ALGORITHMS IN REAL ALGEBRAIC GEOMETRY

ALAATTİN AKYAR

FEBRUARY 2011

ALGORITHMS IN REAL ALGEBRAIC GEOMETRY

by
ALAATTİN AKYAR

THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
THE ABANT İZZET BAYSAL UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE
OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF MATHEMATICS

FEBRUARY 2011

Approval of the Graduate School of Natural and Applied Sciences.

Prof. Dr. Nihat ÇELEBİ
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Harun KARSLI
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Ali ÖZTÜRK
Supervisor

Examining Committee Members

Assoc. Prof. Dr.Soner DURMUŞ ---------------------------

Assistant Prof. Dr.Erol YILMAZ ---------------------------

Assistant Prof. Dr.Ali ÖZTÜRK ---------------------------

ABSTRACT

ALGORITHMS IN REAL ALGEBRAIC GEOMETRY

Akyar, Alaattin
M.Sc. Department of Mathematics
Supervisor: Assist. Prof. Dr. Ali Öztürk
February 2011, 104 Page.

In this work, properties of Gröbner bases and Homogeneous bases are given. In this context, we give explicit calculations for solving polynomial equation and try to decide which thechnique is the most efficient one.

Keywords: Polynomials ideals, Multivariate polynomials, Gröbner bases, Homogeneous bases, systems of polynomial equations.

ÖZET

REEL CEBİRSEL GEOMETRİDE ALGORİTMALAR

Akyar, Alaattin
Master, Matematik Bölümü
Yönetici: Yrd. Doç. Dr. Ali Öztürk
February 2011, 104 Sayfa.

Bu çalışmada Gröbner tabanlarının ve Homogeneous tabanlarının özellikleri verilmiştir. Bu bağlamda, polinom denklem sistemlerini çözmek için farklı yöntemler verdik ve hangi tekniğin daha etkili olduğuna karar vermeye çalıştık.

Anahtar Kelimeler: Polinom idealleri, Çok değişkenli polinomlar, Gröbner tabanları, Homogeneous tabanları, Polinon denklem sistemler.

ACKNOWLEDGEMENTS

I would like to acknowledge my indebtedness to my supervisor Assistant. Prof. Dr. Ali Öztürk who has guided, encouraged and believed in me throughout this thesis. I am grateful to him for a critical reading of my studies and valuable suggestions in correcting my errors. I would also like to thank to the other members of my Committee, Assoc. Prof. Dr. Soner Durmuş And Assistant. Prof. Dr. Erol Yılmaz for their assistance.

It is also a pleasure to acknowledge a special dept of my gratitude to all the professors who gave me help in my master studies.

Finally, I would like to thank to my family for their un-vanishing support and encouragement.

TABLE OF CONTENTS

CHAPTER 1

INRODUCTION

1.1 Introduction

A polynomial equation corresponds to a polynomial function $f(x)$ which is set to zero. It is so called a zero function which means that $f(x)=0$ for all $x \in k$, k is any infinite field. The solutions to the equation are called the roots of the polynomial and they are the zeros of the function. If $x=a$ is a root of a polynomial, then $(x-a)$ is a factor of that polynomial, which gives the zero function on the affine space k.

Solving a polynomial equation in one variable is easily done on computer by some well known root-finding algorithms. Formulas for the roots of polynomials up to a degree of 2 have been known since ancient times and up to a degree of 4 since the 16^{th} century. But formulas for degree 5 eluded researchers. In 1824, Niels Henrik Abel proved that there is no general formula for the roots of a polynomial of degree 5 or greater in terms of its coefficients.

A system of polynomial equations is a set of n polynomials with coefficients over an arbitrary field. Solving systems of polynomial equations is a fundamental problem in geometric computations. In particular, it is a crucial or most challenging problem in algorithmic algebra and the computational complexity makes it very difficult to solve for some problems in practice. In 1981, Yun and Pohst study the difficulties in computational methods for ideal bases which is useful for solving a system of polynomial equations. However, the problems of finding the common zeros of polynomial equations are far from satisfactorily solved. The investigations also reveal that polynomial systems often result in large number of solutions [1].

The theory on systems of multivariate polynomial equations also involves field and ideal theory. The search for efficient algorithms for solving systems of polynomial equations has received renewed attention due to their importance to a variety of problems of both practical and theoretical interests. The need to count real solutions or to find exact or approximate solutions to such systems has arisen in a wide range of practical areas, including robotics and kinematics, computational number theory, solid modeling, quantifier elimination and geometric reasoning problems.

The currently known techniques for solving polynomial systems can be classified into symbolic, numeric and geometric. In the context of finding exact solutions, symbolic method based on Gröbner bases and resultants originate from algebraic geometry and can be used for eliminating variables, which reduces the problem to finding roots of univariate polynomials. However, if the reduced equation is of degree 5 or more, there are no radical formulas that can solve the equation. In such cases, combining the techniques of Gröbner bases with other numerical techniques, elimination ideal and extension theorem may be desirable.

New methods for Gröbner bases conversion such as the well known FGLM algorithm [2] and the Grobner Walk algorithm [2] can be applied to address the question of an efficient elimination methods using a suitable order by using basis conversion. While the main ideas of the Gröbner Walk is simple, the actual implementation of the algorithm is less understood.

Later improvement of Buchberger algorithm is the F_4 algorithm which was first described in [3] and is claimed to be the fastest routines for computing Gröbner bases in current implementation by Farr and Pearce in 2005 [4]. The routines have been tested under Magma and the time results are presented on Steel's web page [5].

Algebraic geometry relates to the study of geometric objects defined by polynomial equations using algebraic tools and is also called a symbolic method. In general, the basic problem of algebraic geometry is to study the set of points in k^n satisfying a system of equations $f_1(x_1,...,x_n)=0,...,f_m(x_1,...,x_n)=0$ where k is a field and $f_1,...,f_m$ belongs to the polynomial ring $k[x_1,...,x_n]$.The solution set of $f_1=...=f_m=0$ is called the algebraic set, referred also as algebraic or affine variety of $f_1,...,f_m$ and is denoted as $V=V(f_1,...,f_m)$.The geometry of interest is the affine varieties of curves and surfaces defined by polynomial equations. In finding effective solutions of the affine varieties, the relation between algebra and geometry can be investigated by considering the algebraic and geometric objects such as fields, ideals, affine varieties and propositions, theorems or corollaries involving them.

This work consists of three Chapters. In Chapter 2, we will give some basic concept and definitions. In Chapter 3, we do the computations for solving polynomial equation by using Gröbner bases and Homogeneous bases.

CHAPTER 2

PRELIMINARY CONCEPTS AND DEFINITIONS

In this chapter we give a number of definitions and theorems used in subsequent parts of the thesis. More detail information can be found in [6], [7] and [8].

2.1 Polynomials and Ideals

Let $k[x_1,...,x_n]$ be the ring of the polynomials over a field.

Definition 2.1 A monomial in a collection of variables $x_1,...,x_n$ is a product of the form $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot ... \cdot x_n^{\alpha_n}$, where the α_i are non-negative integers. The total degree of this monomial is the sum $\alpha_1 + \alpha_2 + ... + \alpha_n$.

For brevity, let $x = (x_1,...,x_n)$ and $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$. Then the monomial can be written as x^α. We also let $|\alpha| = \alpha_1 + \alpha_2 + ... + \alpha_n$ denote the total degree of monomial x^α.

For example; let $x^\alpha = x_1^3 \cdot x_2^2 \cdot x_4$. Then $|\alpha| = 3 + 2 + 0 + 1 = 6$ since $\alpha = (3,2,0,1)$.

Definition 2.2 A polynomial f is a finite linear combination of monomials with coefficients in a field k. A polynomial f will be written in the form $f = \sum_\alpha c_\alpha x^\alpha$,

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $c_\alpha \in k - \{0\}$. The total degree of f, denoted $\deg(f)$, is the maximum $|\alpha| = \alpha_1 + \alpha_2 + ... + \alpha_n$ in the expression of f. For example; taking k to be the filed $\mathbb{Q}$ of rational numbers, and denoting the variables by x, y, z. Then, $f = x^2 + 2y^3z + xz - z + 1$ is a polynomial containing five terms and $\deg(f) = 0 + 3 + 1 = 4$.

In our examples, the field of coefficients will be either the field of rational numbers $\mathbb{Q}$, the field of real numbers $\mathbb{R}$, or the field of complex numbers $\mathbb{C}$. Polynomials in $k[x_1,...,x_n]$ can be added and multiplied, so $k[x_1,...,x_n]$ has the structure of a commutative ring (with identity).

However, only nonzero constant polynomials have multiplicative inverses in $k[x_1,...,x_n]$, so $k[x_1,...,x_n]$ is not a field, but the set of rational functions $\{f|g : f,g \in k[x_1,...,x_n], g \neq 0\}$ is a field, denote by $k(x_1,...,x_n)$.

Given a collection of polynomials, $f_1,...,f_s \in k[x_1,...,x_n]$, we can consider all polynomials which can be written as a linear combination of these polynomials.

Definition 2.3 Let $I \subset k[x_1,...,x_n]$ be a nonempty subset. I is said to be an ideal if

(i) $f+g \in I$ where $f \in I$ and $g \in I$, and

(ii) $pf \in I$ whenever $f \in I$ and, $p \in k[x_1,...,x_n]$ is an arbitrary polynomial.

Definition 2.4 Let $f_1,...,f_s \in k[x_1,...,x_n]$. We let $\langle f_1,...,f_s \rangle$ denote the collection

$\langle f_1,...,f_s \rangle = \{c_1 f_1 + ... + c_s f_s : c_i \in k[x_1,...,x_n], 1 \leq i \leq s\}$.

It is easy to show that $\langle f_1,...,f_s \rangle$ is an ideal of $k[x_1,...,x_n]$ and called ideal generated by $f_1,...,f_s$.

Example 2.5 Show that $x^2 \in \langle x-y^2, xy \rangle$ in $k[x,y]$ (k any field).

We can write $x^2 = xf_1 + yf_2$. This shows $x^2 \in \langle x-y^2, xy \rangle$.

Example 2.6 Show that $\langle x-y^2, xy, y^2 \rangle = \langle x, y^2 \rangle$. Consider $p,q,r \in k[x,y]$.

Let $f \in \langle x-y^2, xy, y^2 \rangle \Rightarrow f = p(x-y^2) + qxy + ry^2$

$$\Rightarrow f = (p+qy)x + (-p+r)y^2.$$

Thus, $f \in \langle x, y^2 \rangle$. Then,

$$\langle x-y^2, xy, y^2 \rangle \subseteq \langle x, y^2 \rangle \tag{1}$$

Let $f \in \langle x, y^2 \rangle \Rightarrow f = px + qy^2$

$$\begin{aligned} &= p(x-y^2) + py^2 + qy^2 \\ &= p(x-y^2) + (p+q)y^2 \end{aligned}$$

Thus, $f \in \langle x-y^2, xy, y^2 \rangle$. Then,

$$\langle x, y^2 \rangle \subseteq \langle x-y^2, xy, y^2 \rangle \tag{2}$$

From (1) and (2), $\langle x-y^2, xy, y^2 \rangle = \langle x, y^2 \rangle$.

Example 2.7 Show that $\langle y-x^2, z-x^3 \rangle = \langle z-xy, y-x^2 \rangle$ in $\mathbb{Q}[x,y,z]$.

Let $a_1, a_2 \in \mathbb{Q}[x,y]$ and $f \in \langle y-x^2, z-x^3 \rangle$. Then

$$\begin{aligned} f &= a_1(y-x^2) + a_2(z-x^3) \\ &= a_1(y-x^2) + a_2[1(z-xy+x(y-x^2)] \\ &= (a_1+a_2x)(y-x^2) + a_2(z-xy). \end{aligned}$$

We have $f \in \langle z-xy, y-x^2 \rangle$. Thus, $\langle y-x^2, z-x^3 \rangle \subseteq \langle z-xy, y-x^2 \rangle$ (1)

Let $f \in \langle z-xy, y-x^2 \rangle$. Then

$$\begin{aligned} f &= a_1(z-xy) + a_2(y-x^2) \\ &= a_1\left[-x(y-x^2) + 1(z-x^3)\right] + a_2(y-x^2) \\ &= (-a_1x+a_2)(y-x^2) + a_1(z-x^3). \end{aligned}$$

We have $f \in \langle y-x^2, z-x^3 \rangle$. Thus,

$$\langle z-xy, y-x^2\rangle \subseteq \langle z-xy, y-x^2\rangle. \tag{2}$$

From (1) and (2):

$$\langle y-x^2, z-x^3\rangle = \langle z-xy, y-x^2\rangle.$$

Example 2.8 Show that $\langle f_1,...,f_s\rangle$ is closed under sums in $k[x_1,...,x_n]$. Also show that if $f \in \langle f_1,...,f_s\rangle$, and $p \in k[x_1,...,x_n]$ is an arbitrary, then $p.f \in \langle f_1,...,f_s\rangle$.

For first case:

Let $f, g \in I = \langle f_1,...,f_s\rangle$. Then $f = \sum_{i=1}^{s} p_i f_i$ and $g = \sum_{i=1}^{s} q_i f_i$, $p_i, q_i \in k[x_1,...,x_n]$.

Thus

$$\begin{aligned} f+g &= \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i \\ &= \sum_{i=1}^{s} (p_i+q_i) f_i \ , \ r_i = p_i + q_i \in k[x_1,...,x_n] \\ &= \sum_{i=1}^{s} r_i f_i. \end{aligned}$$

Finally, $\langle f_1,...,f_s\rangle$ is closed under sums in $k[x_1,...,x_n]$.

For second case:

Suppose that $f = \sum_{i=1}^{s} q_i f_i$ and let $p \in k[x_1,...,x_n]$.Then

$$\begin{aligned} p.f &= \sum_{i=1}^{s} (p.q_i).f_i \ ; \quad a_i = p.q_i \in k[x_1,...,x_n] \\ &= \sum_{i=1}^{s} a_i.f_i \end{aligned}$$

Thus $p.f \in \langle f_1,...,f_s\rangle$.

The two properties in above example are the defining properties of ideals in the ring $k[x_1,...,x_n]$.

Example 2.9 The subset I of $k[x,y,z]$ consisting of all polynomials of the form

$$p_1(x,y,z)x^2 + p_2(x,y,z)y,$$

where p_1 and p_2 are arbitrary polynomials, is an ideal of $k[x,y,z]$. The ideal I is generated by $\{x^2, y\}$, that $\{x^2, y\}$ is a basis for I, and we write $I = \langle x^2, y\rangle$.

Given an ideal, or several ideals in $k[x_1,...,x_n]$, there are a number of algebraic constructions that yield other ideals. One of the most important of these for geometry is the following.

Definition 2.10 Let $I \subset k[x_1,...,x_n]$ be an ideal. The radical of I is the set $\sqrt{I} = \{g \in k[x_1,...,x_n] : g^m \in I \text{ for some } m \geq 1\}$. An ideal I is said to be a radical ideal if $\sqrt{I} = I$.

Example 2.11 Let $I = \langle x^2 + 3xy, 3xy + y^2\rangle$ in $\mathbb{Q}[x,y]$. What is $\sqrt{I}$?

For m=3, $(x+y)^3 = x(x^2+3xy) + y(3xy+y^2)$. Then $(x+y)^3 \in I$. Thus,

$$\begin{aligned}\sqrt{I} &= \{g(x,y) = x+y \in \mathbb{Q}[x,y] : g^3 \in I\}\\ &= \langle x+y\rangle.\end{aligned}$$

Example 2.12 Let $I = \langle x^2, y^3\rangle$ in $\mathbb{Q}[\text{x,y}]$. What is $\sqrt{I}$?

It is clear that $x \notin I$ and $y \notin I$ but $x \in \sqrt{I}$ and $y \in \sqrt{I}$. Also, $(xy)^2 = x^2y^2 \in I$. Finally, $x + y \in \sqrt{I}$. Thus, we have $(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$.

Then $(x+y)^4 \in I$, therefore $(x+y) \in \sqrt{I}$. Finally, $\sqrt{I} = \langle x, y\rangle$.

Although it is not obviously from definition, we have the following property of the radical.

Property 2.13 [Radical Ideal Property] For every ideal $I \subset k[x_1,...,x_n]$, $\sqrt{I}$ is an ideal containing I.

One of the most important general facts about ideal in $k[x_1,...,x_n]$ is know as the Hilbert Basis Theorem. In this thesis a basis is another name for a generating set for an ideal. The well-know Hilbert Basis Theorem states that every ideal of $k[x_1,...,x_n]$ is finitely generated. In other words, given an ideal I, there exists a finite collection of polynomials $\{f_1,...,f_s\} \subset k[x_1,...,x_n]$ such that $I = \langle f_1,...,f_s \rangle$. For polynomials in one variable, this is a standard consequence of the one variable polynomial division algorithm. Given two polynomials $f, g \in k[x]$, we can divide f by g, producing a unique quotient q an remainder r such that

$$f = qg + r,$$

and either $r = 0$, or r has degree strictly smaller than degree of g.

For polynomials in several variables, the Hilbert Basis Theorem can be proved either as a byproduct of the theory of Gröbner bases to be reviewed in the next section, or inductively by showing that if every ideal in a ring $k[x_1,...,x_n]$ is finitely generated.

Definition 2.14 Let a field k and a positive integer n, we will call the set

$$k^n = \{(a_1,...,a_n) : a_1,...,a_n \in k\}$$

the affine n-dimensional space over k.

Each polynomial $f \in k[x_1,...,x_n]$ defines a function $f : k^n \to k$. The value of f at $(a_1,...,a_n) \in k^n$ is obtained by the resulting expression in k.

For Example; Let $f \in k[x, y, z]$ and $f(x, y, z) = xy^2z^3$. Then $k^3 \xrightarrow{f} k$. Thus, since $(1,3,2) \in k^3, f(1,3,2) = 1.3^2.2^3 = 72 \in k$.

Definition 2.15 If k is an infinite field, then $f : k^n \to k$ is zero function if and only if $f = 0 \in k[x_1,...,x_n]$.

The notion of a variety is therefore inevitable. The set of all solutions to a system of equations $f_1(x_1,...,x_n) = ... = f_s(x_1,...,x_n) = 0$ is called an affine variety, explicitly defined as follows.

Definition 2.16

(i) Let $I = \langle f_1,..., f_s \rangle$ be ideal in $k[x_1,...,x_n]$. The set of zero locus of polynomials of I, $V(I) = \{(a_1,...,a_n) \in k^n : f_i(a_1,...,a_n) = 0, \textit{for all } 1 \le i \le s\}$ is called variety of ideal I.

(ii) Let $V \subset k^n$ be a variety. The collection of polynomials $I(V) = \{f \in k[x_1,...,x_n] : f(a_1,...,a_n) = 0, \forall (a_1,...,a_n) \in V\}$ is called ideal of variety V.

Example 2.17 For $f = x^2 + z^2 - 1 \in \mathbb{R}[x, y, z]$ we will write

$$V(f) = \left\{(x, y, z) \in \mathbb{R}^3 \middle| f(x, y, z) = x^2 + z^2 - 1 = 0\right\}.$$

Note that $V(f)$ is a circular cylinder of radius 1 along the y-axis.

Any finite intersection of affine varieties is also an affine variety. Any finite union of affine varieties is also an affine variety.

Lemma 2.18 If $\mathcal{V} = V(f_1,...,f_s), \mathcal{W} = V(g_1,...,g_t) \subset k^n$ are affine varieties, then so are

$$\mathcal{V} \cap \mathcal{W} = V(f_1,...,f_s,g_1,...,g_t),$$
$$\mathcal{V} \cup \mathcal{W} = V(f_i g_i : 1 \le i \le s, 1 \le j \le t).$$

Example 2.19 $\mathcal{V} = V(x^2 + z^2 - 1)$ in $\mathbb{R}^3$ is the cylinder. $\mathcal{W} = V(x^2 + y^2 + (z-1)^2 - 4)$ in $\mathbb{R}^3$ is the sphere of radius 2 centred at $(0,0,1)$. Thus,

The variety $\mathcal{V} \cap \mathcal{W} = V(x^2 + z^2 - 1, x^2 + y^2 + (z-1)^2 - 4)$ is the curve of intersection of the cylinder and the sphere.

The variety $\mathcal{V} \cup \mathcal{W} = V((x^2 + z^2 - 1)(x^2 + y^2 + (z-1)^2 - 4))$ is the union of the sphere and cylinder.

Definition 2.20 Ideal I is zero-dimensional if the associated variety $V(I)$ is a finite set.

Property 2.21[Equal Ideals Have Equal Varieties]

If $\langle f_1,...,f_s \rangle = \langle g_1,...,g_t \rangle$ in $k[x_1,...,x_n]$, then $V(f_1,...,f_s) = V(g_1,...,g_t)$.

Proof. Every $f \in \langle f_1,...,f_s \rangle$ is also in $\langle g_1,...,g_t \rangle$ and can therefore be expressed as $h_1 g_1 + ... + h_t g_t$. Hence, every $a = (a_1,...,a_n) \in V(g_1,...,g_t)$ satisfies $f(a) = 0$ and vice versa for all $g \in \langle g_1,...,g_t \rangle$. This shows that both varieties consist of the same points.

□

Gröbner bases are very useful for solving systems of polynomial equations. The variety does not change if we replace F by another set of polynomials that generates the same ideal in $k[x_1,...,x_n]$.

In particular, Gröbner basis G for the ideal $\langle F\rangle$ specifies the same variety:

$$V(F)=V(\langle F\rangle)=V(\langle G\rangle)=V(G).$$

The advantage of G is that it reveals geometric properties of the variety that are not visible from F.

Theorem 2.22 [Strong Nullstellensatz] If k is an algebraically closed field and I is an ideal in $k[x_1,...,x_n]$, then $I(V(I))=\sqrt{I}$.

Definition 2.23 An ideal $I\subset k[x_1,...,x_n]$ is amonomial ideal if $I=\langle x^\alpha:\alpha\in A\rangle$ for some $A\subset\mathbb{Z}^n_{\geq 0}$.

For example; $I=\langle x^2y^5,x^4y^3,x^5y\rangle$ is a monomaial ideal.

Lemma 2.24 Let $I=\langle x^\alpha:\alpha\in A\rangle$ be a monomial ideal. Then a monomial $x^\beta\in I$ if and only if x^α divides x^β for some α.

Proof. First, if x^β is a multiple of x^α for some $\alpha\in A$ then $x^\beta\in I$ because I is an ideal. Conversely, if $x^\beta\in I$ then we can write as a linear combination of x^{α_i} with polynomial coefficients. Then expanding each polynomial as a sum of monomials we have x^β as a sum of monomials each divisible by some x^α. But this is a polynomial identity so in fact x^β must be exactly one of these monomials and thus has the same monomials.□

Lemma 2.25 Let I be a monomial ideal and $f\in k[x_1,...,x_n]$. Then $f\in I$ if and only if f is a $k-$linear combination of monomials in I.

Proof. Clearly, if f is a $k-$linear combination of monomials in I then $f\in I$. For the other direction, if $f\in I$ then f is a $k-$linear combination of monomials of I.

So expanding this out we see that f is a $k-$linear combination of monomials which are in I by Lemma 2.24.□

Example 2.26 Let $I=\langle x^2, xy^3, y^4z, xyz\rangle \subset k[x,y,z]$ and

$f=3x^7+7xy^3+2y^4z+xy^2z^2$.

Then f is in I, since $x^7=(x^2)(x^5), xy^3z=(xy^3)(z), xy^2z^2=(xyz)(yz)$.

Lemma 2.27 [Dickson, 1913] Every monomial ideal $I \subset k[x_1,...,x_n]$ is generated by a finite number of monomials.

Proof. By induction on the number of variables.

If $n=1$, then let $\beta=\min\{\alpha : x^\alpha \in A\}$.

Inductive step. The result is valid for $k[x_1,...,x_{n-1}]$. We need to deduce it for $k[x_1,...,x_{n-1},y]$. Let $I \subset k[x_1,...,x_{n-1},y]$ be a monomial ideal with n variables. We write a monomial in $k[x_1,...,x_{n-1},y]$ as $x^\alpha y^m$. Consider the following set of monomials

$$I_m \subset k[x_1,...,x_{n-1}]$$
$$I_m=\{x^\alpha \in k[x_1,...,x_{n-1}] : x^\alpha y^m \in I\}$$

satisfying the ascending sequence

$$I_0 \subset I_1 \subset ...$$

Each I_k is finitely generated. This sequence terminates. Then the ideal I is a set of all monomials from the sequence.□

For example; Let $k[x,y]$, and consider $\langle x^2, x^2y, x^2y^2, ...\rangle$. The catch: we must elimininate redundant generators $\langle x^2, x^2y, x^2y^2, ...\rangle = \langle x^2\rangle$.

2.2 Monomial Orders

In general, it can be difficult to determine by inspection or by trial and error whether a given polynomial $f \in k[x_1,...,x_n]$ is a element of a given ideal $I = \langle f_1,...,f_s \rangle$, or whether two ideals $I = \langle f_1,...,f_s \rangle$ and $J = \langle f_1,...,f_t \rangle$ are equal. In this section and next one, we will consider a collection of algorithms that can be used to solve problems such as deciding ideal membership, computing ideal intersection and quotients, and computing elimination ideals.

The starting point for these algorithms is, in a sense, the polynomial division algorithm in $k[x]$, we saw that the division algorithm implies that every $I \subset k[x]$ has the form $I = \langle g \rangle$ for some g. Hence, if $f \in k[x_1,...,x_n]$, we can also use division to determine whether $f \in I$.

Given the usefulness of division for polynomials in one variable, we may ask: Is there a corresponding notion for polynomials in several variables? The answer is yes, and to describe it, we need to being by considering different ways to order the monomials appearing within a polynomial.

Definition 2.28 A monomial order on $k[x_1,...,x_n]$ is any relation $\succ$ on the set of monomials x^α in $k[x_1,...,x_n]$(or equivalently on the exponent vector $\alpha \in \mathbb{Z}^n_{\geq 0}$ satisfying:

(i) $\succ$ is a total(linear) ordering on $\mathbb{Z}^n_{\geq 0}$.

(ii) $\succ$ is compatible with multiplication in $k[x_1,...,x_n]$, in the sense that if $x^\alpha \succ x^\beta$ and x^γ is any monomial, then $x^\alpha x^\gamma = x^{\alpha+\gamma} \succ x^{\beta+\gamma} = x^\beta x^\gamma$.

(iii) $\succ$ is a well-ordering. That is, every nonempty collection of monomials has a smallest element under $\succ$.

The division algorithm in $k[x]$ makes use of a monomial order implicitly: when we divide g into f by hand, we always compare the leading term (the term of heights degree) in g with the leading term of the intermediate dividend. In fact there is no choice in the matter in this case.

For polynomials rings in several variables, there are many choices monomial orders. In writing the exponent vectors α and β in monomials x^{α} and x^{β} as ordered n-tuples, we implicitly set up an ordering on the variables x_i in $k[x_1,...,x_n]$:

$$x_1 \succ x_2 \succ ... \succ x_n.$$

With this choice, there are still many ways to define monomials orders. Three of the most important are given in the following definitions.

Definition 2.29 [Lexicographic Order (lex)]

Let x^{α} and x^{β} be monomials in $k[x_1,...,x_n]$. We say $x^{\alpha} \succ_{lex} x^{\beta}$ if in the difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive. Lexicographic order is analogous to the ordering of words used in dictionaries. For instance, $arrow \succ_{lex} arson$.

Definition 2.30 [Graded Lexicographic Order (grlex)]

Let x^{α} and x^{β} be monomials in $k[x_1,...,x_n]$.

We say $x^{\alpha} \succ_{grlex} x^{\beta}$ if $|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$, or $x^{\alpha} \succ_{lex} x^{\beta}$ if $|\alpha| = |\beta|$.

Definition 2.31 [Graded Reverse Lexicographic Order (grevlex)]

Let x^{α} and x^{β} be monomials in $k[x_1,...,x_n]$. We say $x^{\alpha} \succ_{grevlex} x^{\beta}$ if $\sum_{i=1}^{n}\alpha_i > \sum_{i=1}^{n}\beta_i$,

or if $\sum_{i=1}^{n}\alpha_i = \sum_{i=1}^{n}\beta_i$ and in the difference $\alpha-\beta \in \mathbb{Z}^n$, the right-most nonzero entry is negative.

Example 2.32 $x^3y^2z \succ_{lex} xy^2z^4$, since $\alpha-\beta=(3,2,1)-(1,2,4)=(2,0,-3)$ the left-most nonzero entry is positive, and $x^2y^4z \succ_{grlex} xy^6$, since $2+4+1=1+6+0$ but $\alpha-\beta=(2,4,1)-(1,6,0)=(1,-2,1)$ the left-most nonzero entry is positive. However $xy^3z \succ_{grevlex} xy^2z^2$ since $1+3+1=1+2+2$ but $\alpha-\beta=(1,3,1)-(1,2,2)=(0,1,-1)$ the right-most nonzero entry is negative.

Example 2.33 Show that the monomials of a fixed total degree d in two variables $x>y$ are ordered in the same sequence by $\succ_{lex}$ and $\succ_{grevlex}$.

Let $x^{\alpha}=x_1^{\alpha_1}x_2^{\alpha_2}, x^{\beta}=x_1^{\beta_1}x_2^{\beta_2}$ and $|\alpha|=|\beta|=d$.Thus,

$$\begin{aligned}x^{\alpha} \succ_{lex} x^{\beta} &\Leftrightarrow x_1^{\alpha_1}x_2^{\alpha_2} \succ_{lex} x_1^{\beta_1}x_2^{\beta_2}\\ &\Leftrightarrow \alpha_1 > \beta_1.\end{aligned}$$

Then, $\alpha_1-\beta_1>0.$ Since

$$\begin{aligned}|\alpha|=|\beta|=d &\Rightarrow \alpha_1+\alpha_2=\beta_1+\beta_2\\ &\Rightarrow \alpha_1-\beta_1=\beta_2-\alpha_2>0\\ &\Rightarrow \alpha_2-\beta_2<0.\end{aligned}$$

Thus $x^{\alpha} \succ_{grevlex} x^{\beta}$.

Now fixing a monomial order we can write a multivariate polynomial with the terms in decreasing order.

Definition 2.34 Let $f = \sum_{\alpha=1}^{n} a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1,...,x_n]$ and let $\succ$ be monomial order.

(i) The multi-degree of f is $multi\deg(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0)$

(ii) The leading monomial coefficient of f is $LC(f) = a_{multi\deg(f)} \in k$

(iii) The leading monomial of f is $LM(f) = x^{multi\deg(f)}$

(iv) The leading term of f is $LT(f) = LC(f) \cdot LM(f)$

(v) The polynomial f is called monic if $LC(f) = 1$.

Example 2.35 Let $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ in $k[x,y,z]$. Then, with respect to the lex order, f is reordered in decreasing order as:

$$f(x,y,z) = -3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$$

$$multi\deg(f) = (5,1,4), LC(f) = -3, LM(f) = x^5yz^4, LT(f) = -3x^5yz^4 .$$

With respect to the grlex order, f is reordered in decreasing order as:

$$f(x,y,z) = -3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$$

$$multi\deg(f) = (5,1,4), LC(f) = -3, LM(f) = x^5yz^4, LT(f) = -3x^5yz^4 .$$

With respect to the grevlex order, f is reordered in decreasing order as:

$$f(x,y,z) = 2x^2y^8 - 3x^5yz^4 - xy^4 + xyz^3$$

$$multi\deg(f) = (2,8,0), LC(f) = 2, LM(f) = x^2y^8, LT(f) = 2x^2y^8 .$$

2.3 Division Algorithm

Choosing any monomial order in $k[x_1,...,x_n]$ gives all the information necessary to establish a generalized division algorithm. The following is the well-known division algorithm on $k[x_1,...,x_n]$.

Theorem 2.36 Fix a monomial order $\succ$, and let $F=\{f_1,...,f_s\}$ be an ordered s-tuple of polynomials in $k[x_1,...,x_n]$. Then every $f\in k[x_1,...,x_n]$ can be written as

$$f=a_1f_1+...+a_sf_s+r,$$

where $a_i,r\in k[x_1,...,x_n]$, and either $r=0$ or r is a k-linear combination of monomials, none of which is divisible by any $LT(f_1),...,LT(f_s)$. r is called remainder of f on division by F. This can be written using reduction notation

$$f\xrightarrow{F}r \text{ or } f^{-F}=r.$$

Furthermore, if $a_if_i\neq 0$, then $multi\deg(f)\geq multi\deg(a_if_i)$.

Proof: The existence of $a_1,...,a_s$ and r is proved by the following constructive algorithm.

INPUT: $f,f_1,...,f_s\in k[x_1,...,x_n]$ with $f_i\neq 0\ (1\leq i\leq s)$

OUTPUT: $a_1,...,a_s,r$ such that $f=a_1f_1+...+a_sf_s+r$ and

r is reduce with respect to $F=\{f_1,...,f_s\}$ and

$\max\{LM(a_1)LM(f_1),...,LM(a_s)LM(f_s),LM(r)\}=LM(f)$.

INITIALIZATION: $a_1:=0,a_2:=0,...,a_S:=0,r:=0,h:=f$

WHILE $h\neq 0$ DO

IF there exists i such that $LM(f_i)$ divides $LM(h)$ THEN

Choose i least such that $LM(f_i)$ divides $LM(h)$

$$a_i := a_i + \frac{LT(h)}{LT(f_i)}$$
$$h := h - \frac{LT(h)}{LT(f_i)} f_i$$

ELSE

$$r := r + LT(h)$$
$$h := h - LT(h)$$

Algorithm 2.36 Multivariable Division Algorithm. □

In some situations, permutations of the set $\{f_1, ..., f_s\}$ do lead to different remainders. This situation can see in the following examples. As we shall see in section 2.4, this is not the case when the set is a Gröbner Basis.

Example 2.37 Let us consider dividing $f_1 = x^2y^2 - x$ and $f_2 = xy^3 + y$ in to $f = x^3y^2 + 2xy^4$. Using the lex order on $k[x, y]$ with $x > y$ and $F = \{x^2y^2 - x, xy^3 + y\}$. What is $\overline{f}^F$?

Lets divide $f = x^3y^2 + 2xy^4$ by $f_1 = x^2y^2 - x$ and $f_2 = xy^3 + y$ using lex order.

$$a_1 : x$$
$$a_2 : 2y$$

$$
\begin{array}{l|l}
f_1 = x^2y^2 - x & x^3y^2 + 2xy^4 \\
f_2 = xy^3 + y & x^3y^2 - x^2 \\
\hline
\end{array}
$$

$$x^2 + 2xy^4 \dashrightarrow x^2$$

$$
\begin{array}{l}
2xy^4 \\
2xy^4 + 2y^2 \\
\hline
-2y^2 \dashrightarrow -2y^2 \\
\hline
0
\end{array}
$$

Thus, $\overline{f}^F = x^2 - 2y^2$.

Using the steps of Multivariable Division Algorithm are:

INITIALIZATION: $a_1 := 0, r := 0, h = x^3y^2 + 2xy^4$

First pass through the WHILE loop:

$LM(f_1) = x^2y^2$ divides $LM(h) = x^3y^2$

$$a_2 := a_1 + \frac{x^3y^2}{x^2y^2} = x$$

$$h := h - \frac{x^3y^2}{x^2y^2}(x^2y^2 - x) = x^2 + 2xy^4$$

Second pass through the WHILE loop:

$LM(f_1) = x^2y^2$ and $LM(f_2) = xy^3$ does not divide $LM(h) = x^2$

$$r := r + x^2 = x^2$$
$$h := h - x^2 = 2xy^4$$

Third pass through the WHILE loop:

$LM(f_2) = xy^3$ divides $LM(h) = xy^4$

$$a_3 := a_2 + \frac{2xy^4}{xy^3} = x + 2y$$
$$h := h - \frac{2xy^4}{xy^3}(xy^3 + y) = -2y^2$$

Third pass through the WHILE loop:

$LM(f_1)$ and $LM(f_1)$ does not divide $LM(h)$

$$r := x^2 + (-2y^2) = x^2 - 2y^2$$
$$h := -2y^2 - (-2y^2) = 0$$

The WHILE loop stops,and we have $\overline{f}^F = x^2 - 2y^2$.

Most computer algebra system that have implementations of the division algorithm. For instance, the Mathematica and Maple computes a remainder on division of a polynomial by any collection of polynomials. The Mathematica commands for our example:

In[1]:= PolynomialReduce[x^3*y^2+2*x*y^4,{x^2*y^2-x,x*y^3+y},{x,y}]

Out[1]= {{x,2y},x^2-2y^2}

This mean $f = x(x^2y^2 - x) + 2y(xy^3 + y) + x^2 - 2y^2$. Thus, $\overline{f}^F = x^2 - 2y^2$.

When we change the order of divisors we see that this affects the output of the division algorithm.

Example 2.38 Let $f = x^2y + xy^2 + y^2$ and $f_1 = xy - 1$, $f_2 = y^2 - 1 \in k[x, y]$. Using lex order with $x > y$ and $F = \{f_1, f_2\}$. What is $\overline{f}^F$?

Lets divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_1 = y^2 - 1$ using lex order:

$$
\begin{array}{l|l l}
 & a_1 : x + y & \\
 & a_2 : 1 & \\
\hline
f_1 = xy - 1 & x^2y + xy^2 + y^2 & \\
f_2 = y^2 - 1 & x^2y - x & \\
\cline{2-2}
 & xy^2 + x + y^2 & \\
 & xy^2 - y & \\
\cline{2-2}
 & x + y^2 + y & \dashrightarrow x \\
\cline{2-2}
 & y^2 + y & \\
 & y^2 - 1 & \\
\cline{2-2}
 & y + 1 & \dashrightarrow y \\
\cline{2-2}
 & 1 & \dashrightarrow 1 \\
\cline{2-2}
 & 0 &
\end{array}
$$

We have $f = (x + y)f_1 + f_2 + x + y + 1$.

Using the steps of Multivariable Division Algorithm are:

INITIALIZATION: $a_1 := 0, r := 0, h = x^2y + xy^2 + y^2$

First pass through the WHILE loop:

$LM(f_1)$ divides $LM(h)$

$$a_2 := a_1 + \frac{x^2y}{xy} = x$$

$$h := (x^2y + xy^2 + y^2) - \frac{x^3y}{xy}(xy - 1) = xy^2 + x + y^2$$

Second pass through the WHILE loop:

$LM(f_1)$ divides $LM(h)$

$$a_3 := a_2 + \frac{xy^2}{xy} = x + y$$
$$h := h - \frac{xy^2}{xy}(xy - 1) = x + y^2 + y$$

Third pass through the WHILE loop:

$LM(f_1)$ and $LM(f_2)$ does not divide $LM(h)$

$$r := r + x = x$$
$$h := h - x = y^2 + y$$

Fourth pass through the WHILE loop:

$LM(f_2)$ divides $LM(h)$

$$a_4 := a_3 + \frac{y^2}{y^2} = x + y + 1$$
$$h := h - \frac{y^2}{y^2}(xy - 1) = y + 1$$

Fifth pass through the WHILE loop

$LM(f_1)$ and $LM(f_2)$ does not divide $LM(h)$

$$r := r + y = x + y$$
$$h := h - y = 1$$

Sixth pass through the WHILE loop

$LM(f_1)$ and $LM(f_2)$ does not divide $LM(h)$

$$r := r + 1 = x + y + 1$$
$$h := h - 1 = 0$$

The WHILE loop stops, and we have $\overline{f}^F = x + y + 1$.

Let consider we change the order of f_1 and f_2. Namely, let $F=\{f_2,f_1\}$.

Using the steps of Multivariable Division Algorithm are:

First pass through the WHILE loop:

$LM(f_1)$ divides $LM(h)$

$$a_2 := a_1 + \frac{x^2 y}{xy} = x$$
$$h := (x^2 y + xy^2 + y^2) - \frac{x^3 y}{xy}(xy-1) = xy^2 + x + y^2$$

Second pass through the WHILE loop:

$LM(f_2)$ divides $LM(h)$

$$a_3 := a_2 + \frac{xy^2}{y^2} = 2x$$
$$h := h - \frac{xy^2}{y^2}(y^2-1) = 2x + y^2$$

Third pass through the WHILE loop:

$LM(f_1)$ and $LM(f_2)$ does not divide $LM(h)$

$$r := r + 2x = 2x$$
$$h := h - 2x = y^2$$

Fourth pass through the WHILE loop:

$LM(f_2)$ divides $LM(h)$

$$a_4 := a_3 + \frac{y^2}{y^2} = 2x + 1$$
$$h := h - \frac{y^2}{y^2}(y^2-1) = 1$$

Fifth pass through the WHILE loop:

$r := r + 1 = 2x + 1$
$h := h - 1 = 0$

The WHILE loop stops, and we have $\overline{f}^F = 2x + 1$.

The Mathematica commands for our example:

In[1]:= PolynomialReduce[x^2*y + x*y^2 + y^2, {x*y - 1, y^2 - 1}, {x, y}]

Out[1]= {{x + y, 1}, 1 + x + y}

This mean $f = (x + y)(xy - 1) + 1.(y^2 - 1) + x + y + 1$.

In[2]:= PolynomialReduce[x^2*y + x*y^2 + y^2, {y^2 - 1, x*y - 1}, {x, y}]

Out[2]= {{1 + x, x}, 1 + 2 x}

This mean $f = (x + 1)(y^2 - 1) + x.(xy - 1) + 2x + 1$.

We have, $f = (x + 1) f_2 + x f_1 + 2x + 1$. Thus, $\overline{f}^F = 2x + 1$.

When we change the order of divisors, we see that this affects the output of the division algorithm. Namely, in the first case, we get $x + y + 1$ as the remainder and when we changed the order, the remainder became $2x + 1$. So for the ideal $I = \langle f_1, f_2 \rangle$ we see that $\{f_1, f_2\}$ is not a nice basis.

One natural question one might ask is that does there always exist a nice basis for polynomial ideals and if so how can we find it. In 1965, Buchberger gave a complete answer to this question as a result of his Phd studies. He named such bases as Gröbner bases to honor his advisor W. Gröbner. He also introduced an algorithm which outputs a Gröbner basis. Finally, if F is a Gröbner basis then this is not the above case.

2.4 Gröbner Basis for Polynomials Ideals

Since we now have a division algorithm in $k[x_1,...,x_n]$ that seems to have many of the same features as the one-variable version, it is natural to ask if deciding whether a given $f \in k\left[x_1,...,x_n\right]$ is a member of a given ideal $I = \langle f_1,...,f_s \rangle$ can be done along the lines of above examples, by computing the remainder on division. One direction is easy. Namely, it follows that if $r = \overline{f}^F = 0$ on dividing by $F = \{f_1,...,f_s\}$, then $f = a_1 f_1 + ... + a_s f_s$. By definition then, $f \in \langle f_1,...,f_s \rangle$. On the other hand, the above examples shows that we are not guaranteed to get $\overline{f}^F = 0$ for every $f \in \langle f_1,...,f_s \rangle$ if we use an arbitrary basis F for I.

Definition 2.39 Fix a monomial ordering. A finite subset $G = \{g_1,...,g_t\}$ of an ideal I is said to be a Gröbner Basis if for every nonzero $f \in I$, $LT(f)$ is divisible by $LT(g_i)$ for some i.

A Gröbner basis for I is indeed a generating set for I. Existence of Gröbner basis for an arbitrary ideal is an easy consequence of Hilbert Basis theorem. Moreover, remainders computed by division with respect to a Gröbner basis are much better behaved than those computed with respect to arbitrary sets of divisors.

Theorem 2.40 Let $G = \{g_1,...,g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1,...,x_n]$. Then any $f \in k[x_1,...,x_n]$ has a unique remainder on division by G.

Proof. Suppose $f = \sum_{i=1}^{t} a_i g_i + r = \sum_{i=1}^{t} a_i' g_i + r'$. Then $r - r' = \sum_{i=1}^{t} (a_i' - a_i) g_i \in I$. Hence $LT(r-r') \in \langle LT(g_1),...,LT(g_t) \rangle$, i.e., $LT(r-r')$ is divisible by some $LT(g_i)$. But this is impossible since no term of r, r' is divisible by any of $LT(g_1),...,LT(g_t)$. Thus $r-r'=0$ and uniqueness is proved.□

Theorem 2.41 [Hilbert Basis Theorem] Every ideal $I \subset k[x_1,...,x_n]$ is finitely generating set.

Proof. If $I=\{0\}$ then we are done. Assume $I \neq \{0\}$. Clearly the ideal $\langle LT(I)\rangle$ is a monomial ideal.We have that there exists a finite generating set $f_1,...,f_s \in I$ such that $\langle LT(I)\rangle = \langle LT(f_1),...,LT(f_s)\rangle$. We claim that $I=\langle f_1,...,f_s\rangle$. Clearly $\langle f_1,...,f_s\rangle \subset I$. In the direction, consider any $f \in I$. We can apply the Division Algorithm to obtain $f=a_1f_1+...+a_sf_s+r$, where no term of r is divisible by any of $LT(f_1),...,LT(f_s)$. Clearly $r \in I$, and if $r \neq 0$ then $LT(r) \in \langle LT(I)\rangle = \langle LT(f_1),...,LT(f_s)\rangle$. By Theorem 2.36 we have that $\langle LT(r)\rangle$ must be divisible by one of the $\langle LT(f_i)\rangle$. This is contradiction. Hence $r=0$ and so $f \in \langle f_1,...,f_s\rangle$. The result follows.□

Theorem 2.42 Let $G=\{g_1,...,g_t\}$ is a Gröbner basis for ideal $I \subset k[x_1,...,x_n]$ and let $f \in k[x_1,...,x_n]$. Then $f \in I$ if and only if the remainder of f on division by G is zero.

Proof. If the remainder is zero then $f \in I$. Conversely, if $f \in I$ then $f=f+0$ which satisfies the conditions above and thus by uniqueness any remainder r must be zero. □

Crollary 2.43 Every none-zero ideal $I \subset k[x_1,...,x_n]$ has a Gröbner basis.

Proof. It follows directly from the the proof of Hilbert's basis theorem.

More useful for many purposes than the existence proof for Gröbner bases in an algorithm, due to Buchberger, that takes an arbitrary generating set $\{f_1,...,f_s\}$ for I and produce a Gröbner basis G for I from it. This algorithm works by forming new elements of I using expression guaranteed to cancel leading terms and uncover other possible leading terms.

Definition 2.44 Let $f,g \in k[x_1,...,x_n]$ be nonzero polynomials.

(i) If $multi\deg(f)=\alpha$ and $multi\deg(g)=\beta$, then $\gamma=\{\gamma_1,...,\gamma_n\}$ where $\gamma_i=\max(\alpha_i\beta_i)$ for each i. x^γ is called the least common multiple of $LM(f)$ and $LM(g)$, written as $x^\gamma = LCM(LM(f),LM(g))$.

(ii) The $S-polynomial$ of f and g is combination

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

Example 2.45 Let $f=x^2y^3+xy^4-x$ and $g=x^4y+y^2$ in $k[x,y]$ with the grlex order.

Then, $\gamma=(4,3)$ and

$$\begin{aligned}S(f,g)&=\frac{x^4y^3}{x^2y^3}f-\frac{x^4y^3}{x^4y}g\\&=x^2f-y^2g\\&=x^3y^4-x^3-y^4.\end{aligned}$$

Maple can calculate the $S-polynomial$ for we:

With(Groebner):

spoly(y-x^2,z-x^3,plex(x,y,z));

$\{x^3y^4-x^3-y^4\}$.

The next theorem gives a criterion for when a basis of an ideal is a Gröbner basis.

Theorem 2.46 Let I be a polynomial ideal. Then a basis $G=\{g_1,...,g_t\}$ for I Gröbner basis if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.

Using this criteria above, Buchberger's Algorithm computes a Gröbner basis for an ideal I.

Algorithm 2.47 Let $F=\langle f_1,...,f_s\rangle$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in finite steps by the following algorithm:

INPUT: $F=\langle f_1,...,f_s\rangle \subset k[x_1,...,x_2]$ with $f_i \neq 0 (1 \leq i \leq s)$

OUTPUT: $G=\{g_1,...,g_t\}$ a Gröbner basis for $F=\langle f_1,...,f_s\rangle$

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

Fix a monomial order.

WHILE $G' \neq \phi$ DO

Choose any $(f, g) \in G'$

$G' := G' - \{(f, g)\}$
$h := \overline{S(g, f)}^{G}$

IF $h \neq 0$ THEN

$G' := G' \cup \{(u, h) | \mathit{for\ all}\ u \in G'\}$
$G := G \cup \{h\}$

Where $\overline{S(g, f)}^{G}$ is remainder on division of $S(f, g)$ by G.

Algorithm 2.47 Bucberger's Algorithm for computing Gröbner Basis.

Buchberger's Algrotihm is the oldest and most well-known method of transforming a given set of generators for a polynomial ideal into a Gröbner basis.

Example 2.48 Consider $k[x,y]$ with lex order, $x>y$ and let $I=\langle xy-x,x^2-y\rangle$. We will calculate a Gröbner bases for I.

Let $G=\{xy-x,x^2-y\}$ and $f=xy-x$, $g=x^2-y$.

$$\begin{aligned}S(f,g)&=\frac{x^2y}{xy}(xy-x)-\frac{x^2y}{x^2}(x^2-y)\\&=-x^2+y^2\end{aligned}$$

Thus $\overline{S(f,g)}^G=y^2-y$, then $h=y^2-y$.

We have $G=\{f,g,h\}$. Then, $\overline{S(f,g)}^G=0$. Next pair:

$$\begin{aligned}S(f,h)&=\frac{xy^2}{xy}(xy-x)-\frac{xy^2}{y^2}(y^2-y)\\&=y(xy-x)-x(y^2-y)\\&=xy^2-xy-xy^2+xy\\&=0.\end{aligned}$$

Thus, $\overline{S(f,h)}^G=0$ and next pair:

$$\begin{aligned}S(g,h)&=\frac{x^2y^2}{x^2}(x^2-y)-\frac{x^2y^2}{y^2}(y^2-y)\\&=y^2(x^2-y)-x^2(y^2-y)\\&=x^2y^2-y^3-x^2y^2+x^2y\\&=x^2y-y^3\end{aligned}$$

Then $\overline{S(g,h)}^G=0$.

Finally, $G=\{xy-x,x^2-y,y^2-y\}$ is a Gröbner basis for I.

The Mathematica code:

In[1]:= $f = x*y - x;$

In[2]:= $g = x\wedge 2 - y;$

In[3]:= $Sfg = x*f - y*g\,//\,Simplify$

Out[3]= $-x^2 + y^2$

In[4]:= $Polynomial\,\mathrm{Re}\,duce[Sfg, \{f, g\}, \{x, y\}]$

Out[4]= $\{\{0, -1\}, -y + y^2\}$

In[5]:= $h = -y + y^2;$

In[6]:= $Sfh = y*f - x*h\,//\,Simplify$

Out[6]= 0

In[7]:= $Sfh = y\wedge 2*g - x\wedge 2*h\,//\,Simplify$

Out[7]= $y(x^2 - y^2)$

In[8]:= $Polynomial\,\mathrm{Re}\,duce[Sgh, \{f, g, h\}, \{x, y\}]$

Out[8]= $\{\{x, 1, -1 - y\}, 0\}$

Then $G = \{xy - x, x^2 - y, y^2 - y\}$ is a Gröbner bases for I.

Or we can use the following command in a briefly:

In[9]:= $GroebnerBasis[\{f, g\}, \{x, y\}]$

Out[10]= $\{-y + y^2, -x + xy, x^2 - y\}$

Example 2.49 Consider $k[x, y]$ with lex order $x > y > z$ and let $I = \left\langle x^2 y + z, xz + y \right\rangle$.

We will calculate a Gröbner bases for I.

In[1]:= $f1 = x\wedge 2*y + z;$

In[2]:= $f2 = x*z + y;$

In[3]:= $S12 = z * f1 - x * y * f2 // Simplify$

Out[3]= $-xy^2 + z^2$;

In[4]:= $Polynomial\,\mathrm{Re}\,duce[S12, \{f1, f2\}, \{x, y, z\}]$

Out[4]= $\{\{0,0\}, -xy^2 + z^2\}$

In[5]:= $f3 = -xy^2 + z^2$;

In[6]:= $S13 = y * f1 - (-x) * f3 // Simplify$

Out[6]= $z(y + xz)$

In[7]:= $Polynomial\,\mathrm{Re}\,duce[S13, \{f1, f2, f3\}, \{x, y, z\}]$

Out[7]= $\{\{0, z, 0\}, 0\}$

In[8]:= $S23 = y \wedge 2 * f2 - (-2) * f3 // Simplify$

Out[8]= $y^3 + z^3$

In[9]:= $f4 = y^3 + z^3$;

In[10]:= $S14 = y \wedge 2 * f1 - x \wedge 2 * f4 // Simplify$

Out[10]= $-x^3z^2 + y^2z$

In[11]:= $Polynomial\,\mathrm{Re}\,duce[S14, \{f1, f2, f3, f4\}, \{x, y, z\}]$

Out[11]= $\{\{0, yz - xz^2 0, 0\}, 0\}$

In[11]:= $S24 = y \wedge 3 * f2 - x * z * f4 // Simplify$

Out[11]= $y^4 - xz^4$

In[12]:= $Polynomial\,\mathrm{Re}\,duce[S24, \{f1, f2, f3, f4\}, \{x, y, z\}]$

Out[12]= $\{\{0, -z^3, 0, y\}, 0\}$

In[13]:= $S34 = (-y) * f3 - x * f4 // Siplify$

Out[13]= $-z^2(y+xz)$

In[14]:= $PolynomialReduce[S34,\{f1,f2,f3,f4\},\{x,y,z\}]$

Out[[14]= $\{\{0,-z^2,0,0\},0\}$

Thus,

$G=\{x^2y+z, xz+y, -xy^2+z^2, y^3+z^3\}$ is Gröbner basis for the ideal I.

Or we can use the following command in a briefly:

In[16]:= $GroebnerBasis[\{f1,f2\},\{x,y,z\}]$

Out[16]= $\{y^3+z^3, y+xz, xy^2-z^2, x^2y+z\}$

Example 2.50 Consider $k[x,y]$ with lex order $y>x$ and let

$I=\left\langle y^2+xy+x^2, y+x, y\right\rangle$. We will calculate a Gröbner bases for I.

Gröbner basis of I can be as $G=\{f_1,f_2,f_3,f_4,f_5\}=\{y^2+xy+x^2, y+x, y, x^2, x\}$.

Since $LT(f_4)=x^2$ is divisible by $LT(f_5)=x$, $G'=\{f_1,f_2,f_3,f_5\}$ is also a Gröbner basis for I. Thus we can give following lemma and definition.

Lemma 2.51 Let G be a Gröbner basis for the polynomial ideal I. Let $g\in G$ be a polynomial such that $LT(g)\in\left\langle G-\{g\}\right\rangle$. Then $G-\{g\}$ is still a Gröbner basis for I.

Poof. Note that $\left\langle LT(G-\{g\})\right\rangle=\left\langle LT(G)\right\rangle=\left\langle LT(I)\right\rangle$. Hence $G-\{g\}$ is still a Gröbner basis for I.□

Definition 2.52 A minimal Gröbner basis for I is a Gröbner basis G for I such that

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

(ii) for all $g\in G$, $LT(g)\notin\left\langle LT(G)\setminus\{g\}\right\rangle$.

How to obtained a minimal basis? We must eliminiate all g_i for which there exists $i \neq j$ such that $LM(g_j)$ divides $LM(g_i)$.

Example 2.53 Consider $I = \langle F \rangle$, where $F = \{x^2 + 2xy^2, xy + 2y^3 - 1\}$ with lex order and $x > y$ in $k[x, y]$.

Gröbner basis of I can be as $G = \{x^2 + 2xy, xy + 2y^2 - 1, x, 2y^3 - 1\}$. We can eliminate g_1 and g_2 since their leading terms are both multiplies of the leading term of g_3. This leads to basis $G = \{x, y^3 - 1/2\}$. Thus a minimal Gröbner basis of the I is $G = \{x, y^3 - 1/2\}$.

Definition 2.54 A reduced Gröbner basis for I is a Gröbner basis G for I such that

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

(ii) for all $g \in G$, no monomial of g lies in $LT(g) \notin \langle LT(G) \setminus \{g\}) \rangle$.

Example 2.55 Consider the ideal $I = \langle xy - z, yz - x, zx - y \rangle \subset \mathbb{Q}[x, y, z]$ with lex order and $x < y < z$. We obtain the Gröbner basis as follows:

$$G = \{x^3 - x, yx^2 - y, y^2 - x^2, z - xy\}.$$

We can directly deduce from Definition 2.54 that G is a reduced Gröbner basis for I.

From the above theorme and definitions, we can give following theorem.

Theorem 2.56 Let I be a non-zero ideal of $k[x_1, ..., x_n]$. The following are equivalent for a set of non-zero polynomials $G = \{g_1, ..., g_t\} \subseteq I$:

(i) G is a Gröbner basis for I,

(ii) $f \in I$ if and only if $\overline{f}^G = 0$,

(iii) $LT(G) = LT(I)$,

(iv) $f \in I$ if and only if $LM(f) = \max_{1 \le i \le m} \{LM(h_i), LM(g_i)\}$.

Multivariate division requires a monomial ordering, the basis depends on the monomial ordering chosen, and different orderings can give rise to radically different Gröbner bases. Two of the commonly used orderings are lexicographic ordering, and degree reverse lexicographic ordering. Lexicographic order eliminates variables, however the resulting Gröbner bases are often very large and expensive to compute. Degree reverse lexicographic order typicall provides for the fastest Gröbner basis compuatation.

What is a Gröbner basis? A Gröbner basis is a set of multivariate polynomials that has desirable algorithmic properties. Every set of polynomials can be transformed into a Gröbner basis. This process generalizes three familiar techniques:

(i) Gaussian elimination for solving linear system of equations,

(ii) The Euclidean Algorithm for computing the greatest common divisor of two univariate polynomials,

(iii) The Simplex Algorithm for linear programing.

2.5 Syzygy Modules

Definition 2.57 A module over a ring R (or $R-\text{mod}ule$) is set M together with a binary operation, usually written as addition of R on M, and an operation of R on M, called scalar multiplication, satisfying properties.

(i) M is an Abelian group under addition.

(ii) For all $a \in R$ and all $f, g \in M, a(f+g) = af + ag$.

(iii) For all $a,b \in R$ and all $f \in M, (a+b)f = af + bf$.

(iv) For all $a,b \in R$ and all $f \in M, (ab)f = a(bf)$.

(v) If is multiplicative identity in R, $1.f = f$ for all $f \in M$.

Definition 2.58 Let M be a module over a ring R. M is said to be free module if M has a module basis (that is, a generating set which is $R-$linearly independent).

For instance, the $R-\text{mod}\,ule$ $M = R^m$ is a free module. The standard vectors $e_1 = (1,0,0,...,0)^T, e_2 = (0,1,0,...,0)^T,...., e_m = (0,0,0,...,1)^T$ form one basis for M as $R-\text{mod}\,ule$.

One obtains other examples of $R-\text{mod}\,ules$ by considering submodules of R^m, that is, subset of R^m which are closed under addition and scalar multiplication by elements of R and which are, therefore, modules in their own right.

We might, for example, choose a finite set of vectors $f_1,...,f_s$ and consider the set of all vectors which can be written as an $R-$linear combination of these vectors: $\{a_1 f_1 + ... + a_s f_s \in R^m, a_1,...,a_s \in R\}$.

We denote this set $\langle f_1,...,f_s \rangle$, and we can easily show that it is a submodule of R^m. These kind of submodules are called finitely generated submodules.

In this section, we consider finitely generated submodules of free module R^m where $R = k[x_1,...,x_n]$ is the polynomial ring over some field k. In particular, we will consider what we call syzygy submodules of R^m.

Definition 2.59 Let $R = k\left[x_1,...,x_n\right]$, and let $(f_1,...,f_t)$ be an ordered $t-$tuple of elements $f_i \in R$. The set of all $(a_1,...,a_t)^T \in R^t$ such that $a_1 f_1 + ... + a_t f_t = 0$ is an

$R-$submodule of R^t, called the (first) syzygy module of $(f_1,...,f_t)$, and denoted $syz(f_1,...,f_t)$.

The syzygy modules are finitely generated $R-$modules, and a set of generators for them can be computed. If the starting point is a Gröbner basis, then finding a set of generators for the syzygy module is accomplished using Buchberger's algorithm. While computing a Gröbner basis $G=\{g_1,...,g_s\}$ for an ideal $I \subset R$ with respect to some fixed monomial ordering, a slight modification of the algorithm would actually compute a set of generators for the syzygy module $syz(g_1,...,g_s)$ as well as the g_i's themselves.

Let $S(g_i,g_j)$ be the $S-$polynomial of g_i and g_j:

$$S(g_i,g_j)=\frac{x^{\gamma_{ij}}}{LT(g_i)}g_i-\frac{x^{\gamma_{ij}}}{LT(g)}g_j,$$

where $x^{\gamma_{ij}}$ is the least common multiple of $LM(g_i)$ and $LM(g_j)$. Since G is a Gröbner basis, the remainder of $S(g_i,g_j)$ on division by G is zero, and division algorithm gives an expression

$$S(g_i,g_j)=\sum_{k=1}^{s}a_{ijk}g_k \ ,$$

where $a_{ijk} \in R$, and $LT(a_{ijk}) \le LT(S(g_i,g_j)$ for all i,j,k.

Let $a_{ij} \in R^s$ denote the column vector

$$a_{ij}=a_{ij1}e_1+...+a_{ijs}e_s=(a_{ij1},...,a_{ijs})$$

and define $s_{ij} \in R$ by setting

$$s_{ij} = \frac{x^{\gamma_{ij}}}{LT(g_i)} e_i - \frac{x^{\gamma_{ij}}}{LT(g_j)} e_j + a_{ij} \qquad (*)$$

in R^s. Then the next theorem shows how to find a basis for the syzygy module.

Theorem 2.60 Let $G = \{g_1,...,g_s\}$ be a Gröbner basis of an ideal I in R with respect to some fixed monomial order, and let $M = syz(g_1,...,g_t)$. The collection $\{s_{ij}, 1 \le i, j \le s\}$ from (*) generates M as an $R-\mathrm{mod}ule$.

The next step is to compute $syz(f_1,...,f_t)$ for a collection $\{f_1,...,f_t\}$ of non-zero polynomial is R which may not from a Gröbner basis. First compute a Gröbner basis $\{g_1,...,g_s\}$ for $\langle f_1,...,f_t \rangle$. Set $F = (f_1,...,f_t)$ and $G = (g_1,...,g_s)$. Since the elements of F and G generator the same ideal, there are a txs matrix A and sxt matrix B, both with entries in R, such that $G = FA$ and $F = GB$. The matrix B can be compute by applying the division algorithm with respect to G. The matrix A can be obtained by keeping track of reductions of $S-$polynomials on the division process during Buchberger's Algorithm.

A generating set $\{s_1,...,s_p\}$ for $syz(G)$ (the s_i's are column vectors in R^s) can be computed using Theorem 2.60. Let $r_1,...,r_t$ be the column of the matrix $I_t - AB$.

Theorem 2.61 With the notation above,

$$\{As_1, As_2,..., As_p, r_1, r_2,..., r_t\}$$

is a generating set for $syz(f_1,...,f_t)$.

Example 2.62 Let $M = \langle f_1, f_2 \rangle$ in $R = k[x, y]$ where

$$f_1 = xy + x, \quad f_2 = y^2 + 1.$$

Using the lex monomial order, the reduced Gröbner basis for M consist of

$$g_1 = x, \quad g_2 = y^2 + 1 .$$

Then it is easy to check that

$$f_1 = (y+1)g_1$$

$$g_1 = -(\frac{1}{2})(y-1)f_1 + (\frac{1}{2})xf_2 ,$$

so that

$$G = (g_1, g_2) = (f_1, f_2)\begin{pmatrix} -(y-1)/2 & 0 \\ x/2 & 1 \end{pmatrix} = FA$$

and

$$F = (f_1, f_2) = (g_1, g_2)\begin{pmatrix} y+1 & 0 \\ x/2 & 1 \end{pmatrix} = GB .$$

Since

$$S(g_1, g_2) = y^2 g_1 - x g_2 = -x = -g_1 ,$$

by Theorem 2.60 we have that

$$s_{12} = \begin{pmatrix} y^2 + 1 \\ -x \end{pmatrix}$$

generates $syz(g_1, g_2)$. Multiplying by A we get

$$As_{12} = \begin{pmatrix} -(y-1)/2 & 0 \\ x/2 & 1 \end{pmatrix}\begin{pmatrix} y^2+1 \\ -x \end{pmatrix}$$

$$= \begin{pmatrix} -(y^3 - y^2 + y - 1)/2 \\ (xy^2 - x)/2 \end{pmatrix}.$$

The columns of $I_2 - AB$ are

$$S_1 = \begin{pmatrix} (y^2+1)/2 \\ -(xy+x)/2 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

So by the Theorem 2.61,

$$syz(f_1, f_2) = \langle As_{12}, S_1 \rangle.$$

Example 2.63 Let $M = \langle f_1, f_2 \rangle$ in $R = k[x, y, z]$ where

$$f_1 = x^2 y + z, \quad f_2 = xz + y.$$

Using the lex monomial order and $x > y > z$, the reduced Gröbner basis for M :

In[1]:= $GroebnerBasis[\{x \wedge 2 * y + z, x * z + y\}, \{x, y, z\}]$
Out[1]= $\{y^3 + z^3, y + xz, xy^2 - z^2, x^2 y + z\}$

Thus $g_1 = x^2 y + z,\ \ g_2 = y + xz,\ \ g_3 = xy^2 - z^2,\ \ g_4 = y^3 + z^3$ .Then

In[2]:= $Polynomial\,\mathrm{Re}\,duce[g_1, \{f_1, f_2\}, \{x, y, z\}]$
Out[2]= $\{\{1, 0\}, 0\}$

This mean

$$g_1 = 1.f_1 + 0.f_2.$$

In[3]:= $Polynomial\,\mathrm{Re}\,duce[g_2, \{f_1, f_2\}, \{x, y, z\}]$
Out[3]= $\{\{0, 1\}, 0\}$

This mean

$$g_2 = 0.f_1 + 1.f_2$$

So as $g_3 = (-z) \cdot f_1 + (xy) \cdot f_2$ and $g_4 = z^2 \cdot f_1 + (-xyz + y^2) \cdot f_2$.

$$[g_1 \quad g_2 \quad g_3 \quad g_4] = [f_1 \quad f_2] \begin{bmatrix} 1 & 0 & -z & z^2 \\ 0 & 1 & xy & -xyz + y^2 \end{bmatrix} = FA$$

and

$$\begin{bmatrix} f_1 & f_2 \end{bmatrix} = [g_1 \quad g_2 \quad g_3 \quad g_4] \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} = GB .$$

Since

$$\begin{aligned} S(g_1, g_2) &= \frac{x^2yz}{x^2y}(x^2y+z) - \frac{x^2yz}{xz}(y+xz) \\ &= z(x^2y+z) + (-xy)(y+xz) \\ &= -xy^2 + z^2 \\ &= (-1)(xy^2 - z^2) \\ &= (-1).g_3 \end{aligned}$$

by Theorem 2.60

$s_{12} = (z, -xy, 1, 0)$. And

$$\begin{aligned} S(g_1, g_3) &= \frac{x^2y^2}{x^2y}(x^2y+z) - \frac{x^2y^2}{xy^2}(xy^2 - z^2) \\ &= y(x^2y+z) + (-x)(xy^2 - z^2) \\ &= z(xz+y) \\ &= z.g_2 \end{aligned}$$

So by the Theorem 2.61,

$s_{13} = (y, -z, -x, 0)$.

Similarly $s_{23} = (0, y^2, -z, -1)$ and $s_{34} = (0, z^2, y, -x)$.

We can use a computer algebra system for polynomial computations to find s_{12}, s_{13}, s_{23} and s_{34}. Using singular [9]:

$> ring\ r = 0,\ (x, y, z),\ dp;$

$>\ ideal\ i = x2y + z,\ y + xz,\ xy2 - z2,\ y3 + z3;$

$> Syz(i);$

$[1] = x * gen(3) - y * gen(1) + z * gen(2)$

$[2] = z2 * gen(2) - x * gen(4) + y * gen(3)$

$[3] = y2 * gen(2) - z * gen(3) - gen(4)$

$[4] = xy * gen(2) - z * gen(1) - gen(3)$

We have $syz(g_1, g_2, g_3, g_4) = \langle s_{12}, s_{13}, s_{23}, s_{34} \rangle$.

Multiplying by A we get

$$As_{12} = \begin{bmatrix} 1 & 0 & -z & z^2 \\ 1 & 0 & xy & -xyz + y^2 \end{bmatrix} \begin{bmatrix} z \\ -xy \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$As_{13} = \begin{bmatrix} 1 & 0 & -z & z^2 \\ 1 & 0 & xy & -xyz + y^2 \end{bmatrix} \begin{bmatrix} y \\ -z \\ -x \\ 0 \end{bmatrix} = \begin{bmatrix} xz + y \\ -1.(x^2y + z) \end{bmatrix} = \begin{bmatrix} g_2 \\ -g_1 \end{bmatrix}$$

$$As_{23} = \begin{bmatrix} 1 & 0 & -z & z^2 \\ 1 & 0 & xy & -xyz + y^2 \end{bmatrix} \begin{bmatrix} 0 \\ y^2 \\ -z \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

and

$$As_{34} = \begin{bmatrix} 1 & 0 & -z & z^2 \\ 1 & 0 & xy & -xyz + y^2 \end{bmatrix} \begin{bmatrix} 0 \\ z^2 \\ y \\ -x \end{bmatrix} = \begin{bmatrix} -xz^2 - yz \\ x^2yz + z^2 \end{bmatrix} = \begin{bmatrix} -z.g_2 \\ z.g_1 \end{bmatrix}.$$

Other hand $I_2 - AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Therefore $syz(f_1, f_2) = \langle s_{13}, s_{34} \rangle$.

2.6 Homogeneous Bases for Polynomial Ideals

More detail information can be found in [10] and [11] .

Definition 2.64 A polynomial $f \in k[x_1,...,x_n]$ is homogeneous of total degree d provided that every term appearing in f has total degree d.

For example; $f = 2x^4 - 5x^2y^2 + z^4$, $g = 2x^4 - 5x^2y^2 + z^3 \in \mathbb{Q}[x,y,z]$. Then, f is a homogeneous polynomial of degree 4, g is not a homogenous polynomial.

An important fact is that every polynomial can be written uniquely as a sum of homogeneous polynomials. Namely, given $f \in k[x_1,...,x_n]$, let f_k be the sum of all terms of f of total degree k. Then each f_k is homogeneous and $f = \sum_k f_k$. Each f_k is called the $k-th$ homogeneous component of f.

For instance, let $f = x^3y^2z - xyz + x^2y^2z^2 - y^2z^3 \in \mathbb{Q}[x,y,z]$. Then

$$f = x^3y^2z + x^2y^2z^2 - y^2z^3 - xyz .$$

Definition 2.65 Let $g(x_1,...,x_n) \in k[x_1,...,x_n]$ be a polynomial of total degree d and $f = \sum_{i=0}^{d} g_i$ be the decomposition of g as the sum of its homogeneous components, where g_i has total degree i, then

$$g^h(x_0,x_1,...,x_n) = \sum_{i=0}^{d} g_i(x_1,...,x_n)x_0^{d-i}$$

is called the homogenization of g with respect to x_0.

The next theorem states some facts regarding the process of the homogenization.

Proposition 2.66 [7] Let $g(x_1,...,x_2) \in k[x_1,...,x_n]$ be a polynomial of total degree d.

(i) The homogenization of g, g^h, is a homogeneous polynomial of total degree d.

(ii) The homogenization of g can be computed using the formula $g^h = x_0{}^d g(\frac{x_1}{x_0},...,\frac{x_n}{x_0})$.

(iii) De homogenizing g^h yields g. That is $g^h(1,x_1,...,x_n) = g(x_1,...,x_n)$.

(iv) Let $F(x_0,x_1,...,x_n)$ be a homogeneous polynomial and let x_0^e be the highest power x_0 dividing F. If $f = F(1,x_1,...,x_n)$ is the de homogenization of F, then $F = x_0^e f^h$.

(v) $f^h g^h = (fg)^h$.

For instance, let above example $f = x^3y^2z + x^2y^2z^2 - y^2z^3 - xyz$.

The homogenization of f with respect to x_0:

$f^h = (x^3y^2z)x_0^0 + (x^2y^2z^2)x_0^0 - (y^2z^3)x_0^1 - (xyz)x_0^3$ and de homogenizing f^h: let x_0=1 then $f^h(1,x,y,z) = x^3y^2z + x^2y^2z^2 - y^2z^3 - xyz = f(x,y,z)$.

Definition 2.67 An ideal I in $k[x_0,x_1,...,x_n]$ is said to be homogeneous if for each $f \in I$, the homogeneous components f_i of f are in I as well.

Proposition 2.68 [7] Let $I \subset k[x_0,x_1,...,x_n]$ be an ideal. Then the following are equivalent:

(i) I is a homogeneous ideal of $k[x_0,x_1,...,x_n]$.

(ii) There exists some homogeneous polynomial $f_1,...,f_s$, such that $I = \langle f_1,...,f_s \rangle$.

The next lemma gives a property of homogeneous ideal which will be used to find a criterion for the homogeneous bases.

Lemma 2.69 Let $f_1,...,f_s$ be homogeneous polynomials of total degree $d_1 \le d_2 \le ... \le d_s$ and let $I = \langle f_1,...,f_s \rangle$. If g is another homogeneous polynomial of degree d in I. Then g must be element of $I_d = \langle f_i : \deg(f_i) \le d \rangle \subset I$. Moreover, there exist $q_1,...,q_t$ with $g = \sum_{i=1}^{t} q_i f_i$ such that each q_i is homogeneous of total degree $d - d_i$.

Proof. Assume there exist t such that $\deg(f_i) > d$ for $i > t$. Let

$$g = p_1 f_1 + ... + p_t f_t + p_s f_s$$

since $\deg(g) = d$ and $\deg(p_i f_i) > d$ for $i \ge j$, $p_t f_t + ... + p_s f_s = 0$. Since $f_i \ne 0$, $p_i = 0$ for $i > t$. Therefore,

$$g = p_1 f_1 + ... + p_t f_t .$$

If p_i written as sum of two polynomials $p_i = q_i + r_i$ where q_i is a homogeneous polynomial of total degree $d - d_i$ and r_i is the other part p_i, then the multiplication $r_i \times f_i$ produces monomials which have total degree different from d. Since g is a homogeneous polynomial of total degree d, $r_i f_i = 0$ for all i. Hence

$$g = p_1 f_1 + ... + p_t f_t + p_s f_s . \square$$

Definition 2.70 Let I be an ideal in $k[x_1,...,x_n]$. The homogenization of I is defined to be the ideal,

$$I^h = \langle f^h : f \in I \rangle \subset k[x_0, x_1,...,x_n],$$

where f^h is homogenization of f with respect to x_0.

Proposition 2.71 For any ideal $I \subset k[x_1,...,x_n]$, homogenization I^h is homogeneous ideal in $k[x_0,x_1,...,x_n]$.

Proof. By the Hilbert Basis Theorem, there exists polynomials $g_1,...,g_s \in I^h$ such that $I^h = \langle g_1,...,g_s \rangle$. By the definition of I^h,

$$g_i = \sum a_{ij} f_{ij}^h,$$

where $f_{ij} \in I$ .Since f_{ij}^h's are homogeneous and $I^h = \langle f_{ij}^h \rangle$, I^h is a homogeneous ideal by Proposition 2.68.□

Definition 2.70 is not entirely satisfactory because it does not give us a finite generating set for the ideal I^h. Given a particular finite generating set $f_1,...,f_s$ for $I \subset k[x_1,...,x_n]$, it always true that $\langle f_1^h,...,f_s^h \rangle$ is a homogeneous ideal contained in I^h. As the next example shows, however, I^h can be strictly larger than $\langle f_1^h,...,f_s^h \rangle$.

Example 2.72 Let $I = \langle f_1, f_2 \rangle = \langle y - x^2, z - x^3 \rangle$, the ideal of the twisted cubic in $\mathbb{R}^3$. The homogenization of f_1 and f_2 gives $J = \langle yt - x^2, zt^2 - x^3 \rangle$ in $\mathbb{R}[t,x,y,z]$. To prove $J \neq I^h$, consider the polynomial

$$f_3 = f_2 - xf_1 = z - x^3 - x(y - x^2) = z - xy \in I.$$

Then $f_3^h = tz - xy$ is a homogeneous polynomial of degree 2 in I^h. Since the generators of J are also homogeneous, of degree 2 and 3 respectively, if $f_3^h \in I^h$, then

f_3^h should be constant multiple of f_1^h by Lemma 2.69. Since this is clearly false, $f_3^h \notin J$ and , thus, $J \neq I^h$.

Definition 2.73 Let $I = \langle f_1, ..., f_t \rangle$ be an ideal in $k[x_1, ..., x_n]$. If the homogenization of I, $I^h = \langle f_1^h, ..., f_t^h \rangle$, then $\{f_1, ..., f_t\}$ is said to be a homogeneous basis for I.

Proposition 2.74 [7] Assume $\{g_1, ..., g_s\}$ is a Gröbner basis for an ideal I with respect to a graded monomial order $\succ$ in $k[x_1, ..., x_n]$. Then $\{g_1, ..., g_s\}$ is a homogeneous basis for I. Note that grlex and grevlex are graded monomial orders, whereas lex is not.

Example 2.75 Let us once again take the ideal of the twisted cubic in $\mathbb{R}^3$, $I = \langle f_1, f_2 \rangle = \langle z - x^3, y - x^2 \rangle$. Using the graded lexicographic order with $x > y > z$, a Gröbner basis of I can be as follows:

Let $G = \{x^3 - z, x^2 - y\}$ and $f_1 = x^3 - z$, $f_2 = x^2 - y$

$$\begin{aligned} S(f_1, f_2) &= \frac{x^3}{x^3}(x^3 - z) - \frac{x^3}{x^2}(x^2 - y) \\ &= xy - z \;. \end{aligned}$$

Thus $\overline{S(f_1, f_2)}^G = xy - z$, then $f_3 = xy - z$.

We have $G = \{f_1, f_2, f_3\}$. Then, $\overline{S(f_1, f_2)}^G = 0$. Next pair:

$$\begin{aligned} S(f_1, f_3) &= \frac{x^3 y}{x^3}(x^3 - z) - \frac{x^3 y}{xy}(xy - z) \\ &= z.f_2. \end{aligned}$$

Thus, $\overline{S(f_1, f_3)}^G = 0$ and next pair:

$$S(f_2, f_3) = \frac{x^2y}{x^2}(x^2 - y) - \frac{x^2y}{xy}(xy - z)$$
$$= xz - y^2.$$

Thus $\overline{S(f_2, f_3)}^G = xz - y^2$, then $f_4 = xz - y^2$.

We have $G = \{f_1, f_2, f_3, f_4\}$. Then, $\overline{S(f_2, f_3)}^G = 0$. Next pair:

$$S(f_3, f_4) = \frac{xyz}{xy}(xy - z) - \frac{xyz}{xz}(xz - y^2)$$
$$= y^3 - z^2$$

Thus $\overline{S(f_3, f_4)}^G = y^3 - z^2$, then $f_5 = y^3 - z^2$.

We have $G = \{f_1, f_2, f_3, f_4, f_5\}$. Then, $\overline{S(f_3, f_4)}^G = 0$

The other remainders of $S - polynomials$ are zero. Therefore, $G = \{f_1, f_2, f_3, f_4, f_5\}$ is a Gröbner basis for I. Since $LT(f_1) = x^3$ is divisible by $LT(f_2) = x^2$, $G' = \{x^2 - y, xy - z, xz - y^2, y^3 - z^2\}$ is a minimal Gröbner basis, and it also a homogeneous basis for I.

CHAPTER 3

SOLVING POLYNOMIAL EQUATIONS

In this chapter we will discuss several approaches to solving systems of polynomial equations. First, we will discuss a straightforward approach based on the eliminiation properties of lexicographic Gröbner bases.

3.1 Solving Equations via Gröbner Bases

The central problem of this chapter, finding the solutions of system of polynomial equations $f_1(x_1,...,x_n) = ... = f_s(x_1,...,x_n) = 0$ over $\mathbb{C}$ or $\mathbb{R}$, rephrases in fancier language to find the points of the variety $V(I)$, where I is the ideal generated by $f_1,...,f_s$.We assume that the systems of equations we are dealing with are in the variables $x_1,...,x_n$ with lexicographic order $x_1 > ... > x_n$. We begin by this definition:

Definition 3.1 Given $I = \langle f_1,...,f_s \rangle \subset k[x_1,...,x_n]$ the *ith* elimination ideal I_i is the ideal of $k[x_{i+1},...,x_n]$ defined by $I_i = I \cap k[x_{i+1},...,x_n]$.

For example; let $I = \langle x^2 + y^2, x^2 - z^3 \rangle \subset k[x, y, z]$, show that $y^3 + z^3$ is in the first elimination ideal I_1.

$$\begin{aligned} I_1 &= (x^2 + y^2) - (x^2 - z^3) \\ &= y^2 + z^3. \end{aligned}$$

Thus, I_i consists of all consequences of $f_1(x_1,...,x_n) = ... = f_s(x_1,...,x_n) = 0$ which eliminate the variables $x_1,...,x_i$. We see that eliminating $x_1,...,x_i$ means finding nonzero polynomials in the *ith* elimination ideal I_i and significance of Gröbner Bases for solving system of equations stems from the fact that, for Gröbner bases, it is simple to construct all of the elimination ideals. During the construction of Gröbner bases, variables are eliminated successively. Also, the order of elimination corresponds to the ordering of variables: x_1 is eliminated first, then x_2 is eliminated, and so on.

Definition 3.2 A point $(a_{l+1},...,a_n) \in V(I_l) \subset k^{n-l}$ is called a partial solution. Any solution $(a_1,...,a_n) \in V(I) \subset k^n$ truncates to a partial solutions, but the converse may fail-not all partial solutions extend to solutions.

This is where the Extension Theorem comes in. To prepare for the statement, note that each f in I_{l-1} can be written as a polynomial in x_l, whose coefficients are polynomials in $x_{l+1},...,x_n$:

$$f = c_q(x_{l+1},...,x_n)x_l^q + ... + c_0(x_{l+1},...,x_n).$$

We call c_q the leading coefficient polynomial of f if x_l^q is the highest power of x_l apperring in f.

Theorem 3.3 [The Extension Theorem] If k is algebraically closed , then a partial solutions $(a_{l+1},...,a_n)$ in $V(I_l)$ extends to $(a_l, a_{l+1},...,a_n)$ in $V(I_{l-1})$ provided that the leading coefficient polynomials of the elements of a *lex* Gröbner basis for I_{l-1} do not all vanish at $(a_{l+1},...,a_n)$.

To solve a system F of polynomial equations (Which determines the ideal $I = \langle F \rangle$). We proceed as follows:

(i) Compute the Göbner basis, G, of I with respect to the lex order.

(ii) Find the roots of generator in x_n by applying one-variable techniques.

(iii) Apply back substitution to find the roots of all generators in G.

(iv) Roots of generators in G are extended to solutions of the original equations.

First let us decide whether the system F has any solutions in $k[x_1,...,x_n]$.

Theorem 3.4 Let G be a reduced Gröbner basis of I. F is solvable in $k[x_1,...,x_n]$ if and only if $1 \notin G$.($1 \in G$ implies that the equation $1=0$ has a solution whch is a contradiction).

For example; let $I = \langle F \rangle = \langle xy^2, x-1, y-1 \rangle$. F is not solvable since $G = \{1\}$.

And let $I = \langle F \rangle = \langle xy^2, y-1 \rangle$. F is solvable since $G = \{x-1, y-1\}$.

Now suppose that the system F is solvable. We want to determine whether there are finitely or infinitely many solution of the system F. In the other words, whether or not the ideal I is zero-dimensional.

We now show how Gröbner bases can be applied to solving system of polynomial equations. Consider the polynomial equations

$$\begin{aligned} xy - 2y &= 0 \\ 2y^2 - x^2 &= 0. \end{aligned}$$

To solve these equations, we first compute a Gröbner basis for the ideal they generate using Mathematica:

In[1]:= GroebnerBasis[{x*y - 2*y, 2*y^2 - x^2}, {y, x}]

Out[1]= {-2 x^2 + x^3 , -2 y + x y, -x^2 + 2 y^2 }

By the fact that F and G generate the same ideal, F and G have the same solution. The elimination property of Gröbner basis guarantees, that, in case G as only finitely many solutions, G contains a univarete polynomial in x. Note that, here we use the lexicographic order with $y > x$. In our example, the univarete polynomial in x contained in G is

$$-2x^2 + x^3.$$

We now can solve this polynomial for x:

```
In[2]:= Solve[-2*x^2 + x^3 == 0, x]

Out[2]= {{x -> 0}, {x -> 0}, {x -> 2}}
```

This mean: $x_1 = 0, x_2 = 0, x_3 = 2$.

If we now plug in, say x_1, x_2 and x_3 in the second and third polynomial of G, we obtained:

```
In[3]:= x = 0;

In[4]:= Solve[-2*y + x*y == 0, y]

Out[4]= {{y -> 0}}

In[5]:= Solve[-x^2 + 2*y^2 == 0, y]

Out[5]= {{y -> 0}, {y -> 0}}

In[6]:= x = 2;

In[7]:= Solve[-2*y + x*y == 0, y]

Out[7]= {{}}

In[8]:= Solve[-x^2 + 2*y^2 == 0, y]

Out[8]= {{y -> -Sqrt[2]}, {y -> Sqrt[2]}}
```

We have the three points as following:

$$(0,0),(2,-\sqrt{2}),(2,\sqrt{2})).$$

In this way, we can obtain all the solutions of G and, hence, of F.

Example 3.5 Consider the system of equations

$$x^2+y^2+z^2=4$$
$$x^2+2y^2=5$$
$$xz=1.$$

How many solutions are there in $\mathbb{R}^3$?

In[1]:= GroebnerBasis[{x^2 + y^2 + z^2 - 4, x^2 + 2*y^2 - 5, x*z - 1}, {x, y, z}]

Out[1]= {1 - 3 z^2 + 2 z^4 , -1 + y^2 - z^2 , x - 3 z + 2 z^3 }

In[2]:= Factor[1 - 3*z^2 + 2*z^4]

Out[2]= (-1 + z) (1 + z) (-1 + 2 z^2)

In[3]:= Solve[1 - 3*z^2 + 2*z^4 == 0, z]

Out[3]= {{z -> -1}, {z -> 1}, {z -> -1/Sqrt[2]}, {z -> 1/Sqrt[2]}

Where by the Elimination Thoerem, the first elimination ideal $I_1 = I \cap \mathbb{C}[y,z]$ is

$$y^2-z^2-1$$
$$2z^4-3z^2+1.$$

Since the coefficient of y^2 in the first polynomial is a nonzero constant, every partial solution in $V(I_1)$. There are eight such points in all. Now we will these solutions:

In[4]:= z = 1;

In[5]:= {-1 + y^2 - z^2, x - 3*z + 2*z^3}

Out[5]= {-2 + y^2 , -1 + x}

In[6]:= Solve[-2 + y^2 == 0, y]

Out[6]= {{y -> -Sqrt[2]}, {y -> Sqrt[2]}}

In[7]:= Solve[-1 + x == 0, x]

Out[7]= {{x -> 1}}

In[8]:= z = -1;

In[9]:= {-1 + y^2 - z^2, x - 3*z + 2*z^3}

Out[9]= {-2 + y^2 , 1 + x}

In[10]:= Solve[-2 + y^2 == 0, y]

Out[10]= {{y -> -Sqrt[2]}, {y -> Sqrt[2]}}

In[11]:= Solve[-1 + x == 0, x]

Out[11]= {{x -> 1}}

In[12]:= z = 1/Sqrt[2];

In[13]:= {-1 + y^2 - z^2, x - 3*z + 2*z^3}

Out[13]= {-(3/2) + y^2 , -Sqrt[2] + x}

In[14]:= Solve[(-3/2) + y^2 == 0,y]

Out[14]= {{y -> -Sqrt[3/2]}, {y -> Sqrt[3/2]}}

In[15]:= Solve[-Sqrt[2] + x == 0, x]

Out[15]= {{x -> Sqrt[2]}}

In[16]:= z = -1/Sqrt[2];

In[17]:= Solve[(-3/2) + y^2 == 0, y]

Out[18]= {{y -> -Sqrt[3/2]}, {y -> Sqrt[3/2]}}

In[19]:= Solve[-Sqrt[2] + x == 0, x]

Out[20]= {{x -> Sqrt[2]}}

Finally we have

$(1,\pm\sqrt{2},1),(-1,\pm\sqrt{2},-1),(\sqrt{2},\pm\sqrt{3/2},1/\sqrt{2}),(-\sqrt{2},\pm\sqrt{3/2},-1/\sqrt{2})$.

The system of polynomial equations in above example is relatively simple because the coordinates of the solutions can all be expressed in terms of square roots of rational numbers. Unfortunately, general systems of polynomial equations are rarely this nice. We will see this case by taking the system of equations given in Example 3.4 and change the first term in the fist polynomial from x^2 to x^5.

Example 3.6 Consider the system of equations

$$\begin{aligned} x^5 + y^2 + z^2 &= 4 \\ x^2 + 2y^2 &= 5 \\ xz &= 1 \end{aligned}$$

How many solutions are there in $\mathbb{R}^3$; how many are there in $\mathbb{C}^3$?

In[1]:= f1 = x^5 + y^2 + z^2 - 4;

In[2]:= f2 = x^2 + 2*y^2 - 5;

In[3]:= f3 = x*z - 1;

In[4]:= GroebnerBasis[{f1, f2, f3}, {x, y, z}]

Out[4]= $\{2 - z^3 - 3z^5 + 2z^7, -10 + 4y^2 + z + 3z^3 - 2z^5, 2x - z^2 - 3z^4 + 2z^6\}$

In[5]:= Solve[(-1 + z)(-2 - 2*z - 2*z^2 - z^3 - z^4 + 2*z^5 + 2*z^6) == 0, z]

Out[5]= {{z -> 1}, {z -> Root[-2 - 2 #1 - 2 $\#1^2$ - $\#1^3$ - $\#1^4$ + 2 $\#1^5$ + 2 $\#1^6$ & , 1]},

> {z -> Root[-2 - 2 #1 - 2 $\#1^2$ - $\#1^3$ - $\#1^4$ + 2 $\#1^5$ + 2 $\#1^6$ & , 2]},

> {z -> Root[-2 - 2 #1 - 2 $\#1^2$ - $\#1^3$ - $\#1^4$ + 2 $\#1^5$ + 2 $\#1^6$ & , 3]},

> {z -> Root[-2 - 2 #1 - 2 $\#1^2$ - $\#1^3$ - $\#1^4$ + 2 $\#1^5$ + 2 $\#1^6$ & , 4]},

> {z -> Root[-2 - 2 #1 - 2 $\#1^2$ - $\#1^3$ - $\#1^4$ + 2 $\#1^5$ + 2 $\#1^6$ & , 5]},

> {z -> Root[-2 - 2 #1 - 2 $\#1^2$ - $\#1^3$ - $\#1^4$ + 2 $\#1^5$ + 2 $\#1^6$ & , 6]},

In[6]:= NSolve[(-1 + z)(-2 - 2*z - 2*z^2 - z^3 - z^4 + 2*z^5 + 2*z^6) == 0, z]

Out[6]={{z -> -1.39505},{z -> -0.61526 - 0.608323 I},{z -> -0.61526 + 0.608323 I},

> {z -> 0.210764 - 0.866518 I}, {z -> 0.210764 + 0.866518 I}, {z -> 1.}, {z -> 1.20404}}

In[7]:= z = -1.39505;

```
In[8]:= {2 - z^3 - 3 *z^5 + 2*z^7, -10 + 4 *y^2 + z + 3 *z^3 - 2 *z^5,
        2* x - z^2 - 3* z^4 + 2 *z^6}
```

Out[8]= {0.0000816876, -8.97238 + 4y^2 , 1.43358 + 2 x}

```
In[9]:= Solve[-8.97238 + 4*y^2 == 0, y]
Out[9]= {{y -> -1.4977}, {y -> 1.4977}}
In[10]:= Solve[1.43358 + 2*x == 0, x]
Out[10]= {{x -> -0.71679}}
In[11]:= z = -0.61526 - 0.608323 I;
In[12]:= {2 - z^3 - 3 *z^5 + 2*z^7, -10 + 4 *y^2 + z + 3 *z^3 - 2 *z^5,
        2* x - z^2 - 3* z^4 + 2 *z^6}
```

Out[12]= {-3.50085 .10^{-6} + 3.31944. 10^{-6} I, (-9.96971 - 2.67148 I) + 4 y^2, (1.64376 - 1.62523 I) + 2 x}

```
In[13]:= Solve[(-9.96971 - 2.67148 I) + 4* y^2 == 0, y]
Out[13]= {{y -> -1.59261 - 0.209678 I}, {y -> 1.59261 + 0.209678 I}}
In[14]:= Solve[(1.64376 - 1.62523 I) + 2 *x == 0, x]
Out[14]= {{x -> -0.82188 + 0.812615 I}}
In[15]:= z = -0.61526 + 0.608323 I;
In[16]:= {2 - z^3 - 3 *z^5 + 2*z^7, -10 + 4 *y^2 + z + 3 *z^3 - 2 *z^5,
        2* x - z^2 - 3* z^4 + 2 *z^6}
```

Out[16]= {-3.50085 .10^{-6} - 3.31944.10^{-6} I, (-9.96971 + 2.67148 I) + 4 y^2 , (1.64376 + 1.62523 I) + 2 x}

```
In[17]:= Solve[(-9.96971 - 2.67148 I) + 4* y^2 == 0, y]
Out[17]= {{y -> -1.59261 - 0.209678 I}, {y -> 1.59261 + 0.209678 I}}
```

In[18]:= Solve[(1.64376 - 1.62523 I) + 2 *x == 0, x]

Out[18]= {{x -> -0.82188 + 0.812615 I}}

In[19]:= z = 0.210764 - 0.866518 I;

In[20]:= {2 - z^3 - 3 *z^5 + 2*z^7, -10 + 4 *y^2 + z + 3 *z^3 - 2 *z^5,

2* x - z^2 - 3* z^4 + 2 *z^6}

Out[20]= {3.59222. 10^{-6} + 5.51216 .10^{-6} I, (-12.2339 + 1.15505 I) + 4 y^2 ,

(-0.530047 - 2.17916 I) + 2 x}

In[21]:= Solve[(-12.2339 + 1.15505 I) + 4* y^2 == 0, y]

Out[21]= {{y -> -1.75079 + 0.0824662 I}, {y -> 1.75079 - 0.0824662 I}}

In[22]:= Solve[(-0.530047 - 2.17916 I) + 2* x == 0, x]

Out[22]= {{x -> 0.265024 + 1.08958 I}}

In[23]:= z = 0.210764 + 0.866518 I;

In[24]:= {2 - z^3 - 3 *z^5 + 2*z^7, -10 + 4 *y^2 + z + 3 *z^3 - 2 *z^5,

2* x - z^2 - 3* z^4 + 2 *z^6}

Out[24]= {3.59222 .10^{-6} - 5.51216 .10^{-6} I, (-12.2339 - 1.15505 I) + 4 y^2,

(-0.530047 + 2.17916 I) + 2 x}

In[25]:= Solve[(-12.2339 - 1.15505 I) + 4* y^2 == 0, y]

Out[25]= {{y -> -1.75079 - 0.0824662 I}, {y -> 1.75079 + 0.0824662 I}}

In[26]:= Solve[(-0.530047 + 2.17916 I) + 2 *x == 0, x]

Out[26]= {{x -> 0.265024 - 1.08958 I}}

In[27]:= z = 1.;

In[28]:= {2 - z^3 - 3 *z^5 + 2*z^7, -10 + 4 *y^2 + z + 3 *z^3 - 2 *z^5,

2* x - z^2 - 3* z^4 + 2 *z^6}

Out[28]= {0., -8. + 4 y^2 , -2. + 2 x}

In[29]:= Solve[-8. + 4* y^2 == 0, y]

Out[29]= {{y -> -1.41421}, {y -> 1.41421}}

In[30]:= Solve[-2. + 2 x == 0, x]

Out[30]= {{x -> 1.}}

In[31]:= z = 1.20404;

In[32]:= {2 - z^3 - 3 *z^5 + 2*z^7, -10 + 4 *y^2 + z + 3 *z^3 - 2 *z^5,

2* x - z^2 - 3* z^4 + 2 *z^6}

Out[32]= {-0.000016529, -8.6204 + 4 y^2 , -1.66109 + 2 x}

In[33]:= Solve[-8.6204 + 4 *y^2 == 0, y]

Out[33]= {{y -> -1.46803}, {y -> 1.46803}}

In[34]:= Solve[-1.66109 + 2 *x == 0]

Out[34]= {{x -> 0.830545}}

Finally, we have

> {x -> 1., y -> -1.41421, z -> 1.}, {x -> -0.821879 - 0.812613 I, y -> 1.59261 - 0.209678 I,

> z -> -0.61526 + 0.608323 I}, {x -> -0.821879 + 0.812613 I, y -> 1.59261 + 0.209678 I,

> z -> -0.61526 - 0.608323 I}, {x -> 0.265021 + 1.08958 I, y -> -1.75079 + 0.0824661 I,

> z -> 0.210764 - 0.866518 I}, {x -> 0.265021 - 1.08958 I, y -> -1.75079 - 0.0824661 I,

> z -> 0.210764 + 0.866518 I}, {x -> 0.265021 + 1.08958 I, y -> 1.75079 - 0.0824661 I,

> z -> 0.210764 - 0.866518 I}, {x -> 0.265021 - 1.08958 I, y -> 1.75079 + 0.0824661 I,

> z -> 0.210764 + 0.866518 I}, {x -> -0.821879 + 0.812613 I, y -> -1.59261 - 0.209678 I,
> z -> -0.61526 - 0.608323 I}, {x -> -0.821879 - 0.812613 I, y -> -1.59261 + 0.209678 I,
> z -> -0.61526 + 0.608323 I}, {x -> -0.716819, y -> -1.49769, z -> -1.39505},
> {x -> 1., y -> 1.41421, z -> 1.}, {x -> 0.830536, y -> 1.46803, z -> 1.20404}}

There are six solutions in $\mathbb{R}^3$ and eight solutions in $\mathbb{C}^3$.

The solution of problem for G can often be easily translated back into a solution of the problem for F. Hence, the worst-case complexity of any algorithm that computes Gröbner bases in fully generality must be high. Thus, examples in three or four may already fail to terminate in reasonable time or exceed available memory even on very fast machines. For example, trying to find a Gröbner basis, w.r.t to a lexicographic ordering, for the set

$$\{xy^3 - 2yz - z^2 + 13, y^2 - x^2 z + xz^2 + 3, z^2 x - y^2 x^2 + xy + y^3 + 12\}$$

may already exhaust your computer resources.

3.2 Solving Equations via Eigenvalues and Eigenvectors

In this section, we lay out a path from solving a set of polynomial equations problems to eigenvalue problems. The main tool we need are the Finiteness Thorem.

Theorem 3.7 [Finiteness Theorem] Let $k \in \mathbb{C}$ be a field, and $I \subset k[x_1, \ldots x_n]$ be an ideal. Then the following conditions are equivalent:

(i) The algebra $A = k[x_1, \ldots, x_n]/I$ is finite-dimensional over k.

(ii) The variety $V(I) \subset \mathbb{C}^n$ is a finite set.

(iii) If G is a Gröbner basis for I, then for each $i, 1 \le i \le n$, there is an $m_i \ge 0$ such that $x_i^{m_i} = LT(g)$ for some $g \in G$.

Thus,

A is a finite-dimensional algebra $\Leftrightarrow$ I is a zero-dimansional ideal.

When the system has only finitely many solutions, i.e, when $V(I)$ is a finite set, the Finiteness Theorem says that I is a zero-dimensional ideal and algebra $A = \mathbb{C}[x_1,...,x_n]/I$ is a finite-dimensional vector space over $\mathbb{C}$. The structure of A in this case to evaluate an arbitrary polynomial f at the point of $V(I)$; in particular evaluating the polynomials $f = x_i$ gives the coordinates of $V(I)$ turn out to be eigenvalues of certain linear mappings on A, and the remainder of the section discusses techniques for evaluating them. We begin with the easy observation that given a polynomial $f \in \mathbb{C}[x_1,...,x_n]$, we can use multiplication to define a linear map m_f from $A = \mathbb{C}[x_1,...,x_n]/I$ to itself. More precisely, f gives the $Coset[f] \in A$, and we define $m_f : A \to A$ by the rule: if $[g] \in A$, then

$$m_f([g]) = [f][g] = [fg] \in A.$$

Then m_f has the following basic properties:

Proposition 3.8 Let $f \in \mathbb{C}[x_1,...,x_n]$. Then,

(i) The map m_f is linear mapping from A to A.

(ii) We have $m_f = m_g$ exactly when $f - g \in I$.

Thus two polynomials give the same liner map if and only if they different by an element of I. In particular, m_f is the zero map exactly when $f \in I$.

Proof. The proof of part (i) is just the distrubutive law for multiplication over addition in ring A. If $[g],[h] \in A$ and $c \in k$, then

$$
\begin{aligned}
m_f(c[g]+[h]) &= [f].(c[g]+[h]) \\
&= c[f][g]+[f][h] \\
&= cm_f([g])+m_f([h]).
\end{aligned}
$$

Part (ii) is equally easy. Since $[1]\in A$ is amultiplicative identity, if $m_f = m_g$, then

$$[f]=[f][1]=m_f([1])=[g][1]=[g],$$

so $f-g\in I$. Conversely, if $f-g\in I$, then

$[f]=[g]$ in A, so $m_f = m_g$.□

Since A is a finite-dimensional vector space over $\mathbb{C}$, we can represent m_f by its matrix with respect to a basis. On the other hand an important observation is the remainders are linear combinations of the monomials $x^\alpha \notin \langle LT(I)\rangle$ in this vector space structure. Thise set of monomials is linearly independet in A, it can be regarded as a basis of A. In other words, the monomials $B=\{x^\alpha : x^\alpha \notin \langle LT(I)\rangle$ form a basis of A (more precisely, their cosets are a basis). We will refer to elements of B a basis monomials. In the literature, basis monomials are often called standart monomials. The following example illustrate how to compute in A using basis monomials.

Example 3.9 Let $G=\{x^2+3xy/2+y^2/2-3x/2-3y/2, xy^2-x, y^3-y\}$ using the grevllex order with $x>y$. G is a Gröbner basis for the ideal $I=\langle G\rangle\subset\mathbb{C}[x,y]$ generated by G.

We have $\langle LT(I)\rangle = \langle x^2, xy^2, y^3\rangle$. The only monomials not lying in this ideal are those in

$$B=\{1,x,y,xy,y^2\}.$$

so that by the above observation, these five monomials form a vector space basis for $A = \mathbb{C}[x, y]/I$ over $\mathbb{C}$.

The multiplication table for the elements of the basis B is:

$\cdot$	1	x	y	xy	y^2
1	1	x	y	xy	y^2
x	x	α	xy	β	x
y	y	xy	y^2	x	y
xy	xy	β	x	α	xy
y^2	y^2	x	y	xy	y^2

Where

$$x.x = x^2 \xrightarrow{G} -3xy/2 - y^2/2 + 3x/2 + 3y/2 = \alpha$$

and

$$x.xy = x^2 y \xrightarrow{G} 3xy/2 - 3x/2 + 3y^2/2 - y/2 = \beta .$$

Similarly, $x.y^2 \xrightarrow{G} x, y.y \xrightarrow{G} y^2$ and $y.y^3 \xrightarrow{G} y$.

Then A is finite-dimensional as a vector space over $\mathbb{C}$. We have a $5x5$ matrix whose jth column is the vector of coefficients in the expansion in terms of B of the image under m_f of the jth basis monomial. With $f = x$;

$$m_x(1) = \overline{x.1}^G = 0.1 + 1.x + 0.y + 0.xy + 0.y^2$$
$$m_x(x) = \overline{x^2}^G = 0.1 + \frac{3}{2}.x + \frac{3}{2}.y - \frac{3}{2}.xy - \frac{1}{2}.y^2$$
$$m_x(y) = \overline{x.y}^G = 0.1 + 0.x + 0.y + 1.xy + 0.y^2 \qquad .$$
$$m_x(xy) = \overline{x^2.y}^G = 0.1 - \frac{3}{2}.x - \frac{1}{2}.y + \frac{3}{2}.xy + \frac{3}{2}.y^2$$
$$m_x(y^2) = \overline{x.y^2}^G = 0.1 + 1.x + o.y + 0.xy + 0.y^2$$

We obtained

$$m_x = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 3/2 & 0 & -3/2 & 1 \\ 0 & 3/2 & 0 & -1/2 & 0 \\ 0 & -3/2 & 1 & 3/2 & 0 \\ 0 & -1/2 & 0 & 3/2 & 0 \end{pmatrix}.$$

For $f = y$;

$$m_y(1) = \overline{y.1}^G = 0.1 + 0.x + 1.y + 0.xy + 0.y^2$$
$$m_y(x) = \overline{y.x}^G = 0.1 + 0.x + 0.y + 1.xy + 0.y^2$$
$$m_y(y) = \overline{y^2}^G = 0.1 + 0.x + 0.y + 0.xy + 1.y^2 \qquad .$$
$$m_y(xy) = \overline{x.y^2}^G = 0.1 + 1.x + 0.y + 0.xy + 0.y^2$$
$$m_y(y^2) = \overline{y^3}^G = 0.1 + 0.x + 1.y + 0.xy + 0.y^2$$

We obtained

$$m_y = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Proposition 3.10 Let f, g be elements of the algebra A. Then

(i) $\quad m_{f+g} = m_f + m_g$

(ii) $m_{f.g} = m_f.m_g$ (where the product on right means composition of linear operators or matrix multiplication).

This proposition says that the map sending $f \in \mathbb{C}[x_1,...,x_n]$ to the matrix m_f defines a ring homomorphism from $f \in \mathbb{C}[x_1,...,x_n]$ to the ring $M_{dxd}(\mathbb{C})$ of dxd matrices, where d is the dimension of A as a $\mathbb{C}-$vector space. Furthermore, part(i) of proposition 3.8 and Fundamental Theorem of Homomorphisms show that $[f] \to m_f$ induces a one-to-one homomorphism $A \to M_{dxd}(\mathbb{C})$.

For use later, we also point out a corollary of proposition 3.10. Let

$$h(t) = \sum_{i=0}^{m} c_i t^i \in \mathbb{C}[t]$$

be a polynomial. The expression $h(f) = \sum_{i=0}^{m} c_i f^i$ makes sense as an element of $f \in \mathbb{C}[x_1,...,x_n]$. Similarly $h(m_f) = \sum_{i=0}^{m} c_i (m_f)^i$ is a well-defined matrix.

Corollary 3.11 In the situation of above proposition 3.10, let $h \in \mathbb{C}[x_1,...,x_n]$. Then

$$m_{h(f)} = h(m_f).$$

Recall that a polynomial $f \in \mathbb{C}[x_1,...,x_n]$ gives the $Coset[f] \in A$. Since A is finite-dimensional, as we noted above for $f = x_i$, the set $\{1,[f],[f]^2,...\}$ must be linearly dependent in vector space structure of A. In other words, there is a linear combination

$$\sum_{i=0}^{m} c_i [f]^i = [0]$$

in A, where $c_i \in \mathbb{C}$ are not all zero. By the definition of the quotient ring, this is equivalent to stay that

$$\sum_{i=0}^{m} c_i f^i \in I .$$

Hence $\sum_{i=0}^{m} c_i f^i$ vanishes at every point of $V(I)$. We are looking for the points in $V(I)$, I a zero-dimensional ideal. Let $h(t) \in \mathbb{C}[t]$, and let $f \in \mathbb{C}[x_1,...,x_n]$. By corollary 3.11,

$$h(m_f) = 0 \Leftrightarrow h([f]) = [0]$$

in A. The polynomials h such that $h(m_f) = 0$ form an ideal in $\mathbb{C}[t]$. The nonzero monic generator h_M of the ideal I_M called the minimal polynomial of M. By the basic properties of ideals in $k[t]$, if h is any polynomial with $h(M) = 0$, the minimal polynomial h_M divides h. In particular, the Cayley-Hamilton Theorem from linear algebra tell us that h_M divides the characteristic polynomial of M. As a consequence if $k = \mathbb{C}$, the roots of h_M are eigenvalues of M. Furthermore, all eigenvalues of M occur as roots of the minimial polynomial.

Let h_f denote the minimal polynomial of the mutiplication operator m_f on A. Then we have three interesting sets of numbers:

(i) the roots of the equation $h_f(t) = 0$,

(ii) the eigenvalues of the matrix m_f, and

(iii) the values of the function f on $V(I)$, the set of points we are looking for.

Theorem 3.12 Let $I \subset \mathbb{C}[x_1,...,x_n]$ be zero-dimensional, let $f \in \mathbb{C}[x_1,...,x_n]$, and let h_f be the minimal polynomial of m_f on $A = [x_1,...,x_n]/I$. Then, for $\lambda \in \mathbb{C}$, the following are equivalent:

(i) λ is a root of the equation $h_f(t) = 0$,

(ii) λ is an eigenvalue of the matrix m_f, and

(iii) λ is an value of the function f on $V(I)$.

Crollary 3.13 Let $I \subset \mathbb{C}[x_1,...,x_n]$ be zero-dimensional ideal. Then the eigenvalues of the multiplication operator m_{x_i} on A coincide with the x_i-coordinates of the points of $V(I)$. Moreover, substituting $t = x_i$ in the minimal polynomial h_{x_i} yields the unique monic generator of the elimination ideal $I \cap \mathbb{C}[x_i]$.

Corollary 3.13 indicates that it is possible to solve equations by computing eigenvalues of the multiplication operators m_{x_i}.

In elementary linear algebra, eigenvalues of a matrix M are usually determined by solving the characteristic polynomial equation:

$$\det(M - tI) = 0.$$

The degree of the polynomial on the left hand side is the size of matrix M. But computing $\det(M - tI)$ for large matrices is large job itself. Exact solutions of polynomial equations of high degree over $\mathbb{R}$ or $\mathbb{C}$ can be hard to come by, so characteristic polynomials is almost never used in practice. So other metods are needed.We will apply the ideas sketched above to find approximations to the complex solutions of the system in Example 3.9;

```
> with(Groebner):
> gb:=gbasis({x^2+3*x*y/2+y^2/2-3*x/2-3*y/2,x*y^2-x,y^3-y},tdeg(x,y));
```

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

```
> (ns,rv):=SetBasis(gb,tdeg(x,y)):
> ns;
```

$$[1, y, x, y^2, x\,y]$$

```
> nops(ns);
```

$$5$$

```
> Mx:=MulMatrix(x,ns,rv,gb,tdeg(x,y));
```

$$Mx := \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & \frac{3}{2} & \frac{3}{2} & -\frac{1}{2} & -\frac{3}{2} \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{3}{2} & \frac{3}{2} & \frac{3}{2} \end{bmatrix}$$

```
> with(linalg):
> eigenvalues(Mx);
```

$$0, 2, -1, 1, 1$$

```
> evalf((%));
```

$$0., 2., -1., 1., 1.$$

```
> with(LinearAlgebra):
> mp:=MinimalPolynomial(Mx,t);
```

$$mp := 2\,t - t^2 - 2\,t^3 + t^4$$

```
> solve(mp);
```

$$0, -1, 1, 2$$

```
> evalf((%));
```

$0., -1., 1., 2.$

```
> My:=MulMatrix(y,ns,rv,gb,tdeg(x,y));
```

$$My := \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

```
> with(linalg):
> eigenvalues(My);
```

$0, 1, -1, 1, -1$

```
> evalf((%));
```

$0., 1., -1., 1., -1.$

```
> mp:=MinimalPolynomial(My,t);
```

$mp := -t + t^3$

```
> solve(mp);
```

$0, 1, -1$

```
> evalf((%));
```

$0., 1., -1.$

We have $(0,0),(-1,1),(1,1),(1,-1),(2,-1)$.

Example 3.14 Let the system of equations

$$\begin{aligned} x^2 - 2xz + 5 &= 0 \\ xy^2 + yz + 1 &= 0 \\ 3y^2 - 8xz &= 0. \end{aligned}$$

How many solutions are there in $\mathbb{R}^3$; How many are there in $\mathbb{C}^3$.

First, compute a Gröbner basis to determine the monomial basis for the quotient algebra. We can use the grewlex (Maple tdeg) monomial order.

```
> with(Groebner):
gb:=gbasis({x^2-2*x*z+5,x*y^2+y*z+1,3*y^2-8*x*z},tdeg(x,y,z));
```

$$gb := [3\,y^2 - 8\,x\,z, x^2 - 2\,x\,z + 5, 415\,y\,z - 30\,y - 224\,z + 15 + 160\,z^3 + 12\,x - 160\,x\,z, -9\,x\,y + 18\,y\,z + 120\,z^2 - 120\,x + 1600\,x\,z + 240\,y\,z^2 + 240\,z, 3\,y\,z + 3 + 16\,x\,z^2 - 40\,z, -3\,x\,y + 40\,x\,y\,z + 6\,y\,z + 40\,z^2]$$

```
>  (ns,rv):=SetBasis(gb,tdeg(x,y,z)):
> ns;
```

$$[1, z, y, x, z^2, y\,z, x\,z, x\,y]$$

```
> nops(ns);
```

$$8$$

```
> Mx:=MulMatrix(x,ns,rv,gb,tdeg(x,y,z));
```

$$Mx := \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -5 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ -\frac{3}{16} & \frac{5}{2} & 0 & 0 & 0 & -\frac{3}{16} & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -\frac{3}{20} & 0 & \frac{3}{40} \\ -\frac{3}{8} & 0 & 0 & 0 & 0 & -\frac{3}{8} & 0 & 0 \\ 0 & 0 & -5 & 0 & -2 & -\frac{3}{10} & 0 & \frac{3}{20} \end{bmatrix}$$

```
> with(linalg):
eigenvalues(Mx);
```

$$RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 1\right), RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 2\right),$$
$$RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 3\right), RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 4\right),$$
$$RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 5\right), RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 6\right),$$
$$RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 7\right), RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 8\right)$$

```
> evalf({%});
```

$$\{0.9657124563, -1.100987715, 0.07664889706 + 2.243123348I, 0.07249081131 + 2.236999053I, -0.08150207886 + 0.9310707226I, -0.08150207886 - 0.9310707226I, 0.07249081131 - 2.236999053I, 0.07664889706 - 2.243123348I\}$$

```
> with(LinearAlgebra):
> mp := MinimalPolynomial(Mx,t);
```

$$mp := -\frac{375}{16} - \frac{27}{2}t^2 + \frac{15}{2}t^3 + \frac{355}{16}t^4 + \frac{3}{2}t^5 + \frac{157}{16}t^6 + t^8$$

```
> solve(mp);
```

$$RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 1\right), RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 2\right),$$
$$RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 3\right), RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 4\right),$$
$$RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 5\right), RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 6\right),$$
$$RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 7\right), RootOf\left(16\_Z^8 + 157\_Z^6 + 24\_Z^5 + 355\_Z^4 + 120\_Z^3 - 216\_Z^2 - 375, index = 8\right)$$

> evalf({%});

$$\{0.9657124563, -1.100987715, 0.07664889706 + 2.243123348I, 0.07249081131 + 2.236999053I, -0.08150207886 + 0.9310707226I, -0.08150207886 - 0.9310707226I, 0.07249081131 - 2.236999053I, 0.07664889706 - 2.243123348I\}$$

> My:=MulMatrix(y,ns,rv,gb,tdeg(x,y,z));

$$My := \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{8}{3} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{3}{40} & -\frac{20}{3} & \frac{3}{80} \\ -\frac{1}{2} & \frac{20}{3} & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -\frac{3}{20} & 0 & \frac{3}{40} \\ -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{bmatrix}$$

> with(linalg):

eigenvalues(My);

$$RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 1\right), RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 2\right),$$
$$RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 3\right), RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 4\right),$$
$$RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 5\right), RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 6\right),$$
$$RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 7\right), RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 8\right)$$

> evalf({%});

$$\{0.4612299831 - 0.4970273310 I, 2.349791604 - 0.04305868335 I, 0.4612299831 + 0.4970273310 I, -0.4657722908 + 0.4642093126 I, -2.812496056, -2.878002536, -0.4657722908 - 0.4642093126 I, 2.349791604 + 0.04305868335 I\}$$

> mp := MinimalPolynomial(My,t);

$$mp := \frac{80}{9} - \frac{4}{3}t^2 + \frac{400}{9}t^4 - \frac{20}{3}t^5 - \frac{157}{12}t^6 + t^7 + t^8$$

> solve(mp);

$$RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 1\right), RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 2\right),$$
$$RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 3\right), RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 4\right),$$
$$RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 5\right), RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 6\right),$$
$$RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 7\right), RootOf\left(36\_Z^8 + 36\_Z^7 - 471\_Z^6 - 240\_Z^5 + 1600\_Z^4 - 48\_Z^2 + 320, index = 8\right)$$

```
> evalf({%});
```

$$\{0.4612299831 - 0.4970273310 I, 2.349791604 - 0.0430586833 5I, 0.4612299831 + 0.4970273310 I, -0.4657722908 + 0.4642093126 I, -2.812496056, -2.878002536, -0.4657722908 - 0.4642093126 I, 2.349791604 + 0.04305868335 I\}$$

```
> Mz:=MulMatrix(z,ns,rv,gb,tdeg(x,y,z));
```

$$Mz := \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -\frac{3}{32} & \frac{7}{5} & \frac{3}{16} & -\frac{3}{40} & 0 & -\frac{83}{32} & 1 & 0 \\ 0 & -1 & 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{3}{40} & -\frac{20}{3} & \frac{3}{80} \\ -\frac{3}{16} & \frac{5}{2} & 0 & 0 & 0 & -\frac{3}{16} & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -\frac{3}{20} & 0 & \frac{3}{40} \end{bmatrix}$$

```
> with(linalg):
```

eigenvalues(Mz);

$$\frac{1}{2}\,\mathit{RootOf}\big(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, \mathit{index} = 1\big),$$
$$\frac{1}{2}\,\mathit{RootOf}\big(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, \mathit{index} = 2\big),$$
$$\frac{1}{2}\,\mathit{RootOf}\big(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, \mathit{index} = 3\big),$$
$$\frac{1}{2}\,\mathit{RootOf}\big(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, \mathit{index} = 4\big),$$
$$\frac{1}{2}\,\mathit{RootOf}\big(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, \mathit{index} = 5\big),$$
$$\frac{1}{2}\,\mathit{RootOf}\big(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, \mathit{index} = 6\big),$$
$$\frac{1}{2}\,\mathit{RootOf}\big(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, \mathit{index} = 7\big),$$
$$\frac{1}{2}\,\mathit{RootOf}\big(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, \mathit{index} = 8\big)$$

> evalf({%});

$$\{3.071618528, 0.07242265570 + 0.002103219128\,I, 0.07636377400 + 0.008344102200\,I, 0.07636377400 - 0.008344102200\,I, 0.07242265570 - 0.002103219128\,I, -0.2740045805 - 2.199127259\,I, -0.2740045805 + 2.199127259\,I, -2.821182227\}$$

> mp := MinimalPolynomial(Mz,t);

$$mp := -\frac{27}{20480} + \frac{9}{128} t - \frac{45}{32} t^2 + \frac{3991}{320} t^3 - \frac{157093}{3840} t^4 - \frac{77}{16} t^5$$
$$- \frac{1263}{320} t^6 + t^8$$

> solve(mp);

$$\frac{1}{2} RootOf\left(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, index = 1\right),$$
$$\frac{1}{2} RootOf\left(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, index = 2\right),$$
$$\frac{1}{2} RootOf\left(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, index = 3\right),$$
$$\frac{1}{2} RootOf\left(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, index = 4\right),$$
$$\frac{1}{2} RootOf\left(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, index = 5\right),$$
$$\frac{1}{2} RootOf\left(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, index = 6\right),$$
$$\frac{1}{2} RootOf\left(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, index = 7\right),$$
$$\frac{1}{2} RootOf\left(240\_Z^8 - 3789\_Z^6 - 9240\_Z^5 - 157093\_Z^4 + 95784\_Z^3 - 21600\_Z^2 + 2160\_Z - 81, index = 8\right)$$

> evalf({%});

{3.071618528, 0.07242265570 + 0.002103219128 I, 0.07636377400
+ 0.008344102200 I, 0.07636377400 − 0.008344102200 I,
0.07242265570 − 0.002103219128 I, −0.2740045805
− 2.199127259 I, −0.2740045805 + 2.199127259 I, −2.821182227}

We have :

> {x -> -0.0815021 - 0.931071 I, y -> 2.34979 + 0.0430587 I, z -> -0.274005 + 2.19913 I},

> {x -> -0.0815021 + 0.931071 I, y -> 2.34979 - 0.0430587 I, z -> -0.274005 - 2.19913 I},

> {x -> 0.0724908 - 2.237 I, y -> -0.465772 + 0.464209 I, z -> 0.0724227 - 0.00210322 I},

> {x -> 0.0724908 + 2.237 I, y -> -0.465772 - 0.464209 I, z -> 0.0724227 + 0.00210322 I},

> {x -> 0.0766489 - 2.24312 I, y -> 0.46123 - 0.497027 I, z -> 0.0763638 - 0.0083441 I},

> {x -> 0.0766489 + 2.24312 I, y -> 0.46123 + 0.497027 I, z -> 0.0763638 + 0.0083441 I},

> {x -> 0.965712, y -> -2.8125, z -> 3.07162}}

There are two solutions in $\mathbb{R}^3$ and six solutions in $\mathbb{C}^3$.

3.3 Solving Equations via Homogeneous Bases

We apply H-bases to the solving of polynomial systems by the Eigenmethod. More detail can be found in [12] and [13].

We consider polynomials in n variables $x_1,...,x_n$ with coefficients from a field k. For short, we write

$$\mathcal{P} := k[x_1,...,x_n].$$

Given a set $\mathcal{F} \subset \mathcal{P}$, the set

$$I := \{\sum_{f \in F} h_f f \mid h_f \in \mathcal{P}, \text{only finitely many } h_f \neq 0\}$$

is the ideal generated by $\mathcal{F}$.

Let $\mathbf{\Gamma}$ denote an ordered monoid, i.e. an abelian semigroup under an operation +, equipped with a total ordering $\prec$ such that, for all $\alpha, \beta, \gamma \in \mathbf{\Gamma}$,

$$\alpha \prec \beta \Rightarrow \alpha + \gamma \prec \beta + \gamma . \qquad (*)$$

Definition 3.15 A direct sum

$$\mathcal{P} := \bigoplus_{\gamma \in \mathbf{\Gamma}} \mathcal{P}_{\gamma}^{(\mathbf{\Gamma})}$$

is called a *grading* (induced by $\mathbf{\Gamma}$) or briefly a $\mathbf{\Gamma}-$*grading* if for all $\alpha, \beta \in \mathbf{\Gamma}$

$$f \in P_{\alpha}^{(\mathbf{\Gamma})}, g \in P_{\beta}^{(\mathbf{\Gamma})} \Rightarrow f.g \in P_{\alpha+\beta}^{(\mathbf{\Gamma})} .$$

Since the decomposition above is a direct sum, each polynomial $f \neq 0$ has a unique representation

$$f = \sum_{i=1}^{s} f_{\gamma_i}, \ 0 \neq f_{\gamma_i} \in \mathcal{P}_{\gamma_i}^{(\mathbf{\Gamma})} .$$

Assuming that $\gamma_1 \prec ... \prec \gamma_s$, the $\mathbf{\Gamma}-$homogeneous term f_{γ_s} is called the max*imal part* of f, denote by $M^{(\mathbf{\Gamma})}(f) := f_{\gamma_s}$, and $f - M^{(\mathbf{\Gamma})}(f)$ is called the *reductum* of f.

Example 3.16 Let $f = x^2y + xy^2 + x^3 + y^2 + xy - y \in k[x, y]$. Then

$$f_{\gamma_1} = -y, f_{\gamma_2} = y^2 + xy \text{ and } f_{\gamma_3} = x^2y + xy^2 + x^3.$$

Thus, $M^{(\Gamma)}(f) := x^2y + xy^2 + x^3$. Other hand, The *reductum* of f is

$$f - M^{(\Gamma)}(f) := y^2 + xy - y.$$

There are two major examples of gradings. The first one is the grading by degrees,

$$\mathcal{P}_d^{(\Gamma)} := \{p \in \mathcal{P} \,|\, p \text{ homogeneous of degree } d\} \quad \forall \mathrm{d} \in \mathbb{N}_0.$$

Here, $\mathbf{\Gamma} = \mathbb{N}_0$ with natural total ordering. This grading is called the $H-grading$ because of the homogeneous polynomials. Therefore we also write H in place of this $\mathbf{\Gamma}$. The space of all polynomials of degree at most d can now be written as

$$\mathcal{P}_d := \bigoplus_{k=0}^{d} \mathcal{P}_k^{(H)}.$$

The maximal part of a polynomial $f \neq 0$ is its homogeneous form of highest degree, $M^{(H)}(f)$. For simplicity, let $M^{(H)}(0) := 0$.

Definition 3.17 A finite set $\mathcal{G} := \{g_1, ..., g_s\} \subset \mathcal{P} \setminus \{0\}$ is called an $H-basis$ of the ideal $I :=< g_1, ..., g_s >$ if, for all $0 \neq p \in I$,

$$\exists h_1, ..., h_s : p = \sum_{i=1}^{s} h_i g_i \text{ and } \deg(h_i) + \deg(g_i) \leq \deg(p),\ i = 1, ..., s. \text{ (**)}$$

The representation for p in (**) is also called its $H-$*representation with respect to* $\mathcal{G}$.

Example 3.18 Let $I=\langle y^2-x, xy-x^2\rangle$. Easy to check that $\{y^2-x, xy-x^2\}$

is an $H-basis$ of I.

Obviously, for all $0\neq p\in I$ of the form

$$h_1(x,y)(y^2-x)+h_2(x,y)(xy-x^2)$$

such that

$$\deg(h_i)+\deg(g_i)\leq \deg(p),\ i=1,2.$$

To obtain more insigth into $H-basis$, we will give equivalent definitions.

Definition 3.19 For given $f, f_1,\ldots,f_m\in\mathcal{P}$ we say that f *reduces to* $\tilde{f}$ mod*ulo* $\mathcal{F}:=\{f_1,\ldots,f_m\}$ if

$$\tilde{f}=f-\sum_{i=1}^{m} g_i f_i,\ \deg(\tilde{f})<d,$$

holds with polynomials g_i satisfying $\deg(g_i)\leq\deg(f)-\deg(f_i),\ i=1,\ldots,m$. In this case we write $f\xrightarrow[\mathcal{F}]{}\tilde{f}$.

Theorem 3.20 Let $\mathcal{F}:=\{f_1,\ldots,f_s\}$ and $I=<\mathcal{F}>$. Then the following conditions are equivalent

(i) $\mathcal{F}$ is an $H-basis$ of I.

(ii) $\langle M^{(H)}(f_1),...,M^{(H)}(f_s)\rangle = \langle \{M^{(H)}(f) \mid f \in I\}\rangle$.

(iii) Every $f \in I$ reduces modulo $\mathcal{F}$ to 0.

Note that Hilbert Basis Theorem says that any ideal in $\mathcal{P}$ has a finite basis, hence, by (ii), any ideal in $\mathcal{P}$ has an $H-basis$.

The second major example of gradings leads to the Gröbner basis concept. Here $\mathbf{\Gamma} = \mathbb{N}_o^n$ with componentwise addition and equipped with a total ordering $\prec$ satisfaying (*) and in addition $0 \preceq \gamma \quad \forall \gamma \in \mathbf{\Gamma}$. For arbitrary $\gamma = (\gamma_1,...,\gamma_n) \in \mathbf{\Gamma}$, the space $\mathcal{P}_\gamma^{(\Gamma)}$ is then a vector space of dimension 1, namely

$$\mathcal{P}_\gamma^{(\Gamma)} = \{c.x_1^{\gamma_1}...x_n^{\gamma_n} \mid c \in k\}.$$

The maximal part of a polynomial is now a product of a ledaing coefficient and a leading power product, $M^{(\Gamma)}(f) = LC(f) \cdot LT(f)$, $LC(f) \in k, LT(f)$ a power product. The reduction $f \xrightarrow[\mathcal{G}]{} \tilde{f}$ is defined if there exists a polynomial $g \in \mathcal{G}$ such that $LM(g)$ divides $LM(f)$ and then we set $\tilde{f} = f - \dfrac{M^{(\Gamma)}(f)}{M^{(\Gamma)}(g)} g.$

A Gröbner basis $\mathcal{G}$ is a finite set of polynomials, say $\{g_1,...,g_s\}$, generating the ideal I and satisfying one of the following equivalent conditions

(i) Every $f \in I$ has a representation

$$f = \sum_{i=1}^{s} h_i g_i, \ \max LT(h_i)LT(g_i) \le LT(f).$$

(ii) $\left\langle M^{(\Gamma)}(g_1),\ldots,M^{(\Gamma)}(g_s)\right\rangle = \left\langle \{M^{(\Gamma)}(f) \mid f \in I\}\right\rangle$.

(iii) Every $f \in I$ reduces modulo $\mathcal{G}$ to 0.

If an admissible ordering is compatible with the semi-ordering by degrees,

$$\deg(x^{\gamma}) < \deg(x^{\gamma'}) \Rightarrow \gamma \prec \gamma', \quad \gamma,\gamma' \in \mathbb{N}_0^d,$$

then any Gröbner-representation as given in (i) is an H-representation, in other words, a Gröbner basis with respect to a degree compatible ordering is an $H-basis$ as well. The converse is false as the following examples shows.

Example 3.21 Let $f_1 := x^4 + 2x^2y^2 + y^4 - 1$ and $f_2 := xy(x^2 - y^2)$. Then these polynomials constitute already an $H-basis$. If we order the power products first by degree and same degrees by lower powers in x first, then we get a degree compatible ordering called “total degree ordering” in MAPLE. Since then

$$\left\langle \{M^{(\Gamma)}(f) \mid f \in I\}\right\rangle = \left\langle x^3y, x^4, x^2y^3, xy^5, y^7\right\rangle,$$

every Gröbner basis $\mathcal{G}$ w.r.t. this ordering contains at least 5 elements, for instance MAPLE computes $G = \{g_1,\ldots.,g_s\}$ with

$$\begin{aligned} g_1 &:= x^3y - xy^3 = f_2, \\ g_2 &:= x^4 + 2x^2y^2 + y^4 - 1 = f_1, \\ g_3 &:= 3x^2y^3 + y^5 - y, \\ g_4 &:= 4xy^5 - xy, \\ g_5 &:= 4y^7 - 4y^3 + 3x^2y. \end{aligned}$$

Obviously, this $G-basis$ is an $H-basis$ as well.

The definition of $H-bases$ shows that having an $H-basis$ $g_1,....,g_s$ of an ideal I, the finite dimensional vector space of all $p \in I$ with degree at most d, i.e. the space $I \cap \mathcal{P}_d$, is generated by all power product multiplies $x_1^{i_1}....x_n^{i_n}.g_j$ with $i_1 + ... + i_n + \deg(g_j) \le d$. Hence, problems like the membership problem $p \in I$ can be displayed as a problem in a finite dimensional vector space and solved by linear algebra techniques if an $H-basis$ of I is known. In this section we consider some finite dimensional vector spaces in connection with ideals.

Set, for given polynomials $f_1,...,f_s$ and $d \in \mathbb{N}_0$,

$$V_d(f_1,...,f_s) := \left\{ \sum_{i=1}^{s} h_i M^{(H)}\left(f_i\right) \mid h_i \in \mathcal{P}^{(H)}_{d-\deg(f_i)}, i = 1,...,s \right\}$$

where as a convention, $\mathcal{P}_k^{(H)} = \{0\}$ if $k < 0$. Clearly, $V_d(f_1,...,f_s)$ is a linear subspace of $\mathcal{P}_d^{(H)}$. For convenience, we also define for ideals I

$$V_d(I) := \left\{ M^{(H)}(f) \mid f \in I, \deg(f) = d \text{ or } f = 0 \right\}.$$

This is a linear subspace of $\mathcal{P}_d^{(H)}$ as well.

Fix an inner product $(.,.)$ in $\mathcal{P}$, for instance the scalar product of the coeficient vectors or an inner product $(f,g):=L(fg)$, where L is a strictly positive functional. Then, the orthogonal complements of $V_d(f_1,...,f_m)$ and $V_d(I)$ in $\mathcal{P}_d^{(H)}$ are useful tools. To fix notations, let

$$\mathcal{P}_d^{(H)} = V_d(f_1,...,f_s) \oplus W_d(f_1,...,f_s),$$
$$\mathcal{P}_d^{(H)} = V_d(I) \oplus W_d(I).$$

We will also use the shorthand notation $\odot$, for example $W_d(I) = \mathcal{P}_d^{(H)} \odot V_d(I)$, to express this relationship.

Definition 3.22 For given polynomials $g_1,...,g_m \in \mathcal{P}$ let

$$syz(g_1,...,g_m) := \{(h_1,...,h_m) \in \mathcal{P}^m \mid \sum_{i=1}^{m} h_i g_i = 0\}$$

be the module of syzygies with respect to $g_1,...,g_m$. For every $d \in \mathbb{N}_0$ let

$$S_d(g_1,...,g_m) := \{(h_1,...,h_m) \in \otimes \mathcal{P}_{d-\deg(g_i)}^{(H)} \mid \sum_{i=1}^{m} h_i M^{(H)}(g_i) = 0\}.$$

Lemma 3.23 Let $\mathcal{F} := \{f_1,...,f_s\} \subset \mathcal{P}$ be given. Then the following four statements hold.

i) $M^{(H)}(\mathcal{F}) = \underset{d\in\mathbb{N}_0}{\oplus} V_d(f_1,...,f_s).$

ii) $syz(M^{(H)}(f_1),...,M^{(H)}(f_s)) = \underset{d\in\mathbb{N}_0}{\oplus} S_d(f_1,...,f_s).$

iii) $\dim V_d(f_1,...,f_s) = \dim \mathcal{P}_d^{(H)} - \dim W_d(f_1,...,f_s), \forall d \in \mathbb{N}_0.$

iv) $\dim S_d(f_1,...,f_s) = \sum_{i=1}^{s} \dim \mathcal{P}_{d-\deg(f_i)}^{(H)} - \dim V_d(f_1,...,f_s), \forall d \in \mathbb{N}_0.$

For a given set $\mathcal{F} := \{f_1,...,f_s\}$, with defined linear spaces $V_d(f_1,...,f_s)$, and, after having fixed an inner product in $\mathcal{P}$, their orthogonal complements are defined as $W_d(f_1,...,f_s) := \mathcal{P}^{(H)} \odot V_d(f_1,...,f_s)$ .Then the reduction

$$f \xrightarrow[\mathcal{F}]{} \tilde{f} = f - \sum_{i=1}^{m} g_i f_i, \deg(\tilde{f}) < d,$$

can be performed if and only if $M^{(H)}(f) \in V_d(f_1,...,f_s)$, because exactly then the homogeneous part of degree d on the right hand side can cancel.

We generalize this reduction in two ways. We weaken the condition that the complete maximal part $M^{(H)}(f)$ has to vanish and we admit that reductions are performed also for homogeneous components of lower degree.

Theorem 3.24 Let $\mathcal{F} := \{f_1,...,f_s\} \subset \mathcal{P}$. If the leading homogeneous polynomials $M^{(H)}(p_1),...,M^{(H)}(p_n)$ have only the point $(0,...,0)$ as common zero, then $\mathcal{F}$ is a $H-basis$.

Definition 3.25 Let $\mathcal{F} := \{f_1,...,f_s\} \subset \mathcal{P}$ and $\varphi_d = \varphi_d(f_1,...,f_d)$ denote the orthogonal projection of $\mathcal{P}_d^{(H)}$ onto $W_d(f_1,...,f_s), d \in \mathbb{N}_0$. We define recursively a reduction. We say $f \in \mathcal{P}$ reduces fully to $\tilde{f}$ modulo $\mathcal{F}$, if either there are polynomials $g_i \in \mathcal{P}^{(H)}_{\deg(f)-\deg(f_i)}, i = 1,...,s$, such that

$$\tilde{f} = f - \sum_{i=1}^{m} g_i f_i, \;\; M^{(H)}(\tilde{f}) = \varphi_{\deg(f)}(f),$$

or if $M^{(H)}(f) = M^{(H)}(\tilde{f})$ and $f - M^{(H)}(f)$, the reductum of f, reduces fully modulo $\mathcal{F}$ to $\tilde{f} - M^{(H)}(\tilde{f})$, the reductum of $\tilde{f}$.

Each polynomial $f =: \tilde{f}_0$ of degree d can be fully reduced modulo an arbitrary finite polynomial set $\mathcal{F}$. At a first step, we reduce $\tilde{f}_0$ fully modulo $\mathcal{F}$ to a polynomial $w_d + \tilde{f}_1$ with $w_d = \varphi_d(\tilde{f}_0) \in W_d(f_1,...f_s)$ and $\tilde{f}_1 \in \mathcal{P}_{d-1}$. Then we reduce $\tilde{f}_1$ to $w_{d-1} + \tilde{f}_2$ with $w_{d-1} \in W_{d-1}(f_1,...f_s)$ and $\tilde{f}_2 \in \mathcal{P}_{d-2}$ etc. This procedure terminates after d reduction steps. The result is as follows.

Lemma 3.26 Let $\mathcal{F} := \{f_1,...,f_s\} \subset \mathcal{P}$ and $f \in \mathcal{P}_d$. Then there are polynomials g_i with $\deg(g_i) \le \deg(f) - \deg(f_i)$, $i = 1,...,s$, and homogeneous $w_k \in W_k(f_1,...,f_s)$ for $k = 0,...,d$, such that

$$f = w_d + w_{d-1} + ... + w_0 + \sum_{i=1}^{s} g_i f_i \ . \qquad (*)$$

If $\mathcal{F}$ is an $H-basis$, the $w_0,...,w_d$ are uniquely determimed by f (and by $\mathcal{F}$ and inner product) for every $f \in \mathcal{P}$.

Definition 3.27 Let $\mathcal{F} := \{f_1,...,f_s\} \subset \mathcal{P}$. For $f \in \mathcal{P}$ of degree d let $w_0,...,w_d$ be obtained as in (*). Then $\sum_{k=0}^{d} w_k$ is called a completely reduced form of f with respect to F (and the inner product (.,.) in $\mathcal{P}$).

If $\mathcal{F}$ is an $H-basis$, then the completly reduced form of f is also called *normal form* of f, $NF(f,\mathcal{F})$ for short, and for arbitrary $f \in \mathcal{P}$ the polynomial $RRF(f,\mathcal{F}) := f - NF(f - M^{(H)}(f),\mathcal{F})$ is called *the reductum reduced form of f* (with respect to the $H-basis$ $\mathcal{F}$).

The *normal form* and *the reductum reduced form* are both well defined, since the completely reduced form is unique by lemma 3.26 if $\mathcal{F}$ is an $H-basis$.

By theorem 3.20 (ii), $\mathcal{F}$ is an $H-basis$ of I if and only if $V_d(I)=V_d(f_1,...,f_s)$ holds for every $d\in\mathbb{N}_0$. This means that $V_d(I)$ is generated by all $t.M^{(H)}(f_i)$, t a power product (or monomial) of degree $d-\deg(f_i)$, $i=1,...,s$. Let $f_1,...,f_k$ be $H-basis$ elements of degree less than d and $f_1,...,f_l$ those of degree at most d; clearly, $k\le l$.Then $V_d(I)=V_d(f_1,...,f_l)$ holds if and only if $V_{d-1}(I)=V_{d-1}(f_1,...,f_k)$ and the degree d polynomials $M^{(H)}(f_{k+1}),...,M^{(H)}(f_l)$ generate, together with a basis of $V_d(f_1,...,f_k)$ the space $V_d(I)$. Hence, $f_{k+1},...,f_l$ may be chosen such that $M^{(H)}(f_{k+1}),...,M^{(H)}(f_l)$ are mutually orthogonal and also orthogonal to $V_d(f_1,...,f_k)$. The orthogonalization of the maximal parts against $V_d(f_1,...,f_k)$ may introduce homogeneous componenets which do belong to a $V_j(I)$, $j<d$, and not to $W_j(I)$. Therefore, an additioanal transition to reduced forms is necessary.

Consider a set of polynomials $\{f_1,...,f_m\}$ with only finitely many common zeros. Let I be the ideal generated by $f_1,...,f_m$. Then its variety $V(I)$ consists of these finitely many common zeros. We fix an $f\in\mathcal{P}\setminus I$. Denoting by $[g]$ the equivalence class

$$[g]:=\{h\in\mathcal{P}\mid g-h\in I\},$$

the map

$$\psi_f:[g]\mapsto[f.g]$$

is an endomorphisim of $\mathcal{P}\setminus I$. Its eigenvalues are $\{f(z)\mid z\in V(I)\}$. For arbitrary $f,h\in\mathcal{P}$ the identities $\psi_{f+h}=\psi_f+\psi_h$ and $\psi_{f.h}=\psi_f\circ\psi_h=\psi_h\circ\psi_f$ hold.

If $p_1,...,p_N$ are polynomials such that $[p_1],...,[p_N]$ constitute a basis of $\mathcal{P}/I$, then the matrix associated to ψ_f with respect this basis is called the *multiplication table* and denoted by M_f. An Eigenvector for the Eigenvalue $f(z)$ of M_f is given by

$$\chi(z) := (p_1(z),...,p_N(z))^T.$$

Remark that this Eigenvector is independent of the chosen f! If the degree 1 polynomials $x_1,...,x_n$ are among $p_1,...,p_N$, then we can read off all n coordinates of the common zero $z \in V(I)$ from $\chi(z)$.

The construction of a basis $[p_1],...,[p_N]$ is done in [14] by Gröbner bases techniques. The set of all power products $x_1^{i_1},...,x_n^{i_n}$ which are not divisible by leading terms of the polynomials of a Gröbner basis $\mathcal{G}$ of I constitute the so called *normal set* $\mathcal{N}(\mathcal{G})$. The elements of this normal set are taken as $p_1,...,p_N$. The (Gröbner) normal form $NF(.,\mathcal{G})$ maps onto the linear space spanned by $\mathcal{N}(\mathcal{G})$. Hence, the entries m_{ij} of M_f can easily been computed by reducing $p_i f$ to

$$NF(p_i f,\mathcal{G}) = \sum_{j=1}^{N} m_{ij} p_j, i = 1,...,N.$$

With an $H-basis$ $\mathcal{F}$ of I at hand, one can proceed similarly. Every reduction modulo $\mathcal{F}$ remains within an equivalence class $[g]$. Hence the ($H-basis$) normal form $NF(g,\mathcal{F})$ is a minimal total degree polynomial in $[g]$ and we may take this polynomial as the standard representer of the equivalence class $[g]$.

Here, NF maps onto $\sum_{d=0}^{\infty} W_d(I)$. Since the variety $V(I)$ is finite, the ideal I has dimension 0. Therefore the affine Hilbert polynomial of I is a degree 0 polynomial, i.e. a constant. Hence, there is a $T = T(I) \in \mathbb{N}$ such that $H_I(t) = \dim W_t(I) = 0$ for all $t \geq T$. This means that NF maps onto $\sum_{d=0}^{T} W_d(I)$, a finite dimensional vector space. Its dimension equals the constant $N :=^a H_I(T)$. Let $p_1,\ldots,p_N$ denote a basis of $\sum_{d=0}^{T} W_d(I)$. Then $\{[p_1],\ldots,[p_N]\}$ is a basis of $\mathcal{P}/I$ and the entries m_{ij} of a multiplication table M_f can be computed as before by reducing $p_i f$ to $NF(p_i f, \mathcal{F}) = \sum_{j=1}^{N} m_{ij} p_j, i = 1,\ldots,N$.

The Eigenvector $\chi(z)$ for $z \in V(I)$ as given above all n coordinates of z if $x_1,\ldots,x_n$ are among the p_i. This holds if and only if $\dim W_1(I) = n$. Otherwise, I contains some linear polynomials $l \in \mathcal{P}_1$, such that by $l(z) = 0$ the missing coordinates values of z can be reconstructed.

Example 3.28 Let the system of equations

$$x^4 + 2x^2y^2 + y^4 - 1 = 0$$
$$xy(x^2 - y^2) = 0.$$

Let $f_1 := x^4 + 2x^2y^2 + y^4 - 1$ and $f_2 := xy(x^2 - y^2)$ constitute an $H - basis$ of $I = \langle f_1, f_2 \rangle$ for all $d \in \mathbb{N}$.

If we take as inner product in $\mathcal{P}$ the scalar product of the coefficient vectors, then, easy computation shows, three dimensional space $W_4(f_1,f_2)$ orthogonal to $V_4(f_1,f_2)$ is generated by φ_1,φ_2 and φ_3. Now we can compute these:

Let $LT(f_1)=x^4+2x^2y^2+y^4$ and $LT(f_2)=x^3y-xy^3$.

For $d=0;\ W_0(I)\Rightarrow W_0=\langle 1\rangle$

$d=1;\ W_1(I)\Rightarrow W_1=\langle x,y\rangle$

$d=2;\ W_2(I)\Rightarrow W_2=\langle x^2,xy,y^2\rangle$

$d=3;\ W_3(I)\Rightarrow W_3=\langle x^3,x^2y,xy^2,y^3\rangle$

$d=4;\ W_4(I)\Rightarrow W_4=\langle x^4,x^3y,x^2y^2,xy^3,y^4\rangle$

	x^4	x^3y	x^2y^2	xy^3	y^4
$LF(f_1)$	1	0	2	0	1
$LF(f_2)$	0	1	0	-1	0

$$V_4(I)=\{(1,0,2,0,1),(0,1,0,-1,0)\}$$
$$W_4(I)=\{(x_1,x_2,x_3,x_4,x_5):\langle(x_1,x_2,x_3,x_4,x_5),(1,0,2,0,1)\rangle=0,$$
$$\langle(x_1,x_2,x_3,x_4,x_5),(0,1,0,-1,0)\rangle=0\}.$$

We have $x_1+2x_3+x_5=0$ and $x_2-x_4=0$. MAPLE command to solve this equations:

> With(Algebra):

> gb:={x1+2*x3+x5=0,x2-x4=0};

$gb := \{x1 + 2\,x3 + x5 = 0, x2 - x4 = 0\}$

> solve(gb,{x1,x2,x3,x4,x5});

$\{x2 = x4, x5 = x5, x1 = -2\,x3 - x5, x3 = x3, x4 = x4\}$

$$(1,0,0,0,1) \to \varphi_1 = x^4 - y^4$$
$$(1,0,-1,0,1) \to \varphi_2 = x^4 - x^2y^2 + y^4$$
$$(0,1,0,1,0) \to \varphi_3 = x^3y + xy^3.$$

The two dimensional space $W_5(f_1, f_2)$ has as basis:

$$g_1 = x(x^4 + 2x^2y^2 + y^4) = x^5 + 2x^3y^2 + xy^4$$

$$g_2 = y(x^4 + 2x^2y^2 + y^4) = x^4y + 2x^2y^3 + y^5$$

$$g_3 = x(x^3y - xy^3) = x^4y - x^2y^3$$

$$g_4 = y(x^3y - xy^3) = x^3y^2 - xy^4$$

For $d = 5$; $W_5(I) = \left\langle x^5, x^4y, x^3y^2, x^2y^3, xy^4, y^5 \right\rangle$.

x^5	x^4y	x^3y^2	x^2y^3	xy^4	y^5
1	0	2	0	1	0
0	1	0	2	0	1
0	1	0	-1	0	0
0	0	1	0	-1	0
x_1	x_2	x_3	x_4	x_5	x_6

We obtained $x_1 + 2x_3 + x_5 = 0, x_2 + 2x_4 + x_6 = 0, x_2 - x_4 = 0$ and $x_3 - x_5 = 0$.

> With(Algebra):

> gb:={x1+2*x3+x5=0,x2+2*x4+x6=0,x2-x4=0,x3-x5=0};

$gb := \{x1 + 2\,x3 + x5 = 0,\, x3 - x5 = 0,\, x2 - x4 = 0,\, x2 + 2\,x4 + x6 = 0\}$

> solve(gb,{x1,x2,x3,x4,x5});

$$\{x1 = -3\,x3,\, x3 = x3,\, x2 = -\frac{x6}{3},\, x5 = x3,\, x4 = -\frac{x6}{3}\}$$

x_1	x_2	x_3	x_4	x_5	x_6
-3	0	1	0	1	0
0	1	0	1	0	-3

$(-3,0,1,0,1,0) \to \varphi_4 = -3x^5 + x^3y^2 + xy^4$

$(0,1,0,1,0,-3) \to \varphi_5 = x^4y + x^2y^3 - 3y^5.$

And similarly the one dimensional space $W_6(f_1, f_2)$ is generated by

$\varphi_6 = -3x^6 + x^4y^2 + x^2y^4 - 3y^6$. Other hand $W_d(I) = \langle 0 \rangle$.

Then we have as $(p_1, \ldots p_N)$ the vector

$(1; x, y; x^2, xy, y^2; x^3, x^2y, xy^2, y^3; \varphi_1, \varphi_2, \varphi_3; \varphi_4, \varphi_5; \varphi_6)^T$,

where we used a semicolon in place of the usual separating comma in order to separate homogeneous polynomials of different degrees. If we consider the endomorphism ψ_x then its matrix M_x corresponding to the given basis has entries m_{ij}, where

$$NF(x.p_i) = \sum_{j=1}^{16} m_{ij} p_j, \text{ i=1,...,16.}$$

Computation gives

$$M_x = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{3} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
\frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{3} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & -\frac{1}{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{4}{11} & 0 & 0 \\
0 & \frac{2}{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{3}{11} & 0 & 0 \\
0 & 0 & \frac{6}{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{2}{11} & 0 \\
0 & 0 & 0 & -\frac{27}{20} & 0 & \frac{33}{20} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{11}{20} \\
0 & 0 & 0 & 0 & -\frac{1}{4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -3 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

Where

$$\begin{aligned}
NF(x.x^3) &= \frac{3(x^4 - y^4) + 2(x^4 - x^2y^2 + y^4) + 1}{6} \\
&= \frac{1}{2}\varphi_1 + \frac{1}{3}\varphi_2 + 0.\varphi_3 + \frac{1}{6}
\end{aligned}$$

and

$$f_1 = 0 \Rightarrow x^2y^2 = \frac{1-x^4-y^4}{2}$$
$$2x^2y^2 = 1 - x^4 - y^4 + x^2y^2 - x^2y^2$$
$$3x^2y^2 = 1-(x^4 - x^2y^2 + y^4).$$

Thuse $NF(x^2y^2) = \frac{1}{3} + (-\frac{1}{3})\varphi_2$. Similarly, we can find other elements of matrix M_x.

Mathematica code for Characteristic Polynomial of M_x:

In[1]:= CharacteristicPolynomial[M_x];

Out[1]= $gb = \frac{-t^4}{16} + \frac{9t^8}{16} - \frac{3t^{12}}{2} + t^{16}$

In[2]:= NSolve[gb == 0, t]

Out[2]={{t -> -1.},{t ->0},{t -> 0},{t ->0},{t ->0.707107},{t ->1},{t -> 0.707107 I},{t -> 1.}}.

Similarly, we can find the matrix M_y.We have six solutions:{{x=-1,y=0},{x=0,y=-1},{x=0,y=1},{x=0,y=1.I},{x=0.707107,y=0.707107.I},{x=1,y=0},{x=0.707107.I ,y=0.707107},{x=1.I,y=0}}.

CONCLUSIONS

The $H-basis$ were introduced first by Macaulay [15]. His original motivation was the transformation of systems of polynomial equations into simpler ones. The power of this concept was not really understood presumaly because of the lack of facilities for symbolic computations. When ComputerAlgebra Systems came up, Gröbner bases ($G-bases$ for short) were used instead of $H-bases$. These bases, originally invented by Buchberger [16] for computing multiplication tables for factor rings.

We consider $\mathcal{P}$, the ring of polynomials in $x_1,...,x_n$ with coefficients from an infinite field k, i.e. $\mathcal{P}=k[x_1,...,x_n]$, and the subsets $\mathcal{P}_d$ of all polynomials of degree at most d. The $G-basis$ give generating systems to $I\bigcap\mathcal{F}_i$, where $\mathcal{F}_i\subset\mathcal{P}$ is a linear vector space of dimension i, and $\mathcal{F}_i\subset\mathcal{F}_{i+1}$ for all i, and $\mathcal{P}=\bigcup_{i\geq 1}\mathcal{F}_i$. Having an $H-basis$ $\{f_1,...,f_s\}$ for I, then the set of all $p_i.f_i$ with $p_i\in\mathcal{P}_{d-\deg(f_i)}, i=1,...,s$, generates $I\bigcap\mathcal{P}_d$ as a linear vector space. Then every set of polynomials can be transformed into $G-basis$ or $H-basis$. Other hand , $G-basis$, foundation of computer algebra and $H-basis$, a "bridge" between computer algebra in polynomials rings and linear algebra.

Many of the problems in applications which can be solved by Gröbner techniques can also be treated successfully with $H-bases$.$G-bases$ are now a standart tool in Computer Algebra. They are covered by nearly all textboks and contained in almost all computer Algebra System. On the other hand, the construction of $G-bases$ is often difficult or even impossible because of the high complexity of Buchberger's algorithm for computing, and by the, in many applications, artificial term ordering the $G-bases$ allows often only a few insight into the structure of a solution. In the theory of $G-bases$, we need to consider a monomial ordering, but we don't need in the theory of $H-bases$. In the case, $H-bases$ are the most efficient for solving systems of polynomial equations than $G-bases$.

REFERENCES

[1] M. E. Phost and D.Y.Y. Yun , " *On Solving System of Algebraic Equations via Ideal Bases and Elimination Theory*", Proceedings Symposium on Symbolic and Algebraic Manipulations, (1981)

[2] J. C. Faugere, P. Gianni, D. Lazard, and T. Mora, "*Efficient Computation of Zero-Dimensional Gröbner bases by change of ordering"*, J. Symbolic comput. , 16(1993), no. 4, 329-344.

[3] J. C. Faugere, "*A new efficient algorithm for computing Gröbner basis without reduction to Zero (F_5)*", Proceedings of the 2002 Int. Symp. on Symbolic and Algebraic Computation, ACM Press, New York, 75-83, 2002.

[4] J. B. Farr, and R. Pearce, " *Working with Multivariate Polynomials in Maple*", Proceedings of Maple Summer Workshop, (2005).

[5] A. Steel,"*Gröbner Basis Timings Page"*, available from http://Magma maths.usyd.edu.au/users/allan/gb.

[6] W.W. Adams and P. Looustaunau, "*An Introduction to Gröbner Basis"*, Graduate Studies in Mathematics, Vol.3, Providence, R.I., AMS(1996).

[7] D. Cox, J. Little and D. O'Shea. "*Ideals, Varieties and Algorithms*", Springer Verlag(1996).

[8] D. Cox, J. Little and D. O'Shea, "*Using Algebraic Geometry"*, Springer-Verlag(1998).

[9] G.M. Greuel, G.Phister and H. Schonemann, SINGULAR Reference Manual, Center for Computer Algebra, University of Kaiserrlautern, from www.singular.uni-kl.de.

[10] T.Luo and E.Yilmaz , "*On The Lifting Probllem for Homogeneous Ideals, Journal of Pure and Applied Algebra*", **162**(2001), 327-355.

[11] E. Yilmaz and S. Kilicarslan, "*Minimal Homogeneous Basis for Polynomial Ideals, Applicable Algebra in Engineering, Communication and Computing"*, **15**(2004), 267-278.

[12] T. Sauer, "*Grobner Bases, H-Bases and Interpolation*", Transaction of AMS **353**(2001), 2293-2308

[13] H. M. Möller and T. Sauer, "*H-bases for Polynomial Interpolation and System Solving*", Adv. Comput. Math. , 12(2002), no.4, 335-362.

[14] H. M. Möller and H. J. Setter, “*Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems*”. Numer. Math. , 70, (1995), no.3, 311-329.

[15] F. S. Macaulay, “*The Algebraic Theory of Modular Systems”*. Cambridge Tracts in Math. and Math. Phys., 19, Cambridge Univ. Press, 1916.

[16] B. Buchberger, Ein Algortithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, (Doctoral thesis), Univ. Innsbruck, 1965.