.2.6. *(**Graded Reverse lex order**)* [6] *Let* $\alpha, \beta \in \mathbb{Z}^n_{\geq_0}$*,*
we say $\alpha >_{grevlex} \beta$*,If* $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ *or* $|\alpha| = |\beta|$ *and the right most non zero entry of* $\alpha - \beta \in Z^n$ *is negative.*

Like grlex,grevlex orders by total degree, but it "break ties " in different way.

Example 1.2.7. 1. $(4,7,1) >_{grevlex} (4,2,3)$ *since* $|(4,7,1)| = 12 > |(4,2,3)| = 9$

2. $(1,5,2) >_{grevlex} (4,1,3)$ *since* $|(1,5,2)| = |(4,3,1)|$ *and* $(1,5,2) - (4,1,3) = (-3,4,-1)$.

Let us introduce the following definition.

Definition 1.2.8. [6] *Let* $f = \sum_\alpha a_\alpha x^\alpha$ *be non zero polynomial in* $K[x_1,\ldots,x_n]$ *and let* $>$ *be a monomial order*

1. *The multidegree of f is multideg(f)* $= max(\alpha \in \mathbb{Z}^n_{\geq_0} : a_\alpha \neq 0)$ *(The maximum is taken with respect to* $>$ *)*
2. *The leading coefficient of* f *is* $lc(f) = a_{multideg(f)} \in K$
3. *The leading monomial of* f *is* $lm(f) = X^{multideg(f)}$ *(with coefficient 1)*
4. *The leading term of* f *is* $lt(f) = lc(f)lm(f)$

Example 1.2.9. *Let* $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ *then let* $>$ *denote lex order then*
$multideg(f) = (5,1,4)$
$lc(f) = -3$
$lm(f) = x^5yz^4$
$lt(f) = -3x^5yz^4$

Theorem 1.2.10. ***(Division algorithm**)* [1] *Given a set of non-zero polynomials* $F = \{f_1,\ldots,f_s\}$ *and* f *in* $K[x_1,\ldots,x_n]$ *the division algorithm produce a polynomials* $u_1,\ldots,u_s,r \in K[x_1,\ldots,x_n]$ *such that*

$$f = u_1f_1 + \cdots + u_sf_s + r$$

with r *is reduced with respect F,i.e* $r = 0$ *or no power product that appears in* r *is divisible by any one of the* $lm(f_i), i = (1,2,\ldots,s)$ *and*

$$lm(f) = max(max_{1\leq i\leq s}(lm(u_i)lm(f_i)), lm(r))$$

1.3 Groebner Basis

In this section I finally see the fundamental object of this work namely Groebner basis.

Definition 1.3.1. [1] *A set of non-zero polynomial $G = \{g_1, \ldots, g_t\}$ contained in an ideal I is called a Groebner basis for I if and only if for all $f \in I$ such that $f \neq 0$ there exists $i \in \{1, \ldots, t\}$ such that $lm(g_i)$ divides $lm(f)$.*

This definition tells us that if G is Groebner basis for an ideal I, then there is no non-zero polynomial in I reduced with respect to G.

Theorem 1.3.2. [1] *Let I be non-zero ideal of $K[x_1, \ldots, x_n]$, The following statement are equivalent for a set of non zero polynomials $G = \{g_1, \ldots, g_t\} \subseteq I$*

1. *G is a Groebner basis for I.*
2. *$f \in I$ if and only if $f \xrightarrow{G}_+ 0$*
3. *$f \in I$ if and only if $f = \sum_{i=1}^{t} h_i g_i$ with $lm(f) = max_{1 \leq i \leq t}(lm(h_i)lm(g_i))$*
4. *$\langle lt(G) \rangle = \langle lt(I) \rangle$*

Proof. (1)⇒(2) Let $f \in K[x_1, \ldots, x_n]$,by Theorem 1.2.10, there exists $r \in K[x_1, \ldots, x_n]$, reduced with respect to G,such that $f \xrightarrow{G} +r$,thus $f - r \in I$ and so $f \in I$ if and only if $r \in I$.Clearly $r = 0$ (that is,$f \xrightarrow{G}_+ 0$),then $f \in I$.
Conversly if $f \in I$ and $r \neq 0$ then $r \in I$ and by (1),there exists $i \in \{1, 2, \ldots, t\}$ such that $lm(g_i)$ divides $lm(r)$,but this contradicts to the fact r is reduced with respect to G.thus $r = 0$ and $f \xrightarrow{G}_+ 0$.
(2)⇒(3).For $f \in I$,we know that by hypothesis $f \xrightarrow{G}_+ 0$,and since the process of reduction is exactly the same as the Division Algorithm,we see that (3) follows from Theorem 1.2.10 .
(3)⇒(4).Clearly, $\langle lt(G) \rangle \subseteq \langle lt(I) \rangle$. For the reverse inclusion it suffices to show that for all $f \in I$, $lt(f) \in \langle lt(G) \rangle$, since the $lt(f)'s$ generate $\langle lt(I) \rangle$.
Writing f as in the hypothesis, it immediately follows that

$$lt(f) = \sum_i lt(h_i)lt(g_i)$$

where the sum is over all i such that $lm(f) = lm(h_i)lm(g_i)$. The result follows immediately.
(4)⇒(1).Let $f \in I$. Then $lt(f) \in \langle lt(G)\rangle$, and hence

$$lt(f) = \sum_{i=1}^{t} h_i lt(g_i) \tag{1.3.1}$$

for some $h_i \in K[x_1, \ldots, x_n]$. If we expand the right-hand side of Equation (1.3.1), we see that each term is divisible by some $lm(g_i)$.
Thus $lt(f)$, the only term in the left-hand side, is also divisible by some $lm(g_i)$, as desired. □

Corollary 1.3.3. [1]*If $G = \{g_1, \ldots, g_t\}$ is a Groebner basis for the ideal I, then $I = \langle g_1, g_2, \ldots, g_t\rangle$.*

Proof. Clearly $\langle g_1, \ldots, g_t\rangle \subseteq I$,since each g_i is in I. For the reverse inclusion, let $f \in I$. By *Theorem 1.3.2*, $f \xrightarrow{G}_+ 0$, and hence $f \in \langle g_1, \ldots, g_t\rangle$. □

Corollary 1.3.4. [1] *Every non-zero ideal I of $K[x_1, \ldots, x_n]$ of has a Grobner basis.*

Proof. Let $\langle lt(I)\rangle = \{\langle lt(f)\rangle)|f \in I\}$
Let $g \in \langle lt(I)\rangle$,then every term of g is divisible by some $lt(f)$,where $f \in I$.
By Hilbert's basis theorem,$\langle lt(I)\rangle$ is generated by finitely many $g_1, \ldots, g_k$ in $K[x_1, x_2, \ldots, x_n]$.
Since for all $i \in \{1, 2, \ldots, k\}$, $g_i \in \langle lt(I)\rangle$,then every term of g_i is divisible by $lt(f)$ for some $f \in I$.As a result, we obtain a finite set of monomials $X_1, \ldots, X_t$ in $K[x_1, \ldots, x_n]$ which generate the ideal $\langle lt(I)\rangle$.
These monomials are the leading terms of f where $f \in I$,then by (4) of Theorem 1.3.2, I has Groebner basis. □

Since Every non-zero ideal I of $K[x_1, \ldots x_n]$ has a Groebner basis and using the conditions given in the above theorem,we can detect whether a given basis is a Groebner basis for an ideal I.

Proposition 1.3.5. [1] *Let $\{g_1, \ldots, g_t\}$ is a Groebner basis for the ideal I in $K[x_1, \ldots, x_n]$ and f be a polynomial in $K[x_1, \ldots, x_n]$ then there exists a unique r in $K[x_1, \ldots, x_n]$ such that*

1. *r is completely reduced with respect to G*

2. *there is* $g \in K[x_1, \ldots, x_n]$ *such that* $f = g + r$

Proof. The division algorithm gives $f = h_1 g_1 + \cdots + h_t g_t + r$,where r satisfies(1). We can also satisfy (2) by setting $g = h_1 g_1 + \cdots + h_t g_t \in I$. This proves the existence of r.
To prove uniqueness, suppose that $f = g + r = g_o + r_o$ satisfy (1) and (2).
Then $r - r_o = g_o - g \in I$. So that if $r = r_o$, then $lt(r - r_o) \in \langle lt(I) \rangle = \langle lt(g_1), lt(g_2), \ldots, lt(g_t) \rangle$. then it follows that $lt(r - r_o)$ is divisible by some $lt(g_i)$. This is impossible since no term of r, r_o is divisible by one of $lt(g_1), lt(g_2), \ldots, lt(g_t)$. Thus $r - r_o$ must be zero, and uniqueness is proved.
The final part of the proposition follows from the uniqueness of r. □

In particular,r is the remainder on division of f by G,no matter how the elements of G are listed ,when the Division algorithm (bear in mind that the "quotients" h_i produced by the algorithm in $f = h_1 g_1 + \cdots + h_t g_t + r$ may change if we rearrange the $g_i's$.)

1.4 S-polynomials and Bucheberger's Algorithm

We have seen that every non-zero polynomial ideal I of $K[x_1, \ldots, x_n]$ has a Groebner basis but we have not yet seen any of the strategies how to compute Groebner bases. So we can ask the questions that given an ideal $I \subseteq K[x_1, \ldots, x_n]$, then how can we construct a Groebner basis for I?

Answering this question lead us to come up with Buchberger's algorithm and the use of S-polynomials in computing Groebner basis.

Definition 1.4.1. [1] *Fix a monomial order,let f and g be two polynomials in* $K[x_1, \ldots, x_n]$ *and let* $L = lcm(lm(f), lm(g))$.
The S-polynomial of f *and* g *is*

$$S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g$$

Since $\frac{L}{lt(f)}$ and $\frac{L}{lt(g)}$ are monomials ,then $S(f,g)$ belongs to the same ideal to which f and g belongs.

S-polynomials are constructed to cancel $lt(f)$ and $lt(g)$.In fact the two terms from the S-polynomials obtained from f and g, are equal and cancel each other.

We illustrate this with an example below

Example 1.4.2. *Let* $f = 3x^2yz - xy^3$ *and* $g = xy^2 + z^2$ *in* $Q[x,y,z]$ *with lex order* $x > y > z$
Then $lt(f) = 3x^2yz, lm(f) = x^2yz, lt(g) = xy^2, lm(g) = xy^2$ *and*
$L = lcm(lm(f), lm(g)) = x^2y^2z$
Then

$$\begin{aligned} S(f,g) &= \frac{x^2y^2z}{3x^2yz}[3x^2yz - xy^3] - \frac{x^2y^2z}{xy^2}[xy^2 + z^2] \\ &= \frac{1}{3}y[3x^2yz - xy^3] - xz[xy^2 + z^2] \\ &= \underbrace{x^2y^2z} - \frac{1}{3}xy^4 - \underbrace{x^2y^2z} - xz^3 \\ &= -\frac{1}{3}xy^4 - xz^3 \end{aligned}$$

Here we see that the underbraced elements cancelled each other.

We have seen that the S-polynomials was introduced as a means to cancel the leading terms but here we can further use the practical concepts of S-polynomials to compute Groebner basis.

Before proving the main theorem we need this preliminary Lemma.

Lemma 1.4.3. [1] *Let* $f_1, \ldots, f_s \in K[x_1, \ldots x_n]$ *be such that* $lm(f_i) = X \neq 0$ *for all i=1,2,...,s.let* $f = \sum_{i=1}^{s} c_i f_i$ *with* $c_i \in K, i = 1, 2, \ldots, s$. *If* $lm(f) < X$ *,then f is a linear combination of* $S(f_i, f_j)$ *with coefficients in K* $,1 \leq i < j \leq s$

Proof. Write $f_i = a_iX$+lower terms,$a_i \in K$.Then by hypothesis $\sum_{i=1}^{s} c_i a_i = 0$,since the c_i are in K,Now by definition,$S(f_i, f_j) = \frac{1}{a_i}f_i - \frac{1}{a_j}f_j$,

since $lm(f_i) = lm(f_j) = X$.Thus

$$\begin{aligned} f &= c_1f_1 + \cdots + c_sf_s \\ &= c_1a_1(\frac{1}{a_1}f_1) + \cdots + c_sa_s(\frac{1}{a_s}f_s) \\ &= c_1a_1(\frac{1}{a_1}f_1 - \frac{1}{a_2}f_2) + (c_1a_1 + c_2a_2(\frac{1}{a_2}f_2 - \frac{1}{a_3}f_3) + \\ &+ (c_1a_1 + c_2a_2 + \cdots + c_{s-1}a_{s-1})(\frac{1}{a_{s-1}}f_{s-1} - \frac{1}{a_s}f_s) + (c_1a_1 + \cdots + c_{s-1}a_{s-1} + c_sa_s)(\frac{1}{a_s}f_s) \end{aligned}$$

since $c_1a_1 + \cdots + c_sa_s = 0$ then, the Lemma is required. □

Theorem 1.4.4. ***(Buchberger)*** [1] *Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in $K[x_1, \ldots, x_n]$. Then G is a Groebner basis for the ideal $I = \langle g_1, \ldots, g_t\rangle$ if and only if for all $i \neq j$*

$$S(g_i, g_j) \xrightarrow{G}_+ 0$$

Proof. If $G = \{g_1, \ldots, g_t\}$ is a Groebner basis for $I = \langle g_1, g_2, \ldots, g_t\rangle$,
then $S(g_i, g_j) \xrightarrow{G}_+ 0$,for all $i \neq j$ by (2) Theorem 1.3.2, since $S(g_i, g_j) \in I$.
Conversely, let us assume that $S(g_i, g_j) \xrightarrow{G}_+ 0$ for all $i \neq j$.
We will use (3) of Theorem 1.3.2 to prove that G is a Groebner basis for I.
Let $f \in I$. Then f can be written in many ways as a linear combination of the g_i's.
We choose to write $f = \sum_{i=1}^{t} h_ig_i$ with

$$X = max_{1\leq i\leq t}(lm(h_i)lm(g_i))$$

least(here we use the well-ordering property of the term order).
WTS: $X = lm(f)$.
Suppose the contradiction that $lm(f) < X$.

Let $S = \{i|lm(h_i)lm(g_i) = X\}$.For $i \in S$,Write $h_i = c_iX_i$ +lower terms .
Set $g = \sum_{i\in S} c_iX_ig_i$.Then ,$lm(X_ig_i) = X$,for all i ∈ S, but $lm(g) < X$.
By Lemma 1.4.3 , there exist $d_{ij} \in K$ such that,

$$g = \sum_{i\neq j, i,j\in S} d_{ij}S(X_ig_i, X_jg_j)$$

Now $X = lcm(lm(X_i g_i), lm(X_j g_j))$,so

$$\begin{aligned} S(X_i g_i) &= \frac{X}{lt(X_i g_i)} X_i g_i - \frac{X}{lt(X_j g_j)} X_j g_j \\ &= \frac{X}{lt(g_i)} g_i - \frac{X}{lt(g_j)} g_j \\ &= \frac{X}{X_{ij}} S(g_i, g_j), \end{aligned}$$

Where $X_{ij} = lcm(lm(g_i), lm(g_j))$.By hypothesis $S(g_i, g_j) \xrightarrow{G}_+ 0$,and so we see from this last equation that $S(X_i g_i, X_j g_j) \xrightarrow{G}_+ 0$, This gives a representation

$$S(X_i g_i, X_j g_j) = \sum_{v=1}^{t} h_{ijv} g_v$$

where, by Theorem 1.2.10 ,

$$\begin{aligned} max_{i \leqslant v \leqslant t}(lm(h_{ijv}) lm(g_v)) &= lm(S(X_i g_i, X_j g_j)) \\ &< max(lm(X_i g_i), lm(X_j g_j)) = X \end{aligned}$$

Substituting these expressions into g above, and g into f, we get
$f = \sum_{i=1}^{t} k_i g_i$ with $max_{1 \leq i \leq t}(lm(k_i) lm(g_i)) < X$.This contradicts the minimality of X. Therefore G is a Groebner basis. □

We note that Buchberger's Theorem (Theorem 1.4.4) gives a strategy for computing a Groebner basis ,reduce the S-polynomials and if a remainder is non-zero then add this remainder to the list of polynomials in the generating set ; do this until there are "enough" polynomials to make all S-polynomials reduce to zero.

Theorem 1.4.5. [1] *Given* $F = \{f_1, \ldots, f_s\}$ *with* $f_i \neq 0$, $(1 \leq i \leq s)$, *Buchberger's Algorithm (Algorithm 1.4) will produce Groebner basis for the ideal* $I = \langle f_1, f_2, \ldots, f_s \rangle$

INPUT: $F = \{f_1, \ldots, f_s\} \subseteq K[x_1, \ldots, x_n]$ with $f_i \neq 0, (1 \leq i \leq s)$

OUTPUT:$G = \{g_1, \ldots, g_t\}$,a Groebner basis for $\langle f_1, \ldots, f_s \rangle$

INITIALIZATION : $G = F$, $G' = \{\{f_i, f_j | f_i \neq f_j \in G\}$

WHILE ,$G' \neq \phi$ **DO**

Choose any $\{f, g\} \in G'$

$G' := G' - \{\{f, g\}\}$

$S(f, g) \xrightarrow{G}_{+} h$ where h is reduced with respect to G

If $h \neq 0$ **THEN**

$G' = G' \bigcup \{\{u, h\}\}$ for all $u \in G$

$G = G \bigcup \{h\}$

Algorithm 1.4

Proof. We first need to show that this algorithm terminates.
Suppose to the contrary that the algorithm does not terminate. Then, as the algorithm progresses, we construct a set G_i strictly larger than G_{i-1} and obtain a strictly increasing infinite sequence

$$G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \cdots$$

Each G_i is obtained from G_{i-1} by adding some $h \in I$ to G_{i-1} , where h is the non-zero reduction, with respect to G_{i-1}, of an S-polynomial of two elements of G_{i-1}. Since h is reduced with respect to G_{i-1} , we have that $lt(h) \notin lt(G_{i-1})$. Thus we get

$$lt(G_1) \subsetneq lt(G_2) \subsetneq t(G_3) \subsetneq \cdots$$

This is a strictly ascending chain of ideals which contradicts Theorem 1.1.8 .
Now we have $F \subseteq G \subseteq I$,and hence $I = \langle f_1, \ldots, f_s \rangle \subseteq \langle g_1, \ldots, g_t \rangle \subseteq I$.
Thus G is a generating set for the ideal I.Moreover, if g_i, g_j are polynomials in G,then $S(g_i, g_j) \xrightarrow{G} +0$ by construction.
Therefore G is a Groebner basis for I by Theorem 1.4.4. □

Example 1.4.6. *Find the Groebner basis for the ideal*
$I = \langle f_1 = x^2y + z, f_2 = xz + y\rangle \subseteq Q[x, y, z]$ *with respect to deglex with* $x > y > z$
To find Groebner basis for I *we have to apply the algorithm as follows.*
INITIALIZATION*: We first set* $G = F = \{x^2y+z, xz+y\}$ *and* $G' = \{\{f_1, f_2\}\}$. *This is the first assumed Groebner basis for the ideal for which an S-polynomial is to be computed. After initialising we have to apply the* ***WHILE*** *loop in order to determine the rest elements of the basis.*
Apply the ***WHILE*** *loop :*
$G' \neq \emptyset$. *Then choose* $f_1, f_2 \in G$ *to determine the S-polynomial for these two elements of* G.

$$S(f_1, f_2) \xrightarrow{G}_+ -xy^2 + z^2$$

then since $-xy^2 + z^2 \neq 0$ *then add* $-xy^2 + z^2$ *to* G, *say* $f_3 = -xy^2 + z^2$
then update $G = \{f_1, f_2, f_3\}$ *and* $G' = \{\{f_1, f_3\}, \{f_2, f_3\}\}$
Second ***WHILE*** *loop passes through:*
$G' = \{\{f_2, f_3\}\}$
$G = \{f_1, f_2, f_3\}$

$$S(f_1, f_3) \xrightarrow{G}_+ 0$$

Third ***WHILE*** *loop passes through:*
$G' \neq \emptyset$ *and*
$G = \{f_1, f_2, f_3\}$

$$S(f_2, f_3) \xrightarrow{G}_+ y^3 + z^3$$

Since $y^3 + z^3 \neq 0$, *Let* $f_4 = y^3 + z^3$
Fourth ***WHILE*** *loop passes through:*
$G' = \{\{f_2, f_4\}, \{f_3, f_4\}\}$ *and*
$G = \{f_1, f_2, f_3, f_4\}$

$$S(f_1, f_4) \xrightarrow{G}_+ 0$$

Fifth ***WHILE*** *loop passes through:*
$G' = \{\{f_3, f_4\}\}$
$G = \{f_1, f_2, f_3, f_4\}$

$$S(f_2, f_4) \xrightarrow{G}_+ 0$$

Sixth ***WHILE*** *loop passes through:*
$G' \neq \emptyset$ *and*

$G = \{f_1, f_2, f_3, f_4\}$

$$S(f_2, f_4) \xrightarrow{G}_+ 0$$

Now $S(f_i, f_j) \xrightarrow{G}_+ 0$ *for* $1 \leq i < j \leq 4$
Thus $\{x^2y + z, xz + y, -xy^2 + z^2, y^3 + z^3\}$ *is a Groebner basis for* $\langle x^2y + z, xz + y\rangle \subseteq Q[x, y, z]$

1.5 Reduced Groebner basis

In Buchberger's Aigorithm there are two places where choices are made. First, there is the order in which the polynomials are inputed and this affects the application of the Division Algorithm.

Second, in the WHILE loop of Buchberger's Algorithm where we compute S-polynomials, we choose $\{f, g\} \in G$ random. So, if we were to change either of these choices, we might end up with a different Groebner basis.

This lead to the following definition.

Definition 1.5.1. [1] *A Groebner basis* $G = \{g_1, \ldots, g_t\}$ *is called minimal if for all* i, $lc(g_i) = 1$ *and for all* $i \neq j$, $lm(g_i)$*does not divide* $lm(g_j)$.

Lemma 1.5.2. [1] *Let* G *be a Groebner basis for the polynomial ideal I,let* $p \in G$ *be a polynomial such that* $lt(p) \in \langle lt(G - \{p\}\rangle$ *then* $G - \{p\}$ *is also a Groebner basis for* I.

Proof. Let $f \in I$ such that $lm(p)$ divides $lm(f)$, then since $lt(p) \in \langle lt(G - \{p\}\rangle$,then there exists $g_i \in G - \{p\}$ such that $lm(g_i)$ divides $lm(p)$,then $lm(g_i)$ divides $lm(f)$, Since f is arbitrary element of I,then $G - \{p\}$ is also a Groebner basis for I. □

Proposition 1.5.3. [1] *If* $G = \{g_1, \ldots, g_t\}$ *and* $F = \{f_1, \ldots, f_s\}$ *are minimal Groebner basis basis for the ideal* I *,then s=t and after renumbering if necessary ,*$lt(f_i) = lt(g_i)$ *for all* $i = 1, 2, ..., t$.

Proof. Since f_1 is in I and since G is a Groebner basis for I, there exists i such that $lm(g_i)$ divides $lm(f_1)$. After renumbering if necessary, we may assume that $i = 1$. Now g_1 is also in I, and hence, since F is a Groebner basis for I,there exists j such

that $lm(f_j)$ divides $lm(g_1)$, therefore $lm(f_j)$ divides $lm(f_1)$, and hence $j = 1$, since F is a minimal Groebner basis. Thus $lm(g_1) = lm(f_1)$.
Now f_2 is in I, and hence there exists i such that $lm(g_i)$ divides $lm(f_2)$, since G is a Groebner basis. The minimality of F and the fact that $lm(f_1) = lm(g_1)$ imply that $i \neq 1$,and after renumbering if necessary, we may assume that $i = 2$. As above we get that $lm(f_2) = lm(g_2)$. This process continues until all f_i's and g_i's are used up. Thus next we want to show $s = t$.
Suppose $s \neq t$ then with out loss of generality assume $s > t$.
Let $f_s \in F$,then since G is a Groebner basis for I then there exists $i \in \{1, 2, \ldots, t\}$ such that $lm(g_i)$ divides $lm(f_s)$ then by the first part of the proof of the proposition there exists f_i such that $lm(g_i) = lm(f_i)$,then this implies that $lm(f_i)$ divides $lm(f_s)$,but this contradicts the minimality of F. Therefore $s = t$. □

As we mentioned above, minimal Groebner bases are not unique. To get uniqueness, we need to add a stronger condition on the polynomials in the Groebner basis.

Definition 1.5.4. [1] *A Groebner basis $G = \{g_1, \ldots, g_t\}$ is called reduced Groebner basis, if for all i,$lc(g_i) = 1$ and g_i is reduced with respect to $G - \{g_i\}$.That is for all i,no non-zero term in g_i is divisible by any $lm(g_j)$ for any $i \neq j$.*

Note that a reduced Groebner basis is also minimal we now prove that the reduced Groebner basis exist.

Theorem 1.5.5. [1] *Fix a term order. Then every non-zero ideal I has a unique reduced Groebner basis with respect to this term order.*

Proof. Let $G = \{g_1, \ldots, g_t\}$ be a minimal Groebner basis for the ideal I.
Consider the following reduction process:

$$g_1 \xrightarrow{H_1}_+ h_1, \text{ where } h_1 \text{ is reduced with respect to } H_1 = \{g_2, g_2, \ldots, g_t\}$$

$$g_2 \xrightarrow{H_2}_+ h_2, \text{ where } h_2 \text{ is reduced with respect to } H_2 = \{h_1, g_3, \ldots, g_t\}$$

$$g_3 \xrightarrow{H_3}_+ h_3, \text{ where } h_3 \text{ is reduced with respect to } H_3 = \{h_1, h_2, \ldots, g_t\}$$

$$\vdots$$

$$g_t \xrightarrow{H_t}_+ h_t, \text{ where } h_t \text{ is reduced with respect to } H_t = \{h_1, h_2, \ldots, h_{t-1}\}$$

Claim: $H = \{h_1, h_2, \ldots, h_t\}$ is reduced Groebner basis.
Note that, since G is a minimal Groebner basis. We have that $lm(h_i) = lm(g_i)$ for each $i = 1, \ldots, t$. Therefore, H is also a Groebner basis for I.(infact is also a minimal Groebner basis). Since by the Division algorithm criteria h_i is reduced with respect to $H - \{h_i\}$. This implies that H is reduced Groebner basis.
We proved in the previous result that every ideal has a reduced Groebner basis.
Thus we only need to prove uniqueness.
Let $G = \{g_1, \ldots, g_t\}$ and $H = \{h_1, \ldots, h_t\}$ be reduced Groebner bases for I. We note that by Proposition 1.5.3 since a reduced Groebner basis is minimal, both G and H have the same number of elements and we may assume that, for each i, $lt(g_i) = lt(h_i)$.
Let i be given, $1 \leq i \leq t$
W.T.S:$g_i = h_i$ for all i such that $1 \leq i \leq t$ Suppose the contradiction that is $g_i \neq h_i$,then $g_i - h_i \in I$ implies that there exists j such that $lm(h_j)$ divides $lm(g_i - h_i)$, Since $lm(g_i - h_i) < lm(h_i)$, we see that $j \neq i$. But then $lm(h_j) = lm(g_j)$ divides a term of g_i or h_i. This contradicts the fact that G and H are reduced Groebner bases. So $g_i = h_i$.
Therefore Every non-zero ideal has a unique Reduced Groebner basis for a fixed term order. □

Example 1.5.6. *Let $I = \langle 2xy^2 - x, 3x^2y - y - 1\rangle \subseteq \mathbb{R}[x, y]$ with respect to grevlex then*
$\{2xy^2 - x, 3x^2y - y - 1, -\frac{1}{2}x^2 + \frac{1}{3}y^2 + \frac{1}{3}y, -\frac{1}{2}x^2 + \frac{2}{3}y^4 + \frac{2}{3}y^3, \frac{2}{3}y^3 + \frac{2}{3}y^2 - \frac{1}{3}y - \frac{1}{3}\}$ *is*

the Groebner basis for I.
Since $lm(-\frac{1}{2}x^2+\frac{1}{3}y^2+\frac{1}{3}y)=x^2$ divides $lm(3x^2y-y-1)=x^2y$ and
$lm(\frac{2}{3}y^3+\frac{2}{3}y^2-\frac{1}{3}y-\frac{1}{3})=y^3$ divides $lm(-\frac{1}{2}x^2+\frac{2}{3}y^4+\frac{2}{3}y^3)=y^4$ then
$\{2xy^2-x,-\frac{1}{2}x^2+\frac{1}{3}y^2+\frac{1}{3}y,\frac{2}{3}y^3+\frac{2}{3}y^2-\frac{1}{3}y-\frac{1}{3}\}$ is also the Groebner basis for I,then
by finding appropriate inverse for the leading coefficient for the above basis,then
$\{xy^2-\frac{1}{2}x,x^2-\frac{2}{3}y^2-\frac{2}{3}y,y^3+y^2-\frac{1}{2}y-\frac{1}{2}\}$ is a reduced Groebner basis for I.

1.6 Improvements on Buchberger's Algorithm

In this section,we show how the combinatorial complexity of the Buchberger's algorithm can be reduced by testing out certain S-polynomials which need not be considered.

Theorem 1.6.1. *(**Buchberger's first criterion**)* [3] *Let $f,g\in K[x_1,\ldots,x_n]$ with $lt(f)$ and $lt(g)$ are relatively prime then*

$$S(f,g)\xrightarrow{\{f,g\}}_+ 0$$

Proof. Assume that

$$f=\sum_{i=1}^{k}a_is_i \text{ and } g=\sum_{j=1}^{l}b_jt_j$$

where $a_i,b_j\in K$ with $a_i,b_j\neq 0$ and s_i,t_j are monomials in $K[x_1,x_2,\ldots,x_n]$ for $1\leq i\leq k$ and $1\leq j\leq l$
we may assume $s_1>s_2>\cdots>s_k$ and $t_1>t_2>\cdots>t_l$.
since $\gcd(s_1,t_1)=1$,
we must have $\mathrm{lcm}(s_1,t_1)=s_1t_1$ and thus we have

$$S(f,g)=t_1t_1f-a_1s_1g=b_1t_1\sum_{i=2}^{k}a_is_i-a_1s_1\sum_{j=2}^{l}b_jt_j$$

We claim that the two sums have no terms in common.
Suppose the contradiction,
then if $s_it_1=t_js_1$ for some $2\leq i\leq k$ and $2\leq j\leq l$ then s_it_1,being a common multiple of s_1 and t_1 ,is divided by $\mathrm{lcm}(s_1,t_1)=s_1t_1$.

It follows that $s_1t_1 < s_it_1$ and $s_i < s_1$,which is a contradiction.Furthermore,each term in the second is a multiple of $lt(f)$,then reducing by f

$$S(f,g) \xrightarrow{f} b_1t_1\sum_{i=2}^{k} a_is_i + \sum_{j=2}^{l} b_jt_j\sum_{i=2}^{k} a_is_i$$

$$= g\sum_{i=2}^{k} a_is_i$$

$$\xrightarrow{g}_{+} 0.$$

□

This criterion tells us that we can ignore calculating the S-polynomials of a pair whose leading terms are relatively prime. The second criterion which will discussed next is considerably deeper.It say that certain S-polynomials can be deleted despite the fact that they might not be reduced to zero at the time when we drop them. Before considering the second criterion let us use the following lemma as a preliminary.

Lemma 1.6.2. [3] *Let s,t,u are monomials in $K[x_1,\ldots,x_n]$,then the following are equivalent*

1. *t divides $lcm(s,u)$*
2. *$lcm(s,t)$ divide $lcm(s,u)$*
3. *$lcm(t,u)$ divide $lcm(s,u)$*

Proof. Let as assume $lcm(s,t) = k_1$,$lcm(t,u) = k_2$ and $lcm(s,u) = k_3$
(1) $\Rightarrow$ (2) Since $lcm(s,u) = k_3$ then, s divides k_3, then both s and t divide k_3, then by the property of least common multiple k_1 divides k_3.
(2) $\Rightarrow$ (3) $lcm(t,u) = k_2$,then both t and u divide k_2 and $lcm(s,u) = k_3$ this implies that u divides k_3 and by (2) t divides k_3, this shows that k_2 divides k_3.
(3) $\Rightarrow$ (1) Since k_2 divides k_3 and k_2 is a multiple of t,it is an immediate that t divides k_3. □

Theorem 1.6.3. ***(Buchberger's second criterion)*** [3]
Let $F=\{f_1,\ldots,f_s\} \subseteq K[x_1,\ldots,x_n]$,Consider $\{f_i,f_j\}$ in order to compute the S-polynomial and if there is another element,say $f_t \in F$ (with $f_i,f_j \neq f_t$) such that

1. *$lcm(lm(f_i),lm(f_j))$ is a multiple of the $lm(f_t)$*
2. *$S(f_i,f_t)$ and $S(f_t,f_j)$ have already been considered*

then

$$S(f_i,f_j) \xrightarrow{F}_+ 0$$

Proof. By assumption(2),there is a representation

$$S(f_i,f_t) = \sum_{i=1}^{k} h_i f_i$$

with $max_{1\leq\leq k}(lm(h_i)lm(f_i)) < lcm(Lm(f_i),lm(f_t))$ and

$$S(f_t,f_j) = \sum_{i=1}^{m} k_i f_i$$

with $max_{1\leq\leq m}(lm(k_i)lm(f_i)) < lcm(lm(f_t),lm(f_j))$ then by Lemma 1.6.2 and hypothesis (1) of Theorem 1.6.3 there exists s_1,t_1 such that

$$s_1 lcm(lm(f_i),lm(f_t)) = lcm(lm(f_i),lm(f_j))$$

$$s_1 lcm(lm(f_t),lm(f_j)) = lcm(lm(f_i),lm(f_j))$$

Let $a=lc(f_i)$, $b=lc(f_t)$, $c=lc(f_j)$ and $u_1,v_1,u_2,v_2 \in K[x_1,\ldots,x_n]$ such that

$$lcm(lm(f_i),lm(f_t)) = u_1 lm(f_i) = v_1 lm(f_t)$$

$$lcm(lm(f_t),lm(f_j)) = u_2 lm(f_t) = v_1 lm(f_j)$$

then $s_1v_1 = s_2u_2$ and we obtain

$$\begin{aligned}
abc \quad & [s_1S(f_i,f_t) + s_2S(f_t,f_j)] \\
= \quad & abc[(s_1(\frac{u_1f_i}{a} - \frac{v_1f_t}{b}) + s_2(\frac{u_2f_t}{b} - \frac{v_2f_j}{c})] \\
= \quad & cs_1(bu_1f_i - av_1f_t) + as_2(cu_2f_t - bv_2f_j) \\
= \quad & b[cs_1u_1f_i - as_2v_2f_j] \\
= \quad & abc[\frac{s_1u_1f_i}{a} - \frac{s_2v_2f_j}{c}] \\
= \quad & abc[S(f_i,f_j)]
\end{aligned}$$

Substituting the representations of the first two S-polynomials into the equation yields

$$S(f_i, f_j) = S(f_i, f_t) + S(f_t, f_j)$$

then by hypothesis (1.6.3)

$$S(f_i, j_j) \xrightarrow{F}_+ 0.$$

□

Furthermore,Buchberger designed a strategy in selecting pairs for the computation of S- polynomials. It can be shown that if we always select a pair $\{f_i, f_j\}$ such that lcm$(lm(f_i), lm(f_j))$ is as small as possible with respect to the chosen monomial ordering (the so called normal selection strategy), then criteria 1 and 2 are good in the sense that all possible reductions of S(f_i, f_j) yields 0.

So,based on the above two basic criteria the Buchberger's Algorithm can further improved as follows:

INPUT: A polynomial set $F=\{f_1, \ldots, f_s\} \subseteq K[x_1, \ldots, x_n]$ with $f_i \neq 0 (1 \leq i \leq t)$

OUTPUT:A reduced Groebner basis $G = \{g_1, \ldots, g_t\}$ that generates I

Set:$G = F$

$G' = \{\{(f_i, f_j) : 1 \leq i < j \leq s\}$

WHILE$(G' \neq 0)$ **DO**

$\{f_i, f_j\}$= a pair in G' such that lcm$(lm(f_i), lm(f_j))$ is minimal w.r.t the term order

$G' = G' - \{\{f_i, f_j\}\}$

IF(Criteria 1$(\{f_i, f_j\})$) **AND NOT**(Criteria 2 $(\{f_i, f_j\}, G, G')$) **THEN**

$S = S - polynomial\ of\ \{f_i, f_j\}$

$h = NormalForm(S, G)$

$G' = G' \bigcup \{\{g, h\}\}$ for $g \in G$

$G = G \bigcup \{h\}$

Example 1.6.4. *Consider the ideal*
$I = \langle f_1 = x^2 + 2xy^2, f_2 = xy + 2y^3 - 1\rangle \subseteq \mathbb{R}[x, y]$ *with lex order* $x > y$ *then to compute Groebner basis for* I

Let $G = f_1, f_2$ *and* $G' = \{\{f_1, f_2\}\}$
$S(f_1, f_2) \xrightarrow{G}_+ x$ *then* $f_3 = x$
then in the next ***WHILE*** *loop*
$G = \{f_1, f_2, f_3\}$
$G' = \{\{f_1, f_3\}, \{f_2, f_3\}\}$
since when we compare $lcm(lm(f_1), lm(f_3))$=x^2 *and* $lcm(lm(f_2), lm(f_3))$=xy *then* xy *is minimal with lex order then Normal selection strategy we compute*
$S(f_2, f_3) \xrightarrow{G}_+ 2y^3 - 1$ *this implies* $f_4 = 2y^3 - 1$
Then we obtain $G = \{f_1, f_2, f_3, f_4\}$ *and*
$G' = \{\{f_1, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$ *Then we have:*

$$lcm(lm(f_1), lm(f_3)) = x^2$$

$$lcm(lm(f_1), lm(f_4)) = x^2y^3$$

$$lcm(lm(f_2), lm(f_4)) = xy^3$$

$$lcm(lm(f_3), lm(f_4)) = xy^3$$

We can choose either of $\{f_2, f_4\}$ *or* $\{f_3, f_4\}$. *The reason why we prefer these from other pairs, is because of the strategy proposed by Buchberger and to apply Criterion* 2 *if Criterion* 1 *fails. But we can skip* $\{f_1, f_4\}$ *and* $\{f_3, f_4\}$ *by Criterion* 1. *Then let us look at* $\{f_2, f_4\}$.*But* $lcm(lm(f_2), lm(f_4))$*is a multiple of* $lm(f_3)$ *and* $S(f_2, f_3)$ *and* $S(f_3, f_4)$ *are already considered then by Criterion* 2 $S(f_2, f_4) \xrightarrow{G}_+ 0$.
Moreover,when we compute $S(f_1, f_3)$ *then it reduce to 0 with respect to G. So,no more elements are added. This implies that* $G = \{f_1, f_2, f_3, f_4\}$.*But since* $lm(f_1)$ *and* $lm(f_2)$ *are multiples of* $lm(f_3)$ *then G can reduce to* f_3, f_4.
$G = \{x, y^3 - \frac{1}{2}\}$ *is a reduced Groebner basis for* $I = \langle x^2 + 2xy^2, xy + 2y^3 - 1\rangle$.

Hence,we conclude by noting that the above two criteria proposed by Buchberger as criteria 1 and 2 are powerful commands that optimize Buchberger's Algorithm to compute S-polynomials.

In the next chapter we will see another version of **" Improvement on Buchbeger's Algorithm"** by using the properties **"Syzygies"**.

Chapter 2

Groebner basis over a Ring

In the previous chapter we considered the theory of Groebner bases in the ring $K[x_1, \ldots, x_n]$,where K is a field. In this chapter we are going to generalize the theory to the case $R[x_1, \ldots, x_n]$, where R is Noetherian commutative ring.

Many scholars use different techniques for computing Groebner basis over a ring but in this section we use the technique which is proposed by Möller by computing appropriate Syzygies for the algorithm.

2.1 Basic concepts of Module

Definition 2.1.1. [1] *Let A be a ring with unity 1 and M be a non-empty set such that M is an additive abelian group with scalar multiplication by elements of A(i.e if $x \in M$ and $a \in A$,then ax is uniquely determined elements of M). The set M is called an A-module(or module over A)if the following conditions are satisfied:*

1. $a(m + m') = am + am', for\ all\ a \in A\ and\ m, m' \in M$
2. $(a + a')m = am + a'm, for\ all\ a, a' \in A\ and\ m \in M$
3. $a(a'm) = (aa')m, for\ all\ a, a' \in A\ and\ m \in M$
4. $1m = m, for\ all\ m \in M$

Example 2.1.2. *Let A be a commutative ring and let I be an ideal of A*

1. *Then A is, of course, an abelian group and the scalar multiplication in A satisfies the ring axioms which turns A into an A-module. Thus a very important example of the A-module is A itself.*

2. *Since I is closed under addition and scalar multiplication by an arbitrary element of A, it follows that I is an A-module under the addition and multiplication of A.*

3. *The quotient ring A/I can also be viewed as an A-module. Of course, A/I has a natural abelian structure, so we need to provide it with a scalar multiplication by elements of A.*
   Let $a, a' \in A$ such that $a + I = a' + I \in A/I$.
   Let $r \in A$,thus $a - a' \in I$,and so $ra - ra' \in I$.Hence $ra + I = ra' + I$
   This can be demonstrated by defining it as

$$A \times A/I \longrightarrow A/I$$

$$(r, s + I) \longrightarrow rs + I$$

   One can easily show that A/I becomes an A-module with respect to this scalar multiplication. This concept of an A-module A/I will be discussed later in a Cartesian product A^s.

Definition 2.1.3. [1] *Let M be a module over a commutative ring A, and let N be a subset of M. We say that N is a sub-module of M precisely when N is itself an A-module with respect to the operation for M.*

A non-empty subset N of M will be a sub-module of M if and only if it is closed under addition and $am \in N$ for $m \in N$ and $a \in A$.

Theorem 2.1.4. *(**The submodule Criterion**)* [1] *Let A be a commutative ring and let N be a subset of the $A-$module .Then N is will be a submodule of M if and only if the following conditions hold:*

1. *$N \neq \emptyset$*

2. *Whenever $n, n' \in N$ and $a, a' \in A$,then $an + a'n' \in N$*

If $a_1, \ldots, a_n$ are elements of A-module M,an elements of M of the form

$$b_1a_1 + \cdots + b_na_n \; where \; each \; b_i \in A$$

may be naturally called a linear combination of $a_1, a_2, \ldots, a_n$.

The set of all linear combination of $a_1, \ldots, a_n$ is a submodule of M.

Note that a submodule of M is an abelian subgroup of the additive group M, and so must have the same zero element as M. Furthermore, M itself is a submodule of M and also the set $\{0\}$; the latter is known as the zero submodule of M Consider any submodule N of an A-Module M defined by

$$M/N = \{m + N | m \in M\}$$

Then M/N is the quotient abelian group and can be an A-module by defining

$$a(m + N) = am + N, for \; all \; a \in A, m \in M$$

This multiplication is well defined for $a \in A$ and $m \in M$ and by using definition(2.1.1), we also let $m, m' \in M$ and $a, a' \in A$

1. We can easily show that M/N is an abelian group.
2. $a(m + N) + (m' + N) = (am + N) + (am' + N)$
3. $(a + a')(m + N) = a(m + N) + a'(m + N)$
4. $a(a'(m + N) = aa'(m + N)$
5. $1(m + N) = 1m + N = m + N$

Since M is A-module,hence M/N has the structure of an A-module and is called the quotient module of M by N.

A function $\phi : M \longrightarrow M'$ is called an A-module homomorphism provided that it is an abelian group homomorphism and scalar multiplication is also preserved,that is

1. $\phi(m + m') = \phi(m) + \phi(m')$
2. $a\phi(m) = \phi(am), for\ all\ a \in A, m \in M$

For the two A-module M and M' given by above. If there exist A-homomorphism ϕ of M and M',we say that M' is homomorphic image of M.If ϕ is one-to-one,the homomorphism ϕ is called an isomorphism and we write $M \cong M'$.

Let $N = \ker(\phi) = \{\phi(m) = 0 | m \in M\}$.Then it can be easily show that N and $\phi(M)$ are submodule of M and M' respectively.From the theory of abelian group we know that $M/N \cong \phi(M)$ under the map

$$M/N \longrightarrow \phi(M)$$

$$m + N \longrightarrow \phi(m)$$

which is an A-module isomorphism as discussed above and referred to as "The First isomorphism Theorem of modules".

Let A be commutative ring $K[x_1, \ldots, x_n]$, K is field ,having discussed some elementary aspect of modules.

Let us shift a gear to address modules of commutative ring A of the form A^m.

Definition 2.1.5. [1] *Consider the Cartesian product*

$$A^m = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_s \end{bmatrix} | a_i \in A, for\ i = 1, 2, \ldots, s \right\}$$

where A^m consists of all column vectors with coordinates in A of length m. The set A^m is called a free A-module since every element $a = (a_1, \ldots, a_s)$ can be uniquely written as

$$a = \sum_{i=1}^{s} a_i e_i, where\ a_i \in A$$

with $e_i = (1, 0, \ldots, 0), \ldots, e_m = (0, 0, \ldots, 1)$ which are called the standard basis of A^m.

Definition 2.1.6. [1] *In a given Cartesian product of a ring A, the set $M \subseteq A^m$ is called an A-module provided that M is an additive abelian group undergoing scalar multiplication by elements of A. All the elements should satisfy conditions given in definition2.1.1 with the difference that in this case elements of M are column vectors. Moreover, the scalar multiplication in this definition is done component wise.*
For instance, for vectors $a_1, \ldots, a_s$ as elements of an A-module, A^m,we have

$$M = \{b_1 a_1 + \cdots + b_s a_s | b_i \in A, i = 1, 2, \ldots, s\} \subseteq A^m.$$

M is a submodule of A^m denoted by $\langle a_1, \ldots, a_s \rangle \subseteq A^m$,and The set $\{a_1, \ldots, a_n\}$ is the generating set of M.
If there is a single element a of M such that $M = \langle a \rangle$,we say M is called module with generator a.

A finite set $a_1, \ldots, a_s$ of the A-module is said to be independent is if

$$b_1 a_1 + \cdots + b_s a_s = 0, for\ all\ b_i \in A$$

implies that $b_i = 0\ for\ all\ i = 1, 2, \ldots, s$.

If $a_1, \ldots, a_s$ is independent and generates M,then $a_1, \ldots, a_s$ said to be basis of M.

The concept of A-module and vector space is similar except that the set of scalars in the module case is in the ring A, which is not necessarily a field. Submodules of A^m are used for a linear algebra in A^m in the same way that subspaces of K^m are used for linear algebra in K^m.

Theorem 2.1.7. [1] *Every submodule of A^m has finitely generating set.*

Proof. Let M be a submodule of A^m. By induction, if m = 1, then M is a finitely generated ideal of A by Hilbert Basis Theorem.
If m=1,let

$$I = \{a \in A | a \; is the first \; coordinate \; of \; element \; of \; M\}$$

Then I is an ideal of A and therefore finitely generated by the Hilbert's Basis Theorem. We are interested in showing that the module M has a finitely generated set.
Let

$$I = \langle a_1, \ldots, a_t \rangle$$

Let $m_1, \ldots, m_t \in M$,with a_i being the first coordinate of m_i.
Assume that the theorem holds true for submodules of A^{m-1}. Now consider $M' \in A^{m-1}$ such that $M' = \{(b_2, b_3, \ldots, b_m) | (0, b_2, \ldots, b_m) \in M\}$. Then we can note that M' is a submodule of A^{m-1} and by induction, is finitely generated (due to our assumption). Suppose $n'_1, n'_2, \ldots, n'_l \in M' \subseteq A^{m-1}$,for are the generators of M', for $i = 1, \ldots, l$.
Let $n_i \in A^m$, with 0 in the first coordinate, and n'_i is the vector with the remaining m-1 coordinates. Note that $n_i \in M$.
We show that $M = \langle m_1, m_2, \ldots, m_t, n_1, n_2, \ldots, n_l \rangle$.
Let $m \in M$. Now let m_1 be the first coordinate of m. Then

$$m_1 = \sum_{i=1}^{d} d_i a_i$$

again consider $m' = m - \sum_{i=1}^{d} d_i a_i$.This implies $m' \in M$ with first coordinate equal to zero. Hence, $m' = \sum_{i=1}^{l} c_i n_i$ which leads us to the end of the proof that:

$$m = m' + \sum_{i=1}^{t} d_i m_i = \sum_{i=1}^{l} c_i n_i + \sum_{i=1}^{t} d_i m_i$$

Hence M is finitely generated. □

Now,consider A-module M with $m_1, m_2, \ldots, m_s \in M$ and consider an

A-module homomorphism

$$\phi : A^s \longrightarrow M \; defined \; by$$

$$\phi(a_1, \ldots, a_s) = \sum_{i=1}^{s} a_i m_i$$

Then for $a = (a_1, \ldots, a_s)$,$a' = (a'_1, \ldots, a'_s) \subseteq A^s$ and $c \in A$,we can easily show that

1. $\phi(a + a') = \phi(a) + \phi(a')$,for all $a, a' \in A^s$

2. $c\phi(a) = \phi(ca)$,for all $a \in A^s$ and $c \in A$

Then by (1) and (2), ϕ is an A-module homomorphism,Moreover the image of ϕ is the submodule of M generated by $m_1, \ldots, m_s$.

Hence if $m_1, \ldots, m_s$ generate M,then ϕ is onto.

Let $e_1, \ldots, e_s$ denote the standard basis elements in A^s, we note that ϕ is uniquely defined by specifying the image of each $e_i \in A^s$, namely by specifying $\phi(e_i) = m_i$. We will often define a homomorphism ϕ from A^s by simply specifying $\phi(e_i)$, for $i = 1, \ldots, s$

Now let $M = \langle m_1, \ldots, m_s \rangle$ and $N = \ker(\phi) = \{a \in A^s | \phi(a) = 0\}$ and the map

$$\phi : A^s \longrightarrow M \; defined \; as$$

$$\phi(a_1, \ldots, a_s) = \sum_{i=1}^{s} a_i m_i$$

1. We can easily show that the map is a homomorphism

2. Since $m_1, \ldots, m_s$ generate M,we see that ϕ is onto and consider elements $a, a' \in A^s$ and $m \in M$.we can easily verify that if $\phi(a + N) = \phi(a' + N)$ then $a + N = a' + N$ which implies that $\phi$is one-to-one ,then by these steps or generally by "The First Isomorphism Theorem",we have

$$M \approxeq A^s/N$$

We therefore conclude the above by the following Lemma.

Lemma 2.1.8. [1] *Every finitely generated A-module is isomorphic to A^s/N for some positive integer s and some submodule N of A^s.*

Here we note that for a submodule M of A^s, if we have $m_1, \ldots, m_t \in A^s$ for $t < s$ such that $M = \langle m_1, m_2, \ldots, m_t \rangle$ and for another submodule N of M.The module M/N can be explicitly given as
$M/N = \langle m_1 + N, m_2 + N, \ldots, m_t + N \rangle$ which is a submodule of M/N.

2.2 Groebner basis and Syzygies

Let A be the Noetherian ring $K[x_1, \ldots, x_n]$ and $I = \langle f_1, \ldots, f_s \rangle$ be an ideal of A.we consider A-module homomorphism ϕ defined as

$$\phi : A^s \longrightarrow I \text{ given by}$$

$$(h_1, \ldots, h_s) \longrightarrow \sum_{i=1}^{s} h_i f_i$$

then

$$I \approxeq A^s / \ker(\phi) \text{ as } A - \text{module}$$

Definition 2.2.1. [1] *The kernel of the map ϕ is called the Syzygy module of the $1 \times s$ matrix $[f_1, \ldots, f_s]$.it is denoted $Syz(f_1, \ldots, f_s)$.An element $(h_1, \ldots, h_s)$ of $Syz(f_1, \ldots, f_s)$ is called a syzygy of $[f_1, \ldots, f_s]$ and satisfies*

$$h_1 f_1 + \cdots + h_s f_s = 0$$

We note that the map ϕ can also be viewed as matrix multiplication

$$\phi(h_1, \ldots, h_s) = [f_1, \ldots, f_s] \begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix} = \sum_{i=1}^{s} h_i f_i$$

That is ,if F is the $1 \times s$ matrix $[f_1, \ldots, f_s]$ and $h = \begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix} \in A^s$
then $\phi(h_1, \ldots, h_s) = Fh$ and $Syz(f_1, \ldots, f_s)$ is the set of all solutions h of the linear equation $Fh = 0$.

Example 2.2.2. *Let* $A = \mathbb{Q}[x, y, z]$ *and* $I = \langle x^2 - y, xy - z, y^2 - xz \rangle$
The map ϕ *is*

$$\phi : A^3 \longrightarrow I$$

given by

$$(h_1, h_2, h_3) \longrightarrow h_1(x^2 - y) + h_2(xy - z) + h_3(y^2 - xz)$$

Since $z(x^2 - y) - y(xy - z) + x(y^2 - xz) = 0$
and $y(x^2 - y) - x(xy - z) + 1(y^2 - xz) = 0$
Then $Syz(x^2 - y, xy - z, y^2 - xz) = \langle (z, -y, x), (y, -x, 1) \rangle$

Because $I \cong A^s/\ker(\phi)$ for the map $\phi :\longrightarrow A^s/I$. The ideal I can be described as a quotient of free A-module and $Syz(f_1, \ldots, f_s)$.

Note that $Syz(f_1, \ldots, f_s) \subseteq A^s$ is finitely generated since it is a submodule of A^s.

Proposition 2.2.3. [1] *Let* $c_1, \ldots, c_s \in K - \{0\}$ *and let* $X_1, \ldots, X_s$ *be monomials in* A. *For* $i \neq j \in \{1, \ldots, s\}$ *we define* $X_{ij} = lcm(X_i, X_j)$,*then the module* $Syz(c_1X_1, \ldots, c_sX_s)$ *is generated by*

$$\left\{ \frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j \in A^s | 1 \leq i < j \leq s \right\},$$

where $e_1, \ldots, e_s$ *are standard basis of* A^s.

Proof. First note that for all $i \neq j$ since

$$[c_1X_1, \ldots, c_sX_s](0, \ldots, 0, \underbrace{\frac{X_{ij}}{c_iX_i}}_{i^{th}coor}, 0, \ldots, 0, \underbrace{-\frac{X_{ij}}{c_jX_j}}_{j^{th}coor}, 0, \ldots, 0) = 0$$

then $\frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j \in Syz(c_1X_1, \ldots, c_sX_s)$
Therefore

$$\left\langle \frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j | 1 \leq i < j \leq s \right\rangle \subseteq Syz(c_1X_1, \ldots, c_sX_s)$$

To prove the converse, let $(h_1, \ldots, h_s)$ be Syzygy of $[c_1X_1, \ldots, c_sX_s]$,that is,

$$h_1c_1X_1 + \cdots + h_sc_sX_s = 0$$

Let X be a monomial in A.Then the coefficient of $h_1c_1X_1 + \cdots + h_sc_sX_s$ must be zero. Let us consider $h_i = c_i'X_i', i = 1, \ldots, s$,and then $c_i' = 0$ for all $i \in \{1, \ldots, s\}$ or there exists terms such that $X_i'X_i = X$ with $c_i' \neq 0$.
Let $c_1', \ldots, c_t'$ be non-zero c_j''s,then we have

$$c_1'c_1 + \cdots + c_s'c_s = c_1'c_1 + \cdots + c_t'c_t = 0,$$

Therefore

$$\begin{aligned}
(h_1, \ldots, h_s) &= (c_1'X_1', \ldots, c_s'X_s') = c_1'X_1'e_1 + \cdots + c_t'X_t'e_t \\
&= c_1'c_1\frac{X}{c_1X_1}e_1 + \cdots + c_t'c_t\frac{X}{c_tX_t}e_t \\
&= c_1'c_1\frac{X}{X_{12}}(\frac{X_{12}}{c_1X_1}e_1 - \frac{X_{12}}{c_2X_2}e_2) + (c_1'c_1 + c_2'c_2)\frac{X}{X_{23}}(\frac{X_{23}}{c_2X_2}e_2 - \frac{X_{23}}{c_3X_3}e_3) + \cdots \\
&+ (c_1'c_1 + \cdots + c_{t-1}'c_{t-1})\frac{X}{c_{t-1t}X_{t-1t}}(\frac{X_{t-1t}}{c_{t-1}X_{t-1}}e_{t-1} - \frac{X_{t-1t}}{c_tX_t}e_t) \\
&+ (\underbrace{c_1'c_1 + \cdots + c_t'c_t}_{=0})\frac{X}{c_tX_t}e_t
\end{aligned}$$

then

$$(h_1, \ldots, h_s) \subseteq \left\langle \frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j | 1 \leq i < j \leq s \right\rangle \subseteq A^s$$

then the proposition is required. □

The above proposition is a special case and we will generalize it as **Schreyer's** Theorem.

We observe that if $c_1X_1, \ldots, c_sX_s$ are the leading terms of the polynomials $f_1, \ldots, f_s$ respectively and if $(h_1, \ldots, h_s) \in Syz[c_1X_s, \ldots, c_sX_s]$,then $\sum_{i=1}^{s} h_i f_i$ has leading term strictly smaller than

$$\max_{i \leq i \leq s}(lm(h_i)lm(f_i))$$

In particular the syzygy $\frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j$ of $[c_1X_1, \ldots, c_sX_s]$ gives rise to the S-polynomials of f_i, f_j since

$$[f_1, \ldots, f_s](\frac{X_{ij}}{c_iX_i}e_i - \frac{X_{ij}}{c_jX_j}e_j) =$$

$$[f_1, \ldots, f_s](0, \ldots, 0, \underbrace{\frac{X_{ij}}{c_iX_i}}_{i^{th}coor}, 0, \ldots, 0, \underbrace{-\frac{X_{ij}}{c_jX_j}}_{j^{th}coor}, \ldots, 0) =$$

$$\frac{X_{ij}}{c_iX_i}f_i - \frac{X_{ij}}{c_jX_j}f_j = S(f_i, f_j)$$

The above observation and proposition 2.2.3 seem to indicate that the syzygy module of $[lt(f_1), \ldots, lt(f_s)]$ might be relevant to the computation of Groebner basis for $\langle f_1, \ldots, f_s \rangle$.

Definition 2.2.4. [1] *Let $X_1, \ldots, X_s$ be a monomials in $K[x_1, \ldots, x_n]$ and $c_1, \ldots, c_s \in K - \{0\}$,then for a monomial X,we call a syzygy $h = (h_1, \ldots, h_s) \in Syz(c_1X_1, \ldots, c_sX_s)$ homogeneous of degree X provided that each h_i is a term(i.e $lt(h_i) = h_i$ for all i) and $X_i lm(h_i) = X$ for all i such that $h_i \neq 0$,we say that $h \in Syz(c_1X_1, \ldots, c_sX_s)$ is homogeneous if it is homogeneous of degree X for some monomial X.*

Theorem 2.2.5. [1] *Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomial in A. Let B be a homogeneous generating set $Syz(lt(g_1), \ldots, lt(g_t))$,then G is a Groebner basis for the ideal $\langle g_1, \ldots, g_t \rangle$ if and only if for all $(h_1, \ldots, h_t) \in B$,we have*

$$h_1g_1 + \cdots + h_tg_t \xrightarrow{G}_{+} 0$$

Proof. If G is a Groebner basis,and $h_1g_1 + \cdots + h_tg_t \in G$,then
by Theorem 1.3.2 $h_1g_1 + \cdots + h_tg_t \xrightarrow{G}_{+} 0$
Conversely let $g \in \langle g_1, \ldots, g_t \rangle$,then

$$g = u_1g_1 + \cdots + u_tg_t \tag{2.2.1}$$

Choose a representation for the above equation (2.2.1)

$$X = \max_{1\leq i\leq t}(lm(u_i)lm(g_i)) \text{ be least}$$

least,Since,by Theorem 1.3.2,we need to show that g can be written as in equation (2.2.1) with $X = lm(g)$
Suppose the contradiction that $lm(g) < X$.
Let $S = \{i \in \{1,\ldots,t\} | lm(u_i)lm(g_i) = X\}$

$$\sum_{i\in S} lt(u_i)lt(g_i) = 0, \text{ since } lm(g) < X$$

Let $h = \sum_{i\in S} lt(u_i)e_i($ where $e_1,\ldots,e_t$ is the standard basis in A^t).
Then $h \in Syz(lt(g_1),\ldots,lt(g_t))$ and h is homogeneous.Now let $B = (h_1,\ldots,h_l)$,where for each $j = 1,\ldots,l$,$h_j = (h_{1j},\ldots,h_{tj})$.So $h = \sum_{j=1}^{l} a_j h_j$,where, since h is a homogeneous syzygy,we may assume that the a_j's are terms such that
$lm(a_j)lm(h_{ij})lm(g_i) = X$ for all i,j such that $a_j h_j \neq 0$. By hypothesis,
for each j,$\sum_{i=1}^{t} h_{ij}g_i \xrightarrow{G}_+ 0$.Thus by Theorem 1.2.10, we have for each $j = 1,\ldots,l$

$$\sum_{i=1}^{t} h_{ij}g_i = \sum_{i=1}^{t} u_{ij}g_i$$

such that

$$\max_{1\leq i\leq t} lm(u_{ij})lm(g_i) = lm(\sum_{i=1}^{t} h_{ij}g_i) < \max_{1\leq i\leq t} lm(h_{ij})lm(g_i)$$

The later strict inequality is because $\sum_{i=1}^{t} h_{ij}lt(g_i) = 0$.
Thus

$$\begin{aligned} g &= u_1g_1 + \cdots + u_tg_t \\ &= \sum_{i\in S} lt(u_i)g_i + \underbrace{\sum_{i\in S}(u_i - lt(u_i))g_i + \sum_{i\notin S} u_ig_i}_{\text{terms lower than } X} \\ &= \sum_{j=1}^{l}\sum_{i=1}^{t} a_jh_{ij}g_i + \text{ terms lower than } X. \\ &= \sum_{j=1}^{l}\sum_{i=1}^{t} a_ju_{ij}g_i + \text{ terms lower than } X. \end{aligned}$$

We have

$$\max_{i,j} lm(a_j)lm(h_{ij})lm(g_i) < \max_{i,j} lm(a_j)lm(h_{ij})lm(g_i) = X$$

But this contradicts the minimality of X. Therefore $lm(g) = X$,then by Theorem 1.3.2, G is a Groebner basis. □

Example 2.2.6. *Let* $G = \{g_1 = x + y, g_2 = x + 1\} \subseteq \mathbb{Q}[x, y]$,*we use lex order with* $x > y$
Then $lt(g_1) = x = lt(g_2)$,*then Since* $x+1(x)+(-x-1)(x) = 0$ *and* $x(x)+(-x)(x) = 0$.
This implies that $Syz(lt(g_1), lt(g_2)) = \langle (x + 1, -x - 1), (x, -x)\rangle$ *and*
$(x + 1)g_1 + (-x - 1)g_2 \xrightarrow{G}_+ 0$ *and* $(x)g_1 + (-x)g_2 \xrightarrow{G}_+ 0$.
But G *is not a Groebner basis for* $\langle g_1, g_2\rangle$ *because* $S(g_1, g_2) \xrightarrow{G}_+ y - 1$.

From the example we have seen that the hypothesis that the generating set of syzygies be homogeneous is necessary.

Corollary 2.2.7. [1] *Let* $G = \{g_1, \ldots, g_t\}$ *be a set of non-zero polynomials in* A.*Then* G *is a Groebner basis if and only if for* $i, j = 1, \ldots, t$

$$S(g_i, g_j) \xrightarrow{G}_+ 0$$

Proof. Let G is a Groebner basis for $\langle g_1, \ldots, g_t\rangle$ and $S(g_i, g_j) \in \langle g_1, \ldots, g_t\rangle$,then $S(g_i, g_j) \xrightarrow{G}_+ 0$.
For the converse let us consider the set
$B = \{\frac{X_{ij}}{lt(g_i)}e_i - \frac{X_{ij}}{lt(g_j)}e_j | i < j, i, j = 1, \ldots, t\}$ is the homogeneous generating of the module $Syz(lt(g_1), \ldots, lt(g_t))$.

$$[g_1, \ldots, g_t](0, \ldots, \underbrace{\frac{X_{ij}}{lt(g_i)}}_{i^{th}coor}, 0, \ldots, \underbrace{-\frac{X_{ij}}{lt(g_j)}}_{j^{th}coor}, 0, \ldots, 0) = \frac{X_{ij}}{lt(g_i)}g_i - \frac{X_{ij}}{lt(g_j)}g_j = S(g_i, g_j)$$

Since by hypothesis that, $S(g_i, g_j) \xrightarrow{G}_+ 0$.Therefore by Theorem 2.2.5, G is a Groebner basis. □

2.3 Computation of the Syzygy module

Let $\{g_1, \ldots, g_t\}$ be a Groebner basis,we let $X_{ij} = lcm(lm(g_i), lm(g_j))$,then the S-polynomial of g_i and g_j is given by

$$S(g_i, g_j) = \frac{X_{ij}}{lt(g_i)}g_i - \frac{X_{ij}}{lt(g_j)}g_j,$$

then by by Theorem 1.3.2, we have

$$S(g_i, g_j) = \sum_{i=1}^{t} k_i g_i$$

for some $k_i \in A$, such that

$$\max_{1 \leq i \leq t} lm(k_i) lm(g_i) = lm(S(g_i, g_j))$$

Having this in mind we will generalize Theorem 2.2.3.

Theorem 2.3.1. ***(Schreyer)***[1] *Let $\{g_1, \ldots, g_t\}$ be a Groebner basis for an ideal I in A,let $e_1, \ldots, e_t$ be standard basis in A^t, then let us define $i, j = 1, \ldots, t, i \neq j$*

$$s_{ij} = \frac{X_{ij}}{lt(g_i)} e_i - \frac{X_{ij}}{lt(g_j)} e_j - (k_1, \ldots, k_t) \in A^t$$

then the collection $\{s_{ij} | 1 \leq i < j \leq t\}$ is the generating set for $Syz(g_1, \ldots, g_t)$.

Proof. $s_{ij} \in Syz(g_1, \ldots, g_t)$ since

$$\begin{aligned} [g_1, \ldots, g_t] s_{ij} &= [g_1, \ldots, g_t]\left(\frac{X_{ij}}{lt(g_i)} e_i - \frac{X_{ij}}{lt(g_j)} e_j\right) - [g_1, \ldots, g_t](k_1, \ldots, k_t) \\ &= S(g_i, g_j) - \sum_{i=1}^{t} k_i g_i = 0 \end{aligned}$$

then $\langle s_{ij} | 1 \leq i < j \leq t \rangle \subseteq Syz(g_1, \ldots, g_t)$
For the converse we proceed by contradiction,
Let

$$(u_1, \ldots, u_t) \in Syz(g_1, \ldots, g_t) - \langle s_{ij} | 1 \leq i < j \leq t \rangle$$

Then, we can choose such a $(u_1, \ldots, u_t)$ with $\max_{1 \leq i \leq t}(lm(u_i) lm(g_i)) = X$ be least
Let

$$S = \{i \in \{1, \ldots, t\} | lm(u_i) lm(g_i) = X\}$$

Now for each $i \in \{1, \ldots, t\}$ we define v_i as follows:

$$v_i = \begin{cases} u_i \ if \ i \notin S \\ u_i - lt(u_i) \ if \ i \in S \end{cases}$$

Also,for $i \in S$,let $lt(u_i) = c_i X_i'$,where $c_i \in K$ and X_i' is a monomial in $K[x_1, \ldots, x_n]$. since $(u_1, \ldots, u_t) \in Syz(g_1, \ldots, g_t)$,we see that

$$\sum_{i \in S} lt(u_i) lt(g_i) = 0$$

and so

$$\sum_{i \in S} c_i X_i' e_i \in Syz(lt(g_i) | i \in S)$$

Thus by Theorem 2.2.3,we have

$$\sum_{i \in S} c_i X_i' e_i = \sum_{i,j \in S, i<j} a_{ij} \left(\frac{X_{ij}}{lt(g_i)} e_i - \frac{X_{ij}}{lt(g_j)} e_j\right),$$

for some $a_{ij} \in A$.Since each coordinate of the vector in the left-hand side of the equation above is homogeneous,and since $X_i' lm(g_i) = X$,we can choose a_{ij} to be a constant multiple of $\frac{X}{X_{ij}}$. Then we have

$$\begin{aligned}
(u_1, \ldots, u_t) &= \sum_{i \in S} c_i X_i' e_i + (v_1, \ldots, v_t) \\
&= \sum_{i<j, i,j \in S} a_{ij} \left(\frac{X_{ij}}{lt(g_i)} e_i - \frac{X_{ij}}{lt(g_j)} e_j\right) + (v_1, \ldots, v_t) \\
&= \sum_{i<j, i,j \in S} a_{ij} s_{ij} + (v_1, \ldots, v_t) + \sum_{i<j, i,j \in S} a_{ij} (k_1, \ldots, k_t)
\end{aligned}$$

We define $(p_1, \ldots, p_t) = (v_1, \ldots, v_t) + \sum_{i<j, i,j \in S} a_{ij} (k_1, \ldots, k_t)$.
Since $(u_1, \ldots, u_t) \in Syz(g_1, \ldots, g_t) - \langle s_{ij} | 1 \leq i < j \leq t \rangle$,then
$(p_1, \ldots, p_t) \in Syz(g_1, \ldots, g_t)$
For each $r \in \{1, \ldots, t\}$ we have

$$\begin{aligned}
lm(p_r) lm(g_r) &= lm(v_r + \sum_{i<j, i,j \in S} a_{ij} k_r) lm(g_r) \\
&\leq \max(lm(v_r, \max_{i<j, i,j \in S} (lm(a_{ij}) lm(k_r))) lm(g_r)
\end{aligned}$$

But,by definition of v_r,we have $lm(v_r) lm(g_r) < X$. Also,as mentioned above a_{ij} is the constant multiple of $\frac{X}{X_{ij}}$,and for all $i, j \in S, i < j$,we have

$$lm(a_{ij}) lm(k_r) lm(g_r) = \frac{X}{X_{ij}} lm(k_r) lm(g_r) = \frac{X}{X_{ij}} lm(S(g_i, g_j)) < X$$

Therefore $lm(p_r) lm(g_r) < X$,but this contradict that $X = \max_{1 \leq r \leq t} lm(u_r) lm(g_r)$ is least.
Therefore $\{s_{ij} | 1 \leq i < j \leq t\}$ is the generating set for $Syz(g_1, \ldots, g_t)$. □

Example 2.3.2. *Let* $g_1 = x - z, g_2 = y - z, g_3 = z^2 + 1$. *These form a reduced Groebner basis with respect to the lex order* $x > y > z$ *for the ideal* $\langle g_1, g_2, g_3 \rangle$
With the notation in the above Theorem we have:
$X_1 = x, X_2 = y, X_3 = z^2, X_{12} = xy, X_{13} = xz^2, X_{23} = yz^2$
Now $S(g_1, g_2) = xz - yz$, *so* $S(g_1, g_2) = zg_1 + (-z)g_2$
Therefore

$$s_{12} = \frac{X_{12}}{X_1}e_1 - \frac{X_{12}}{x_2}e_2 - (z, -z, 0) = (y - z, -x + z, 0)$$

Also $S(g_1, g_3) = -x - z^3 = (-1)g_1 + (-z)g_3$

$$s_{13} = \frac{X_{13}}{X_1}e_1 - \frac{X_{13}}{X_3}e_3 - (-1, 0, -z) = (z^2 + 1, 0, -x + z)$$

Finally,$S(g_2, g_3) = -y - z^3 = (-1)g_2 + (-z)g_3$

$$s_{23} = \frac{X_{23}}{X_2}e_2 - \frac{X_{23}}{X_3}e_3 - (0, -1, -z) = (0, z^2 + 1, -y + z)$$

Then by Theorem 2.3.1

$$Syz(g_1, g_2, g_3) = \langle (y - z, -x + z, 0), (z^2 + 1, 0, -x + z), (0, z^2 + 1, -y + z) \rangle$$

We now turn our attention of computing $Syz(f_1, \ldots, f_s)$ for the collection $\{f_1, \ldots, f_s\}$ of non-zero polynomials in A which are not Groebner basis.

we first compute a Groebner basis $\{g_1, \ldots, g_t\}$ for $\langle f_1, \ldots, f_s \rangle$ and set $F = [f_1, \ldots, f_s]$ and $G = [g_1, \ldots, g_t]$. Then there exists $t \times s$ matrix S which is obtained by division algorithm such that $F = GS$ and an $t \times s$ matrix T which is obtained keeping track of the reductions during Buchberger's Algorithm such that $G = FT$. Keeping this in mind we will use the following theorem to compute $Syz(f_1, \ldots, f_s)$.

Theorem 2.3.3. [1] *Let* $\{f_1, \ldots, f_s\}$ *be a collection of non-zero polynomials and* $\{g_1, \ldots, g_t\}$ *is a Groebner basis for* $\langle f_1, \ldots, f_s \rangle$ *and* $\{s_1, \ldots, s_r\}$*(where* s_i*'s are the column vectors in* A^t*) is the generating set for* $Syz(g_1, \ldots, g_t)$ *and* $r_1, \ldots, r_s$ *are the columns of* $I_s - TS$ *where* I_s *is* $s \times s$ *identity matrix,then*

$$Syz(f_1, \ldots, f_s) = \langle Ts_1, \ldots, Ts_r, r_1, \ldots, r_s \rangle \subseteq A^s$$

Proof. Since $\{s_1, \ldots, s_r\}$ is the generating set for $Syz(g_1, \ldots, g_t)$

$$0 = G(s_i) = FT(s_i) = F(Ts_i)$$

and ,hence

$$\langle Ts_i | i = 1, \ldots, r\rangle \subseteq Syz(f_1, \ldots, f_s)$$

Moreover, if we let I_s be the $s \times s$ identity matrix, we have

$$F(I_s - TS) = F - FTS = F - (FT)S = F - GS = F - F = 0$$

and hence $r_1, \ldots, r_s$ is the columns of $I_s - TS$, then $r_1, \ldots, r_s$ in $Syz(f_1, \ldots, f_s)$

$$\langle Ts_1, \ldots, Ts_r, r_1, \ldots, r_s\rangle \subseteq Syz(f_1, \ldots, f_s)$$

For the converse,let $p = (a_1, \ldots, a_s) \in Syz(f_1, \ldots, f_s)$.Then $0 = Fp = GSp$ and hence $Sp \in Syz(g_1, \ldots, g_t)$.By definition of $s_1, \ldots, s_r$ such that we have $Sp = \sum_{i=1}^{r} h_i s_i$,for some $h_i \in A$. Thus we have $TSp = \sum_{i=1}^{r} h_i(Ts_i)$. Finally

$$p = p - TSp + TSp = (I_s - TS)p + \sum_{i=1}^{r} h_i(Ts_i) = \sum_{i=1}^{s} a_i r_i + \sum_{i=1}^{r} h_i(Ts_i).$$

Then, $Syz(f_1, \ldots, f_s) \subseteq \langle Ts_1, \ldots, Ts_r, r_1, \ldots, r_s\rangle$
Thus the Theorem is required. □

Example 2.3.4. *Consider the polynomials $f_1 = xy + 1, f_2 = xz + 1$ and $f_3 = yz + 1 \in \mathbb{Q}[x, y, z]$,then to compute $Syz(f_1, f_2, f_3)$*
We first compute the Groebner basis for $\langle f_1, f_2, f_3\rangle$ with respect to lex ordering with $x > y > z$.
Then we find $G = [g_1 = x - z, g_2 = y - z, g_3 = z^2 + 1]$ a Groebner basis for $\langle f_1, f_2, f_3\rangle$
We have

$$[f_1, f_2, f_3] = [g_1, g_2, g_3] \underbrace{\begin{bmatrix} y & z & 0 \\ z & 0 & z \\ 1 & 1 & 1 \end{bmatrix}}_{S}$$

and

$$[g_1, g_2, g_3] = [f_1, f_2, f_3] \underbrace{\begin{bmatrix} -z & -z & z^2 \\ 0 & y & -yz \\ x & 0 & 1 \end{bmatrix}}_{T}$$

Then by Example 2.3.2
$Syz(g_1, g_2, g_3) = \langle (y-z, -x+z, 0), (z^2+1, 0, -x+z), (0, z^2+1, -y+z) \rangle$

$$Ts_{12} = T \begin{bmatrix} y-z \\ -x+z \\ 0 \end{bmatrix} = \begin{bmatrix} xz-yz \\ -xy+yz \\ xy-xz \end{bmatrix}$$

$$Ts_{13} = T \begin{bmatrix} z^2+1 \\ 0 \\ -x+z \end{bmatrix} = \begin{bmatrix} -xz^2-z \\ xyz-yz^2 \\ xz^2+z \end{bmatrix}$$

$$Ts_{23} = T \begin{bmatrix} 0 \\ z^2+1 \\ -y+z \end{bmatrix} = \begin{bmatrix} -yz^2-z \\ y^2z+y \\ -y+z \end{bmatrix}$$

$$I_3 - TS = \begin{bmatrix} yz+1 & 0 & 0 \\ 0 & yz+1 & 0 \\ -xy-1 & -xz-1 & 0 \end{bmatrix}$$

then we take only non-zero columns of $I_3 - TS$
Therefore $r_1 = (yz+1, 0, -xy-1)$ *and* $r_2 = (0, yz+1, -xz-1)$,*then*

$$Syz(f_1, f_2, f_3) = \langle Ts_{12}, Ts_{13}, Ts_{23}, r_1, r_2 \rangle$$

2.4 Improvement on Buchberger's Algorithms by using Syzygies

In the previous section ,we were discuss the improvement of Buchberger's Algorithm by detecting out the property of leading monomials to reduce the number of computation of S-polynomials as Buchberger's criterion 1 and 2.

In this section,we will use another version of improvement on Buchberger's Algorithm by using Syzygies.

Lemma 2.4.1. [1] *Let $X_1, \ldots, X_s$ be monomials in $K[x_1, \ldots, x_n]$ and let $c_1, \ldots, c_s \in K - \{0\}$.For $i, j = 1, \ldots, s$ define $X_{ij} = lcm(X_i, X_j)$ and let $\tau_{ij} = \frac{X_{ij}}{c_i X_i} e_i - \frac{X_{ij}}{c_j X_j} e_j \in Syz(c_1 X_1, \ldots, c_s X_s) \subseteq A^s$,where $e_1, \ldots, e_s$ are the standard basis for A^s. For each $i, j, l = 1, \ldots, s$, let $X_{ijl} = lcm(X_i, X_j, X_l)$ then we have*

$$\frac{X_{ijl}}{X_{ij}}\tau_{ij} + \frac{X_{ijl}}{X_{jl}}\tau_{jl} + \frac{X_{ijl}}{X_{li}}\tau_{li} = 0$$

Proof. We have

$$\frac{X_{ijl}}{X_{ij}}\tau_{ij} + \frac{X_{ijl}}{X_{jl}}\tau_{jl} + \frac{X_{ijl}}{X_{li}}\tau_{li} =$$

$$\frac{X_{ijl}}{X_{ij}}\left(\frac{X_{ij}}{c_i X_i}e_i - \frac{X_{ij}}{c_j X_j}e_j\right) + \frac{X_{ijl}}{X_{jl}}\left(\frac{X_{jl}}{c_j X_j}e_j - \frac{X_{jl}}{c_l X_l}e_l\right) + \frac{X_{ijl}}{X_{li}}\left(\frac{X_{li}}{c_l X_l}e_l - \frac{X_{li}}{c_i X_i}e_i\right)$$

$$= \frac{X_{ijl}}{c_i X_i}e_i - \frac{X_{ijl}}{c_j X_j}e_j + \frac{X_{ijl}}{c_j X_j}e_j - \frac{X_{ijj}}{c_l X_l}e_l + \frac{X_{ijl}}{c_l X_l}e_l - \frac{X_{ijl}}{c_i X_i}e_i = 0$$

This proves the Lemma. □

Corollary 2.4.2. [1] *We continue the notation of Lemma* 2.4.1, *let $B \subseteq \{\tau_{ij} | 1 \leq i < j \leq s\}$ be the generating set for $Syz(c_1 X_1, \ldots, c_s X_s)$.Suppose we have three distinct indices i, j, l such that $\tau_{ij}, \tau_{jl}, \tau_{li} \in B$ and such that X_l divides $X_{ij} = lcm(X_i, X_j)$. Then $B - \{\tau_{ij}\}$ is also the generating set for $Syz(c_1 X_1, \ldots, c_s X_s)$.*

Proof. By Lemma 2.4.1

$$\frac{X_{ijl}}{X_{ij}}\tau_{ij} + \frac{X_{ijl}}{X_{jl}}\tau_{jl} + \frac{X_{ijl}}{X_{li}}\tau_{li} = 0$$

If X_l divides X_{ij},then $X_{ijl} = X_{ij}$,then we have

$$\tau_{ij} + \frac{X_{ij}}{X_{jl}}\tau_{jl} + \frac{X_{ij}}{X_{li}}\tau_{li} = 0$$

This implies that

$$\tau_{ij} = -\frac{X_{ij}}{X_{jl}}\tau_{jl} - \frac{X_{ij}}{X_{li}}\tau_{li}$$

Hence, τ_{ij} is generated by τ_{jl} and τ_{li}.
Therefore $B - \{\tau_{ij}\}$ is the generating set for $Syz(c_1 X_1, \ldots, c_s X_s)$. □

We will use Corollary 2.4.2 to improve Buchberger's algorithm in the following way.

Let $\{f_1, \ldots, f_s\}$ is the generating set for the ideal I of $K[x_1, \ldots, x_n]$.

Let $lt(f_i) = c_i X_i$.We will use the same notation as given in the corollary and eliminate as many $\tau_{ij} \in B$(by applying Corollary 2.4.2) to obtain a smaller set of generators for $Syz(lt(f_1), \ldots, lt(f_s))$. Then we need to find the S-polynomial $S(f_i, f_j)$,corresponding to one of the τ_{ij} remaining in B and reduce it.We then add the reduced S-polynomial, say f_{s+1},to the set $\{f_1, \ldots, f_s\}$ if $f_{s+1} \neq 0$; otherwise ignore it.Now the generating set B is enlarged to $\{\tau_{i,s+1} | 1 \leq i \leq t\}$ which generates $Syz(lt(f_1), \ldots, lt(f_s), lt(f_{s+1}))$. Again we apply the steps in Corollary 2.4.2 to eliminate as many τ_{ij}'s from the new set, to obtain a smaller generating set for $Syz(lt(f_1), \ldots, lt(f_s), lt(f_{s+1}))$. Then find S-polynomial, $S(f_i, f_j)$, corresponding to a τ_{ij} remaining in B and reduce it. We have to keep doing this until all S-polynomials are reduced to zero. If all these
S-polynomials are reduced to zero, then we maintain the set B as a basis of the current syzygy module.

The main objective of the algorithm is to reduce the S-polynomials either to zero, and ignore the pairs or reduce it and add the new polynomial to the set. So, we need to have techniques to do this. Now let us see how the algorithm is set to compute these S-polynomials and reduce them.

We first subdivide the set of indices $\{\{i, j\}\tau_{ij} \in B\}$ into two subsets:

the computed set $C = \{\{i, j\}, \tau_{ij} \in B \; for \; which \; an \; S{-}polynomial \; has \; been \; computed\}$

and the non-computed set

$NC = \{\{i, j\}, \tau_{ij} \in B \; for \; which \; an \; S - polynomial \; has \; not \; been \; computed\}$.

Here we note that at any time in the algorithm after NC has been initialized, $\{\tau_{ij} | \{i, j\} \in NC \bigcup C\}$ is the generating set of the syzygy module of the current set of leading terms. We continue the algorithm until $NC = \emptyset$.

With these ideas acting as foundation, we can now introduce the improved version of Buchberger's Algorithm to compute Groebner bases using syzygies. The improvement of the performance of the algorithm is based on the following two main criteria $Crit1(i,j)$ and $Crit2(i,j)$ given below:

1. $Crit1(i,j)$:

   It turns "TRUE" if and only if $lm(f_i)$ and $lp(f_j)$ are relatively prime.

   If $Crit1(i,j)$ =TRUE, we can ignore computing $S(f_if_j)$ since $S(f_if_j)$ reduces to zero modulo G by Lemma 1.6.1 . So, nothing is added to the basis and $\{i,j\}$ is added to C . We pick a pair of $\{f_i,f_j\}$ such that $lm(f_i)$ and $lp(f_j)$ are not relatively prime.

2. $Crit2(NC,C,s)$:

   This command is given as an algorithm 2.2 and is used to eliminate pairs from the set NC with out computing their S-polynomial. It is the implementation of the ideas in Corollary 2.4.2. As it will be seen from algorithm 2.2 , the basic idea is to find triples of indices ν,μ,ρ such that the three pairs $\{\nu,\mu\},\{\nu,\rho\},\{\mu,\rho\}$ are in $NC\bigcup C$ and X_ρ divides $\text{lcm}(X_\nu,X_\mu)$

Since we are interested in doing the first main WHILE loop of algorithm 2.2 , we only need to consider one of ν,μ,ρ is equal to s. This is because the cases of all triples with ν,μ,ρ all less than s were checked before. Since μ and ρ are interchangeable, it is enough to consider the cases $\rho=s$ and $\nu=s$ in order to go through that eliminate pairs from the set NC without computing the S-polynomial. Moreover, we note that a pair of the form $\{i,s\}$ cannot lie in C (this explains why checking membership in $NC\bigcup C$ was often done by just checking membership in NC). Finally, we only check, in the second main WHILE loop, whether $\{i,j\}$ is in NC since we are only interested

in eliminating it from NC.

First of all we take (NC, C, s) from algorithm 2.1 as an input for algorithm 2.2, to allow us to eliminate pairs from the set NC which were not already eliminated by algorithm 2.1.

Consider a pair $\{i, s\} \in NC(i < s)$ to check whether this pair is to be eliminated from NC or not.We start a pair $\{l, s\}$ where $1 \leq l < s$.Then if we have $\{l, s\} \in NC$ and the pairs $\{i, l\} \in NC \bigcup C$ with $\{i, s\} \in NC$,then we are supposed to check only whether X_l divides $\text{lcm}(X_i, X_s)$ such that the pair $\{i, s\}$ can be eliminated from NC and NC will be updated to $NC - \{\{i, s\}\}$; otherwise the pair $\{i, s\}$ will remain in the set NC. We proceed checking for different $i, l < s$ until checking for every pair of the form $\{i, s\}$ is completed.

The second main WHILE loop starts to check whether the pair $\{i, j\}$, where $i, j < s$, will be eliminated from the set NC or not. Here we note that since $i, j < s$, the pair was checked before but not eliminated. Now consider the pair $\{i, s\} \in NC$. In fact, the pair can not lie in C. Hence,for $j < s$ and if the pairs $\{j, s\}$ and $\{i, j\}$ are both in NC, and X_s divides $\text{lcm}(X_i, X_j)$, then the pair $\{i, j\}$ will be eliminated from the set NC otherwise it will be updated as an element of NC. We proceed checking for pairs of $\{i, j\}$ with $i, j < s$ and update the set.

Finally, after we had finished going through the loops and determining which pairs are to be eliminated, and if we still have pairs in the set, we compute the S-polynomial of a pair from the set NC based on the strategy proposed by Buchberger, and update the set NC. Actually, In algorithm 2.1 we do not give a rule for choosing the pair $\{i, j\} \in NC$, for which we compute the corresponding S-polynomial. Buchberger

proposed a strategy to speed up our calculation. Often the S-polynomials are computed in such a way that $S(f_i, f_j)$ is computed first if lcm$(lm(f_i), lm(f_j))$is least (with respect to the current term order) among the lcm$(lm(f_i), lm(f_j))$. This process is called the *normal selection strategy*. This strategy is used to speed up the calculation that regards the procedure to select a pair. It can be shown that if we always select a pair $\{f_i, f_j\}$ such that lcm$(lm(f_i), lm(f_j))$ is as small as possible with respect to the chosen term ordering, then $Crit1$ and $Crit2$ are "good" in the sense that all possible reductions of $S(f_i, f_j)$ will yield zero. Finally,if the degree ordering is used, this strategy seems to lead to simpler polynomials than other possible choices.

INPUT:$F = \{f_1, \ldots, f_s\} \subseteq K[x_1, \ldots, x_n]$

OUTPUT:A Groebner basis G for $\langle f_1, \ldots, f_s \rangle$

INITIALIZATION:$G = F$

$C = \emptyset$

$NC = \{\{1, 2\}\}$

$i = 2$

WHILE:$i < s$ **DO**

$NC = NC \bigcup \{\{j, i+1\} | 1 \leq j \leq i\}$

$NC = Crit2(NC, C, i+1)$

$i = i + 1$

WHILE:$NC \neq \emptyset$ **DO**

Choose $\{i, j\} \in NC$

$NC = NC - \{\{i, j\}\}$

$C = C \bigcup \{\{i, j\}\}$

IF $Crit1(i, j)$=FALSE **THEN**

$S(f_i, f_j) \xrightarrow{G}_+ h$ where h is reduced with respect to G

IF $h \neq 0$ **THEN**

$f_{s+1} = h$

$G = G \bigcup \{f_{s+1}\}$

$s = s + 1$

$NC = NC \bigcup \{\{i, s | 1 \leq i \leq s-1\}$

$NC = Crit2(NC, C, s)$

Algorithm 2.1 Improved Buchberger's algorithm.

Proposition 2.4.3. [1] *Given a set of non-zero polynomials $F = \{f_1, \ldots, f_s\}$, the improved Buchberger's Algorithm (Algorithm 2.1 and Algorithm 2.2)will produce a Groebner basis for $I = \langle f_1, \ldots, f_s \rangle$.*

Proof. Similar to Buchberger's Algorithm seen in the previous Chapter, we start with $F = G$ and when we compute S-polynomials the number of elements may increase. So, let us assume that we have t elements where $t \geq s$.

Let $G = \{f_1, \ldots, f_t\}$ $(t \geq s)$ be the output of the algorithm we have in Algorithm 2.1. We see that every S-polynomial corresponding to every pair in C reduces to zero.It then suffices to show that $\{\tau_{ij} | \{i, j\} \in C\}$ is the generating set for $Syz(lt(f_1), \ldots, lt(f_t))$, and since at any time in the algorithm after NC has been initialized, it suffices to show that $\{\tau_{ij} | \{i, j\} \in NC \bigcup C\}$ is a generating set for the syzygy module of current leading terms.
So, at each stage of the algorithm, we can have either the S-polynomial reducing to zero, and $NC \bigcup C$ doesn't change, or a polynomial being added to G. This latter option will lead to other relevant pairs being added to $NC \bigcup C$, and so that the set of τ_{ij}'s corresponding to this update $NC \bigcup C$ is a generating set for the syzygy module of the new set of leading terms. And then $Crit2$ is to be applied to the new set of NC, which will not alter this last statement, according to Corollary 2.4.2.
The algorithm terminates due to the Hilbert basis Theorem. □

INPUT :(NC, C, s) from algorithm 2.1

OUTPUT:NC pair will be deleted by Corollary 2.4.2

INITIALIZATION:$l = 1$

WHILE $l < s$

IF $\{l, s\} \in NC$ **THEN**

$i = 1$

WHILE $i < s$ **DO**

IF $\{i, s\} \in NC \bigcup C$ **AND** $\{i, s\} \in NC$ **THEN**

IF X_l Divides $\text{lcm}(X_i, X_s$ **THEN**

$NC = NC - \{\{i, s\}\}$

$i = i + 1$

$l = l + 1$

$i = 1$

WHILE $i < s$ **DO**

IF $\{i, s\} \in NC$ **DO**

$j = i + 1$

WHILE $j < s$ **DO**

IF $\{j, s\} \in NC$ **AND** $\{j, i\} \in NC$ **THEN**

IF X_s Divides $\text{lcm}(X_i, X_j)$ **THEN**

$NC = NC - \{\{i, j\}\}$

$j = j + 1$

$i = i + 1$

Algorithm 2.2 $Crit2(NC, C, s)$

Example 2.4.4. *Consider the polynomials* $f_1 = x^2y^2 - z^2$,$f_2 = xy^2z - xyz$ *and* $f_3 = xyz^3 - xz^2 \in \mathbb{Q}[x, y, z]$ *with term order grlex such that* $x < y < z$. *We need to find the Groebner basis using the improved Buchberger's Algorithm.*
We follow Algorithm 2.1 *and* 2.2 *with the proposed strategy, called the normal strategy, to speed up our computation in selecting pairs to compute S-polynomials.*
We start with the assumption that $G = \{f_1, f_2, f_3\}$, $C = \emptyset$ *and*

$NC = \{\{1,2\},\{1,3\},\{2,3\}\}$. *We have that* $lcm(lm(f_1), lm(f_3))$ *is divisible by* $lm(f_2)$ *which implies that we do not consider* $\{1,3\}$. *Then we have that*
$NC = Crit2(NC, C, 3) = \{\{1,2\},\{2,3\}\}$.
• *Using the strategy proposed by Buchberger to choose and compute the S-polynomial from NC,we choose pair* $\{1,2\}$ *and compute the S-polynomial that brings*
$NC = \{\{2,3\}\}$ *and* $C = \{\{1,2\}\}$ *with* $S(f_1, f_2) = x^2yz - z^3$ *which is reduced with respect to G. Now we let* $f_4 = x^2yz - z^3$ *to be added to G and then NC will be updated as* $NC = \{\{2,3\},\{1,4\},\{2,4\},\{3,4\}\}$ *and* $C = \{\{1,2\}\}$.
• *Apply Crit2 and for* $l = 2$, *we eliminate* $\{2,4\} \in NC$ *since* $\{1,2\} \in NC \bigcup C$,$\{1,4\}$ *and* $lm(f_1)$ *divides* $lcm(lm(f_2), lm(f_4))$. *But we do not have any to eliminate for* $l = 2$ *and* $l = 3$. *Then the new* $NC = \{\{2,3\}\{1,4\},\{3,4\}\}$. *We choose to calculate* $\{1,4\}$ *to calculate the S-polynomial by the normal selection strategy such that* $S(f_1, f_4) = yz^3 - z^3$, *Say* $f_5 = yz^3 - z^3$, *which brings* $NC = \{\{2,3\},\{3,4\}\}$ *and* $C = \{\{1,2\},\{1,4\}\}$. *Then we update NC to include a pair of* f_5 *and*
$NC = \{\{2,3\},\{3,4\},\{1,5\},\{2,5\},\{3,5\},\{4,5\}\}$ *and* $C = \{\{1,2\},\{1,4\}\}$.
• *Apply* $Crit2$: *for* $l = 2$, *we eliminate* $\{1,5\}$, *since* $\{1,2\} \in NC \bigcup C$, $\{2,5\} \in NC$ *and* $lm(f_2)$ *divides* $lcm(lm(f_1), lm(f_5))$. *For* $l = 3$ *we eliminate* $\{2,5\}$, *since*
$\{2,3\} \in NC \bigcup C$, $\{3,5\} \in NC$, *and* $lm(f_3)$ *divides* $lcm(lm(f_2), lm(f_5))$ *and similarly for* $l = 4$ *we eliminate* $\{4,5\}$. *But we have no pair that can be eliminated for* $l = 1$. *Then we have* $NC = \{\{2,3\},\{3,4\},\{3,5\}\}$. *We apply normal selection strategy to choose* $\{3,5\}$ *and compute the S-polynomial such that* $S(f_3, f_5) = xz^3 - xz^2$, *Say* $f_6 = xz^3 - xz^2$. *Then we update* $NC = \{\{2,3\},\{3,4\},\{1,6\},\{2,6\},\{3,6\},\{4,6\},\{5,6\}\}$ *and* $C = \{\{1,2\},\{1,4\},\{3,5\}\}$
• *Apply* $Crit2$: *For* $l = 2$ *we eliminate* $\{1,6\}$ *since* $\{1,2\} \in NC \bigcup C$,
$\{2,6\} \in NC$ *and* $lm(f_2)$ *divides* $lcm(lm(f_1), lm(f_6))$. *and For* $l = 3$ *we eliminate* $\{2,6\}$, *since* $\{2,3\} \in NC \bigcup C, \{3,6\} \in NC$, *and* $lm(f_3)$ *divides* $lcm(lm(f_2), lm(f_6))$. *For* $l = 3$ *we eliminate* $\{4,6\}$ *and* $\{5,6\}$ *since* $\{3,6\} \in NC$ *such that* $lm(f_3)$ *divide* $lcm(lm(f_4, lm(f_6))$ *and* $lcm(lm(f_5), lm(f_6))$. *But for* $l = 1$ *and* $l = 5$ *we have nothing to eliminate using* $Crit2$. *Now we are left with* $NC = \{\{2,3\},\{3,4\},\{3,6\}\}$. *We apply the normal selection strategy to choose* $\{3,6\}$ *and compute the S-polynomial such that* $S(f_3, f_6) = xyz^2 - xz^2$ *and* $f_7 = xyz^2 - xz^2$. *We then update*
$NC = \{\{2,3\},\{3,4\},\{1,7\},\{2,7\},\{3,7\},\{4,4\},\{5,7\},\{6,7\}\}$ *and*
$C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\}\}$.
• *Apply* $Crit2$: *For* $l = 2$ *We eliminate* $\{1,7\}$, *since* $\{1,2\} \in NC \bigcup C$,
$\{2,7\} \in NC$ *and* $lm(f_2)$ *divides* $lcm(lm(f_1), lm(f_7)$. *For* $l = 3$ *we can eliminate* $\{5,7\}$ *and* $\{6,7\}$ *since* $lm(f_3)$ *divide both* $lcm(lm(f_5), lm(f_7))$ *and* $lcm(lm(f_6), lm(f_7))$. *In*

addition,using the second main WHILE loop of algorithm 2.2 *we can eliminate* $\{2,3\}$ *taking* $s=7, i=2$ *and* $j=3$, *since* $\{2,7\} \in NC$,$\{2,3\} \in NC$,$\{3,7\} \in NC$ *and* $lm(f_7)$ *divide* $lcm(lm(f_2), lm(f_3))$ *then we can eliminate* $\{2,3\}$. *We also eliminate* $\{3,4\}$ *from NC since* $\{3,7\} \in NC$, $\{4,7\} \in NC$, *and* $lm(f_7)$ *divide* $lcm(lm(f_3), lm(f_4))$. *Hence we have* $NC = \{\{2,7\},\{3,7\},\{4,7\}\}$. *Again using normal selection strategy we choose* $\{4,7\}$ *to compute the S -polynomial such that* $S(f_4, f_7) = -z^4 + x^2z^2$, *and say* $f_8 = -z^4 + x^2z^2$. *We then update* $NC = \{\{2,7\},\{3,7\},\{1,8\},\ldots,\{7,8\}\}$ *and* $C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\},\{4,7\}\}$.

• *Apply* $Crit2$: *For* $l=2$ *We eliminate* $\{1,8\}$ *since* $\{1,2\} \in NC \bigcup C$, $\{2,8\} \in NC$ *and* $lm(f_2)$ *divides* $lcm(lm(f_1), lm(f_8))$. *For* $l=3$ *we eliminate* $\{7,8\}$ *since* $\{3,8\} \in NC$ *and* $lm(f_3)$ *divides* $lcm(lm(f_7), lm(f_8))$, *and For* $l=5$ *we eliminate* $\{3,8\}$ *since* $\{5,8\} \in NC$ *and* $lm(f_5)$ *divides* $lcm(lm(f_3), lm(f_8))$ *Moreover,when* $S(f_2, f_7) \xrightarrow{G}_+ 0$ *and* $S(f_3, f_7) \xrightarrow{G}_+ 0$ *which lead us to eliminate* $\{2,7\}$ *and* $\{3,7\}$ *results* $NC = \{\{2,8\},\{4,8\},\{5,8\},\{6,8\}\}$. *Using normal selection strategy we also choose* $\{6,8\}$ *to compute the S-polynomial such that* $S(f_6, f_8) = x^3z^2 - xz^3$ *and* $f_9 = x^3z^2 - xz^3$. *We update* $NC = \{\{2,8\},\{4,8\},\{5,8\},\{1,9\},\{2,9\},\ldots,\{8,9\}\}$ $C = \{\{1,2\},\{1,4\},\{3,5\},\{3,6\},\{4,7\},\{6,8\}\}$.

• *Apply* $Crit2$ *For* $l=2$ *we eliminate* $\{1,9\}$ *since* $\{1,2\} \in NC \bigcup C$, $\{2,9\} \in NC$ *and* $lm(f_2)$ *divides* $lcm(lm(f_1), lm(f_9))$. *for* $l=3$ *we eliminate* $\{2,9\}$ *since* $\{3,9\} \in NC$ *and* $lm(f_3)$ *divide* $lcm(lm(f_2), lm(f_9))$ *and*

For $l=4$ *we eliminate* $\{3,9\},\{5,9\},\{7,9\}$ *since* $\{4,9\} \in NC$ *and* $lm(f_4)$ *divide* $lcm(lm(f_3), lm(f_9)), lcm(lm(f_5), lm(f_9))$ *and* $lcm(lm(f_7), lm(f_9))$.

For $l=6$ *we eliminate* $\{8,9\}$ *since* $\{6,9\} \in NC$ *and* $lm(f_6)$ *divides* $lcm(lm(f_8), lm(f_9))$. *Then we have* $NC = \{\{2,8\},\{4,8\},\{5,8\},\{4,9\},\{6,9\}\}$. *But the S-polynomial corresponding to the remaining pairs in NC all reduce to zero which gives* $NC = \emptyset$. *Thus*

$G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9\}$ *is the Groebner basis for the ideal* $I = \langle f_1, f_2, f_3\rangle$.

2.5 Groebner basis over ring

Definition 2.5.1. [1] *Given two polynomials f and h and a set of non-zero polynomials $F = \{f_1, \ldots, f_s\}$ in A, we say that f reduces to h modulo F in one step,denoted*

$$f \xrightarrow{F} h$$

if and only if

$$h = f - (c_1 X_1 f_1 + \cdots + c_s X_s f_s)$$

$c_1, \ldots, c_s \in R$ and monomials $X_1, \ldots, X_s$ where $lm(f) = X_i lm(f_i)$ for all i such that $c_i \neq 0$ and $lt(f) = c_1 X_1 lt(f_1) + \cdots + c_s X_s lt(f_s)$.

Example 2.5.2. *Let $f = 2x^3y, f_1 = 6x^2 + y + 1, f_2 = 10xy - x - y$ and $f_3 = 15y^2 + x$ in $\mathbb{Z}[x, y]$ with term order deglex such that $x > y$. So with $F = \{f_1, f_2, f_3, \}$ we see that $f \xrightarrow{F}_+ h$ where $h = -x^3 - x^2y - 2xy^2 - 2xy$ since $h = f - (2xyf_1 - x^2 f_2)$ and $2x^3y = lt(f) = 2xylt(f_1) - x^2 lt(f_2)$(Here $c_3 = 0$,since $lm(f) = x^3y$ is not divisible by $lm(f_3) = y^2$.*

We draw attention to the condition $lm(f) = X_i lm(f_i)$ for all i such that $c_i \neq 0$. Its purpose is to ensure that each $c_i X_i lt(f_i)$ in the difference $h = f - (c_1 X_1 f_1 + \cdots + c_s X_s f_s)$ with $c_i \neq 0$ is actually used to help cancel $lt(f)$. Because of the possibility of zero divisors in the ring R, we must be careful about this. For example, if we only required $lm(f) = lm(c_i X_i f_i)$ for all i such that $c_i \neq 0$, we could end up with a term $clm(f)$ remaining in h.

To see that consider the case, $R = \mathbb{Z}_{10}$ with deglex $x > y$ and let $f = 3y, f_1 = 5x^2 + y$ and $f_2 = y$. Then $lt(f) = 2lt(f_1) + 3lt(f_2)$ and $lm(f) = lm(2f_1) = lm(3f_2) = y$ where as $h = f - (2f_1 + 3f_2) = -2y$

Definition 2.5.3. [1] *We will say that linear equation are solvable in R provided that*

1. *Given $a, a_1, \ldots, a_m \in R$,there is an algorithm to determine whether $a \in \langle a_1, \ldots, a_m \rangle_R$ and if it is to compute $b_1, \ldots, b_m \in R$ such that $a = a_1 b_1 + \cdots + a_m b_m$*
2. *Given $a_1, \ldots, a_m \in R$,there is an algorithm that computes a set of generators for the R-module*
   $Syz_R(a_1, \ldots, a_m) = \{(b_1, \ldots, b_m) \in R^m | a_1 b_1 + \cdots + a_m b_m = 0\}$.

Definition 2.5.4. [1] *Let f, h and $f_1, \ldots, f_s$ be polynomials in A with $f_1, \ldots, f_s \neq 0$ and let $F = \{f_1, \ldots, f_s\}$, we say that f reduces to h modulo F,denoted*

$$f \xrightarrow{F}_+ h$$

if and only if there exists polynomials $h_1, \ldots, h_{t-1} \in A$ such that

$$f \xrightarrow{F} h_1 \xrightarrow{F} h_2 \xrightarrow{F} \cdots \xrightarrow{F} h_{t-1} \xrightarrow{F} h.$$

Definition 2.5.5. [1] *A polynomial r is called minimal with respect to a set of non-zero polynomials $F = \{f_1, \ldots, f_s\}$ if r cannot be reduced.*

Lemma 2.5.6. [1] *A polynomial $r \in A$ with $r \neq 0$ is minimal with respect to a set of non-zero polynomials $F = \{f_1, \ldots, f_s\} \subseteq A$ if and only if $lt(r) \notin \langle lt(F)\rangle$.*

Proof. ($\Rightarrow$) Suppose r is minimal with respect to $F = \{f_1, \ldots, f_s\}$
W.T.S: $lt(r) \notin \langle lt(F)\rangle$.
Suppose the contradiction,that is $lt(r) \notin \langle lt(F)\rangle$, then $lt(r) = h_1 lt(f_1) + \cdots + h_s lt(f_s)$ for some polynomial $h_i \in A$. If we expand this equation out into its individual terms, we see that the only monomial that can occur with a non-zero coefficient is $lm(r)$; we may assume that h_i is a term $c_i X_i$,then $r - c_1 X_1 + \cdots + c_s X_s$ is the reduction of r, this implies that r reduced with respect to $F = \{f_1, \ldots, f_s\}$ but this contradict our assumption.
($\Leftarrow$) Suppose $lt(r) \notin \langle lt(F)\rangle$
let r is not minimal ,then r can be reduced and so by Definition 2.5.1 we have $lt(r) = c_1 X_1 lt(f_1) + \cdots + c_1 X_1 lt(f_s)$ for $c_i \in R$ and X_i are monomials in A,this implies that $lt(r) \in \langle lt)(F)\rangle$,this contradicts our assumption,
Therefore r is minimal. □

Theorem 2.5.7. *(**Division algorithm over a ring**)* [1] *Let $f, f_1, \ldots, f_s \in A$ with $f, f_1, \ldots, f_s \neq 0$, and set $F = \{f_1, \ldots, f_s\}$. Then there is an $r \in A$, minimal with respect to F ,such that $f \xrightarrow{F}_+ r$. Moreover there are $h_1, \ldots, h_s \in A$*

$$f = h_1 f_1 + \cdots + h_s f_s + r$$

with

$$lm(f) = max((max_{1 \leq i \leq s} lm(h_i) lm(f_i)), lm(r))$$

If linear equations are solvable in R,then $h_1, \ldots, h_s, r$ are computable.

Theorem 2.5.8. [1] *Let I be an ideal of A and let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in I ,Then the following are equivalent*

1. $\langle lt(G)\rangle = \langle lt(I)\rangle$
2. *For any polynomial $f \in A$ we have*

$$f \in I \text{ if and only if } f \xrightarrow{G}_+ 0$$

3. *For all $f \in I, f = h_1g_1 + \cdots + h_tg_t$,for some $h_1, \ldots, h_t \in A$ such that*

$$lm(f) = max_{1\leq i\leq t}(lm(h_i)lm(g_i))$$

Proof. (1) $\Rightarrow$ (2) Assume that $f \in I$. Then by Theorem 2.5.7,that $f \xrightarrow{G}_+ r$ with r is minimal.
If $r \neq 0$,then,by Lemma 2.5.6, $lt(r) \notin \langle lt(G)\rangle$. But $f \in I$ and $f - r \in I$ imply that $r \in I$ and so $lt(r) \in \langle lt(I)\rangle = \langle lt(G)\rangle$,which is a contradiction.
Conversely, if $f \xrightarrow{G}_+ 0$, then $f \in I$
(2) $\Rightarrow$ (3) This is a special case for $r = 0$ of Theorem 2.5.7
(3) $\Rightarrow$ (1) Since $G \subseteq I$,then $\langle lt(G)\rangle \subseteq \langle lt(I)\rangle$,for the reverse direction
Let $f \in I$. We have that $f = h_1g_1 + \cdots + h_tg_t$ such that $lm(f) = max_{1\leq i\leq t}(lm(h_i)lm(g_i))$

$$lt(f) = \sum_i lt(h_i)lt(g_i)$$

Where the sum is over all i satisfying $lm(f) = lm(f_i)lm(g_i)$.
Thus $lt(f) \in \langle lt(G)\rangle$
It is important to notice the form of Statement (3) in the Theorem. We use $lm(f) = max_{1\leq i\leq t}(lm(h_i)lm(g_i))$ instead of $lm(f) = max_{1\leq i\leq t}lm(h_ig_i)$, since over a ring R with zero divisors, we need not have $lm(h_i)lm(g_i) = lm(h_ig_i)$. □

Definition 2.5.9. [1] *A set G of non-zero polynomials contained in an ideal I is called a Groebner basis for I provided that G satisfies any one of the three equivalent conditions of Theorem* 2.5.8. *A set G of non-zero polynomials contained in A is called a Groebner basis provided that G is a Groebner basis for $\langle G\rangle$.*

Example 2.5.10. *Let $f_1 = 3x^2y - x, f_2 = 2z^2 - x \subseteq \mathbb{Z}[x, y, z]$, then $\{f_1, f_2\}$ is a Groebner basis for $\langle f_1, f_2\rangle$ with respect ta deglex where $x > y > z$ since by looking at all linear combination of f_1 and f_2 such that*

$\langle lt(I)\rangle = \langle 3x^2y, 2z^2, x^2yz^2\rangle = \langle 3x^2y, 2z^2\rangle = \langle lt(f_1), lt(f_2)\rangle$, *but* $\{f_1, f_2\}$ *is not a Groebner basis for* $\langle f_1, f_2\rangle$, *with respect to lex* $x > y > z$ *because* $3x^2y - 2z^2 \in \langle f_1, f_2\rangle$.
$3x^2y - 2z^2 \xrightarrow{\{f_1,f_2\}}_+ r$, *then* r *is not equal to* 0 *when we interchange the position of* f_1 *and* f_2.

Corollary 2.5.11. [1] *If* G *is a Groebner basis and* $f \in \langle G\rangle$ *and* $f \xrightarrow{G}_+ r$, *where* r *is minimal,then* $r = 0$

Proof. Since $f \in \langle G\rangle$ we have that $r \in \langle G\rangle$ and so, since G is a Groebner basis, we see that if $r \neq 0$ then r cannot be minimal by Lemma 2.5.6. □

2.6 Computing Groebner basis over a ring

Definition 2.6.1. [1] *For any subset* $J \subseteq \{1, \ldots, s\}$, *set* $X_J = lcm(X_j | j \in J)$. *We say that* J *is saturated with respect to* $X_1, \ldots, X_s$ *provided that for all* $j \in \{1, \ldots, s\}$,*if* X_j *divides* X_J ,*then* $j \in J$. *For any subset* $J \subseteq \{1, \ldots, s\}$, *we call the saturation of* J *the set* J' *consisting of all* $j \in J$ *such that* X_j *divides* X_J.

Example 2.6.2. *Let* $X_1 = xy, X_2 = x^2, X_3 = y$ *and* $X_4 = x^4$. *Then if*
$J = \{1, 2\}$ *we see that* $X_J = x^2y$ *and* J *is not saturated since* $3 \notin J$, *while* $X_3 = y$ *divides* X_J.
On the other hand if $J = \{1, 2, 3\}$ *we see that* $X_J = x^2y$, *then* J *is saturated since* 4 *is the only element of* $\{1, 2, 3, 4\}$ *not in* J *and* $X_4 = x^4$ *does not divide* x^2y.

Theorem 2.6.3. [1] *For each set* $J \subseteq \{1, \ldots, s\}$ *which is saturated with respect to* $X_1, \ldots, X_s$,*let* $B_J = \{b_{1J}, \ldots, b_{vjJ}\}$ *be generating set for the R-module of Syzygies* $Syz_R(c_j | j \in J)$. *(Note that each of the vectors* b_{vJ} *is in the R-module* $R^{|J|}$,*where* $|J|$ *denotes the cardinality of J.)For each such* b_{vJ}, *denotes its jth coordinate,for* $j \in J$, *by* b_{jvJ}. *Set*

$$S_{vJ} = \sum_{j \in J} b_{jvJ} \frac{X_J}{X_j} e_j$$

(Note that each of the vectors S_{vJ} *is in* A^s.*)Then the set of vectors* S_{vJ}, *for J ranging over all such saturated subsets of* $\{1, \ldots, s\}$ *and* $1 \leq v \leq vJ$, *forms a homogeneous generating set for the syzygy module* $Syz(c_1X_1, \ldots, c_sX_s)$.

Proof. Since each vectors S_{vJ} is homogeneous of degree X_J. Moreover,

S_{vJ} is a Syzygy of $[c_1X_1, \ldots, c_sX_s]$, Since

$$\begin{aligned}[c_1X_1, \ldots, c_sX_s]S_{vJ} &= [c_1X_1, \ldots, c_sX_s]\sum_{j\in J} b_{jvJ}\frac{X_J}{X_j}e_j \\ &= \sum_{j\in J} b_{jvJ}\frac{X_J}{X_j}c_jX_j = X_J\sum_{j\in J} b_{jvJ}c_j = 0\end{aligned}$$

By definition of b_{vJ}. Now, let $h = (h_1, \ldots, h_s) \in Syz(c_1X_1, \ldots, c_sX_s)$. Since $Syz(c_1X_1, \ldots, c_sX_s)$ is generated by homogeneous syzygies, it suffices to write h as a linear combination of the s_{vJ}'s in the case that h is a homogeneous syzygy , say of degree Y. We write $h = (d_1Y_1, \ldots, d_sY_s)$ for $d_1, \ldots, d_s \in R$ and monomials $Y_1, \ldots, Y_s$. Set $J = \{j|d_j \neq 0\}$ and let J' be saturation of J. We have that $Y_jX_j = Y$ for all $j \in J$,since h is homogeneous of degree Y. Then since h is a syzygy of $[c_1X_1, \ldots, c_sX_s]$,
We have $\sum_{j\in J} d_jY_jc_jX_j = Y\sum_{j\in J} d_jc_j = 0$. Thus $(d_j|j \in J')$ is the syzygy of $[c_j|j \in J']$ and by hypothesis

$$(d_j|j \in J') = \sum_{v=1}^{vJ'} r_v b_{vJ'}$$

that is, for each $j \in J'$

$$d_j = \sum_{v=1}^{vJ'} r_v b_{jvJ'}$$

for some $r_v \in R$. Now $Y_jX_j = Y$ for all $j \in J$ implies that $X_J = X_{J'}$ divides Y. It now follows that

$$\sum_{v=1}^{vJ'} r_v\frac{Y}{X_{J'}}S_{vJ'} = \sum_{v=1}^{vJ'}\sum_{j\in J'} r_v\frac{Y}{X_{J'}}\frac{X_{J'}}{X_j}b_{jvJ'}e_j$$

$$= \sum_{j\in J}(\sum_{v=1}^{vJ'} r_v b_{jvJ'})Y_je_j = \sum_{j\in J'} d_jY_je_j = \sum_{j=1}^{s} d_jY_je_j = h,$$

as desired.

□

Theorem 2.6.4. [1] *If R is Noetherian ring and linear equations are solvable in R then Algorithm 2.3 produces a Groebner basis $\langle f_1, \ldots, f_s\rangle$.*

INPUT:$F = \{f_1, \ldots, f_s\} \subseteq A = K[x_1, \ldots, x_n]$ with $f_i \neq 0$ $(1 \leq i \leq s)$

OUTPUT:$G = \{g_1, \ldots, g_t\}$,a Groebner basis for $\langle f_1, \ldots, f_s \rangle$

INITIALIZATION:$G = \emptyset$,$G' = F$

WHILE $G' \neq G$ **DO**

$G = G'$

Let the elements of G be $g_1, \ldots, g_t$

Compute B, a homogeneous generating set for $Syz(lt(g_1), \ldots, lt(g_t))$

FOR each $h = (h_1, \ldots, h_t) \in B$ **DO**

Reduce $h_1 g_1 + \cdots + h_t g_t \xrightarrow{G'}_+ r$, with r minimal with respect to G'

IF $r \neq 0$ **THEN**

$G' = G' \bigcup \{r\}$

Algorithm 2.3 Groebner basis Algorithm over a Ring

Proof. If the algorithm stops, it clearly, by Theorem 2.2.5,gives a Groebner basis for the ideal $\langle f_1, \ldots, f_s \rangle$. As the algorithm progresses we add ta a set of polynomials G a polynomial r, minimal with respect to G, to obtain a new set G'.
By Lemma 2.5.6, $lt(r) \notin \langle lt(G) \rangle$ and so $\langle lt(G) \rangle \subseteq \langle lt(G') \rangle$. Thus, since the ring A is Noetherian, the algorithm stops. □

We will incorporate the above algorithm with a more efficient method for computing the relevant syzygies which is proposed by Möller.

Möller has given a method for computing the syzygies that arise in

Algorithm 2.3. In particular, this method gives an efficient way ta avoid duplication in the computation of syzygies (see Algorithm 2.4).At each stage of Algorithm 2.3 we add one or more polynomials to the generating set for the ideal $\langle f_1, \ldots, f_s \rangle$. So we have ta compute a generating set for the syzygy module of this increased set of leading terms. The idea of Möller is to use the computations of syzygies already done in order to compute the new syzygies. Note that any syzygy of a set of leading terms

is automatically a syzygy of a larger set of leading terms (using zeros for the extra leading terms).

Again consider monomials $X_1, \ldots, X_s$ and a non-zero elements $c_1, \ldots, c_s \in R$. Let $S_\sigma = Syz(c_1X_1, \ldots, c_sX_\sigma)$ for $1 \leq \sigma \leq s$. We will compute a homogeneous generating set of $S_s = Syz(c_1X_1, \ldots, c_sX_s)$ by inductively constructing generating sets for the S_σ. We note that a homogeneous generating set of S_1,consists of a generating set of the ideal $\{r \in R | rc_1 = 0\}$ of R (called the annihilator of c_1 and denoted by $ann(c_1)$ viewed as a subset of A.

Also, if we take a homogeneous syzygy $(b_1Y_1, \ldots, b_\sigma Y_\sigma)$ in S_σ, there are two possibilities. Either $b_\sigma = 0$ and $(b_1Y_1, \ldots, b_{\sigma-1}Y_{\sigma-1})$ is a homogeneous syzygy in $S_{\sigma-1}$; or $b_\sigma \neq 0$ and $b_\sigma \in \langle c_1, \ldots, _{\sigma-1} \rangle_R : \langle c_\sigma \rangle_R$.

So we proceed as follows. We consider all subsets J of $\{1, \ldots, \sigma\}$, saturated with respect to $X_1, \ldots, X_\sigma$, such that $\sigma \in J$. For each such J let $b_{1J}, \ldots, b_{\mu J}$ denote a generating set for the ideal in R, $\langle c_j | j \in J, j \neq \sigma \rangle_R : \langle c_\sigma \rangle_R$. Now for each $b_{\mu J}$ there are $b_j \in R$ such that

$$\sum_{j \in J, j \neq \sigma} b_j c_j + b_{\mu J} c_\sigma = 0,$$

and we define the homogeneous syzygy in S_σ by

$$s_{\mu J} = \sum_{j \in J, j \neq \sigma} b_j \frac{X_J}{X_j} e_j + b_{\mu J} \frac{X_J}{X_\sigma} e_\sigma$$

(The b_j's may not be unique, but any choice will do.) We also consider a homogeneous generating set $a_1, \ldots, a_m$ for $S_{\sigma-1}$, which we assume by induction,has been computed. Define for $1 \leq i \leq m$, $(a_i, 0)$ to be the homogeneous syzygy in S_σ with the coordinates of a_i in the first $\sigma - 1$ coordinates and 0 in the last coordinate. We now can state

Theorem 2.6.5. [1] *The syzygies* $(a_1, 0), \ldots, (a_m, 0)$ *together with the syzygies* $s_{\mu J}$ *for* $J \subseteq \{1, \ldots, \sigma\}$ *saturated with respect to* $X_1, \ldots, X_\sigma$ *with* $\sigma \in J$*, form a homogeneous generating set for the syzygy module* S_σ*.*

Proof. Let $d = (d_1 Y_1, \ldots, d_\sigma Y_\sigma)$, for $d_1, \ldots, d_\sigma \in R$, and monomials $Y_1, \ldots, Y_\sigma$, be homogeneous syzygy in S_σ of degree Y.
If $d_\sigma = 0$,then $a_1, \ldots, a_{\sigma-1}$ are the homogeneous generating set for $S_{\sigma-1}$, This implies that $(a_1, 0), \ldots, (a_m, 0)$ are the generating set for S_σ,then d is a linear combination of $(a_1, 0), \ldots, (a_m, 0)$.
Suppose $d_\sigma \neq 0$. Let J' be the set of all j such that $d_j \neq 0$ and J be the saturation of J' in $\{1, \ldots, \sigma\}$. Note that $X_J = X_{J'}$ divides Y.
Then $d_\sigma \in \langle c_j | j \in J, j \neq \sigma \rangle_R : \langle c_\sigma \rangle_R$ and so $d_\sigma = \sum_{i=1}^{\mu J} r_i d_{\mu J}$
Let $s_{\mu J} = \sum_{j \in J, j \neq \sigma} d_j \frac{X_J}{X_j} e_j + d_{\mu J} \frac{X_J}{X_\sigma} e_\sigma$

$$((d_1 Y_1, \ldots, d_\sigma Y_\sigma) - \sum_{\mu=1}^{\mu J} r_\mu s_{\mu J} \frac{Y}{X_J})(c_1 X_1, \ldots, c_\sigma X_\sigma)$$

$$((d_1 Y_1, \ldots, d_\sigma Y_\sigma)(c_1 X_1, \ldots, c_\sigma X_\sigma) - (\sum_{\mu=1}^{\mu J} r_\mu s_{\mu J} \frac{Y}{X_J})(c_1 X_1, \ldots, c_\sigma X_\sigma)$$

$$Y \underbrace{\sum_{i=1}^{\sigma} d_i c_i}_{0} - \underbrace{(\sum_{\mu=1}^{\mu J} r_\mu s_{\mu J} \frac{Y}{X_J})(c_1 X_1), \ldots, c_\sigma X_\sigma)}_{0 (by\ definition\ of\ s_{\mu J})}$$

Then $d - \sum_{\mu=1}^{\mu J} r_\mu s_{\mu J} \frac{Y}{X_J}$ is a homogeneous syzygy with a zero in its σ^{th} coordinate and so is a linear combination of $(a_1, 0), \ldots, (a_m, 0)$, giving the desired result. □

Example 2.6.6. *To compute the generator for the* $Syz(3x^2y, 5x^2z, 9yz^2, 7xy^2z)$ *using the above theorem where* $R = \mathbb{Z}$*.*
Let $S_1 = Syz(3x^2y) = \langle 0 \rangle_\mathbb{Z}$
Let $S_2 = Syz(3x^2y, 5x^2z)$*,then the saturated subsets of* $\{1, 2\}$ *containing* 2 *are* 2 *and* $\{1, 2\}$ *but* $\mathbb{Z}$ *singletons does not form non-zero polynomial.so we compute for the set* $\{1, 2\}$ *then* $\langle 3 \rangle_\mathbb{Z} : \langle 5 \rangle_\mathbb{Z} = \langle 3 \rangle_\mathbb{Z}$ *then the corresponding syzygy will be* $(-5z, 3y, 0, 0)$*.*
$S_3 = Syz(3x^2y, 5x^2z, 9yz^2)$*, then the saturated subsets of* $\{1, 2, 3\}$ *containing containing* 3 *are* $\{3\}$ *and* $\{1, 2, 3\}$*, but we take set* $\{1, 2, 3\}$*, then we compute*
$\langle 3, 5 \rangle_\mathbb{Z} : \langle 9 \rangle_\mathbb{Z} = \langle 3 \rangle_\mathbb{Z} : \langle 9 \rangle_\mathbb{Z} = \langle 1 \rangle_\mathbb{Z}$ *then the corresponding syzygy will be* $(-3z^2, 0, x^2, 0)$*.*
$S_4 = Syz(3x^2y, 5x^2z, 9yz^2, 7xy^2z)$*, the saturated subset of* $\{1, 2, 3, 4\}$ *containing* 4 *are* $\{3, 4\}$*,*$\{1, 2, 4\}$ *and* $\{1, 2, 3, 4\}$*. For the set* $\{3, 4\}$ *we compute* $\langle 9 \rangle_\mathbb{Z} : \langle 7 \rangle_\mathbb{Z} = \langle 9 \rangle_\mathbb{Z}$ *then*

the corresponding syzygy will be $(0, 0, -7xy, 9z)$.
For the set $\{1, 2, 4\}$ *we compute* $\langle 3, 5\rangle_{\mathbb{Z}} : \langle 7\rangle_{\mathbb{Z}} = \langle 1\rangle_{\mathbb{Z}}$ *the corresponding Syzygy will be* $(-4yz, y^2, 0, x)$.
Then $Syz(3x^2y, 5x^2z, 9yz^2) = \langle(-5z, 3y, 0, 0), (-3z^2, 0, x^2, 0), (0, 0, -7xy, 9z), (-4yz, y^2, 0, x)\rangle$.

INPUT:$F = \{f_1, \ldots, f_s\} \subseteq R[x_1, \ldots, x_n]$ with $f_i \neq 0 (1 \leq i \leq s)$

OUTPUT:G a Groebner basis for $\langle f_1, \ldots, f_s\rangle$

INITIALIZATION:$G = F$ $\sigma = 1$,$m = s$

WHILE $\sigma \leq m$ **DO**

Compute $S = \{subset\ of\ \{1, \ldots, s\}\}$

saturated with respect to $lm(f_1), \ldots, lm(f_\sigma)$ *which contain* σ

FOR $J \in S$ **DO**

$X_J = lcm(X_j | j \in J)$

Compute generators b_{iJ} $i = 1, \ldots, \mu J$ for $\langle lc(f_j) | j \in J, j \neq \sigma\rangle_R : \langle lc(f_\sigma)\rangle_R$

FOR $1, \ldots, \mu j$ **DO**

Compute $b_j \in R, j \in J, j \neq \sigma$ such that

$\sum_{j\in J, j\neq\sigma} b_j lc(f_j) + b_{iJ} lc(f_\sigma) = 0$

Reduce$\sum_{j\in J, j\neq\sigma} b_j \frac{X_J}{lm(f_j)} f_j + b_{iJ} \frac{X_J}{lm(F_\sigma)} f_\sigma \xrightarrow{G}_+ r$ where r is minimal with respect to G

IF $r \neq 0$ **THEN**

$f_{m+1} = r$

$G = G \bigcup \{r\}$

$m = m + 1$

$\sigma = \sigma + 1$

Algorithm 2.4 Groebner basis Algorithm in $R[x_1, \ldots, x_n]$ using Möller's Method.

Using the following examples we will verify how to use Algorithm 2.3 and Algorithm 2.4.

Example 2.6.7. *Let* $f_1 = 3x^2y - 3yz + y, f_2 = 5x^2z - 8z^2 \subseteq \mathbb{Z}[x, y, z]$ *with a term order deglex such* $x > y > z$, *then to compute a Groebner basis for* $\langle f_1, f_2\rangle$ *we use algorithm* 2.3 *and* 2.4
Let $lt(f_1) = 3x^2y$ *and* $lt(f_2) = 5x^2z$.

For the case $\sigma = 1$ in the algorithm does not generate new polynomials, since $\langle 0\rangle_{\mathbb{Z}} : \langle 3\rangle_{\mathbb{Z}} = \langle 0\rangle_{\mathbb{Z}}$
For the case $\sigma = 2$, The only non-singleton saturated subset of $\{1,2\}$ containing 2 is $\{1,2\}$. We compute $\langle 3\rangle_{\mathbb{Z}} : \langle 5\rangle_{\mathbb{Z}} = \langle 3\rangle_{\mathbb{Z}}$ which gives the syzygies $(5z, -3y)$ in $Syz(3x^2y, 5x^2z)$, then the corresponding S-polynomial is $5zf_1 - 3yf_2 = 9yz^2 + 5yz$ which is minimal with respect to G,then say $f_3 = 9yz^2 + 5yz$.
To compute the new syzygies,we need to consider the non-singleton saturated subset of $\{1,2,3\}$ containing 3, thus $\{1,2,3\}$ is the only saturated subset of $\{1,2,3\}$.
For $\{1,2,3\}$ compute $\langle 3,5\rangle_{\mathbb{Z}} : \langle 9\rangle_{\mathbb{Z}} = \langle 1\rangle_{\mathbb{Z}}$ giving the syzygy $(3z^2, 0, -x^2)$ in $Syz(3x^2y, 5x^2z, 9yz^2)$, then the corresponding S-polynomial is $3z^2f_1 - x^2f_3 = -5x^2yz - 9yz^3 - 3yz^2$, then

$$-5x^2yz - 9yz^3 - 3yz^2 \xrightarrow{f_2}_{+} -9yz^3 - 5yz^2 \xrightarrow{f_3}_{+} 0$$

Then $\{f_1, f_2, f_3\}$ is a Groebner basis for $\langle f_1, f_2\rangle$.

Remark: In the above example we take only non-singleton saturated subset because $\mathbb{Z}$ is an integral domain such that $\langle 0\rangle_{\mathbb{Z}} : \langle n\rangle_{\mathbb{Z}} = \langle 0\rangle_{\mathbb{Z}}$, for $n \in \mathbb{Z}$.

Example 2.6.8. *We consider the polynomials $f_1 = 2x^2y + 3z, f_2 = 5x^2z + y$ in $\mathbb{Z}_{15}[x,y,z]$ with a term order deglex such that $x > y > z$.*
Then to compute a Groebner basis for $\langle f_1, f_2\rangle$.
We first consider $\sigma = 1$, we do not consider because we can not add non-zero polynomial.
We next compute the saturated subsets of $\{1,2\}$ which contain 2, these are $\{2\}$ and $\{1,2\}$. For the set $\{2\}$. We compute $\langle 0\rangle_{\mathbb{Z}_{15}} : \langle 5\rangle_{\mathbb{Z}_{15}} = \langle 3\rangle_{\mathbb{Z}_{15}}$. This gives S-polynomial $3f_2 = 3y$. and say $f_3 = 3y$.
For the set $\{1,2\}$. We compute $\langle 2\rangle_{\mathbb{Z}_{15}} : \langle 5\rangle_{\mathbb{Z}_{15}} = \langle 1\rangle_{\mathbb{Z}_{15}}$, which gives the S-polynomials $10zf_1 - yf_2 = 14y^2$ and it is reduced with respect to $G = \{f_1, f_2, f_3\}$,then add to G as $f_4 = 14y^2$.
We now compute the saturated subset of $\{1,2,3\}$ which contain 3, these are $\{3\}, \{1,3\}$ and $\{1,2,3\}$.
For the set $\{3\}$, we compute $\langle 0\rangle_{\mathbb{Z}_{15}} : \langle 3\rangle_{\mathbb{Z}_{15}} = \langle 5\rangle_{\mathbb{Z}_{15}}$, which gives the S-polynomial $5f_3 = 0$.
For the set $\{1,3\}$ we compute $\langle 2\rangle_{\mathbb{Z}_{15}} : \langle 3\rangle_{\mathbb{Z}_{15}} = \langle 1\rangle_{\mathbb{Z}_{15}}$, which gives the S-polynomial $9f_1 - x^2f_3 = 12z$ which is minimal then add $f_5 = 12z$ to G.
For the set $\{1,2,3\}$. we compute $\langle 2,5\rangle_{\mathbb{Z}_{15}} : \langle 3\rangle_{\mathbb{Z}_{15}} = \langle 2\rangle_{\mathbb{Z}_{15}} : \langle 3\rangle_{\mathbb{Z}_{15}} = \langle 1\rangle_{\mathbb{Z}_{15}}$ which

gives the same polynomial to $\{1,3\}$.
We next compute the saturated subset of $\{1,2,3,4\}$ *which contain* 4, *these are* $\{3,4\}$ *and* $\{1,3,4\}$.
For the set $\{3,4\}$, *we compute* $\langle 3\rangle_{\mathbb{Z}_{15}} : \langle 14\rangle_{\mathbb{Z}_{15}} = \langle 3\rangle_{\mathbb{Z}_{15}}$, *which gives the S-polynomials* $14yf_3 - 3f_4 = 0$.
For the set $\{1,3,4\}$, *we compute* $\langle 2,3\rangle_{\mathbb{Z}_{15}} : \langle 14\rangle_{\mathbb{Z}_{15}} = \langle 2\rangle_{\mathbb{Z}_{15}} : \langle 14\rangle_{\mathbb{Z}_{15}} = \langle 1\rangle_{\mathbb{Z}_{15}}$, *which gives the S-polynomial* $7yf_1 - x^2f_4 = 6yz \xrightarrow{f_3}_{+} 0$.
Next we compute the saturated subset of $\{1,2,3,4,5\}$ *contain* 5, *these are* $\{2,5\}$,$\{3,5\}$,$\{3,4,5\}$, $\{1,2,3,5\}$ *and* $\{1,2,3,4,5\}$.
For the set $\{2,5\}$, *we compute* $\langle 5\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}} = \langle 5\rangle_{\mathbb{Z}_{15}}$, *which gives the S-polynomial* $12f_2 - 5x^2f_5 = 12y \xrightarrow{f_3}_{+} 0$.
For the set $\{3,5\}$, *we compute* $\langle 3\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}} = \langle 1\rangle_{\mathbb{Z}_{15}}$ *which gives the S-polynomial* $12zf_3 - yf_5 = 9yz \xrightarrow{f_3}_{+} 0$.
For the set $\{3,4,5\}$, *we compute* $\langle 3,14\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}} = \langle 14\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}} = \langle 1\rangle_{\mathbb{Z}_{15}}$, *which gives the same polynomial to* $\{3,5\}$.
For the set $\{1,2,3,5\}$, *we compute* $\langle 2,5,3\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}} = \langle 5,3\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}} = \langle 1\rangle_{\mathbb{Z}_{15}}$, *which rise the S-polynomial to zero.*
For the set $\{1,2,3,4,5\}$, *we compute*
$\langle 2,5,3,14\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}} = \langle ,5,3,14\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}} = \langle 3,14\rangle_{\mathbb{Z}_{15}} : \langle 12\rangle_{\mathbb{Z}_{15}}$ *which is the same to the set* $\{3,4,5\}$ *the nothing to be add to the polynomial.*
Then $\{f_1,f_2,f_3,f_4,f_5\}$ *is a Groebner basis for the ideal* $\langle f_1,f_2\rangle$.

Chapter 3

Application of Groebner Basis

This section devoted to giving a number of applications of the theory developed in the previous section to computations in polynomial rings and also give some applications to computations which use polynomial rings.

Since Groebner basis has many applications in many disciplines,we only focus in algebraic geometry and commutative algebra.

3.1 Elementary Applications of Groebner Basis

3.1.1 Ideal Membership Problem

Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal of $K[x_1, \ldots, x_n]$, Given $f \in K[x_1, \ldots, x_n]$, to determine whether $f \in I$, that is find $u_1, \ldots, u_s \in K[x_1, \ldots, x_n]$ such that

$$f = u_1 f_1 + \cdots + u_s f_s$$

By Theorem 1.3.2 if $F = \{f_1, \ldots, f_s\}$ is a Groebner basis for I, then

$$f \in I \Longleftrightarrow f \xrightarrow{F}_{+} 0$$

So if $F = \{f_1, \ldots, f_s\}$ is not a Groebner basis for I, we can not determine whether f belongs to I due to the fact that if we interchange the position of the f_i's the

remainder is not unique. Since every ideal has a Groebner basis then we compute the Groebner basis for the ideal to solve the ideal membership problem.

Example 3.1.1. *Let* $I = \langle f_1 = -x^3 + y, f_2 = x^2y - z\rangle \subseteq \mathbb{Q}[x, y, z]$ *with a term order lex, and* $f = xy^3 - z^2 + y^5 - z^3$, *to decide whether* f *belongs to* I, *if we use directly division algorithm it is impossible since* $lt(f_1)$ *and* $lt(f_2)$ *do not divide* $lt(f)$ *,the we need to find the Groebner basis for* I.
Then $\{g_1 = x^3 - y, g_2 = x^2y - z, g_3 = y^5 - z^3, g_4 = xz - y^2, g_5 = xy^3 - z^2\}$ *is a Groebner basis for* I, *then*

$$f = g_3 + g_5$$

This implies $f \in I$.

3.1.2 Quotients of Polynomial Rings

Definition 3.1.2. [6] *Let* $I \subset K[x_1, \ldots, x_n]$ *be an ideal and let* $f, g \in K[x_1, \ldots, x_n]$. *We say that* f *and* g *are congruent modulo* I, *written as* $f \equiv g(modI)$, *if* $f - g \in I$

Theorem 3.1.3. [6] *Let* $I \subset K[x_1, \ldots, x_n]$, *Then congruence modulo* I *is an equivalence relation on* $K[x_1, \ldots, x_n]$.

Proof. Congruence modulo I is reflexive since $f-f = 0 \in I$, for every f in $K[x_1, \ldots, x_n]$. To prove symmetry, suppose that $f \equiv g(modI)$. Then $f - g \in I$, which implies that $g-f = (-1)(f-g) \in I$ as well.Hence $g \equiv f(modI)$ also. Finally, we need to consider transitivity. If $f \equiv g(modI)$ and $g \equiv h(modI)$, then $f-g, g-h \in I$. Since I is closed under addition then $f - h = f - g + g - h \in I$. Hence $f \equiv h(modI)$. □

An equivalence relation on the set S partitions S into a collection of disjoint subsets called equivalence class. For any $f \in K[x_1, \ldots, x_n]$,the class f is the set

$$[f] = \{g \in K[x_1, \ldots, x_n] | g \equiv f(modI)\}$$

Definition 3.1.4. [6] *The quotient of* $K[x_1, \ldots, x_n]$ *modulo* I, *written as* $K[x_1, \ldots, x_n]/I$ *is the set of equivalence classes for congruent modulo* I*:*

$$K[x_1, \ldots, x_n]/I = \{[f] : f \in K[x_1, \ldots, x_n]\}$$

Theorem 3.1.5. [6] *Let I be an ideal in $K[x_1, \ldots, x_n]$. The quotient $K[x_1, \ldots, x_n]/I$ is commutative ring under the sum and product operation given below*
$[f] + [g] = [f + g]$ *(sum in $K[x_1, \ldots, x_n]$)*
$[f][g] = [fg]$ *(product in $K[x_1, \ldots, x_n]$)*

Proof. First we need to show well-defined property of the operations.
If $f' \in [f]$ and $g' \in [g]$, then $f' = f + a$ and $g' = g + b$, where $a, b \in I$. Hence

$$f' + g' = (f + a) + (g + b) = (f + g) + (a + b)$$

Since $a + b \in I$, it follows that $f' + g' \equiv f + g(modI)$, so $[f' + g'] = [f + g]$
Similarly

$$f'g' = (f + a)(g + b) = fg + fb + ag + ab$$

since $a, b \in I$, $fb + ag + ab \in I$. Thus $f'g' \equiv fg(modI)$, So
$[f'g'] = [fg]$
Since the above operations are well-defined other properties of to be commutative ring satisfied immediately with additive identity $[0] \in K[x_1, \ldots, x_n]/I$ and multiplicative identity $[1] \in K[x_1, \ldots, x_n]/I$. □

3.1.3 Algorithmic computations in $K[x_1, \ldots, x_n]/I$

In this section, we will use the division algorithm to produce simple representatives of equivalence classes for congruence modulo I, where $I \subset K[x_1, \ldots, x_n]$ is an ideal.These representatives will enable us to develop an explicit method for computing the sum and product operations in a quotient ring $K[x_1, \ldots, x_n]/I$.

The basic idea that we will use is a direct consequence of the fact that the remainder on division of a polynomial f by a Groebner basis G for an ideal I is uniquely determined by the polynomial f.

Theorem 3.1.6. [6] *Fix a monomial ordering on $K[x_1, \ldots, x_n]$ and let $I \subset K[x_1, \ldots, x_n]$ be an ideal, let $\langle lt(I) \rangle$ will denote the ideal generated by the leading terms of elements of I*

1. *Every $f \in K[x_1, \ldots, x_n]$ is congruent modulo I to a unique polynomial r which is K-linear combination of the monomials in the complement of $\langle lt(I) \rangle$.*

2. *The element of* $\{X^\alpha : X^\alpha \notin \langle lt(I)\rangle\}$ *are "linearly independent modulo* I*" that is*

$$\sum_\alpha c_\alpha X^\alpha \equiv 0(modI)$$

Where the X^α *are all the in the complement of* $\langle lt(I)\rangle$*,then* $c_\alpha = 0$ *for all* α*.*

Proof. (1) Let G be a Groebner basis for I and $f \in K[x_1, \ldots, x_n]$. Then by Proposition 1.3.5, $f = q + r$ where $q \in I$ and $r \in K[x_1, \ldots, x_n]$. Hence $f - r = q \in I$, so $f \equiv r(modI)$. The division algorithm tells us that r is a K-linear combination of the monomials $X^\alpha \notin \langle lt(I)\rangle$. The uniqueness of r is from Proposition 1.3.5.
(2) To show $\{X^\alpha : X^\alpha \notin \langle lt(I)\rangle\}$ is "linearly independent modulo I"
Suppose the contradiction, that is there exist c_α's not all zero such that

$$\sum_\alpha c_\alpha X^\alpha \equiv 0(modI)$$

then there exist some α's such that $\sum_\alpha c_\alpha X^\alpha \in I$. But it contradicts the hypothesis that $X^\alpha \notin \langle lt(I)\rangle$.
Therefore $\{X^\alpha : X^\alpha \notin \langle lt(I)\rangle\}$ is "linearly independent modulo I." □

Theorem 3.1.7. [6] *Let* $I \subset K[x_1, \ldots, x_n]$ *be an ideal.Then* $K[x_1, \ldots, x_n]/I$ *is isomorphic as* K*-vector space to* $S = \langle X^\alpha : X^\alpha \notin \langle lt(I)\rangle$.

Proof. Let us define a map $\Phi : K[x_1, \ldots, x_n]/I \longrightarrow S$ defined as
$\Phi([f]) = N_G(f)$,where $N_G(f)$ is a normal form f with respect to G, where G is a Groebner basis for I.
(i)W.T.S: Φ is well-defined
Let $[f], [g] \in K[x_1, \ldots, x_n]/I$, such that $[f] = [g]$, this implies $f \equiv g(modI)$, then there exists $q \in I$, such that $f = q + g$. Thus $N_G(f) = N_G(q) + N_G(g)$. But $N_G(q) = 0$, since $q \in I$, so $N_G(f) = N_G(g)$. Then Φ is well-defined.
(ii) Φ is one-to-one

$$\begin{aligned} \Phi([f]) &= \Phi([g]), for\ [f], [g] \in K[x_1, \ldots, x_n]/I. \\ N_G(f) &= N_G(g) \end{aligned}$$

Then $f - g = (f - N_G(f)) - (g - N_G(g)) \in I$ and hence $f - g \in I$ implies that $f \equiv g(modI)$, then $[f] = [g]$.
(iii) Φ is onto due to Proposition 1.3.5

Hence it remain to show that Φ preserves vector space operation.
Let $c_1, c_2 \in K$ and $f_1, f_2 \in K[x_1, \ldots, x_n]$, then $c_1 f_1 + c_2 f_2 - (c_1 N_G(f_1) + c_2 N_G(f_2)) \in I$ and $(c_1 N_G(f_1) + c_2 N_G(f_2))$ is reduced with respect to G.
Then $N_G(c_1 f_1 + c_2 f_2) = c_1 N_G(f_1) + c_2 N_G(f_2)$ Then Φ preserves vector space operation.
$K[x_1, \ldots, x_n]/I$ is isomorphic as K-vector space to $S = \langle X^\alpha : X^\alpha \notin \langle lt(I) \rangle$. □

Corollary 3.1.8. [1] *Let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis for I,a basis of the K-vector space $K[x_1, \ldots, x_n]/I$ consists of the Cosets of all the monomials X such that $lm(g_i)$ does not divide X for all $i = 1, \ldots, t$.*

Proof. Let $f \in K[x_1, \ldots, x_n]$, $f + I = N_G(f) + I$ in $K[x_1, \ldots, x_n]/I$. Since $N_G(f)$ is reduced with respect to G, by the above Theorem $N_G(f)$ is a K-linear combination of monomials X such that $lm(g_i)$ does not divide X for all $i = 1, \ldots, t$. Finally, the cosets of such power products are linearly independent by Theorem 3.1.6. □

Example 3.1.9. *Let $I = \langle x^2 + y - 1, xy - 2y^2 + 2y \rangle \subseteq \mathbb{Q}[x, y, z]$ with term order deglex.*
Then $\langle xy - 2y^2 + 2y, x^2 + y - 1, y^3 - \frac{7}{4}y^2 + \frac{3}{4}y \rangle$ is a Groebner basis for I. Then $\langle lt(I) \rangle = \langle xy, x^2, y^3 \rangle$, Then $\mathbb{Q}[x, y, z]/I$ is generated by $\{1, y, y^2, x\}$.

Next we want to determine whether $f + I$ of $K[x_1, \ldots, x_n]/I$ is invertible or not.

the following theorem gives the answer for our question.

Theorem 3.1.10. [1] *Let $I = \langle f_1, \ldots, f_s \rangle \subset K[x_1, \ldots, x_n]$ be an ideal and $f \in K[x_1, \ldots, x_n]$, then $f + I$ has an inverse in $K[x_1, \ldots, x_n]/I$ if and only if $1 \in \langle f, f_1, \ldots, f_s \rangle$.*

Proof. Suppose $f + I$ has an inverse in $K[x_1, \ldots, x_n]/I$, then there exists $g \in K[x_1, \ldots, x_n]$, such that

$$(f + I)(g + I) = 1 + I$$

then $fg - 1 \in \langle f_1, \ldots, f_s \rangle$.

$$1 = \underbrace{1 - fg}_{\in \langle f_1, \ldots, f_s \rangle} + \underbrace{fg}_{\in \langle f \rangle}$$

then $1 \in \langle f, f_1, \ldots, f_s \rangle$.
Suppose $1 \in \langle f, f_1, \ldots, f_s \rangle$, then

$$1 = gf + \sum_{i=1}^{s} h_i f_i$$

Where $g, h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$
Then

$$\begin{aligned} fg &\in I \\ fg + I &= 1 + I \\ (f + I)(g + I) &= 1 + I \end{aligned}$$

then $g + I$ is the inverse of $f + I$. □

Thus, given an ideal $I = \langle f_1, \ldots, f_s \rangle$ and a polynomial $f \in K[x_1, \ldots, x_n]$, to determine $f + I$ has an inverse in $K[x_1, \ldots, x_n]/I$ and to compute the inverse, we first find a reduced Groebner basis H for the ideal $\langle f, f_1, \ldots, f_s \rangle$. If $H \neq \{1\}$, then $f + I$ does not have an inverse in $K[x_1, \ldots, x_n]/I$.

If $H = \{1\}$, 1 can be expressed as linear combination of $f, f_1, \ldots, f_s$, then

$$1 = h_1 f_1 + \cdots + h_s f_s + gf$$

Where $g, h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$

Then the polynomial g is then the inverse of f modulo I.

Example 3.1.11. *Let $I = \langle f_1 = x^2 + y^2 + 1, f_2 = x^2y + 2xy + x \rangle \subset \mathbb{Z}_5[x, y]$ with term order lex, let $y^2 + I \in \mathbb{Z}_5[x, y]/I$, to determine $y^2 + I$ is invertible in $\mathbb{Z}_5[x, y]/I$, We compute the Groebner basis for*
$\langle x^2 + y^2 + 1, x^2y + 2xy + x, y^2 \rangle$, Then $\{1\}$ is a Groebner basis for $\langle x^2 + y^2 + 1, x^2y + 2xy + x, y^2 \rangle$, so $y^2 + I$ is invertible in $\mathbb{Z}_5[x, y]/I$,
To find the inverse of $y^2 + I$, we find the Groebner basis for I, then $\{x^2 + y^2 + 1, xy + 3x + 2y^3 + 2y, y^5 + 2y^4 + 4y^2 + 4y + 2\}$ is a Groebner basis for I, then $\{1, x, y, y^2, y^3, y^4\}$ are the basis of $\mathbb{Z}_5[x, y]$.
Then we need to find $a, b, c, d, e, f \in \mathbb{Z}_5$, such that

$$(ax + by^4 + cy^3 + dy^2 + ey + f)(y^2) \equiv 1 (mod I)$$

Now,

$(ax + by^4 + cy^3 + dy^2 + ey + f)(y^2)$

$$\begin{aligned} &= axy^2 + by^6 + cy^5 + dy^4 + ey^3 + fy^2 \\ &\equiv 4ax + 3ay^4 + ay^3 + 3ay^2 + ay + 4by^4 \\ &+ by^3 + 4by^2 + by + 4b + 3cy^4 + cy^2 + cy + 3c + dy^4 + ey^3 + fy^2 (mod I) \\ &= 4ax + (3a + 4b + 3c + d)y^4 + (a + b + e)y^3 + (3a + 4b + c + f)y^2 + (a + b + c)y \\ &+ (4b + 3c) \end{aligned}$$

So $(ax + by^4 + cy^3 + dy^2 + ey + f)(y^2) \equiv 1(mod I)$ *if and only if*

$$\begin{aligned} 4a &= 0 \\ 3a + 4b + 3c + d &= 0 \\ a + b + e &= 0 \\ 3a + 4b + c + f &= 0 \\ a + b + c &= 0 \\ 4b + 3c &= 1 \end{aligned}$$

When we solve the above equation we get that,
$a = 0, b = 1, c = 4, d = 4, e = 4$ *and* $f = 2$,
Then, $y^4 + 4y^3 + 4y^2 + 4y + 2 + I$ *is the inverse of* $y^2 + I$ *in* $\mathbb{Z}_5[x, y]/I$

3.2 Basic Algorithms In Ideal Theory

In this section we will discuss and develop a number of algorithms to carry out the algebraic operations that make use of Groebner basis.

3.2.1 Elimination Theorem

Definition 3.2.1. [6] *Given* $I = \langle f_1, \ldots, f_s \rangle \subset K[x_1, \ldots, x_n]$, *the* k^{th} *elimination ideal* I_k *is the ideal of* $K[x_{k+1}, \ldots, x_n]$ *defined by*

$$I_k = I \cap K[x_{k+1}, \ldots, x_n].$$

Theorem 3.2.2. ***(Elimination Theorem.)*** [6] *Let* $I \subset K[x_1, \ldots, x_n]$ *be an ideal and let* G *be a Groebner basis for* I *with respect to fixed term order where* $x_1 > x_2 > \cdots > x_n$. *Then for every* $0 \leq k \leq n$. *the set*

$$G_k = G \cap K[x_{x+1}, \ldots, x_n]$$

is a Groebner basis of the k^{th} *elimination ideal.*

Proof. Fix k between 0 and n. Since $G_k \subseteq I_k$ by construction,it suffices to show that $\langle lt(G_k)\rangle = \langle lt(I_k)\rangle$.
By definition of Groebner basis $\langle lt(G_k)\rangle \subseteq \langle lt(I_k)\rangle$. To prove the other inclusion
Let $f \in I_k$, then $f \in I$, and thus f is reducible modulo G, say $f \xrightarrow{g}_+ h$, with $g \in G$, since $lt(g)$ divides $lt(f)$, then leading term of g are in $x_{k+1} > \cdots > x_n$, then $g \in G_k$ then $\langle lt(I_k)\rangle \subseteq \langle lt(G_k)\rangle$.
Therefore G_k is a Groebner basis for I_k. □

The following are the basic applications of Elimination Theory.

3.2.2 Intersection of Ideals

Definition 3.2.3. [6] *The intersection $I \cap J$ of two ideals I and J in $K[x_1, \ldots, x_n]$ is the set of polynomials which belongs to both I and J.*

Theorem 3.2.4. *If I and J are ideals in $K[x_1, \ldots, x_n]$, then $I \cap J$ is also $K[x_1, \ldots, x_n]$.*

Proof. Note that $0 \in I \cap J$ since $0 \in I$ and $0 \in J$. If $f, g \in I \cap J$, then $f+g \in I$ because $f, g \in I$. Similarly $f + g \in J$ and, hence, $f + g \in I \cap J$. Finally, to check closure under multiplication, let $f \in I \cap J$ and h be any polynomial in $k[x_1, \ldots, x_n]$. Since $f \in I$ and I is an ideal, we have $hf \in I$. Similarly $hf \in J$ and, hence, $h \cdot f \in I \cap J$. □

Theorem 3.2.5. [3] *Let $I_1, \ldots, I_m$ be ideals of $K[x_1, \ldots, x_n]$ and let $J = \langle 1 - (y_1 + \cdots + y_m), y_1 I_1, \ldots, y_m I_m\rangle \subset K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, then*

$$\bigcap_{i=1}^{m} I_i = J \cap K[x_1, \ldots, x_n]$$

Proof. Let $f \in J \cap K[x_1, \ldots, x_n]$, then $f \in J$. we can represent f as

$$f = g(1 - \sum_{i=1}^{m} y_i) + \sum_{i=1}^{m} \sum_{j=1}^{k_i} g_{ij} y_i s_{ij}$$

Where $k_1, \ldots, k_m \in \mathbb{N}$, $g, g_{ij} \in K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and $s_{ij} \in I_i$ for $1 \leq i \leq m$ and $1 \leq j \leq k_i$.
Now let $1 \leq k \leq m$. Setting $y_k = 1$ and $y_i = 0$ for $i \neq k$ leaves the left-hand side unchanged and turns the right-side into an element of I_k.

Then, $f \in \bigcap_{i=1}^{m} I_i$
Conversely, let $f \in \bigcap_{i=1}^{m} I_i$. Then the equation,

$$f = f(1 - \sum_{i=1}^{m} y_i) + \sum_{i=1}^{m} y_i f$$

Then $f \in J \cap K[x_1, \ldots, x_n]$.

$$\bigcap_{i=1}^{m} I_i = J \cap K[x_1, \ldots, x_n]$$

□

Corollary 3.2.6. [1] *Let I and J be ideals in $K[x_1, \ldots, x_n]$, and t be a new variable. Consider the ideal $\langle tI, (1-t)J \rangle$ in $K[x_1, \ldots, x_n, t]$. Then*

$$I \cap J = \langle tI, (1-t)J \rangle \cap K[x_1, \ldots, x_n]$$

Proof. Let $f \in I \cap J$, Since

$$f = tf + (1-t)f$$

we have $f \in \langle tI, (1-t)J \rangle \cap K[x_1, \ldots, x_n]$
Conversely,suppose $f \in \langle tI, (1-t)J \rangle \cap K[x_1, \ldots, x_n]$, then
$f \in \langle tI, (1-t)J \rangle \subseteq K[x_1, \ldots, x_n, t]$

$$f = \sum_{i=1}^{m} t f_i h_i + \sum_{i=1}^{n} (1-t) p_i k_i$$

where f_i's and p_i's are the generators of I and J respectively and $h_i, k_i \in K[x_1, \ldots, x_n, t]$
Since the variable t does not appear in f, we can let $t = 1$, then $f \in I$ and if $t = 0$, then $f \in J$. □

The above results and the Elimination Theorem leads to the following **algorithm for computing intersection of ideals:**

Let $I_1, \ldots, I_m$ be ideals in $K[x_1, \ldots, x_n]$, We consider the ideal

$J = \langle 1 - (y_1 + \cdots + y_m), y_1 I_1, \ldots, y_m I_m \rangle \subseteq K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and compute the Groebner basis for J with respect to lex such that $y_1 > \cdots > y_m > x_1 > \cdots > x_n$. The elements of this basis which do not contain the variable y_i's will form a basis of $\bigcap_{i=1}^{m} I_i$.

Example 3.2.7. *Let* $I_1 = \langle x, y\rangle, I_2 = \langle x-1, y\rangle, I_3 = \langle x-2, y-2\rangle \subseteq \mathbb{Q}[x, y]$, *then to find* $I_1 \cap I_2 \cap I_3$, *we compute the Groebner basis for*

$$\langle 1-a-b-c, ax, ay, bx-b, by, cx-2c, cy-2c\rangle$$

with lex such that $a > b > c > x > y$.
then $\{a+b+c-1, b-x+y, 2c-y, x^2-xy-x+y, xy-y^2, y^2-2y\}$ *is the Groebner basis of* $\langle 1-a-b-c, ax, ay, bx-b, by, cx-2c, cy-2c\rangle$.
Then from the set of basis we take elements with out the variables a, b *and* c.
Therefore, $I_1 \cap I_2 \cap I_3 = \langle x^2-xy-x+y, xy-y^2, y^2-2y\rangle$.

Definition 3.2.8. *Fix a term order on* $K[x_1, \ldots, x_n]$, *for* $f, g \in K[x_1, \ldots, x_n]$*both non-zero,we define*
*(i)**The Greatest Common of Divisor** of* f *and* g *denoted by* $gcd(f, g)$ *to be the polynomial* d *such that*

1. $lc(d) = 1$
2. d *divides both* f *and* g
3. *If* h *is another polynomial that divide both* f *and* g, *then* h *divides* h.

*(ii)**The Least Common Multiple** of* f *and* g *denoted by* $lcm(f, g)$ *to be the polynomial* k *if*

1. f *divides* k *and* g *divides* k.
2. k *divides any polynomial which both* f *and* g *divide.*

Remark: It is true that $f \cdot g = lcm(f, g) \cdot gcd(f, g)$.

Lemma 3.2.9. [6] *For* $f, g \in K[x_1, \ldots, x_n]$, *both are non-zero, we have*

$$\langle f\rangle \cap \langle g\rangle = \langle lcm(f, g)\rangle.$$

Proof. Let $k = lcm(f, g)$, then by definition of k, $k \in \langle f\rangle \cap \langle g\rangle$.
Conversely,if $h \in \langle f\rangle \cap \langle g\rangle$, then $h = af$ and $h = bg$, for some
$a, b \in K[x_1, \ldots, x_n]$. Hence f divides h and g divides h, and thus k divides h by the definition of $lcm(f, g)$, so that $h \in \langle k\rangle$. then

$$\langle f\rangle \cap \langle g\rangle = \langle lcm(f, g)\rangle$$

□

Therefore to compute the *lcm* and then the *gcd* of two non-zero polynomials f and g in $K[x_1, \ldots, x_n]$, we first compute the reduced Groebner basis G for the ideal $\langle tf, (1-t)g\rangle$ with respect to an elimination order with $x_1, \ldots, x_n$ smaller than t. Then $lcm(f, g)$ is a polynomial in G in which t does not appear. To obtain $gcd(f, g)$, we use the Division Algorithm to compute

$$gcd(f, g) = \frac{f \cdot g}{lcm(f, g)}$$

Example 3.2.10. *Let* $f = x^4 + x^3y + x^2z^2 - x^2y^2 + x^2yz^2 - xy^3 - xy^2z^2 - y^3z^2$ *and* $g = x^4 + 2x^3z^2 - x^2y^2 + x^2z^4 - 2xy^2z^2 - y^2z^4$. *Then to find* $\langle f\rangle \cap \langle g\rangle$, *since* $f = (x-y)(x+y)^2(x+z^2)$ *and* $g = (x-y)(x+y)(x+z^2)^2$, *then*
$lcm(f, g) = (x-y)(x+y)^2(x+z^2)^2$.
Therefore $\langle f\rangle \cap \langle g\rangle = \langle (x-y)(x+y)^2(x+z^2)^2\rangle$.

3.2.3 Colon Ideals

Definition 3.2.11. [6] *If* I, J *are ideals in* $K[x_1, \ldots, x_n]$, *then* $I : J$ *is the set* $\{f \in K[x_1, \ldots, x_n] : fg \in I, for\ all\ g \in J\}$ *and is called the ideal quotient(colon ideal) of* I *by* J.

Theorem 3.2.12. [1] *If* I, J *are ideals in* $K[x_1, \ldots, x_n]$, *then* $I : J$ *is an ideal of* $K[x_1, \ldots, x_n]$ *and* $I : J$ *contains* I.

Proof. Since $0 \cdot g = 0 \in I$ for all $g \in J$, then $0 \in I : J$.
Let $f_1, f_2 \in I : J$. Then f_1g, f_2g are in I for all $g \in J$. Since I is an ideal $(f_1 + f_2)g = f_1g + f_2g \in I$ for all $g \in J$. Thus $f_1 + f_2 \in I$.
To check closure under multiplication, if $f \in I : J$ and $h \in K[x_1, \ldots, x_n]$, then $fg \in I$, since I is an ideal $hfg \in I$ for all $g \in J$, which means $hf \in I$. □

Lemma 3.2.13. [1] *Let* I *and* $J = \langle f_1, \ldots, f_s\rangle$ *be ideals in* $K[x_1, \ldots, x_n]$, *then*

$$I : J = \bigcap_{i=1}^{s} I : \langle f_i\rangle$$

Proof. If $g \in I : J$, then $gJ \subseteq I$, so in particular $gf_i \in I$ for all $i = 1, \ldots, s$, and hence $g \in \bigcap_{i=1}^{s} I : \langle f_i\rangle$. Conversely , if $g \in \bigcap_{i=1}^{s} I : \langle f_i\rangle$, then $g\langle f_i\rangle \subseteq I$ for all $i = 1, \ldots, s$, and hence $gJ \subseteq I$, so that $g \in I : J$. □

Theorem 3.2.14. [1] *Let I be an ideal and $f \neq 0$ be a polynomial in $K[x_1, \ldots, x_n]$, then*

$$I : \langle f \rangle = \frac{1}{f}(I \cap \langle f \rangle)$$

Proof. If $g \in \frac{1}{f}(I \cap \langle f \rangle)$, then $gf \in I$ and hence $g \in I : \langle f \rangle$.
Conversely,if $g \in I : \langle f \rangle$, then $gf \in I$, and hence $gf \in I \cap \langle f \rangle$, so that
$g \in \frac{1}{f}(I \cap \langle f \rangle)$. □

This theorem,together with our procedure for computing intersections of ideals immediately leads to an **algorithm for computing a basis of an ideal quotient.** Namely if $I = \langle f_1, \ldots, f_s \rangle$ and $J = \langle g_1, \ldots, g_t \rangle$, to compute basis of $I : J$, we first compute $I : \langle g_i \rangle$ for all i. We first compute a basis of $\langle f_1, \ldots, f_s \rangle \cap \langle g_i \rangle$, then using division algorithm,we divide each of these elements by g_i to get a basis for $I : \langle g_i \rangle$. Finally, we compute a basis for $I : J$ by applying the intersection algorithm $t - 1$ times, computing first basis for $I : \langle g_1, g_2 \rangle = (I : g_1) \cap (I : g_2)$, then the basis for $I : \langle g_1, g_2, g_3 \rangle = (I : \langle g_1, g_2 \rangle) \cap (I : \langle g_3 \rangle)$, and continue in such way.

Example 3.2.15. *Let $I = \langle x^2y + x - y, xy^2 - x \rangle$ and $J = \langle x^2 + y^2, x^3 + y \rangle$ in $\mathbb{Q}[x, y]$, then to compute $I : J$, first compute the basis for $I : \langle x^2 + y^2 \rangle$ and $I : \langle x^3 + y \rangle$*
To find the basis for $I : \langle x^2 + y^2 \rangle$ first compute the basis for $I \cap \langle x^2 + y^2 \rangle$,then
$I \cap \langle x^2 + y^2 \rangle = \langle (x^2 + y^2)(y^2 - 1), (x^2 + y^2)(x^2 - y^2 + 3xy - 2xy^3)$
Then $I : \langle x^2 + y^2 \rangle = \langle y^2 - 1, x^2 - y^2 + 3xy - 2xy^3 \rangle$
and $I \cap \langle x^3 + y \rangle = \langle (x^3 + y)(y^2 - 1), (x^3 + y)(x^2 - y^2 + xy^3)$.
Then $I : \langle x^3 + y \rangle = \langle y^2 - 1, x^2 - y^2 + xy^3 \rangle$.
So $I : \langle x^2 + y^2, x^3 + y \rangle = (I : \langle x^2 + y^2 \rangle) \cap (I : \langle x^3 + y \rangle)$. Then by applying Elimination Theorem and algorithm for intersection of ideals we get that
$I : J = \langle y^2 - 1, x^2 + xy - 1 \rangle$.

3.2.4 Saturation Ideals

Definition 3.2.16. [6] *Let $I \subset K[x_1, \ldots, x_n]$ be an ideal and fix $f \in K[x_1, \ldots, x_n]$, Then the saturation of I with respect to f is the set*

$$I : f^\infty = \{g \in K[x_1, \ldots, x_n] | f^m g \in I \text{ for some } m > 0\}.$$

Theorem 3.2.17. [6] *Let $I \subset K[x_1, \ldots, x_n]$ be an ideal and fix $f \in K[x_1, \ldots, x_n]$,*

1. *$I : f^\infty$ is an ideal of $K[x_1, \ldots, x_n]$.*
2. *We have an ascending chain of ideals*
   $I : f \subset I : f^2 \subset \cdots$
3. *By part 2 and the ascending chain condition we have*
   $I : f^N = I : f^{N+1} = \cdots$ for some integer N and $I : f^\infty = I : f^N$

Proof. (1) Since $f^m \cdot 0 = 0 \in I$ for some $m > 0$, then $0 \in I : f^\infty$.
Let $g_1, g_2 \in I : f^\infty$, then $f^m g_1, f^m g_2 \in I$, since I is an ideal, $f^m g_1 + f^m g_2 \in I$, then $f^m(g_1 + g_2) \in I$ which implies $g_1 + g_2 \in I : f^\infty$.
Let $h \in K[x_1, \ldots, x_n]$ and $g \in I : f^\infty$, then for some $m > 0$ $f^m g \in I$, since I is an ideal then $f^m gh \in I$ which implies $hg \in I : f^\infty$.
(2)Suppose $m > n$, for some positive integers m and n, then $\langle f^m \rangle \subseteq \langle f^n \rangle$.
Let $g \in I : f^n$, then $f^n g \in I$, then $f^m g \in I$, due to that $\langle f^m \rangle \subseteq \langle f^n \rangle$.
(3) It is true by Hilbert's Basis Theorem. □

Theorem 3.2.18. [3] *Let I be an ideal of $K[x_1, \ldots, x_n]$, $0 \neq f \in K[x_1, \ldots, x_n]$ and $J = \langle I, 1 - yf \rangle \subset K[x_1, \ldots, x_n, y]$, then*

$$I : f^\infty = J \cap K[x_1, \ldots, x_n]$$

and if $\{f_1, \ldots, f_s\}$ be the basis of I and $\{g_1, \ldots, g_t\}$ is the basis for $J \cap K[x_1, \ldots, x_n]$ with

$$g_i = h_i(1 - yf) + \sum_{j=1}^{s} h_{ij} f_j (1 \leq i \leq t)$$

Where $h_i, h_{ij} \in K[x_1, \ldots, x_n, y]$, then

$$k = max\{deg_y(h_{ij}), 1 \leq i \leq t, 1 \leq j \leq s\}$$

satisfies $I : f^k = I : f^\infty$.

Proof. Let $g \in J \cap K[x_1, \ldots, x_n]$, then

$$g = \sum_{i=1}^{s} q_i f_i + q(1 - yf)$$

where $q, q_i \in K[x_1, \ldots, x_n, y]$. Temporarily passing to the field of quotients $K(x_1, \ldots, x_n, y)$ of $K[x_1, \ldots, x_n, y]$, we may replace y by $\frac{1}{f}$ and then multiply the equation by f^d, where $d = max\{deg_y(q_i)\}$. Thus we obtain an equation $f^d g = \sum_{i=1}^{s} h_i f_i$ with $h_i \in K[x_1, \ldots, x_n]$, which implies $g \in I : f^\infty$.
Conversely, let $g \in I : f^\infty$, then for some $m > 0$, $f^m g \in I \subseteq J$.
Since $1 \equiv yf(modJ)$ we conclude $1 \equiv (yf)^m(modJ)$. We then have

$$g \equiv y^m f^m g \equiv 0(modJ).$$

Then $g \in J \cap K[x_1, \ldots, x_n]$.
It remain to show that $I : f^\infty = I : f^k$.
Let $g \in I : f^\infty$, Then

$$\begin{aligned} g &= \sum_{i=1}^{t} p_i g_i, \ (p_i \in K[x_1, \ldots, x_n]) \\ &= \sum_{i=1}^{t} p_i (h_i(1 - yf) + \sum_{j=1}^{s} h_{ij} f_j) \end{aligned}$$

If once again replace y by $\frac{1}{f}$ and multiply by f^k, then we see that $f^k g \in I$, then $g \in I : f^k$. The other direction is true by Theorem 3.2.17.

□

Remark:There is no clear computational method to find minimal k to make $I : f^k = I : f^\infty$, but the least k will be obtained by trial and error method.

The above algorithm is another version of "Radical Membership Problem" that we have seen in the next section.

3.3 Hilbert Nullstellensatz

Hilbert's Nullstellensatz may be seen as the starting point of algebraic geometry.It provides a bijective correspondence between affine varieties, which are geometric objects, and ideals in a polynomial ring, which are algebraic objects. In this section, we give the proofs and their implication of the three versions of the Nullstellensatz.

Definition 3.3.1. [6] *Let I be an ideal in $K[x_1, \ldots, x_n]$, we can define the set*

$$V(I) = \{x \in K^n | f(x) = 0 \ for \ all \ f \in I\}$$

and it is called an affine variety defined by I.

Thus an affine variety $V(I)$ is the set of all common roots for polynomials those belong to I.

Definition 3.3.2. [6] *Let $V \subseteq K^n$ be an affine variety, then we set*

$$I(V) = \{f \in K[x_1, \ldots, x_n] | f(x) = 0, \ for \ all \ x \in V\}$$

Lemma 3.3.3. [6] *Let $V \subseteq K^n$ is an affine variety ,then $I(V)$ is an ideal of $K[x_1, \ldots, x_n]$. We call $I(V)$ is the ideal of V.*

Proof. Since the Zero polynomial vanishes on all of K^n, then $0 \in I(V)$.
Let $f, g \in I(V)$ and $h \in K[x_1, \ldots, x_n]$ and $x \in V$ be arbitrary,then

$$f(x) + g(x) = 0 + 0 = 0$$
$$(f + g)(x) = 0$$
$$h(x)f(x) = h(x) \cdot 0 = 0$$
$$(hf)(x) = 0$$

So,$I(V)$ is an ideal. □

Lemma 3.3.4. [6] *Let $f_1 \ldots, f_s \in K[x_1, \ldots, x_n]$, then $\langle f_1, \ldots, f_s \rangle \subset I(V(f_1, \ldots, f_s))$*

Proof. Let $f \in \langle f_1, \ldots, f_s \rangle$, then $f = \sum_{i=1}^{s} h_i f_i$ for $h_i \in K[x_1, \ldots, x_n]$. Since $f_1, \ldots, f_s$ vanishes on $V(f_1, \ldots, f_s)$, so is $\sum_{i=1}^{s} h_i f_i$. Thus f vanishes on $V(f_1, \ldots, f_s)$, then $f \in I(V(f_1, \ldots, f_s))$. □

Definition 3.3.5. [6] *An ideal $I \subset K[x_1, \ldots, x_n]$ is said to be maximal if $I \neq K[x_1, \ldots, x_n]$ and any ideal J containing I is such either $J = I$ or $J = K[x_1, \ldots, x_n]$.*

Lemma 3.3.6. [6] *If K is any field and $I \subset K[x_1, \ldots, x_n]$ of the form*

$$I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

where $a_1, \ldots, a_n \in K$ is maximal.

Proof. Suppose J is some ideal containing I. Then there exist $f \in J$ such that $f \notin I$. then by division algorithm we can write f as

$$f = h_1(x_1 - a_1) + \cdots + h_n(x_n - a_n) + r$$

for $h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$ and $r \in K$
Since $h_1(x_1 - a_1) + \cdots + h_n(x_n - a_n) \in I$ and $f \notin I$, we must have $r \neq 0$. However $f \in J$ and $h_1(x_1 - a_1) + \cdots + h_n(x_n - a_n) \in I \subset J$, we also have

$$r = f - (h_1(x_1 - a_1) + \cdots + h_n(x_n - a_n)) \in J$$

Since r is non-zero, $1 = \frac{1}{b}b \in J$, So $J = K[x_1, \ldots, x_n]$. □

Lemma 3.3.7. *(Maximal ideals in polynomial ring)* [13] *Let K be an algebraically closed field and $\boldsymbol{m} \subset K[x_1, \ldots, x_n]$ be maximal ideal in a polynomial ring over K. Then there exist a point $P = (a_1, \ldots, a_n) \in K^n$ such that*

$$\boldsymbol{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$

Proof. Let $\varphi : K[x_i] \longrightarrow K[x_1, \ldots, x_n]$ defined as $\varphi(f) = f$ is a ring homomorphism. Since by Elimination theory $\boldsymbol{m} \cap K[x_i]$ is an ideal of $K[x_i]$.
Let $\phi : K[x_i] \longrightarrow K[x_1, \ldots, x_n]/\boldsymbol{m}$, defined as $\phi(f) = f + \boldsymbol{m}$. Then ϕ is ring homomorphism.
Claim:$\ker(\phi) = \boldsymbol{m} \cap K[x_i]$

$$Let\ h \in \ker(\phi), then\ \phi(h) = \boldsymbol{m} = h + \boldsymbol{m}$$

Then $h \in \boldsymbol{m}$, which implies $h \in \boldsymbol{m} \cap K[x_i]$
Conversely,let $h \in \boldsymbol{m} \cap K[x_i]$, then $h \in \boldsymbol{m}$, which implies $h + \boldsymbol{m} = \boldsymbol{m}$
Therefore,$\phi(h) = \boldsymbol{m}$, which shows $h \in \ker(\phi)$.
Then $\ker(\phi) = \boldsymbol{m} \cap K[x_i]$.
Then by First Isomorphism Theorem, $K[x_i]/\boldsymbol{m} \cap K[x_i] \cong K[x_1, \ldots, x_n]/\boldsymbol{m}$.
Since $\boldsymbol{m}$ is maximal then $K[x_1, \ldots, x_n]/\boldsymbol{m}$ is a field,then $K[x_i]/\boldsymbol{m} \cap K[x_i]$ is a field.
Then $\boldsymbol{m} \cap K[x_i]$ is maximal.
Since $K[x_i]$ is principal,then there exists $f \in K[x_i]$ such that $\boldsymbol{m} \cap K[x_i] = \langle f \rangle$, since $\boldsymbol{m} \cap K[x_i]$ is maximal,then f is irreducible. But K is algebraically closed the irreducible polynomial is linear.i.e $f = x_i - a_i$ for some $a_i \in K$.
Then $x_i - a_i \in \boldsymbol{m}$ for all $i = 1, \ldots, n$, then

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq \boldsymbol{m}$$

But by Lemma 3.3.7, $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal,then

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle = \boldsymbol{m}$$

□

Let K be field,then different ideals have the same variety,for example let us take ideals $I_1 = \langle x^2 + y^2 + 1 \rangle, I_2 = \langle 1 \rangle \in \mathbb{R}[x, y]$, then $V(I_1) = V(I_2) = \emptyset$.
Does is it true if K is algebraically closed? The following Theorem gives the answer for this question.

Theorem 3.3.8. ***(The Weak Hilbert Nullstellensatz)*** [13]
Let K be algebraically closed field and let $I \subset K[x_1, \ldots, x_n]$ be an ideal. Then $V(I) = \emptyset$ if and only if $I = K[x_1, \ldots, x_n]$.

Proof. Suppose $V(I) = \emptyset$, we want to show that $I = K[x_1, \ldots, x_n]$.
Suppose the contradiction,then I is maximal or I is contained in some maximal ideal $\boldsymbol{m}$, since K is algebraically closed there exist $a_1, \ldots, a_n \in K$ such that

$$\boldsymbol{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$

Then, $V(\boldsymbol{m}) = (a_1, \ldots, a_n)$.
If $I \subseteq \boldsymbol{m}$, then $V(\boldsymbol{m}) \subseteq V(I)$, then $(a_1, \ldots, a_n) \in V(I)$, which contradicts our assumption.
for the converse if $I = K[x_1, \ldots, x_n]$, then since $\langle 1 \rangle = K[x_1, \ldots, x_n]$,
then $V(1) = \emptyset = V(K[x_1, \ldots, x_n]) = V(I)$. □

The Weak Hilbert Nullstellensatz allows us to solve *consistency problem*(does the system of polynomial equation have a common solution or not) that is if we have system polynomials $f_1 = 0, \ldots, f_s = 0$. Then the polynomials fail to have a common solution if $V(f_1, \ldots, f_s) = \emptyset$.

To apply the **consistency algorithm**: let K is algebraically closed, if we have polynomials $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, we compute a reduced Groebner basis of the ideal they generate with respect to any ordering. If this basis is $\{1\}$, the polynomials

have no common zero in K^n; if the basis is not $\{1\}$, they must have a common zero. If we are working over a field K which is not algebraically closed, then the consistency algorithm still works in one direction: if $\{1\}$ is a reduced Groebner basis of $\{f_1, \ldots, f_s\}$ then the equations $f_1 = \cdots = f_s = 0$ have no common solution.The converse is not always true.

Theorem 3.3.9. *(**Hilbert's Nullstellensatz**)* [6] *Let K be an algebraically closed field. If $f, f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ are such that $f \in I(V(f_1, \ldots, f_s))$, then there exists an integer $m \geq 1$ such that*

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

and Conversely.

Proof. Consider the ideal

$$I' = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset K[x_1, \ldots, x_n, y]$$

where $f, f_1, \ldots, f_s$ are as the above.
We claim that $V(I') = \emptyset$
To see this,let $(a_1, \ldots, a_n, a_{n+1}) \in K^{n+1}$. Either
• $(a_1, \ldots, a_n)$ is common zero of $f_1, \ldots, f_s$, or
• $(a_1, \ldots, a_n)$. is not common zero of $f_1, \ldots, f_s$
If $(a_1, \ldots, a_n)$ is common zero of $f_1, \ldots, f_s$, then $f(a_1, \ldots, a_n) = 0$, since
$f \in I(V(f_1, \ldots, f_s))$.
Thus,the polynomial $1 - yf$ takes the value $1 - a_{n+1}f(a_1, \ldots, a_n) = 1 \neq 0$ at the point $(a_1, \ldots, a_n, a_{n+1})$.
In particular $(a_1, \ldots, a_n, a_{n+1}) \notin V(I')$.
For the second case, suppose there exists some $f_i, 1 \leq i \leq s$, such that
$f_i(a_1, \ldots, a_n) \neq 0$. Consider f_i as a polynomial in $n+1$ variables which does not depend on the last variable,we have $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$. In particular, we again conclude $(a_1, \ldots, a_n, a_{n+1}) \notin V(I')$.
Since $(a_1, \ldots, a_n, a_{n+1}) \in K^{n+1}$ was arbitrary,we conclude $V(I') = \emptyset$.
Thus by Weak Hilbert Nullstellensatz, $1 \in I'$, That is

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

where $q, p_i \in K[x_1, \ldots, x_n, y]$. Now set $y = 1/f(x_1, \ldots, x_n)$, Then

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i$$

Multiply both sides of this equation by a power f^m, where m is chosen sufficiently large to clear all the denominators. This yields

$$f^m = \sum_{i=1}^{s} h_i f_i$$

for some $h_i \in K[x_1, \ldots, x_n]$. Thus
$f^m \in \langle f_1, \ldots, f_s \rangle$.
Conversely, $f^m \in \langle f_1, \ldots, f_s \rangle$ and $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$, then
$f^m(a_1, \ldots, a_n) = 0$, since K is an integral domain $f(a_1, \ldots, a_n) = 0$, which implies $f \in I(V(f_1, \ldots, f_s))$. □

The Hilbert Nullstellensatz states that, over an algebraically closed field, this is the only reason that different ideals can give the same variety: if a polynomial f vanishes at all points of some variety $V(I)$, then some power of f must belong to I.

Definition 3.3.10. [6] *An ideal $I \subset K[x_1, \ldots, x_n]$. The radical of I denoted by $\sqrt{I}$ is the set*

$$\sqrt{I} = \{f \in K[x_1, \ldots, x_n] | \text{ there exists } m \in \mathbb{N} \text{ such that } f^m \in I\}$$

Lemma 3.3.11. [6] *If I is an ideal in $K[x_1, \ldots, x_n]$, then $\sqrt{I}$ is an ideal in $K[x_1, \ldots, x_n]$ containing I.*

Proof. Since $0^m \in I$, then $0 \in I$, therefore $0 \in \sqrt{I}$.
Let $f, g \in \sqrt{I}$, then there exist $m, n \in \mathbb{N}$, such that $f^m, g^n \in I$. But in the Binomial expansion $(f+g)^{m+n-1}$ every term has a factor $f^i g^j$ with $i + j = m + n - 1$. Since either $i \geq m$ or $j \geq n$, either $f^i \in I$ or $g^j \in I$, hence $f^i g^j$ and every term in the binomial expansion is in I. Hence ,$(f+g)^{m+n-1} \in I$,then $f + g\sqrt{I}$.
Let $h \in K[x_1, \ldots, x_n]$ and $f \in \sqrt{I}$, then $f^m \in I$ for some $m \in \mathbb{N}$. Since I is an ideal,$(hf)^m = h^m f^m \in I$. Then $hf \in \sqrt{I}$.
Let $f \in I$, then $f^1 \in I$ which implies $I \subseteq \sqrt{I}$. □

Theorem 3.3.12. *(**The Strong Nullstellensatz**)* [6] *Let K be algebraically closed field. If I is an ideal in $K[x_1, \ldots, x_n]$. Then*

$$I(V(I)) = \sqrt{I}$$

Proof. Suppose $f \in I(V(I))$. Then by definition, f vanishes on $V(I)$. By Hilbert's Nullstellensatz, there exists an integer $m \geq 1$ such that $f^m \in I$, then $f \in \sqrt{I}$. Since f is arbitrary, $I(V(I)) \subseteq \sqrt{I}$.
Conversely,let $f \in \sqrt{I}$ implies that $f^m \in I$ for some m, then f^m vanishes on $V(I)$, which implies that f vanishes on $V(I)$. Thus $f \in I(V(I))$. □

The above Theorem implies that $V(I_1) = V(I_2)$ if and only if $\sqrt{I_1} = \sqrt{I_2}$.

Theorem 3.3.13. *(**Radical Membership**)*[1] *Let K be arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subset K[x_1, \ldots, x_n]$ be an ideal then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $I' = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset K[x_1, \ldots, x_n, y]$.*

Proof. Suppose $f \in \sqrt{I}$, then $f^m \in I \subset I'$ for some $m \in \mathbb{N}$, and since $1 - yf \in I'$, we have

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + \cdots + y^{m-1} f^{m-1}) \in I'$$

Conversely,let $f \in I'$, then

$$f = \sum_{i=1}^{s} h_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

Where $q, h_i \in K[x_1, \ldots, x_n, y]$
Now set $y = 1/f(x_1, \ldots, x_n)$, then

$$f = \sum_{i=1}^{s} h_i(x_1, \ldots, x_n, 1/f) f_i$$

Multiply both sides by f^d where d is as large as possible to eliminate the denominators. This yields

$$f^{d+1} = \sum_{i=1}^{s} p_i f_i$$

where $p_i \in K[x_1, \ldots, x_n]$, then $f^{d+1} \in I$, which implies $f \in \sqrt{I}$. □

If $I = \langle f_1, \ldots, f_s \rangle$ and given $f \in K[x_1, \ldots, x_n]$, to determine $f \in \sqrt{I}$ we apply **radical membership algorithm**.that is find the reduced Groebner basis for the ideal $\langle f_1, \ldots, f_s, 1-yf \rangle \subset K[x_1, \ldots, x_n, y]$, if the basis is $\{1\}$, then $f \in \sqrt{I}$, otherwise, $f \notin \sqrt{I}$.

Example 3.3.14. *Let* $I = \langle x^4y^2 + z^2 - 4xy^3z - 2y^5z, x^2 + 2xy^2 + y^4 \rangle$ *and* $f = -x^3 + yz \in \mathbb{Q}[x, y, z]$, *the to determine* $f \in \sqrt{I}$, *we compute the reduced Groebner basis* G *for the ideal* $\langle x^4y^2 + z^2 - 4xy^3z - 2y^5z, x^2 + 2xy^2 + y^4, 1 + wx^3 - wxyz \rangle \subset \mathbb{Q}[x, y, z, w]$ *and* $G = \{1\}$, *So* $f \in \sqrt{I}$.

Theorem 3.3.15. [1] *Let* K *be algebraically closed field and* I *be an ideal in* $K[x_1, \ldots, x_n]$, *Fix a monomial order on* $K[x_1, \ldots, x_n]$, *then the following are equivalent*

1. *The variety* $V(I)$ *is finite*
2. *For each* $i = 1, \ldots, n$, *there exist* $j \in \{1, \ldots, t\}$ *such that* $lm(g_j) = x_i^v$ *for some* $v \in \mathbb{N}$, *where* $\{g_1, \ldots, g_t\}$ *is a Groebner basis for* I.
3. *The dimension of the* K*-vector space* $K[x_1, \ldots, x_n]/I$ *is finite.*

Proof. (1) $\Rightarrow$ (2) Assume that $V(I)$ is finite. If $V(I) = \emptyset$, by the Weak Nullstellensatz Theorem $I = K[x_1, \ldots, x_n]$, then $G = \{1\}$ and (2) satisfied immediately.
Suppose that $V(I) \neq \emptyset$. Fix $i \in \{1, \ldots, n\}$. Let $a_{ij}, j = 1, \ldots, l$ be the distinct i^{th} coordinates of the points in $V(I)$. For each $j, 1 \leq j \leq l$, let $0 \neq f_j \in K[x_i] \subset K[x_1, \ldots, x_n]$ be such that $f_j(a_{ij}) = 0$.
Let $f = f_1 f_2 \cdots f_l \in K[x_i] \subset K[x_1, \ldots, x_n]$. Then by construction we see that $f \in I(V(I))$, then by Theorem 3.3.9 there exists $m \in \mathbb{N}$ such that $f^m \in I$. Since $lm(f) = x_i^{mn}$ for some natural number n, and since the leading monomial of every element of I is divisible by the leading monomial of some element of G, there exists a polynomial in G whose leading monomial is a power of x_i alone.This is true for all $i = 1, \ldots, t$.
(2) $\Rightarrow$ (3) We saw in Section 3.1 that the K-basis of $K[x_1, \ldots, x_n]/I$ is the set of all Cosets of monomials which are reduced with respect to G. Since for every $i \in \{1, \ldots, n\}$ a power of of x_i is the leading monomial of of some g_j, there are finitely many monomials which are reduced with respect to G, hence $dim(K[x_1, \ldots, x_n]/I)$ is finite.

(3) $\Rightarrow$ (1) We want to show that for any $i = 1, \ldots, n$, there are only finitely many distinct values for the i^{th} coordinate of points in $V(I)$. Since by assumption,$K[x_1, \ldots, x_n]/I$ is finite dimensional K-vector space, the powers $1, x_i, x_i^2, \ldots$ of x_i are linearly dependent modulo I. Therefore there is an integer m and constants $c_j \in K, 0 \leq j \leq m$, not all zero,such that

$$\sum_{j=0}^{m} c_j x_i^j \in I$$

Since the above polynomial can only have finitely many roots in K, there are only finitely many values for the i^{th} coordinates of the points of $V(I)$. □

Definition 3.3.16. [1] *An ideal $I \neq K[x_1, \ldots, x_n]$ that satisfies one of the equivalent condition in Theorem* 3.3.15 *is called* ***Zero-dimensional ideal****.*

Theorem 3.3.17. [7] *Let K be algebraically closed field and let $I \subset K[x_1, \ldots, x_n]$ be zero-dimensional ideal. Then* $\dim(K[x_1, \ldots, x_n]/I)$ *is greater than or equal to the number of points in $V(I)$. Moreover, equality occurs if and only if I is a radical ideal.*

Proof. Let I be a zero-dimensional ideal.Then $V(I)$ is finite in K^n.
Say $V(I) = \{v_1, \ldots, v_m\}$. Consider the mapping

$$\begin{aligned} \varphi : K[x_1, \ldots, x_n]/I &\longrightarrow K^m \\ [f] &\longmapsto (f(v_1), \ldots, f(v_m)) \end{aligned}$$

Claim: φ is well-defined
Let $[f] = [g]$ which implies that $f - g \in I$, then $f(v) - g(v) = 0$, then $f(v) = g(v)$. Therefore φ is well-defined.
Next, we show that given distinct points $v_1, \ldots, v_m$, there exist a polynomial $f_1 \in K[x_1, \ldots, x_n]$ with $f_1(v_1) = 0$ and $f_1(v_2) = \cdots = f_1(v_m) = 0$. To prove this note that if $a \neq b \in K^n$, then they must differ at some coordinate, say the j^{th} and it follows that $g = \frac{(x_j - b_j)}{a_j - b_j}$ satisfies $g(a) = 1$ and $g(b) = 0$. If we apply this observation to each pair $v_1 \neq v_i, i \geq 2$, we get polynomials g_i such that $g_i(v_1) = 1$ and $g_i(v_i) = 0$ for $i \geq 2$. Then $f_1 = g_2 \cdots g_m$ has the desired property.
In the argument just given,there is nothing special about v_1. if we apply the same argument with v_1 replaced by each $p_2, \ldots, p_m$ in turn, we get polynomials $f_2, \ldots, f_m$ such that $f_i(v_j) = 1$ for $i = j$ and $f_i(v_j) = 0$ for $i \neq j$.
Now,let $f_1, \ldots, f_m$ be collections which satisfies the above condition and given arbitrary $(\lambda_1, \ldots, \lambda_m) \in K^m$, let $f = \sum_{i=1}^{m} \lambda_i f_i$, then $\varphi[f] = (\lambda_1, \ldots, \lambda_m)$. Thus φ is onto, and hence $\dim(K[x_1, \ldots, x_n]/I) \geq m$.

Now suppose that I is radical. If $[f] \in \ker(\varphi)$, the $f(v_i) = 0$ for all i, so that by the Strong Nullstellensatz, $f \in I(V(I)) = \sqrt{I} = I$. Thus $[f] = [0]$, which shows that φ is one-to-one as well onto.Then φ is isomorphism, which proves that $\dim(K[x_1, \ldots, x_n]/I) = m$ if I is radical.
Conversely,if $\dim(K[x_1, \ldots, x_n]/I) = m$, then φ is an isomorphism since it is an onto linear map between vector spaces of the same dimension. Hence φ is one-to-one.
Let $f \in \sqrt{I} = I(V(I))$, then $f(v_i) = 0$, for all i, which implies that $\varphi([f]) = (0, \ldots, 0)$. Since φ is one-to-one,we conclude that $[f] = [0]$, which implies that $f \in I$, then $\sqrt{I} \subseteq I$. The reverse direction is clear. □

The Weak Nullstellensatz Theorem and Theorem 3.3.15 are the main guide lines to solve a system of polynomials in polynomial ring over algebraically closed field. The Weak Nullstellensatz Theorem guarantees the existence of common solution for the system and Theorem 3.3.15 tells us the finiteness of common solution.

Example 3.3.18. *Let us take the system of equations*

$$\begin{aligned} x^3 + xy + y^2 - z^2 &= 0 \\ x^2 - xz + y + 2z &= 2 \\ x^4 + xyz + yz + z^2 &= 2 \\ x^2 - y - 2z &= -1 \end{aligned}$$

Then to solve this system of we must know the existence of common solution by finding the reduced Groebner basis for the ideal

$$I = \langle x^3 + xy + y^2 - z^2, x^2 - xz + y + 2z - 2, x^4 + xyz + yz + z^2 - 2, x^2 - y - 2z + 1 \rangle$$

then

$$G = \{x + \frac{1}{2}y^2 + \frac{1}{2}yz - 2y + \frac{1}{2}z^2 - \frac{9}{2}z + 3, y + \frac{2248}{32779}z^4 - \frac{4524}{32779}z^3 - \frac{28942}{32779}z^2 + \frac{123317}{32779}z - \frac{92299}{32779}, z - 1\}$$

is the reduced Groebner basis for I.
Since $G \neq \{1\}$, the systems have a common solution and the leading monomials of elements of G are x, y and z respectively, then the system has a finite solution.
Then by applying back substitution we get that, $z = 1, y = 0$ and $x = 1$. Then the system a solution set of $\{(1, 0, 1)\}$.

3.4 Polynomial Maps

In this section we are interested in K-algebra homomorphism between the polynomial rings $K[y_1, \ldots, y_m]$ and $K[x_1, \ldots, x_n]$. we recall that a K-algebra homomorphism is ring homomorphism.

$$\phi : K[y_1, \ldots, y_m] \longrightarrow K[x_1, \ldots, x_n]$$

which is also K-vector space linear transformation. such a map is uniquely determined by

$$\phi : y_i \longrightarrow f_i \tag{3.4.1}$$

where $f_i \in K[x_1, \ldots, x_n], 1 \leq i \leq m$, that is, if we let $h \in K[y_1, \ldots, y_m]$,
say $h = \sum_v c_v y_1^{v_1} \cdots y_m^{v_m}$, where $c_v \in K$ and $v = (v_1, \ldots, v_m) \in \mathbb{N}^m$ and only finitely many c_v's are non-zero,then we have

$$\phi(h) = \sum_v c_v f_1^{v_1} \cdots f_m^{v_m} = h(f_1, \ldots, f_m) \in K[x_1, \ldots, x_n] \tag{3.4.2}$$

Also conversely given such assignment (equation 3), we get a K-algebra homomorphism from formula (equation 4).
Recall that the *kernel* of ϕ is the ideal

$$\ker \phi = \{h \in K[y_1, \ldots, y_m] | \phi(h) = 0$$

and the *image* of ϕ is the K-algebra of $K[x_1, \ldots, x_n]$

$$im(\phi) = \{f \in K[x_1, \ldots, x_n] |\ there\ exist\ h \in K[y_1, \ldots, y_m]\ with\ f = \phi(h)\}.$$

This sub-algebra is denoted by $K[f_1, \ldots, f_m]$. We know that from the theory of abelian group that

$$K[y_1, \ldots, y_m]/\ker(\phi) \cong K[f_1, \ldots, f_m]$$

as abelian groups under the map

$$K[y_1, \ldots, y_m]/\ker(\phi) \longrightarrow K[f_1, \ldots, f_m]$$

defined by

$$g + \ker(\phi) \longrightarrow \phi(g)$$

This is called the First Isomorphism Theorem for k-algebras.

Lemma 3.4.1. [1] *Let $a_1, \ldots, a_n, b_1, \ldots, b_n$ be elements of the commutative ring R. Then the elements $a_1a_2 \cdots a_n - b_1b_2 \cdots b_n$ is in the ideal $\langle a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n\rangle$.*

Proof. The proof is done by induction, that is
For $n = 2$, $a_1a_2 - b_1b_2 = a_1(a_2 - b_2) + b_2(a_1 - b_1) \in \langle a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n\rangle$
By induction assumption the Lemma is true for $n - 1$, then
$a_1a_2 \cdots a_n - b_1b_2 \cdots b_n = a_1(a_2 \cdots a_n - b_2 \cdots b_n) + b_2 \cdots b_n(a_1 - b_1)$.
Then the Lemma required. □

Theorem 3.4.2. [1] *Let $\phi : K[y_1, \ldots, y_m] \longrightarrow K[x_1, \ldots, x_n]$ be K-algebra homomorphism and $J = \langle y_1 - f_1, \ldots, y_m - f_m\rangle \subseteq K[y_1, \ldots, y_m, x_1, \ldots, x_n]$, Then*

$$\ker(\phi) = J \cap K[y_1, \ldots, y_m].$$

Proof. Let $g \in \ker(\phi)$. We can write

$$g = \sum_v c_v y_1^{v_1} \cdots y_m^{v_m}$$

where $c_v \in K, v = (v_1, \ldots, v_m) \in \mathbb{N}^m$ and only finitely many c_v's are non-zero.
Therefore,since $\phi(g) = g(f_1, \ldots, f_m) = 0$, we have

$$g - g(f_1, \ldots, f_m) = \sum_v c_v(y_1^{v_1} \cdots y_m^{v_m} - f_1^{v_1} \cdots f_m^{v_m})$$

By Lemma 3.4.1, each term in the sum above is in the ideal J, and hence
$g \in K \cap K[y_1, \ldots, y_m]$.
Conversely,Let $g \in K \cap K[y_1, \ldots, y_m]$. Then

$$g(y_1, \ldots, y_m) = \sum_{i=1}^{m}(y_i - f_i(x_1, \ldots, x_n))h_i(y_1, \ldots, y_m, x_1, \ldots, x_n)$$

Where $h_i \in K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Since $g(f_1, \ldots, f_m) = 0$, then
$g \in \ker(\phi)$. □

We now have an algorithm for computing a Groebner basis for the kernel of ϕ. We first compute a Groebner basis G for the ideal $J = \langle y_1 - f_1, \ldots, y_m - f_m \rangle$ in $K[y_1, \ldots, y_m, x_1, \ldots, x_n]$ with respect to an elimination order in which the x variables are larger than the y variables. The polynomials in G without any x variables form a Groebner basis for the kernel of ϕ.

Example 3.4.3. *Let us define a map*

$$\phi : \mathbb{Q}[u, v, w] \longmapsto \mathbb{Q}[x, y]$$

defined by $\phi : u \longmapsto x^2 + y, \phi : v \longmapsto x + y$ *and* $\phi : w \longmapsto x - y^2$, *then to compute* $\ker(\phi)$, *first compute the Groebner basis for the ideal*

$$J = \langle u - x^2 - y, v - x - y, w - x + y^2 \rangle,$$

then
$G = \{u^2 - 2uv^2 - 4uv + 2uw + v^4 + 2v^2w + 3v^2 - 4vw + w^2, 2yv + u - v^2 - v + w, yu - yv^2 - yv + yw + 2v^2 - 2vw, y^2 + y - v + w, x + y - v\}$ *is a Groebner basis for* J *with term order lex such that* $x > y > u > v > w$.
Therefore the Groebner basis for $\ker(\phi)$ *is*

$$J \cap \mathbb{Q}[u, v, w] = \{u^2 - 2uv^2 - 4uv + 2uw + v^4 + 2v^2w + 3v^2 - 4vw + w^2\}$$

We now turn our attention to the question of finding an algorithm to determine whether an element $f \in K[x_1, \ldots, x_n]$ is in the image of the map ϕ and an algorithm to determine whether ϕ is onto.

Theorem 3.4.4. [1] *Let* $J = \langle y_1 - f_1, \ldots, y_m - f_m \rangle \subseteq K[y_1, \ldots, y_m, x_1, \ldots, x_n]$ *be the ideal considered in Theorem* 3.4.2, *and let* G *be reduced Groebner basis for* J *with respect to an elimination order with the* x *variables larger than the* y *variables. Then* $f \in K[x_1, \ldots, x_n]$ *is in the image of* ϕ *if and only if there exists* $h \in K[y_1, \ldots, y_m]$ *such that* $f \xrightarrow{G}_+ h$. *In case* $f = \phi(h) = h(f_1, \ldots, f_m)$.

Proof. Let $f \in K[x_1, \ldots, x_n]$ be in $im(\phi)$. Then $f = g(f_1, \ldots, f_m)$ for some $g \in K[y_1, \ldots, y_m]$. Consider the polynomial

$$f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) \subseteq K[y_1, \ldots, y_m, x_1, \ldots, x_n]$$

and $f(x_1,\ldots,x_n)-g(y_1,\ldots,y_m)=g(f_1,\ldots,f_m)-g(y_1,\ldots,y_m)$, and hence by Lemma 3.4.1 $f(x_1,\ldots,x_n)-g(y_1,\ldots,y_m)\in J$, then since $f\equiv g(modJ)$, then $f\xrightarrow{G}_+ h$ and $g\xrightarrow{G}_+ h$ where h is the normal form of g and f. But since $g\in K[y_1,\ldots,y_m]$, g can only be reduced by polynomials in G which have leading terms in the y variables alone.Since the x variables are larger than the y variables in our elimination order, the polynomials used to reduce g are in $K[y_1,\ldots,y_m]$. Therefore $h\in K[y_1,\ldots,y_m]$.
Conversely,let $f\xrightarrow{G}_+ h$, where $h\in K[y_1,\ldots,y_m]$. Then $f-h\in J$, so

$$\begin{aligned} f(x_1,\ldots,x_n) &- h(y_1,\ldots,y_m) \\ &= \sum_{i=m}^{m} g_i(y_1,\ldots,y_m,x_1,\ldots,x_n)(y_i-f_i(x_1,\ldots,x_n)) \end{aligned}$$

If we substitute f_i for y_i, we see that $f=h(f_1,\ldots,f_m)=\phi(h)$, and f is in the image of ϕ. □

Corollary 3.4.5. [1] *With the notation of Theorem* 3.4.4, $f\in K[x_1,\ldots,x_n]$ *is in the image of* ϕ *if and only if normal form of* f *with respect to* G *denoted as* $N_G(f)\in K[y_1,\ldots,y_m]$

Proof. If $f\in Im(\phi)$, then by Theorem 3.4.4 $f\xrightarrow{G}_+ h$, where $h\in K[y_1,\ldots,y_m]$, then $N_G(f)=N_G(h)$, Since $h\in K[y_1,\ldots,y_m]$ and the x variables are larger than y then h is reduced only by y variables. Then $N_G(h)\in K[y_1,\ldots,y_m]$.
Conversely,if $N_G(f)\in K[y_1,\ldots,y_m]$, then,since $f\xrightarrow{G}_+ N_G(f)$, then by Theorem 3.4.4, $f\in Im(\phi)$. □

The above Corollary helps us to show that $f\in K[x_1,\ldots,x_n]$ is in the image of ϕ, but the next Theorem gives us an algorithm to determine $f\in K[x_1,\ldots,x_n]$ and also ϕ is onto by simply inspecting the Groebner basis.

Theorem 3.4.6. [1] *Let* $J=\langle y_1-f_1,\ldots,y_m-f_m\rangle\subseteq K[y_1,\ldots,y_m,x_1,\ldots,x_n]$ *be the ideal considered in Theorem* 3.4.2, *and let* G *be reduced Groebner basis for* J *with respect to an elimination order with the* x *variables larger than the* y *variables. Then* ϕ *is onto if and only if for each* $i=1,\ldots,n$, *there exists* $g_i\in G$ *such that* $g_i=x_i-h_i$, *where* $h_i\in K[y_1,\ldots,y_m]$. *Moreover in this case* $x_i=h_i(f_1,\ldots,f_m)$.

Proof. Let ϕ is onto.Assume, with out loss of generality,let us assume the order in such way that $x_1<x_2<\cdots<x_n$.

Since $x_1 \in Im(\phi)$, the by Theorem 3.4.4, there exists $p_1 \in K[y_1, \ldots, y_m]$, such that $x_1 \xrightarrow{G}_+ p_1$. Therefore $x_1 - p_1 \in J$, hence there exists $g_1 \in G$ such that $lm(g_1)$ divides $lm(x_1 - p_1) = x_1$. Therefore, since the only terms strictly smaller than x_1 are terms in the y variables alone.Then $g_1 = x_1 - h_1$ for some $h_1 \in K[y_1, \ldots, y_m]$.
Similarly,since x_2 is in the image of ϕ, there exists $p_2 \in K[y_1, \ldots, y_m]$, such that $x_2 \xrightarrow{G}_+ p_2$, then $x_2 - p_2 \in J$, hence there exist $g_2 \in G$ such that $lm(g_2)$ divides $lm(x_2 - p_2) = x_2$. Since the only terms strictly smaller than x_2 are terms involving x_1 and the y variables only, and since G is the reduced Groebner basis and any term involving x_1 could be reduced using $g_1 = x_1 - h_1$, we must have $g_2 = x_2 - h_2$, for some $h_2 \in K[y_1, \ldots, y_m]$. We proceed in a similar fashion for the remaining x_i's.
Conversely, since $x_i - h_i \in G, 1 \leq i \leq n$, for some $h_i \in K[y_1, \ldots, y_m]$, we have $x_i \xrightarrow{G}_+ h_i$, then by Theorem 3.4.4, $x_i \in Im(\phi)$, then ϕ is onto. □

The above result gives an algorithm for determining whether the map ϕ is onto or not. We first compute the reduced Groebner basis G for the ideal J, and, by inspection, we check whether there exists $g_i = x_i - h_i \in G$ for each $i = 1, \ldots, n$ with $h_i \in K[y_1, \ldots, y_m]$.

Example 3.4.7. *Let a map* $\phi : \mathbb{Q}[t, u, v, w] \longrightarrow \mathbb{Q}[x, y]$ *defined as*
$\phi : t \longmapsto x^2 + y, \phi : u \longmapsto x + y, \phi : v \longmapsto x - y^2$ *and* $\phi : w \longmapsto x^2 + y^2$.*Then to show* ϕ *is onto, first compute the Groebner basis for*

$$J = \langle t - x^2 - y, u - x - y, v - x + y^2, w - x^2 - y^2 \rangle$$

then
$G = \{2y - t + u + v + w, x + y - u, tu - uv - uw + t - u + v, t^2 - 2tv - 2tw + u^2 + v^2 + 2vw + w^2 - 2w, u^3 - 2tv - tw + u^2 - 2uw + 2v^2 + 3vw + w^2 - t + u - v - 2w\}$ *is a Groebner basis for* J *with a term order deglex*
such that $x > y > t > u > v > w$.
Since we have $2y - t + u + v + w, x + y - u \in G$, *the map* ϕ *is onto.*

We now extends the preceding results to quotient ring of polynomials.It is one of the application of Invariant Theory.

Definition 3.4.8. [12] *An* K*-algebra is called an affine* K*-algebra if it is isomorphic to* $K[x_1, \ldots, x_n]/I$ *for some ideal* I *of* $K[x_1, \ldots, x_n]$.

Clearly,the polynomial ring $K[x_1, \ldots, x_n]$ is an affine K-algebra. Moreover,if $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ then,as we saw at the beginning of this section, the image ,$K[f_1, \ldots, f_m]$ of the map

$$\phi : K[y_1, \ldots, y_m] \longrightarrow K[x_1, \ldots, x_n]$$

which sends y_i to f_i is isomorphic to $K[f_1, \ldots, f_m]/\ker(\phi)$ and hence is an affine K-algebra.

We now want to study K-algebra homomorphism between affine K-algebra.

Let J be an ideal of $K[y_1, \ldots, y_m]$ and let I be an ideal of $K[x_1, \ldots, x_n]$. consider a K-algebra homomorphism

$$\phi : K[y_1, \ldots, y_m]/J \longrightarrow K[x_1, \ldots, x_n]/I.$$

Let as assume that

$$\phi : y_i + J \longrightarrow f_i + I$$

we note that the map ϕ is well-defined if and only if the following condition is satisfied.

If $J = \langle g_1, \ldots, g_t \rangle$ then for $i = 1, \ldots, t, g_i(f_1, \ldots, f_m) \in I$.

Then we are going to generalize Theorem 3.4.2

Theorem 3.4.9. [1] *Let H be an ideal of $K[y_1, \ldots, y_m, x_1, \ldots, x_n]$ whose generators are those of I together with the polynomials $y_i - f_i, 1 \leq i \leq m$, that is*
$H = \langle I, y_1 - f_1, \ldots, y_m - f_m \rangle$. Then $\ker(\phi) = H \cap K[y_1, \ldots, y_m](modJ)$. That is if $H \cap K[y_1, \ldots, y_m] = \langle f'_1, \ldots, f'_p \rangle$, then $\ker(\phi) = \langle f'_1 + J, \ldots, f'_p + J \rangle$

Proof. Let $h_1, \ldots, h_s$ be the the generators of I, and let $f' \in H \cap K[y_1, \ldots, y_m]$, then

$$f'(y_1, \ldots, y_m) = \sum_{i=1}^{m} (y_i - f_i(x_1, \ldots, x_n)) p_i(y_1, \ldots, y_m, x_1, \ldots, x_n) + w(y_1, \ldots, y_m, x_1, \ldots, x_n)$$

where

$$w(y_1, \ldots, y_m, x_1, \ldots, x_n) = \sum_{i=1}^{s} q_i(y_1, \ldots, y_m, x_1, \ldots, x_n) h_i(x_1, \ldots, x_n)$$

with $p_i, q_i \in K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Then

$$\phi(f') = f'(f_1, \ldots, f_m) + I = w(f_1, \ldots, f_m, x_1, \ldots, x_n) + I = 0$$

Since

$$w(f_1, \ldots, f_m, x_1, \ldots, x_n) = \sum_{i=1}^{s} q_i(f_1, \ldots, f_m, x_1, \ldots, x_n) h_i(x_1, \ldots, x_n) \in I$$

Conversely,let $f' \in K[y_1, \ldots, y_m]$ with $\phi(f' + J) = 0$. Then $f'(f_1, \ldots, f_m) \in I$.
Let $f'(y_1, \ldots, y_m) = \sum_v c_v y_1^{v_1} \cdots y_m^{v_m}$, where $v = (v_1, \ldots, v_m) \in \mathbb{N}^m, c_v \in K$ and only finitely many of c_v's are non-zero. Then

$$\begin{aligned} f'(y_1, \ldots, y_m) &= (f'(y_1, \ldots, _m) - f'(f_1, \ldots, f_m)) + f'(f_1, \ldots, f_m) \\ &= \sum_v c_v (y_1^{v_1} \cdots y_m^{v_m} - f_1^{v_1} \cdots f_m^{v_m}) + f'(f_1, \ldots, f_m) \end{aligned}$$

Then by Lemma 3.4.1

$$\sum_v c_v (y_1^{v_1} \cdots y_m^{v_m} - f_1^{v_1} \cdots f_m^{v_m})$$

is in the ideal $\langle y_1 - f_1, \ldots, y_m - f_m \rangle$ and hence

$$f'(y_1, \ldots, y_m) \in \langle I, y_1 - f_1, \ldots, y_m - f_m \rangle = H$$

Since $f'(f_1, \ldots, f_m) \in I$. Therefore $f'(y_1, \ldots, y_m) \in H \cap K[y_1, \ldots, y_m]$. □

We now prove the analog of Theorem 3.4.4

Theorem 3.4.10. [1] *Let $H = \langle I, y_1 - f_1, \ldots, y_m - f_m \rangle$ be the ideal as in Theorem 3.4.9 and let G be the Groebner basis for H with respect to an elimination order with the x variables larger than the y variables.Then $f + I \in K[x_1, \ldots, x_n]/I$ is in the image of ϕ if and only if there exists $h \in K[y_1, \ldots, y_m]$ such that $f \xrightarrow{G}_+ h$. In case $f + I = \phi(h + J) = h(f_1, \ldots, f_m) + I$.*

Proof. Let $f + I$ in the image of ϕ, then there exists $g \in K[y_1, \ldots, y_m]$ such that $f - g(f_1, \ldots, f_m) \in I$.
We consider the polynomial $f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) \in K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Since

$$f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) = g(f_1, \ldots, f_m) - g(y_1, \ldots, y_m) + (f(x_1, \ldots, x_n) - g(f_1, \ldots, f_m)).$$

Then by Lemma 3.4.1, $f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) \in H$.
Conversely,Let $f \in K[x_1, \ldots, x_n]$ be such that $f \xrightarrow{G}_+ h$, where $h \in K[y_1, \ldots, y_m]$. Then $f - h \in H$, and hence

$$f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) =$$
$$\sum_{i=1}^{m} g_i(y_1, \ldots, y_m, x_1, \ldots, x_n)(y_i - f_i(x_1, \ldots, x_n)) + w(y_1, \ldots, y_m, x_1, \ldots, x_n)$$

Where

$$w(y_1, \ldots, y_m, x_1, \ldots, x_n) = \sum_{i=1}^{s} q_i(y_1, \ldots, y_m, x_1, \ldots, x_n) h_i(x_1, \ldots, x_n)$$

With h_i is the generators of I and $g_i, q_i \in K[y_1, \ldots, y_m, x_1, \ldots, x_n]$.
If we substitute f_i for y_i, we see that $f - h(f_1, \ldots, f_m) \in I$, and hence $f + I = \phi(h + J)$. □

Corollary 3.4.11. [1] *Continuing the notation of Theorem* 3.4.10, *we have that* $f + I \in K[x_1, \ldots, x_n]/I$ *is in the image of* ϕ *if and only if* $N_G(f) \in K[y_1, \ldots, y_m]$.

Proof. Let $f + I \in K[x_1, \ldots, x_n]/I$ is in the image of ϕ,
then by Theorem 3.4.10 there exists $h \in K[y_1, \ldots, y_m]$ such that $f \xrightarrow{G}_+ h$.
Then since $N_G(f) = N_G(h)$. Since $h \in K[y_1, \ldots, y_m]$ and the x variables are larger than y variables, then h is reduced by y variables.
Then $N_G(h) \in K[y_1, \ldots, y_m]$.
Conversely,If $N_G(f) \in K[y_1, \ldots, y_m]$, then $f \xrightarrow{G}_+ h$.
Then by Theorem 3.4.10, $f + I \in Im(\phi)$. □

Theorem 3.4.12. [1] *Let* H *be an ideal in Theorem* 3.4.10, *and let* G *be the reduced Groebner basis for* H *with respect to an elimination order with the* x *variables larger than the* y *variables. Then* ϕ *is is onto if and only if for each* $i = 1, \ldots, t$ *there exists a polynomial* $g_i = x_i - h_i \in G$, *where* $h_i \in K[y_1, \ldots, y_m]$.

Proof. Let ϕ is onto.Assume, with out loss of generality,let us assume the order in such way that $x_1 < x_2 < \cdots < x_n$.
Since $x_1 + I \in Im(\phi)$, the by Theorem 3.4.4, there exists $p_1 \in K[y_1, \ldots, y_m]$, such that $x_1 \xrightarrow{G}_+ p_1$. Therefore $x_1 - p_1 \in J$, hence there exists $g_1 \in G$ such that $lm(g_1)$ divides $lm(x_1 - p_1) = x_1$. Therefore, since the only terms strictly smaller than x_1 are terms in the y variables alone.then $g_1 = x_1 - h_1$ for some $h_1 \in K[y_1, \ldots, y_m]$.

Similarly,since $x_2 + I$ is in the image of ϕ, there exists $p_2 \in K[y_1, \ldots, y_m]$, such that $x_2 \xrightarrow{G}_+ p_2$, then $x_2 - p_2 \in J$, hence there exist $g_2 \in G$ such that $lm(g_2)$ divides $lm(x_2 - p_2) = x_2$. Since the only terms strictly smaller than x_2 are terms involving x_1 and the y variables only, and since G is the reduced Groebner basis and any term involving x_1 could be reduced using $g_1 = x_1 - h_1$, we must have $g_2 = x_2 - h_2$, for some $h_2 \in K[y_1, \ldots, y_m]$. We proceed in a similar fashion for the remaining x_i's.
Conversely, since $x_i - h_i \in G, 1 \leq i \leq n$, for some $h_i \in K[y_1, \ldots, y_m]$, we have $x_i \xrightarrow{G}_+ h_i$, then by Theorem 3.4.4, $x_i + I \in Im(\phi)$, then ϕ is onto. □

Example 3.4.13. *Consider the following $\mathbb{Q}$-algebra homomorphism*

$$\begin{aligned} \phi : \mathbb{Q}[u, v, w]/J &\longrightarrow \mathbb{Q}[x, y] \\ u + J &\longrightarrow x^2 + y + I \\ v + J &\longrightarrow x + y + I \\ w + J &\longrightarrow x^3 + xy^2 + I \end{aligned}$$

Where $J = \langle uv - w \rangle$ and $I = \langle xy, y^2 \rangle$. Then to find $\ker(\phi)$ and to show ϕ is onto,first of we must show that ϕ is well-defined.
Since

$$\begin{aligned} \phi(uv - w) &= (x^2 + y)(x + y) - (x^3 + xy^2) + I \\ &= x^2y + xy + y^2 - xy^2 + I = 0 \end{aligned}$$

We now compute kernel of ϕ. Let

$$H = \langle xy, y^2, u - x^2 - y, v - x - y, w - x^3 - xy^2 \rangle \subseteq \mathbb{Q}[x, y, u, v, w]$$

We compute a reduced Groebner basis G for H with respect to the lex order with $x > y > u > v > w$. Then
$G = \{v^3 - w, uw - v^2w, uv - v^3, u^2 - uv^2, y - u + v^2, x + y - v\}$
Then

$$\begin{aligned} \ker(\phi) &= \{v^3 - w + J, uw - v^2w + J, uv - v^3 + J, u^2 - uv^2 + J\} \\ &= \{v^3 - w + J, uw - v^2w + J, u^2 - uv^2 + J\} \end{aligned}$$

The map ϕ is onto because $x + u - v^2 - v$ and $y - u + v^2$ are in G.

3.5 Some Application to Algebraic Geometry

Algebraic geometry is the study of geometric objects defined by polynomial equations,using algebraic means. It serves as a bridge between algebraic objects(Ideals)and geometric objects(Varieties).

Let I be an ideal in $K[x_1, \ldots, x_n]$ and K be algebraically closed field, we will consider the variety $V(I)$.

3.5.1 Zariski Closure

We begin by considering projection maps

$$\begin{aligned} \pi_m : K^{m+n} &\longrightarrow K^m \\ (a_1, \ldots, a_m, b_1, \ldots, b_n) &\longmapsto (a_1, \ldots, a_m) \end{aligned}$$

If we apply this map to a variety V, we may obtain a variety.For example the variety $V(xy-1)$ projects onto the x-axis minus the origin.we are interested in finding the smallest containing $\pi(V)$.

Theorem 3.5.1. [6] *If $S \subseteq K^n$, then $V(I(S))$ is the smallest variety containing S. That is, if W is any variety containing S, then $V(I(S)) \subseteq W$. This set is called the Zariski closure of S.*

Proof. Let W be a variety containing S, then $I(W) \subset I(S)$, which implies $V(I(S) \subset V(I(W))$. Since W is an affine variety, $W = V(I(W))$, then $V(I(S)) \subset W$. □

Theorem 3.5.2. [6] *Let K be algebraically closed field and let I be an ideal in $K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. The Zariski closure of $\pi_m(V(I))$ is $V(I \cap K[y_1, \ldots, y_m])$.*

Proof. Let $V = V(I)$ and $I_m = I \cap K[y_1, \ldots, y_m]$. Let first prove that $\pi_m(V) \subseteq V(I_m)$. Let $(a_1, \ldots, a_m, b_1, \ldots, b_n) \in V$, then $(a_1, \ldots, a_m) \in \pi_m(V)$.

If $f \in I_m$, since $f \in I$, $f(a_1, \ldots, a_m, b_1, \ldots, b_n) = 0$, since f is a polynomial with y variables, so we can write

$$f(a_1, \ldots, a_m) = f(\pi_m(a_1, \ldots, a_m)) = 0$$

This shows that f vanishes at all points of $\pi_m(V)$. Therefore $\pi_m(V) \subseteq V(I_m)$.
In view of Theorem 3.5.1,we need to show that $V(I_m) \subseteq V(I(\pi_m(V))$.
Let $f \in I(\pi_m(V))$, so that $f(a_1, \ldots, a_m) = 0$ for all $(a_1, \ldots, a_m) \in \pi_m(V)$. If we view f as an element of $K[y_1, \ldots, y_m, x_1, \ldots, x_n]$, then
$f(a_1, \ldots, a_m, b_1, \ldots, b_n) = 0$ for all $(a_1, \ldots, a_m, b_1, \ldots, b_n) \in V$.
By Theorem 3.3.9, there exists $k \in \mathbb{N}$ such that $f^k \in I$. But, since f involves only in y variables, $f^k \in I_m$, and hence $f \in \sqrt{I_m}$.
We have that $V(I_m) = V(\sqrt{I_m}) \subseteq V(I(\pi_m(V))$. This complete the proof. □

3.5.2 Implicitization

Let K be algebraically closed field, we consider the map

$$\varphi : K^n \longrightarrow K^m$$

given by $\varphi(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$, where f_i's are in $K[x_1, \ldots, x_n]$.

We can parametrized this by $f_1, \ldots, f_m$ as a subset of K^m as:

$$\begin{aligned} y_1 &= f_1(x_1, \ldots, x_n) \\ y_2 &= f_2(x_1, \ldots, x_n) \\ &\vdots \\ y_m &= f_m(x_1, \ldots, x_n) \end{aligned}$$

These equations define a variety in K^{n+m}, namely

$$V = V(y_1 - f_1, \ldots, y_m - f_m)$$

We want to convert the parametric equations into polynomial equations in the variable alone.This process is called *Implicitization*.Since parametric equations do not always

define a variety and so we will find the Zariski closure of $Im(\varphi)$.

Consider the projection:

$$\begin{aligned} \pi_m : K^{n+m} &\longrightarrow K^m \\ (y_1, \ldots, y_m, x_1, \ldots, x_n) &\longmapsto (y_1, \ldots, y_m) \end{aligned}$$

Then we can see that $\pi_m(V)$ is the image of φ and so we apply Theorem 3.5.2.

That is we let

$$I = \langle y_1 - f_1, \ldots, y_m - f_m \rangle \subseteq K[y_1, \ldots, y_m, x_1, \ldots, x_n].$$

Then the Zariski closure of $\pi_m(V)$ is $V(I \cap K[y_1, \ldots, y_m])$.

Therefore, to find a set of defining equations for that variety, one computes a Groebner basis G for I with respect to an elimination order with the x variables larger than the y variables. The polynomials in G which are in the y variables only are the desired polynomials.

Example 3.5.3. *Consider the map*

$$\begin{aligned} \varphi : \mathbb{C}^2 &\longrightarrow \mathbb{C}^4 \\ (x, y) &\longmapsto (x^4, x^3y, xy^3, y^4) \end{aligned}$$

so that the parametrization is given by:

$$\begin{aligned} r &= x^4 \\ u &= x^3y \\ v &= xy^3 \\ w &= y^4 \end{aligned}$$

The Groebner basis for the idealI $= \langle r - x^4, u - x^3y, v - xy^3, w - y^4 \rangle$ *with respect to the lex term ordering with* $x > y > u > v > w$ *is*

$G = \{uw^2 - v^3, rw - uv, -rv^2 + u^2w, -r^2v + u^3, -y^4 + w, -xw + yv, -xv^2 + yuw, -xu + yr, xrv - yu^2, -xy^3 + v, -x^2v + y^2u, -x^2y^2r + u^2, -x^3y + u, -x^4 + r\}$. *The polynomials that do not involve x or y are-those that determine the smallest variety containing the solutions of the parametric equations:*

$$uw^2 - v^3, rw - uv, -rv^2 + u^2w, -r^2v + u^3.$$

More generally,we consider the map between two affine varieties $V \subseteq K^n$ and $W \subseteq K^m$ given by polynomials; that is

$$\begin{aligned} \alpha : V &\longrightarrow W \\ (a_1, \ldots, a_n) &\longmapsto (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)) \end{aligned}$$

where f_i's in $K[x_1, \ldots, x_n]$.

Such a map α gives rise to a K-algebra homomorphism α^* between the affine K-algebras $K[y_1, \ldots, y_m]/I(W)$ and $K[x_1, \ldots, x_n]/I(V)$ as follows

$$\begin{aligned} \alpha^* : K[y_1, \ldots, y_m]/I(W) &\longrightarrow K[x_1, \ldots, x_n]/I(V) \\ y_i + I(W) &\longmapsto f_i + I(V) \end{aligned}$$

Claim: α^* is well-defined.

Let $g_1 + I(W) = g_2 + I(W)$, for $g_1, g_2 \in K[y_1, \ldots, y_m]$, then

$g = g_1 - g_2 \in I(W)$.

Let $(a_1, \ldots, a_n) \in V$, we have $\alpha(a_1, \ldots, a_n) \in W$, and hence

$$0 = g(\alpha(a_1, \ldots, a_n) = g(f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n))$$

Then, $g(f_1, \ldots, f_m) \in I(V)$, which implies that α^* is well-defined.

We call α^* is called **Pullback Mapping.**

Let V be the variety in K^n and a map into K^m given by the polynomials

$f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$

$$\begin{aligned} \alpha : V &\longrightarrow K^m \\ (a_1, \ldots, a_n) &\longmapsto (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)) \end{aligned}$$

We would like to determine $I(im(\alpha))$ by considering the map:

$$\begin{aligned} \alpha^* : K[y_1, \ldots, y_m] &\longrightarrow K[x_1, \ldots, x_n]/I(V) \\ y_i &\longmapsto f_i + I(V) \end{aligned}$$

Theorem 3.5.4. [1] *A polynomial $g \in K[y_1, \ldots, y_m]$ is in $I(im(\alpha))$ if and only if $g \in \ker(\alpha^*)$.*

Proof. Let $g \in I(im(\alpha))$. Then for any $(a_1, \ldots, a_n) \in V$, $g(\alpha(a_1, \ldots, a_n)) = 0$ and hence $g(\alpha(x_1, \ldots, x_n)) \in I(V)$, so that $\alpha^*(g) = 0$ and $g \in \ker(\alpha^*)$
Conversely,let $g \in \ker(\alpha^*)$, then $\alpha^*(g) = 0$, which implies that
$g(f_1, \ldots, f_m) + I(V) = I(V)$, hence $g(f_1, \ldots, f_m) \in I(V)$. Therefore for all
$(a_1, \ldots, a_n) \in V$, $g(f_1, \ldots, f_m)(a_1, \ldots, a_n) = 0 = g(\alpha(a_1, \ldots, a_n))$, then
$g \in I(im(\alpha)$. □

This Theorem together with Theorem 3.4.9 gives us an algorithm for computing the ideal $I(im(\alpha))$.

Example 3.5.5. *Let V be a variety in $\mathbb{C}^3$ defined by $x^2 + y^2 - z^2 = 0$ and $x^3 + y = 0$.*
Define $\alpha : V \longrightarrow \mathbb{C}^4$ by $(a, b, c) \longmapsto (a^2, a + b, c^2 + a, c)$.
The corresponding map α^* is

$$\begin{aligned} \alpha^* : \mathbb{C}[u, v, w, t] &\longrightarrow \mathbb{C}[x, y, z]/\langle x^2 + y^2 - z^2, xy^2 - xz^2 - y \rangle \\ u &\longmapsto x^2 \\ v &\longmapsto x + y \\ w &\longmapsto z^2 + x \\ t &\longmapsto z \end{aligned}$$

To find $I(im(\alpha))$, we consider the ideal
$H = \langle x^2 + y^2 - z^2, xy^2 - xz^2 - y, u - x^2, v - x - y, w - z^2 - x, t - z \rangle$ and find a Groebner

basis G for H with respect to the deglex term ordering with $x > y > z > u > v > w > t$ to get
$G = \{z-t, x+y-v, t^2-y+v-w, 2u^2+v^2-y+v-w, yu-uv-y, y^2-2yv+v^2-u, 2v^3-8yu+4yw+4uv+v^2-6vw-y+6u+v-w, uv^2+2u^2-uw+v^2-2u-v+w\}$.
Therefore

$$I(im(\alpha)) = \ker(\alpha^*) = H \cap \mathbb{C}[u,v,w,t] = \langle uv^2+2u^2-uw+v^2-2u-v+w\rangle.$$

Next we will see that when we say two varieties are isomorphic.

Definition 3.5.6. [8] *Two varieties $V \subseteq K^n$ and $W \subseteq K^m$ are said to be isomorphic over K if there are maps $\alpha : V \longrightarrow W$ and $\beta : W \longrightarrow V$ given by polynomials with coefficients in K such that $\alpha \circ \beta = id_W$ and $\beta \circ \alpha = id_V$, where id_V and id_W are the identity maps of V and W respectively.*

Theorem 3.5.7. [1] *The varieties $V \subseteq K^n$ and $W \subseteq K^m$ are said to be isomorphic over K if and only if there exists a K-algebra isomorphism of the affine K-algebras*

$$K[y_1,\ldots,y_m]/I(W) \text{ and } K[x_1,\ldots,x_n]/I(V)$$

Proof. First let α and β be inverse polynomial maps. Suppose that

$$\begin{aligned} \alpha : V &\longrightarrow W \\ (a_1,\ldots,a_n) &\longmapsto (f_1(a_1,\ldots,a_n),\ldots,f_m(a_1,\ldots,a_n)) \end{aligned}$$

where $f_1,\ldots,f_m \in K[x_1,\ldots,x_n]$, and suppose that

$$\begin{aligned} \beta : W &\longrightarrow V \\ (b_1,\ldots,b_m) &\longmapsto (g_1(b_1,\ldots,b_m),\ldots,g_n(b_1,\ldots,b_m)) \end{aligned}$$

where $g_1,\ldots,g_n \in K[y_1,\ldots,y_m]$.
$(\beta\circ\alpha)^*$ is defined by $x_i \longmapsto g_i(f_1,\ldots,f_m)$ while the map $\alpha^*\circ\beta^*$ is defined by

$$x_i \longmapsto g_i \longmapsto g_i(f_1,\ldots,f_m),$$

and so ,$(\beta\circ\alpha)^* = \alpha^*\circ\beta^*$. Now , since $\beta\circ\alpha = id_V$, $(\beta\circ\alpha)^* = id_{K[x_1,\ldots,x_n]/I(V)}$ and hence $\alpha^*\circ\beta^*$ is also the identity of $K[x_1,\ldots,x_n]/I(V)$ onto itself.Similarly, we have that $\beta^*\circ\alpha^*$ is the identity of $K[y_1,\ldots,y_m]/I(W)$ onto itself. α^* is K-algebra isomorphism.
For the converse,we assume that we have K-algebra isomorphism

$$\Theta : K[y_1,\ldots,y_m]/I(W) \longrightarrow K[x_1,\ldots,x_n]/I(V)$$

Let $\Theta(y_i + I(W)) = f_i + I(V)$, where $f_i \in K[x_1, \ldots, x_n]$ for $1, \ldots, m$, and let $\Theta^{-1}(x_j + I(V) = g_j + I(W)$, where $g_j \in K[y_1, \ldots, y_m]$ for $1, \ldots, n$.
Consider the maps

$$\begin{aligned} \alpha : V &\longrightarrow W \\ (a_1, \ldots, a_n) &\longmapsto (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)) \end{aligned}$$

and

$$\begin{aligned} \beta : W &\longrightarrow V \\ (b_1, \ldots, b_m) &\longmapsto (g_1(b_1, \ldots, b_m), \ldots, g_n(b_1, \ldots, b_m)) \end{aligned}$$

Since $\Theta = \alpha^*$ for a map $\alpha : V \longrightarrow W$ and $\Theta^{-1} = \beta^*$ for $\beta : W \longrightarrow V$.
Let $\alpha \circ \beta : W \longrightarrow W$, thus

$$(\alpha \circ \beta)^*(g_i + I(W)) = \beta^*(\alpha^*(g_i + I(V))) = \Theta^{-1}(\Theta(g_i + I(W))) = g_i + I(W)$$

So $(\alpha \circ \beta)^* = id_W^*$ and this implies that $\alpha \circ \beta = id_W$. In similar fashion $\beta \circ \alpha = id_V$.
Therefore α and β are inverse mapping. □

Then to to determine variety isomorphism, we need to check whether α^* is a K-algebra isomorphism. We have seen in Theorem 3.4.9 how to compute the kernel of α^* and in Theorem 3.4.10 how to determine whether α^* is onto.

Example 3.5.8. *Let in* $\mathbb{C}[x, y, z], J = \langle -2y - y^2 + 2z + z^2, 2x - yz - z^2 \rangle$ *and in* $\mathbb{C}[u, v]$, *let* $I = \langle uv + v \rangle$. *Define a map* $\alpha : V(I) \longrightarrow V(J)$ *defined by* $(u, v) \longmapsto (u^2 + v, u + v, u - v)$. *We want to show* α *defines isomorphism between* $V = V(I)$ *and* $W = V(J)$.
First we must show that α *maps* V *into* W.*So let* $(u, v) \in V$ *if we replace* $x, y,$ *and* z *by* $u^2 + v, u + v$ *and* $u - v$ *respectively in the equation defining* W *we get*

$$-2(u + v) - (u + v)^2 + 2(u - v) + (u - v)^2 = -4(uv + v) = 0$$

$$2(u^2 + v) - (u + v)(u - v) - (u - v)^2 = 2(uv + v) = 0$$

Since $(u, v) \in V$
Now consider the corresponding mapping

$$\begin{aligned} \alpha^* : \mathbb{C}[x, y, z]/J &\longrightarrow \mathbb{C}[u, v]/I \\ f + J &\longmapsto f(u^2 + v, u + v, u - v) \end{aligned}$$

where $J = \langle -2y - y^2 + 2z + z^2, 2x - yz - z^2 \rangle$ *and* $I = \langle uv + v \rangle$, *where* $I(W) = J$ *and* $I(V) = I$*(due to that both* I *and* J *are radical ideals).*
Let $H = \langle uv + v, x - u^2 - v, y - u - v, z - u + v \rangle$ *be an ideal in* $\mathbb{C}[x, y, z, u, v]$ *as in Theorem* 3.4.9. *We compute the Groebner basis for* H *with respect to the lex term ordering with* $u > v > x > y > z$ *to get*

$$G = \{u - v - z, 2v - y + z, 2x - yz - z^2, y^2 + 2y - 2z - z^2\}$$

Thus,$H \cap \mathbb{C}[x, y.z] = \langle 2x - yz - z^2, y^2 + 2y - 2z - z^2 \rangle = J$, *and hence* $\ker(\alpha^*) = 0$ *by Theorem* 3.4.9 *and so* α^* *is one to one. Also,since* $u + \frac{1}{2}y - \frac{3}{2}z$ *and* $v - \frac{1}{2}y + \frac{1}{2}z$ *are in* G, *the map* α^* *is onto by Theorem* 3.4.10. *Therefore* $\alpha*$ *is* $\mathbb{C}$*-Isomorphism and, by Theorem* 3.5.7, α *gives an isomorphism of the varieties* V *and* W.

3.6 Minimal Polynomials Of Elements In Field Extensions

In this section we will use the results of Section 2.4 to find the minimal polynomial of an element algebraic over a field K.

Let $k \subseteq K$ be a field extension.Recall that if $\alpha \in K$ is algebraic over k, then the minimal polynomial of α over k is defined ta be the monic polynomial p in one variable, with coefficients in k, of smallest degree such $p(\alpha) = 0$. Alternatively,considering the k-algebra homomorphism $\phi : k[x] \longrightarrow k(\alpha)$ defined by $x \longmapsto \alpha$, we have that $\ker(\phi) = \langle p \rangle$. Moreover the map ϕ is onto, since α is algebraic,and so

$$k[x]/\langle p \rangle \cong k(\alpha). \tag{3.6.1}$$

under the map defined by $x + \langle p \rangle \longmapsto \alpha$

We first consider the case where $K = k(\alpha)$, with α algebraic over k, and our goal is to compute the minimal polynomial of any $\beta \in K$. We note that in order to compute in $k(\alpha)$ it suffices, by Equation (5), to compute in the affine k-algebra $k[x]/\langle p \rangle$. We assume that we know the minimal polynomial p of α.

Theorem 3.6.1. [1] *Let $k \subseteq K$ be a field extension, and let $\alpha \in K$ be algebraic over k.Let $p \in k[x]$ be minimal polynomial of α over k. Let $0 \neq \beta \in k(\alpha)$*

$$\beta = \frac{a_o + a_1\alpha + \cdots + a_n\alpha^n}{b_o + b_1\alpha + \cdots + b_m\alpha^m}$$

where $a_i, b_j \in k, 0 \leq i \leq n, 0 \leq j \leq m$. let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$ be the corresponding polynomials in $k[x]$. Consider the ideal $J = \langle p, gy - f\rangle$ of $k[x, y]$. The minimal polynomial of β over k is a monic polynomial that generate the ideal $J \cap k[y]$.

Proof. Since $k[x]/\langle p\rangle$ is a field and $g(\alpha) \neq 0$ (it is the denominator of β), there is a polynomial $l \in k[x]$ such that $gl \equiv (mod\langle p\rangle)$, that is $gl - 1 \in \langle p\rangle$.
Let $h = fl$. Note that $h(\alpha) = \beta$. Now consider ϕ, the composition of the affine algebra homomorphisms

$$\phi : k[y] \longrightarrow k[x]/\langle p\rangle \xrightarrow{\cong} k(\alpha)$$
$$y \longmapsto h + \langle p\rangle \longmapsto \beta$$

Note that q is in the kernel of ϕ if and only if $q(\beta) = 0$. Therefore to find the minimal polynomial of β, we find the generator of the kernel of ϕ. By Theorem 3.4.9, the kernel of the map ϕ is $\langle p, y-h\rangle \cap k[y]$. Therefore it suffices to show that $\langle p, y-h\rangle = \langle p, gy-1\rangle$. First note that $y - h = y - fl \equiv f(gy - 1)(mod\langle p\rangle)$, and hence $y - h \in \langle p, gy - f\rangle$ so that $\langle p, y - h\rangle \subseteq \langle p, gy - f\rangle$.
Conversely, $gy - f \equiv g(y - fl) = g(y - h)(mod\langle p\rangle)$.
Therefore $gy - f \in \langle p, y - h\rangle$, and $\langle p, gy - f\rangle \subseteq \langle p, y - h\rangle$. □

The above result gives an algorithm for finding the minimal polynomial of an element $\beta \in k(\alpha)$: given α and β as in the theorem, we compute the reduced Groebner basis G for the ideal $\langle p, gy - f\rangle$ of $k[x, y]$ with respect to the lex term ordering with $x > y$. The polynomial in G which is in y alone is the minimal polynomial of β.

Example 3.6.2. *Consider the extension field $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$, where $\alpha^3 - \alpha - 1 = 0$. Now consider $\beta = \frac{\alpha^2+\alpha}{\alpha+3} \in \mathbb{Q}(\alpha)$. We want to find the minimal polynomial of β. Consider the ideal $J = \langle x^3-x-1, xy+3y-x^2-x\rangle \in \mathbb{Q}[x, y]$. We compute the reduced Groebner basis G for J with respect to the lex term ordering with $x > y$ to obtain*

$$G = \{25y^3 - 6y^2 - 7y - 1, 5x - 150y^2 + 61y + 26\}$$

Therefore the minimal polynomial of β is $25y^3 - 6y^2 - 7y - 1$.

This technique can be extended to a more general setting of field extensions of the form $K = k(\alpha_1, \ldots, \alpha_n)$. For this we need the following notation which we use for the remainder of this section.For $i = 1, \ldots, n$ and $p \in k(\alpha_i, \ldots, \alpha_{i-1})$, we let $\overline{p}$ be any polynomial in $k[x_1, \ldots, x_n]$ such that $\overline{p}(\alpha_i, \ldots, \alpha_{i-1}) = p$. We now determine the minimal polynomial of any element β of $k(\alpha_1, \ldots, \alpha_n)$ using the following result, which is similar to Theorem 3.6.1 using the following result.

Theorem 3.6.3. [1] *Let $K = k(\alpha_1, \ldots, \alpha_n)$ be an algebraic extension of k, for $i = 1, \ldots, n$. let $p_i \in k(\alpha_1, \ldots, \alpha_{i-1})[x_i]$ be the polynomial of α_i over $k(\alpha_1, \ldots, \alpha_{i-1})$. let $\beta \in k(\alpha_1, \ldots, \alpha_n)$ say*

$$\beta = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}.$$

where $f, g \in k[x_1, \ldots, x_n]$. consider $J = \langle \overline{p}_1, \ldots, \overline{p}_n, gy - f \rangle$ contained $k[x_1, \ldots, x_n, y]$. Then the minimal polynomial of β over k is the monic polynomial that generates the ideal $J \cap k[y]$.

Proof. We first show that

$$k[x_1, \ldots, x_n]/\langle \overline{p}_1, \ldots, \overline{p}_n \rangle \cong k(\alpha_1, \ldots, \alpha_n)$$

Using the map

$$\begin{aligned} \phi_n : k[x_1, \ldots, x_n] &\longrightarrow k(\alpha_1, \ldots, \alpha_n) \\ x_i &\longmapsto \alpha_i \end{aligned}$$

Since $\alpha_1, \ldots, \alpha_n$ is algebraic over k, ϕ_n is onto. it remain to show that $\ker(\phi_n) = \langle \overline{p}_1, \ldots, \overline{p}_n \rangle$. For this we use induction on n. The case $n = 1$ is equation (5).The fact that $\overline{p}_1, \ldots, \overline{p}_n \in \ker(\phi_n)$ is immediate. Now let $f \in k[x_1, \ldots, x_n]$ be such that $f(\alpha_1, \ldots, \alpha_n) = 0$. Let

$$h(x_n) = f(\alpha_1, \ldots, x_n) \in k(\alpha_1, \ldots, \alpha_{n-1})[x_n],$$

and note that $h(\alpha_n) = 0$. Therefore p_n divides h, by definition of h_n. Say $h = p_n l_n$, for some $l_n \in k(\alpha_1, \ldots, \alpha_{n-1})[x_n]$. Consider $f - \overline{p}_n \overline{l}_n \in k[x_1, \ldots, x_n]$ and write

$$f - \overline{p}_n \overline{l}_n = \sum_i g_i(x_1, \ldots, x_{n-1}) x_n^i$$

Then, since

$$f - \overline{p}_n \bar{l}_n(\alpha_1, \ldots, \alpha_{n-1}, x_n) = h - p_n l_n = 0,$$

we see that for all i, $g_i(\alpha_1, \ldots, \alpha_{n-1}) = 0$. Therefore $g_i(x_1, \ldots, x_{n-1})$ is in the kernel of

$$\phi_{n-1} : k[x_1, \ldots, x_{n-1}] \longrightarrow k(\alpha_1, \ldots, \alpha_{n-1})$$

and hence

$$g_i(x_1, \ldots, x_{n-1}) \in \langle \overline{p}_1, \ldots, \overline{p}_{n-1} \rangle$$

by induction. Thus $f - \overline{p}_n \bar{l}_n \in \langle \overline{p}_1, \ldots, \overline{p}_{n-1} \rangle$ and $f \in \langle \overline{p}_1, \ldots, \overline{p}_n \rangle$. Thus $\ker(\phi_n) = \langle \overline{p}_1, \ldots, \overline{p}_n \rangle$ as desired. □

The proof now proceeds as in Theorem 3.6.1.

Example 3.6.4. *Consider the field extension* $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. *The minimal polynomial of* $\sqrt{2}$ *over* $\mathbb{Q}$ *is* $x_1^2 - 2 \in \mathbb{Q}[x_1]$ *and the minimal polynomial of* $\sqrt{3}$ *over* $\mathbb{Q}(\sqrt{2})$ *is* $p_2 = x_2^2 - 3 \in \mathbb{Q}(\sqrt{2})[x_2]$ *and the minimal polynomial of* $\sqrt{5}$ *over* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *is* $p_3 = x_3^2 - 5 \in \mathbb{Q}(\sqrt{2}, \sqrt{3})[x_3]$. *We compute the reduced Groebner basis* G *for the ideal*

$$J = \langle \overline{p}_1, \overline{p}_2, \overline{p}_3, y - (x_1 + x_2 + x_3) \rangle = \langle x_1^2 - 2, x_2^2 - 3, x_3^2 - 5, y - (x_1 + x_2 + x_3) \rangle$$

with respect to the lex term ordering with $x_1 > x_2 > x_3 > y$ *to obtain*
$G = \{y^8 - 40y^6 + 352y^4 - 96y^2 + 576, 576x_3 - 5y^7 + 194y^5 - 1520y^3 + 2544y, 2x_2 + 3x_3^2 y - 3x_3 y^2 + 6x_3 + y^3 - 6y, x_1 + x_2 + x_3 - y\}$
Therefore the minimal polynomial of $\sqrt{2} + \sqrt{3} + \sqrt{5}$ *is* $y^8 - 40y^6 + 352y^4 - 96y^2 + 576$.

Theorem 3.6.5. [1] *Let* $\alpha_1, \ldots, \alpha_n$ *and* $\overline{p}_1, \ldots, \overline{p}_n$ *be as in Theorem* 3.6.3. *Let* $\beta \in k(\alpha_1, \ldots, \alpha_n)$, *say* $\beta = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$, *with* $f, g \in k[x_1, \ldots, x_n]$. *Let* J *be as in Theorem* 3.6.3, *and let* G *be the reduced Groebner basis for* J *with respect to an elimination order with the* x *variables larger than* y. *Then* $k(\alpha_1, \ldots, \alpha_n) = k(\beta)$ *if and only if, for each* $i = 1, \ldots, n$, *there is a polynomial* $g_i \in G$ *such that* $g_i = x_i - h_i$ *for some* $h_i \in k[y]$. *Moreover,in the case,* $\alpha_i = h_i(\beta)$.

Proof. Let $I = \langle \overline{p}_1, \ldots, \overline{p}_n \rangle$, and let $l \in k[x_1, \ldots, x_n]$ be such that $gl - 1 \in I$. Set $h = fl$, and note that $h(\alpha_1, \ldots, \alpha_n) = \beta$. consider

$$k[y] \xrightarrow{\phi} k[x_1, \ldots, x_n]/I \xrightarrow{\approx} k(\alpha_1, \ldots, \alpha_n)$$

$$y \longmapsto h + I \longmapsto \beta$$

Then $k(\alpha_1, \ldots, \alpha_n) = k(\beta)$ if and only if ϕ is onto. We conclude by using Theorem 3.4.12 and the fact that $J = \langle I, y - h \rangle$. □

Example 3.6.6. *Consider the field extension* $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. *The minimal polynomial of* $\sqrt{2}$ *over* $\mathbb{Q}$ *is* $x_1^2 - 2 \in \mathbb{Q}[x_1]$ *and the minimal polynomial of* $\sqrt{3}$ *over* $\mathbb{Q}(\sqrt{2})$ *is* $x_2^2 - 3 \in \mathbb{Q}(\sqrt{2})[x_2]$. *We want to find the minimal polynomial of* $\sqrt{2} + \sqrt{3}$. *We compute the Groebner basis* G *for the ideal*

$$J = \langle x_1^2 - 2, x_2^2 - 3, y - (x_1 + x_2) \rangle \subseteq \mathbb{Q}[x_1, x_2, y]$$

with respect to the lex term ordering with $x_1 > x_2 > y$ *to obtain*
$G = \{y^4 - 10y^2 + 1, x_2 + \frac{1}{2}y^3 - \frac{11}{2}y, x_1 - \frac{1}{2}y^3 + \frac{9}{2}y\}$.
Therefore,both

$$x_1 - \frac{1}{2}y^3 + \frac{9}{2}y$$

and

$$x_2 + \frac{1}{2}y^3 - \frac{11}{2}y$$

are in G.
This gives another proof that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. *Moreover,we have*

$$\sqrt{2} = \frac{1}{2}(\sqrt{2} + \sqrt{3})^3 - \frac{9}{2}(\sqrt{2} + \sqrt{3})$$

and

$$\sqrt{3} = -\frac{1}{2}(\sqrt{2} + \sqrt{3})^3 + \frac{11}{2}(\sqrt{2} + \sqrt{3}).$$

3.7 Radicals of Zero-Dimensional Ideals

Definition 3.7.1. [3] *Let* $f \in K[x_1, \ldots, x_n]$ *and* f *can be written in the form*

$$f = f_1^{\alpha_1} \cdots f_n^{\alpha_n},$$

where f_i*'s are irreducible for* $1 \leq i \leq n$, *then the square free part of* f *is* $f_1 \cdots f_n$, *denoted as* f^*
and f *is squarefree if* $\langle f^* \rangle = \sqrt{\langle f \rangle}$.

Theorem 3.7.2. [6] *Let* $f \in K[x_1, \ldots, x_n]$ *and* $I = \langle f \rangle$. *If* $f = f_1^{\alpha_1} \cdots f_n^{\alpha_n}$, *is the factorization of* f *into a product of distinct irreducible polynomials, then*

$$\sqrt{I} = \sqrt{\langle f \rangle} = f_1 \cdots f_n$$

Proof. We first show that $f_1 \cdots f_n \in \sqrt{I}$. Let N be an integer which is strictly larger than maximum of $\alpha_1, \ldots, \alpha_n$. Then

$$(f_1 \cdots f_n)^N = f_1^{N-\alpha_1} \cdots f_n^{N-\alpha_n} f$$

is a polynomial multiple of f. This shows that $(f_1 \cdots f_n)^N \in I$, which implies that $f_1 \cdots f_n \in \sqrt{I}$, then $\langle f_1 \cdots f_n \rangle \subseteq \sqrt{I}$.
Conversely, suppose that $g \in \sqrt{I}$. Then there exists a positive integer M such that $g^M \in I$. This means $g^M = hf$ for some polynomial h. Now suppose that $g = g_1^{b_1} \cdots g_t^{b_t}$ is the factorization of g into a product of distinct irreducible polynomials. Then, $g^M = g_1^{b_1 M} \cdots g_t^{b_t M}$ is the factorization of g^M into a product of distinct irreducible polynomials. Thus,

$$g_1^{b_1 M} \cdots g_t^{b_t M} = h f_1^{\alpha_1} \cdots f_n^{\alpha_n}$$

But, by unique factorization, the irreducible polynomials on both sides of the above equation must be the same. Since $f_1, \ldots, f_n$ are irreducible,each $f_i, 1 \leq i \leq n$ is the constant multiple of g_j. This implies that g is a polynomial multiple of $f_1 \cdots f_n$ and,therefore g is contained in the ideal $\langle f_1 \cdots f_n \rangle$. □

Lemma 3.7.3. [6] *Suppose that K is a field and let $I = \langle f \rangle$ be a principal ideal in $K[x_1, \ldots, x_n]$. Then $\sqrt{I} = \langle f^* \rangle$, where*

$$f^* = \frac{f}{Gcd(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n})}$$

Proof. Let $f = f_1^{\alpha_1} \cdots f_n^{\alpha_n}$, by the above Theorem $\sqrt{I} = f_1 \cdots f_n$. Thus it suffices to show that

$$Gcd(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}) = f_1^{\alpha_1 - 1} \cdots f_n^{\alpha_n - 1}$$

We first use the product rule to note that

$$\frac{\partial f}{\partial x_j} = f_1^{\alpha_1 - 1} \cdots f_n^{\alpha_n - 1} (\alpha_1 \frac{\partial f_1}{\partial x_j} f_2 \cdots f_n + \cdots + \alpha_n f_1 \cdots f_{n-1} \frac{\partial f_n}{\partial x_j})$$

This proves that $f_1^{\alpha_1 - 1} \cdots f_n^{\alpha_n - 1}$ divides the *Gcd*. It remains to show that for each i, there is some $\frac{\partial f}{\partial x_j}$ which is not divisible by $f_i^{\alpha_i}$.
Write $f = f_i^{\alpha_i} h_i$, where h_i is not divisible by f_i. Since f_i is non-constant,some variable x_j is appear in f_i. The product rule gives us

$$\frac{\partial f}{\partial x_j} = f_i^{\alpha - 1} (\alpha_i \frac{\partial f_i}{\partial x_j} h_i + f_i \frac{\partial h_i}{\partial x_j})$$

If this expression is divisible by $f_i^{\alpha_i}$, then $\frac{\partial f_i}{\partial x_j}h_i$ is divisible by f_i. Since f_i is irreducible and does not divide h_i, this forces f_i to divide $\frac{\partial f_i}{\partial x_j}$. As $\frac{\partial f_i}{\partial x_j}$ also has smaller total degree than f_i, it follows that f_i cannot divide $\frac{\partial f_i}{\partial x_j}$. Consequently, $\frac{\partial f_i}{\partial x_j}$ is not divisible by $f_i^{\alpha_i}$, which proves the Lemma. □

Lemma 3.7.4. [14] *Let K be a field and let $f \in k[x]$ with $gcd(f, f') = 1$, then f is squarefree.*

Proof. Assume the contradiction that that f is not squarefree. Then there exists $g, h \in K[x]$ with g is non-constant and $f = g^2h$. It follows that

$$f' = 2gg' + g^2h'$$

and we see that g is a common factor of f and f', which is a contradiction. □

Lemma 3.7.5. ***(Seidenberg's Lemma)*** [14] *Let K be a field and $I \subseteq K[x_1, \ldots, x_n]$ be zero-dimensional ideal. suppose that for every $i \in \{1, \ldots, n\}$, there exists a non-zero polynomial $g_i \in I \cap K[x_i]$ such that $gcd(g_i, g_i') = 1$. Then I is radical ideal.*

Proof. By the above Lemma 3.7.4, g_i is squarefree, for $1 \leq i \leq n$. To prove the Lemma we proceed by induction. If $n = 1$, let $g \in K[x_1]$ which is squarefree, since $K[x_1]$ is principal,then g is generated by squarefree polynomial. Then I is radical ideal.
Now, let $n > 1$. We write $g_1 = h_1 \cdots h_t$ with irreducible polynomials $h_1, \ldots h_t \in K[x_1]$. We claim that $I = \cap_{i=1}^{t}(I + \langle h_i \rangle)$.
For $f \in \cap_{i=1}^{t}(I + \langle h_i \rangle)$, there are $r_i \in I$ and $q_i \in K[x_1, \ldots, x_n]$ such that
$f = r_i + q_i h_i$ for $i = 1, \ldots, t$. since $f \cdot \prod_{j \neq i}^{t} h_j \in I$ for $i = 1, \ldots, t$ and because of $gcd(\prod_{j \neq 1}^{t} h_j, \ldots, \prod_{j \neq t}^{t} h_j) = 1$, we find $l_1, \ldots, l_t \in K[x_1]$ such that $l_1 \prod_{j \neq 1}^{t} h_j + \cdots + l_t \prod_{j \neq t}^{t} h_j = 1$. Altogether,

$$f = \sum_{i=1}^{t} l_i f \prod_{j \neq i}^{t} h_j \in I$$

Because of this claim and the fact that a finite intersection of radical ideals is again radical, it suffices to show that $I + \langle h_i \rangle$ is radical ideal for $i = 1, \ldots, t$.
So we may assume that g_1 is irreducible. Hence the field $K[x_1]/\langle g_1 \rangle$ is a finite K-vector space,and we may consider the canonical homomorphism

$$\Psi : K[x_1] \longrightarrow K[x_1]/\langle g_1 \rangle$$

which induces the canonical surjective homomorphism

$$\varphi : K[x_1][x_2, \ldots, x_n] \longrightarrow K[x_1]/\langle g_1\rangle[x_2, \ldots, x_n]$$

Then $\ker(\varphi) = \langle g_1\rangle \subseteq I$. Since $K[x_1]/\langle g_1\rangle[x_2, \ldots, x_n] \cong K[x_1, \ldots, x_n]/I$, then $\varphi(I)$ is zero-dimensional ideal.
For $i = 2, \ldots, n$, the polynomial $\varphi(g_i) = g_i \in K[x_1]/\langle g_1\rangle[x_2, \ldots, x_n]$ satisfy
$gcd(g_i, g_i') = 1$ over the field $K[x_1]/\langle g_1\rangle$ .Therefore $\varphi(I)$ is radical ideal by the inductive hypothesis, i.e we have no non-zero nilpotents in $K[x_1]/\langle g_1\rangle[x_2, \ldots, x_n]$. The isomorphism shows that $K[x_1, \ldots, x_n]/I$ has no non-zero nilpotent. Hence I is radical ideal. □

As a consequence of Seidenberg's Lemma, we can now prove the following straightforward algorithm for computing the radical of a zero-dimensional polynomial ideal.

Theorem 3.7.6. [7] *Let K be algebraically closed field and let $I \subseteq K[x_1, \ldots, x_n]$ is zero-dimensional ideal. For each $i = 1, \ldots, n$, let g_i be the unique monic generator of $I \cap K[x_i]$ and let g_i^* be the squarefree part of g_i. Then*

$$\sqrt{I} = I + \langle g_1^*, \ldots, g_n^*\rangle$$

Proof. Let $J = I + \langle g_1^*, \ldots, g_n^*\rangle$. We must prove that J is radical ideal, i.e $\sqrt{J} = J$. for each i, using the fact that K is algebraically closed we can factor g_i^* to obtain

$$g_i^* = (x_i - a_{i1}) \cdots (x_i - a_{ij}),$$

where a_{ij} are distinct. Then

$$J = J + \langle g_1^*\rangle = \bigcap_j (J + \langle x_1 - a_{1j}\rangle$$

Now use g_2^* to decompose each $J + \langle x_1 - a_{1j}\rangle$ in the same way. This gives

$$J = \bigcap_{j,k} (J + \langle x_1 - x_{1j}, x_2 - _{2k})$$

If we do this for all $i = 1, \ldots, n$, we get an expression

$$J = \bigcap_{j_1, \ldots, j_n} (J + \langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n}\rangle)$$

Since $\langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n}\rangle$ is maximal ideal,the ideal $J + \langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n}\rangle$ is either $\langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n}\rangle$ or the whole ring $K[x_1, \ldots, x_n]$. It follows that J is a finite intersection of maximal ideals.
Since a maximal ideal is radical in algebraically closed field and an intersection of radical ideals is radical, we conclude that J is a radical ideal.
Now we can prove that $J = \sqrt{I}$.
$I \subset J$ is from the definition of J and since the squarefree parts of the g_i vanishes at $V(I)$, by Strong Nullstellensatz $J \subset \sqrt{I}$. Hence we have

$$I \subset J \subset \sqrt{I}.$$

Taking radicals in this chain of inclusions shows that $\sqrt{J} = \sqrt{I}$. But J is radical, $J = \sqrt{J}$ and we are done. □

Example 3.7.7. *Consider the ideal* $I = \langle y^4x + 3x^3 - y^4 - 3x^2, x^2y - 2x^2, 2y^4x - x^3 - 2y^4 + x^2\rangle \subset \mathbb{C}[x, y]$ *Then to compute the radical of* I*, first let us find the Groebner basis* G *for* I *with a term order lex such that* $x > y$*. Then*

$$G = \{y^4 - 2y^4, xy^4 - y^4, 16x^2 - xy^4\}$$

Then by inspecting the Groebner basis we see that I *is zero-dimensional.*
Therefore by Elimination Theorem

$$I \cap \mathbb{C}[y] = \langle y^4 - 2y^4\rangle$$

and

$$I \cap \mathbb{C}[x] = \langle x^3 - x^2\rangle.$$

Then we are going to find the squarefree part of by writing $g_1 = y^4 - 2y^4$ *and* $g_2 = x^3 - x^2$.
Then

$$g_1^* = \frac{g_1}{gcd(g_1, \frac{dg_1}{dy})} = y(y-2)$$

and

$$g_2^* = \frac{g_2}{gcd(g_2, \frac{dg_2}{dx})} = x(x-1)$$

Then by the above Theorem

$$\sqrt{I} = \langle y^4x + 3x^3 - y^4 - 3x^2, x^2y - 2x^2, 2y^4x - x^3 - 2y^4 + x^2, x(x-1), y(y-2)\rangle$$

3.8 The k-Color Problem

In this section we want to illustrate how one can apply the technique of Groebner bases to solve a well-known problem in graph theory: determining whether a given graph can be k-colored.

Definition 3.8.1. [5] *Let G be a simple graph $G = (V, E)$ with vertices $V = \{1, \ldots, n\}$ and edges E*

1. *A k-coloring of G is an assignment of k colors to the vertices of G.*
2. *A k-coloring is proper if adjacent vertices receive different colors.*
3. *A graph is k-colorable if it has a proper k-coloring.*

First, we let $\xi = e^{\frac{2\pi i}{k}} \in \mathbb{C}$ be a k^{th} root of unity(that is $\xi^k = 1$.) We represent the k-colors by $1, \xi, \ldots, \xi^{k-1}$ the distinct k^{th} roots of unity.

Now, we let $x_1, \ldots, x_n$ be variables representing the distinct vertices of the graph G. Each vertex is to be assigned one of the k-colors $1, \xi, \ldots, \xi^{k-1}$.

This can be represented by the following n equations

$$x_i^k - 1 = 0, 1 \leq i \leq n$$

Now, let $I_k = \langle x_1^k - 1, \ldots, x_n^k - 1 \rangle \subseteq \mathbb{C}[x_1, \ldots, x_n]$.

Also, if the vertices x_i and x_j are connected by an edge, they need to have a different color. Since $x_i^k = x_j^k$, we have $(x_i - x_j)(x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1}) = 0$. Therefore, x_i and x_j have different colors if and only if

$$x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1} = 0$$

Now,let

$$I = I_k + \langle x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1} | (i, j) \in E \rangle \in \mathbb{C}[x_1, \ldots, x_n]$$

Let us denote that $\Gamma_k \subseteq \mathbb{C}^n$ be the set of all k-coloring of G and $\Gamma \subseteq \mathbb{C}^n$ be the set of all proper coloring of G.

Lemma 3.8.2. [5] *I_k and I are zero dimensional radical ideals.*

Proof. From the construction of the ideals I and I_k, we see that $I_k \subset I$, then by ideal-variety correspondence, $V(I) \subseteq V(I_k)$, when we see the nature of I_k, every leading terms of the generator of I_k are relatively prime,then the set $\{x_1^k - 1, \ldots, x_n^k - 1\}$ is the Groebner basis for I_k, the by Theorem 3.3.15, I_k is Zero-dimensional ideal, that is $V(I_k)$ is finite, thus $V(I)$ is finite, which implies that I is Zero-dimensional ideal.
If we let, $f_i = x_i^k - 1$, then $f_i' = kx_i^{k-1}$, since the characteristic of $\mathbb{C}$ does not divide k. This shows that $gcd(f_i, f_i') = 1$. It follows that f_i is square free, the by Lemma 3.7.5 I_k is radical ideal.
Since $I_k \subset I$, then by Seidenberg's Lemma, I is radical ideal. □

Lemma 3.8.3. [5] *I_k and I are the vanishing ideals of the set of all k-colorings of G and the set of all proper k-colorings of G, respectively.*

Proof. Since,I_k is radical ideal, by Hilbert's Nullstellensatz, $I_k = I(V(I_k))$.
Therefore $I_k = \Gamma_k$.
Since $I_k \subset I$, $V(I) \subseteq V(I_k)$. Now let

$$h_{\{i,j\}}^{k-1} = x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1},$$

and let $v = (v_1, \ldots, v_n) \in V(I_k)$ be any k-coloring of G. If v is not proper,there exists vertices $\{i, j\} \in E$, such that $v_i = v_j$.

$$h_{\{i,j\}}^{k-1}(v) = kv_i^{k-1} \neq 0,$$

Since the characteristic of $\mathbb{C}$ does not divide k, then $V(I) \subseteq \Gamma$
To get the reverse direction, notice that

$$(v_i - v_j)(h_{\{i,j\}}^{k-1}(v)) = v_i^k - v_j^k = 1 - 1 = 0$$

Hence, if v is proper, $h_{\{i,j\}}^{k-1}(v)) = 0$, for all $\{i, j\} \in E$. This shows that $\Gamma \subseteq V(I)$. then since I is radical ideal ,then by Hilbert's Nullstellensatz $I = I(V(\Gamma))$. □

Let f_G be the graph polynomial of G given by

$$f_G = \prod_{\{i,j\} \in E, i<j} (x_i - x_j)$$

Lemma 3.8.4. [5] $I_k : \langle f_G \rangle = I$

Proof. Since $\langle f_G \rangle$ is a radical ideal, the by Hilbert's Nullstellensatz

$$\langle f_G \rangle = I(V(\langle f_G \rangle)).$$

Next,let $v = (v_1, \ldots, v_n) \in \Gamma_k$ be any coloring of G. Then $f_G(v) = 0$ if and only if v is improper. Hence

$$\Gamma_k \setminus V(\langle f_G \rangle) = \Gamma$$

Then

$$\begin{aligned} I_k : \langle f_G \rangle &= I(\Gamma_k) : \langle f_G \rangle \\ &= I(\Gamma_k) : I(V(\langle f_G \rangle)) \\ &= I(\Gamma_k \setminus V(\langle f_G \rangle)) \\ &= I(\Gamma) \\ &= I \end{aligned}$$

□

The following Theorem is necessary guide line for whether a given graph is k-colorable or not.

Theorem 3.8.5. [5] *Let I and I_k are the same in the above notation, the following conditions are equivalent*

1. *The graph G is not k-colorable.*
2. *The vector space dimension $\mathbb{C}[x_1, \ldots, x_n]/I$ over $\mathbb{C}$ is zero.*
3. *The constant polynomial 1 belongs to the graph ideal I.*
4. *The graph polynomial f_G belongs to the ideal I_k.*

Proof. (1) $\Rightarrow$ (2) The graph G is not k-colorable if and only if the number of proper k-colorings of G is zero.Therefore $\Gamma = \emptyset$, then
$I(V(I)) = I(\Gamma) = I(\emptyset)$.
Since $\mathbb{C}$ algebraically closed, $I(\emptyset) = \mathbb{C}[x_1, \ldots, x_n] = \langle 1 \rangle$.
Therefore, the vector space dimension $\mathbb{C}[x_1, \ldots, x_n]/I$ over $\mathbb{C}$ is zero.
(2) $\Rightarrow$ (3) Suppose that $dim(\mathbb{C}[x_1, \ldots, x_n]/I) = 0$

Since $\mathbb{C}$ is algebraically closed and $dim(\mathbb{C}[x_1, \ldots, x_n]/I) = 0$ and I is radical ideal, then the number of points to $V(I)$ is equal to zero.Then $V(I) = \emptyset$, then by Weak Nullstellensatz Theorem $I = \mathbb{C}[x_1, \ldots, x_n]$, then $1 \in I$.
(3) $\Rightarrow$ (4) Since by Lemma 3.8.4, $I_k : \langle f_G \rangle = I$, and $I = \langle 1 \rangle$, then $\langle f_G \rangle \subseteq I_k$.
(4) $\Rightarrow$ (1) Let $v = (v_1, \ldots, v_n) \in V(I_k)$, then given that $\langle f_G \rangle \subseteq I_k$, which implies that $v = (v_1, \ldots, v_n) \in V(\langle f_G \rangle)$. Then $f_G = 0$ if and only if $v_i = v_j$, then v is improper, so G is not k-colorable. □

Corollary 3.8.6. [1] *The graph G is k-colorable if and only if $V(I) \neq \emptyset$.*

Proof. Suppose G is k-colorable, Assume the contradiction
Let $V(I) = \emptyset$, then $1 \in I$, which implies that G is not k- colorable.
Suppose $V(I) \neq \emptyset$, since I is zero-dimensional,then $V(I)$ is finite and I is radical, $I = I(V(I)) = I(\Gamma)$, then G is k-colorable. □

Then, Using the above Theorem and Corollary, to determine the given graph G is k-colorable ,first compute the Groebner basis for I, if 1 belongs to the Groebner basis,then G is not k-colorable,otherwise it is k-colorable.

Conclusion

In this thesis we reviewed in detail the theory of Groebner basis over a field and also over commutative ring and we have reviewed improved Buchberger's algorithms to reduce the computation of S-polynomials as Criteria 1 and 2 and also improvements on Buchberger's algorithm using the concept of Syzygies.

At last we saw that the application of Groebner basis in commutative algebra and algebraic geometry and graph theory.

Since different orderings gives us different Groebner basis, and every ideal has only finitely many distinct initial ideals(ideals that are generated by the set of leading terms).Possible extension of this work may encompass to universal Groebner basis and in this thesis we reviewed only Groebner basis over a commutative Noetherian ring, then in future we will see Groebner basis over non-commutative ring.

Bibliography

[1] W. Adams and P. Loustaunau, *An Introduction to Groeobner Bases*, AMS, Providence RI, 1994.

[2] D. Bayer, *The Division Algorithm and the Hilbert Scheme*, Ph.D. Thesis,Harvard University, Cambridge, MA, 1982.

[3] T. Becker and V. Weispfenning, Grobner Bases: A *Computational Approach to Commutative Algebra*, Springer Verlag, Berlin and New York, 1993.

[4] B. Buchberger, *An Algorithm for finding a basis for the residue class ring of a non zero-dimensional polynomial ideal*. Doctoral Dissertation, Math. Institute University of Innsbruck,1965 Austria.

[5] C.J. Hillar, T. Windfeldt / Journal of Combinatorial Theory, Series B 98 (2008) 400-414

[6] D. Cox, J. Little and D. O'Shea , *Using Algebraic Geometry*, Springer-Verlag, New York-Berlin-Heidelberg,1998.

[7] D. Cox, J. Little, and D. O'Shea, Ideals, *Varieties, and Algorithms:An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer Verlag, Berlin and New York,2000.

[8] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 1995.

[9] R. Fröberg , *An Introduction to Groebner Bases*, John Wiley and Sons, 1997.

[10] Gert-Martin Greuel and Gerhard Pfister, *A Singular Introduction to Commutative Algebra*, Springer-Verlag Berlin Heidelberg, 2002.

[11] G.M. Greuel, G. Pfister and H. Schoenemann,*SINGULAR 3.1.4, A Computer Algebra System for Polynomial Computations*, Centre for Computer Algebra, University of Kaiserslautern, http://www.singular.uni-kl. de, 2012.

[12] J. Herzog and T. Hibi, Monomial Ideals, Graduate Texts in Mathematics, Springer-Verlag London,2011.

[13] G. Kemper,A Course in Commutative Algebra,Graduate Texts in Mathematics, Springer-Verlag,Berlin,2011

[14] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1*, Springer-Verlag, Berlin, 2000.

[15] H.M. Möller, *On the construction of Groebner bases using syzygies*, J.Symb. Comp. 6 (1988), 345-359.

Example3.8.7: Consider the graph *G* of Figure 3.8.1

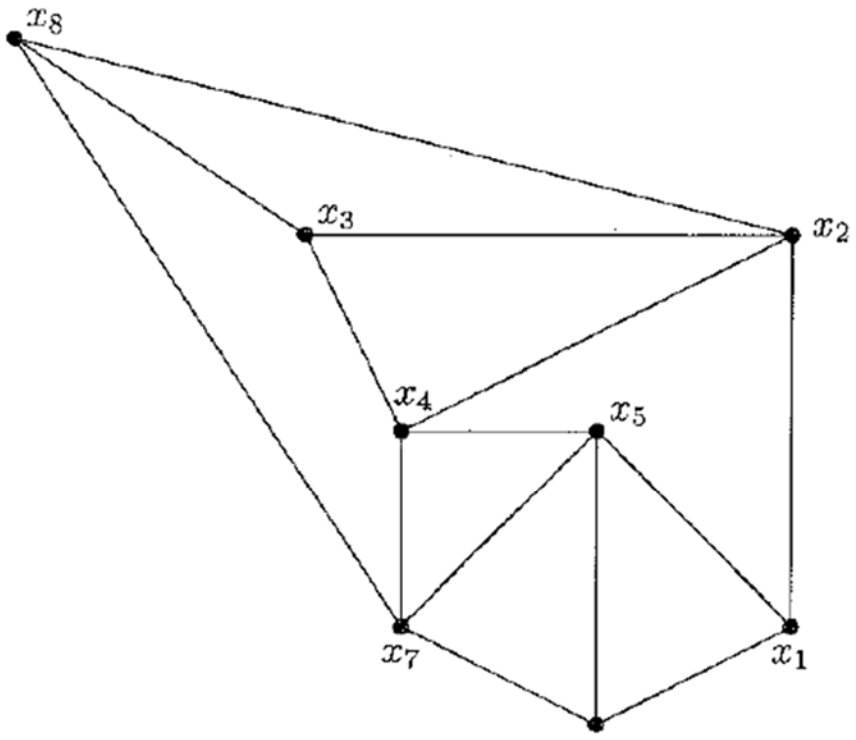

Figure 3.8.1

Let the polynomials corresponding to *G* are

$\{x_i^3$-1, for i= 1, 2,…, 8$\}$

and $x_i^2 + x_i x_j + x_j^2$ for the pair

(i,j)$\in$ {(1,2),(1,5),(1,6),(2,3),(2,4),(2,8),(3,4),(3,8),(4,5),(4,7),(5,6),(5,7),(6,7),(7,8)}.

We compute a Groebner basis G for the ideal I corresponding to the above polynomials with the term order lex such that $x_1 > x_2 > x_3 > x_4 > x_5 > x_6 > x_7 > x_8$.

We obtain

G=$\{x_1$-x_7,x_2+$x_7 + x_8, x_3$-x_7, x_4-x_8,x_5+$x_7 + x_8, x_6$-$x_8, x_7^2 + x_7x_8 + x_8^2$,$x_8^3-1\}$.

Since 1$\notin$ G, we have V(I)$\neq \emptyset$, then G is 3-colorable.