University of Benghazi
Faculty of Science
Department of Mathematics

Operations on Ideals with Maple

A dissertation submitted to the Department of Mathematics in partial Fulfillment of the requirements for the degree of Master of science in Mathematics

By
Sumaia Mohammed Al mogawab

Supervisor
Prof. Kahtan H. Alzubaidy

Benghazi-Libya
2015

Contents

Abstract

Ideals in a polynomial ring of several variables $F[x_1, \dots, x_n]$ are studied. The operations on such ideals are computed. This includes radicals, intersections, sums, products and quotients. The method used is by Groebner basis together with Maple programme.

Introduction

The operations on the ideals in $F[x_1, \dots, x_n]$ including radicals, intersections, sums, products and quotients are computed. The method used is by Groebner basis together with the software Maple13 for the explicit computations of these operations. Some applications of Groebner bases are given. These are ideal membership, equality of two ideals and elimination theory for solutions of non-linear systems of polynomials equations.

The thesis contains four Chapters. **Chapter zero** deals with rings and ideals as necessary background. **Chapter one** studies polynomials of several indeterminates. **Chapter two** studies Groebner basis it's computations and applications. Operations on ideals are introduced in **Chapter three**. And **Appendix** about Maple Programme is put at the end together with a list of used

Chapter zero

Rings and Ideals

This chapter contains the basic definitions and properties of rings, integral domains and fields. It also contains the basic properties of ideals together with the operations of ideals.

Definition

A ring R is anon empty set with two binary operations addition (+) and multiplication (·) such that:

i. $(R, +)$ is an abelian group.
ii. $a(bc) = (ab)c \; for \; all \; a, b, c \in R.$
iii. $a(b + c) = ab + ac \quad and$

$(b + c)a = ba + ca \; for \; all \; a, b, c \in R$.

iv. If $ab = ba \; \forall \, a, b \in R,$ then R is colled **a commutative ring**.
v. If $\exists 1 \in R$ Such that $a \cdot 1 = a = 1.a \quad \forall a \in R, then \; R$ is called **a ring with unity**.

Definition

A ring R with unity is called **a division ring** if every nonzero element of R is a unit (has a multiplicative inverse).

Definition

A commutative ring R with unity is called **integral domain** if $ab = 0$ $implies\ that\ a = 0\ or\ b = 0\ where\ a, b \in R$ [$or\ a \neq 0, b \neq 0 \Longrightarrow ab \neq 0$].

Definition

A field is anon- trivial commutative ring with unity such that every nonzero element has multiplicative inverse.

Definition

Let R be a ring and I a sub ring of R, I is called:

i. **a left ideal** if $ra \in I \quad , \forall\ r \in R \quad , \forall a \in I$

ii. **a right ideal** if $ar \in I \quad , \forall\ r \in R \quad , \forall a \in I$

iii. an ideal (**two sided ideal**) if $ra \in I \quad , ar \in I , \forall\ r \in R\ , a \in I$

Note that left and right ideals are the same if R is commutative.

Definition

Let R be a ring and I an ideal in R. The left cost $r + I = \{r + a : a \in I\}$

$R/I = \{r + I : r \in R\}$, the set of all left cosets of I in R. Addition and multiplication are defined on R/I as follows:

$(r_1 + I) + (r_2 + I) = r_1 + r_2 + I$

$(r_1 + I)(r_2 + I) = r_1 r_2 + I$

The two operations are well-defined.

Definition

A function $f : R \rightarrow R'$ between two ring is called **homomorphism** , if for all $x, y \in R$ we have:

i. $f(x+y) = f(x) + f(y)$

ii. $f(xy) = f(x)f(y)$

The homomorphism is called **epimorphism** if it is onto.

It is called **monomorphism** if it is 1-1.

The homomorphism is called **isomorphism** if it is one-to-one and onto.

$R \cong R'$ Means that R and R' are **isomorphic**.

Definition

Let $f : R \to R'$ be a ring homomorphism . The **kernel** of f is defined by

Ker f = $\{x \in R : f(x) = 0'\} \subseteq R$

Ker f =$f^{-1}(\{\acute{0}\})$. Ker f is an ideal of$R$.

Theorem(0.1) (1st isomorphism theorem)

Let $f : R \to R'$ be an onto ring homorphism then $R/_{kerf} \cong R'$.

Types of Ideals

Principal Ideal

Let R be a commutative ring with unity and $a \in R$. **A principal ideal generated** by a is defined

$$\langle a \rangle = \{ra : r \in R\} \equiv Ra$$

Prime Ideal

Let R be a commutative ring and N an ideal with $N \neq R$. N is called **a prime ideal** if $ab \in N$ implies $a \in N$ or $b \in N$ where $a, b \in R$.

Theorem (0.2)

N is a prime ideal iff R/N is an integral domain.

Maximal Ideal

Let R be a ring and M an ideal of R with $M \neq R$. M is called **a maximal ideal** of R if there is no ideal I. Such that $M \subset I \subset R$.

i.e the only ideals containing M are M and R.

Theorem (0.3)

Let R be a commutative ring with unity. Then M is maximal iff R/M is afield.

Definition

An integral domain in which every ideal is principal ideal is called **a principal ideal domain** (PID).

Definition

An integral domain D is **Euclidean domain** if for each non-zero element $a \in D$ there exists a non-negative integer $d(a)$ such that

i. If a and b are non-zero element of D then

$d(a) \leq d(ab)$.

ii. If $a, b \in D,$ with $b \neq 0$,then there exists elements $q, r \in D$ such that $a = bq + r$ with $r = 0$ or $d(r) < d(b)$.

Theorem (0.4)

Every Euclidean domain is principal ideal domain.

Definition

A unique factorization domain (UFD) is integral domain D satisfying the following properties:

i. Every non-zero element a in D can be expressed as

$a = up_1 \dots p_n$, Where u is unit and the p_i are irreducible.

ii. If a has another factorization, say $a = uq_1 \dots q_m$, where u is unit and the q_i are irreducible, then $n = m$ and after reordering if necessary p_i and q_i are associates for each i.

Theorem (0.5)

Every principal ideal domain is unique factorization domain.

Theorem (0.6)

Any ED is UFD.

Operations on ideals

Let R be commutative ring with unity. Let I and J be two ideals in R.

I) Radical ideal

The radical of I is defined by $\sqrt{I} = \left\{ r \in R : r^n \in I \text{ for some } n \in \mathbb{Z}^+ \right\}$

$\sqrt{I}$ is an ideal containing I .

The radical I is called ideal if $I = \sqrt{I}$. $\sqrt{\{0\}}$ is called the nil radical of R.

Proposition

$\sqrt{I}$ is an ideal in R.

Proof

First of all $0 \in \sqrt{I}$ since $0 = 0^1 \in \sqrt{I}$

Suppose $x, y \in \sqrt{I}$, then $x^n \in I$ for some $n \geq 1$,

and $y^m \in I$ for some $m \geq 1. Let, N = m + n, then$

$(x - y)^N = \sum_{k=0}^{N} (-1)^k (k)^N x^{N-k} y^k$ *for each* $k, 0 \leq k \leq N$

Either $k \geq m$ *or* $N - k = n + (m - k) \geq n$.

Thus $y^k \in I$ *or* $x^{N-k} \in I$ for every K

Since I is an ideal , it follows that $(x - y)^N \in I$. *Thus* $x - y \in \sqrt{I}$

Suppose that $x \in \sqrt{I}$ and $r \in R$, then $x^n \in I$ *for some* $n \geq 1$,
and then $(rx)^n = r^n x^n \in I$ there fore $rx \in \sqrt{I}$.

Hence $\sqrt{I}$ is an ideal of R.

Examples

1- Every prime ideal is radical ideal.
2- $\sqrt{m\mathbb{Z}}$ = radical $(m)\mathbb{Z}$.

Radical (m)= the product of the prime divisors of m.

e.g.: $\sqrt{5\mathbb{Z}} = 5\mathbb{Z}$, $\sqrt{8\mathbb{Z}} = 2\mathbb{Z}$, $\sqrt{12\mathbb{Z}} = 6\mathbb{Z}$, $\sqrt{4\mathbb{Z}} = 2\mathbb{Z}$.

Proportions

i. If $I \subset J$ *for* , $n \in \mathbb{Z}^+$ then $\sqrt{I} \subseteq \sqrt{J}$.

ii. $\sqrt{I} = \sqrt{\sqrt{I}}$.

iii. $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

iv. I is radical iff R/I is radical.

(i.e R/I has no non-zero nilpotent element).

II) Intersections of ideals

$I \cap J = \{a \in R : a \in I, a \in J\}$.

Proposition

$I \cap J$ is an ideal of R.

Proof

The set $I \cap J$ is nonempty since $0 \in I$ and $0 \in J$ so $0 \in I \cap J$.

Let $a, b \in I \cap J$, *then* $a, b \in I$ *and* $a, b \in J$

Since I *and* J are ideals ,we have

$a - b \in I$ *and* $a - b \in J$,*so* $a - b \in I \cap J$.

Let $r \in R$, $a \in I$ then $ra \in I$ since I is an ideal of R.

Also $a \in J$ so $ra \in J$ since J is an ideal of R hence $ra \in I \cap J$.

Thus $I \cap J$ is an ideal of R.

Example

In $\mathbb{Z}$ *we have* $\langle m \rangle \cap \langle n \rangle = \langle r \rangle$,*where* r *is the lcm of* m *and* n.

III) Union

$I \cup J$ is not ideal in general but $\langle I \cup J \rangle$ is the ideal generated by the set $I \cup J$.

Example

In $\mathbb{Z}$ *we have* $\langle\langle m\mathbb{Z}\rangle \cup \langle n\mathbb{Z}\rangle\rangle = \langle m\mathbb{Z} \cup n\mathbb{Z}\rangle$.

IV) sums of ideals

The sum of I *and* J denoted by $I + J$ is the set

$I + J = \{ a + b , a \epsilon I$ and $b \epsilon J \}$.

Proposition

$I + J$ is an ideal of R.

Proof

We have that $I + J$ is nonempty since

$0 = 0 + 0 \in I + J$ *let* $x , y , \in I + J$, by defined $x = a + b$ and $y = c + d$ for some $a , c \in I$ and $b, d \in J$.

Then $x - y = (a + b) - (c + d) = (a - c) + (b - d) \in I + J$

since I and J are ideals.

Suppose $r \in R \quad x = a + b \in I + J$.

$r\,a \in I$ *and* $r\,b \in J$ *since* I *and* J *are ideals* .

Hence $r\,x = r\,a + r\,b \in I + J$

Thus $I + J$ is an ideal of R .

Example

In $\mathbb{Z}$ *we have* $\langle m\rangle + \langle n\rangle = \langle (m, n)\rangle$.

(IV) products of ideals

Define the product of two ideals by

$I\,J \;= \{\, \sum_{i=1}^{n} a_i b_i : a_i \;\in\; I$ and $b_i \;\in\; J\,, n \;\in N \,\}$.

Proposition

$I\,J$ is an ideal of R.

Proof

Consider tow arbitrary element of $I\,J$ say

$a_1 b_1 + \ldots + a_m b_m\,, c_1 d_1 + \ldots + c_n d_n \;\in I\,J$

Where $a_1\,, \ldots\,, a_m\,, c_1\,, \ldots\,, c_m \;\in\; I$ and $b_1\,, \ldots\,, b_n\,,\; d_1\,, \ldots\,, d_n \in J$.

Ideals are closed under differences and contain 0 .So ideal are closed under additive inverse (-).

That is , if $a \;\in I$ then $-a = 0 - a \;\in I$.

Thus $a_1\,, \ldots\,, a_m\,, -c_1\,, \ldots\,, -c_m \;\in I$ and $b_1\,, \ldots\,, b_n\,, d_1\,, \ldots, d_n \;\in J$ so the difference of two elements in $I\,J$ is again in $I\,J$ because it is a finite sum of products of the form $a\,b\;(\,a \;\in\; I\,, b \;\in\; J\,)$.

$$a_1 b_1 + \ldots + a_m b_m - (c_1\, d_1 + \ldots + c_n d_n)$$
$$= a_1 b_1 + \ldots + a_m b_m + (-c_1) d_1 + \ldots + (-c_n) d_n \;\in\; I\,J$$

For any $r \;\in R$, we have $r\,a_1\,, \ldots\,, r\,a_m \;\;\in I$ since I is an ideal

$b_1 r\,, \ldots\,, b_m r \in J$ Since J is an ideal and

$r\,(a_1 b_1 + \;\ldots + a_m b_m) = (r\,a_1)\,b_1 + \ldots + (r\,a_m)\,b_m \;\in I\,J$

$$(a_1 b_1 + \;\ldots + a_m b_m)\,r = a_1(\,b_1\,r) + \;\ldots + \;a_m\,(b_m r) \;\;\in\; I\,J$$

So $I\,J$ is an ideal because it is closed under difference and also closed under left and right multiplication by arbitrary element of R.

Example

In $\mathbb{Z}$ *we have* $\langle m\rangle\langle n\rangle = \langle mn\rangle$.

(VI) Quotient of ideals

Quotient of I by J is defined by

$I : J = \{r \in R : r\,b \in I$ for each $b \in J\}$.

Proposition

$I : J$ is an ideal of R.

Proof

Let $r_1, r_2 \in I : J$ Then $r_1 b \in I$ for all $b \in J$, $r_2 b \in$ I for all $b \in J$

So we have $r_1 b - r_2 b \in I$ since I is an ideal, then $(r_1 - r_2)b \in I$

Thus $(r_1 - r_2) \in I : J$

Let $r \in I : J$ and $\bar{r} \in R$

So $r \in I : J$ implies $r\,b \in$I for all $\in J$.

But $\bar{r}\,b \in J$ since J is an ideal, then $r(\bar{r}\,b) \in I$, $r\,\bar{r} \epsilon I : J$

Thus $I : J$ is an ideal of R.

Chapter one

Polynomials

In this chapter we outline the definitions and basic properties of polynomials in single and several indeterminates.

Polynomial in one Indeterminate

Let R be commutative ring with unity and x is an indeterminate (x is a symbol not in R).

A polynomial in x over R is an expression

$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$,Where $a_n, a_{n-1}, \ldots a_1, a_0$ are called the coefficients of the polynomial and $n > 0$ an integer.

If$a_n \neq 0$, then the polynomial is said to be of degree n,

$a_n x^n$ is called the leading term and a_n is called the leading coefficient.

If a_n= 1 the polynomial is called a monic polynomial.

A polynomial of degree 0 is called a constant polynomial

$a = a + 0\,x + \cdots + 0\,x^{\,n}$

A zero polynomial $0 = 0 + 0x + \ldots + 0\,x^n$.

Notation

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in R, n > 0\}.$$

The set $R[x]$ is called the ring of polynomials over R in the indeterminate x with coefficients in R.

Operations on $R[x]$

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and

$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in R[x]$.

(I) Equality of $R[x]$

$$f(x) = g(x) \text{ iff } m = n \ \ and \ \ a_0 = b_0\ ,\ a_1 = b_1, \dots, a_n = b_n\,.$$

(II) Addition of $R[x]$

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0,$$

Where s is the maximum of m and n , $a_i = 0\ for\ i > n$

and $b_i = 0\ for\ i > m$.

$f(x) + g(x) \in R[x]$ and $\deg(f(x) + g(x)) \leq Max\,(\deg f(x), \deg g(x))$.

(III) Multiplication of $R[x]$

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1 x + c_0\ \ ,$$

Where $c_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$

For $k = 0, \dots m + n$.

$f(x)g(x) \in R[x]$ and $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

Theorem (1.1)

If R is a commutative ring with unity, then so is $R[x]$.

Theorem (1.2)

If R is an integral domain, then so is $R[x]$.

$\mathbb{Z}[x]$ is integral domain.

Corollary (1.1)

If F is a field, then $F[x]$is an integral domain.

$\mathbb{Q}[x]$, $\mathbb{R}[x]$, c $[x]$, $\mathbb{Z}_p$ $[x]$ are integral domains.

Divisibly in F [x]

Definition

Let F be afield and $f(x)$, $g(x) \in F[x]$, $g(x) \neq 0$, $g(x)$ divides $f(x)$, denoted by $g(x)|f(x)$ if $\exists$ $h(x) \in F[x]$ such that $f(x) = h(x)\, g(x)$.

Properties

1. $f(x)|f(x)$.
2. If $f(x)|g(x)$ and $g(x)|f(x)$, then $f(x) = c\, g(x)$.
3. If $f(x)|g(x)$ and $g(x)|h(x)$, then $f(x)|h(x)$.
4. If $g(x)|f(x)$, then $\deg g(x) \leq \deg f(x)$.
5. If $g(x)|f(x)$, then $c\, g(x)|f(x)$, $c \neq 0$.

Theorem (1.3) (division algorithm)

Let $f(x)$, $g(x) \epsilon F[x]$ with , $g(x) \neq 0$, then $\exists$ unique polynomials $q(x)$and $r(x)$ such that:

$f(x) = q(x)g(x) + r(x)$, Where $r(x) = 0$ *or* $\deg r(x) < \deg g(x)$.

$q(x)$ is called **the quotient** and $r(x)$ is **the remainder**.

Theorem (1.4) (Remainder)

Let F be a field , $a \in F$ and $f(x) \in F[x]$.

Then $f(a)$ is the remainder in the division of $f(x)$ by $x-a$.

Definition

$\alpha \in F$ is called **a root** or zero of $f(x) \in F[x]$ if $f(\alpha)=0$.

Theorem (1.5) (Factor)

Let F be afield , $a \in F$ and $f(x) \in F[x]$.

Then a is a zero of $f(x)$ if and only if $x-a$ is a factor of $f(x)$.

Theorem (1.6)

A polynomial of degree n over afield F has at most n roots in .

Definition

Let $f(x), g(x) \in F[x]$. Amonic $d(x) \in F[x]$ is **greatest common divisor** of $f(x)$ and $g(x)$, if

i. $d(x)|f(x), d(x)|g(x)$.
ii. If $\acute{d}(x)|f(x), \acute{d}(x)|g(x), then\ \acute{d}(x)|d(x)$.

We write $\gcd\big(f(x), g(x)\big)=d(x)$.

$f(x)$and $g(x)$ are relatively prime, if gcd $\big(f(x), g(x)\big)=1$.

Theorem (1.7)

For $f(x), g(x) \in F[x]$, $\gcd\big(f(x), g(x)\big)$ exists and is unique.

Theorem (1.8)

gcd $\big(f(x), g(x)\big)= u(x)f(x)+v(x)g(x)$ For some $u(x), v(x) \epsilon F[x]$.

Definition

Let $f(x), g(x) \in F[x]$, $l(x) \in F[x]$ is a **least common multiple** of $f(x)$ and $g(x)$ if :

i. $f(x)|l(x)$ and $g(x)|l(x)$.

ii. If $f(x)\big|\grave{l}(x)$ and $g(x)\big|\grave{l}(x)$, then $l(x)\big|\grave{l}(x)$ we write

$$lcm\big(f(x), g(x)\big) = l(x).$$

Theorem (1.9)

$\gcd\big(f(x), g(x)\big) . lcm\big(f(x), g(x)\big) = f(x)\, g(x)$ For any

$f(x), g(x) \in F[x]$.

Definition

A non-constant polynomial in $F[x]$is **irreducible** if it can not be factored in $F[x]$ *into* a product of two polynomials of lowers degrees. Otherwise it is called **reducible.**

Theorem (1.10)

Let $f(x), g(x), p(x), \in F[x]$ and $p(x)$ irreducible if $p(x)|f(x)\, g(x)$, then either $p(x)|f(x)$ or $p(x)|g(x)$.

Theorem (1.11)

Any non-constant polynomial in $F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials.

The product is unique up to the order and units.

Corollary (1.2)

$F[x]$ is UFD (unique factorization domain).

Theorem (1.12)

$F[x]$ is $a\ PID$ for any field F.

Remark

$\mathbb{Z}[x]$ is not PID .

Theorem (1.13)

If F is a field, then $F[x]$ is a Euclidean domain with $d\big(f(x)\big) = \deg f(x)$.

Theorem (1.14)

Let $p(x) \in F[x]$. Then $p(x)$ is irreducible iff $\langle p(x)\rangle$ is a maximal ideal in $F[x]$.

Operations on ideal in $F[x]$

1. If $f(x)|\text{g}(x)\ then \langle \text{g}(x)\rangle \subseteq \langle f(x)\rangle$.
2. $\langle f(x)\rangle \cap \langle \text{g}(x)\rangle = \langle L.c.m\ \big(f(x)\ ,\text{g}(x)\big)\rangle$.
3. $\langle f(x)\rangle + \langle \text{g}(x)\rangle = \langle f(x)\ , g(x)\rangle$
   $= \langle \text{gcd}\ \big(f(x)\ ,\text{g}\ (x)\big)\rangle$.
4. $\langle f(x)\rangle\langle \text{g}(x)\rangle = \langle f(x)\ \text{g}(x)\rangle$.
5. $\langle c\rangle = F[x]\ , c = constant.$
6. If $f(x) = c\ \text{g}\ (x)$, then $\langle f(x)\rangle = \langle \text{g}(x)\rangle$.

Theorem (1.15)

Let $f(x)\ \in\ F[x]$ of degree n then

i. $F[x]/\langle f(x)\rangle$ is ring.

ii. $F[x]/\langle f(x)\rangle = \{a_{n-1}x^{n-1} + \ldots + ax_1 + a_o + \langle f(x)\rangle : a_i \in F\}$

$\equiv \{a_{n-1}x^{n-1} + \ldots + ax_1 + a_o : a_i \in F, f(x) = 0\}.$

Theorem (1.16) (Chinese remainder theorem)

Let $\mathrm{g}(x)$ be a non-constant polynomial in $F[x]$ with its factorization into distinct irreducible

$\mathrm{g}(x) = \left(f_1(x)\right)^{n_1} \ldots \left(f_k(x)\right)^{n_k}$.

Then $F[x]/\langle \mathrm{g}(x)\rangle \cong F[x]/\langle f_1(x)\rangle^n \times \ldots \times F[x]/\langle f(x_k)^{nk}\rangle$.

Theorem (1.17) (kroncker)

Let $p(x)$ be irreducible over F of degree n then

i. $F[x]/\langle p(x)\rangle$ is a field.

ii. $F[x]/\langle p(x)\rangle = \{a_{n-1}x^{n-1} + \ldots + a_1x + a_o + \langle p(x)\rangle : a_i \in F\}$

$\equiv \{a_{n-1}x^{n-1} + \ldots + a_1x + a_o : a_i \in F, p(x) = 0\}.$

iii. $\{a + \langle p(x)\rangle : a \in F\}$ is a subfield of $F[x]/\langle p(x)\rangle$.

iv. $\{a + \langle p(x)\rangle : a \in F\} \cong F$.

v. $x + \langle p(x)\rangle$ is a root of $p(x)$ in $F[x]/\langle p(x)\rangle$.

Remarks

1. Let $f(x)$ be anon constant polynomial in $F[x]$. Then there exists a field extension E of F such that E continues a root of $f(x)$
2. Let $f(x)$ be an on constant polynomial in $F[x]$ of degree n then there a field extension E of F such that $f(x)$ be factored a product of n linear factors $i.e$ E contains all the roots of $f(x)$.

Multivariate polynomials

Let R be a commutative ring with unity and $x_1, x_2, \dots, x_n$ algebraically independent indeterminates over R.

A monomial is $x_1^{\epsilon_1} \; x_2^{\epsilon_2} \; \dots \; x_n^{\epsilon_n}$; where $\epsilon_1, \epsilon_2, \dots, \epsilon_n \in \{0, 1, 2 \dots\}$.

The degree of the monomial is $(\epsilon_1, \epsilon_2, \dots, \epsilon_n)$.

The total degree of the monomial is $\epsilon_1 + \epsilon_2 + \dots + \epsilon_n$.

A term is $a_{\epsilon_1 \dots \epsilon_n} x_1^{\epsilon_1} \; \dots \; x_n^{\epsilon_n}$ where $a_{\epsilon_1 \dots \epsilon_n} \epsilon R$ is the coefficient.

A polynomial in $x_1, x_2, \dots, x_n$ over R is a finite sum of terms

$f(x_1, x_2, \dots, x_n) = \sum a_{\epsilon_1 \dots \epsilon_n} x_1^{\epsilon_1} \; x_2^{\epsilon_2} \; \dots \; x_n^{\epsilon_n}$.

The degree of $f(x_1, x_2, \dots, x_n)$ is the maximum total degree of its monomials.

Examples

1- $f(x, y) = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3$
is a polynomial of degree 3 in x, y over R.

2- $f(x, y, z) = 2x^2y^2 z + 3x^2y z - 4xyz + 7$ is a polynomial of degree 5 in x, y, z over $\mathbb{Z}$.

Notation

$R[x_1, x_2, \dots, x_n]$ is the set of all polynomials in $x_1, x_2, \dots, x_n$ over R.

Equality and addition of polynomial in $R[x_1, x_2, \dots, x_n]$ are defined coefficient wise.

Addition in $R[x_1, \dots, x_n]$ is defined as usual.

Multiplication in $R[x_1, x_2, \dots, x_n]$ is defined by using distributive law and the rule of exponents.

$$(x_1^{\epsilon_1}\ x_2^{\epsilon_2}\ \dots\ x_n^{\epsilon_n})\left(x_1^{\delta_1}\ x_2^{\delta_2}\ \dots\ x_n^{\delta_n}\right) = \left(x_1^{\epsilon_1+s_1}\ x_2^{\epsilon_2+\delta_2}\ \dots\ x_n^{\epsilon_n+\delta_n}\right).$$

Proposition

$R[x_1, \dots, x_n]$ is a commutative ring with unity.

Another definition of $R[x_1, \dots, x_n]$

$R[x_1, x_2, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n], n \geq 2$.

Note that $R[x_1, x_2, \dots, x_n]$ is a commutative ring with unity by induction on.

Example

$f = 2x^3y + x^2y^2 - 5xy^2 + 2x + 3y + 1 \in \mathbb{Z}[x, y]$.

$f = (x^2 - 5x)y^2 + (2x^3 + 3)y + (2x + 1) \in \mathbb{Z}[x][y] = \mathbb{Z}[x, y]$.

$f = (2y)x^3 + (y^2)x^2 + (-5y^2 + 2)x + (3y + 1) \in \mathbb{Z}[y][x] = \mathbb{Z}[y, x]$.

Proposition

The two definitions of $R[x_1, x_2, \dots, x_n]$ are equivalent.

Proposition

$R[x_1, x_2, \dots, x_n] \cong \mathrm{R}\left[x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}\right]$, for any permutation σ of degree n .

Remarks

i. $R \leq R[x] \leq R[x_1, \dots, x_n] \leq \cdots \leq R[x_1, x_2, \dots, x_n]$, a chain of sub rings.

ii. If $S \leq R$,then$S[x_1, \dots, x_n] \leq R[x_1, \dots, x_n]$.

iii. Let I be an ideal of R, then

1- $I[x_1, \dots, x_n]$ is an ideal of $R[x_1, \dots, x_n]$.

2- $R[x_1, \dots, x_n]/I[x_1, \dots, x_n] \cong (R/I)[x_1, \dots, x_n]$.

Proposition

If D is an integral domain ,then so is D $[x_1, x_2, \dots, x_n]$.

Corollary (1.3)

If F is a field then $F[x_1, \dots, x_n]$ is an integral domain.

Remarks

i. $F[x]$ is ED and hence PID and UFD.

ii. $F[x_1, \dots, x_n]$ is not PID and hence not ED.

Example

Consider $\mathbb{Q}[x, y]$

$\langle x, y\rangle \neq \mathbb{Q}[x, y]$, Since $\langle x, y\rangle$ contains no constants

$\langle x, y\rangle$ Can not be generated by any $f(x, y) \in \mathbb{Q}[x, y]$

$\therefore \mathbb{Q}[x, y]$ is not PID.

Proposition

If R is UFD, then so is $R[x_1, \dots, x_n]$.

Proposition

$\mathbb{Z}[x_1 , \dots , x_n]$ is UFD.

Corollary (1.4)

$F[x_1 , \dots , x_n]$ is UFD for any field F.

Remarks

i. There is no division algorithm in $F[x_1, \dots, x_n]$.

ii. gcd exists and unique in $F\ [x_1 , x_2 , \dots , x_n]$.

iii. gcd $(f, \mathrm{g}) = uf + v\mathrm{g}$ for sum $u, v\ \in\ F[x_1 , \dots , x_n]$ is not valid in $F[x_1 , \dots , x_n]$.

Chapter two

Groebner Bases

In this chapter we introduce the general division algorithm and Groebner basis for an ideal in $F[x_1, \dots, x_n]$. Calculations are done by using Maple program.

Monomial Ordering

Consider $F\,[x_1, \dots, x_n]$. Fix an order $x_1 > x_2 > \cdots > x_n$ on the indeterminates $x_1, x_2, \dots, x_n$. There are $n!$ orders on$x_1, x_2, \dots, x_n$. A monomial ${x_1}^{\epsilon_1}{x_2}^{\epsilon_2} \dots {x_n}^{\epsilon_n}$ can be written briefly as x^{ϵ} where $\epsilon = (\epsilon_1, \dots, \epsilon_n)$. Thus $x^{\epsilon} = {x_1}^{\epsilon_1}, {x_2}^{\epsilon_2}, \dots, {x_n}^{\epsilon_n}$. Denotes

$|\epsilon| = \epsilon_1 + \epsilon_2 + \cdots + \epsilon_n.$

A monomial ordering is an order $>$ such that:

i. $>$ is total order,
ii. $>$ is a well order ,
iii. if $x^{\alpha} > x^{\beta}$ $, then\ x^{\alpha}x^{\gamma} > x^{\beta}x^{\gamma}.$

The following monomial orders are usually used:

1. Lexicographic order (Lex)

$x^{\alpha} \ >_{Lex} \ x^{\beta}$ if the left most nonzero entry of $\alpha - \beta$ is positive.

2. Graded Lexicographic order (grlex)

If $|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$, then $x^{\alpha} >_{grLex} x^{\beta}$.

If $|\alpha| = |\beta|$, use $>_{Lex}$.

3. Graded Reverse Lexicographic Order (grevlex)

If $|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$,then $x^\alpha >_{grevlex} x^\beta$.

If $|\alpha| = |\beta|$ $x^\alpha >_{grevlex} x^\beta$ when the right most nonzero entry of $\alpha - \beta$ is negative.

Example

Let $x > y > z$

Lex: $x^3y^2z > xy^5 > y^3z^4$

grlex: $y^3z^4 > x^3y^2z > xy^5$

grevlex: $y^3z^4 > xy^5 > x^3y^2z$

Notations

Let $f \in F[x_1, x_2, \dots, x_n]$. With a given order on monomials:

i. Multideg (f) =max $(\epsilon: x^\epsilon$ is a monomial of f)the multidegree of f.

ii. $LC(f) = a_{\text{multideg}(f)}$,the leading coefficient of.

iii. $LM(f) = x^\epsilon$, where $\epsilon = \text{multideg}(f)$, the leading monomial.

iv. $LT(f) = LC(F)LM\,(f)$, the leading term of f .

Example

```
> # Ordering the terms using the lex order,
      the grlex order,and the grevlex order.
> restart;
>
> with(Groebner) :
> f := 4·x·y^2·z + 4·z^2 − 5·x^3 + 7·x^2·z^2;
```

$$f := 4\,x\,y^2\,z + 4\,z^2 - 5\,x^3 + 7\,x^2\,z^2$$

> $sort(f, order = plex(x, y, z));$

$$-5\,x^3 + 7\,x^2\,z^2 + 4\,x\,y^2\,z + 4\,z^2$$

> $sort(f, order = grlex(x, y, z));$

$$7\,x^2\,z^2 + 4\,x\,y^2\,z - 5\,x^3 + 4\,z^2$$

> $sort(f, order = tdeg(x, y, z));$

$$4\,x\,y^2\,z + 7\,x^2\,z^2 - 5\,x^3 + 4\,z^2$$

> $degree(f, \{x, y, z\});$

$$4$$

> $LeadingCoefficient(f, plex(x, y, z));$

$$-5$$

> $LeadingCoefficient(f, grlex(x, y, z));$

$$7$$

> $LeadingCoefficient(f, tdeg(x, y, z));$

$$4$$

> $LeadingMonomial(f, plex(x, y, z));$

$$x^3$$

> $LeadingMonomial(f, grlex(x, y, z));$

$$x^2\,z^2$$

> $LeadingMonomial(f, tdeg(x, y, z));$

$$x\,y^2\,z$$

> $LeadingTerm(f, plex(x, y, z));$

$$-5, x^3$$

> $LeadingTerm(f, grlex(x, y, z));$

$$7, x^2\,z^2$$

> $LeadingTerm(f, tdeg(x, y, z));$

$$4, x\,y^2\,z$$

<u>General Division Algorithm</u>

Unlike $F[x]$ the integral domain $F[x_1, x_2, \dots, x_n]$ has no division algorithm, since $F[x_1, x_2, \dots, x_n]$ is not ED.

Instead we have general division algorithm which states as follows

Suppose that there is a monomial order on $F[x_1, x_2, \dots, x_n]$.

If f, $g_1, g_2, \dots, g_m \in F[x_1, x_2, \dots, x_n]$, then there are $q_1, q_2, \dots, q_m, \in F[x_1, x_2, \dots, x_n]$ such that:

$f = q_1 g_1 + q_2 g_2 + \dots + q_m g_m + r$,where no term of r is divisible by any of LT (g_1) ,LT (g_2) , … , LT (g_m).

Example

Fix $x > y$ as a lex order $F\,[x, y]$ and

Let $f = x^2y + xy^2 + y^2$, $g_1 = xy - 1$, $g_2 = y^2 - 1$.

Divide f by g_1 and then by g_2

$$
\begin{array}{c|l}
xy-1 & x^2y + xy^2 + y^2 \\
\hline
 & \underline{x^2y \qquad -x} \\
x+y & xy^2 + x \quad + y^2 \\
 & \underline{xy^2 \qquad -y} \\
 & x + y + y^2
\end{array}
\qquad \& \qquad
\begin{array}{c|l}
y^2-1 & x + y^2 + y \\
\hline
 & y^2 + y + x \\
1 & \underline{y^2 - 1} \\
 & x + y + 1
\end{array}
$$

$\therefore f = (x + y)g_1 + 1g_2 + (x + y + 1)$. $\therefore r = x + y + 1$.

Now, divide f by g_2 and then by g_1.

$$
\begin{array}{c|l}
y^2-1 & x^2y + xy^2 \quad + y^2
\end{array}
\qquad \& \qquad
\begin{array}{c|l}
xy-1 & x^2y + x + 1 \\
\hline
\end{array}
$$

$$
\begin{array}{lll}
 & xy^2 + y^2 + x^2y & \qquad x \qquad \underline{x^2y - x} \\
\underline{\qquad\qquad} & \underline{xy^2 - x \qquad\qquad} & \qquad\qquad 2x + 1 \\
x + 1 & y^2 + x^2y + x & \\
 & \underline{y^2 - 1 \qquad\qquad} & \\
 & x^2y + x + 1 &
\end{array}
$$

$\therefore f = (x+1)g_2 + xg_1 + (2x+1)$. $\quad \therefore r = 2x + 1$.

Note that q_1, q_2, r are not unique in the two cases above.

Grobner Bases

Let I be an ideal of $F[x_1, \dots, x_n]$.

Theorem (2.1) (Hilbert Basis) [1] [4]

Every ideal in $F[x_1, \dots, x_n]$ has finite generating set,

$I = \langle f_1, \dots, f_m \rangle \quad , \quad f_i \in F[x_1, \dots, x_n]$.

I is a monomial ideal if $I = \langle x^\alpha : \alpha \in \mathbb{N}^n \rangle$.

i.e $I = \langle monomials\ (possibly\ infinite) \rangle$.

Theorem (2.2) (Dickson)[1] [4]

Every monomial is finitely generated (by monomials)

i.e $I = \langle x^{\alpha_1}, \dots, x^{\alpha_k} \rangle$for some $\alpha_1, \dots, \alpha_k \in \mathbb{N}^n$.

Notations

$LT(I) = \{LT(f): f \in I - \{0\}\}$.

$\langle LT(I)\rangle = \langle LT(f): f \in I - \{0\}\rangle$ is a monomial ideal.

Let $I = \langle g_1, \dots, g_t \rangle$, $g_i \in F[x_1, \dots, x_n]$.

$\langle LT(g_1), \dots, LT(g_t)\rangle \subseteq \langle LT(I)\rangle$.

The equality does not hold in general.

Definition (Groebner Basis)

$\{g_1, \dots, g_t\}$ is **a Groebner Basis** of I if $\langle LT(g_1), \dots, LT(g_t)\rangle = \langle LT(I)\rangle$

Properties

i. Any ideal I of $F[x_1, \dots, x_n]$ has a Groebner basis.

ii. Let $\{g_1, \dots, g_t\}$ be a Groebner basis for an ideal I of $F[x_1, \dots, x_n]$ and $f \in F[x_1, \dots, x_n]$. Then $f = q_1 g_1 + \cdots + q_t g_t + r$ where $q_1, \dots, q_t, r \in F[x_1, \dots, x_n]$ and r is unique ((the remainder)).

iii. $f \in I$ iff $r = 0$.

Notations

i. Let $B = \{f_1, \dots, f_m\}$ be basis of an ideal I of $F[x_1, \dots, x_n]$ and $f \in F[x_1, \dots, x_n]$, $f = q_1 f_1 + \dots + q_m f_m + r$

$r = \bar{f}^B$, the remainder.

ii. **S – polynomial**

For $f, g \in F[x_1, \dots, x_n]$,

$$S\,(f\,,\mathrm{g}) = \frac{x^{\gamma}}{LT\,(\,f\,)}\,f - \frac{x^{\gamma}}{LT\,(\,\mathrm{g}\,)}\,\mathrm{g}\,,$$

Where $x^{\gamma} = lcm\,(\,LM\,(\,f\,)\,, LM\,(\,\mathrm{g}\,))$.

Example

```
> # To compute SPolynomial.
> restart;
>
> with(Groebner) :
>
> f := x^3y^2 − x^2y^3 + x;
```

$$f := x^3\,y^2 - x^2\,y^3 + x$$

```
> g := 3 x^4y + y^2;
```

$$g := 3\,x^4\,y + y^2$$

```
> SPolynomial(f, g, grlex(x, y));
```

$$-3\,x^3\,y^3 + 3\,x^2 - y^3$$

Theorem (2.3) (Buchberger) [1]

A basis $G = \{\,\mathrm{g}_1\,, \ldots\,, \mathrm{g}_t\,\}$ of an ideal is Groebner iff $\bar{S}^{\,G}\big(\,\mathrm{g}_i\,,\ \mathrm{g}_j\big) = 0$ for $i < j$.

Construction of Groebner Basis

Algorithm (2.1) (Buchberger)

Let $B\ =\ \{f_1, \ldots, f_m\} \subseteq F[x_1, \ldots, x_n]$.

Step 1: Compute $\bar{S}(f_i, f_j)^B$ for all $i < j$.

Step 2: Add non-zero result of step 1 to B until step 1 terminates (gives only zero).

Lemma (2.1)

Let G be a Groebner basis for an ideal I of $[\,x_1\,, \ldots\,, x_n\,]$.

If g $\in$ G such that $LT(g) \in \langle LT(G-\{g\})\rangle$, then $G-\{g\}$ is also a Groebner basis for$I$.

Minimal Groebner Basis

Definition

A Groebner basis G for an ideal I in $F[x_1, \ldots, x_n]$ is called **minimal** if

i. $LC(g) = 1$ For any g $\in$ G .

ii. $LT(g) \notin \langle LT(G-\{g\})\rangle$ For any g $\in$ G .

A minimal Groebner basis can be obtained from the Groebner basis by applying the previous lemma (2.1) to remove any g with

$LT(g) \in \langle LT(G-\{g\})\rangle$ and by adjusting constants to make leading coefficient 1. Note that minimal Groebner basis is not unique.

Reduced Groebner Basis

Definition

A Groebner basis G for an ideal I in $F[x_1, \ldots, x_n]$ is called **reduced** if

i. $LC(g) = 1$ for any g $\in$ G.

ii. No monomial of g is in $\langle LT(G-\{g\})\rangle$.

Theorem (2.4) [1]

Any ideal in $F[x_1, \ldots, x_n]$ has a unique reduced Groebner basis for a given monomial ordering.

Construction of the reduced Groebner basis :

Let $G = \{g_1, \dots, g_t\}$ be a Groebner basis for an ideal.

Replace each g_i by it remainder on division by

$g_1, \dots, g_{i-1}, \dots, g_{i+1}, \dots, g_t$. Neglect zero remainders.

Adjust the leading coefficient for those left to be 1.

Example

```
> # To Compute Groebner Bases for some ideals,
    also to find remainders.
> restart;
> with(Groebner) :
> ideal := [3·x + 4·y − 5·z + w, x + 3·y + 2·z
     − 2·w, 2·x − 5·y + 7·z + 3·w];
```

$$ideal := [3\,x + 4\,y - 5\,z + w,\ x + 3\,y + 2\,z - 2\,w,\ 2\,x - 5\,y + 7\,z + 3\,w]$$

```
> G := Basis(ideal, plex(x, y, z, w));
```

$$G := [68\,z - 21\,w,\ 68\,y - 49\,w,\ 68\,x + 53\,w]$$

```
> ideal1 := [x·z − y^2, x^3 − z^2];
```

$$ideal1 := [x\,z - y^2,\ x^3 - z^2]$$

```
> G1 := Basis(ideal1, plex(x, y, z));
```

$$G1 := [y^6 - z^5,\ x\,z - y^2,\ y^4\,x - z^4,\ y^2\,x^2 - z^3,\ x^3 - z^2]$$

```
> G2 := Basis(ideal1, grlex(x, y, z));
```

$$G2 := [x\,z - y^2,\ x^3 - z^2,\ y^2\,x^2 - z^3,\ y^4\,x - z^4,\ y^6 - z^5]$$

```
> G3 := Basis(ideal1, tdeg(x, y, z));
```

$$G3 := [y^2 - x\,z,\ x^3 - z^2]$$

```
> f := 2·x^4·y^2·z + 3·x^3·y·z^2 + x·y·z;
```

$$f := 2\,x^4\,y^2\,z + 3\,x^3\,y\,z^2 + x\,y\,z$$

```
> NormalForm(f, G1, plex(x, y, z));
```

$$y^3 + 2\,y^4\,z^2 + 3\,y\,z^4$$

```
> NormalForm(f, G2, grlex(x, y, z));
```

$$y^3 + 2\,y^4\,z^2 + 3\,y\,z^4$$

```
> NormalForm(f, G3, tdeg(x, y, z));
```

$$3\,y\,z^4 + 2\,x^2\,z^4 + x\,y\,z$$

>

>

> $ideal2 := [x^5 + y^3 + z^2 - 1, x^2 + y^2 + z - 1, x^6 + y^5 + z^3 - 1];$

$$ideal2 := [x^5 + y^3 + z^2 - 1, x^2 + y^2 + z - 1, x^6 + y^5 + z^3 - 1]$$

> $G4 := Basis(ideal2, plex(z, y, x));$

$$\begin{aligned}
G4 := [&225 x^4 - 1946 x^{10} - 1983 x^{11} - 10 x^{12} + 1225 x^{13} + 697 x^{14} + 195 x^{15} + 226 x^{16} - x^{18} \\
&+ 139 x^{17} - 13 x^{19} + 3 x^{20} + x^{22} + 2 x^{21} + 315 x^7 + 100 x^8 - 555 x^9 + 675 x^5 + 705 x^6, \\
&4794799513743465 x^4 - 28161279400718496 x^{10} - 13641002940967260 x^{11} \\
&+ 13303041747347884 x^{12} + 12841472514397999 x^{13} + 1936021990228677 x^{14} \\
&+ 2115618449641410 x^{15} + 2686197967416241 x^{16} - 308399336177560 x^{18} \\
&+ 266417434391307 x^{17} + 40028515719740 x^{19} + 22083510506531 x^{20} \\
&+ 20898699599882 x^{21} + 307985585745030 y x^5 - 307985585745030 y x^4 \\
&+ 1305539383606500 x^7 + 426289252230518 x^8 - 12718603398056543 x^9 \\
&+ 9461645755921935 x^5 + 5609230341167770 x^6, -130427012317955273 x^{10} \\
&+ 96308769549551000 x^{11} + 112430217894147542 x^{12} - 28978302929820573 x^{13} \\
&- 8147851966720744 x^{14} + 23240432665880855 x^{15} - 2547153248711687 x^{16} \\
&+ 1957860431279775 x^{18} - 6558796078633904 x^{17} - 154503618530810 x^{19} \\
&+ 226403721396233 x^{20} - 92968302338769 x^{21} + 9239567572350900 x^3 y^2 \\
&- 9239567572350900 y^2 x^2 + 8461551779562300 x^7 - 7477091544441736 x^8 \\
&- 133100833227195819 x^9 + 40874650161525720 x^5 - 3971051857805515 x^6 \\
&- 9239567572350900 x^3 y + 37955678888811405 x^4 + 9239567572350900 y x^2, \\
&-92395675723509000 x^2 - 92395675723509000 y^2 + 267932368916755545 x^4 \\
&+ 92395675723509000 y^2 x^2 - 1553067597584776499 x^{10} - 1058691906621826800 x^{11} \\
&+ 691613184599027638 x^{12} + 932606563955672291 x^{13} + 151389390751950794 x^{14} \\
&+ 95707520810719369 x^{15} + 185431646079855213 x^{16} - 24246152848015907 x^{18} \\
&+ 30397871204445410 x^{17} + 2994483268700962 x^{19} + 1053727522296225 x^{20} \\
&+ 1579303619755253 x^{21} - 321157390519106 20 x^7 - 858543129560584 x^8 \\
&- 533880675743739115 x^9 + 607600416419937750 x^5 + 326949813554222075 x^6 \\
&+ 92395675723509000 y^3, x^2 + y^2 + z - 1]
\end{aligned}$$

Applications

Ideal Membership

If f is a polynomial and I is an ideal, then we can determine if $f \in I$ by finding a Groebner basis G for I, such that $f \in I$ if and only if

remainder $(f) = 0$.

Example

```
> # To determine if f  is in ideal
> restart;
> with(Groebner) :
>
> ideal := [xz - y, xy + 2 z^2, y - z];
```

$$ideal := [xz - y, xy + 2\,z^2, y - z]$$

```
> f := x^3z - 2 y^2;
```

$$f := x^3\,z - 2\,y^2$$

```
> G := Basis(ideal, plex(x, y, z));
```

$$G := [1]$$

```
> NormalForm(f, G, plex(x, y, z));
```

$$0$$

```
>         # Thus f is  in ideal
>
> restart;
> with(Groebner) :
> ideal := [-x^3 + y, x^2y - z];
```

$$ideal := [-x^3 + y, x^2\,y - z]$$

```
> G := Basis(ideal, plex(x, y, z));
```

$$G := [y^5 - z^3, -y^2 + z\,x, y^3\,x - z^2, x^2\,y - z, x^3 - y]$$

```
> f := xy^3 - z^2 + y^5 - z^3;
```

$$f := xy^3 - z^2 + y^5 - z^3$$

```
> NormalForm(f, G, plex(x, y, z));
```

$$xy^3 - z^2$$

```
>         # Thus f is not in ideal
```

<u>Equality of two ideals</u>

Theorem (2.5) [1]

Let $I = \langle f_1, \dots, f_s\rangle$ and $J = \langle g_1, \dots, g_t\rangle$ be two ideals in $F\,[x_1, \dots, x_n]$. Then $I = J$ iff the reduced Groebner Bases of I and J are the same.

Example

```
> # Equality of two ideals
> restart;
> with(Groebner) :
```

> $ideal1 := [3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w];$

$$ideal1 := [3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w]$$

> $G1 := Basis(ideal1, plex(x, y, z, w));$

$$G1 := [3w + z, x - 2y + 2w]$$

>

> $ideal2 := [5x - 10y - 2z + 4w, 4x - 8y - 3z - w, 3x - 6y - z + 3w];$

$$ideal2 := [5x - 10y - 2z + 4w, 4x - 8y - 3z - w, 3x - 6y - z + 3w]$$

> $G2 := Basis(ideal2, plex(x, y, z, w));$

$$G2 := [z + 3w, x - 2y + 2w]$$

>

 # Thus idea1=ideal2

Elimination theory

Elimination theory gives away to solve system of polynomial equation by eliminating some of variables from some equations, and then back – solving.

Theorem (2.6)

The system has a solution, if the reduced Groebner basis $\neq \{1\}$.

Example

We will solve the system of equations

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

Then we can consider the ideal

$$I = \langle\, x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \,\rangle$$

A Groebner basis for I with respect to Lex order is giving by the four polynomials

$$g_1 = x + y + z^2 - 1$$

$$g_2 = y^2 - y - z^2 + z$$

$$g_3 = 2yz^2 - z^4 + z^2$$

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2$$

$$= z^2(z-1)(z^2+2z-1)$$

This system of equations has 5 solutions

(1, 0 , 0) , (0 , 1 , 0) , (0 , 0 , 1) ,

$$(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), \left(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}\right)$$

In solving this system of equations, the process can be divided into parts. First we eliminate variables, called the Elimination step ,and then we extend our solutions by back – solving , called the Extension step.

We study the Elimination step.

Note that observing that g_4 is only in terms of z can also be stated as $g_4 \in I \cap \mathbb{C}[z]$.

Generalizing this leads to a definition.

Definition

Let $I = \langle f_1, f_2, ,, f_n \rangle \subset K[x_1, x_2, ,, x_n]$. The L.th elimination ideal I_L is the ideal of $K[x_{L+1}, ,,, x_n]$ defined by

$I_L = I \cap K[x_{L+1},,,, x_n]$.

Theorem (2.7) (The Elimination Theorem)

Let I be an ideal and G a Groebner basis with respect to Lex order $x_1 > x_2 > . . . > x_n$. Then for any $0 \leq L \leq n$, the set

$$G_L = G \cap K[x_{L+1},,,, x_n]$$

Is a Groebner basis of the L.th elimination ideal I_L .

Example

$$I = \langle x^2 + y + z - 1 , x + y^2 + z - 1 , x + y + z^2 - 1 \rangle$$

A Groebner basis is given

$$g_1 = x + y + z^2 - 1$$

$$g_2 = y^2 - y - z^2 + z$$

$$g_3 = 2yz^2 - z^4 + z^2$$

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2$$

It follows from elimination theorem that

$I_1 = I \cap \mathbb{C}[y, z]$

$= \langle y^2 - y - z^2 + z, 2yz^2 - z^4 + z^2, z^6 - 4z^4 + 4z^3 - z^2 \rangle$

$I_2 = I \cap \mathbb{C}[z] = \langle z^6 - 4z^4 + 4z^3 - z^2 \rangle$

Example

```
> # To compute Groebnen basis for I
> restart;
> with(Groebner):
```

> $ideal := [x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1];$

$$ideal := [x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1]$$

> $G := Basis(ideal, plex(x, y, z));$

$$G := [-z^2 - 4z^4 + 4z^3 + z^6, -z^2 + z^4 + 2z^2 y, -z^2 - y + z + y^2, x + y + z^2 - 1]$$

Chapter three

Operations on Ideals

Operations on ideals in $F[\, x_1 , \dots , x_n \,]$ are studied conceptually and computationally. This operations includes radical , intersections, sums , products and quotients.

Radical ideals

Definition

Let $I \subset F[\, x_1 , \dots , x_n \,]$ be an ideal. The radical of I , dented $\sqrt{I}$, is the set $\{ f : f^m \epsilon I$ for some integer $m \geq 1 \}$.

Theorem (3.1) (radical membership)

Let F be an arbitrary field and let $I = \langle f_1 , \dots , f_s \rangle \subset F[\, x_1 , \dots , x_n \,]$ be an ideal.

Then $f \in \sqrt{I}$ if an only if the constant polynomial 1 belongs to the ideal

$$\tilde{I} \equiv \langle f_1 , \dots , f_s , 1 - yf \rangle \subset F[\, x_1 , \dots , x_n , y \,].$$

Proof

Suppose $1 \in \tilde{I}$. Then we can write as:

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

For some $p_i , q \in F[\, x_1 , \dots , x_n , y \,]$.

We set $= 1/f(x_1 , \dots , x_n),$ then our expression becomes

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

Now we multiply both sides by f^m :

$f^m = \sum_{i=1}^{s} A_i \, f_i$, for some polynomials $A_i \in F[x_1, \dots, x_n]$.

Therefore , $f^m \in I$ and so $f \in \sqrt{I}$.

Gong the other way, suppose that $f \in \sqrt{I}$ then $f^m \in I \subset \tilde{I}$, for some m.

At the same time , $1 - yf \in \tilde{I}$. Then

$$1 = y^m f^m + (1 - y^m f^m)$$

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

Hence , $f \in \sqrt{I}$ implies that $1 \in \tilde{I}$.

Algorithm (3.1)

To determine if $f \in \sqrt{\langle f_1, \dots, f_s \rangle} \subset F[x_1, \dots, x_n]$.

1 - We first compute a reduced Groebner basis for:

$$\langle f_1, \dots, f_s, 1 - yf \rangle \subset F[x_1, \dots, x_n, y] .$$

2- If the result is $\{1\}$, then $f \in \sqrt{I}$. Otherwise , $f \notin \sqrt{I}$.

Example

> *# To determine if* $f = y\text{-}x^2 + 1$ *is* **in** $\sqrt{\langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle}$

> *restart*;

> *with*(*Groebner*) :

> $f := [xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 \text{ -} zy - x^2 z + z]$;

$$f := [xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - zy - x^2 z + z]$$

> $G := Basis(f, plex(x, y, z))$;

$$G := [1]$$

> # Thus f=y-x^2+1 is in $\sqrt{\langle xy^2+2y^2, x^4-2x^2+1\rangle}$

>

> # To determine if f=x^2+y^2 is **not** in $\sqrt{\langle xy^2+2y^2, x^4-2x^2+1\rangle}$

>

> *restart*;

> *with*(*Groebner*) :

> $f := [xy^2+2y^2, x^4-2x^2+1, 1-x^2z+y^2z]$;

$$f := [xy^2+2y^2, x^4-2x^2+1, 1-x^2z+y^2z]$$

> $G := Basis(f, plex(x, y, z))$;

$$G := [4+(-4xy^2-8)z+(4+xy^4+4xy^2)z^2, xy^2+2y^2, -2xy^2-8+(4+xy^4+4xy^2)z+4x^2]$$

>

> # Thus f=x^2+y^2 is **not** in $\sqrt{\langle xy^2+2y, x-2x+1\rangle}$

Theorem (3.2)

Let $f \in F[x_1, \ldots, x_n]$ and $I = \langle f \rangle$ be the principle ideal generated by f. If $f = cf_1^{a1} \ldots f_r^{ar}$ is the factorization of f into a product of distinct irreducible polynomials, then $\sqrt{I} = \sqrt{\langle f \rangle} = \langle f_1 f_2 \ldots f_r\rangle$.

Definition

If $f \in F[x_1, \dots, x_n]$ is a polynomial ,we define **the reduction** of f, denoted f_{red} , to be the polynomial such that $\langle f_{red} \rangle = \sqrt{\langle f \rangle}$

A polynomial is said to be reduced (or square – free) if $f = f_{red}$.

Theorem (3.3)

Let F be a field containing the rational numbers $\mathbb{Q}$ and $I = \langle f \rangle$ be a principle ideal in $F[x_1, \dots, x_n]$ .Then $\sqrt{I} = \langle f_{red} \rangle$,where

$$f_{red} = \frac{f}{GCD\left(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \dots, \frac{\partial f}{\partial x_n}\right)}$$

Proof

Suppose $\sqrt{I} = \langle f_1 f_2 \dots f_r \rangle$ .Thus, it suffices to show that

$$GCD\left(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \dots, \frac{\partial f}{\partial x_n}\right) = f_1^{a_1-1} f_2^{a_2-1} \dots f_r^{a_r-1} .$$

We first use the product rule to not that

$$\frac{\partial f}{\partial x_j} = f_1^{a_1-1} f_2^{a_2-1} \dots f_r^{a_r-1} \left(a_1 \frac{\partial f}{\partial x_j} f_2 \dots f_r + \dots + a_r f_1 f_2 \dots \frac{\partial f_r}{\partial x_j}\right) .$$

This proves that $f_1^{a_1-1} f_2^{a_2-1} \dots f_r^{a_r-1}$ divides the GCD.

If remains to show that for each i, there is some $\frac{\partial f}{\partial x_j}$ which is not divisible by $f_i^{a_i}$ .Write $f = f_i^{a_i} h$,where h_i is not divisible by f_i .

Since f_i is non constant ,some variable x_j must appear in f_i .

The product rule gives us $\frac{\partial f}{\partial x_j} = f_i^{a_i-1} \left(a_1 \frac{\partial f}{\partial x_j} h_i + f_i \frac{\partial h_i}{\partial x_j} \right)$.

If this expression is divisible by$f_i^{a_i}$, then $\frac{\partial f_i}{\partial x_j}$ h_i must be divisible f_i .

Since f_i is irreducible and does not divide h_i , this force f_i to divide $\frac{\partial f_i}{\partial x_j}$.

Example

> *# To compute* $< f_{red} >$

> $restart;$

> $f := x^5 + 3x^4y + 3x^3y^2 - 2x^4y^2 + x^2y^3 + 6x^3y^3 - 6x^2y^4 + x^3y^4 - 2xy^5 + 3x^2y^5 + 3xy^6 + y^7;$

$$f := x^5 + 3x^4y + 3x^3y^2 - 2x^4y^2 + x^2y^3 + 6x^3y^3 - 6x^2y^4 + x^3y^4 - 2xy^5 + 3x^2y^5 + 3xy^6 + y^7$$

> $a := \frac{\partial}{\partial x} f;$

$$a := 5x^4 + 12x^3y + 9x^2y^2 - 8x^3y^2 + 2xy^3 + 18x^2y^3 - 12xy^4 + 3x^2y^4 + 6xy^5$$

> $b := \frac{\partial}{\partial y} f;$

$$b := 3x^4 + 6x^3y - 4x^4y + 3x^2y^2 + 18x^3y^2 - 24x^2y^3 + 4x^3y^3 + 15x^2y^4 + 7y^6$$

> $gcd(a, b);$

$$1$$

> $gcd(gcd(a, b), f);$

$$1$$

> $\langle f_{red} \rangle := \frac{f}{(gcd(gcd(a, b), f)};$

$$\langle (x^5 + 3x^4 y + 3x^3 y^2 - 2x^4 y^2 + x^2 y^3 + 6x^3 y^3 - 6x^2 y^4 + x^3 y^4 - 2xy^5 + 3x^2 y^5 + 3xy^6 + y^7)_{rad} \rangle := x^5 + 3x^4 y + 3x^3 y^2 - 2x^4 y^2 + x^2 y^3 + 6x^3 y^3 - 6x^2 y^4 + x^3 y^4 - 2xy^5 + 3x^2 y^5 + 3xy^6 + y^7$$

Intersections of Ideals

Definition

The intersection $I \cap J$ of two ideals I and J in $F[\,x_1 , \dots , x_n\,]$ is the set of all polynomials which belong to both I and J.

Lemma (3.1)

i. If I is generated as an ideal in $F[\,x_1 , \dots , x_n\,]$ by $p_1(x) , \dots , p_r(x)$ then $f\,(t)\,I$ is generated as an ideal in $F[\,x_1 , \dots , x_n, t\,]$ by $f\,(t).p_1(x) , \dots , f\,(t)\,.p_r(x)$.

ii. If g $(\,x , t\,) \in f\,(t)\,I$ and a is any element of the field, then g$(\,x , a\,) \in I$.

Theorem (3.4)

Let I , J be ideals in $F\,[\,x_1 , \dots , x_n\,]$. Then

$$I \cap J = (\,tI + (\,1 - t)\,J\,) \cap F[\,x_1 , \dots , x_n\,] .$$

Proof

Note that $(tI + (\,1 - t)\,J)$ is an ideal in $F\,[\,x_1 , \dots , x_n, t\,]$.

To establish the desired equality, we use the usual strategy of proving containment both directions.

Suppose $f \in I \cap J$. Since $f \in I$, we have $t.f \in t\,I$, similarly, $f \in J$ implies $(1-t)\,f \in (1-t)\,J$. Thus,

$f = t.f + (1-t)\,.\ f \in t\,I + (1-t)\,J$. Since

$I, J \subset F[x_1, \dots, x_n]$

We have $\in (t\,I + (1-t)\,J) \cap F[x_1, \dots, x_n]$.

This shows that $I \cap J \subset (t\,I + (1-t)\,J) \cap F[x_1, \dots, x_n]$.

To establish containment in the opposite direction, suppose $f \in (t\,I + (1-t)\,J) \cap F[x_1, \dots, x_n]$.

Then $f(x) = \mathrm{g}(x, t) + h(x, t)$, where $\mathrm{g}(x, t) \in t\,I$ and $h(x, t) \in (1-t)J$.

First set $= 0$. Since every element of $t\,I$ is, multiple of t, we have $\mathrm{g}(x, o) = 0$. Thus $f(x) = h(x, o)$ and hence $f(x) \in J$ by lemma(3.1).

On the other hand, set $t = 1$ in the relation:

$f(x) = \mathrm{g}(x, t) + h(x, t)$. Since every element of $(1-t)\,J$ is multiple of $1-t$ we have $h(x, 1) = 0$

Thus $f(x) = \mathrm{g}(x, 1)$ and ,hence $f(x) \in I$ by lemma(3.1).

Since f belongs to both I and J, we have $\in I \cap J$.

Thus, $I \cap J \supset (t\,I + (1-t)\,J) \cap F[x_1, \dots, x_n]$.

Algorithm (3.2)

To compute the intersection of two ideals.

If $I = \langle f_1, \dots, f_r \rangle and\, J = \langle \mathrm{g}_1, \dots, \mathrm{g}_s \rangle$ are ideals in $F[x_1, \dots, x_n]$, then:

1- $\langle f_1, \dots, f_r \rangle \cap \langle g_1, \dots, g_s \rangle =$

$$\langle tf_1, \dots, tf_r, (1-t) g_1, \dots, (1-t) g_s \rangle \subset F[x_1, \dots, x_n, t]$$

2- Compute a Groebner basis with respect to lexicographic order in which t is greater than the x_i .

3- The elimination of t can be done via the elimination property of Groebner basis , we have a Groebner basis of

$$(t I + (1-t) J) \cap F[x_1, \dots, x_n].$$

Thus $I \cap J = \langle tf_1, \dots, tf_r, (1-t) g_1, \dots, (1-t) g_s \rangle \cap F[x_1, \dots, x_n]$.

Example

> *# To compute intersection of ideals*

> *restart*;

> *with*(*PolynomialIdeals*) :

> *with*(*Operators*);

$$[\,`*`,\ `+`,\ Simplify,\ `\wedge`\,]$$

> $J1 := \langle x^2 y \rangle$;

$$J1 := \langle x^2 y \rangle$$

> $J2 := \langle x y^2 \rangle$;

$$J2 := \langle x y^2 \rangle$$

> $K := (t) J1 + (1-t) J2$;

$$K := \langle x^2 y^2, x^2 y t, -x y^2 + x y^2 t \rangle$$

> $EliminationIdeal(K, \{x, y\}) = Intersect(J1, J2)$;

$$\langle x^2 y^2 \rangle = \langle x^2 y^2 \rangle$$

> *# Thus* $J1 \cap J2 = \, < x^2 y^2 >$.

>

> *restart*;

>

> *with*(*PolynomialIdeals*) :

> $with(Operators);$

$$[\,`*`,\ `+`,\ Simplify,\ `\wedge`]$$

> $J1 := \langle x^2 - y^2 \rangle;$

$$J1 := \langle x^2 - y^2 \rangle$$

> $J2 := \langle x^3 - y^3 \rangle;$

$$J2 := \langle x^3 - y^3 \rangle$$

> $K := (t)J1 + (1-t)J2;$

$$K := \langle t\,x^2 - t\,y^2,\ x^4 + x^3\,y - x\,y^3 - y^4,\ t\,x\,y^2 - y^3\,t - x^3 + y^3 \rangle$$

>

> $EliminationIdeal(K, \{x, y\}) = Intersect(J1, J2);$

$$\langle x^4 + x^3\,y - x\,y^3 - y^4 \rangle = \langle x^4 + x^3\,y - x\,y^3 - y^4 \rangle$$

> # *Thus* $J1 \cap J2 = <x^4 + x^3y - xy^3 - y^4>$

>

> *# However there is a commmand which compute directely the intersection of two or more idaels.*

> $restart;$

> $with(PolynomialIdeals):$

> $J1 := \langle x^2 - y^2 \rangle;$

$$J1 := \langle x^2 - y^2 \rangle$$

> $J2 := \langle x^3 - y^3 \rangle;$

$$J2 := \langle x^3 - y^3 \rangle$$

> $I := Intersect(J1, J2);$

$$I := \langle x^4 + x^3\,y - x\,y^3 - y^4 \rangle$$

> # *Thus* $J1 \cap J2 := <x^4 + x^3y - xy^3 - y^4>$

> $restart;$

> $with(PolynomialIdeals):$

> $J1 := \langle x^2 - y \rangle;$

$$J1 := \langle x^2 - y \rangle$$

> $J2 := \langle x^3 - y^3 \rangle;$

$$J2 := \langle x^3 - y^3 \rangle$$

> $J3 := \langle x^4 - y^3 \rangle;$

$$J3 := \langle x^4 - y^3 \rangle$$

> $I := Intersect(J1, J2, J3);$

$$I := \langle y^4 x^4 + y^3 x^5 - y x^7 - x^8 - y^7 - y^6 x + y^4 x^3 + y^3 x^4 \rangle$$

>

> # Thus $J1 \cap J2 \cap J3 := <y^4x^4 + y^3x^5 - yx^7 - x^8 + y^7 - y^6x + y^4x^3 + y^3x^4>$

Sums of Ideals

Definition

If I and J are ideals of the ring $F[x_1, \ldots, x_n]$ then the sum of I and J, denoted $I + J$, is the set

$$I + J = \{ f + g : f \in I, g \in J \}.$$

If $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$ then $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$.

Example

> #To compute sums of ideals

> $restart;$

> $with(PolynomialIdeals):$

> $I1 := \langle x^3 - 1, y^2 - 3 \rangle;$

$$I1 := \langle x^3 - 1, y^2 - 3 \rangle$$

> $I2 := \langle x^2 - z \rangle;$

$$I2 := \langle x^2 - z \rangle$$

> $S := Add(I1, I2);$

$$S := \langle x^2 - z, x^3 - 1, y^2 - 3\rangle$$

Products of Ideals

Definition

If I and J are two ideals in $F[x_1, \ldots, x_n]$,then their product, denoted $I.J$, is defined to be ideal generated by all polynomials $f.g$ where $f \in I$ and $g \in J$. Thus,the product $I.J$ of I and J is the set

$I.J = \{f_1 g_1 + \ldots + f_r g_r : f_1, \ldots, f_r \in I, g_1, \ldots, g_r \in J, r$ is a positive integer$\}$.

Example

> *#To compute products of ideals*

> $restart;$

> $with(PolynomialIdeals):$

> $I1 := \langle x^3 - 1, y^2 - 3\rangle;$

$$I1 := \langle x^3 - 1, y^2 - 3\rangle$$

> $I2 := \langle x^2 - z\rangle;$

$$I2 := \langle x^2 - z\rangle$$

> $P := Multiply(I1, I2);$

$$P := \langle (x^3 - 1)(x^2 - z), (y^2 - 3)(x^2 - z)\rangle$$

Quotient of Ideals

Definition

If I and J are ideals in $F[x_1, \ldots, x_n]$ then,

$I : J$ Is the set $\{ f \in F[x_1, \dots, x_n] : fg \in I$ for all $g \in J \}$.

And is called the ideal quotient for I by J

Proposition

Let I, J and F be ideals in $K[x_1, \dots, x_n]$, then:

i. $I : K[x_1, \dots, x_n] = I$.

ii. $IJ \subset K$ if only if $I \subset K : J$.

iii. $J \subset I$ if and only if $I : J = F[x_1, \dots, x_n]$.

Proposition

Let I, I_i, J, J_i, and K be ideals in $F[x_1, \dots, x_n]$ for $1 \leq i \leq r$. Then

1- $(\bigcap_{i=1}^{r} I_i) : J = \bigcap_{i=1}^{r} (I_i : J)$.

2- $I : (\sum_{i=1}^{r} J_i) = \bigcap_{i=1}^{r} (I : J_i)$.

3- $(I : J) : K = I : JK$.

4- $I : \langle f_1, f_2, \dots, f_r \rangle = \bigcap_{i=1}^{r} (I : f_i)$.

Theorem (3.5)

Let I be an ideal and g an element of $F[x_1, \dots, x_n]$.

If $\{ h_1, \dots, h_p \}$ is a basis of the ideal $I \cap \langle g \rangle$, then

$\{ h_1/g, \dots, h_p/g \}$ is a basis of $I : \langle g \rangle$.

Proof

If $a \in \langle g \rangle$, then $a = bg$ for some polynomial b thus,
if $f \in \langle h_1/g, \dots, h_p/g \rangle$, then

$af = bgf \in \langle h_1, \dots, h_p \rangle = I \cap \langle g \rangle \subset I$. Thus, $\in I : \langle g \rangle$.

Conversely , suppose $\in I : \langle g \rangle$. then $fg \in I$. since $fg \in \langle g \rangle$.

We have $g \in I \cap \langle g \rangle$. If $I \cap \langle g \rangle = \langle h_1, \dots, h_p \rangle$, this means

$f g = \sum r_i h_i$ for some polynomials r_i .

Since each $h_i \in \langle g \rangle$, each h_i/g is polynomial ,and we conclude that
$f = \sum r_i \, (h_i/g)$,

Where $f \in \langle h_1/g , \dots , h_p/g \rangle$.

Algorithm (3.2)

To compute a basis of an ideal quotient.

If $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle = \langle g_1 \rangle + \dots + \langle g_s \rangle$ then

1- We compute a basis of $\langle f_1, \dots, f_r \rangle \cap \langle g_i \rangle$ for each.
2- Finding a Groebner basis of $\langle tf_1, \dots, tf_r , (1 - t) g_i \rangle$ with respect to lex order in which don't depend on$t$ (this is our algorithm for computing ideal intersections) .
3- Using the division algorithm , we divide each of these element by g_i to get a basis for $: \langle g_i \rangle$.
4- Finally we compute a basis for $I : J$ by applying the intersection algorithm $s - 1$ times .
5- Computing first a basis for $I : \langle g_1 , g_2 \rangle = (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle)$, then a 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 so on up to $I : J$

Example

To compute ideal quotient
Let $I = \langle x^2 - y^2 \rangle$, $J = \langle x^3 - y^3 \rangle$
Compute intersection by Maple

$K = tI + (1 - t)J$

$$= \langle x^4 + x^3y - xy^3 - y^4 \rangle$$

By using the division algorithm by $\mathrm{g_i}$ to get a bases for $I:\langle \mathrm{g}_i \rangle$

$$\begin{array}{r|l} x^3 - y^3 & x^4 + x^3y - xy^3 - y^4 \\ \hline x & x^4 \qquad\quad - xy^3 \\ & \overline{\qquad x^3y - y^4 \qquad} \end{array}$$

$$\begin{array}{r|l} x^3 - y^3 & x^3y - y^4 \\ \hline y & x^3y - y^4 \\ & \overline{\qquad 0 \qquad} \end{array}$$

$$I:\langle \mathrm{g}_i \rangle = \langle x + y \rangle$$

```
> # To  compute ideal quotient by maple
> restart;
> with(PolynomialIdeals) :
> I1 := ⟨x^2 − y^2⟩;
```

$$I1 := \langle x^2 - y^2 \rangle$$

```
> J1 := ⟨x^3 − y^3⟩;
```

$$J1 := \langle x^3 - y^3 \rangle$$

```
> Quotient(I1, J1);
```

$$\langle x + y \rangle$$

Appendix

Maple Program

Maple is computer algebra system which makes computations symbolically and numerically .It also makes graphs .It includes general commands and special packages for special subjects.

We introduce below the basic commands for doing computations in polynomials and Groebner Basis.

The version 13 of Maple is used in our computations.

```
> # The general commands used are :-
> # 1) gcd - greatest common divisor of
  polynomials
> # The gcd function computes the greatest common
  divisor of two polynomials
>
> # The packages used are:-
> 1) with(Groebner);
```

[*Basis*, *FGLM*, *HilbertDimension*, *HilbertPolynomial*, *HilbertSeries*, *Homogenize*, *InitialForm*, *InterReduce*, *IsProper*, *IsZeroDimensional*, *LeadingCoefficient*, *LeadingMonomial*, *LeadingTerm*, *MatrixOrder*, *MaximalIndependentSet*, *MonomialOrder*, *MultiplicationMatrix* , *MultivariateCyclicVector* , *NormalForm*, *NormalSet*, *RationalUnivariateRepresentation* , *Reduce*, *RememberBasis*, *SPolynomial*, *Solve*, *SuggestVariableOrder*, *TestOrder*, *ToricIdealBasis*, *TrailingTerm*, *UnivariatePolynomial*, *Walk*, *WeightedDegree*]

```
> # i ) Basis - compute a Groebner basis
```

> # *ii*) ***LeadingCoefficient***
- compute the leading coefficient of a polynomial

> # *iii*) ***LeadingMonomial***
- compute the leading monomial of a polynomial

> # *iv*) ***LeadingTerm***
- compute the leading term of a polynomial

> # *v*) ***NormalForm***
*-compute the remainder of a multivariate polynomial **f** divided* **by** *a list of multivariate polynomial **G***

> # *vi*) ***SPolynomial***
*-compute an spolynomial of **f*** **and** ***g** with respect* **to** *monomial order **T***

> # *vii*) ***TestOrder*** *- compar monomials* **in** *a monomial order*

>

>

> 2) *with*(*PolynomialIdeals*);

$$[<,>, Add, Contract, EliminationIdeal, EquidimensionalDecomposition, Generators, HilbertDimension, IdealContainment, IdealInfo, IdealMembership, Intersect, IsMaximal, IsPrimary, IsPrime, IsProper, IsRadical, IsZeroDimensional, MaximalIndependentSet, Multiply, NumberOfSolutions, Operators, PolynomialIdeal, PrimaryDecomposition, PrimeDecomposition, Quotient, Radical, RadicalMembership, Saturate, Simplify, UnivariatePolynomial, VanishingIdeal, ZeroDimensionalDecomposition, in, subset]$$

> # *i*) ***Add*** *-compute the sum of ideals*

> # *ii*) ***EliminationIdeal*** *-eliminates variables* **from** *an ideal using a Grobner basis computation*

> # *iii*) ***Intersect***
- compute the intersection of two **or** *more polynomial ideals*

> # *iv*) ***Multiply*** – *compute the product of ideals*
> # *v*) ***Operators*** (***subpackage***)
– *binary operators* **for** *ideals*

> # *vi*) ***Quotient***
– *compute the quotient of two ideals*

> # *vii*) ***Radical*** – *compute the radical of an ideal*

References

[1] C. David Cox. John Little, Donal O'shea, Ideals, Varieties, And Algorithms. Third edition (2007).

[2] D .Davids. Dummit, Richard M. Foote Abstract Algebra, Third edition (2004)

[3] D. Jhon R. Durbin , Modern Algebra, An introduction (fifth Edition 2005)

[4] E. Vivana Ene, Jurgen Herzog , Groebner Bases in Cmmutative Algebra (2012)

[5] E . Florian Enescu , Polynomial Rings, Groebner Bases

Georgia state university

[6] G. Joseph A.Gallian , Contemporary Abstract Algebra (1990)

[7] G. William J. Gilbert , W. Keith Nicholson , Modern Algebra with applications, (second edition (2003))

[8] G. Shuhong Goo, A new Algorithm for computing Groebner Bases (September 2011)

[9] K. Richard E.Kakima, Neit Sigmon, Ernest Stitzilger, Applications of Abstract Algebra with Maple (1999)

[10] L. Nids Lauritzen, Concrete Abstract Algebra , From Number to Groebner Bases., Gth Printing (2011)

[11] L. Mathin leslies , Math 53GA paper: Groebner Bases. Math Arizona. Edu/N Meslies/ flues/ Groebner Bases. Pdf (1 December 15.2008)

[12] M. Katlyn moran, Groebner Bases and their Applications

Math. Berkeley. Edu/N a borer/ laithyn .. pdf , (july 30 , 2008)

[13] S. Karlheinz Spindler , Abstract Algebra with Applications into Volumes.Volume II Rings and field (1994)

[14] W. Jhon J. Watkins,Topics in commutative ring theory (2007)

ملخص باللغة العربية

العمليات على المثاليات باستخدام المابل

في هذه الأطروحة تم دراسة العمليات على المثاليات لكثيرات الحدود في أكثر من عنصر عن طريق قاعدة Groebner Basis باستخدام برنامج Maple 13 في حساب هذه العمليات وبعض تطبيقات Groebner Basis وهي العضوية المثالية والتساوي للمثاليات ونظرية إزالة الحلول للأنظمة اللاخطية للمعادلات لكثيرات الحدود في أكثر من عنصر.

تحتوي الاطروحة على أربعة فصول كالتالي:

الفصل صفر يصف البنية الجبرية للحلقات والمثاليات حسب الضرورة.

الفصل الأول تم دراسة كثيرات الحدود في أكثر من عنصر.

الفصل الثاني تم دراسة قاعدة Groebner Basis للحسابات والتطبيقات.

الفصل الثالث تم دراسة العمليات على المثاليات وملحق حول البرنامج (Maple13)

وفي نهاية الأطروحة وضعت قائمة بالمصادر المستخدمة.