On the solution of systems of algebraic (polynomial) and rational equations in several variables

Herman Jaramillo

September 23, 2015

Contents

Chapter 1

Introduction

My motivation to write this document started when trying to find an algebraic equation for Mobius strip, out of a parametric representation described here [1]. I tried to find, out of that parametrization, an algebraic solution as proposed here [2] but I failed and decided that needed to understand more about how solve systems of rational [3] equations in several variables, and of course, to do that I would need to start with polynomial equations. Christian Blatter, in the second link above, presented a solid and simple solution, but it is more like black magic when you find substitutions that solve your problem but without much justification. These notes are about the justification for such substitutions. That is, we should transform the problem to a language that we know and solve it in that language.

Systems of polynomials in one variable can be solved by a simplified method. That is, if $f_1(x) = 0, \cdots, f_m(x) = 0$, then to know if x_0 is a solution we need to divide the greatest common divisor $\gcd(f_1, \cdots, f_n)$ by $x - x_0$, and if the residual is 0 then x_0 is a solution of the system. For multivariate polynomials the problem is harder.

We are interested on learn about polynomials in several variables. The set of polynomials forms a ring. As in linear algebra where vector spaces have subspaces and bases, in rings we have similar structures such as ideals which

[1] http://math.stackexchange.com/questions/638225/understanding-the-equation-of-a-m%C3%B6bius-strip

[2] http://math.stackexchange.com/questions/1366639/derive-cartesian-cubic-m%C3%B6bius-strip-from-parametric

[3] I knew that we could reduce the system to a rational system, by parametrizing $\sin\theta = \frac{1-t^2}{1+t^2}, \cos\theta = \frac{2t}{1+t^2}$, but then how to reduce the resulting system?

are generated by a set of polynomials. Some knowledge on linear algebra would be very beneficial here.

Whenever possible we make analogies with vector spaces since that is assumed to be known territory. Vector subspaces are simpler than ideals of polynomials and borrowing knowledge from vector spaces could speed up learning on ideals of polynomials.

Conventions: I use := to indicate that the left hand side is a definition with its meaning on the right hand side. If A is a set $|A|$ is the cardinal, or the number of elements of the set A.

Bibliography: Adams and Loustaunau [4]

Cox, et. al. [5]

[4] https://books.google.com/books?isbn=0821872168

[5] https://books.google.com/books?isbn=1475726937

Chapter 2

Rings

2.1 Definition and Basics

We assume that we know the definition of fields. Examples of fields are the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, and the complex numbers $\mathbb{C}$ among others. In a **field** we can define addition, subtraction, multiplication, and division with the usual properties including associative, commutative and distributive laws.

Definition 1 (**binary operation**). *A* **binary operation** *in a set A is defined by a mapping $A \times A \to A$.*

Definition 2 (**Commutative Ring**). *A* **commutative ring** *consists of a set R and two binary operations "." and "+" defined on R for which the following conditions are satisfied:*

(i) **Closure:** *For each $a, b \in R$, $a.b \in R$ and $a + b \in R$.*

(ii) **Associative** $(a + b) + c = a + (b + c)$ *and* $(a.b).c = (a.b).c$ *for all* $a, b, c \in R$.

(iii) **Commutative** $a + b = b + a$ *and* $a.b = b.a$ *for all* $a, b \in R$.

(iv) **Distributive** $a.(b + c) = a.b + a.c$ *for all* $a, b \in R$.

(v) **module** *There is an element* $0 \in R$, *such that* $a + 0 = a$ *for all* $a \in R$.

(vi) **Additive inverse:** *Given $a \in R$, there is an element $b \in R$ such that* $a + b = 0$.

If we release the commutativity law (such that as for example $a.b \neq b.a$, then the ring is called non-commutative. We will avoid the study of non-commutative rings in this book. If in addition there is an element 1 called **unity** such that for any $a \in R$, $a = 1.a$ then the ring is called **ring with unity** . Finally, ff we add to this a multiplicative index then we create a **field** .

Here is a bit of history taken from the work of Frédérique Oggier [1], from Wikipedia [2] and from Wikipedia [3] The citation for the original references are found there.

- The name "ring" was coined by Hilbert ("Zahlring") in 1892.
- Dedekind introduced the name "field" (Körper) in 1871. The word means "body" or "corpus" and hence the use of the letter $\mathbb{K}$. The letter $\mathbb{F}$ for field is also commonly used.
- Emmy Noether, about 1921, brought the two theories of rings of polynomials and rings of numbers into a single theory of abstract commutative rings. While the first axiomatic definition of rings was provided by Adolf Fraenkel in 1914, Noether changed it to what we the current definition. However the inclusion of the multiplicative unit into the definition was controversial. Fraenkel required the ring to have a multiplicative identity, while Noether did not have that constraint. Sometimes the rings without identity are called with the name "rng" or "pseudo-ring". .
- While we do not consider non-commutative rings here, we point that Hamilton developed this idea after attempting to generalize the complex numbers to two dimensional algebra over the reals to a three dimensional algebra. Examples of non-commutative objects are found in the matrix multiplication. Matrices were introduce by Cayley in 1850.
- Hamilton introduced the idea of vector space in 1843.
- The term "ideals" was introduced by Kummer in 1849 when trying to find the non-unique decomposition of prime factorization of numbers under the name "ideal complex numbers".

[1] http://www1.spms.ntu.edu.sg/ frederique/chap2.pdf
[2] https://en.wikipedia.org/wiki/Ring_%28mathematics%29#History
[3] https://en.wikipedia.org/wiki/Field_%28mathematics%29#History

Example 2.1.1.

- The classical example of a ring is the integer numbers $\mathbb{Z}$.
- For $m \neq \pm 1$, $m \in \mathbb{Z}$, the set $m\mathbb{Z}$ is a ring without unity. For example the even numbers $2n$, $n \in \mathbb{Z}$ form a ring without unity.
- The polynomials in one or several variables form a ring. In particular all monomials of the form ax, $a, x \in \mathbb{K}$ form a ring without unity.
- The set of square matrices with their addition and product form a non-commutative ring. If the identity is present that ring is a ring with unity, otherwise a ring without unit.
- The rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ are all rings, but they are most commonly used as fields, since in them the multiplicative inverse is defined.
- If we provide the polynomials with division we can convert the ring of polynomials into a field.
- The set $C(\mathbb{R})$ of continuous functions f $f : \mathbb{R} \to \mathbb{R}$ with point-wise addition and multiplication is a ring.

The example of finite rings is important and deserves a section by itself.

2.1.1 Finite Rings

Finite rings can be created using the concept of modulo or residual classes. We introduce here the cyclic rings.

Definition 3 (congruent). *For $n \in \mathbb{Z}^+$ (positive integer) we say that two numbers $x, y \in \mathbb{Z}$ are* **congruent module** *n if the residual n of the division of $x - y$ by n is 0. That is, if n divides the difference $x - y$ evenly. The standard notation from number theory is*

$$x \equiv y \pmod{n}$$

We can rewrite the definition symbolically by writing

$$x \equiv y \pmod{n} \iff n|(x - y).$$

where the symbol | means "divide". When n does not divide the difference, that is when $n \not| (x-y)$ we write $x \not\equiv y$.

It is easy to show (this belongs to the scope of number theory) that the congruence relation is an equivalence relation. This means that is is reflexive ($x \equiv x$, $\forall x \in \mathbb{Z}$), symmetric ($x \equiv y \Longrightarrow y \equiv x$), and transitive ($x \equiv y$ and $y \equiv z \Longrightarrow x \equiv z$). Equivalent relations defined on a set split the set in a **partition** (a set of piecewise disjoint subsets such that their union is the original set,) The elements of the partition are known as equivalence classes.

We then define an **equivalence class** with the equation

$$[x]_n := \bar{x} := \{y : y \equiv x\}$$

For example, for $n = 3$, we have

$$\begin{aligned} \bar{0}_3 &= \{0, \pm 3, \pm 6, \cdots 3m \cdots\}, \\ \bar{1}_3 &= \{-3m+1 \cdots, -5, -2, 1, 4, 7, \cdots 3m+1 \cdots\}, \\ \bar{2}_3 &= \{-3m+2 \cdots, -4, -1, 2, 6, 8, \cdots 3m+2 \cdots\}. \end{aligned} \tag{2.1}$$

Note that we can write this differently as

$$\begin{aligned} \bar{0}_3 &= 0 + 3\mathbb{Z} \\ \bar{1}_3 &= 1 + 3\mathbb{Z} \\ \bar{2}_3 &= 2 + 3\mathbb{Z}, \end{aligned}$$

and in general $\bar{n}_m = n + m\mathbb{Z}$, with $n \in \mathbb{Z}$, $n > 0$, $m < n$. We provide an extension of this in definition 13

We define the set of classes of integers modulo 3 is given by

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}.$$

with the name **cyclic ring** of three elements. We prove that indeed this is a ring. Here we say that $a \in \mathbb{Z}_3$ if the residual of integer division of a by 3 is either $0, 1$, or 2. We see that 0 and 1 are in $\mathbb{Z}_3$. Let us show that the sum and product are closed. We will not prove commutativity, associativity, or distributivity since they are directly inherited by the structure of the sum and product of the integer numbers.

Let us assume that $a, b \in \mathbb{Z}$. Then $a = 3n + r_1$, with some $n \in \mathbb{Z}$ and $r_1 \in \{0, 1, 2\}$. Also $b = 3m + r_2$, with some $n, r_2 \in \mathbb{Z}$ and $r_2 \in \{0, 1, 2\}$. Then

$$(a + b) = 3(n + m) + r_1 + r_2.$$

If $r_1 + r_2 < 3$, then this is it. $a + b \in \mathbb{Z}_3$, otherwise $r_1 + r_2 = 3 + r_3$ (observe that $r_1 + r_2 < 6$) and $r_3 < 3$, so $(a + b) = 3(n + m + 1) + r_3$, with $r_3 < 3$, so $a + b \in \mathbb{Z}_3$.

Now, assume $a \in \mathbb{Z}_3$, and $b \in \mathbb{Z}$. Then $a = 3n + r$, with $n \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$ Then

$$ba = b(3n + r) = 3(bn) + br.$$

Now we can write

$$br = 3k + r$$

with some $k \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$, so

$$ba = 3(bn + k) + r$$

with $r \in \{0, 1, 2\}$. So $ba \in \mathbb{Z}_3$.

This shows the existence of finite rings.

In fact we can define the **residue class of a function** f module n using the notation $f(x) \pmod n$, as the set of all possible values of the residue of $f(x)$ divided by n. That is we write, for example we can compute $x^2 \pmod 3$ as

$$\begin{aligned} 0^2 &= 0 \equiv 0 \pmod 3 \\ 1^2 &= 1 \equiv 1 \pmod 3 \\ 2^2 &= 4 \equiv 1 \pmod 3 \\ 3^3 &= 9 \equiv 0 \pmod 3 \\ &\vdots \\ n^3 &= m \equiv o \pmod 3 \end{aligned}$$

where in the last equation we find that the o is the remainder after dividing $n^3 = m$ by 3. The classical example is found by setting f to the identity. That is we write

$$\begin{aligned} I : \mathbb{Z} &\to \mathbb{Z}_n \\ z &\mapsto r \end{aligned}$$

with r the reminder of dividing z by n. For any number $r = 0, 1, \cdots n-1$ in the set $\mathbb{Z}_n$, the pre-image in the domain is an infinite collection of integers which we call a residual class $[x]_n$, or $\bar{x}_n$. For example if $n = 3$, we have

$$\begin{aligned} \bar{0}_3 &= \{0, \pm 3, \pm 6, \cdots 3m \cdots\}, \\ \bar{1}_3 &= \{-3m+1 \cdots, -5, -2, 1, 4, 7, \cdots 3m+1 \cdots\}, \\ \bar{2}_3 &= \{-3m+2 \cdots, -4, -1, 2, 6, 8, \cdots 3m+2 \cdots\}. \end{aligned}$$

shown in equation 2.1.

The ring of interest in the context of this book is the ring of polynomials in the variables $x_1, \cdots, x_n$ over the field $\mathbb{K}$ that we call $\mathbb{K}[x_1, \cdots, x_n]$. From now on we drop the dot "." and assume that no symbol between two elements means product. That is, for example $fg := f.g$.

To be more specific the multivariate polynomial $\mathbb{K}[x_1, \cdots, x_n]$ is a sum of the form

$$\sum a_{i_1 \cdots i_n} x_1^{\beta_{i_1}} \cdots x_n^{\beta_{i_n}}$$

with $\beta_{i_j} \in \mathbb{N}$. If all coefficients $a_{i_1 \cdots i_n} \in \mathbb{K}$ are zero, then the polynomial is the trivial 0 polynomial. In fact, the set of multivariate polynomials form a vector space with the basis of the form

$$x_1^{\beta_1} \cdots x_n^{\beta_n}$$

where all combinations of powers β_{i_j} up to certain (highest order) are possible. However we are interested on the set of multivariate polynomials more as a ring (and a module, which will be defined later) than as a regular vector space. The non-zero term with the largest $\beta_j = \sum \beta_{i_j}$ is called the **leading term** noted as LT, and β is called the **degree** of the polynomial. If for two terms have the same degree (same β_j) we need to use more criterion. That is if those are the j and the k terms, their exponents can be listed as $(\beta_{j1}, \cdots \beta_{jn})$, and $(\beta_{k1}, \cdots, \beta_{kn})$ respectively. We order the vector in a lexicographic (dictionary) way by giving priority to the first entry, then if equality, the second, until one entry is larger than the other. We will go back to this analysis in more detail in section 3.2. See particularly definitions 23 and 20.

As in vector spaces we have also subsets or rings which are closed under both binary operations. For example the even integers are closed under sum and multiplication (however in the multiplication only one of the elements is required to be on the subset). This motivates the definition of subring presented on the following section.

2.2 Subrings and Homomorphisms

Before we introduce the concept of ideals we provide a few basic definitions. As with most algebraic theories, there is the concept of a substructure which is a subset which preserves the structure of its parent set. This is the case of a subring, which is a subset of a ring R which is closed under the binary operations defined in the ring R and contains the identity of the ring. That is,

Definition 4 (subring). *Let R be a ring, and $S \subset R$ such that*

(i) **Unity** $1 \in S$,

(ii) **closure of addition:** $a + b \in S$ *for all* $a, b \in S$,

(iii) **closure of multiplication** $ab \in S$, *for all* $a, b \in S$.

2.2.1 Subrings Examples

- Trivially, every ring is a subring of itself.
- Every subring is a ring itself.
- Let us define $\mathbb{Z}_p$ [4] as the collection of rational numbers whose denominator is not a multiple of the prime number p, after the fraction is reduced. For example for $p = 3$ we would have numbers such as $\{1, 1/2, 1, 4, 1/5, 1/7\}$ among infinite many. Since $\mathbb{Z}_p \subset \mathbb{Q}$, and $0, 1 \in \mathbb{Z}_p$, we only need to show that $\mathbb{Z}_p$ is closed under sums and products. Let us check this. Let a/b and c/d elements of $\mathbb{Z}_p$, so that $p \not| b$ and $p \not| d$ [5]

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad , \quad \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd},$$

and since $p \not| b$ and $p \not| d$, then p is not a divisor of their product bd. Then sum and multiplication are closed. This shows that $\mathbb{Z}_p$ is a subring. This makes of $\mathbb{Z}_p$ a ring.

[4] Observe that this is different from the definition of $\mathbb{Z}_3$ provided in the examples list 2.1.1

[5] the notation $p \not| b$, means that p is not a divisor of b, or in other words that there is not an integer number q such $b = qp$.

- The set of continuous functions $C([a,b],\mathbb{R})$, with $a,b \in \mathbb{R}$ with $a < b$ is a subring.

- Let us define the set $A_p = \{a + ib\ \sqrt{p}\ : a,b \in \mathbb{Z}\}$, with p a prime (positive) number and $i^2 = -1$ we verify that A_p is a subring of the complex numbers $\mathbb{C}$. Since $\mathbb{C}$ is a field then it is a ring and only need to show closure.

  Let $x, y \in A_p$, that is $x = a + ib\sqrt{p}$, $y = c + id\sqrt{p}$, with $a,b,c,d \in \mathbb{Z}$. Then

  $$x + y = (a + c) + i(b + d)\sqrt{p} \quad , \quad xy = (ac - bd)p + (ad + bc)i\sqrt{p}$$

  and since $a + c, b + d, ac - bd, ad + bc \in \mathbb{Z}$ we have that $x + y, xy \in A_p$. We see that if $a = 1, b = 0$, then $x = 1$, so $1 \in A_p$, and A_p is a subring.

- An arbitrary intersection of subrings is a subring. That is, for a family of indices $\mathcal{A}$,

  $$A = \cap_{\alpha \in \mathcal{A}} R_\alpha$$

  is a subring, if for each α, R_α is a subring. This is easy to verify since $1 \in R_\alpha$, for each α, and if $a, b \in A$, then they are on each R_α and their product and sum should be on the corresponding R_α and so in A.

- The union of subrings is no necessarily a subring. See the example above for A_p, now take another set A_q, with $p \neq q$, and q a primer number. For example choose $p = 3$ and $q = 5$, and take two elements in the union $1 + \sqrt{5}$, and $1 + \sqrt{3}$, The sum $2 + \sqrt{3} + \sqrt{5}$ is not in A_3 neither in A_5, so the union is not a subring. However if the rings form a chain, their union is a ring. That is,

- Let R_i be an ascending chain of subrings of a given ring R. That is, $R_i \subset R_{i+1}$, for all $i \in \mathbb{N}$, such that their union is a subset of R.

  $$\mathcal{R} = \cup_{i=1}^{\infty} R_i.$$

  Then $\mathcal{R}$ is a subring of R. Since each subring has the unit of R the chain has the unit of R. Pick now $a, b \in \mathcal{R}$, then there exists i, j such that $a \in R_i$ and $b \in R_j$, let us say, without loss in generality, that $j > i$, so $a, b \in R_j$, and since R_j is a subring of R, then $a + b \in R_j$ and $ab \in R_j$ but $R_j \subset \mathcal{R}$. So $\mathcal{R}$ is a subring of R.

Definition 5 (Homomorphism). *Let R and S rings and $\phi : R \to S$ a mapping such that*

- $\phi(a+b) = \phi(a) + \phi(b)$ *for all* $a, b \in R$.
- $\phi(ab) = \phi(a)\phi(b)$ *for all* $a, b \in R$.
- $\phi(1_R) = 1_S$

then ϕ is call a **homomorphism of rings** *. If ϕ is injective the homomorphism is called* **embedding** *, if ϕ is bijective it is called* **isomorphism** *, and if $R = S$ an isomorphism takes the name* **automorphism** *, while the homomorphism takes the name* **endomorphism** *. The symbols $1_R, 1_S$ stands from the units on their respective rings. In general, by default we note the unit with the symbol 1.*

2.2.2 Homomorphism Examples

(i) The simplest example (and least interesting) is that of ϕ being the identity function. In this case ϕ is an automorphism.

(ii) Given a subring $S \subset R$, the map $\phi : S \to R$, such that $\phi(a) = a$, for all $a \in S$, is an embedding.

(iii) In the set of examples 2.1.1 we introduced the concept of residue class. The function

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}_n \\ a &\mapsto [a]_n \equiv a \pmod{n}, \end{aligned} \tag{2.2}$$

$n \geq 1$, is a homomorphism. It is easy to show that $[a+b]_n = [a]_n + [b]_n$ and that $[ab]_n = [a]_n[b]_n$. The zero element is $[0]_n = [an] = \mathbb{Z}$, $a \in \mathbb{Z}$, and the one element is $[1]$ since $[1][a] = [1a]$, for all $a \in \mathbb{Z}$.

(iv) Complex conjugation

$$\mathbb{C} \to \mathbb{C} \tag{2.3}$$

$$z \mapsto \bar{z} \tag{2.4}$$

is an automorphism. This is so because $1 \in \mathbb{C}$, and $\overline{z_1 z_2} = \overline{z_1 z_2}$ and $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.

(v) The evaluation of the set of continuous functions $R = C([a,b],\mathbb{R})$, with $a, b \in \mathbb{R}$, $a < b$, is a surjective homomorphism. That is, the mapping

$$R_{x_0} : R \rightarrow \mathbb{R} \tag{2.5}$$
$$f \rightarrow f(x_0) \tag{2.6}$$

is an homomorphism. We fix a point $x_0 \in [a,b]$. By definition, $f, g \in R$, $(fg)(x_0) := f(x_0)g(x_0)$ and $(f+g)(x_0) := f(x_0) + g(x_0)$. Let us now examine the units on each domain. The identity function in $I_{[a,b]}$ is a continuous function, then $I_{[a,b]} \in R$, and $1_R = I_{[a,b]}$. Choosing $x_0 = 1$, we have that $R_1(I_{[a,b]}) = 1$. It is interesting that we should force x_0 to be 1 to have the third condition of the homomorphism definition to be valid. So, strictly speaking, on ly R_1 is an homomorphism.

Proposition 2.2.1. *For any homomorphism $\phi : R \rightarrow S$, $\phi(0) = 0$, and $\phi(-a) = -\phi(a)$, for all $a \in R$.*

Proof.

- Since $\phi(0) = \phi(0+0) = \phi(0) + \phi(0) = 2\phi(0)$, then $\phi(0) = 0$. Now,
- $0 = \phi(0) = \phi(a + (-a)) = \phi(a) + \phi(-a)$, so $\phi(-a) = -\phi(a)$.

This proofs the proposition. □

We now show properties related to the composition of homomorphisms, inverse of isomorphisms, and images of an homomorphism.

Proposition 2.2.2. *Let us assume that $\phi : R \rightarrow S$ and $\varphi : S \rightarrow T$ are homomorphisms.*

(i) *$\varphi \circ \phi : R \rightarrow T$ is an homomorphism. The embedding or the isomorphism properties are inherited.*

(ii) *The image $\phi(R)$ is a subring of S.*

(iii) *If ϕ is an isomorphism then ϕ^{-1} is an isomorphism from S to R.*

Proof.

(i) $(\varphi \circ \phi)(x+y) := \varphi[\phi(x+y)] = \varphi(\phi(x)+\phi(y)) = \varphi(\phi(x)) + \varphi(\phi(y))$. That is $(\varphi \circ \phi)(x+y) = (\varphi \circ \phi)(x) + (\varphi \circ \phi)(y)$, where we used the fact that each function (ϕ, φ) is an homomorphism.

We can prove following the same pattern that

$$(\varphi \circ \phi)(xy) = (\varphi \circ \phi)(x)\,(\varphi \circ \phi)(y).$$

Now,

$$(\varphi \circ \phi)(1_R) := \varphi[\phi(1_R)] = \varphi(1_S) = 1_T.$$

where, again, we used the fact that both ϕ and φ are homomorphisms. The inheritance of embedding or isomorphism comes from the properties of function composition of one-to-one and bijective functions.

(ii) This is trivial from the definition of homomorphism and subring.

(iii) Consider $u, v \in S$. Then there are $x, y \in R$ such that $\phi(x) = u$ and $\phi(y) = v$, and since ϕ is an isomorphism then $\phi(x+y) = \phi(x)+\phi(y) = u+v$. So $x+y = \phi^{-1}(u+v)$, but since $x = \phi^{-1}(u)$ and $y = \phi^{-1}(v)$, then $\phi^{-1}(u+v) = \phi^{-1}(u)+\phi^{-1}(v)$. Along the same lines we show that $\phi^{-1}(uv) = \phi^{-1}(u)\phi^{-1}(v)$.

Finally, since $\phi(1_R) = 1_S$, then $\phi^{-1}(1_S) = 1_R$, and then ϕ^{-1} is an isomorphism.

□

We say that R and S are isomorphic if there is an isomorphism between them. We write $R \simeq S$. From the previous proposition if $R \simeq S$ and $S \simeq T$, then $R \simeq T$, and since $R \simeq R$ (using the identity function), then the isomorphism is an equivalence relation (reflexive, symmetric, and transitive) and it partitions the space of isomorphisms into equivalent classes.

Definition 6 (Kernel). *Let $\phi : R \to S$ be a homomorphism between rings. We define the* **kernel** of ϕ denoted as $\ker(\phi)$ as the preimage of the element zero, O_S. That is

$$\ker(\phi) = \{x \in R : \phi(x) = 0\}.$$

Since $\phi(0) = 0$, we have that $0 \in \ker(\phi)$. As in linear algebra we show that if $\ker(\phi) = \{0\}$, then *phi* is injective. That is

Proposition 2.2.3. *Let ϕ an homomorphism on rings. Then ϕ is injective if and only if* $\ker(\phi) = \{0\}$.

Proof.

"$\Longrightarrow$" Let us assume that ϕ is injective. Then choose $x \in \ker\phi$, we show that $x = 0$. From $\phi(x) = \phi(0) = 0$ and f being injective we see that $x = 0$.

"$\Longleftarrow$" Let us now assume that $\ker(\phi) = \{0\}$. Choose $x, y \in R$, such that $x \neq y$. If $\phi(x) = \phi(y)$, then $\phi(x - y) = \phi(x) - \phi(y) = 0$, and $x - y \in \ker(\phi)$. Then since $\ker(\phi) = \{0\}$, $x = y$, this contradicts the hypothesis. So $\phi(x) \neq \phi(y)$ and ϕ is injective. □

2.3 Ideals

Definition 7 (integral domain). *A ring R is an* **integral domain** *or* **domain** if $0 \neq 1$ and whenever $a, b \in R$ and $ab = 0$, either $a = 0$ or $b = 0$.

Example 2.3.1.

- The set of integers $\mathbb{Z}$ is a domain.
- The ring of continuous functions is not a domain. Pick, for example a function $f(x)$, such that $f(x) = 0, x \in [a, b]$ and $f(x) \neq 0$, $x \in [a, b]$, and a function $g(x)$, such that $g(x) \neq 0, x \in [a, b]$ and $f(x) = 0, x \in [b, c]$ (with $a, b, c \in \mathbb{R}$ with $a < b < c$. Then $fg = 0$, but $f \neq 0$ and $g \neq 0$. So the ring of continuous functions is not a domain.
- The set of univariate polynomials over a ring R. This is defined as $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, with $a_i \in R$ with the addition and multiplication rules from elementary algebra. The largest i such that $a_i \neq 0$, is known as the **degree** of the polynomial and it is noted as $\deg(f)$. If R is a domain, then $\deg(fg) = \deg(f) + \deg(g)$, since R is a domain and the product of the two largest powers, which are both non-zero, should not be zero. So the set of polynomials over a ring R is a domain.

Definition 8 (ideal). *A subset $I \neq \emptyset$ of a commutative ring R is an* **ideal** *if:*

(i) $f, g \in I \Longrightarrow f + g \in I$.

(ii) $f \in I, h \in R \Longrightarrow fg \in I$.

I is called **trivial** *if $I = \{0\}$, and* **proper** *if $I \neq R$.*

The second condition above is sometimes known as the **closure under inside-outside multiplication** . This (and the fact that the unit 1 is not necessarily part of an ideal) make the difference between the definition of an ideal and a subring 4. Any subring is an ideal, but no any ideal is a subring. Recall that a subring needs to have the unit element 1. Ideals do not have to have the unit 1.

The simplest examples of ideals are the trivial sets $\{0\}$ and the whole ring R. Another example is the even numbers (or any set of the form $n\mathbb{Z}$, for a fixed $n > 1$. It is closed under sum and inside-outside multiplication. However this ideal does not have the unit element 1, so it is not a subring. Any homomorphism of rings will create proper ideas. We show this next

Proposition 2.3.1. *Let $\phi : R \to S$ be a homomorphism of rings. Then* $\ker(\phi)$ *is a proper ideal of R.*

Proof. We already showed that $I = \ker(\phi)$ is a subring, then we do not have to show closure. Since $\phi(1) = 1$, we have that $1 \notin I$, so this ideal does not have the unity and so it is a proper set of R □

Definition 9 (**generated ideal**). *Let $f_1, \cdots, f_n$ be a set of elements of a ring R. The generated ideal is defined by the equation:*

$$\langle f_1, \cdots, f_n \rangle = \{h_1 f_1 + \cdots + h_n f_n \mid h_1, \cdots, h_n \in R\}\}$$

The set $\{f_1, \cdots, f_n\}$ is called the **generating set** .

It is easy to show that the generated set is indeed an ideal. Observe that while in vector spaces the coefficients are chosen over the field $\mathbb{K}$ here the coefficients h_i belong to the ring R. As an example if we use the generating set $\{x, x^2\}$, we obtain all polynomials of the form $ax + bx^2$. See that for example constants are not included here, and in particular the unit 1 is not part of the generated ideal. In this case the generated ideal is an ideal without unit.

The generated ideal above has a nice interpretation. Assume that the generator set is $\{f_1, \cdots, f_n\}$. Define the following system of equations $f_1 = f_2 = \cdots f_n = 0$. Then by multiplying each equation by h_i and adding we find

$\sum h_1 f_i = 0$. In this sense the geneated set consists of all polynomial linear combinations of the equations $f_1 = f_2 = \cdots f_n = 0$.

The definition above can be extended to any subset $S \subset R$. That is we can defined $\langle S \rangle$ as the finite linear combinations of elements of S, or in symbols elements of the form $\sum_{i=1}^{n} h_i f_i$, with $h_i \in R$, $f_i \in S$. If the number of elements in S is finite we say that the ring $\langle S \rangle$ is **finitely generated** .

The simplest generated ideal is that spanned by only one element of R. That is, the set $I = \langle f \rangle = \{gf | g \in R\}$ for $f \in R$ is an ideal generated by only one element. This idea is called a **principal ideal** and f is called a **principal generator** of I. In particular $R = \langle 1 \rangle$. A simple example is given by the even numbers. The even numbers are defined as the set $\mathbb{P} := \{2n : n \in \mathbb{Z}\}$. This is the set generated by the integer 2, or is $\mathbb{P} = \langle 2 \rangle$. So the integer set has as many ideals as its size $\aleph_0$. [6]

Definition 10 (**Principal Ideal Domain (PID)**). *If for a given ring R, each ideal is principal the ring is called* **Principal Ideal Domain.**

We show that the integers $\mathbb{Z}$ form a PID.

Proposition 2.3.2. *The integers $\mathbb{Z}$ are PID.*

Proof. Let $I \subset \mathbb{Z}$ be an ideal; we want to show that I is generated by only one element of $\mathbb{I}$, that is, it is a principal. If $I = 0$, then $I = \langle 0 \rangle$. Let us assume then that $I \neq 0$, so there is a smallest positive number on I. We call this number n and claim that $I = \langle n \rangle$. Let us pick $m \in I$ and divide it by n with remainder. The division theorem (a proof of Euclid's the division theorem is found here [7]) states that there should be a quotient q and a remainder r such that $m = qn + r$, with $0 \leq r < n$. We proof that $r = 0$. We have that $r = m - qn \in I$, and since we assumed that n is the smallest positive in I, then $r = 0$. This means that every number on I is of the form qn, and the set $\mathbb{Z}$ is PID. □

We need to be careful here. Assume that we have the following ideal:

$$I_{23} = \langle \{2, 3\} \rangle = \{2n + 3m : n, m \in \mathbb{Z}\}.$$

That is the ideal consists of all the multiples of 2 together with the multiples of 3, and their combinations. Then by choosing $n = 0$ we get all multiples of

[6] We show this in proposition 2.3.2.

[7] http://www.math.fsu.edu/p̃kirby/mad2104/SlideShow/s5_1.pdf

3, and by choosing $m = 0$ we get all multiples of 2. We could say that 2 is the smallest positive integer in the ideal I_{23}, but then that 3 being in I_{23} can not be obtained from 2 with an integer multiplication, so the proof above is wrong. In fact that is not the case. We let to the reader to prove that $I_{23} = \mathbb{Z}$, and that in general $\langle\{p, q\}\rangle$ is equal to $\langle\{o\}\rangle$, where $o = \gcd(p, q)$. It also can be shown that the generated ideal is the smallest set containing the generator set. That is

$$\langle\{a_1, \cdots, a_n\}\rangle = \bigcap_{a_i \in J} J$$

where J is any ideal having any of the a_i, $i = 1, \cdots, n$. The arguments used here

We now extend this result to the univariate polynomials. The Euclid's division theorem was extended to polynomials by Gauss. In this case a polynomial p can be written as a $p = qd + r$, where $0 \leq \deg(r) < \deg(q)$, provided that $q \neq 0$, and we prove this first.

Proposition 2.3.3. *Let $q \in \mathbb{K}[x]$ be a non-zero polynomial. Then for $p \in \mathbb{K}[x]$ there are unique polynomials $d, r \in \mathbb{K}[x]$ such that $p = dq + r$ where $\deg(r) < \deg(q)$.*

Proof. Let us assume first that $\deg(p) < \deg(q)$. Then we can write $p = 0q + r$, where $r = p$, with $\deg(r) < \deg q$, and the theorem was proven. Let us now assume $\deg(p) \geq \deg(q)$. We can write

$$\begin{aligned} p(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ q(x) &= b_0 + b_1 x + \cdots + b_m x^m \end{aligned}$$

with $a_m, b_n \neq 0$, and $n \geq m$.

The idea is proceed as performing the first division step $p(x)/q(x)$, which will lower the degree of the polynomial $p(x)$ and get a residual. That is, from dividing the leading order coefficients and subtracting powers we get the factor $(a_n/b_m)x^{n-m}$, and as in the first step of division we find the residual $r(x)$, by subtracting the multiplication of this monomial by $q(x)$ and subtracting this from $p(x)$. That is

$$r(x) = p(x) - \left(\frac{a_n}{b_m} x^{n-m}\right) q(x).$$

Note that the degree of this residual is lower than n since the term $a_n x^n$ was eliminated by the subtraction. If $\deg(r) < \deg(q)$ we are done, otherwise we can apply the same method (that is divide the resulting $r(x)$ by $d(x)$) which will produce a new residual with lower degree since the leading order is again eliminated. This process should end in $r = 0$, or such that $\deg r < \deg q$, since we are descending from n down by finite steps.

We now show the uniqueness of d and r. Let us assume that there are different d' and r' satisfying the properties of the theorem. Without loss of generality let us assume that $\deg r' \geq \deg r$. That is we have

$$p = dq + r = d'q + r'$$

This is

$$r - r' = q(d - d')$$

So either $\deg(r - r') \geq \deg(q)$ or $r - r' = 0$. $\deg(r - r') < \deg(q)$, so $r = r'$, and then it falls that $d = d'$. This shows the uniqueness of the representation. □

Note that we are basically describing here the algorithm of polynomial division. In this sense this is an algorithmic proof. In fact, the first step of a division is called reduction as shown in the next definition, and an iterative method for reducing polynomials until the residual has lower degree than the quotient is what we know as polynomial division.

Definition 11 (Reduction). *A polynomial r is a reduction of p by q if $h = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(q)} q$ is the remainder after the first step of dividing p by q. This is denoted*

$$p \xrightarrow{q} h.$$

We can apply iterative reductions such as

$$p \xrightarrow{q} h_1 \xrightarrow{q} h_2 \xrightarrow{q} \cdots \xrightarrow{q} h_{n-1} \xrightarrow{q} h_n = r \tag{2.7}$$

until $\deg(h_n) < \deg q$. This is the algorithm to do polynomial division. The whole chain of operations above is noted as

$$p \xrightarrow{q}_{+} r$$

- **Initialization:** $f = f_1 \quad , \quad g = f_2$.
- **while** $g \neq 0$

$$\begin{array}{ccc} f & \xrightarrow{g}_{+} & r \\ f & = & g \\ g & = & r \end{array}$$

Figure 2.1: Greatest Common Divisor (gcd) Algorithm

With this we can easily write the Euclid's algorithm to find the greatest common divisor (gcd) of two polynomials. This is Given two polynomials f_1 and f_2 such that at least one of the is none zero we can find $f = \gcd(f_1, f_2)$ as follows:

We know that a division has four elements: dividend, divisor, quotient, and remainder. The symbol $f \xrightarrow{g} r$ shows three of those elements, f is the dividend, g is the divisor, and r the remainder. While this notation is widely accepted we propose to include in the notation the quotient, since this is useful sometimes, and ignore the inclusion of the quotient when it is not needed. That is, we could write the symbol $f \xrightarrow[q]{g} r$ which shows the four elements of the division, with q being the quotient, to mean that $f = qg + r$. It is interesting that if f, q, g, r and integer numbers we write $f \equiv r \pmod{q}$, to mean the same thing, but here the g factor is left out. So, polynomial reduction can be seen as finding the module of a polynomial in a residual equivalent class.

Proposition 2.3.4. *Let $\mathbb{K}$ be a field. Then the polynomial ring $\mathbb{K}[x]$ is a PID.*

Proof. The proof of this proposition is almost identical to that of proposition 2.3.2. Here we change the "minimal positive number " by the minimal degree of the polynomial, and then the residual $r = m - qn \in I$ should have a smaller degree that the minimal (here r, m, q, n are all polynomials, with $m, q \in I$). Then $r = 0$. Of course, this time we used proposition 2.3.3 instead of the regular division on integer numbers. □

We see that the previous proposition is proved by showing the existence of a single generator for the ideal, however it does not provide an algorithm

to find such a generator. The next proposition shows again that the ring $[K]$ is a PID and it provides an algorithm to find the generator of the ideal. The gcd.

Proposition 2.3.5. *Let $f_1, \cdots, f_n$ be non-zero polynomials in $\mathbb{K}[x]$, then*

$$\langle f_1, \cdots, f_n \rangle = \langle \gcd(f_1, \cdots, f_n) \rangle.$$

Proof. By definition the gcd is a common divisor of each f_i. Let us call this gcd by h, so $f_i = hg_i$ and so any element of the form $f = \sum a_i f_i$ can be written as $f = \sum hg_i f_i = h(\sum g_i f_i)$ so $f \in \langle h \rangle$, since $\sum g_i f_i$ is an element of the ring $\mathbb{K}[x]$. □

Most rings are not PIDs. We illustrate two examples of rings which are no PIDs.

(i) The multivariate polynomials. To make it easy let us use polynomials in just two variables $\mathbb{K}(x, y)$. We choose the ideal $\langle x, y \rangle$. This is given by the set $A = \{\sum(ax + by) : a, b \in \mathbb{K}\}$. The terms ax are generated only by functions of x and the elements by by functions of y, we need at least two functions to generate the whole space so there is no any principal generator and so the set A is not a PID.

(ii) Polynomials over a ring R. Let us consider the set $I = \langle 2, x \rangle$. That is $I = \{2a + bx : a, b \in \mathbb{Z}\}$. If I is a PID this means there there is an element $p \in \mathbb{Z}[x]$ such that $\langle p \rangle = I$. In particular, since $2 \in I$, there exists some q such that $pq = 2$, and since $\deg(2) = 0$, then $\deg q = 0$ (we know that $\deg pq \geq \deg p$ and $\deg pq \geq \deg q$). Hence integer the factorization of 2 into pq, implies that $p = \pm 1$ or $p = \pm 2$. We show that any of these options generates a contradiction, and hence I can not be generated by a single element p. Since $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}[x]$, and $I \subsetneq \mathbb{Z}[x]$, then the choices ± 1 are ruled out. We know that $x \notin \pm\langle 2 \rangle$, so we also rule out ± 2, and conclude that $I \neq \langle p \rangle$ and $\mathbb{Z}[x]$ is not a PID.

Proposition 2.3.6. *A polynomial f is a member of the ideal I generated by g if an only if*

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

Proof. The meaning of $f \xrightarrow{g}_+ 0$ is that the division between f and g is an exact division, or that $f = hg$, for some polynomial h. Then f is in the ideal generated by g. □

We now define the basis of an ideal.

Definition 12 (**basis of an ideal).** *If the every element of an ideal I with generating set $B = \{f_1, \cdots, f_n\}$, is expressed uniquely as a linear combination (product of the form $\sum h_i f_i$ with $h_i \in R$) in a unique way then the generating set B is called a basis for I. As in vector spaces there is no need to have a unique base for an ideal I.*

To appreciate the importance of basis in the solution of equations (as an example) we assume that we want to solve the system of equations

$$f = 0 \quad , \quad f \in I \tag{2.8}$$

where I is an ideal generated by the functions f_i, $i = 1, \cdots, n$. The number of functions in the ideals of polynomials is infinity (unless the ideal is the trivial set $\{0\}$ which does not have interest here). We show that the solution of system 2.8 is the same as the solution of the finite system

$$f_i = 0 \quad , \quad i = 1, \cdots, n.$$

If an element $\boldsymbol{x}$ is in the solution space of $f = 0$, for each f in the ideal, then it is in the solution space of $f_i = 0$, $i = 1, \cdots, n$ since the ideal contains all the equations and in particular those f_i, $i = 1, \cdots, n$. On the other hand, if $\boldsymbol{x}$ is in the solution space of the equations f_i, $i = 1, n$, then $f_i(\boldsymbol{x}) = 0$, and so for any function f such that $f = \sum_{i=1}^{n} a_i f_i$,

$$\sum_{i=1}^{n} a_i f_i(\boldsymbol{x}) = 0.$$

since each $f_i(\boldsymbol{x}) = 0$, so $f(\boldsymbol{x}) = 0$, and $\boldsymbol{x}$ is a solution of the complete system 2.8. Then it is powerful to be able to reduce an infinite number of equations to just a few and obtain the same solution. In fact, we want to go beyond this and be able to transform the finite system of equations into another finite system of equations which is easier to solve and provides the same solution. Think for example in Gaussian elimination. We go from a full matrix (a linear multivariate system) to a triangular matrix which

is much easier to solve. The idea of the Gröbner bases is to extend the Gaussian elimination method to non-linear polynomial equations. That is, replace the system of equations for another which has the same solution but it is easy to understand both from the algebraic (the equations) point of view as well as from the geometric (solution of these equations as set of curves, surfaces,hypersurfaces, or any combination of those) point of view. The solution set of a polynomial or system of polynomial equations is known as a **variety.** For example the solution of the equation $x^2+y^2+z^2-1=0$ is a sphere of radius 1 centered at the origin $(0,0,0)$. The concept of variety is similar to that of **manifold** . The difference is that manifolds can not have singular points while variety can.

We can establish relationships between ideals and varieties. For example given a variety V we can define a map

$$I(V) = \{f \in \mathbb{K}[x_1, \cdots, x_n] \mid f(a_1, \cdots, a_n) = 0 \ \ \forall (a_1, \cdots, a_n) \in V\}.$$

On the other hand given an ideal I, let V be the map

$$V(I) = \{(a_1, \cdots, a_n) \in \mathbb{K}^n : f(a_1, \cdots, a_n) = 0 \quad \forall f \in I\}.$$

Let us show that indeed $I(V)$ is an ideal. Let $f, g \in I(v)$, and $a \in \mathbb{K}$. Then for each $(a_1, \cdots, a_n) \in V$, $f_1(a_1, \cdots, a_n) = 0$, and $f_2(a_2, \cdots, a_n) = 0$. So clearly $[af_1 + f_2](a_1, \cdots, a_n) = 0$, for all $a \in \mathbb{K}$. Then $(af_1 + f_2) \in I(V)$. So $I(V)$ is an ideal. We want to write $I(V)$ as the generated of some set of elements f_i. That is

$$I(v) = \langle f_1, \cdots, f_n \rangle = \left\{ \sum f_i h_i \mid h_i \in R \right\}.$$

There are two questions here

(i) **Existence:** Can we do this? The answer is "yes" and this will be shown as the Hilbert Basis Theorem 2.4.4.

(ii) **How? :** This is the main reason behind this document and will be discussed in detail later.

We need to interact between geometry and algebra. That is, given a variety V can we find an ideal $I(V)$, and vice-versa, given an ideal I can we find a

variety $V(I)$ corresponding to this ideal and what is the relationship of the ideal I and $I(V(I))$? That is, we have the follwing sequence of operations

$$\begin{array}{ccccc} \text{polynomials} & & \text{variety} & & \text{ideal} \\ f_1, \cdots, f_m & \longrightarrow & V(f_1, \cdots, f_m) & \longrightarrow & I(V(f_1, \cdots, f_m)) \, . \end{array}$$

The exact relation between $\langle f_1, \cdots, f_m \langle$ and $I(V(f_1, \cdots, f_m))$ is known as the **Nullstellensatz** problem . The word *Nullstellnsatz* is a german word formed by three words: Null(zero), Stellen(Places), Sats(Theorem).

We ask $I(V(f_1, \cdots, f_m)) \stackrel{?}{=} \langle f_1, \cdots, f_m \rangle$. We show that $\langle f_1, \cdots, f_m \rangle \subset I(V(f_1, \cdots, f_m))$ and then we illustrate with a counter-example that other inclusion is not always true.

Proposition 2.3.7. *If $f_1, \cdots, f_m \in \mathbb{K}[x_1, \cdots, x_n]$, then $\langle f_1, \cdots, f_m \rangle \subset I(V(f_1, \cdots, f_m))$.*

Proof. Let $f \in \langle f_1, \cdots, f_m \rangle$, so $f = \sum_{i=1}^{m} h_i f_i$, for some $h_i \in \mathbb{K}[x_1, \cdots, x_n]$, $i = 1, \cdots, m$. Since $f_i = 0$ in $V(f_1, \cdots, f_m \rangle$, then their weighted sum vanishes as well there and so $f \in I(V(f_1, \cdots, f_m))$. □

For the counter example let us choose $V(x^2, y^2)$. The equations $x^2 = y^2 = 0$, imply that $V(x^2, y^2) = \{0, 0\}$. We show that $I(\{0, 0\}) = \langle x, y \rangle$ for the two variable polyomials. Any polynomial $h_1(x, y)x + h_2(x, y)y$ vanishes at the origin (that is at $x = y = 0$), so $\langle x, y \rangle \subset I(\{0, 0\})$. Let us now assume that $f = \sum_{ij} x^i y^j$ vanishes at the origin, or in otherwords $f \in V(\{0, 0\})$, then we can write

$$\begin{aligned} f &= a_{00} + \sum_{ij>0} a_{ij} x^i y_j \\ &= 0 + \left(\sum_{i>0} a_{ij} x^{i-1} y^2 \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \in \langle x, y \rangle. \end{aligned}$$

Then we found that $I(V(x^2, y^2)) = \langle x, y \rangle$. Still $x \notin \langle x^2, y^2 \rangle$ since every polynomial of the form $h_1(x, y)x^2 + h_2(x, y)y^2$ has degree at least 2. Then $\langle x^2, y^2 \rangle \subsetneqq \langle x, y \rangle$, and $\langle x^2, y^2 \rangle \subsetneqq I(V(x^2, y^2))$.

Another way to generate ideals is by using intersection of other ideals or sums of over ideals. That is I

Proposition 2.3.8. *If I_1 and I_2 are ideals of a ring R, then*

(i) *$I = I_1 \cap I_2$ is an ideal of R.*

(ii) *$J = I_1 + I_2 := \{x_1 + x_2 : x_1 \in I_1, x_2 \in I_2\}$ is an ideal of R with $I_i \subset J$, $i = 1, 2$.*

Proof.

(i) We need to proof closure. Let us assume $i = 1, 2$. If $a, b \in I$, then $a, b \in I_i$, and so $a + b \in I_i$, so $a + b \in I$. Assume now that $h \in R$. The $ha \in I_i$, and so $ha \in I$.

(ii) Let us assume $a, b \in J$ and $h \in R$. Then $a = x_1 + x_2$, $x_i \in I_i$ and $b = y_1 + y_2$, with $y_i \in I_i$. Then $a + b = (x_1 + y_1, x_2 + y_2) \in J$, since I_1 and I_2 are ideals. Now, $ha = hx_1 + hx_2$, and since both I_i, $i = 1, 2$ are ideals then $ha \in J$. So J is an ideal.

Now $I_j \subset J$, since $0 \in I_i$ (take $h = 0$, so $ha = 0$ for each $a \in I_i$), then $I_i = I_i + \{0\} \subset J$.

In fact, in the list of examples 2.2.1 we show that an arbitrary intersection of subrings is a subring. We can extend this proposition to an arbitrary intersection of ideals in the same way, and to a finite sum or ideals for the second part, where and induction argument will apply there. □

We now develop the residue classes on ideals, which generalizes the concept or residual classes shown in section 2.1.1

Definition 13 (Residue class). *Given $a \in R$, and I an ideal of R, the set $[a] := a + I := \{a + x : x \in I\}$ is defined as the* **residue class of a module I.** *The set of residue classes $[a]$, $a \in R$ defines a partition of the ring R given by*

$$\begin{array}{rccc} \phi_{R/I} : R & \to & \mathcal{P}(R) \\ x & \mapsto [x] & \end{array}$$

where is $x \in R$, is associated with its class and $\mathcal{P}(R)$ is the collection of subsets of R. This function is actually a homomorphism, and the collection of classes $[x]$ (also known as **cosets** *) is defined as the* **quotient space** *denoted by R/I.*

If $[a] = [b]$ we say that $a \equiv b \pmod{I}$ as we did in section 2.1.1.

Note that if $I = n\mathbb{Z}$, this reduces to the definition of residue class provided in section 2.1.1. For an example of a quotient space, let $0 < r \in \mathbb{Z}$, then

$$\mathbb{Z}/m\mathbb{Z} = \{i + m\mathbb{Z} : 0 < i < r, i \in \mathbb{Z}\}.$$

We can force the homomorphism above to be surjective by defining it a

$$\begin{aligned} \phi_{R/I} : R &\to R/I \\ x &\mapsto [x] = a + I. \end{aligned} \tag{2.9}$$

This homomorphism is known as **the canonical homomorphism from R to R/I.**

From the set of theorems for homomorphisms in rings we will only present one. Let us assume that $\phi : R \to S$ is an homomorphism. We would like to construct a bridge that goes from R to its canonical representation under some R/I for an ideal I of R, and from there to S. This will prove to be a useful decomposition.

We know that $\ker(\phi)$ is a ring. We can consider an ideal $I \subset \ker(\phi)$, and then use the canonical mapping from $R \to R/I$, and then construct another homomorphism from R/I to S. This map takes any class in R/I and from we define the image of this class as the function ϕ apply to a representative of this class (this function should take all the elements of the class into the same element in S). This is,

Theorem 2.3.9 (**Homomorphism Theorem).** *Let $\phi : R \to S$ be a homomorphism of rings, and I an ideal of a ring R such that $I \subset \ker(\phi)$. Call χ the canonical homomorphism from R to R/I. Then the map*

$$\varphi : R/I \to S \tag{2.10}$$

$$[x] = (x + I) \mapsto \phi(x), \tag{2.11}$$

is a homomorphism of rings such that $\varphi \circ \chi = \phi$. In addition, φ is surjective if an only if ϕ is surjective and it is injective it and only if $I = \ker(\phi)$.

Proof. We prove the theorem in several steps:

- **Verify that φ is well defined.** Note that the class $[x]$ can have up to an infinite number of representatives (any $x + z, z \in I$). We should verify that if two representatives x, y belong to the same class $[x]$, then $\phi(x) = \phi(y)$ and so $\varphi([x]) = \varphi([y])$. First, we see that as sets $x+I = y+I$, and so $x-y \in I$, and since $I \subset \ker(\phi)$, then $\phi(x-y) = 0$, so $\phi(x) = \phi(y)$, so φ is well defined.

- **Verify additivity.** That is $\varphi(x+y) = \varphi(x) + \varphi(y)$. We assert that $[a+b] = [a] + [b]$, since $(a+I) + (b+I) = (a+b) + I$, so if $x = [a]$, and $y = [b]$, $\varphi(x+y) = \varphi([a]+[b]) = \varphi([a+b]) = a+b = \varphi(x) + \varphi(y)$.
- **Verify multiplicability :** Similarly, since $[a][b] = [ab]$ (proof this), then $\varphi(xy) = \varphi(x)\varphi(y)$.
- **Show that the map between units applies.** The unit of R/I is $[1] = 1 + I$, and $\varphi([1]) = 1$.
- **Show the function composition identity.** $(\varphi \circ \phi)(x) = \varphi(\phi(x)) = \varphi([x]) = \phi(x)$**.**
- **Surjectivity.**

$$\begin{aligned} \phi \text{ is subjective} &\iff \forall y \in S, \exists x \in R, \text{ such that } y = \phi(x) \\ &\iff \forall y \in S, \exists x \in R, \text{ such that } y = \varphi([x]) \\ &\iff \varphi \text{ is surjective .} \end{aligned}$$

- **Injectivity for** $I = \ker(\phi)$**.**

  (i) " $\Longrightarrow$ " Let us assume that φ is injective We show that $\ker(\phi) = I$. We already know that from the hypothesis that $I \subset \ker(\phi)$. Let us assume $x \in \ker(\phi)$. Then $\varphi([x]) = \phi(x) = 0$. Since φ is injective, it follows that $[x] = x + I$ is the zero in R/I. That is $x + I = I$. So $x \in I$, and so $\ker(\phi) \subset I$, and $I = \ker(\phi)$. Since I is the zero of R/I, we find that ϕ is

  (ii) "$\Longleftarrow$" Let us assume $I = \ker(\phi)$. Assume $[x], [y] \in R/I$, with $[x] \neq [y]$, then $[x-y] \neq [0] = I$. That is $[x-y] = a + I$, with $a \neq I$, then $\varphi([x-y]) = \varphi([a]) \neq 0$, since $a \notin I = \ker(\phi)$. Then $\varphi([x]) \neq \varphi([y])$ and so φ is injective.

□

We now introduce the definition of **module** which is something like a vector space where instead of using the coefficients from a field $\mathbb{K}$ for scaling vectors, it is using the elements of a ring R.

Definition 14 (**module over a ring** R)**.** *Given a set M together with two binary operations, addition and scalar multiplication, satisfying the following properties:*

(i) **closure:** *M is closed under addition and scalar multiplication. That is, for any $f, g \in M$ and $a \in R$, $af + g \in M$.*

(ii) **dual distribution:** *For all $a, b \in R$ and all $f, g \in M$, we have that $a(f + g) = af + ag$, and $(a + b)f = af + bf$.*

(iii) **associative of scalars:** *For all $a, b \in R$ and $f \in M$, $(ab)f = a(bf)$*

(iv) **addition associative:** *For each $f, g, h \in M$, $(f+g)+h = f+(g+h)$.*

(v) **commutative on addition:** *For each $f, g \in M$, $f + g = g + f$.*

(vi) **Identity in** *R: If 1 is the multiplicative identity in R, then $1f = f$ for all $f \in M$, then we say that M is* **module over the ring** *R.*

A **sub-module** *N, is a subset M which is closed under both binary operators (sum and multiplication).*

It is clear that if $M \subset R$ then M is an ideal. However modules are more general than ideas because they do not necessarily have to be subsets of the ring R. It is in this way that a module is like a vector space over a ring instead of over a field. For example we can think of vectors of elements of the form

$$\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

with $a_i \in R$. These vectors are not elements of a ring (until we define what multiplication of two of these vectors means) but we can provide them with the regular sum (entry-by-entry) commonly used in vector spaces and the scalar product where the scalars are elements of the ring R (or another ring). It is easy to verify that the set of such vectors is a module over a ring R. If the space of scalars R is a field, then there is no distinction between a module and a vector space.

We would like to use all we know from vector spaces into modules, however this is no possible. Modules are a bit more difficult. We will define a base in the same way we defined basis for rings and vector spaces. Bases of modules might or might not exist, and if they do they do not need to have the same cardinal as in the case of vector spaces.

Definition 15 (**generated modules**). *Let $f_1, \cdots, f_n$ be a set of elements of a module M over a ring R. The generated set of M is defined by the equation:*

$$\langle f_1, \cdots, f_n \rangle = \{h_1 f_1 + \cdots + h_n f_n \mid h_1, \cdots, h_n \in R\}$$

The set $\{f_1, \cdots, f_n\}$ is called the **generating set** .

We now define the basis of a module:

Definition 16 (**basis of a module**). *If the every element of a module M with generating set $B = \{f_1, \cdots, f_n\}$, with $f_i \in M$, is expressed uniquely as a linear combination (product of the form $\sum h_i f_i$ with $h_i \in R$) in a unique way then the generating set B is called a basis for the module M. If a module has a basis, then the module is called a* **free module** .

As in vector spaces there is no need to have a unique base for a module M. In fact the existence of a basis is not guaranteed, and if it exists, it does not have to have a fixed cardinal number.

For example, the elements

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} , \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} , \cdots , \boldsymbol{e}_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

form a basis for the module R^n.

We now introduce the definition of a **syzygy module** .

Definition 17 (**sysygy**). *For any $f_i \in \mathbb{K}[x_1, \cdots, x_n]$, $i = 1, \cdots, m$, the set*

$$\text{syz}(f_1, \cdots, f_m) := \{(h_1, \cdots, h_m) \in R^m \mid h_1 f_1 + \cdots + h_m f_m = 0\}$$

is a module over $R = \mathbb{K}[x_1, \cdots, x_n]$ called the **sysygy module** . A **representation** *of f with respect to $(f_1, \cdots, f_m)$, is an element $H = (h_1, \cdots, h_m)$ such $h_i \in \mathbb{K}[x_1, \cdots, x_n]$, and $f = \sum_{i=1}^{m} h_i f_i$.*

As an exercise let us show the first property of a module on the sysygy set. The other properties are easily derived from the fact that R is a ring.

(i) **closure:** Let us assume that $\boldsymbol{h} = (h_1, \cdots, h_m)$ and ,$\boldsymbol{l} = (l_1, \cdots, l_m)$ are in $\text{syz}(f_1, \cdots, f_m)$, and $a \in R = \mathbb{K}[x_1, \cdots, x_n]$. From the definition of sysygy we have that

$$\sum h_i f_i = 0 \quad , \quad \sum l_i f_i = 0$$

so

$$\sum a(h_i + l_i) f_i = a \sum h_i f_i + a \sum l_i f_i = 0.$$

Where we apply the distributive law using the definition of ring in R. By definition of sysygy this means that $a(h_i + l_i) \in \text{syz}(f_1, \cdots, f_m)$.

For the particular case of polynomials on two or three variables the sysygy modules are free modules. It is interesting to observe that the sysygys are like orthogonal spaces to a given "vector" of functions in R^n, and the representation is like the coefficient vector in some basis. Observe that if H and H' are representations of f, then $H - H'$ is in a syzygy of $(f_1, \cdots, f_m)$, and similarly if H is a representaion and S is a sysygy of $(f_1, \cdots, f_m)$, then $H + S$ is a representation of f with respect to $(f_1, \cdots, f_m)$.

2.4 The Hilbert Basis Theorem

The importance of Hilbert Basis Theorem is that it guarantees that the algorithms to find a basis for an ideal are finite and every variety is the solution of a finite set of polynomials. Before stating and showing the theorem we need to set up a few definitions and results.

Definition 18 (**Ascending Chain Condition).** *Assume an arbitrary ascending chain of ideals in a ring R. That is $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$. If there exists $n \in \mathbb{N}$ such that $I_n = I_{n+i}$ $\forall i \in \mathbb{N}$, we say that the chain satisfies the* **ascending chain condition (ACC)** .

We show that the union of a countable set of sets in an ascending chain of ideals is an ideal.

Lemma 2.4.1. *Let us assume a countable chain $\{I_i\}_{i=1}^{\infty}$ of ideals of a ring R. Then*

$$I = \cup_{i=1}^{\infty} I_i$$

is an ideal.

Proof. The last example in the example's list 2.2.1 shows that the union of an ascending chain of subrings is a ring. The same arguments used there apply here. Recall that an ideal does not have to have unity. The closure of the sum can be taken from that of the closure of the sum as a subring. Now for the product. Assume $h \in R$, and $f \in I$, then , $f \in I_i$, for some $i \in \mathbb{N}$, and since I_i is an ideal then $hf \in I_i \subset I$, so I is an ideal.

In particular if the chain is ACC, we have that

$$I = \cup_{i=1}^{\infty} I_i = I_n$$

which is an ideal by hypothesis. □

Definition 19 (**Noetherian Ring**). *An ideal that is finitely generated is called a* **Noetherian Ring** .

We show that the two definitions above are equivalent.

Lemma 2.4.2. *The properties of ACC and Noetherian ring are equivalent.*

Proof.

(i) "$\Longrightarrow$" Let us assume that R satisfies the ACC. We prove by contradiction that this ideal is finitely generated. That is, let us assume that an arbitrary ideal I is not finitely generated. For any $f_1 \in I$, there exists $f_2 \in I$, such that $f_2 \notin \langle f_1 \rangle$ (otherwise I would be generated by f_1). Then we can write $\langle f_1 \rangle \subsetneqq \langle f_1, f_2 \rangle$. Likewise there exists $f_3 \in I$, such that $f_3 \notin \langle f_1, f_2 \rangle$, and so $\langle f_1 \rangle \subsetneqq \langle f_2, f_2 \rangle \subsetneqq \langle f_1, f_2, f_3 \rangle$. We can proceed by induction and find that the chain $\{\langle f_1, \cdots, f_n \rangle\}_{n \in \mathbb{N}}$ does not satisfy the ACC condition, then R does not satisfy the ACC, which contradicts the hypothesis. Then I is finitely generated.

(ii) "$\Longleftarrow$" We assume that R is a Noetherian ring; that is, any ideal in R is finitely generated. We show that it has the ACC property. Let $\{I_i\}$, $i \in \mathbb{N}$ be countable ascending chain of ideals of R. Consider $I = \cup_{i=1}^{\infty} I_i$. From Lemma 2.4.2, we see that I is an ideal. Then I is finitely generated, that is, there is $n \in \mathbb{N}$ such that $I = \langle f_1, \cdots, f_n \rangle$, for some $f_i \in R$, $i = 1, \cdots, n$. For each of these f_i, there is an index $j_i \in \mathbb{N}$, such that $f_i \in I_{j_i}$. Since the number of indices i is finite, so it is the number of indices j_i. Choose $n = \max\{j_i\}_{i=1}^{n}$, then $I = I_n$, and then R has the ACC property.

□

As a final lemma before proving the Hilbert's basis theorem let us state:

Lemma 2.4.3. *If R is a Noetherian ring, then so is $R[x]$.*

Proof. Most of the work on proving Hilbert's theorem basis theorem is put into this lemma. We know about R but no much about $R[x]$. Given an ideal J for $R[x]$ we want to pass information from this ideal to R where we know that R is Noetherian, use all we know and construct (get back) a chain of reasoning that lead us into $R[x]$. In the connection between R and $R[x]$ we know that the coefficients of the polynomials in $R[x]$ are in the ring R. From these coefficients the leading order coefficient is most important since it carries on it the signature for the degree of the polynomial. So the work is use the Noetherian attributes on leading order coefficients and map this back to the polynomials in $R[x]$.

We divide the proof in small sessions.

- **Build an ACC chain.** Let R be a Noetherian ring, and J an ideal of $R[x]$. Any member of $R[x]$ is of the form $p(x) = a_0 + a_1x + \cdots + a_nx^n$, where $a_n \neq 0$. We define $I_n = \{a_n : p(x) \in J\} \cup \{0\}$. To see that I_n is an ideal for R we verify the closure of the sum and the inside/outside product. Given two polynomials of order n, with leading coefficients a_n and b_n, the sum of the polynomials have as a leading coefficient $a_n + b_n$. Now, given an element $h \in R$, and $f \in I_n$, then hI_n corresponds to the set of polynomials of the form $hp[x]$, with $p[x] \in R[x]$. The leading term in any polynomial gets multiplied by h, where h is a zero order polynomial (a constant). So if $h \in R$, and $p[x] \in R[x]$, then $hp \in I_n$. Also $I_n \subset I_{n+1}$, since for $f \in I_n$ means that there is some $a_n \neq 0$, leading order coefficient of a polynomial $p(x)$. Since $R[x]$ is a ring of polynomials in x then $xp(x) \in R[x]$, but the leading coefficient of $xp(x)$, which is a_n is also in I_{n+1}, so $I_n \subset I_{n+1}$. From the definition of Noetherian, and since $I_i \subset R$, then each I_i is finitely generated, and so we apply Lemma 2.4.2 to assert that there is some N such that for any $n \geq N$ $I_N = I_n$.

- **Find a finite generating set.**

  Since each I_i is finitely generated we can write $I_i = \langle r_{i1}, \cdots, r_{ij_i} \rangle$. The idea is to build a set of polynomials which is finite and generates J. Corresponding with each coefficient r_{ik} we can associate a polynomial p_{ik} where r_{ik} is the leading order coefficient. Since the indices i are

finite (N of them) and the indices j are also finite (up to $\max\{j_i\}_{i=1}^{N}$) then their product is a finite number. We assert that the polynomials p_{ik} generate J. We define $L := \langle p_{ij} \rangle$ (with $i = 1, \cdots N$, and $j = 1, \cdots j_i$) and must prove that $J = L$. We show the two inclusions:

(i) "$L \subset J$" : Any element $f \in L$ is of the form $f = \sum a_{ij} p_{ij}[x]$ with $a_{ij} \in R$, with i, j defined above. Since, by definition, the ideal I is an ideal of leading order coefficients of polynomials in J, the leading order coefficients of each $p_{ij}[x]$ are sitting in I, and for each $a_{ij} \in R$, the leading coefficient of $a_{ij} p_{ij}$ should be also in I, and so any sum of these, so $f \in J$. So $L \subset J$.

(ii) "$J \subset L$" : Let us assume $f \in J$ with $\deg f = n$. We use induction over n.

(1) **Initial test:** If $f = 0$ or $n = 0$, then the leading order coefficient is in I_0, and $f \in L$.

(2) **Induction :** Let $n > 0$ and assume that for any $f \in J$ with $\deg(J) < n$, $f \in L$. Call r the leading order coefficient of f.

(a) $n \leq N$: since $r \in I_n$, we have that $r = \sum_{k=1}^{j_n} c_k r_{nk}$, for some $c_k \in R$. Then the polynomial $g = \sum_{k=1}^{j_n} c_k p_{nk}$ is of degree n, and has as leading order coefficient r. Hence $g \in L$, and from the first inclusion above $g \in J$. By construction, since both f, g have the same leading order coefficient r, their difference is such that $\deg(f - g) \leq n - 1$, and $f - g \in J$ (since both f, g are elements of j). By the induction hypothesis $f - g \in L$, and since $g \in L$, then $f \in L$.

(b) $n > N$ $r \in I_n = I_N$, and $r = \sum_{k=1}^{j_N} c_k r_{Nk}$, for some $c_k \in R$. Then the polynomial $g = \sum_{k=1}^{j_N} c_k x^{n-N} p_{Nk}$ is of degree n, and has as leading order coefficient r. Hence $g \in L$, and from the first inclusion above $g \in J$. By construction, since both f, g have the same leading order coefficient r, their difference is such that $\deg(f - g) \leq n - 1$, and $f - g \in J$ (since both f, g are elements of j). By the induction hypothesis $f - g \in L$, and since $g \in L$, then $f \in L$.

□

Here is the statement of the Hilbert Basis Theorem

Theorem 2.4.4 (Hilbert Basis Theorem). *Any ideal I of the multivariate polynomial ring $\mathbb{K}[x_1, \cdots, x_n]$, has a finite generating set. That is, there is a set $\{f_1, \cdots, f_n\}$ such that $I = \langle f_1, \cdots, f_n \rangle$.*

Proof. The proof is by induction. For $n = 1$, the proof is done in the previous lemma 2.4.3. We assume that the theorem is valid for any $n - 1 > 0$. That is, any ideal of the ring $R = \mathbb{K}[x_1, \cdots x_{n-1}]$ has a finite generating set. We apply once more lemma 2.4.3 and find that $R[x_n]$ is Noetherian. However $R[x_n] = \mathbb{K}[x_1, \cdots x_{n-1}][x_n] = \mathbb{K}[x_1, \cdots x_n]$. □

We need to clarify the last equality above. Let us show examples in 2D and then explain the meaning for higher dimensions.

Consider the polynomial $p(x, y) = x^3y^2 - xy + x + 2 \in \mathbb{Z}[x, y]$. We can think about this a as polynomial in x, where the coefficients for the powers $\{1, x, x^2, x^3\}$ are respectively $\{2, 1, -y, y^2\}$. This second set is a set in $\mathbb{Z}[y]$. Seen this way $p(x, y) \in (\mathbb{Z}[y])[x] = \mathbb{Z}[y][x]$. Note the parenthesis around $\mathbb{Z}[y]$. We are saying that $R = \mathbb{Z}[y]$ is a ring of polynomials in one variable y, and that $p(x, y) \in R[x]$. We could have said, that $p(x, y)$ is a polynomial on y, where the coefficients of the powers $\{1, y, y^2\}$ are $\{x + 2, -x, x^3\}$, and this second set in in the ring $R = \mathbb{Z}[x]$, then we say that $p(x, y) \in R[y] = \mathbb{Z}[x][y]$.

In general we write a multivariate polynomial in $(x_1, \cdots, x_n)$ as

$$p(x_1, \cdots, x_n) = \sum_{(i_1, \cdots, i_n) \in \mathbb{N}^n} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$$

for some finite number of multidimensional indices of the form $(i_1, \cdots, i_n)$, and $a_{i_1 \cdots i_n} \in \mathbb{K}$. That is $p(x_1, \cdots, x_n) \in \mathbb{K}[x_1, \cdots, x_n]$. Each $0 \leq i_j \leq N$ is a power of x_j and it limited by some fixed $N \in \mathbb{N}$. We can separate the last variable from the rest and write

$$p(x_1, \cdots, x_n) = \sum_{(i_1, \cdots, i_n) \in \mathbb{N}^n} \left(a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_{n-1}} \right) x_n^{i_n}$$

Each coefficient of $x_n^{i_n}$ is a polynomial in the variables $(x_1, \cdots, x_{n-1})$ in the ring $R = K[x_1, \cdots, x_{n-1}]$. Then we say that

$$p(x_1, \cdots, x_n) \in R[x_n] = K[x_1, \cdots, x_{n-1}][x_n].$$

The proof of Hilbert basis theorem is an existence proof and in no way reveals an algorithm to find such basis. To be of practical use we need to find explicit generators for ideals. This is the topic of the next chapter.

Chapter 3

Gröbner Bases

3.1 Introduction

Hilbert basis theorem 2.4.4 determines that given an ideal of a multivariate polynomial ring, we can find a finite generator set. While the proof is valid it does not suggest of a method to find such generator set. Bruno Buchberger [1] in his Ph.D. thesis in 1965 developed an algorithm to find generators for ideals of multivariate polynomial rings. Buchberger set the Göbner name after his thesis advisor Wolfgang Gröbner [2]

The scope of applications of Gröbner bases is vast. Buchberger [3] himself presents a short and clear introduction to Gröbner bases and its applications. Probably the most common application is in the solution of system of multivariate polynomial equations.

We know (from Hilbert basis theorem) that every ideal $I \subset \mathbb{K}[x_1, \cdots, x_n]$ should be finitely generated. That is, there is a finite collection $\{f_1, \cdots, f_n\}$, such that $I = \langle f_1, \cdots, f_n \rangle$. We would like to find the set of objects f_i. We want to know if given a function f, how can determine if this function belongs to I. We want to know if given a function f, how can we determine if this function belongs to I. For univariate polynomials the answer is simple. For example we can say that $f \in \langle g \rangle$ if by dividing f by g we find zero remainder. The same technique we do for integer division. The difficulty with multivariate polynomials is that the algorithm for division is not unique

[1] https://en.wikipedia.org/wiki/Bruno_Buchberger

[2] https://en.wikipedia.org/wiki/Wolfgang_Gr%C3%B6bner

[3] http://people.reed.edu/ davidp/pcmi/buchberger.pdf

and depends heavily on the ordering set. While there is no question about the ordering of univariate polynomials based on the power of the variable, the power of a variable does not uniquely defines an order in multivariate polynomials. We define ordering in multivariate polynomials in the next section.

3.2 Ordering in multivariate polynomials

The algorithm to perform division of univariate polynomials is strongly dependent on the leading order terms (LT). The division algorithm is shown after the definition of reduction 11.

We know that for univariate polynomials the order is set by the value of the exponent. That is, we can order a univariate polynomial base on the order $x^0 < x^1 < \cdots < x^n$. For example $f(x) = 1 + 2x + x^2$, which is an ascending order. We could also order it according to $x^0 > x^1 > \cdots > x^n$. For example $f(x) = x^2 + 2x + 1$, which is in descending order. There are some syntax rules that we learn from middle school on writing polynomials. For example,

- If the first term is positive we avoid writing the plus "+" sign. That is the default for positive leading order coefficient.
- If the coefficient is "1" we can avoid writing this integer. That is, instead of $1x$ we just write x.
- Parenthesis should not be used to separate one term/factor from another. That is, at least two objects needed to be grouped together need parenthesis.
- etc.

These rules might have an aesthetic character but they are important if we want to implement computer algorithms with polynomials.

For the case of multivariate polynomials we can use either the variables, or the powers on them, or a combination of both. Any multivariate polynomial is a linear combination of monomials of the form $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. More specifically, the set

$$\mathbb{T}^n = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha_i \in \mathbb{N}\,,\, i = 1, \cdots, n\}$$

is a bases which can be use to generate any arbitrary polynomial, provided the exponents α_i are finite. For simplification sometimes we write x^α instead of $x^{\alpha_1} \cdots x^{\alpha_n}$, where $\alpha = (\alpha_1, \cdots, \alpha_n)$.

Definition 20 (**Leading Term, Leading Coefficient, Leading Monomial).** *Let $f \in \mathbb{K}[x_1, \cdots, x_n]$ be a non-zero polynomial. We denote by* $\mathrm{LT}(f)$ *the highest order term in f under a fixed monomial order. The leading monomial is the leading term by replacing whatever coefficient it has by 1. This is noted as* $\mathrm{LM}(f)$*, and it is actually the leading power product in the set $\mathbb{T}^n$. The leading coefficient is the coefficient of the leading term and it is noted* $\mathrm{LC}(f)$.

For example,

$$f(x, y) = 3x^2y + 2x + 6$$

- Leading power product $\mathrm{LM}(f) = x^2y$.
- Leading coefficient $\mathrm{LC}(f) = 3$.
- Leading term $\mathrm{LT}(f) = \mathrm{LC}(f)\mathrm{LM}(f) = 3x^2y$.

We use $\mathrm{LM}(f)$ when we do not want to deal with the coefficient of $LT(f)$. The advantage of $\mathrm{LM}(f)$ over $\mathrm{LT}(f)$ is that $\mathrm{LM}(f)$ is unique while $\mathrm{LT}(f)$ is equal to $\mathrm{LM}(f)$ up to a constant $k \in \mathbb{K}$.

In writing a polynomial we want to be sure that any monomial has a unique representation. For example we do not write $f(x, y) = x^2y + z + 2x^2y$. Instead we write $f(x, y) = 3x^2y + z$. Where we avoid writing the monomial x^2y twice, by collecting terms so that this power representation is unique. For the ordering we want to use what we already know from univariate polynomials. For example, if x^α divides x^β, then we order these terms as $x^\alpha \leq x^\beta$. That is, we impose the order in the exponents $\alpha \leq \beta$. Whatever order we pick it should be a **total order.** That is, any two elements a, b could be compared with any of the three relations

$$a < b \quad , \quad a = b \quad or \quad a > b.$$

We also should have some compatibility rule, that is if for example $1+2x+x^2$ is increasing order, the multiplication of this function by x^4 provides $x^4 + 2x^5 + x^6$, which still is in increasing order. In addition we need to have **well ordering** . That is, any non-empty collection should have a smallest element. More formally:

Definition 21 (monomial order). *A monomial order of* $\mathbb{K}[x_1, \cdots, x_n]$ *is any relation "*$>$*" on a set of monomials* $x^\alpha \in \mathbb{K}[x_1, \cdots, x_n]$ *such that*

(i) *"*$>$*" is a total ordering.*

(ii) *"*$>$*" is compatible with multiplication in* $\mathbb{K}[x_1, \cdots, x_n]$*. That is, if* $x^\alpha > x^\beta$ *and* x^γ *is any monomial, then* $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^{\beta+\gamma} = x^\beta x^\gamma$*.*

(iii) "$>$" *is a well-ordering. That is, every non-empty collection of monomials has a smallest element with respect to "*$>$*".*

We see that for the univariate polynomials $\mathbb{K}[x]$, there is only one monomial ordering which is the degree order

$$x^n > x^{n-1} > \cdots > x^2 > x > 1.$$

however for polynomials in two or more variables the number of ordering choice is infinity. This is given by the following proposition.

Proposition 3.2.1. *If a ring* $\mathbb{K}[x_1, \cdots, x_n]$*, with* $n \geq 2$*, there are uncountable number of distinct monomial orders.*

Proof. As I pointed above the strategy used to proof the infinitiness of an ordering in $\mathbb{N}^2$ is not correct. In fact by defining the comparison as comparison between polynomials, and in the case of a linear equations ($\mathbb{N}^2$), Mohammed (or whoever did this proof) is comparing two lines. We can only compare two lines if they are parallel other than that, if they cross, in some domain some points are above and some are below. Then that is not a well defined order.

Define weights $w_1 \geq 0$ and $w_2 \geq 0$, such that $w = (w_1, w_2)$ and $w_1 + w_2 = 1$.

Then we define $(a_1, a_2) \geq_w (b_1, b_2)$ if $w_1 a_1 + w_2 a_2 \geq w_1 b_1 + w_2 b_2$.

We should first verify (and this did not happen in the proof of "Robbiano's theorem) that $>_w$ is a well defined monomial order. That is we need to prove (and we will at each step) that

(i) $\geq_w$ **is a total order.** That is, either $a >_w b$, or $a <_w b$, or $a =_w b$ Since for any couple $a = (a_1, a_2) \in \mathbb{N}^2, b = (b_1, b_2) \in \mathbb{N}^2$, we have that either $w_1 a_1 + w_2 a_2 < w_1 b_1 + w_2 b_2$, or $w_1 a_1 + w_2 a_2 = w_1 b_1 + w_2 b_2$, or $w_1 a_1 + w_2 a_2 > w_1 b_1 + w_2 b_2$, then $>_w$ is a well a total order.

(ii) "$\geq_w$" **is compatible with multiplication** (or sum in this case). That is, if $a \geq_w b$, then for any $c = (c_1, c_2) \in \mathbb{N}^2$, $a + c \leq_w b + c$.

We show this. We have that, since $w_1(a_1 + c_1) + w_2(a_2 + c_2) = (w_1a_1 + w_2a_2) + (w_1c_1 + w_2c_2) \geq (w_1b_1 + w_2b_2) + (w_1c_1 + w_2c_2) = w_1(b_1 + c_1) + w_2(b_2 + c_2)$ then $a + c \geq_w b + c$.

Here we used the fact that $a \geq_w b$, and that $w_i \geq 0$, $i = 1, 2$.

(iii) $\geq_w$ **is a well-ordering.** That is, there is a minimum. This is true from $a \geq_w 0$. That is $0w_1 + 0w_2 = 0 \leq a_1w_1 + a_2w_2$, for all $(a_1, a_2) \in \mathbb{N}$.

This shows that $\geq_w$ is a valid monomial order. Now, count how many weights can you build with $w_1 \geq 0, w_2 \geq 0$, $w_1 + w_2 = 1$? As many as $\aleph_1$.

Examples: Some orders are listed below, and they are included in the proposed order here. The lexicographic order is found by choosing $w = (1, 0)$, the reverse lexicographic order is found by choosing $w = (0, 1)$, the pure grading order is found by choosing $w = (0.5, 0.5)$. Any order $w = (a, b)$ with $a > b$ gives priority to the first variable. If $b > a$ the priority is given to the second variable. The level of priority for the first variable ranges along the continuous interval $a[0, 1]$ (likewise for the second variable) . The case $a > b$ or $a < b$ is a graded lexicographic order (or reverse lexicographic order).

We still need to show that if there are two weights $w = (w_1, w_2)$, and $v = (v_1, v_2)$, such that $w \neq v$ then we can distinguish one order from the other. That is $\geq_w \neq \geq_v$. For the order $\geq_w$ we have that if $a = (a_1, a_2) \geq_w (b_1, b_2)$ then

$$w_1a_1 + w_2a_2 \geq w_1b_1 + w_2b_2$$

We want to find a, b such that

$$v_1a_1 + v_2a_2 < v_1b_2 + v_2b_2$$

This will make the two weights distinct. We can rewrite these two equations, by defining $c_1 = a_1 - b_1, c_2 = a_2 - b_2$, as

$$\begin{aligned} w_1c_1 + w_2c_2 &\geq 0 \\ v_1c_1 + v_2c_2 &< 0 \end{aligned}$$

Since $w_1 = 1 - w_2$, and $v_1 = 1 - v_2$, then we write

$$w_1 c_1 + (1 - w_1)c_2 \geq 0$$
$$v_1 c_1 + (1 - v_1)c_2 < 0$$

or (assuming $w_1, v_1 \neq 1$). We are counting infinite orders and we do not care about not counting this particular one, still if $w_1 = 1$, this is the reverse lexicographic order, which is a valid order. We have then

$$c_2 \geq \frac{w_1 c_1}{1 - w_1} \tag{3.1}$$
$$c_2 < \frac{v_1 c_1}{1 - v_1} \tag{3.2}$$

The first equation 3.1 corresponds to a half-plane (in the (c_1, c_2) coefficients) above the line $c_2 = w_1 c_1/(1 - w_1)$, which goes through the origin. The second equation 3.2 corresponds to the lower half plane under the line $c_2 = v_1 c/(1 - v_1)$ through the origin. Since the two lines do not have the same slope (otherwise $w = v$), there is an angular intersection with infinite many points (c_1, c_2) such that the two conditions are satisfied.

For the case of $n \geq 2$, choose $w = (w_1, \cdots, w_n)$ and $w_1 + \cdots + w_n = 1$, and fill up the details. □

We introduce two orders.

Definition 22 (Lexicographic Order). *Let $a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n)$, be exponent vectors. We say that $x^a >_{lex} x^b$ if in the vector difference $a - b$, the left most non-zero entry is positive.*

For example the $x_1 x_2^3 >_{lex} x_2^4 x_3^5$, since the vectors a and b here are given by $a = (1, 2, 0)$, and $b = (0, 4, 5)$. The left most entry is $1 > 0$, or $1 - 0 > 0$.

The other order is

Definition 23 (Graded Lexicographic Order). *Let $a = (a_1, \cdots, a_n)$ and $b = (b_1, \cdots, b_n)$ be exponent vectors. We say that $x^a >_{grlex} x^b$ if*

$$|a| = \sum_{i=1}^{n} a_i > |b| = \sum_{i=1}^{n} b_i, \text{ or if } |a| = |b| \text{ then } x^a >_{lex} x^b.$$

That is, in the grlex order we first compute the total degree of the monomial (the sum of all exponents) and if two monomials present the same degree, then we choose the lexicographic order. For example $x_1^2 x_2^3 x_3^3 >_{grlex} x_2^5 x_3^2$.

Now that we have established a proper order we are ready to define a multivariate polynomial division.

3.3 Reduction and Division of Multivariate Polynomials

An important problem in ideals is the *ideal membership problem* for which we establish the following definition:

Definition 24 (Ideal membership problem). *Given an ideal I and a function f we ask whether or not $f \in I$. If the answer is "yes" then we say that f satisfies the ideal membership status with respect to I.*

For example, we ask if $g = x + 1 \in I = \langle x^2 + 1 \rangle$. We could factor $x^2 + 1 = (x - i)(x + i)$, where $i = \sqrt{-1}$, and clearly either $x + i \in I$ and $x - i \in I$, but $x + 1 \notin I$. Factorization (as integration) is not always easy and we want to use a more deterministic tool. That tool is polynomial division (reduction). By dividing $x^2 + 1$, by $x + 1$, we find that the quotient is $x - 1$ and the remainder is 2. That is $x^2 + 1 = (x + 1)(x - 1) + 2$. So since the remainder is not 0, we say that $x + 1 \notin I$, but we have to be more careful if we use multivariate polynomials.

As in the univariate polynomials the key of division is reduction. We reduce a polynomial by "properly" canceling the LT and leaving it to the next lower order term as the new LT. This process is applied iteratively until a finish criterion is reached. In the case of univariate polynomials this criterion is that the remainder has lower degree than the divisor.

The definition of reduction 11 used for univariate polynomials apply equally for multivariate polynomials. We illustrate this with an example.

Let us assume that $f(x, y) = xy^2 + xy + y^3 + 1$ were we are using the lexicographic ordering, and we want to reduce f module $g(x, y) = x + y$. We have $\mathrm{LT}(g) = x$, and $\mathrm{LT}(f) = xy^2$, so $\mathrm{LT}(f)/\mathrm{LT}(g) = y^2$. The reduction step is given by

$$\begin{aligned} f(x,y) - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g(x,y) &= xy^2 + xy + y^3 + 1 - y^2(x + y) \\ &= \cancel{xy^2} + xy + y^3 + 1 - \cancel{xy^2} - y^3 \\ &= xy + \cancel{y^3} + 1 - \cancel{y^3} \\ &= xy + 1 \end{aligned} \tag{3.3}$$

The residual at this point is $r(x, y) = xy + 1$, and the divisor (the same) is $q(x, y) = x + y$. Since in the lexicographic order $r(x, y) > g(x, y)$ we

still have not reach the end of the division. The quotient (or cofactor) is $q(x,y) = \mathrm{LT}(f)/\mathrm{LT}(q) = y^2$.

We say then that f reduces to r mod g and write the symbols In symbols we write

$$f \xrightarrow{g} r.$$

As in equation 2.7 we can apply successive steps like this to achive the multivariate polynomial division. That is,

$$f \xrightarrow{g} h_1 \xrightarrow{g} h_2 \xrightarrow{g} \cdots \xrightarrow{g} h_{n-1} \xrightarrow{g} h_n = r$$

where the h_i are intermediate remainders and $h_n = r$ is the final remainder such that in the in the monomial order $r(x,y) < g(x,y)$.

One more step or reduction is achieved by considering that the current remainder is $h_1(x,y) = xy + 1$ and $h_1(x,y) > g(x,y)$. Since $\mathrm{LT}(h_1)/\mathrm{LT}(g) = y$, we find

$$h_2(x,y) = h_1(x,y) - yg(x,y) = xy + 1 - y(x+y) = 1 - y^2.$$

At this point $h_2(x,y) < g(x,y)$ and the division ends.

This division allows as to express

$$f = r + \sum_{i=1}^{m \leq n} q_i g \tag{3.4}$$

as follows:

(i) In the first step we have that

$$h_1(x,y) = f(x,y) - \frac{\mathrm{LT}[f(x,y)]}{\mathrm{LT}[g(x,y)]} g(x,y) = xy + 1.$$

That is

$$f(x,y) = h_1(x,y) + q_1(x,y)g(x,y), \tag{3.5}$$

with $q_1 = \mathrm{LT}[f(x,y)]/\mathrm{LT}[g(x,y)] = y^2$, then

$$f(x,y) = (xy+1) + y^2(x+y).$$

(ii) In the second step we have

$$h_2(x,y) = h_1(x,y) - q_2(x,y)g(x,y)$$

with $q_2(x,y) = \mathrm{LT}[h_1(x,y)]/\mathrm{LT}[g(x,y)] = y$. Hence

$$h_1(x,y) = h_2(x,y) + \frac{\mathrm{LT}[h_1(x,y)]}{\mathrm{LT}[g(x,y)]}g(x,y).$$

and replacing this in equation 3.5 we find

$$\begin{aligned} f(x,y) &= h_2(x,y) + [q_1(x,y) + q_2(x,y)]g(x,y) \\ &= (1-y^2) + y^2(x+y) + y(x+y) \end{aligned}$$

At this moment since $(1-y^2)$ is not divisible of $(x+y)$ (see that $\mathrm{LT}(1-y^2) = -y^2$ and $\mathrm{LT}(x+y) = x$, and $-y^2$ does not divide x) the division terminated.

The division algorithm shown in 2.7 is finite because the monomial order is a well-ordering method and so there is a minimum, and also since the chain of h_i is a descending chain.

Expression 3.4 allows us to decompse f as a product (factorization) of g with the sum $\sum_{i=1}^{m\geq n} q_i$, with remainder r. If $r = 0$ the division is exact and we found a factorization of f module g. In fact we reduced f module g to 0. Otherwise if $r \neq 0$, we found that $f \equiv r \pmod{g}$.

To show that the division algorithm is non-unique and it depends on the chosen order, let us assume the order $y > x$ and do the division again. Recall

$$f(x,y) = xy^2 + xy + y^3 + 1, \tag{3.6}$$

in the $x > y$, order and

$$f(x,y) = y^3 + y^2x + yx + 1, \tag{3.7}$$

in the $y > x$ order. Likewise $g(x,y) = y + x$. The leading order ratio $L[f(x,y)]/L[g(x,y)]$ is y^2, and $h_1 = yx + 1$, from which $f(x,y) = y^2(x + y) + yx + 1$. Now $\mathrm{LT}[h_1(x,y)]/\mathrm{LT}[g(x,y)] = x$, and $h_2 = -x^2 + 1$ from which $f(x,y) = y^2(x+y) + x(x+y) + 1 - x^2$. Note that in this case, the computations of the reductions on $f(x,y)$ for $y > x$, could have been copied from those assuming $x > y$ by switching the variable names x and y.

Up to this moment we have considered g as a fixed divisor, how about using different divisors each time? For example, let us assume that we have two divisors g_1 and g_2 and we reduce f in the following way

$$f \xrightarrow{g_1} h_1 \xrightarrow{g_2} h_2$$

and so on, In this case we say that

$$\begin{aligned} h_1 &= f - q_1 g_1 \quad \text{for some quotient } q_1 \\ h_2 &= h_1 - q_2 g_2 \quad \text{for some quotient } q_2 \end{aligned} \tag{3.8}$$

from which $f = h_1 + q_1 g_1 = h_2 + q_1 g_1 + g_2 g_2$. In general we can we can write $f = r + \sum q_i f_i$, and if we call $G = (1_1, \cdots, g_n)$, then we can write $f \xrightarrow{G}_+ r$.

We formulate the following definition

Definition 25 (reduction). *Let f, r, and $G = \{g_1, \cdots, g_m\}$ a set of polynomials in $\mathbb{K}[x_1, \cdots, x_n]$, with $g_i \neq 0 (1 \leq i \leq n)$. We say that f* **reduces to** *r* **module** *G , denoted*

$$f \xrightarrow{G}_+ r$$

if and only if there exists a sequence of indices $i_1, \cdots, i_s \in \{1, 2, \cdots, m\}$ and a sequence of polynomials $h_1, \cdots, h_{s-1}$, such that

$$f \xrightarrow{g_{i_1}} h_1 \xrightarrow{g_{i_1}} h_2 \longrightarrow \cdots \longrightarrow \xrightarrow{g_{i_s}} h_s$$

Any g_i could be visit several times or none. As a matter of fact, in the case of a single divisor g this is visited repeatadely until the $\deg(h_i) < \deg(g)$. Let us illustrate this with an example with lexicographic order with $y > x$. Choose $f = y^3x$, $g_1 = yx + y, g_2 = y^2 - y, g_3 = y^2$. We have the following chain of operations:

$$f = y^3x \xrightarrow{g_1} y^3x - \frac{y^3x}{yx}(yx+y) = -y^3 \xrightarrow{g_2} -y^3 + \frac{y^3}{y^2}(y^2-y) = -y^2 \xrightarrow{g_3} 0.$$

That is, we could write

$$f = y^2(yx + y) - y(y^2 - y) - 1y^2 = y^2 g_1 - y g_2 - g_3.$$

Then $f \in \langle g_1, g_2, g_3 \rangle$, with representation coefficients $\{q_1, q_2, q_3\} = \{y^2, -y, 1\}$.

In the rest of this section we dicuss the following three questions:

(i) Is this a unique representation in terms of the "basis" $G = \{g_1, g_2, g_3\}$ as in vector spaces?

(ii) What if the residual is non-zero.

(iii) What if the residual h after some reduction using some g_i is such that no g_i in the collection G would divide h ($g_i \not| h$, $i = 1, 2, 3$?)

3.3.1 Uniqueness of Representation

We start with the first question. Let us permute the functions g_i. $\{g_1, g_2, g_3\} = \{y^2 - y, y^2, yx + y\}$ and perform the reduction in this order. That is

$$f = y^3x \xrightarrow{g_1} y^3x - \frac{y^3x}{y^2}(y^2 - y) = y^2x \xrightarrow{g_2} y^2x - \frac{y^2x}{y^2}y^2 = 0.$$

This means that

$$f = yx(y^2 - y) + xy^2 + 0(yx + y).$$

Considering the initial order in g_i we write

$$f = 0(yx + y) + yx(y^2 - y) + xy^2.$$

So while for the first order used in the reduction the coefficients for the original g_i bases where $\{y^2, -y, 1\}$, in the second reduction order the coefficients with respect to the same bases (in the original order) is $\{0, yx, xy^2\}$. Due to the no linearity of the problem and very different from linear vectors spaces, here there could be several representations in terms of the same g_i base functions.

3.3.2 Zero Residual

Now for the second question. Let us consider the set $g_1 = yx + y, g_2 = y^2 - y, g_3 = y^2 + x$. where we just added x at the end of the third g_3 original function. The procedure is almost the same shown above but there is a little change at the end. Let us see:

$$f = y^3x \xrightarrow{g_1} y^3x - \frac{y^3x}{yx}(yx + y) = -y^3 \xrightarrow{g_2} -y^3 + \frac{y^3}{y^2}(y^2 - y) = -y^2$$

At this point the analysis is the same done above, but since now $g_3 = y^2 + x$ we do not have zero residual. That is, following the chain we find

$$-y^2 \xrightarrow{g_3} = -y^2 + \frac{y^2}{y^2}(y^2 + x) = x.$$

We we have a remainder $r = x$. Then we write

$$f = r + \sum_{i=1}^{3} q_i g_i$$

That is

$$f = x + y^2(yx + y) - y(y^2 - y) - (y^2 + x)$$

Then $f \in \langle g_1, g_2, g_3 \rangle + x$. We say that $f \equiv x \pmod{G}$ respecting the order of reduction in G. It might be that a different order produces no residual or a different residual.

In general we can always express

$$f = r + \sum_{i=1}^{m} q_i g_i$$

where q_i are some quotients, r is the residual and g_i is the provided "bases" data set to be used as a reference. More precisely since any g_i could be visited several times we should write

$$f = r + \sum_{i=1}^{m} \left(\sum_{j=1}^{j_i} q_{i_j} \right) g_i$$

and we mark a termination step when $\deg(r) < \deg g_i$, $i = 1, \cdots, m$.

It is interesting that if we found zero remainder $r = 0$, then we found a way to express f as a generated function by the set G, that is if $r = 0$ then $f \in \langle g_1, \cdots, g_m \rangle$, however this is an strict implication and not an equivalence. That is, there could that $f \in \langle g_1, \cdots, g_m \rangle$ and $r \neq 0$ as we show in the following example.

Example 3.3.1. Let $g_1 = xy + 1, g_2 = y^2 - 1 \in \mathbb{K}[x, y]$ with lexicographic order. Dividing $f = xy^2 - x$ by $G = (g_1, g_2)$, result in

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + r$$

with $= -x - y$, so $r \neq 0$. However,

$$xy^2 - x = x(y^2 - 1) + 0.(xy + 1) + 0$$

that is $f \in \langle g_1, g_2 \rangle$ still in lexicographic order the division produces a non-zero resdidual.

Gröbner bases do not suffer from this inconsistency issues, they have unique residual, and if the function is in the ideal, the residual is 0 no matter the order chosen to do the multivariate/multidivisors polynomial division.

3.3.3 Dead End on Residual

Finally, to address the third question we provide the following example:

Assume graded lexicographic order with $x > y$, and

$$\begin{aligned} f &= x^2y + 2y^2 + x + 1 \\ g_1 &= x^2 + 1 \\ g_2 &= y + 1. \end{aligned}$$

Then

$$f = x^2y + y^2 + x + 1 \xrightarrow{g_1} x^2y + y^2 + x + 1 - \frac{x^2y}{x^2}(2x^2 + 1).$$

That is,

$$f \xrightarrow{g_1} h_1 = y^2 + x - y$$
$$q_1 = \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_1)} = \frac{x^2y}{x^2} = y.$$

At this point we recognize that $\mathrm{LT}(g_1) \not| \mathrm{LT}(h_1)$, but $\mathrm{LT}(g_2) | \mathrm{LT}(h_1)$, so we use g_2. Then

$$h_1 \xrightarrow{g_2} h_2 = y^2 + x - y - \frac{y^2}{y}(y + 1) = x - 2y$$
$$q_2 = \frac{\mathrm{LT}(h_1)}{\mathrm{LT}(g_2)} = \frac{y^2}{y} = y.$$

We see that $g_1 \not| h_2$ and $g_2 \not| h_2$. We seem to be locked. However we can try other terms of h_2 which are of lower degree. We can not remove the $\mathrm{LT}(h_2)$ arbitrarily but we can move it to the residual (which at initialization is 0). That is,

$$\begin{aligned} r &= x \\ h_2 &= -2y \end{aligned}$$

This is a valid operations since in the representation $f = r + \sum q_i g_i$, the residual is an independent quantity which can receive any contribution from the h_i expressions which are all residuals of of single step reductions. Now we see that $g_2 | h_2$, so we write

$$h_2 \xrightarrow{g_2} h_3 = -2y - \frac{y^2}{y}(y+1) = -2y + \frac{2y}{y}(y+1) = 2$$
$$q_3 = \frac{\mathrm{LT}(h_2)}{\mathrm{LT}(g_2)} = \frac{-2y}{y} = -2$$

We then have

$$f = x^2y + y^2 + x + 1 = r + q_1 g_1 + q_2 g_2 + q_3 g_2.$$

We formulate the general algorithm for multivariate polynomial division on several divisors in Figure 3.1. The vector $\boldsymbol{q} = (q_1, \cdots, q_m)$ is the vector of quotients. Each q_i can be visited several times, or none. For example for $f(x,y) = x^2$, and $g_1 = x, g_2 = y$ g_2 will not visit the algorithm and $q_2 = 0$, we have $f = r + g_1 q_1$ with $r = 0$, and $q_1 = x$. The "while" loop will finish since eventually h will become zero. At some point r will be reduced in such a way that $r \not| g_i$ for any $i = 1, \cdots m$, in which case the flag "found" will be set to 1, then the last if statement will result in $h : r - r = 0$.

Let us develop a complete example.

Example 3.3.2. This example is taken from the Adams and Loustaunau [4] book.

Let $f = x^2y^2 - w^2, g_1 = x - y^2w, g_2 = y - zw, g_3 = z - w^3, g_4 = w^3 - w$ in $\mathbb{Q}[x,y,z,w]$. We use the lexicographic order $x > y > z > w$ to reduce f

[4] http://www.ams.org/bookstore-getitem/item=GSM-3

Input: $f, g_1, \cdots, g_m$, $f_i \neq 0 \quad i = 1 \cdots m$
Output: $q_1, \cdots, q_m, r$, such that $f = r + \sum q_i g_i$
Initialization: $q_i = 0$, $i = 1, , \cdots, m$, $r = 0$, $h = f$
Flags found=0

Loop:

while $h \neq 0$ do
found := 0
for$(i = 1, \cdots m)$
if $\mathrm{LT}(g_i)|\mathrm{LT}(h)$
$q_i := q_i + \dfrac{\mathrm{LT}(h)}{\mathrm{LT}(g_i)}$
$h := h - \dfrac{\mathrm{LT}(h)}{\mathrm{LT}(g_i)}$
found := 1
end if
if found == 1
break
end if
end for
if found == 0
$r := r + \mathrm{LT}(h)$
$h := r - \mathrm{LT}(h)$
end if
end while

Figure 3.1: Multivariate polynomial division with multiple divisors. The symbol := means assignment. The double equal sign == is used to ask in an "if" statement. The "break" instruction exits the "for" loop.

via $G = \{g_1, g_2, g_3, g_4\}$. While the computer algorithm uses h as the symbol to recycle the memory of the remainder after each reduction, for efficiency purposes, we use h_i for clarity in the description.

- g_1 :
  - We initialize $q_i = 0$, $r = 0$, and found $= 0$, $i = 1, 2, 3, 4$. Set $h_1 = f = x^2y^2 - w^2$, and try to do the reduction $f \xrightarrow{g_1} h_2$. That is, $q_1 = \mathrm{LT}(h_1)/\mathrm{LT}(g_1) = x^2y^2/x = xy^2$, and $h_2 = xy^4w - w^2$. The flag found is turned to 1, that is,
  - found $= 1$, so the "for loop " exits and since $h_2 \neq 0$, the for loops restarts again with g_1. That is, we need now to reduce $h_2 \xrightarrow{g_1} h_3$. Since $\mathrm{LT}(g_1) = x | \mathrm{LT}(h_2) = xy^4w$, we have that $q_2 = \mathrm{LT}(h_2)/\mathrm{LT}(g_1) = y^4w$, and $h_3 = y^6w^2 - w^2$.

  At this point we have

  $$f = (q_1 + q_2)g_1 + h_3$$

  which is easy to verify by direct evaluation.

- g_2:
  - Since $\mathrm{LT}(g_1) = x \nmid \mathrm{LT}(h_3) = y^6w^2$, the index i gets incremented. Now we have $\mathrm{LT}(h_3) | \mathrm{LT}(g_2) = y$. Then we find $q_3 = y^5w^2$, and $h_4 = y^5zw^3 - w^2$.
  - Still $\mathrm{LT}(g_2) | \mathrm{LT}(h_4)$ and $\mathrm{LT}(h_4)/\mathrm{LT}(g_2) = y^4zw^3$, so $q_4 = y^4zw^3$, and $h_5 = y^4z^2w^4 - w^2$.
  - Still $\mathrm{LT}(g_2) = y | \mathrm{LT}(h_5) = y^4z^2w^4$, then $\mathrm{LT}(h_5)/\mathrm{LT}(g_2) = y^3z^2w^4$, so $q_5 = y^3z^2w^4$, and $h_6 = y^3z^3w^5 - w^2$.
  - Still $\mathrm{LT}(g_2) = y | \mathrm{LT}(h_6) = y^3z^2w^5$, then $\mathrm{LT}(h_6)/\mathrm{LT}(g_2) = y^2z^3w^5$, so $q_6 = y^2z^3w^5$, and $h_7 = y^2z^4w^6 - w^2$.
  - Still $\mathrm{LT}(g_2) | \mathrm{LT}(h_7) = y^2z^4w^6$, with $\mathrm{LT}(h_7)/\mathrm{LT}(g_2) = yz^4w^6$, so $q_7 = yz^4w^6$, and $h_8 = yz^5w^7 - w^2$.
  - Still $\mathrm{LT}(g_2) | \mathrm{LT}(h_8)$, and $\mathrm{LT}(h_8)/\mathrm{LT}(g_2) = z^5w^7$, with $h_9 = z^6w^8 - w^2$, and $q_8 = z^5w^7$.

We find then that

$$\begin{aligned} h_3 &= (q_3+q_4+q_5+q_6+q_7+q_8)g_2+h_9 \\ f &= g_1\sum_{i=1}^{2} q_i + g_2\sum_{i=3}^{8} q_i + h_9 \end{aligned}$$

- g_3:
  - At this point $\mathrm{LT}(g_2) \nmid \mathrm{LT}(h_9)$, and since the "found" flag is set to 1 the loops exit and starts again (since $h \neq 0$), this time it will go as far as $i = 3$. That is we have that $\mathrm{LT}(g_3) = z|\mathrm{LT}(h_9) = z^6w^8 - w^2$, with $\mathrm{LT}(h_9)/\mathrm{LT}(g_3) = z^5w^8$, so $q_9 = z^5w^8$ and $h_{10} = z^5w^{11} - w^2$.
  - Still $\mathrm{LT}(g_3)|h_{10}$ and $\mathrm{LT}(h_{10})/\mathrm{LT}(g_3) = z^4w^{11}$ with so $q_{10} = z^4w^{11}$, and $h_{11} = z^4w^{14} - w^2$.
  - Still $\mathrm{LT}(g_3)|h_{11}$ with $\mathrm{LT}(h_{11})/\mathrm{LT}(g_3) = z^3w^{14}$, so $q_{11} = z^3w^{14}$, and $h_{12} = z^3w^{17} - w^2$.
  - Still $\mathrm{LT}(g_3)|h_{12}$ with $\mathrm{LT}(h_{12})/\mathrm{LT}(g_3) = z^2w^{17}$, so $q_{12} = z^2w^{17}$ and $h_{13} = z^2w^{20} - w^2$.
  - Still $\mathrm{LT}(g_3)|h_{13}$, with $\mathrm{LT}(h_{13})/\mathrm{LT}(g_3) = zw^{20}$, so $q_{13} = zw^{20}$, and $h_{14} = zw^{23} - w^2$.
  - Still $\mathrm{LT}(g_3)|\mathrm{LT}(h_{14})$ with $\mathrm{LT}(h_{14})/\mathrm{LT}(g_3) = w^{23}$, so $q_{14} = w^{23}$, and $h_{15} = w^{26} - w^2$.

We have

$$\begin{aligned} h_9 &= (q_9+q_{10}+q_{11}+q_{12}+q_{13}+q_{14})g_3+h_{15} \\ f &= g_1\sum_{i=1}^{2} q_i + g_2\sum_{i=3}^{8} q_i + g_3\sum_{i=9}^{14} + h_{15}. \end{aligned}$$

-
  - At this point g_3 does not longer divides h_{15} but we have that $\mathrm{LT}(g_4) = w^3|\mathrm{LT}(h_{15}) = w^{26}$, and $\mathrm{LT}(h_{15})/\mathrm{LT}(g_4) = w^{23}$, setting $q_{15} = w^{23}$, and $h_{16} = w^{24} - w^2$.
  - Still $\mathrm{LT}(g_4)|\mathrm{LT}(h_{16})$ with $\mathrm{LT}(h_{16})/\mathrm{LT}(g_2) = w^{21}$ so $q_{16} = w^{21}$, and $h_{17} = w^{22} - w^2$,
  - Still $\mathrm{LT}(g_4)|\mathrm{LT}(h_{17})$ with $q_{17} = \mathrm{LT}(h_{17})/\mathrm{LT}(g_4) = w^{19}$, and $h_{18} = w^{20} - w^2$.

- Still $\mathrm{LT}(g_4)|\mathrm{LT}(h_{18})$ with $q_{18} = \mathrm{LT}(h_{18})/\mathrm{LT}(g_4) = w^{17}$, and $h_{19} = w^{18} - w^2$.
- We find $q_{19} = \mathrm{LT}(h_{19})/\mathrm{LT}(g_4) = w^{16}$, and $h_{20} = w^{16} - w^2$.
- We find $q_{20} = \mathrm{LT}(h_{20})/\mathrm{LT}(g_4) = w^{13}$, and $h_{21} = w^{14} - w^2$.
- We find $q_{21} = \mathrm{LT}(h_{21})/\mathrm{LT}(g_4) = w^{11}$, and $h_{22} = w^{12} - w^2$.
- We find $q_{22} = \mathrm{LT}(h_{22})/\mathrm{LT}(g_4) = w^9$, and $h_{23} = w^{10} - w^2$.
- We find $q_{23} = \mathrm{LT}(h_{23})/\mathrm{LT}(g_4) = w^7$, and $h_{24} = w^8 - w^2$.
- We find $q_{24} = \mathrm{LT}(h_{24})/\mathrm{LT}(g_4) = w^5$, and $h_{25} = w^6 - w^2$.
- We find $q_{25} = \mathrm{LT}(h_{25})/\mathrm{LT}(g_4) = w^3$, and $h_{26} = w^4 - w^2$.
- We find $q_{26} = \mathrm{LT}(h_{26})/\mathrm{LT}(g_4) = w$, and $h_{27} = 0$.

So

$$h_{15} = g_4 \sum_{i=15}^{24} q_i$$

Then we finally find that

$$f = g_1 \sum_{i=1}^{2} q_i + g_2 \sum_{i=3}^{8} q_i + g_3 \sum_{i=9}^{14} + g_4 \sum_{i=15}^{21} q_i$$

This result is verified by the packge Maxima (previously Macsyma) which produces the following result:

```
(%i52) poly_pseudo_divide(f,[g1,g2,g3,g4],[x,y,z,w]);
4      2   7  5    6    4    5  2  3    4  3  2    3  4      2  5
(%o52) [[w y  + x y , w  z  + w  y z  + w  y  z  + w  y  z  + w  y  z + w  y ,
  8  5    11  4    14  3    17  2    20      23
  w  z  + w   z  + w   z  + w   z  + w   z + w  ,
  23    21    19    17    15    13    11    9    7    5    3
w   + w   + w   + w   + w   + w   + w   + w  + w  + w  + w  + w], 0, 1, 26]
```

Recall that our order is $x > y > z > w$, Maxima does not acknowledges the monomial order in its display. It returns the strings of quotients (corresponding to g_1, g_2, g_3, g_4 in that order) separated by commas "," then the residual (here $r = 0$), then the coefficient "1" indicates here that the output is still in the ring $\mathbb{Q}[x, y, z, w]$, and the number 26, indicates the number of reductions needed.

In summary we obtain that the division of f by G in the order $x > y > z > w$, results in

$$\begin{aligned}
\text{quotient for } g_1 &: xy^2 + y^4w \\
\text{quotient for } g_2 &: y^5w^2 + y^4zw^3 + y^3z^2w^4 + y^2z^3w^5 + yz^4w^6 + z^5w^7 \\
\text{quotient for } g_3 &: z^5w^8 + z^2w^{11} + z^3w^{14} + z^2w^{17} + zw^{20} + w^{23} \\
\text{quotient for } g_4 &: \sum_{i=0}^{11} z^{2i+1}. \\
r &= 0.
\end{aligned}$$

A good practice exercise is to go through the same algorithm by reversing the order of G, that is choosing $G = \{g_4, g_3, g_2, g_1\}$, in that order. The result would be

$$\begin{aligned}
\text{quotient for } g_4 &: xy^2 + xy + x^2yw + x^2z + xyw^2 + x^2w + \\
&+ xw^2 + x + yz + yw + z + w \\
\text{quotient for } g_3 &: x^2yw + x^2w + xyw^2 + xw^2 + yw + w \\
\text{quotient for } g_2 &: x^2y + x^2w^2 + xyw + xw^2 + xw + w^2 \\
\text{quotient for } g_1 &: xw^2 + w.
\end{aligned}$$

It is interesting to observe that the permutation of the g_i polynomials provided the same zero residual $r = 0$, but different quotients. We will refer to this example in the next section.

We now introduce an example with multiple problems, where most of the computations are hidden in purpose, no to deceive the reader but instead, to encapsulate complexity and reveal the important point at this time. A good roadmap for the computational details is provided.

Example 3.3.3. Given $G = \{g_1, g_2, g_3, g_4\}$

$$\begin{aligned}
g_1 &= xy^2 - xz + y \\
g_2 &= xy - xz^2 - yz^4 \\
g_3 &= xz^4 - xz + y^2z^4 + yz^6 + y \\
g_4 &= -y^4z^4 - y^3z^6 - y^3 + y^2z^5 + yz^7 + yz^4 \\
g_5 &= -y^3z^4 - y^2 + yz^5 + yz^2
\end{aligned}$$

provide the following reductions of f with respect to G using the lexicographic order $x > y > z$:

(i) $f = xyz^2 - xz + y^2z^4 + y.$

(ii) $f = xy^2z - xz^5 - y^4z^4 - y^3z^6 - y^3 + yz^4.$

(iii) $f = xyz - xz^6 - y^3z^4 - y^2z^6 - y^2 - yz^8.$

(iv) $f = -xy^3z^6 - xy^3 + xyz^7 + xyz^4 + y^3z^4.$

(v) $f = -2xy^3z^6 - xy^3 + xy^2z^5 + xyz^7 + xyz^4 - y^4z^8.$

(vi) $f = -xy^4z - xy^3z^6 - xy^3 + xy^2z^5 + xyz^7 + xyz^4 + y^6z^4 + y^5z^6 + y^5.$

Solution:

(i) Since $\mathrm{LT}(g_1)$ does not divide $\mathrm{LT}(f)$, then the reduction of (i) under g_1 will provide a 0 quotient. In general, if $\mathrm{LT}(g_i) \nmid f$, $i = 1, \cdots, 4$ and $j, k \in \mathbb{N}$, then the quotient is 0 and the residual is the input (dividend).

$$f \xrightarrow[0]{g_1} f \xrightarrow[z^2]{g_2} xz^4 - xz + y^2z^4 + yz^6 + y.$$

That is

$$f \xrightarrow{\{g_1,g_2\}}_+ xz^4 - xz + y^2z^4 + yz^6 + y \tag{3.9}$$

since this expression is already equal to g_3, then the reduction with respect to g_3 produces 0 residual, further reductions will produce 0 residual. That is

$$f \xrightarrow{G}_+ 0.$$

(ii) $f = xy^2z - xz^5 - y^4z^4 - y^3z^6 - y^3 + yz^4.$

We want to reduce f with respect to G. That is,

$$\begin{aligned} f &\xrightarrow[z]{g_1} \quad -xz^5 + xz^2 - y^4z^4 - y^3z^6 + yz^4 - yz - y^3 \\ &\xrightarrow[0]{g_2} \quad -xz^5 + xz^2 - y^4z^4 - y^3z^6 + yz^4 - yz - y^3 \\ &\xrightarrow[-z]{g_3} \quad -y^4z^4 - y^3z^6 - y^3 + y^2z^5 + yz^7 + yz^4, \end{aligned}$$

Then

$$f \xrightarrow{\{g_1,g_2,g_3\}}_+ -y^4z^4 - y^3z^6 - y^3 + y^2z^5 + yz^7 + yz^4 \tag{3.10}$$

Note that this last polynomial is g_4 so, by using the same arguments as above, we have that

$$f \xrightarrow{G}_+ 0.$$

(iii) Let us reduce $f = xyz - xz^6 - y^3z^4 - y^2z^6 - y^2 - yz^8$ with respect to G.

$$\begin{aligned}
f &\xrightarrow[0]{g_1} && f \\
&\xrightarrow[z]{g_2} && -xz^6 + xz^3 - y^3z^4 - y^2z^6 - y^2 - yz^8 + yz^5 \\
&\xrightarrow[-z^2]{g_3} && -y^3z^4 - y^2 + yz^5 + yz^2 \\
&\xrightarrow[0]{g_4} && -y^3z^4 - y^2 + yz^5 + yz^2
\end{aligned}$$

Then

$$f \xrightarrow{\{g_1,g_2,g_3,g_4\}}_+ -y^3z^4 - y^2 + yz^5 + yz^2 \tag{3.11}$$

and this remainder is precisely g_5, so

$$f \xrightarrow{G}_+ 0.$$

(iv) Let $f = -xy^3z^6 - xy^3 + xyz^7 + xyz^4 + y^3z^4$. We reduce f with respect to G.

$$\begin{aligned}
f &\xrightarrow[-yz^6-y]{g_1} && -xyz^4 - xyz + y^3z^4 + y^2z^6 + y^2 \\
&\xrightarrow[-z+z^4]{g_2} && -xz^3 + y^3z^4 + y^2z^6 + y^2 - yz^5 \\
&\xrightarrow[z^2]{g_3} && +y^3z^4 + y^2 - yz^5 - yz^2 \\
&\xrightarrow[0]{g_4} && y^3z^4 + y^2 - yz^5 - yz^2
\end{aligned}$$

since $\mathrm{LM}(g_4) \nmid y^3z^4$.

Then

$$f \xrightarrow{\{g_1,g_2,g_3,g_4\}}_+ -y^3z^4 + y^2 - yz^5 - yz^2 \tag{3.12}$$

and this remainder is precisely $-g_5$, so

$$f \xrightarrow{G}_+ 0.$$

(v) We reduce $f = -2xy^3z^6 - xy^3 + xy^2z^5 + xyz^7 + xyz^4 - y^4z^8$ with respect to G.

$$\begin{aligned} f &\xrightarrow[-2yz^6-y+z^5]{g_1} -xyz^7 + xyz^4 - xyz + xz^6 + 2y^2z^6 - y^4z^8 + y^2 - yz^5 \\ &\xrightarrow[-z^7+z^4-z]{g_2} -xz^9 + 2xz^6 - xz^3 - y^4z^8 + 2y^2z^6 + y^2 - yz^{11} + yz^8 - 2yz^5 \\ &\xrightarrow[-z^5+z^2]{g_3} -y^4z^8 + y^2z^9 + y^2z^6 + y^2 - yz^5 - yz^2 \\ &\xrightarrow[z^4]{g_4} \quad y^3z^{10} + y^3z^4 + y^2z^6 + y^2 - yz^{11} - yz^8 - yz^5 - yz^2 \end{aligned}$$

(vi) We reduce $f = -xy^4z - xy^3z^6 - xy^3 + xy^2z^5 + xyz^7 + xyz^4 + y^6z^4 + y^5z^6 + y^5$ with respect to G:

$$\begin{aligned} f \xrightarrow[-y^2z-yz^6-y+z^5-z^2]{g_1} & xyz^4 - xyz + xz^6 - xz^3 + y^6z^4 + y^5z^6 + y^5 + y^3z + \\ & y^2z^6 + y^2 - yz^5 + yz^2 \\ \xrightarrow[z^4-z]{g_1} & 2xz^6 - 2xz^3 + y^6z^4 + y^5z^6 + y^5 + y^3z + y^2z^6 + y^2 \\ & + yz^8 - 2yz^5 + yz^2 \\ \xrightarrow[2z^2]{g_3} & y^6z^4 + y^5z^6 + y^5 + y^3z - y^2z^6 + y^2 - yz^8 - 2yz^5 - yz^2 \\ \xrightarrow[-z-y^2]{g_4} & -yz^5 + y^3z^4 - yz^2 + y^2 \end{aligned}$$

and since this last remainder is exactly $-g_5$ then we have that $f \xrightarrow{G} 0$.

Finally let us prove an important property of reductions.

Proposition 3.3.1. *Let $f, g \in \mathbb{K}[x_1, \cdots, x_n]$. For any finite set of non-zero polynomials $G \subset \mathbb{K}[x_1, \cdots, x_n]$, and a power product $X \in \mathbb{T}^n$, we have*

(i) *If $f \in G$, then $f\, g \xrightarrow{G}_+ 0$.*

(ii) *If $f \xrightarrow{G}_+ g \implies Xf \xrightarrow{G}_+ Xg$.*

Proof.

(i) If $f \in G$, then the division fg/f, for non-zero $f \in G$ (if $g = 0$, the result is trivially true) provides a quotient of q and a remainder of 0, since then $fg = qf + r$, with $q = g \in \mathbb{K}[x_1, \cdots, x_n]$, $f \in G$, and $r = 0$.

(ii) Let us assume that $f \xrightarrow{G}_+ g$. That is $f = \sum_{i=1}^m h_i g_i + r$, with some $g_i \in G$, and a remainder $r \in \mathbb{K}[x_1, \cdots, x_n]$, with $\deg(r) < \deg(g_i)$, $i = 1, \cdots, m$. Then $Xf = \sum_{i=1}^m Xh_i g_i + Xr = \sum_{i=1}^m h_i(Xg_i) + R$, with $R = Xr$. Note that $\deg(R) < \deg(Xg_i)$. So $Xf \xrightarrow{G}_+ Xg$.

□

With this we are ready to go into the Gröbner bases theory.

3.4 Gröbner Bases: Theory

The main purpose of this section is to provide a definition for a Gröbner bases and 5 different equivalent characterizations. Each characterization could have been used as a definition and then the original definition would be a new characterization together with the other 4 characterizations. In this section we use the notation $R = \mathbb{K}[x_1, \cdots, x_n]$.

We start with the definition.

Definition 26 (Gröbner Bases). *A set of non-zero polynomials $G = \{g_1, \cdots, g_m\} \subset I$ where I is some ideal on R, is called* **Gröbner basis** *for I if an only if for each $f \in I$ such that $f \neq 0$, there exists $i \in \{1, \cdots, m\}$ such that $\mathrm{LT}(g_i) | \mathrm{LT}(f)$.*

Gröbner bases are sometimes called **standard basis.** Before showing the characterization of the Gröbner bases let us first define the leading term ideal of a subset $S \subset R$.

Definition 27 (**Leading Term Ideal**). *The* **leading term ideal of a subset** $S \subset R$ *is defined by the equation*

$$\mathrm{LT}(S) := \langle \mathrm{LT}(s) : s \in S \rangle.^5$$

We could think that for a given set $G = \{g_1, \cdots, g_m\} \in S$, such that $S = \langle g_1, \cdots, g_n \rangle$, then $\mathrm{LT}(G) := \langle \mathrm{LT}(g_1) \cdots, \mathrm{LT}(g_n) \rangle \stackrel{?}{=} \mathrm{LT}(S)$. However this is not the case. For example, consider $S = \langle g_1 = x + y, g_2 = xy - y \rangle$, using the monomial ordering $x > y$. We have

$$\mathrm{LT}(G) := \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2) \rangle = \langle x, xy \rangle = \langle x \rangle,$$

and $y^2 + y = y(x + y) - (xy - y)$, so $y^2 \in \mathrm{LT}(S)$, but $y^2 \notin \mathrm{LT}(G)$. That is $\langle \mathrm{LT}(G) \rangle \subsetneqq \langle \mathrm{LT}(\langle G \rangle) \rangle$.

One way to prove that a set $G = \{g_1, \cdots, g_m\}$ is not a Gröbner basis for an ideal I, is to find $f \in I$ such that $\mathrm{LT}(f) \notin \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m) \rangle$. For example, choose $g_1 = x^3 - 2xy$, and $g_2 = x^2y - 2y^2 + x$. Then we find that $-yg_1 + xg_2 = x^2$, so $x^2 \in \langle g_1, g_2 \rangle$, still $x^2 = \mathrm{LT}(x^2) \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2) \rangle = \langle x^3, x^2y \rangle$.

We now present a theorem that shows the many forms in which we could see a Gröbner bases. Sometimes one of this forms is considered as a definition.

Theorem 3.4.1. *Let $I \subset R$ a non-zero ideal. The following statements are equivalent for a set $G = \{g_1, \cdots g_m\} \subset I$ of polynomials:*

(i) *G is a Gröbner basis for I.*

(ii) *$f \in I$ if and only $f \xrightarrow{G}_+ 0$.*

(iii) *$f \in I$ if and only if $f = \sum_{i=1}^m q_i g_i$, for some $g_i \in I$, $i = 1, \cdots m$.*

(iv) $\mathrm{LT}(G) = \mathrm{LT}(I)$.

Proof.

- "(i) $\implies$ (ii)"

[5] Notation varies. For example some authors Cox, Little and O'Shea define $\mathrm{LT}(S) = \{\mathrm{LT}(s) : s \in S\}$, and refer to the ideal as $\langle \mathrm{LT}(S) \rangle$.

- " $\Longrightarrow$ " Let $f \in I$. Then there exists r such that $f \xrightarrow{G}_+ r$. That is we can write $f = r + \sum_{i=1}^{m} q_i g_i$. Since $f_i \in I$, $i = 1, \cdots m$, and $f \in I$, then $r \in I$. If $r \neq 0$, then from the definition of Gröbner bases 26 there is an $i \in \{1, \cdots m\}$ such that $\mathrm{LT}(g_i)|\mathrm{LT}(r)$, but this is a contradiction because r is supposed to be reduced with respect to G. Then $r = 0$ and $f \xrightarrow{G}_+ 0$.
- " $\Longleftarrow$" If $f \xrightarrow{G}_+ 0$, then we can find $\{q_1, \cdots q_m\} \subset R$ such that

$$f = \sum_{i=1}^{m} q_i g_i \in I$$

- "(ii) $\Longrightarrow$ (iii)"
  - " $\Longrightarrow$ " Let $f \in I$. This is equivalent to $f \xrightarrow{G}_+ 0$. Then there is a set $\{q_1, \cdots, q_m\} \in I$ such that $f = \sum_{i=1}^{m} q_i g_i$, $(r = 0)$.
  - " $\Longleftarrow$" Since $q_i, g_i \in I$, then $f = \sum_{i=1}^{m} q_i g_i \in I$.
- "(iii) $\Longrightarrow$ (iv)"
  - "$\subset$" Since $G \subset I$, $\mathrm{LT}(G) := \langle \mathrm{LT}(G) : g \in G \rangle \subset \langle \mathrm{LT}(I) : g \in I \rangle = \mathrm{LT}(I)$. Then $\mathrm{LT}(G) \subset \mathrm{LT}(I)$.
  - "$\supset$" Pick $f \in \mathrm{LT}(I)$. We should show that $f \in \mathrm{LT}(G)$. From (iii) $f = \sum_{i=1}^{m} q_i g_i$. It is sufficient to show that $\mathrm{LT}(f) \in \mathrm{LT}(G)$. There exists $i \in \{1, \cdots, m\}$ such that $\mathrm{LT}(f) = \mathrm{LT}(q_i g_i)$, but since $g_i \in G$, then $\mathrm{LT}(q_i g_i) \in \mathrm{LT}(G)$, so $\mathrm{LT}(f) \in LG_G$, so $\mathrm{LT}(I) = \mathrm{LT}(G)$.
- "(iv) $\Longrightarrow$ (i)" Let $f \in I$. By (iv), $\mathrm{LT}(f) \in \mathrm{LT}(I) = \mathrm{LT}(G)$, so

$$f = \sum q_i \mathrm{LT}(g_i).$$

Then $\mathrm{LT}(g_i)|\mathrm{LT}(f)$ and then G is a Gröbner basis.

□

As a consequence we find that if $G = \{g_1, \cdots, g_m\} \subset I$ is a Gröbner basis for an ideal I, then $I = \langle g_1, \cdots, g_m \rangle$. It is obvious that $\langle g_1, \cdots, g_m \rangle \subset I$. Now, if $f \in I$, then since G is a Gröbner basis, and from the previous theorem, $f \xrightarrow{G}_+ 0$ and then $f \in \langle g_1, \cdots, g_m \rangle$.

This result is very important. It says that any ideal I can be generated by the Gröbner basis, which is a finite set.

Proposition 3.4.2. *Let I be an ideal generated by a set S of non-zero terms, and $f \in R$. Then*

(i) $f \in I \iff$ for each term X of $f, \exists Y \in S : Y|X$.

(ii) There exists a finite subset $S_0 \subset S$, such that $I = \langle S_0 \rangle$.

Proof.

(i)
- " $\Longrightarrow$ " Choose $f \in I$. Then since $I = \langle S \rangle$, $f = \sum_{s \in \mathcal{A}} h_s g_s$, with $\mathcal{A}$ some index set over which S is defined, and $h_s \in R$. The set $\mathcal{A}$ should be finite. On the other hand $f = \sum T_i$, where T_i are its terms (monomials). Since the two sums are equal we have

$$f = \sum_{i=1}^{k} T_k = \sum_{s \in \mathcal{A}} h_s g_s.$$

  We match the monomials T_i with the terms (or sum of them) in $\sum h_s g_s$. In this matching, since the monomials are unique, we might have to group several g_s together. If that is the case each group could be identified with

$$Y = \sum_{j_k} g_{j_k} = T_k$$

  and since Y is a monomial $Y|g_{j_k}$ for all possible j_k, since they all have to share the same power term of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.
- " $\Longleftarrow$ " If , for each term X of f , there is $Y \in S$, such that $Y|X$ this means that $f = \sum X_i = \sum h_i Y_i$, with $Y_i \in S$ and $h_i \in R$ and so obviously $f \in \langle S \rangle = I$.

(ii) This is a consequence of Hilbert Basis Theorem 2.4.4. That is $I = \langle g_1, \cdots, g_m \rangle$ for some $g_i \in R$. Then we can write $f = \sum h_i g_i$ for $i = 1, \cdots m$ with $h_i \in \mathbb{K}$. Now from part (i) there is $Y_i \in S | X_i = h_i g_i$. Choose $S_0 = \{Y_1, \cdots Y_m\}$ and since $m < \infty$, this proofs the second part. □

Proposition 3.4.3. *Every non-zero ideal I of R has a Gröbner basis.*

Proof. Let $I \setminus \{0\}$ an ideal. From I we can build a leading term ideal $I = \mathrm{LT}(I)$ generated form all monomials $g \in I \setminus \{0\}$. From the previous proposition $\mathrm{LT}(I)$ can be finitely generated by a set $G := \{\mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m)\}$, and so $\mathrm{LT}(I) = \mathrm{LT}(G)$ and from Theorem 3.4.1, part (iv), we have that G is a Gröbner basis. □

Lemma 3.4.4. *Let $G = \{g_1, \cdots, g_m\}$ a set of non-zero polynomials in R. Assume $c \in \mathbb{K}$, $X \in \mathbb{T}^n$ a power product, and $g \in R$ such that $g \xrightarrow{G}_+ r$ with r, a unique remainder reduced with respect to G. Then $(g - cXg_i) \xrightarrow{G}_+ r$ for each $i = 1, \cdots m$.*

Proof. If $c = 0$, the statement is obviously true since then $g - cXg_i = g$. Let us then assume that $c \neq 0$. The idea to reduce any function f by G is get rid of its leading order term $\mathrm{LT}(f)$, by subtracting from f the term $(\mathrm{LT}(f)/\mathrm{LT}(g_i))g_i$, as indicated in definition 11. If, for whatever reason $\mathrm{LT}(cXg_i) = \mathrm{LT}(g)$ then we performed the first step on the reduction of g to r via G. That is, $g \xrightarrow{g_i} g - cXg_i \xrightarrow{G}_+ r$. Otherwise we have the reduction chain $g \xrightarrow{g_i} (g - cXg_i) \xrightarrow{G}_+ r_1$, but since r is unique, then $r_1 = r$. □

We now present the fifth characterization of the Gröbner bases. We showed above in section 3.3.1 how the remainder in reductions in multivariate polynomials could depend on the order that we use to perform such reductions. The author of Gröbner basis Bruno Buchberger [6] presents this uniqueness as the definition of Gröbner basis. Here this turns out to be the fifth characterization for Gröbner basis.

Theorem 3.4.5. *Let $G = \{g_1, \cdots, g_m\} \subset R$. Then G is a Gröbner basis if an only if $\forall f \in R$, the remainder of dividing f by G is unique.*

Proof.

(i) " $\Longrightarrow$ " Let $f \xrightarrow{G}_+ r$. From Theorem 3.4.1 part (ii) we see that $r = 0$. This shows uniqueness on r.

(ii) " $\Longleftarrow$ " We assume that the remainders r such that $f \xrightarrow{G}_+ r$, are unique. We show that $r = 0$ and then from Theorem 3.4.1 part (ii) that G is a Gröbner basis. Let $f \in \langle G \rangle$ and suppose tht $f \xrightarrow{G}_+ r$

[6] http://people.reed.edu/ davidp/pcmi/buchberger.pdf

such that r is reduced with respect to G. We show that $r = 0$; for this we use Lemma 3.4.4. Since $f \in I$ we have that $f = \sum_{i=1}^{k} c_i X_i g_{i_k}$, with $c_i \in \mathbb{K}$ and X_i a non-zero product in $\mathbb{T}_n$. In a method that resmblest the Gram-Schmidth ortogonalization in linear algebra we start subtracting g_i components from f until we will be end with $r = 0$. That is, in the first step we find $f - c_1 X_1 g_{i_1}$, in the second step $f - c_2 X_2 g_{i_2}$, and so we continue until $f - \sum_{i=1}^{k} c_i X_i g_{i_k} = r$ as implied by Lemma 3.4.4. But then from the decomposition of f above we see that $r = 0$.

□

Example 3.3.2 shows that reversing the order of g_i we could get different quotients. So while the uniqueness of the remainder is guaranteed, this quality is not transfered to the quotients. It is then interesing that different from vector spaces where there is the concept of linearly independent vectors with unique coefficients (the quotients in this case), here in ring theory we can not enjoy of that same, sometimes convenient, attribute. We now prove that the set G (on whatever order) from example 3.3.2 forms a Gröbner basis.

Example 3.4.1. Let $G = \{g_1 = x - y^2 w, g_2 = y - zw, g_3 = z - w^3, g_4 = w^3 - w\}$, in $\mathbb{Q}[x, y, z, w]$.

(i) Show that G is a Gröbner basis in $I = \langle g_1, g_2, g_3, g_4 \rangle$ if the lexicographic order $x > y > z > w$ is in place.

(ii) Show that under lexicographic order $w > x > y > z$, G is not a Gröbner basis in I.

Solution:

(i) Let us assume that it is not. That is, there exists $f \in I$, such that $\mathrm{LT}(f) \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3), \mathrm{LT}(g_4) \rangle = \langle x, y, z, w^3 \rangle$. Then $x \nmid \mathrm{LT}(f)$, and $y \nmid \mathrm{LT}(f)$, and $z \nmid \mathrm{LT}(f)$. So because the monomial order is $x > y > z > w$, $f \in Q[w]$. Let us now assume that there exits $q_1, q_2, q_3, q_4 \in \mathbb{Q}[x, y, z, w]$, such that $f = q_1 g_1 + q_2 g_2 + q_3 g_3 + q_4 g_4$. That is,

$$f = q_1(x - y^2 w) + q_2(y - zw) + q_3(z - w^3) + q_4(w^3 - w).$$

Since $f = f(w)$, $q_1 = q_2 = q_3 = 0$, and so $f = q_4(w^3 - w)$ and $\mathrm{LT}(f) \in \langle w^3 \rangle \subset \langle x, y, z, w^3 \rangle$ which contradicts the first statement above. Then G is a Gröbner basis.

(ii) We assume the monomial order $w > x > y > z$. Then $\mathrm{LT}(g_1) = -wy^2$, $\mathrm{LT}(g_2) = -wz$, $\mathrm{LT}(g_3) = -w^3$ and $\mathrm{LT}(g_4) = w^3$. Then $\langle \mathrm{LT}(G) \rangle = \langle -wy^2, -wz, w^3 \rangle$, and for example $f = x - y^2w \notin \langle \mathrm{LT}(G) \rangle$, yet $x - y^2w = g_1 + 0g_2 + 0g_3 + 0g_4 \in \langle G \rangle = I$. so G is not a Gröbner basis for the ideal I with the $w > x > y > z$ order.

We see then that while changing the order of the members $g_i \in G$, can change the coefficient values (divisors) for the g_i, changing the monomial order can make G go from being a Gröbner basis to a set with is not a Gröbner basis.

3.5 Gröbner Bases: Algorithms

Up to this point we showed the existence of Gröbner bases but we need to develop practical methods to compute them. Before we list the Buchberger's algorithm which is central to the treatment of Gröbner bases we illustrate algorithms that we aleady know.

3.5.1 Gaussian Elimination

Consider for example the set $G = \{g_1, g_2, g_3\}$, where g_i $i = 1, 2, 3$ are linear equations in a number of variables. $x_1, \cdots, x_n$. If we assume that the equations g_i are linearly independent then the solution of the system $g_i = 0$, for $i = 1, 2, 3$, is a hyperplane of $n - 3$ dimensions. So if for example $n = 3$, the solution is a point. Recall that the solution of this system is the variety $V(G)$, and that the ideal $I = \langle G \rangle$ spans all polynomials of the form $\sum q_i g_i = 0$, $i = 1, 2, 3$. The method of Gassian elimination let us reduce the sytem by eliminating redundant variables, and the final result is a system of parametric equations. This is better understood with an example.

Example 3.5.1. Let us assume polynomials $g_1 := 2u - 3v - x + 2y + 3z - 4$, $g_2 := 2u - 5v - 2x + 2y - z - 9$ $g_3 := 4u - 4v - x + 4y + 11z - 4$, in $\mathbb{Q}[u, v, x, y, z]$

The variety $V(g_1, g_2, g_3)$, is given by the solutions of the system

$$\begin{aligned} 2u - 3v - x + 2y + 3z - 4 &= 0 \\ 2u - 5v - 2x + 2y - z - 9 &= 0 \\ 4u - 4v - x + 4y + 11z - 4 &= 0 \end{aligned}$$

Instead of doing Gaussian elimination we want to reduce this system using polynomial division. We show with this example that polynomial division and Gaussian elimination produce the same result.

If the monomial order is given by $u > v > x > y > z$, then the polynomials are already sorted. We want to reduce g_2 and g_3 with respect to g_3 and show that this provides the first step of the Gaussian elimination on zeroing out the first column of the coefficient matrix starting at the second row.

By dividing g_2 by g_1 we find the reduction

$$g_2 \xrightarrow[1]{g_1} h_2 = -2v - x - 4z - 5$$

which in Gaussian ellimination is $g_2 - 2g_1$, now since $\mathrm{LT}(g_2)/\mathrm{LT}(g_1) = 2$, then $h_2 = g_2 - \mathrm{LT}(g_2)/\mathrm{LT}(g_1)g_1 = g_2 - 2g_1$, is the same expression obtained from Gaussian elimination. We note that h_2 is simpler than g_2 since it has no terms in u and y which were eliminated.

We now divide g_3 by g_1, and find

$$g_3 \xrightarrow[2]{g_1} h_3 = 2v + x + 5z + 4$$

By calling $h_1 = g_1$ we reduce the system above to

$$\begin{aligned} h_1 := 2u - 3v - x + 2y + 3z - 4 &= 0 \\ h_2 := -2v - x - 4z - 5 &= 0 \\ h_3 := 2v + x + 5z + 4 &= 0 \end{aligned}$$

which in matrix form is

$$\begin{pmatrix} 2 & -3 & -1 & 2 & 3 & -4 \\ 0 & -2 & -1 & 0 & -4 & -5 \\ 0 & 2 & 1 & 0 & 5 & 4 \end{pmatrix} \tag{3.13}$$

The two reductions produced zeroes below the first raw in the first column.

We now need one more reduction. It is clear from Gaussian elimination that replacing the third row bu the sum of the second and third rows will do the job. In terms of multivariate polynomial division we say that we divide h_3 by h_2, then

$$h_3 \xrightarrow[-1]{g_2} h_4 = z - 1,$$

with $h_3 = g_3 - 2g_1$. So as claimed the new h_4 element is the sum $h_3 + h_2$. The new matrix is

$$\begin{pmatrix} 2 & -3 & -1 & 2 & 3 & -4 \\ 0 & -2 & -1 & 0 & -4 & -5 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix} \tag{3.14}$$

which written back in terms of equations is

$$\begin{aligned} h_1 := 2u - 3v - x + 2y + 3z - 4 &= 0 \\ h_2 := -2v - x - 4z - 5 &= 0 \\ h_4 := z - 1 &= 0 \end{aligned}$$

This is the same system that would have been obtained by regular Gaussian elimination, which is easier to solve that the original system. The question is if the solution of this simplified system is the same as that of the original. That is if $V(g_1, g_2, g_3) = V(h_1, h_2, h_4)$. We show that the ideal as $I = \langle g_1, g_2, g_3 \rangle$ and $J = \langle h_1, h_2, h_4 \rangle$ are the same. That is $I = J$. For this we see that

$$\begin{aligned} h_1 &= g_1 \\ h_2 &= g_2 - g_1 \\ h_4 = h_3 - g_2 &= g_3 - 2g_1 - g_2 \end{aligned}$$

so clearly the sytem $J \subset I$. On the other hand we can write

$$\begin{aligned} g_1 &= h_1 \\ g_2 &= h_1 + h_2 \\ g_3 &= 2h_1 + (h_1 + h_2) + h_4 = 3h_1 + h_2 + h_4, \end{aligned}$$

so $I \subset J$, and then $I = J$, then $V(I) = V(J)$.

By solving backwards the system for u, v, x, y, z, we see that

$$\begin{aligned} z &= 1 \\ v &= \frac{1}{2}(-x - 9) \\ u &= \frac{1}{4}(2x + 2y + 3z + 23) \end{aligned}$$

then z is eliminated from the system and we find two parameteric equations for (u, v) depending on three parameters (x, y, z). The three degree freedom tells us that $V(g_1, g_2, g_3)$ is a 3D manifold (hyper-plane) embeded in a sixth dimensional space.

We used a simple example to illustrate the reduction of a system of linear equations, the Buchberger algorithm shown in section 3.5.3 shows how the Gaussian elimination is a particular case of that more general algorithm.

3.5.2 Greatest Common Divisor (gcd)

This applies only to univariate polynomials. We already showed the gcd algorithm in Figure 2.1 and hence we do not have much to say here other than from the definition of gdc, every polynomial in an ideal $I = \langle G \rangle$ where $G = \{g_1, \cdots, g_m\}$, should be multiple of the gdc(G) and so gdc(G) is the smallest basis (of just a single element) that generates the ideal I.

3.5.3 The Buchberger Algorithm

The Buchberger algorithm is at the hearth of the Gröbner bases. We indicated that the Hilbert basis theorem guarantees the existence of a basis of an ideal, however Hilbert basis theorem is not a constructive theorem.

Let us assume that we have a set $G = \{g_1, \cdots, g_m\}$ of non-zero polynomials in some ideal I. We would like to know if they form a Gröbner basis or not. From the definition of Gröbner bases we want to guarantee that given $f \in I$, we can find some $g_i \in G$ such that $\mathrm{LT}(g_i)|\mathrm{LT}(f)$. We repeat here a paragraph written just before Theorem 3.4.1: " One way to prove that a set $G = \{g_1, \cdots, g_m\}$ is not a Gröbner basis for an ideal I, is to find $f \in I$ such that $\mathrm{LT}(f) \notin \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m) \rangle$. For example, choose $g_1 = x^3 - 2xy$, and $g_2 = x^2y - 2y^2 + x$. Then we find that $-yg_1 + xg_2 = x^2$, so $x^2 \in \langle g_1, g_2 \rangle$, still $x^2 = \mathrm{LT}(x^2) \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2) \rangle = \langle x^3, x^2y \rangle$." Observe that a weighted sum of two functions (here of order 3) can produce a function with lower order (here of order 2). Note that the leading order terms in g_1 and g_2 were tossed out with the combination $x^2 = -yg_1 + xg_2$. We then find that $\{g_1, g_2\}$ can not be a Gröbner basis since $x^2 =\notin \langle LT(g_1), LT(g_2) \rangle$. We forced that term out. How did we do this? We can derive the equation that produces the elimination of the leading order terms from g_1, g_2. That is, we want a linear

combination

$$h_1 g_1 + h_2 g_2$$

such that the leading order term of g_1 and g_2 disappear. We want

$$h_1 \mathrm{LT}(g_1) + h_2 \mathrm{LT}(g_2) = 0. \tag{3.15}$$

There are too many solutions for h_1 and h_2, we try to characterize them. For example,

$$h_2 \;=\; -h_1 \frac{\mathrm{LT}(g_1)}{\mathrm{LT}(g_2)} \tag{3.16}$$

where we are free to assign to h_1 any value as long as h_2 is still a polynomial. We do not want to relate g_1 and g_2 in any way. That is, we assume $g_1 \nmid g_2$ and $g_2 \nmid g_1$, otherwise $g_1 \in \langle g_2 \rangle$ and they are redundant. We want some kind of "linear independence". Then $h_1 \mathrm{L}(g_1)$ needs to be a multiple of of both g_1 and g_2 (so that h_2 is a well defined polynomial). We choose the least common multiple $L = \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$. That is

$$h_1 L(g_1) = L$$

where in L we ignore the coefficients and use LM instead of LC (they would cancel anyway)

$$h_1 = \frac{\mathrm{LT}}{L(g_1)} \qquad h_2 = -\frac{\mathrm{LT}}{L(g_2)}$$

This motivates the following definition.

Definition 28 (S-polynomial). *Let $f, g \in \mathbb{K}[x_1, \cdots, x_n]$. Select the least common multiple $L = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$, the smallest of all multiples of the leading monomial products of f and g. Then the polynomial*

$$S(f, g) = \frac{L}{\mathrm{LT}(f)} f - \frac{L}{\mathrm{LT}(g)} g \tag{3.17}$$

is called the S-polynomial of f and g .

The symbol S is sometimes referred to *"sysygy"* or sometimes to *"subtraction"* . We infer three things from here

(i) $S(f,g)$ cancels the leading order terms both in f and g. That is, the polynomial $S(f,g)$ does not have any of the leading order terms either in f or g.

Let $LT(f) = cx^{\alpha}$ and $LT(g) = dx^{\beta}$, with $x = (x_1, \cdots, x_n) \in \mathbb{N}$, $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N})$, and $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{N}$. The mcm of both is $\text{mcm}(f,g) = \text{mcm}(c,d)$ so $LM(f) = x^{\alpha}$, and $LM(g) = x^{\beta}$, and $L = \text{lcm}(\text{LM}(f), \text{LM}(g)) = x^{\gamma}$, where $\gamma_i = \max\{\alpha_i, \beta_i\}, i = 1, \cdots, n$.

Then

$$S(f,g) = \frac{x^{\gamma}}{cx^{\alpha}}(cx^{\alpha} + \text{l.o.t.}) - \frac{x^{\gamma}}{dx^{\beta}}(dx^{\beta} + \text{l.o.t.})$$

where l.o.t means lower order terms. Now observe that the leading order term $LT(f) = cx^{\alpha}$ became x^{γ} and the leading order term $LT(g) = dx^{\beta}$ became x^{γ}, which due to the minus sing cancels. So both leading order terms disappear in the new polynomials $S(f,g)$. Since the degree of the l.o.t chain is smaller or equal than α, then the degree of $S(f,g)$ is at most γ. This elimination is expected from the construction above.

(ii) $S(f,g)$ is the smallest degree polynomial with the property in (i). Since L is the least common multiple of $\text{LM}(f)$ and $\text{LM}(g)$, γ above is the least exponent sequence with the property that all its components are larger or equal than 0. Any other power smaller than γ, will not produce a valid monomial since then $x^{\gamma+\alpha}/(cx^{\alpha}) = x^{\gamma}/c$ would have at least a negative power on one of its x_i, $i = 1, \cdots, n$ variables.

(iii) This is the most important property of the S-polynomial s . By construction this polynomial is such that if f, g are independent (that is $f \neq hg$, for a polynomial $h \in \mathbb{K}[x_1, \cdots, x_n]$), then S is not redundant in any way since it is guaranteed to have a leading order term that is not a combination of the leading order terms of f and g. In this way, it is either 0, or a good addition to the base. In this way, the algorithm will always make progress over the previous found elements of the base.

Example 3.5.2. Given $G = \{g_1, g_2, g_3, g_4\}$ with

$$\begin{aligned} g_1 &= xy^2 - xz + y \\ g_2 &= xy - xz^2 - yz^4 \\ g_3 &= xz^4 - xz + y^2z^4 + yz^6 + y \\ g_4 &= -y^4z^4 - y^3z^6 - y^3 + y^2z^5 + yz^4 + yz^7 \end{aligned}$$

in the lex order $x > y > z$, find $S(g_i, g_j)$ for $i \neq j$, $i, j = 1, \cdots 4$. We need to find $(4)(3)/2 = 6$ combinations. Those are:

(i) $S(g_1, g_2)$:

We have that $L = \text{lcm}(\text{LM}(g_1), \text{LM}(g_2)) = xy^2$. Now, from the definition of S-polynomial 3.17 we have that

$$S(g_1, g_2) = \frac{L}{\text{LT}(g_1)} g_1 - \frac{L}{\text{LT}(g_2)} g_2 = g_1 - yg_2 \tag{3.18}$$

That is

$$S(g_1, g_2) = xyz^2 - xz + y^2z^4 + y \tag{3.19}$$

(ii) $S(g_1, g_3)$:

Since $L = \text{lcm}(\text{LM}(g_1), \text{LM}(g_3)) = xy^2z^4$, then

$$\begin{aligned} S(g_1, g_3) &= z^4 g_1 - y^2 g_3 \\ &= xy^2z - xz^5 - y^4z^4 - y^3z^6 - y^3yz^4. \end{aligned} \tag{3.20}$$

(iii) $S(g_1, g_4)$: Since $L = \text{lcm}(\text{LM}(g_1), \text{LM}(g_4)) = xy^4z^4$, then

$$\begin{aligned} S(g_1, g_4) &= y^2z^4 g_1 + xg_4 \\ &= \cancel{-xy^2z^5} - y^3z^4 - xy^3z^6 - xy^3 + \cancel{xy^2z^5} + xyz^7 + xyz^4 \\ &= -xy^3z^6 - xy^3 + xyz^7 + xyz^4 - y^3z^4. \end{aligned} \tag{3.21}$$

(iv) $S(g_2, g_3)$: Since $L = \text{lcm}(\text{LM}(g_2), \text{LM}(g_3)) = xyz^4$ then

$$S(g_2, g_3) = z^4 g_2 - y g_3 = xyz - xz^6 - y^3 z^4 - y^2 z^6 - y^2 - yz^8. \quad (3.22)$$

(v) $S(g_2, g_4)$:

Since $L = \text{lcm}(\text{LM}(g_2), \text{LM}(g_4)) = xy^4 z^4$ then

$$\begin{aligned} S(g_2, g_4) &= y^3 z^4 g_2 + x g_4 \\ &= -xy^3 z^6 - y^4 z^8 - xy^3 z^6 - xy^3 + xy^2 z^5 + xyz^4 + xyz^7 \\ &= -2xy^3 z^6 - xy^3 + xy^2 z^5 + xyz^7 + xyz^4 - y^4 z^8. \end{aligned} \quad (3.23)$$

(vi) $S(g_3, g_4)$: Since $L = \text{lcm}(\text{LM}(g_3), \text{LM}(g_4)) = xy^4 z^4$ then

$$\begin{aligned} S(g_3, g_4) &= y^4 g_3 + x g_4 \\ &= -xy^4 z + y^6 z^4 + y^5 z^6 + y^5 - xy^3 z^6 - xy^3 + xy^2 z^5 + xyz^4 + xyz^7 \\ &= -xy^4 z - xy^3 z^6 - xy^3 + xy^2 z^5 + xyz^7 + xyz^4 + y^6 z^4 + y^5 z^6 + y^5 \end{aligned} \quad (3.24)$$

The objective of $S(f, g)$ is not to reduce the leading terms of f and g simultaneously but to remove ambiguities. Note, for example, that the degree of $S(g_1, g_2)$ above is 4, which is larger than the degree of g_1 (3) and g_2 (2). So, which ambiguities are we removing? Assume that a polynomial f has a term X and that there are two g_i, g_j, $(i \neq j)$ such that $\text{LT}(g_i)|X$ and $\text{LT}(g_j)|X$, then $L = \text{lcm}(\text{LT}(g_i), \text{LT}(f_j))$ divides X as well. If we reduce f using g_i, we get the polymial $h_1 = f - \frac{X}{\text{LT}(g_i)} g_i$, and if we reduce f using g_j, we get the polymial $h_2 = f - \frac{X}{\text{LT}(g_j)} g_j$. Note that $h_1 = h_2$, so this is the ambiguity. By using $S(g_1, g_2)$, instead of g_1 and g_2 individually accomplish the simultanous reduction in one step.

Before showing the main theorem for the Buchberger algorithm we must be able to transform a linear combination of functions f_i, $(i = 1, \cdots, m)$ into a linear combination of S-poylymoials $S(f_i, f_j)$. We show this in the next Lemma.

Lemma 3.5.1. *Let* $g_1, \cdots, g_m \in \mathbb{K}[x_1, \cdots, x_n]$ *be such that* $\text{LM}(g_i) = X \neq 0$ *for all* $i = 1, \cdots, m$. *Let* $f = \sum_{i=1}^{m} c_i g_i$ *with* $c_i \in \mathbb{K}$, $i = 1, \cdots, m$. *If* $\text{LM}(f) < X$ *, then*

$$f = \sum_{i=1}^{m-1} d_i S(g_i, g_{i+1}),$$

for some coefficients $d_i \in \mathbb{K}$.

Proof. Let us write $g_i = a_i X + \text{l.o.t}$, with $a_i \in \mathbb{K}$. Then since the leading order coefficient of f is smaller than X, the weighted sum has a 0 matching this leading the coefficient of X. That is $\sum_{i=1}^{m} c_i a_i = 0$. Since $L = X$, $\text{LT}(g_i) = a_i X$, and $\text{LT}(g_j) = a_j X$, then from the definition of S-polynomial $S(g_i, g_j) = g_i/a_i - g_j/a_j$,

$$f = \sum_{i=1}^{m} c_i g_i = \sum_{i=1}^{m} c_i a_i \frac{g_i}{a_i}$$

Now since $\sum_{i=1}^{m} c_i a_i = 0$, and applying the telescopic rule of the sum

$$\begin{aligned} f &= \sum_{i=1}^{m} c_i a_i \left(\frac{g_i}{a_i} - \frac{g_1}{a_1} \right) \\ &= \sum_{i=1}^{m} c_i a_i \sum_{j=2}^{i} \left(\frac{g_j}{a_j} - \frac{g_{j-1}}{a_{j-1}} \right) \\ &= \sum_{i=1}^{m} c_i a_i \sum_{j=2}^{i} S(g_j, g_{j-1}) \\ &= \sum_{j=2}^{m} \left(\sum_{i=1}^{j} c_i a_i \right) S(g_j, g_{j-1}) \end{aligned}$$

We note that since $S(g_i, g_j) = S(g_j, g_i)$ we write

$$f = \sum_{j=2}^{m} d_j S(g_{j-1}, g_j) = \sum_{j=1}^{m-1} d_j S(g_j, g_{j+1})$$

with $d_j = \sum_{i=1}^{j} c_i a_i$. It is sometimes convenient to write

$$f = \sum_{i \neq j}^{m} d_{ij} S(g_i, g_j)$$

we could say that $j = i + 1$ but we will not need this particular piece of information. □

Let us now show Buchberger's Theorem

Theorem 3.5.2 (Buchberger). *Let $G = \{g_1, \cdots, g_m\}$ be a set of non-zero polynomials in $\mathbb{K}[x_1, \cdots, x_n]$. Then G is a Gröbner basis for the ideal $I = \langle g_1, \cdots, g_m \rangle$ if and only if for all $i \neq j$,*

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

Proof. (i) " $\Longrightarrow$ " This is a direct consequence of Theorem 3.4.1, part (ii) since $S(g_i, g_j) \in I = \langle g_1, \cdots, g_m \rangle$.

(ii) " $\Longleftarrow$ " Provided the hypothesis of $S(g_i, g_j) \xrightarrow{G}_+ 0$, we pick $f \in I$, non-zero and show that $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m) \rangle$. Since $I = \langle g_1, \cdots, g_m \rangle$ then we can write

$$f = \sum_{i=1}^{m} h_i g_i, \tag{3.25}$$

for some $h_i \in \mathbb{K}[x_1, \cdots, x_n]$. Let $X_i = \mathrm{LM}(h_i)\mathrm{LM}(g_i)$ and $X = \max_{i=1}^{m} X_i$. If $\mathrm{LM}(f) = X$, then $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m) \rangle$ and we are done. If $\mathrm{LM}(f) < X$, some cancellation must have ocurred, and f can be expressed in therms of S-polynomials, using Lemma 3.5.1. In this way we can find another expression such as 3.25 with new coefficients h_i' and lower degree. We ask again if the leading order product degree of the sum is equal to that of f, in which case we are done, otherwise we need to iterate once more. The number of iterations is finite, since the degree of the sum is reduced after each iteration. After finishing the ieterations the maximum degree of the sum is non-zero because f is not a constant (if f is a constant in $\mathbb{K}$) there is nothing to do), so at finishing we have that the leading order of f is that of the maximum leading order of terms in the sum and we are done. We develope the details next.

Given any expression 3.25 for f, let $m(i) = \deg(h_i g_i)$, and defined $\delta = \max_{i=1}^{m} m(i)$. Since we are using a monomial order we can always choose the expresson 3.25 such that the leading order has $\delta = \max m(i)$, is the least of all possible combinations. When this happens we show that $\deg(f) = \delta$ and we are done, since then $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m) \rangle$.

We show this by contradiction. That is, let us assume that after trying all possible arrangements of $\sum h_i g_i$, we find that $\deg f < \delta$. We then isolated those terms where $m(i) = \delta$, as follows:

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned}$$

The monomials appearing in the second and third sums on the last equation have a degree $< \delta$. Then since $\deg(f) < \delta$ we find that the degree in the first sum is also $< \delta$. Let $\mathrm{LT}(h_i) = c_i x^{\alpha_i}$. Then $\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha_i} g_i$. This is the part where we use Lemma 3.5.1 since this expression fits the conditions of that Lemma with $g_i = x^{\alpha_i} g_i$. That is,

$$\sum_{m(i)=\delta} c_i x^{\alpha_i} g_i = \sum d_{ij} S(x^{\alpha_j} g_i, x^{\alpha_j} g_j).$$

Now, form the definition of S-polynomial 3.17,

$$S(x^{\alpha_j} g_i, x^{\alpha_j} g_j) = \frac{L x^{\alpha_i} g_i}{x^{\alpha_i} \mathrm{LT}(g_i)} - \frac{L x^{\alpha_j} g_j}{x^{\alpha_j} \mathrm{LT}(g_j)},$$

and since

$$L = \mathrm{lcm}\ (\mathrm{LM}(x^{\alpha_i}(g_i)), \mathrm{LM}(x^{\alpha_j} g_j)) = x^{\delta},$$

then we have

$$\begin{aligned} S(x^{\alpha_i} g_i, x^{\alpha_j} g_j) &= \frac{x^{\cancel{\alpha_i}+\delta} g_i}{\cancel{x^{\alpha_i}} \mathrm{LT}(g_i)} - \frac{x^{\cancel{\alpha_j}+\delta} g_j}{\cancel{x^{\alpha_j}} \mathrm{LT}(g_j)} \\ &= x^{\delta - L_{ij}} S(g_i, g_j), \end{aligned}$$

with $L_{jk} = \mathrm{lcm}(\mathrm{LM}(g_j), \mathrm{LM}(g_k))$. Hence we have that

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{i \neq j} d_{ij} x^{\delta - L_{ij}} S(g_i, g_j). \tag{3.26}$$

We now use the hypothesis. That is, since $S(g_i, g_j)$ has zero remainder we can write

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

with $c_{ijk} \in \mathbb{K}[x_1, \cdots, x_n]$, with $\deg(c_{ijk} g_k) \leq \deg(S(g_i, g_j))$. Then

$$x^{\delta - L_{ij}} S(g_i, g_j) = \sum_{k=1}^{m} b_{ijk} g_k,$$

with $b_{ijk} = x^{\delta - L_{ij}} c_{ijk}$, and

$$\deg(b_{ijk} g_k) \leq \deg x^{\delta - L_{ij}} S(g_i, g_j)$$

and since $\deg(S(g_i, g_j)) < L_{ij}$ then $\deg(b_{ijk} g_k) < \delta$. Then

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i g_i) = \sum_{i \neq j, k} b_{ijk} x^{\delta - L_{ij}} S(g_i, g_j) = \sum_{i \neq j} d_{ij} \sum_{k} c_{ijk} g_k = \sum_{i} h'_i g_i$$

From $\deg(h'_i g_i) < \delta$, we violate the fact that we wrote f as a linear combination of g_i terms where their largest degree is no smaller than δ. □

With this, the Buchgerger's algorithm to compute Gröbner bases is as shown in Figure 3.2

We show how the Buchberger's algorithm is a generalization of Euclid's algorithm to find $\gcd(f, g)$, (or a larger number of polynomials) or to the Gaussian elimination problem. Let us start with the Buchberger's algorithm versus the Euclid's algorithm

Proposition 3.5.3. *Given two univariate polynomials f and g, the Buchberger's algorithm in Figure 3.2 reduces to the Euclid's algorithm to find the* $\gcd(f, g)$.

Proof. Assume

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_0 \quad , \quad g(x) = b_m x^m + b_{n-1} x^{n-1} + \cdots b_0,$$

and $n \geq m$, $a_n \neq 0 \neq b_m$.

We have $\mathrm{LM}(f) = x^n$ and $\mathrm{LM}(g) = x^m$.
We call $L = \mathrm{LCM}[\,\mathrm{LM}(f), \mathrm{LM}(g)] = x^{n-m}$. Then by definition

$$\begin{aligned} S(f,g) &= \frac{L}{\mathrm{LT}(f)} f - \frac{L}{\mathrm{LT}(g)} g \\ &= \frac{x^n}{a_n x^n} f - \frac{x^n}{b_m x^m} g \\ &= \frac{1}{a_n}\left(f - \frac{a_n x_n}{b_m x^m} g \right) \\ &= \frac{1}{a_n}\left(f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g \right) \end{aligned}$$

On the other hand the first step on the Euclidean algorithm is the division of f by g. This step is achieved by finding the remainder

$$r_1 = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g. \tag{3.27}$$

Setting the $1/a_n$ aside (ideals are invariant under scaling by the field elements) we have that $S(f,g) = r_1$.

The Buchberger algorithm starts with $G = \{f, g\}$, and then, if $r_1 \neq 0$, add (append) r to G. That is $G = \{f, g, r_1\}$. The next step is to reduce r_1 with respect to G. Since $\deg(r) < \deg(f)$, we only need to reduce r with respect to g. That is we divide r by g, and keep doing this until $r_n = 0$ (the alogirthm finishes). Then $G = \{f, r_1, \cdots, r_{n-1}\}$. We find that $\gcd(f,g) = r_{n-1}$, and it is found as if were doing Euclid's algorithm instead of Buchberger's algorithm.

□

We found that G can be reduced to $G = \{r_{n-1}\} = \{\gcd(f,g)\}$. The discussion of the redundance of the Gröbner basis from the Buchberger's algorithm is adressed in the next section.

We use example 3.5.1 again to illustrate the finding of the Gröbner basis on a linear system.

Example 3.5.3. Let us assume polynomials $g_1 := 2u - 3v - x + 2y + 3z - 4$, $g_2 := 2u - 5v - 2x + 2y - z - 9$ $g_3 := 4u - 4v - x + 4y + 11z - 4$, in $\mathbb{Q}[u, v, x, y, z]$ Find the Gröbner basis for this system.

- **Input** $F = \{F_1, \cdots, F_m\} \subset \mathbb{K}[x_1, \cdots, x_n]$ with $g_i \neq 0, i = 1, \cdots m$.
- **Output** $G = \{g_1, \cdots, g_s\}$a Gröbner basis for $\langle f_1, \cdots, f_m \rangle$
- **Initialization** $G = F, \mathcal{G} = \{(f_i, f_j) | f_i \neq f_j \in G\}$
- **while** $\mathcal{G} \neq \emptyset$

  Choose any $(f, g) \in \mathcal{G}$
  $\mathcal{G} = \mathcal{G} - \{(f, g)\}$
  $S(f, g) \xrightarrow{G}_+ h$, where h is reduced with respect to G
  If $h \neq 0$
    $\mathcal{G} = \mathcal{G} \cup \{(u, h) : \text{ such that } u \in G\}$
    $G = G \cup \{h\}$

Figure 3.2: Buchberger Algorithm to compute a Gröbner basis

We start with $G = \{g_1, g_2, g_3\}$ and find initially find

$$\begin{aligned} S(g_1, g_2) &= g_1 - g_2 = 2v + x + 4z + 5 \\ S(g_1, g_3) &= \frac{1}{2}g_1 - \frac{1}{4}g_2 = -\frac{v}{2} - \frac{x}{4} - \frac{5z}{4} - 1 \\ S(g_1, g_3) &= \frac{1}{2}g_1 - \frac{1}{4}g_2 = -\frac{3v}{2} - \frac{3x}{4} - \frac{13z}{4} - \frac{7}{2}. \end{aligned}$$

It is convenient to remove the denominators and nothing changes (from the Buchberger's algorithm point of view) . We scale the second and third polynomials by 4 to find

$$\begin{aligned} S(g_1, g_2) &= 2v + x + 4z + 5 \\ S(g_1, g_3) &= -2v - x - 5z - 4 \\ S(g_2, g_3) &= -6v - 3x - 13z - 14. \end{aligned}$$

Note that in all cases we remove the u variable from the equations. We now see that, since any $S(g_i, g_j)$, with $i \neq j, = 1, 2, 3$, does not have an u term, none of the g_i in G divides the $S(g_i, g_j)$. So no reduction exists, and

then we can integrate a new member $g_4 = S(g_1, g_2) = 2v + x + 4z + 5$ to the Gröebner list. Now, we check the reduction of $S(g_1, g_3)$ against g_4 [7]. This is,

$$S(g_1, g_3) \xrightarrow[-1]{g_4} -z + 1$$

and since this remainder is non-zero we can call it $g_5 = -z+1$. Now we reduce $S(g_2, g_3)$ with respect to $G = \{g_1, g_2, g_3, g_4, g_5\}$. For the same argument stated above, we do not need to find reduction of $S(g_2, g_3)$ with respect to g_1, g_2, g_3, and

$$S(g_2, g_3) \xrightarrow[-3]{g_4} -z + 1.$$

which is already g_5, so we need no further reduction or addition of terms since all combinations of $S(g_i, g_j)$, for $i \neq j, = 1, 2, 3.4$ are already considered. Then

$$G = \{g_1, g_2, g_4, g_4, g_5\}$$

with

$$\begin{aligned}
g_1 &= 2\,u - 3\,v - x + 2\,y + 3\,z - 4 \\
g_2 &= 2\,u - 5\,v - 2\,x + 2\,y - z - 9 \\
g_3 &= 4\,u - 4\,v - x + 4\,y + 11\,z - 4 \\
g_4 &= 2\,v + x + 4\,z + 5 \\
g_5 &= -z + 1.
\end{aligned}$$

It is interesting that except the last three equations, the system does not look as reduced in the Gauss-Jordan echelon form. In fact if we do back substitution (starting at the last equation) we find that:

$$\begin{aligned}
z &= 1 \\
v &= -\frac{x+9}{2} \\
u &= -\frac{x+4y+25}{4}
\end{aligned} \tag{3.28}$$

making of the solution a 2D hyperplane (manifold). The first two equations were not needed here. We see then that Buchberger's algorithms has room

[7] No need to try to find a reduction with respect to g_1, g_2, g_3 for the reasons explained above

for further reduction and this will be discussed in the next chapter. Note that the parametric representation 3.28 could be converted into an implicit form (implicitation) by plugging the second equation into the third. That is, from the second equation $x = -2v - 9$, and this into the third equation yields

$$u = -\frac{-2v - 9 + 4y + 25}{4}$$

or

$$4u - 2v + 4y + 16 = 0.$$

which is a plane in the (u, v, y) coordinate system, with normal vector $(4, -2, 4)$, and distance to the origin of $8/3$ units.

We now illustrate the algorithm with an example, which uses the results obtained in examples 3.3.3 and 3.5.2.

Example 3.5.4. Let $G = \{g_1, g_2\} = \{xy^2 - xz + y\ ,\ xy - xz^2 - yz^4\}$ with lexicographic order with $x > y > z$. Determine if G is a Gröbner basis.

This example is based on previous examples 3.3.3 and 3.5.2. Most of the computations needed here are already provided on those previous examples. In this way we can remove some of the painful algebraic details and focus on the important aspects of the algorithm.

We should build the $S(g_i, g_j)$ S-polynomials and show that their reduction with respect to G is 0. Let us build the S-polynomial (only one is needed).

- – From 3.19 we find $S(g_1, g_2) = xyz^2 - xz + y^2z^4 + y$.
  - – Now from equation 3.9 we find $S(g_1, g_2) \xrightarrow{G}_+ xz^4 - xz + y^2z^4 + yz^6 + y$.
  - – Then we define $g_3 = xz^4 - xz + y^2z^4 + yz^6 + y$, and add it to the list G, that is, now $G = \{g_1, g_2, g_3\}$.
- – From equation 3.20 we see that $S(g_1, g_3) = xy^2z - xz^5 - y^4z^4 - y^3z^6 - y^3 + yz^4$, and the reduction of this polynomial with respect to G is given by equation 3.10. We add the residual there to G to find $G = \{g_1, g_2, g_3, g_4\}$, with
  –

$$g_4 = -y^4z^4 - y^3z^6 - y^3 + y^2z^5 + yz^7 + yz^4.$$

- – From equation 3.22 we find that $S(g_2, g_3) = xyz - xz^6 - y^3z^4 - y^2z^6 - y^2 - yz^8$.
  – The reduction of $S(g_2, g_3)$ with respect to G is given by equation 3.11. That is, $S(g_2, g_3) \xrightarrow{G}_+ -y^3z^4 - y^2 + yz^5 + yz^2$. We add $g_5 = -y^3z^4 - y^2 + yz^5 + yz^2$ to G.
  – From equation 3.23 we find that $S(g_2, g_4) = -2xy^3z^6 - xy^3 + xy^2z^5 + xyz^7 + xyz^4 - y^4z^8$. The reduction of this equation with respect to G is listed in 3.12 which is precisely $-g_5$, so $S(g_2, g_4) \xrightarrow{G}_+ 0$.
  – Now we need to find $S(g_i, g_5)$ for $i = 1, \cdots, 4$. Since

$$\text{lcm}(\text{LM}(g_1), \text{LM}(g_5)) = xy^3z^4,$$

then

$$\begin{aligned} S(g_1, g_5) &= yz^4 g_1 + xg_5 \\ &= \cancel{-xyz^5} + y^2z^4 + \cancel{xyz^5} + xyz^2 - xy^2 \\ &= -xy^2 + xyz^2 + y^2z^4 \end{aligned}$$

We note that $S(g_1, g_5) = -yg_2$, so $S(g_1, g_5) \xrightarrow{G}_+ 0$.
Since

$$\text{LCM}(\text{LM}(g_2), \text{LM}(g_5)) = xy^3z^4$$

then

$$\begin{aligned} S(g_2, g_5) = y^2z^4 g_1 + xg_5 &= -xy^2z^6 - y^3z^8 - xy^2 + xyz^5 + xyz^2 \\ &= -xy^2z^6 - xy^2 + xyz^5 + xyz^2 - y^3z^8. \end{aligned}$$

We need to reduce this polynomial with respect to G. That is

$$\begin{aligned} S(g_2, g_5) &\xrightarrow[-z^6-1]{g_1} && x\,y\,z^5 + x\,y\,z^2 - x\,z^7 - x\,z - y^3z^8 + y\,z^6 + y \\ &\xrightarrow[z^5+z^2]{g_2} && x\,z^4 - x\,z - y^3\,z^8 + yz^9 + 2\,y\,z^6 + y \\ &\xrightarrow[1]{g_3} && -y^3\,z^8 - y^2\,z^4 + y\,z^9 + y\,z^6 \end{aligned}$$

We note that this residual is $z^4 g_5$, so $S(g_2, g_5) \xrightarrow{G}_+ 0$.

Since

$$\text{LCM}(\text{LM}(g_3), \text{LM}(g_5)) = xy^3z^4,$$

we see that

$$\begin{aligned} S(g_3, g_5) &= y^3 g_3 + x g_5 \\ &= -xy^3z + y^5z^4 + y^4z^6 + y^4 - xy^2 + xyz^5 + xyz^2 \\ &= -xy^3z - xy^2 + xyz^5 + xyz^2 + y^5z^4 + y^4z^6 + y^4 \end{aligned}$$

We now reduce $S(g_3, g_5)$ with respect to G.

$$\begin{aligned} S(g_3, g_5) &\xrightarrow[-yz-1]{g_1} x\,y\,z^5 - x\,z + y^5\,z^4 + y^4\,z^6 + y^4 + y^2\,z + y \\ &\xrightarrow[z^5]{g_2} xz^7 - xz + y^5z^4 + y^4z^6 + y^4 + y^2z + yz^9 + y \\ &\xrightarrow[z^3+1]{g_3} y^5z^4 + y^4z^6 + y^4 - y^2z^7 - y^2z^4 + y^2\,z - yz^6 - yz^3 \\ &\xrightarrow[-y]{g_4} y^3z^5 + y^2z - yz^6 - yz^3 \end{aligned}$$

We recognize that this last remainder is $-zg_5$, from which $S(g_3, g_5) \xrightarrow{G}_+ 0$. Now, for the final computation we find $S(g_4, g_5)$. Since

$$\text{LCM}(\text{LM}(g_4), \text{LM}(g_5)) = y^4z^4$$

then

$$\begin{aligned} S(g_4, g_5) &= -g_4 + y g_5 \\ &= y^3z^6 + \cancel{y^3} - \cancel{y^2z^5} - yz^7 - yz^4 - \cancel{y^3} + \cancel{y^2z^5} + y^2z^2 \\ &= y^3z^6 + y^2z^2 - yz^7 - yz^4. \end{aligned}$$

We now reduce $S(g_4, g_5)$ with respect to G. We observe that $S(g_4, g_5) = -z^2 g_5$, and so

$$S(g_4, g_5) \xrightarrow{G}_+ 0,$$

In summary we found Gröbner basis $G = \{g_1, g_2, g_3, g_4, g_5\}$ with

$$\begin{aligned} g_1 &= xy^2 - xz + y \\ g_2 &= xy - xz^2 - yz^4 \\ g_3 &= xz^4 - xz + y^2z^4 + yz^6 + y \\ g_4 &= -y^4z^4 - y^3z^6 - y^3 + y^2z^5 + yz^7 + yz^4 \\ g_5 &= -y^3z^4 - y^2 + yz^5 + yz^2. \end{aligned} \tag{3.29}$$

The previous example shows how a simple two polynomial where each polyomial has only three terms, can lead to a computational intensive work in the finding of its Gröbner basis. The algebra is tedious and could take hours if done by hand, still it takes fraction of a second in a computer.

We now illustrate that the Gröbner basis for this example could be even smaller. Let us review the previous example and stop just after finding g_3, that is we have at this moment $G = \{g_1, g_2, g_3\}$. Instead of reducing $S(g_1, g_3)$ with respect to G, we change the order and choose to reduce $S(g_2, g_3)$ first. Recall that $S(g_2, g_3) = xyz - xz^6 - y^3z^4 - y^2z^6 - y^2 - yz^8$, and and the reduction for this polynomial with respect to G is given by 3.12. as $S(g_2, g_3) \xrightarrow{G}_+ -y^3z^4 - y^2 + yz^5 + yz^2$, We then define $g_4 = -y^3z^4 - y^2 + yz^5 + yz^2$. We now show that the new set $G = \{g_1, g_2, g_3, g_4\}$ is a Gröbner basis and we did not need 5 elements. We find $S(g_i, g_4)$, $i = 1, 2, 3$, and reduce them with respect to G.

$$\operatorname{lcm}(\operatorname{LM}(g_1), \operatorname{LM}(g_4)) = xy^3z^4,$$

so

$$\begin{aligned} S(g_1, g_4) &= yz^4 g_1 + x g_4 \\ &= -\cancel{xyz^5} + y^2z^4 - xy^2 + \cancel{xyz^5} + xyz^2 \\ &= -xy^2 + xyz^2 + y^2z^4 \end{aligned}$$

and since $S(g_1, g_4) = -y g_2$, then $S(g_1, g_4) \xrightarrow{G}_+ 0$.

$$\operatorname{lcm}(\operatorname{LM}(g_2), \operatorname{LM}(g_4)) = xy^3z^4,$$

so

$$\begin{aligned} S(g_2, g_4) &= y^2z^4 g_2 + x g_4 \\ &= -xy^2z^6 + y^3z^8 - xy^2 + xyz^5 + xyz^2 \\ &= -xy^2z^6 - xy^2 + xyz^5 + xyz^2 - y^3z^8 \end{aligned}$$

Now,

$$\begin{aligned} S(g_2,g_4) &\xrightarrow[z^6+1]{g_1} && x\,y\,z^5+x\,y\,z^2-x\,z^7-x\,z-y^3\,z^8+y\,z^6+y \\ &\xrightarrow[-z^5-z^2]{g_2} && x\,z^4-x\,z-y^3\,z^8+y\,z^9+2\,y\,z^6+y \\ &\xrightarrow[-1]{g_3} && -y^3\,z^8-y^2\,z^4+y\,z^9+y\,z^6 \\ &\xrightarrow[z^4]{g_4} && 0 \end{aligned}$$

since the last non-zero remainder is $z^4 g_4$.

Now, for the finaly S-polynomial $S(g_3, g_4)$. Since,

$$\mathrm{lcm}(\mathrm{LM}(g_3), \mathrm{LM}(g_4)) = xy^3z^4,$$

then

$$\begin{aligned} S(g_3,g_4) &= y^3 g_3 + x g_4 \\ &= -xy^3z + y^5z^4 + y^4z^6 + y^4 - xy^2 + xyz^5 + xyz^2 \\ &= -xy^3z - xy^2 + xyz^5 + xyz^2 + y^5z^4 + y^4z^6 + y^4 \end{aligned}$$

The reduction is

$$\begin{aligned} S(g_3,g_4) &\xrightarrow[yz+1]{g_1} && x\,y\,z^5-x\,z+y^5\,z^4+y^4\,z^6+y^4+y^2\,z+y \\ &\xrightarrow[-z^5]{g_2} && x\,z^7-x\,z+y^5\,z^4+y^4\,z^6+y^4+y^2\,z+y\,z^9+y \\ &\xrightarrow[-z^3-1]{g_3} && y^5\,z^4+y^4\,z^6+y^4-y^2\,z^7-y^2\,z^4+y^2\,z-y\,z^6-y\,z^3 \\ &\xrightarrow[yz^2+z+y^2]{g_4} && 0 \end{aligned}$$

so indeed only 4 terms $g_i, i = 1, \cdots, 4$ are required to form a Gröbner basis starting at with g_1, g_2. These new basis is listed here

$$\begin{aligned} g_1 &= xy^2 - xz + y \\ g_2 &= xy - xz^2 - yz^4 \\ g_3 &= xz^4 - xz + y^2z^4 + yz^6 + y \\ g_4 &= -y^3z^4 - y^2 + yz^5 + yz^2. \end{aligned} \tag{3.30}$$

This kind of unconsitencies make the treatment or polynomial rings much more complicated than that of vector spaces where all bases have the same number of elements and the finding of basis is much easier than the computation of the Buchberger's algorithm. We show in the next chapter how to reduce the Gröbner basis further so that there is some kind of uniqueness.

3.6 Reduced Gröbner Bases

We discussed after example 3.5.4 that there is no a unique Gröbner basis found using Buchberger algorithm. We want to optimize the output and find a way to provide the smallest basis possible. The next proposition shows that there are ways to reduce Gröbner basis sets.

Proposition 3.6.1. *Let G be a Gröbner basis for the polynomial ideal I. Let $p \in G$ be a polynomial such that $p \in \langle G - \{p\}\rangle$. Then $G - \{p\}$ is also a Gröbner basis for I.*

Proof. Since $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$, $\mathrm{LT}(p) \in \langle \mathrm{LT}(G-\{p\}\rangle$ implies that $\langle \mathrm{LT}(G-\{p\})\rangle = \langle \mathrm{LT}(G)\rangle$, so $G - \{p\}$ is also a Gröbner basis. □

This proposition refines the Buchberger's algorithm by eliminating those p such that their leading term is spanned by the leading term of its siblings. Then the following definition is natural, after also imposing that all leading coefficients are 1 (normalization).

Definition 29 ([**Minimal Gröbner basis).** *A Gröbner basis G such that*

(i) $\mathrm{LC}(p) = 1\ \forall p \in G$.

(ii) $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\ \forall p \in G$,

is said to be a **minimal Gröbner basis.**

For the use of this property on simplification of Gröbner basis we visit example 3.5.3. Since, after normalization $\mathrm{LT}(p) = \mathrm{LM}(p)$, we use the notation LM. Since $\mathrm{LM}(g_2) = u|\mathrm{LM}(g_1)$, we can remove g_1. Now since $\mathrm{LM}(g_3) = u|\mathrm{LM}(g_2)$ we can remove g_2, and we end up with

$$
\begin{aligned}
g_3 &= 4\,u - 4\,v - x + 4\,y + 11\,z - 4\\
g_4 &= 2\,v + x + 4\,z + 5\\
g_5 &= -z + 1.
\end{aligned}
$$

which we can normalize by writing (and redefining the g_is)

$$\begin{aligned} g_1 &= u - v - \frac{1}{4}x + \frac{11}{4}z - 1 \\ g_4 &= v + \frac{x}{2} + 2z + \frac{5}{2} \\ g_5 &= z - 1. \end{aligned}$$

Which is in reduced echelon form. Note that we could had also remove any two pairs from the set $\{g_1, g_2, g_3\}$, since they all have the same $\mathrm{LM}(g_i)$, as in Gaussian-Jordan elimination we can reorder the equations as we wish. This implies then that we can not have a unique Gröbner basis, but that after reduction we get the same number of base members (3 in this case).

We now visit example 3.5.4, and query the basis listed in equation 3.29. We observe that $\mathrm{LM}(g_5)|\mathrm{LM}(g_4)$ from which we can remove g_4 and justify the reduction from equation 3.29 to equation 3.30. Note that $LC(g_4) = -1$. Reversing the sign of g_4 will set the basis in the standard minimal form. Let us list this Gröbner basis:

$$\begin{aligned} g_1 &= xy^2 - xz + y \\ g_2 &= xy - xz^2 - yz^4 \\ g_3 &= xz^4 - xz + y^2z^4 + yz^6 + y \\ g_4 &= y^3z^4 + y^2 - yz^5 - yz^2. \end{aligned}$$

Still we see that $\mathrm{LT}(g_2)|\mathrm{LT}(g_1)$, so we can suppress g_1, and after renaming we find

$$\begin{aligned} g_1 &= xy - xz^2 - yz^4 \\ g_2 &= xz^4 - xz + y^2z^4 + yz^6 + y \\ g_3 &= y^3z^4 + y^2 - yz^5 - yz^2. \end{aligned} \tag{3.31}$$

We show next that all minimal Gröbner bases have the same number of elements, as well as the same leading terms. In this regard this statement is closer to that of vector spaces.

Now as in vector spaces we change g_3 by $g_3 + ag_1$, with $a \in \mathbb{K}$, and for example $\mathbb{K} = \mathbb{R}$ then we have an infinite number of ways to choose minimal Gröbner basis. Let us first deal with the cardinal of Gröbner basis and then with the uniqueness issue later.

Proposition 3.6.2. *If $G = \{g_1, \cdots, g_o\}$, and $F = \{f_1, \cdots, f_p\}$ are two minimal Gröbner bases corresponding to the same ideal I, then $o = p$, and for each g_i there is exactly an f_j such that $LT(g_i) = LT(f_j)$.*

Proof. Let us assume a set of indices $1 \leq i_k \leq p$, and $1 \leq j_k \leq o$, with $k = \min\{o, p\}$.

Choose any $f_{i_1} \in F$. Since G is a Gröbner basis for I, there is some j_1 such that $\mathrm{LT}(g_{j_1})|\mathrm{LT}(f_{i_1})$. On the other hand, since F is also a Gröbner basis for I, there is some $1 \leq m \leq p$, such that $\mathrm{LT}(f_m)|\mathrm{LT}(g_{j_1})$. By transitivity $\mathrm{LT}(f_m)|\mathrm{LT}(f_{i_1})$, but if $m \neq i_1$, then f_m should not be in F otherwise F would not be minimal, then $m = i_1$, and $\mathrm{LT}(g_{j_1}) = \mathrm{LT}(f_{i_1})$. We can cross out f_j and g_i from the F and G lists. Repeating the same process we pick another $f_{i_2}, i_2 \neq i_1$ and match it agains some f_{j_2} finding that $\mathrm{LT}(g_{j_2}) = \mathrm{LT}(f_{i_2})$.

If the two sets (F and G) have different cardinality, let us say for example, and without the loss of generality, that $i > o$, then there would be an element $f_{i_{o+1}} \in F$ without a match in G, but since G is a Gröbner basis, there need to be a $g_{j_{o+1}}$ in G such that $\mathrm{LT}(g_{j_{o+1}})|\mathrm{LT}(f_{i_{o+1}})$, and since F is a Gröbner basis there is some $1 \leq m \leq p$, such that $\mathrm{LT}(f_m)|\mathrm{LT}(g_{j_{o+1}})$. So indeed $f_{i_{o+1}}$ has a match and since all elements of G are different, and o of them are already taken, the element $g_{j_{o+1}}$ exists in G making G having more than o elements which is a contradiction. Then $i = o$ and each $LT(f_i) \in F$ has exactly one match $LT(g_i) \in G$.

□

As indicated above there are still infinite number of ways to choose minimal Gröbner basis. This is also an attribute of vector space basis. However in vector spaces we can use method such as Gram Schmidt to find a unique orthonormal basis that span the same original basis subspace. Here we do not have such a thing as a Gram-Schmidt method, but we can force another constraint into a minimal basis to make it unique. This is introduced in the next definition.

Definition 30 (**Reduced Gröbner Basis).** *A Gröbner basis G such that*

(i) $\mathrm{LC}(p) = 1 \ \forall p \in G$.

(ii) $m \notin \langle \mathrm{LT}(G - \{p\}) \rangle \ \forall m$ monomial of $p \in G$,

is said to be a **reduced Gröbner basis.** We say that p is **reduced for G** .

Note that this definition is almost identical to definition 29. The difference is that here, each monomial (and not just the leading term as in definition 29) is checked against the set $\langle \mathrm{LT}(G - \{p\})\rangle$. We see that the functions in 3.31 form a reduced Gröbner basis. Any function of the form $g_3 + ag_1$, with $a \neq 0$, will introduce monomials which are already in the span $\langle \mathrm{LT}(G - \{g_3 + ag_1\})\rangle$, so a needs to be zero. While this is not in any way similar to a Gram-Schmidt orthogonalization in vector spaces, it provides, as in Gram-Schmidt some uniqueness on the bases. We present a formal proof of the existence and uniqueness of reduced Gröbner bases.

Proposition 3.6.3 (Existence and uniqueness of the reduced Gröbner bases). *Let $G = \{g_1, \cdots, g_m\}$ be a minimal Gröbner basis for the polynomial ideal I. Then there exists a reduced Gröbner basis.*

Proof. We start with the minimal Gröbner basis G for the polynomial ideal I. Construct a set H, which will be the reduced Gröbner basis. This is built by replacing one-by-one, each g_i by an h_i, obtained from the process $g_i \xrightarrow{H_i}_+ h_i$, where h_i is reduced with respect to $H_i = \{h_1, h_2, \cdots h_{i-1}, g_i, \cdots, g_m\}$, with $H_1 = G \setminus \{g_1\}$. In short, we replace each g_i by the remainder on dividing g_i by $G \setminus \{g_i\}$, where G is dynamically changing through the H_i phases.

We show that $H = \{h_1, h_2, \cdots, h_m\}$ is a reduced Gröbner basis with respect to I. To show this we should show that

(i) $\mathrm{LC}(h_i) = 1$.

(ii) No term h_i is divisible by any object in the set

$$H \setminus \{h_i\} = \{\mathrm{LT}(h_1), \cdots, \mathrm{LT}(h_{i-1}), \mathrm{LT}(h_{i+1}) \cdots, h_m\}$$

Part (i) is trivial. Ideals are invariant under scaling, and we can always normalized the polynomial with respect to the field.

To show part (ii) we observe that, because all objects $\mathrm{LT}(h_j)$, with $j = 1, \cdots i-1$, came from a multivariate division then the remainders have lower degree that the dividends, and each term of h_i belongs to the remainder on the chain that preceeds it. The polynomial h_i comes from dividing g_i by $H_i \setminus \{g_i\}$ and so $\deg(h_i) < \deg(h_j)$, with $1 \leq j < i$, so $h_j \nmid h_i$. In the set $H_i \setminus \{g_i\}$ we have not yet replaced g_j by h_j, for $m \geq j > i$, but once we reach H_m, $\deg(h_i) < \deg(h_j)$, for $j < m$, so we are done.

We now prove the uniqueness statement Let us assume two minimal reduced bases $G = \{g_1, \cdots, g_m\}$, $H = \{h_1, \cdots, h_m\}$. Note that since they

are minimal they have the same number of elements. Since (they are minimal we can say that $\mathrm{LT}(g_i) = \mathrm{LT}(h_i)$. Let us choose i, $1 \leq i \leq m$. If $g_i \neq h_i$, then $g_i - h_i \in I$ so that there exists j such that $\mathrm{LM}(h_j)|\mathrm{LM}(g_i - h_i)$. Since the leading order of g_i and h_i are the same the subtraction cancel the leading orders and we have that for each i, $\mathrm{LM}(g_i - h_i) < \mathrm{LM}(h_i)$, so $j \neq i$. and $\mathrm{LM}(h_j) = \mathrm{LM}(g_j)$ divides either a term of g_i or h_i (otherwise $\mathrm{LM}(g_i - h_i) \nmid \mathrm{LM}(h_i)$). This contradicts that G and H are reduced Gröbner bases. So $g_i = h_i$. □

We do not provide examples here since the next chapter is all about examples of the use of Gröbner bases.

Chapter 4

Applications of Gröbner Bases

4.1 The Ideal Membership Problem

4.1.1 The Theory

In vector spaces we can ask if a point (x, y) belongs a given line L or not. For example the line spanned by the vector $(1, 2)$ has all points of the form $(x, 2x)$, so a point such $(1, 3)$ will not be on that line. Similarly we can ask if a point (x, y, z) is in a given plane P or not. The plane can be spanned by two vectors, (a_1, b_1, c_1) and (a_2, b_2, c_2). The answering of these type of questions requires the solution of linear equations. In the case of rings of polynomials the problem is a bit more complicated but the question is the same. Whatever an ideal I is we want to know if a given function f belongs or not to that ideal.

Definition 31 (**Ideal Membership Problem**). *Let us provide a target polynomial f and a set of $F = \{f_1, \cdots, f_m\}$, with $f_i \in \mathbb{K}[x_1, \cdots, x_n]$, $i = 1, \cdots, m$. We define the generated ideal $I = \langle f_1, \cdots, f_m \rangle$. If $f \in I$ we say that f is a member of the ideal I. The problem of determining this membership is the so called* **ideal membership problem.**

A way to solve this problem is to find a Gröbner basis $G = \{g_1, \cdots, g_t\}$ for the ideal I, and use this basis instead of the set F, since it should be simplified. That is, we want to find a set of polynomials $H = \{h_1, \cdots, h_t\}$, such that $f = \sum_{i=1}^{t} h_i g_i$. If we succeed then f belongs to the ideal I. Eventually we should be able to write $f = \sum_{i=1}^{s} v_i f_i$, with $v_i \in I$, $i = 1, \cdots, s$, with $1 \leq s \leq m$. This can be achieved by using Theorem 3.4.1, part (ii). That

is $f \in I \iff f \xrightarrow{G}_+ 0$. This allows us to write $f = \sum_{i=1}^{t} h_i g_i$. From the algorithm 3.2, we see that G starts with F. That is, $g_i = f_i$, for $i = 1, \cdots, m$, then each additional g_j, with $j > m$, is computed from the reduction of the $S(g_{j_1}, g_{j_2})$ with $j_1, j_2 < j$. That is $g_m = S(g_{j_1}, g_{j_2}) - \sum_{i=1}^{l} w_i g_i$, with $i < j$. So at the end we can find f in terms of the f_is. That is $f = \sum_{i=1}^{s} v_i f_i$.

Let us visit once more Example 3.5.4.

Example 4.1.1. Let $F = \{f_1, f_2\} = \{xy^2 - xz + y \ , \ xy - xz^2 - yz^4\}$ with lexicographic order $x > y > z$. Determine the membership of f to I in the following list. If f is a member of I find the representation of f in terms of the f_1 and f_2.

(i) $f(x, y, z) = x^2 + y^2$

(ii) $f(x, y, z) = xyz^2$.

(iii) $f(x, y, z) = xy^3 + xz^2 + y$.

(iv) $f(x, y, z) = x^2y^2 - x^2z - xy^2 + xyz^2 + xy + y^2z^4$

Solution: We could start by reducing f with respect to the Gröbner basis $G = \{g_1, g_2, g_3, g_4\}$ found under equation 3.30, which we rewrite here reversing the sign of g_4.

$$\begin{aligned} g_1 &= xy^2 - xz + y \\ g_2 &= xy - xz^2 - yz^4 \\ g_3 &= xz^4 - xz + y^2z^4 + yz^6 + y \\ g_4 &= y^3z^4 + y^2 - yz^5 - yz^2. \end{aligned}$$

If the final remainder is 0 we say that f does not belong to the ideal $I = \langle f_1, f_2 \rangle$ otherwise f is not a member of the ideal I. Another way to test for ideal membership is to check that the leading order term of at least one g_i divides the leading order term of f. This method is faster to rule out a membership. We should apply this last method initially and then if there is membership use the reduction to find an explicit representation of f in terms of the elements of F.

(i) We observe that the leading order of each of the g_is with $i = 1, \cdots, 4$, does not divide the leading order term x^2. Each leading order of g_i has factors other than x. For example $\mathrm{LT}(g_1)$ and $\mathrm{LT}(g_2)$ have y factors, while $\mathrm{LT}(g_3)$ and $\mathrm{LT}(g_4)$ have z factors. Hence f is not a member of I. The reader can check that $f \xrightarrow[+]{G} f$.

(ii) We observe that the only leading order term of the g_i , $i = 1, \cdots, 4$ which divides $f(x, y, z) = xyz^2$, is g_2. Then some reduction is achieved but the reduction will produce a non-zero remainder. The reader can check that

$$\begin{aligned} f &\xrightarrow[0]{g_1} && g_1 \\ &\xrightarrow[z^2]{g_2} && yz^6 + xz^4 \\ &\xrightarrow[1]{g_3} && -y^2z^4 + xz - y \\ &\xrightarrow[0]{g_4} && -y^2z^4 + xz - y. \end{aligned}$$

Since the reduction did not generate a 0 remainder f is not a member of I.

(iii) We observe that $\mathrm{LT}(g_i)|\mathrm{LT}(f) = xy^3$, with $i = 1, 2$, however for $i = 3, 4$ $\mathrm{LT}(g_i) \nmid \mathrm{LT}(f)$. Then f could be a member of I. The reader can check that

$$\begin{aligned} f &\xrightarrow[y]{g_1} && xyz + xz^2 - y^2 + y \\ &\xrightarrow[z]{g_2} && xz^3 + xz^2 - y^2 + yz^5 + y \\ &\xrightarrow[0]{g_3} && xz^3 + xz^2 - y^2 + yz^5 + y \\ &\xrightarrow[0]{g_4} && xz^3 + xz^2 - y^2 + yz^5 + y \end{aligned}$$

and so f is not a member of I.

(iv) As in the previous example $\mathrm{LT}(g_i)|\mathrm{LT}(f) = x^2y^2$, with $i = 1, 2$, but $\mathrm{LT}(g_i) \nmid \mathrm{LT}(f)$ for $i = 3, 4$. Then f could be a member of I. We show

that in fact this is the case.

$$\begin{aligned} f &\xrightarrow[x-1]{g_1} && xyz^2 - xz + y^2z^4 + y \\ &\xrightarrow[z^2]{g_2} && xz^4 - xz + yz^6 + yz^4 + y \\ &\xrightarrow[1]{g_3} && 0 \\ &\xrightarrow[0]{g_4} && 0. \end{aligned}$$

From here

$$\begin{aligned} f(x,y,z) &= g_1(x-1) + xyz^2 - xz + y^2z^4 + y \\ &= g_1(x-1) + g_2z^2 + xz^4 - xz + yz^6 + yz^4 + y \\ &= g_1(x-1) + g_2z^2 + g_3 \end{aligned}$$

We know that $g_i = f_i$, for $i = 1, 2$, but still we need to reduce g_3 in terms of f_1 and f_2. We know that g_3 came from the reduction of $S(f_1, f_2) = S(g_1, g_2) = f_1 - yf_2$ (see equation 3.18) The reduction of $S(g_1, g_2)$ is given by equation 3.9. Then, by reversing the process in equation 3.9 we find

$$f_1 - yf_2 = z^2g_2 + g_3$$

from which $g_3 = f_1 - yf_2 - z^2f_2$, and so

$$f(x,y,z) = f_1(x-1) + f_2z^2 + f_1 - yf_2 - z^2f_2 = xf_1 - yf_2.$$

4.1.2 Applications

We show how two fields (graph theory, and polynomial ideals) which seem to be unrelated interact to solve a common problem.

The idea is to define a graph Γ and study a given property of that graph $P(\Gamma)$ (for example the coloring of its nodes, or the existence of edges) by establishing a connection with polynomial ideal properties. That is, we find a polynomial representation of the graph f_Γ,, and find an equivalence between this property and the property of the polynomial; mainly

$$P(\Gamma) \iff f_\Gamma \in I \tag{4.1}$$

where I is a certain ideal connected with the property. A simple illustration of this is presented in section 4.1.2.1.

There are seveval ways to use polynomials to make connections with problems. For example:

(i) Use the roots of the polynomial to make the connections. For example solving non-linear equations.

(ii) Use the coefficients of the polynomial to make the connections. For example to compute convolutions, correlations, or filtering of digital signals.

(iii) Use variables of the polynomial to make the connections. See 4.1.2.1, for an example of the use of variables of the polynomial in the solution of a graph theory problem.

For the problems we want to solve we use the variables to make the connections. Please check any document on graph theory for the basic tools. My document (to be linked here in the future) provides all the necessary definitions and properties required to understand the applications of Gröbner basis to the solution of graph theory problems.

We now define the graph polynomial.

Definition 32 (Graph Polynomial). *The* **graph polynomial** f_Γ *associated to the graph* $\Gamma(V, E)$ *is an element of the ring* $\mathbb{K}(V)$*, given by*

$$f_\Gamma = \prod_{\substack{x_i > x_j \\ (x_i, x_j) \in E}} (x_i - x_j)$$

with $V = \{x_1, \cdots, x_n\}$*,* $i, j \in \{1, \cdots, n\}$*, and "*$>$*" is a monomial order in the* x_i *variables.*

4.1.2.1 The Existence of Edges

The first application is the proof that any graph has at least one edge.

We will find a property $P(\Gamma)$ which is equivalent to $f_\Gamma \in I$ for some ideal I as suggested by equation 4.1. Let us call E the set of edges of a graph with vertices $\{x_1, \cdots, x_n\}$. Saying that E is non empty means that there is at least one edge. That is, the property $P(\Gamma)$ that we want to invoke is

that E is non empty. On the other hand, the existence of at least one edge will guarantee the existence of a polynomial f_Γ. Each edges introduces a polynomial of degree 1 into the product. The degree of the polynomial f_Γ is the number of edges in the set E. The ideal $I = \langle x_1, \cdots, x_n \rangle$ has all linear combinations of $x_i - x_j$ (among other non-linear terms), and so it generates all possible edge combinations. Having no edges means that the polynomial f_Γ will have a zero degree, and so it could not be the generated of the set $\{x_1, \cdots, x_n\}$. Then we clearly see the equivalence of the ideal membership problem ($f_\Gamma \in I$) and the existence of at least one edge $P(\Gamma)$.

4.2 Parametrization

4.3 Implicitation

Chapter 5

μ (rational) Bases

Chapter 6

Applications of μ Bases

Index