UNIVERSITY OF BELGRADE

FACULTY OF MATHEMATICS

Samira M. Zeada

Classification of Monomial Orders In Polynomial Rings and Gröbner Basis

DOCTORAL DISSERTATION

BELGRADE, 2015

CHAPTER 1

INTRODUCTION

1.1 Univariate polynomial division

It is assumed that the reader already knows how to divide two univariate polynomials using polynomial long division. In this section we consider polynomials in $K[x]$, that is, the ring of polynomials in one variable with coefficients in K (K is a field) and we will consider Euclidean Algorithm. We will present some of the standard material concerning $K[x]$ but will present this material using notation that will be more immediately generalizable to the study of polynomials in many variables.
Suppose $0 \neq f \in K[x]$, if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, with $a_0, \cdots, a_n \in k$ and $a_n \neq 0$, so that f has degree n, denoted $deg(f) = n$. The leading term of f denoted $LT(f) = a_n x^n$, is the term of f with highest degree, and the leading coefficient of f, denoted $LC(f) = a_n$, is the coefficient in the leading term of f. Note that if we have two polynomials f and g, then $deg(f) \leq deg(g)$ if and only if $LT(f)$ divides $LT(g)$.
We call that a subset $I \subseteq K[x]$ is an ideal if the following holds :

- $0 \in I$.
- If $f_1, f_2 \in I$, then $f_1 + f_2 \in I$.
- If $g \in K[x]$ and $f_1 \in I$, then $gf_1 \in I$.

The main tool in the Euclidean Algorithm is the division algorithm (also known as long division of polynomials).

Example 1 . *Let $f = 2x^4 - 3x^3 + 6x^2 + 5x$, and $g = 3x^3 + x^2 + 6$ be in $\mathbb{Q}[x]$ we divide f by g to get quotient $\frac{2}{3}x - \frac{11}{9}$ and the remainder $\frac{65}{9}x^2 + x + \frac{22}{3}$ as follows:*

$$\begin{array}{r|l} & \frac{2}{3}x - \frac{11}{9} \\ \hline 3x^3 + x^2 + 6) & 2x^4 - 3x^3 + 6x^2 + 5x \\ & \underline{-2x^4 - \frac{2}{3}x^3 \qquad - 4x} \\ & -\frac{11}{3}x^3 + 6x^2 + x \\ & \underline{\frac{11}{3}x^3 + \frac{11}{9}x^2 \qquad + \frac{22}{3}} \\ & \frac{65}{9}x^2 + x + \frac{22}{3} \end{array}$$

So,

$$\frac{f}{g} = \frac{2}{3}x - \frac{11}{9} + \frac{\frac{65}{9}x^2 + x + \frac{22}{3}}{3x^3 + x^2 + 6}$$

or, equivalently,

$$f = \left(\frac{2}{3}x - \frac{11}{9}\right) g + \left(\frac{65}{9}x^2 + x + \frac{22}{3}\right)$$

We first multiplied g by $\frac{2}{3}x$ and subtracted the resulting product from f. After this first cancellation we get the first remainder $h = f - \frac{2}{3}xg = \frac{-11}{3}x^3 + 6x^2 + x$.

In general if we have two polynomials $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$, with $n = deg(f) \geq m = deg(g)$, then the first step in the division of f by g is to subtract from f the product $\frac{LT(f)}{LT(g)}g = \frac{a_n}{b_m}x^{n-m}g$, and we get $h = f - \frac{LT(f)}{LT(g)}g$ as the first remainder.

Definition 1 . *Let $f, g, h \in K[x]$ with $g \neq 0$. We say that f reduces to h modulo g in one step if $h = f - \frac{LT(f)}{LT(g)}g$, and denoted $f \xrightarrow{g} h$*

Going back to the previous example, we had $f = 2x^4 - 3x^3 + 6x^2 + 5x$, $g = 3x^3 + x^2 + 6$ and $h = \frac{-11}{3}x^3 + 6x^2 + x$, where h was the first remainder in the division process. We repeat the process on h. By subtracting $\frac{LT(h)}{LT(g)}g =$

$\frac{-11}{3}x^3 - \frac{11}{9}x^2 - \frac{22}{3}$ from h we get the second remainder $r = \frac{65}{9}x^2 + x + \frac{22}{3}$, which is the final in this example.
We can use the reduction notation $f \xrightarrow{g} h \xrightarrow{g} r$ or $f \xrightarrow{g}_+ r$ for repetition of the reduction steps. In the reduction, the polynomial h has degree strictly less than the degree of f. When we continue this process the degree keeps going down until the degree is less than the degree of g. So we can describe the division algorithm.

Theorem 1 *.(Division Algorithm) Let g be a nonzero polynomial in $K[x]$, then for any $f \in K[x]$, there exist q and r in $K[x]$ such that $f = qg + r$, with $r = o$ or $deg(r) < deg(g)$. The polynomials q and r are unique.*

The proof can be found in the most of algebra text books. (See[7],[24])
Now let $I = \langle f, g\rangle$ be the ideal generated by f, g, and suppose that $f \xrightarrow{g} h$. Then $h = f - \frac{LT(f)}{LT(g)}g$, it is easy to see that $I = \langle h, g\rangle$, so we can replace f by h in the generating set of I. By using this idea we can prove the following result.

Theorem 2 *. Let $I \subset K[x]$ be an ideal. Then there exists $h \in K[x]$ with $I = \langle h\rangle$.*

Proof. Let h be a nonzero element of I, of minimal degree. For any $f \in I$, we have by using Division Algorithm $f = qh + r$ with $q, r \in K[x]$ and $deg(r) < deg(h)$. Since $r = f - qh \in I$ we get that $r = 0$ as h is of minimal degree in I, It follows that $f = qh$. $\square$
In general, an ideal generated by one element is called a principal ideal. So we can say that $K[x]$ is a principal ideal domain, or PID. An example of PID is the ring of integers $\mathbb{Z}$. However, the ring of bivariate polynomials $K[x, y]$ is not a PID, as we can see from the example.
Take $I = \langle x, y\rangle$. If $I = \langle f\rangle$, then $f \setminus x$, $f \setminus y$, $deg(f) = 1$, $f(x, y) = ax + by$, which is a contradiction.
From the last theorem we know that the generator of an ideal in $K[x]$ is the nonzero polynomial of minimum degree contained in the ideal but this description is not useful in practice. To require that, we need to check the degree of all polynomials (there are infinitly many) in the ideal. We will first discuss ideals $I = \langle f, g\rangle \subset K[x]$, generated by two polynomils $(f, g \neq 0)$. There is some $h \in K[x]$ such that $I = \langle h\rangle$. How can we find such an h ?.
The above question can be answered using the greatest common divisor.

Definition 2 *. Let $f_1, f_2 \in K[x]$. Then a polynomial $r \in K[x]$ is called a greatest common divisor of f_1 and f_2 if the following holds:*

1. *r divides both f_1 and f_2.*

2. *If $g \in K[x]$ also divides f_1 and f_2, then g divides r.*

We will denote the greatest common divisor by $r = GCD(f_1, f_2)$.

Theorem 3 . *If $f_1, f_2, r \in K[x]$ and $r = GCD(f_1, f_2)$, then the following holds:*

1. *r is unique up to a constant multiple.*

2. *r generates the ideal $\langle f_1, f_2 \rangle$.*

3. *There is a way to find r, called the Euclidean Algorithm.*

We will explain the Euclidean Algorithm in few steps and then give an example.
Euclidean Algorithm: Suppose f and g are polynomials in $K[x]$.

- When we divide f by g, we will get $f = q_1 g + r_1$, with $q_1, r_1 \in K[x]$, $0 < deg(r_1) < deg(g)$.
- We then look at g and divide by the remainder r_1. This will give us a new polynomial and a new remainder.
- Now look at the old remainder and divide it by the new remainder. Continue in this way until the final remainder is zero:

$$\begin{gathered} f = q_1 g + r_1, 0 < deg(r_1) < deg(g), \\ g = q_2 r_1 + r_2, 0 < deg(r_2) < deg(r_1), \\ r_1 = q_3 r_2 + r_3, 0 < deg(r_3) < deg(r_2), \\ \vdots \\ r_{n-2} = q_n r_{n-1} + r_n, 0 < deg(r_n) < deg(r_{n-1}), \\ r_{n-1} = q_{n+1} r_n + 0 \end{gathered}$$

- The last nonzero remainder r_n is the GCD of f and g. Further, by working back up this list we can find $p(x)$, $q(x) \in K[x]$ such that

$$GCD(f(x), g(x)) = p(x)f(x) + q(x)g(x).$$

For the proof (see [7], [24]).

Example 2 *.Let* $K = \mathbb{Q}$, $f(x) = 5x^3 + 2x^2 + 3x - 10$, *and* $g(x) = x^3 + 2x^2 - 5x + 2$.

$$5x^3 + 2x^2 + 3x - 10 = 5(x^3 + 2x^2 - 5x + 2) + (-8x^2 + 28x - 20)$$
$$x^3 + 2x^2 - 5x + 2 = (\frac{-1}{8}x - \frac{11}{16})(-8x^2 + 28x - 20) + (\frac{47}{4}x - \frac{47}{4})$$
$$-8x^2 + 28x - 20 = \frac{4}{47}(-8x + 20)(\frac{47}{4}x - \frac{47}{4}) + 0$$

We kept applying the division algorithm until the remainder was zero. Then $GCD(f, g) = \frac{47}{4}(x-1)$ tells us that the simpler polynomial $x-1$ also divides both $f(x)$ and $g(x)$,

$$I = \langle f(x), g(x) \rangle = \langle x - 1 \rangle .$$

The algorithm for computing GCD's depends on the Division Algorithm and the following fact.

Lemma 1 . *If* $f, g \in K[x]$, *with one of* f, g *not zero, then* $GCD(f, g) = GCD(f - qg, g)$ *for all* $q \in K[x]$.

(see [24] p.13)
In the case of ideals generated by more than two polynomials, $I = \langle f_1, \cdots, f_s \rangle$ with all of the $f_i's$ not zero, we get the following theorem.

Theorem 4 . *Let* $f_1, \cdots, f_t \in K[x]$, *where* $t \geq 3$ *then:*

1. $GCD(f_1, \cdots, f_t)$ *exists and is unique up to a nonzero constant.*
2. $\langle GCD(f_1, \cdots, f_t) \rangle = \langle f_1, \cdots, f_t \rangle$.
3. *For* $t \geq 3$, $GCD(f_1, \cdots, f_t) = GCD(f_1, GCD(f_2, \cdots, f_t))$.
4. *There is an algorithm to calculate the GCD.*

For example let $f_1, f_2, f_3 \in K[x]$. To find $g = GCD(f_1, f_2, f_3)$, we first find $r = GCD(f_2, f_3)$. Then $g = GCD(f_1, f_2, f_3) = GCD(f_1, r)$.

Definition 3 . *The Least Common Multiple of polynomials f and g, denoted by $LCM(f, g)$, is the unique polynomial q such that both f and g divide q and that q is the smallest such polynomial in the sense that q divides any polynomial which both f and g divide.*

CHAPTER 2

MULTIVARIATE POLYNOMIALS AND TERM ORDERS

2.1 Multivariate polynomials

The most important algorithm in the polynomial ring is the division algorithm, which is responsible for many nice properties of rings of integers $\mathbb{Z}$ and polynomials $K[x]$ over a field K as we have seen in the introduction. Classical division algorithm for integers goes back to ancient times, and its main properties are described in Euclid's "Elements", including the important Euclidean algorithm for determining the greatest common divisor of two numbers. The corresponding division algorithm for polynomials is possible due to the existence of a natural ordering of monomials $1 < x < x^2 < \ldots < x^n < x^{n+1} < \ldots$ which corresponds to natural ordering of their powers i.e. of integers: $0 < 1 < 2 < \ldots < n < n+1 < \ldots$. All math students are (or at least, should be) familiar with this division and its properties, including the Euclidean algorithm for polynomials. However, in the multivariate polynomial ring there is no such natural linear ordering. Therefore, there is no natural division algorithm in the ring of polynomials with many variables $K[x_1, \ldots, x_n]$. There are various conventions, leading to a number of different possible "orderings" of monomials

and division algorithms. Certainly it is not enough to compare the (total) degree of multivariate monomials, since this would leave us unclear as to whether $x^3y^2z < x^3\ yz^2$ or $x^3y^2z > x^3\ yz^2$.
It is clear that ordering of monomials is equivalent to ordering of their power exponents: there is a correspondence between a monomial $x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ and its multiindex or exponent $\alpha = (\alpha_1, \dots \alpha_n) \in \mathbb{N}_0^n$ (the set of nonnegative integers will be denoted by $\mathbb{N}_0$). Monomial orderings are a particular concern in computation and the results of certain important algorithms, such as the division algorithm, can vary depending on which monomial ordering is chosen.

Definition 4 . *Let $\alpha = (\alpha_1, \dots, \alpha_n)$ be a vector in $\mathbb{N}^n$,and let $x_1, x_2, \dots, x_n$ be any n variables.Then a monomial x^α in $x_1, x_2, \dots, x_n$ is defined as the product $x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$. Moreover, the total degree of the monomial x^α is defined as $|\alpha| = \alpha_1 + \dots + \alpha_n$. A term is an element of the form $cx_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$, where c is a coefficient in a field K.*

Definition 5 . *A multivariate polynomial f in $x_1, x_2, \dots, x_n$ with coefficients in a field K is a finite linear combination,*

$$f(x_1, x_2, \dots, x_n) = \sum_\alpha a_\alpha x^\alpha$$

of monomials x^α and coefficients $a_\alpha \in K$.
The multidegree of f is $multideg(f) = \max\{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\}$ (the maximum is taken with respect to $<$ as we will see later in this chapter).

Definition 6 . *The set of all multivariate polynomials in $x_1, x_2, \dots, x_n$ with coefficients in a field K is denoted by $K[x_1, \dots, x_n]$, it will be called a polynomial ring. It is easy to Check that $K[x_1, \dots, x_n]$ forms a commutative ring.*

Another way to define $K[x_1, \dots, x_n]$ is by induction:

$$K[x_1, \dots, x_n] := (K[x_1, \dots, x_{n-1}])[x_n]$$

Definition 7 . *Let $I \subseteq K[x_1, \dots, x_n]$, $I \neq \phi$. I is an ideal in $K[x_1, \dots, x_n]$ if :*

1. $f, g \in I$ *implies that* $f + g \in I$.

2. $f \in I$ *and* $h \in K[x_1, \ldots, x_n]$ *implies that* $hf \in I$.

Definition 8 . *Let* $F = \{f_1, \ldots, f_s\}$ *be a set of multivariate polynomials. Then the ideal generated by* F*, denoted by* $I = \langle F \rangle$*, is given by:*

$$\left\{ \sum_{i=1}^{s} g_i f_i : g_i \in K\left[x_1, \ldots, x_n\right], i = 1, \ldots, n \right\}.$$

The polynomials $f_1, \ldots, f_s$ *are called a basis for the ideal they generate. Since* F *is finite, we say the ideal is finitely generated.*

Definition 9 . *A partial order on a set* X *is a relation* $\leq$ *on* X *such that:*

(i) $a \leq a$ *for every* $a \in X$*, for all* $a \in X$ *(the relation is reflexive),*

(ii) if $a \leq b$ *and* $b \leq c$ *then* $a \leq c$*, for all* $a, b, c \in X$ *(the relation is transitive),*

(iii) if $a \leq b$ *and* $b \leq a$*, then* $a = b$*, for all* $a, b \in X$ *(the relation is antisymmetric).*

A partial order is called a total (linear) order if, in addition,

(iv) for all $a, b \in X$*, either* $a \leq b$ *or* $b \leq a$.

A partial order is called a well-ordering if moreover the following holds:

(v) Every nonempty subset $S \subset X$ *has a least element in this ordering.*

A corresponding strict order with notation:

$$a < b \Leftrightarrow a \leq b \wedge a \neq b,$$

will be also used in the sequel. In fact every well ordered set is totally ordered set, but only a finite set with a total order is well ordered, and this is not true of infinite sets.

2.2 Monomial orderings

In this section we discuss different ways to order the monomials of a polynomial ring. This is needed in order to set up a division algorithm in the case of several variables. A set of monomials in n variables can be considered as the set of the formal expressions $\mathbb{T}^n = \{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} | \alpha_i \in \mathbb{N}_0, i = 1, \dots, n\}$. That is the so called multiplicative form of a monomial. So every power product is a term (with coefficient 1), but a term is not necessarily a power product. Notice that a term order gives a total order on $\mathbb{N}_0^n$ by the rule :

$$\alpha < \beta \Leftrightarrow x^\alpha < x^\beta,$$

for $\alpha, \beta \in \mathbb{N}_0^n$. So we can consider term orders to be defined on $\mathbb{N}_0^n$.
First, notice that a term order on $\mathbb{N}_0^n$ can be extended to a total order on $\mathbb{N}^n$ that is compatible with its properties as an additive group. For any $\alpha, \beta \in \mathbb{Z}^n$, the rule for the extended order is :

$$\alpha < \beta \Leftrightarrow x^{\alpha+\gamma} < x^{\beta+\gamma},$$

for some $\gamma \in \mathbb{N}_0^n$ such that $\alpha + \gamma, \beta + \gamma \in \mathbb{N}_0^n$.
Let a total ordering $<$ on $\mathbb{T}^n$ or $(\mathbb{N}_0^n)$ be fixed, i.e. any two different monomials are comparable and $<$ is irreflexible, antisymmetric and transitive.

Definition 10 . *A term ordering on $K[x_1, \dots, x_n]$ is a total ordering $<$ on $\mathbb{T}^n$ such that:*

1. *$1 < N$ for every $N \in \mathbb{T}^n$, $M \neq 1$.*

2. *For every $N_1, N_2, N \in \mathbb{T}^n$ with $N_1 < N_2$, then $N_1.N < N_2.N$.*

Definition 11 . *Let K be a field. A monomial ordering on $K[x_1, \dots, x_n]$ is any partial order relation $<$ on $\mathbb{N}_0^n$, or equivalently, any partial order relation on the set of monomials $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$ such that:*

1. *$<$ is a total (linear) ordering on $\mathbb{N}_0^n$,*

2. *If $\alpha < \beta \in \mathbb{N}_0^n$ and $\gamma \in \mathbb{N}_0^n$ then $\alpha + \gamma < \beta + \gamma$ (the additive property),*

3. *$<$ is a well-ordering on $\mathbb{N}_0^n$.*

Note that every well-ordering is automatically a total order, so condition (3) implies (1).

Lemma 2 . *The element* $0 = (0, \ldots, 0) \in \mathbb{N}_0^n$ *is necessarily the smallest element in* $\mathbb{N}_0^n$ *under any order.*

Proof. If $\alpha < 0$ then, since $\alpha \in \mathbb{N}_0^n$, the additive property implies that $\alpha + \alpha < 0 + \alpha$ or $2\alpha < \alpha$. We repeat this argument to get that

$$0 > \alpha > 2\alpha > 3\alpha > \ldots .$$

Then the set $\{0, \alpha, 2\alpha, \ldots\}$ doesn't have a smallest element and the ordering is not a well-ordering. $\square$
This is equivalent to condition (3).

Proposition 1 . *Let the ordering* $<$ *on* $\mathbb{N}_0^n$ *satisfy the following properties:*

1. *It is a total ordering.*
2. *It is additive in* $\mathbb{N}_0^n$ *i.e.* $i < j \Rightarrow i + k < j + k$.
3. $0 < i$ *for all* $i \in \mathbb{N}_0^n$.

Then $<$ *is a well-ordering.*

Proof. Conditions 2.) and 3.) clearly imply that $i \in j + \mathbb{N}_0^n \Rightarrow j \preceq i$ or equivalently, $i < j \Rightarrow i \notin j + \mathbb{N}_0^n$. Now, it is sufficient to prove that $<$ satisfies the descending chain condition (DCC for short).
Let now

$$S : \ldots < i^{(k)} = \left(i_1^{(k)}, \ldots, i_n^{(k)}\right) < \ldots < i^{(1)} = \left(i_1^{(1)}, \ldots, i_n^{(1)}\right)$$

be a descending chain in $\mathbb{N}_0^n$. It would suffice to show that the set $S_1 = \left\{i^{(k)} \in S | i_1^{(k)} < i_1^{(1)}\right\} \subset S$ is finite, since this can be applied to any coordinate $i_1, \ldots, i_n$. Let $i_1' = \max\left\{i_1^{(k)} | i^{(k)} \in S_1\right\} < i_1^{(1)}$ be the biggest first coordinate of elements in S_1. Condition 1) and the property following from 2.) and 3.) imply that there can be only finitely many points in S_1 with the first coordinate i_1', and there is the smallest one (with respect to $<$) $i^{(m)} \in S_1$. So, $i_1^{(m)} = i_1' < i_1^{(1)}$. By infinite descent reasoning, one obtains that the set S_1 must be finite. $\square$

Note that we have defined a monomial ordering as an ordering on n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$. Since there is a one–to–one relationship between the monomials in $K[x_1, \ldots x_n]$ and $\mathbb{N}_0^n$ so that monomial $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ corresponds to n-tuple α (its exponent), the ordering $<$ on $\mathbb{N}_0^n$ gives us an ordering on monomials in $K[x_1, \ldots, x_n]$. This is, if $\alpha < \beta$ then $x^\alpha < x^\beta$. Obviously, the additive property changes to multiplicative property in this case. The monomial ordering in one variable case can also be thought of simply as divisibility. That is x is smaller than x^2, since x divides x^2. One can easily see that divisibility is not a monomial ordering in $K[x_1, \ldots, x_n]$ for $n > 1$, since divisibility can not help us to decide in general whether one monomial is greater than another. In the terms of exponents, divisibility corresponds to addition:

$$x^\alpha | x^\beta \Leftrightarrow \exists \gamma : \beta = \alpha + \gamma.$$

This implies, but is not equivalent to $\alpha < \beta$. We must have some way of ordering these variables.

2.3 Examples of monomial orderings

1. **Lexicographic order**
The lexicographic order (*lex*) with $x_1 > \ldots > x_n$ on the monomials of $K[x_1, \ldots, x_n]$ is defined as follows:
For $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}_0^n$, we define $x^\alpha <_{lex} x^\beta$ if the first coordinates α_i and β_i in α and β from the left, which are different, satisfy $\alpha_i < \beta_i$. So, we say

$$x^\alpha <_{lex} x^\beta \quad \text{if} \quad \alpha <_{lex} \beta.$$

It is important to realize that there are many *lex* orders, corresponding to how variables are ordered.
For example, if the variables are x and y, then we get one *lex* order with $x < y$ and another with $y < x$. In the general case of n variables, there are $n!$ different *lex* orders.

2. **Graded lexicographic order**
The graded lexicographic order (*grlex*) with $x_1 > \ldots > x_n$ on the monomials of $K[x_1, \ldots, x_n]$ is defined as follows:
For α and $\beta \in \mathbb{N}_0^n$, $x^\alpha <_{grlex} x^\beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i < |\beta| = \sum_{i=1}^n \beta_i$ or $|\alpha| = |\beta|$ and $x^\alpha <_{lex} x^\beta$. The number $|\alpha|$ is called the degree of α.

3. **Graded reverse lexicographic order**
The graded reverse lexicographic order (*grevlex*) with $x_1 > \ldots > x_n$ on the monomials of $K[x_1, \ldots, x_n]$ is defined as follows:
For α and $\beta \in \mathbb{N}_0^n$, $x^\alpha <_{grevlex} x^\beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i < |\beta| = \sum_{i=1}^n \beta_1$ or $|\alpha| = |\beta|$ and the first coordinates α_i and β_i in α and β from the right, which are differen, satisfy $\alpha_i > \beta_i$

Definition 12 . *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $K[x_1, \ldots, x_n]$ and let $<$ be a monomial order, then:*

1. *The leading coefficient of f is $LC(f) = a_{multideg(f)} \in K$,*
2. *The leading monomial of f is $LM(f) = x^{multideg(f)}$ (with coefficient 1),*
3. *The leading term of f is $LT(f) = LC(f) \cdot LM(f)$,*
4. *The support of a polynomial f is the set $supp(f) = \{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\} \subset \mathbb{N}_0^n$.*

We will consider the polynomial $f = 4x^2y^3z^2 + 3y^5z - 5x^3 + 3xy^2z^3$ in $K[x, y, z]$, to see how the different monomial orderings affect the ordering of polynomials then.

(a) We order the terms of f with respect to the (*lex*) order, as follows:

$$f = -5x^3 + 4x^2y^3z^2 + 3xy^2z^3 + 3y^5z$$

$multideg(f) = (3, 0, 0)$, $LM(f) = x^3$, $LC(f) = -5$, $LT(f) = -5x^3$.

(b) We order the terms of f with respect to the (*grlex*) order, as follows:

$$f = 4x^2y^3z^2 + 3xy^2z^3 + 3y^5z - 5x^3$$

$multideg(f) = (2, 3, 2), LM(f) = x^2y^3z^2, LC(f) = 4, LT(f) = 4x^2y^3z^2$.

(c) We order the terms of f with respect to the (*grevlex*) order, as follows:

$$f = 4x^2y^3z^2 + 3y^5z + 3xy^2z^3 - 5x^3$$

$multideg(f) = (2, 3, 2), LM(f) = x^2y^3z^2, LC(f) = 4, LT(f) = 4x^2y^3z^2$.

4. **Matrix ordering**
Let $\alpha, \beta \in \mathbb{N}_0^n$ and let $M \in GL(n, \mathbb{R})$ be an invertible matrix over real numbers. We define a relation $<_M$ on $\mathbb{N}_0^n$ by the condition:

$$\alpha <_M \beta \Longleftrightarrow M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} <_{lex} M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

This is a total ordering since M is invertible. It is monomial if for all $\alpha \in \mathbb{N}_0^n$ the first nonzero term of $M\,(\alpha_1, \ldots, \alpha_n)^T$ is positive (because the monomial 1 is the minimal element on $\mathbb{T}^n$ the set of monomials in $K\,[x_1, \ldots, x_n]$).
Here are some examples of matrix orderings.
The matrix associated with lexicographic ordering (*lex*) in three variables is:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and *deglex* is given by $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$,

and *degrevlex* is given by $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$.

The matrix associated with the given monomial ordering is clearly not uniquely determined.(see [1],[8][19])

Lemma 3 *([7] p. 60). Let $f, g \in K[x_1, \ldots, x_n]$ be nonzero polynomials. Then:*

1. *$multideg(fg) = multideg(f) + multideg(g)$.*
2. *If $f + g \neq 0$, then $multideg(f + g) \leq max(multideg(f), multideg(g))$. If, in addition, $multideg(f) \neq multideg(g)$ then equality occurs.*

Proof. Let $f = \sum_\alpha a_\alpha x^\alpha$ and $g = \sum_\beta b_\beta x^\beta$ for $\alpha, \beta \in \mathbb{N}_0^n$.

1. first we have to proof that $multideg(fg) = multideg(f) + multideg(g)$.

$$fg = \sum_\alpha a_\alpha x^\alpha \sum_\beta b_\beta x^\beta$$

$$= \sum_{\alpha}\sum_{\beta} a_\alpha b_\beta x^\alpha x^\beta$$
$$= \sum_{\alpha}\sum_{\beta} a_\alpha b_\beta x^{\alpha+\beta}$$

Then

$$\begin{aligned} multideg(fg) &= max(\alpha+\beta \in \mathbb{N}_0^n : a_\alpha b_\beta \neq 0) \\ &= max(\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0) + max(\beta \in \mathbb{N}_0^n : b_\beta \neq 0) \\ &= multideg(f) + multideg(g). \end{aligned}$$

2. Suppose that $f+g \neq 0$ and that $multideg(f) = multideg(g)$. So $LM(f) = LM(g)$. We have to proof that:

$$multideg(f+g) \leq max(multideg(f), multideg(g)).$$

If $LC(f)+LC(g) = 0$, then $LT(f)$ and $LT(g)$ cancel and $multideg(f+g) < max(multideg(f), multideg(g))$. If $LC(f)+LC(g) \neq 0$, then $LM(f+g) = LM(f) = LM(g)$.

Suppose that $f+g \neq 0$ and $multideg(f) \neq multideg(g)$. If, $multideg(f) > multideg(g)$. Then $LM(f) > LM(g)$ and so $LM(f+g) = LM(f)$. Therefore $multideg(f+g) = multideg(f) = max(multideg(f), multideg(g))$. □

2.4 Classification of monomial orders

The orderings on a polynomial ring are related with the computation of Gröbner bases and the efficiency of Buchberger Algorithm. These orderings have been classified by L. Robbiano in [18] by using ordered systems of vectors. He showed that term orders are in one-to-one correspondence with a certain subset of real matrices. And this classification was originally done by C.Riquier [6] G.Trevisan [13] and E.R.Kolehin [12]. Unfortunately his classification gives little information as to the intuitive shape of these sets. He classified total orders on $\mathbb{Q}^n$ that are compatible with the vector space structure of $\mathbb{Q}^n$ to characterize term orders. An ordering on $\mathbb{Z}^n$ can be extended to an ordering on $\mathbb{Q}^n$ that is compatible with its properties as an abelian group. For any $\alpha, \beta \in \mathbb{Q}^n$, the rule for the extension is:

$$\alpha < \beta \Leftrightarrow \begin{cases} r\alpha < r\beta & \text{with respect to the order on } \mathbb{Z}^n \\ \text{for some } r \in \mathbb{Z}^+ \text{ such that } r\alpha, r\beta \in \mathbb{Z}^n. \end{cases}$$

Furthermore, a total ordering on $\mathbb{Q}^n$ compatible with its properties as an abelian group can be restricted to a term order if $\alpha > (0, \ldots, 0)$ for all $\alpha \in \mathbb{N}_0^n - (0, \ldots, 0)$.
For example, lexicographic order will be used both as a term order on the terms of $K[x_1, \ldots, x_n]$ and as an order on $\mathbb{R}^n$ with $\alpha, \beta \in \mathbb{R}^n$.
Sturmfels discusses another method for classifying term orders in [4] by using weight vectors and arbitrary term orders, to describe term orders in $K[x_1, \ldots, x_n]$.

Definition 13 . *let $\omega = (\omega_1, \omega_2, \ldots, \omega_n)$ be a nonzero vector with real entries (called a weight vector), and arbitrary term order $<$ on $K[x_1, \ldots, x_n]$. We define the term order $<_\omega$ for $\omega \geq 0$ by:*
$x^\alpha <_\omega x^\beta$ if $\alpha.\omega < \beta.\omega$ or $\alpha.\omega = \beta.\omega$ and $x^\alpha < x^\beta$.

For example, take $\omega = (1, 2)$ and consider $x^2 + y^2$. Then $(2, 0).\omega = 2$ while $(0, 2).\omega = 4$, which would give that $x^2 < y^2$. And we can see that orders $<_\omega$, for $\omega \geq 0$ correspond to previously mentioned examples of term orders.

Proposition 2 . *For an arbitrary term order $<$ and $\omega \geq 0$, then $<_\omega$ satisfies the conditions of a term order.*

Proof. We want to show that each of the three conditions are true.
1. Take two power vectors $\alpha \neq \beta$. Then for $\omega \geq 0$ either $\alpha.\omega > \beta.\omega, \alpha.\omega < \beta.\omega$ or $\alpha.\omega = \beta.\omega$. In the first two cases, we have that $\alpha >_\omega \beta$ and $\alpha <_\omega \beta$ respectively. In the third case, the term order $<$ implies that either $\alpha > \beta$ or $\alpha < \beta$.
2. Since $\omega, \alpha \in \mathbb{N}_0^n$, then we have $\alpha.\omega \geq 0$. If $\alpha.\omega > 0$, then $\alpha >_\omega 0$. If $\alpha.\omega = 0$ then $\alpha > 0$ because $<$ is a term order, therefore $\alpha >_\omega 0$.
3. Let α, β two power vectors and suppose that $\alpha >_\omega \beta$. Then either $\alpha.\omega > \beta.\omega$ or $\alpha.\omega = \beta.\omega$ and $\alpha > \beta$. Suppose that $\alpha.\omega > \beta.\omega$, then $(\gamma + \alpha).\omega = (\gamma.\omega) + (\alpha.\omega) > (\gamma.\omega) + (\beta.\omega) = (\gamma + \beta).\omega$ for all $\gamma \in \mathbb{N}_0^n$ and thus $\gamma + \alpha >_\omega \gamma + \beta$.
Now suppose $\alpha.\omega = \beta.\omega$, then we have that $\alpha > \beta$ in the term order $<$. Since $<$ is a term order, $\gamma + \alpha > \gamma + \beta$ and thus $\gamma + \alpha >_\omega \gamma + \beta$ $\square$

Definition 14 . *Let $\omega \in \mathbb{R}^n$. For any polynomial $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha \in K[x_1, \ldots, x_n]$ we define the initial form*

$$in_\omega(f) = \sum_{\alpha' \in \mathbb{N}^n} a_{\alpha'} X^{\alpha'},$$

where the vectors α' maximize $\omega.\alpha'$ in $\{\alpha | a_\alpha \neq 0\}$ that is $\omega.\alpha' \geq \omega.\alpha$ for any α with $a_\alpha \neq 0$.

Definition 15 . *For an ideal $I \subset K[x_1, \ldots, x_n]$ we define the initial form of the ideal I:*

$$in_\omega(I) = \langle in_\omega(f) | f \in I \rangle$$

Example 3 . *Let I be an ideal generated by*

$$f(x, y) = x^6y^2 + x^5y^3 - x^3 + 2x^2y^4 + x^2 - xy + y^2 - 2$$

We can compute the initial form for $\omega = (2, 1)$ and $\omega = (1, 1)$, as follows:
The vectors α with $a_\alpha \neq 0$ are $\alpha_1 = (6, 2), \alpha_2 = (5, 3), \alpha_3 = (3, 0), \alpha_4 = (2, 4), \alpha_5 = (2, 0), \alpha_6 = (1, 1), \alpha_7 = (0, 2), \alpha_8 = (0, 0)$.
For $\omega = (2, 1)$ then $\omega.\alpha_i = \{14, 13, 6, 8, 4, 3, 2, 0\}$, $i = 1, \ldots, 8$ and the maximum of this list is $\omega.\alpha_1 = 14$. So $in_\omega(f) = x^6y^2$, and $in_\omega(I) = \langle x^6y^2 \rangle$. This is a monomial ideal.
For $\omega = (1, 1)$ then $\omega.\alpha_i = \{8, 8, 3, 6, 2, 2, 2, 0\}$, $i = 1, \ldots, 8$ and the maximum of this list is 8 given by $\omega.\alpha_1$ and $\omega.\alpha_2$. So $in_\omega(f) = x^6y^2 + x^5y^3$, and $in_\omega(I) = \langle x^6y^2 + x^5y^3 \rangle$. Which is not a monomial ideal.

Also, Sturmfels mentions to important results for term ordering with respect to weight vectors.

Corollary 1 . *If $\omega \geq 0$ and $in_\omega(I)$ is a monomial ideal, then $in_\omega(I) = in_{<_\omega}(I)$, $(in_{<_\omega}(I) = in_< \langle in_\omega(I) \rangle)$.*

And the following proposition shows, for every term order $<$, we can find a vector ω which represents this term order and it is easier to use it instead of $<$ in computations.

Proposition 3 . *For any term order $<$ and any ideal $I \subset K[x_1, \ldots, x_n]$, there exists a non-negative integer vector $\omega \in \mathbb{R}^n$ such that $in_\omega(I) = in_<(I)$.*

For $\omega \in \mathbb{R}^n$ and a term order $<$ such that $in_\omega(I) = in_<(I)$, we call ω a term order for I which represents the term order $<$. For proofs and more details(see [4]).

There is a geometrical point of view, which deals with convex hulls and supporting planes. In the case of two variables, the weight vectors can be expressed as line slopes. So the weight vector $\omega = (p, q)$ is converted to $\frac{q}{p}$, where $p \neq 0$ (and ∞ if $p = 0$). The slope m represents the weight vector $\omega_m = (1, m)$ and the corresponding family of parallel lines $x + my = d$. We start with two important propositions about irrational slopes.

Proposition 4 . *Any positive irrational number m determines a term order.*

Proof. Let $\omega = \omega_m = (1, m)$ with m irrational, and choose an arbitrary term order $<$. Then we can compare any two exponent vectors $e_1 = (a_1, b_1)$, and $e_2 = (a_2, b_2)$ using $<_m$. If we define term order $<_m$ on $K[x_1, \ldots, x_n]$ for nonzero weight vector by $x^\alpha <_m y^\beta$ if $\alpha.\omega_m < \beta.\omega_m$ or if $\alpha.\omega_m = \beta.\omega_m$ and $x^\alpha < y^\beta$, then

$$e_1 <_m e_2 \Leftrightarrow e_1.\omega_m < e_2.\omega_m \quad \text{or} \quad e_1.\omega_m = e_2.\omega_m \quad \text{and} \quad e_1 < e_2.$$

But m is irrational and $a_1+b_1m \neq a_2+b_2m$ (since $a_1+b_1m = a_2+b_2m$ would imply $m = \frac{a_1-a_2}{b_2-b_1} \in \mathbb{Q}$), $e_1 <_m e_2 \Leftrightarrow a_1 + b_1m < a_2 + b_2m \Leftrightarrow e_1.\omega_m < e_2.\omega_m$. The vector ω_m determines a family of lines $(x, y).\omega_m = d$ or $x + my = d$ with different d's.
Since m is irrational, every such line can contain at most one point from $\mathbb{Z}^2$. The relation $e_1 <_m e_2$ means that points e_1 and e_2 lay on different lines with respective parameters $d_1 < d_2$. $\square$

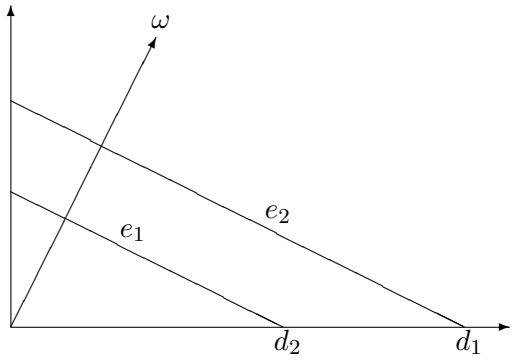

Figure 2.1:

One can immediately see that the resulting order $<_m$ for irrational m does not depend on the choice of the original order $<$ in $\mathbb{Z}^2$.

Proposition 5 . *Different numbers give different term orders.*

Proof. Take two positive numbers $m_1 \neq m_2$, then there exists a rational $\frac{p}{q}$ such that $m_1 < \frac{p}{q} < m_2$. Take $\omega_1 = (1, m_1)$, $\omega_2 = (1, m_2)$ two weight vectors. For the two points $(p, 0), (0, q) \in \mathbb{Z}^2$ one has $(p, 0) >_{\omega_1} (0, q)$, but $(p, 0) <_{\omega_2} (0, q)$. Hence m_1 and m_2 represent different term orders. □

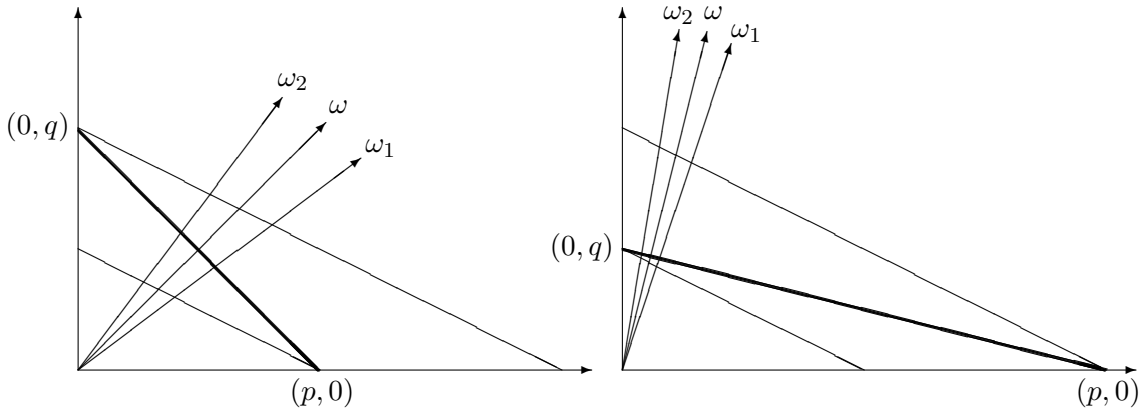

Figure 2.2:

Proposition 6 . *Any positive rational q defines exactly two different term orders.*

Proof. If we have $q = \frac{s}{r} \neq 0$ a rational number, where $r, s \in \mathbb{Z}^2$ then the polynomial $f = x^s + y^r$ represents a tie between the terms. So, here a "tiebreaking" order is needed. In two variables, there is a simple choice. We can choose *lex* with $x < y$ or *lex* with $y < x$.
Geometrically, in this case we have two points $(s, 0)$ and $(0, r)$ on the same line $x+qy = s$ look at the Figure (1.3), and we have to compare them: either $(s, 0) < (0, r)$ or $(0, r) < (s, 0)$. We will use q^- to represent the term order defined by q with the tiebreaker of *lex* with $y < x$ and q^+ to represent the term order defined by q with the tiebreaker of *lex* with $x < y$. Obviously, q^+ and q^- are different term orders. □

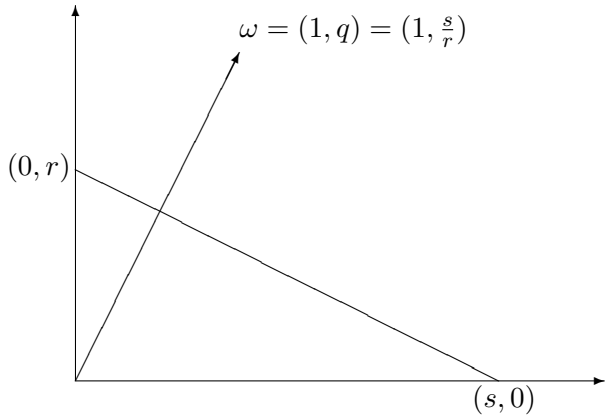

Figure 2.3:

There are two exceptions. The first term order is described by the slope $0 : m = 0$, $\omega = (1, 0)$ (we need only to consider the case 0^+). So that weight 1 is given to the x component of the exponent vector, but no weight is given to the y component. Geometrically, the lines of this family are parallel to y-axis and contain infinitely many net points, and the order is uniquely determined by the condition $(0, 0) < (0, 1)$. This order is denoted by 0^+. It is actually *lex* with $y < x$. The second one is the term order described by the slope ∞ (we need only to consider the case ∞^-): $m = \infty$, $\omega = (1, \infty) = (0, 1)$. Geometrically, the lines of this family are parallel to x-axis and contain infinitely many net points, and the order is uniquely determined by the condition $(0, 0) < (1, 0)$, this order is denoted by ∞^-. It is actually *lex* with $x < y$.

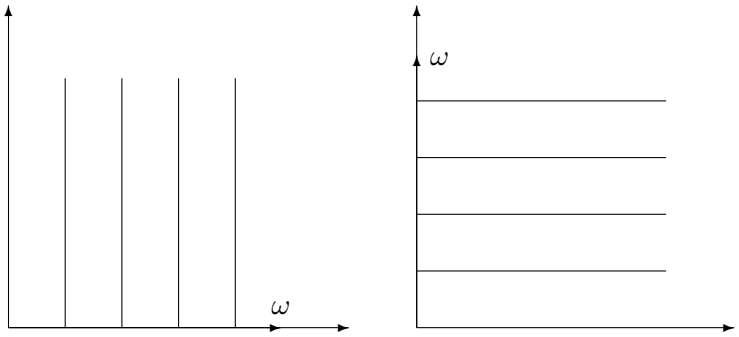

Figure 2.4:

We will give some examples for these term orders to calculate a Gröbner basis for ideals in the chapter[4].

Theorem 5 . *The set of all term orders on* $\mathbb{N}_0^2$ *is*
$\{0^+, \infty^-\} \cup \{q^+, q^- : q \text{ positive rational}\} \cup \{m : m \text{ positive irrational}\}$.

Proof. We first remark that any term order $<$ on $\mathbb{N}_0^2$ is determined by all pairs $(s,r) \in \mathbb{N}^2$ such that $(s,0) < (0,r)$.
Indeed, take $\alpha, \beta \in \mathbb{N}_0^2$. If $(0,0) \neq \alpha - \beta \in \mathbb{N}_0^2$, then α is bigger then β with respect to any term order. So, it remains to compare $\alpha = (x_1, y_1), \beta = (x_2, y_2) \in \mathbb{N}_0^2$ such that $\alpha - \beta \in \mathbb{N} \times (-\mathbb{N})$, that is $x_1 > x_2$, $y_2 > y_1$. Term orders are total and additive, therefore in this case we have $\alpha \prec \beta \Leftrightarrow (x_1 - x_2, 0) < (0, y_2 - y_1)$.
For a given term order $<$ define the non-empty subset $\Lambda_<$ of $\mathbb{Q}_{\geq 0}$ by

$$\Lambda_< = \left\{ \frac{s}{r} : (s,r) \in \mathbb{N}_0 \times \mathbb{N}, (s,0) < (0,r) \right\}.$$

Then, take its least upper bound $\ell = \sup(\Lambda_<) \in \mathbb{R}_{\geq 0} \cup \{\infty\}$. According to previous propositions, $\Lambda_<$ determines another order $<' = \begin{cases} \ell^+, & \text{if } \ell \in \Lambda_<; \\ \ell^-, & \text{if } \ell \notin \Lambda_<. \end{cases}$
If $(s,r) \in \mathbb{N}_0 \times \mathbb{N}$ then $(s,0) <' (0,r) \Leftrightarrow \begin{cases} \frac{s}{r} \leq \ell, & \ell \in \Lambda_<; \\ \frac{s}{r} < \ell, & \ell \notin \Lambda_<. \end{cases}$
We want to prove that this order is the same as the original one. According to the initial remark, it is sufficient to show that for all $(s,r) \in \mathbb{N}^2$ one has $(s,0) < (0,r) \Leftrightarrow (s,0) <' (0,r)$.
First, note that $(s,0) < (0,r) \Rightarrow \frac{s}{r} \in \Lambda_< \Rightarrow \frac{s}{r} \leq \ell \Rightarrow (s,0) <' (0,r)$.
Now, assume that $(s,0) <' (0,r)$ and consider the above definitions.
If $\frac{s}{r} = \ell \in \Lambda_<$, then $(s,0) < (0,r)$.
If $\frac{s}{r} < \ell$, then there exists $\frac{s'}{r'} \in \Lambda_<$ such that $\frac{s}{r} < \frac{s'}{r'} \leq \ell$ and $(s',0) < (0,r')$. Therefore $r's < rs'$ and $(r's, 0) < (rs', 0) < (0, rr')$. The latter imply $(r's, 0) < (0, rr')$. Hence $(s,0) < (0,r)$, as required.
Symbols α,α',β,β',γ, k, k' from the second picture correspond to $(0,r)$,$(0,r')$,$(s,0)$,$(s',0)$,$r'\alpha = r\alpha', r', r$ from the proof. $\square$

This classification agrees with classification of Robbiano in [18] for the case $n = 2$. If we denote the set of all term orders in $\mathbb{N}_0^n$ by $Term(2)$ and introduce an order topology in it as in [9], then there are specific links between the Cantor set and the set $Term(2)$ obtaind by using the topological fact that any compact, perfect, totally disconnected metric space is homeomorphic to the Cantor set (See[])

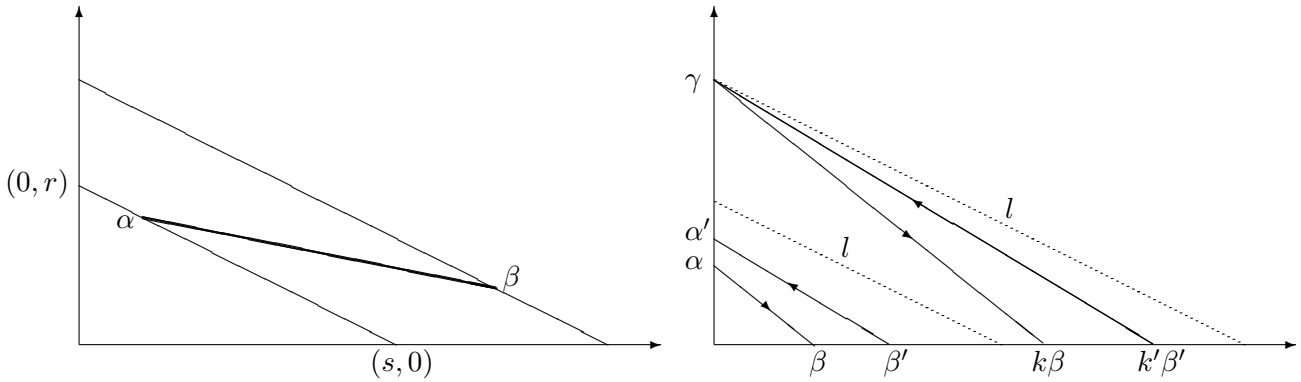

Figure 2.5:

Theorem 6 . *$Term(2)$ is homeomorphic to the Cantor set.*

For the proof in [9]. This classification will lead to a natural approach to some of results of T. Mora and L. Robbiano in the the bivariate case [22].

CHAPTER 3

MULTIVARIATE REDUCTION AND DIVISION

3.1 Multivariate reduction

The multivariable division algorithm consists of a sequence of reduction steps as follows.

Definition 16 . *Let $f, g, h \in K[x_1, \ldots, x_n]$ with $g \neq 0$. We say that f reduces to h modulo g in one step, denoted*

$$f \to_g h,$$

if and only if $LM(g)$ divides a non-zero term ax^α that appears in f and

$$h = f - \frac{ax^\alpha}{LT(g)}g.$$

This mimics the steps in the univariate polynomial long division as we have seen in our previous example(1). In the multivariate case, one can think of h in Definition(16) as the remainder of an one step division of f by g.
In the multivariate case, it may also be the case that we have to divide by more than one polynomial at a time. We extend the previous Definition to include this possibility:

Definition 17 . *Let f,h and $f_1, \ldots, f_s$ be polynomials in $K[x_1, \ldots, x_n]$ with $f_i \neq 0$ for $i = 1, \ldots, s$. Let $F = \{f_1, \ldots, f_s\}$. We say that f reduces to h modulo F, denoted*

$$f \to_F^+ h,$$

if and only if there exist a sequence of indices $i_1, i_2, \ldots, i_t \in \{1, \ldots, s\}$ and a sequence of polynomials $h_1, \ldots, h_{t-1} \in K[x_1, \ldots, x_n]$ such that

$$f \to_{f_{i_1}} h_1 \to_{f_{i_2}} h_2 \to_{f_{i_3}} \ldots \to_{f_{i_{t-1}}} h_{t-1} \to_{f_{i_t}} h.$$

A polynomial h is called reduced with respect to a set of non-zero polynomials $F = \{f_1, \ldots, f_s\}$ if $h = 0$ or no monomial that appears in h is divisible by any one of the $LM(f_i), i = 1, \ldots, s$. Then we call h a remainder for f with respect to F.

Example 4 . *Let $F = \{f_1, f_2\}$, where $f_1 = 3xy^2 + 2x + y^2$ and $f_2 = 2y^2 - y - 1$. Consider the polynomial $f = x^3y^3 + 2y^2$. These polynomials are ordered with respect to the lex order with $y < x$ in $\mathbb{Q}[x, y]$.*
First, we reduce f modulo f_1 in one step:
We have $LT(f_1) = 3xy^2$, and $ax^\alpha = x^3y^3$ is a power product in f such that $LT(f_1)$ divides it. So, we get

$$\begin{aligned} h_1 &= f - \frac{ax^\alpha}{LT(f_1)} f_1 \\ &= x^3y^3 + 2y^2 - \frac{x^3y^3}{3xy^2}(3xy^2 + 2x + y^2) \\ &= -\frac{2}{3}x^3y - \frac{1}{3}x^2y^3 + 2y^2. \end{aligned}$$

That is, $f \to_{f_1} h_1$.
Second, we reduce h_1 modulo f_2 in one step:
We have $LT(f_2) = 2y^2$. Since $LT(f_2)$ divides both $-\frac{1}{3}x^2y^3$ and $2y^2$, we have two choices for ax^α. We let $ax^\alpha = -\frac{1}{3}x^2y^3$. Then, we get

$$\begin{aligned} h_2 &= h_1 - \frac{ax^\alpha}{LT(f_2)} f_2 \\ &= -\frac{2}{3}x^3y - \frac{1}{3}x^2y^3 + 2y^2 - \frac{-\frac{1}{3}x^2y^3}{2y^2}(2y^2 - y - 1) \\ &= -\frac{2}{3}x^3y - \frac{1}{6}x^2y^2 - \frac{1}{6}x^2y + 2y^2. \end{aligned}$$

That is, $h_1 \rightarrow_{f_2} h_2$. If we take $ax^\alpha = 2y^2$, then we get

$$\begin{aligned} h_2 &= h_1 - \frac{ax^\alpha}{LT(f_2)} f_2 \\ &= -\frac{2}{3}x^3y - \frac{1}{3}x^2y^3 + 2y^2 - \frac{2y^2}{2y^2}(2y^2 - y - 1) \\ &= -\frac{2}{3}x^3y - \frac{1}{3}x^2y^3 + y + 1. \end{aligned}$$

It is also $h_1 \rightarrow_{f_2} h_2$.

3.2 Multivariable division algorithm

In the division algorithm for polynomials in one variable as stated in the introduction, for the input of a divisor and a dividend we are guaranteed a unique and well defined output of a quotient and remainder. However, in the case of multivariate polynomials, the "quotients" and remainder depend on the monomial ordering and on the order of the divisors in the division. The division algorithm in the multivariable case allows us to divide $f \in K[x_1, \ldots, x_n]$ by $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, so that we can express f in the form $f = q_1 f_1 + \ldots + q_s f_s + r$ where $q_1, \ldots, q_s, r \in K[x_1, \ldots, x_n]$. The strategy is to repeatedly cancel the leading term of f by subtracting off an appropriate multiple of one of the f_i. However, the result of the division algorithm fails to be unique for multivariate polynomials because there may be a choice of divisor at each step.
The division algorithm is described in what follows.

1. Start with $q_1 = q_2 = \ldots = q_i = r = 0$.

2. If $f = 0$, stop. Otherwise, for each $i = 1, \ldots, s$ check if $LT(f_i)$ divides $LT(f)$. If so, replace f by $f - \frac{LT(f)}{LT(f_i)}$, add $\frac{LT(f)}{LT(f_i)}$ to q_i and then return to the beginning of 2). If $LT(g_i)$ doesn't divide $LT(f)$ for any i, continue to 3).

3. Add $LT(f)$ to r, replace f by $f - LT(f)$, and then return to the beginning of 2).

This algorithm always terminates, because we have built in the definition of a monomial order that it is well-ordered, and the multidegree of f is reduced in each iteration. Recall that an ideal I in a commutative ring R is an additive subgroup in R which has the ideal property: $a \in R, b \in I \Rightarrow ab \in I$.

The ideal $I = \langle b_1, \ldots, b_n \rangle \subset R$ generated by $b_1, \ldots, b_n \in R$ is the set of all elements of the form $a_1 b_1 + \ldots + a_n b_n$, where $a_1, \ldots, a_n \in R$. Now, if the remainder when f is divided by $f_1, \ldots, f_s$ is zero, then clearly f is in the ideal generated by f_i. However, as examples show, the converse does not hold.

Theorem 7 . *(Division algorithm in $K[x_1, \ldots, x_n]$). Fix a monomial order $<$ on $\mathbb{N}_0^n$, and let $G = \{f_1, \ldots, f_s\}$ be an ordered s-tuple of polynomials in $K[x_1, \ldots, x_n]$. Then every $f \in K[x_1, \ldots, x_n]$ can be written as:*

$$f = q_1 f_1 + \ldots + q_s f_s + r,$$

where $q_i, r \in K[x_1, \ldots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in K of monomials none of which is divisible by any of $LT(f_1), \ldots, LT(f_s)$. We call r a remainder of f in division by G. Furthermore, if $q_i f_i \neq 0$ then we have

$$multideg(f) \geq multideg(q_i f_i)$$

.

For the proof (see [7] p. 64-66)

Example 5 . *We will divide $f = x^2y^3 + 2xy + x + 1$ by $f_1 = x^2 + 1$ and $f_2 = y^3 + 1$ using lex order with $y < x$. Then according to our algorithm we get the following:*

$(x^2y^3+2xy+x+1)$	$: (x^2+1)$	$= y^3$	$\underline{r}$
$-(x^2y^3 + y^3)$			
$(2xy + x - y^3 + 1)$	$: (y^3+1)$	$= -1$	$\rightarrow 2xy+x$
$-(-y^3 - 1)$			
2			$\rightarrow 2xy+x+2$

The graphical representation used above for the division process is standard. After dividing f by $LT(f_1)$, we get the polynomial $2xy + x - y^3 + 1$ with no terms that are divisible by the $LT(f_1)$. Furthermore, the first low terms, $2xy$ and x are not divisible by the $LT(f_2)$, so these go to the remainder column $\underline{r}$. We are left with $-y^3 + 1$ and we divide this by the $LT(f_2)$. We get $q_1 = y^3$. After dividing by the $LT(f_2)$, we get the 2, and so this term is

sent to the remainder column $\underline{r}$ and we have a total remainder $2xy + x + 2$. Thus we get $q_2 = -1$ and

$$f = q_1 f_1 + q_2 f_2 + \underline{r}$$
$$x^2y^3 + 2xy + x + 1 = y^3(x^2 + 1) + (-1)(y^3 + 1) + (2xy + x + 2).$$

Example 6 . *Let us divide $f = x^3y^2 - 2xy$ by $f_1 = x^3y - 2x$ and $f_2 = y^2 + 3$. We will use lex order with $y < x$. we have to change the order of the divisors.*

Our first case will be $F = \{f_1, f_2\}$. Then, by the procedure described above we obtain

$(x^3y^2 - 2xy)$	$: (x^3y - 2x)$	$= y$	$\underline{r}$
$-(x^3y^2 - 2xy)$			0

And

$$x^3y^2 - 2xy = y(x^3y - 2x) + 0(y^2 + 3) + 0.$$

If, however, we take $F = \{f_2, f_1\}$ in the second case, then we obtain

$(x^3y^2 - 2xy)$	$: (y^2 + 3)$	$= x^3$	$\underline{r}$
$-(x^3y^2 + 3x^3)$			
$(-3x^3 - 2xy)$			$2xy + x$

And

$$x^3y^2 - 2xy = x^3(y^2 + 3) + 0(x^3y - 2x) - 3x^3 - 2xy.$$

So we can see that the two cases in the example produce two different remainders, 0 and $-3x^3 - 2xy$, respectively, due to a switch in the order of polynomials in F.

This shows that the remainder r is not uniquely characterized by the requirement that none of its terms be divisible by $LT(f_i), \ldots, LT(f_s)$. And the q_i and r can change if we rearrange the f_i (may also change if we change the monomial ordering). If after division of f by $F = \{f_1, \ldots, f_s\}$ we obtain a remainder $r = 0$, then

$$f = q_1 f_1 + \ldots + q_s f_s,$$

so, that $f \in \langle f_1, \ldots, f_s \rangle$. Thus $r = 0$ is a sufficient condition for ideal membership, but is not a necessary condition for being in the ideal. we wil see the division procedure in the ring of multivariate polynomials over a field terminates even if the division term is not the leading term, but is freely chosen.
Now, introduce the support of f with respect to g

$$\begin{aligned} Supp_g(f) &= \{i \in Supp(f) \,|\, i = \deg(g) + k for some k \in \mathbb{N}_0^n\} \\ &= Supp(f) \cap (\deg(g) + \mathbb{N}_0^n) \subset \mathbb{N}_0^n \end{aligned}$$

as the set of multiindices of all monomials in f divisible by $LT(g)$. The standard algorithm described above takes for the next division step the maximal divisible term in f, which corresponds to the multiindex

$$\max Supp_g(f).$$

Clearly, r is the remainder in the division algorithm $f = gh + r \Leftrightarrow Supp_g(r) = \emptyset$. It is not obvious whether the algorithm would stop if, instead of always choosing the maximal index in the set $Supp_g(f)$, one chooses an arbitrary one. This is because after reducing f modulo g_1 and then modulo g_2, it is possible that some terms divisible by $LT(g_1)$, which were previously eliminated, reappear. Therefore, it is natural to ask whether *any* reduction process modulo a given m-tuple $(g_1, \ldots, g_m)$, with arbitrary choice of division term in each step would terminate? For a set of m polynomials $G = \{g_1, \ldots, g_m\}$ let us introduce $Supp_G(f) = Supp_g(f) \cup \ldots \cup Supp_g(f)$.

Theorem 8 *Let $f \in K[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_m\}$ a set of m polynomials, $g_i \in K[x_1, \ldots, x_n]$. Then, any reduction process (with arbitrary choice of the next reduction term in $Supp_{g_{i_j}}(f_{j-1})$)*

$$f \to_{g_{i_1}} f_1 \to_{g_{i_2}} f_2 \to \ldots$$

with $g_{i_k} \in G$ must terminate in finitely many steps. This means that there exists k such that f_k does not contain a term divisible by any of the $LT(g_1), \ldots, LT(g_m)$.

Proof. Let r_j be the index used for reduction by $g_{i_{j+1}}$ and let $m_j = \max Supp_{g_{i_{j+1}}}(f_j)$ $(j = 0, 1, 2, \ldots, f_0 := f)$.
Clearly, $r_j \in Supp_{g_{i_{j+1}}}(f_j)$ and $r_j \leq m_j$. It is easy to see that

$$m_0 \geq m_1 \geq \ldots$$

According to DCC, from some point on $m_{k_1} = m_{k_1+1} = \ldots$.
Let $m_{k_1}^{(1)} = \max[Supp_{g_{i_{k_1+1}}}(f_{k_1}) \setminus \{m_{k_1}\}] < m_{k_1}$. Clearly, $r_{k_1} \leq m_{k_1}^{(1)} < m_{k_1}$.
Repeat the process for the sequence $m_{k_1}^{(1)} \geq m_{k_1+1}^{(1)} \geq \ldots$. In this way we obtain a sequence of indices

$$m_{k_1}^{(1)} \geq m_{k_2}^{(2)} \geq \ldots .$$

Again, according to DCC, this sequence must be stationary from some point on $m_{k_p}^{(p)} = m_{k_{p+1}}^{(p+1)} = \ldots$, which means that from that point on, $Supp_{g_{i_p}}(f_{p-1}) = \emptyset$ and the reduction process terminates. $\square$
So, no matter how we choose the next term in the division algorithm (in the set of all possible terms), the algorithm will stop in finitely many steps. The polynomial f_k obtained in this way is then the remainder of the particular reduction process. As we have already noted, the remainder depends on the order in which the reductions are performed.

3.3 Ordered sets and multivariate division

The fact that in the reduction process one can arbitrarily choose the term for the next reduction in the set $Supp_G(f)$ was known to Buchberger (see [3] p. 14). However, it was not widely used and even not mentioned in the standard textbooks. Buchbergers argument in [3] involves extension of a given monomial order to a partial order on the set of all polynomials. This order seems somehow unnatural. It is not total because the coefficients are also taken into account. However, we have already seen that it is not necessary to speak about monomials and polynomials, but about underlying monomial orders on the exponent set $\mathbb{N}_0^n = (\mathbb{Z}_+^n)$ instead. When we took a closer look, we discovered more natural, underlying combinatorial fact about total orders, which actually belongs to set theory.

Lemma 4 . *Let $(X, \leq)$ be totally ordered and $A \subset X$ its nonempty finite subset. Then the minimal element $minA$ and the maximal element $maxA$ of A exist and are unique. Actually, the elements in A are ordered in a unique way.*

As we know ordered set $(X, \leq)$ is well-ordered if every nonempty subset has a least element. A well-ordered set is totally ordered. We now come to the settheoretic essence of the division algorithm in the multivariate polynomial ring, Buchbergers polynomial order and Buchbergers proof.

Let $(X, \leq)$ be a well-ordered set and F the family of all its (nonempty) finite subsets. Consider the following binary relation on F :

$$A < B \Leftrightarrow max(A\Delta B) \in B$$

. Here, $A\Delta B = (A \setminus B) \cup (B \setminus A)$ is a common symmetric difference of the two sets. It is easy to see that this definition is equivalent to the following : $A < B \Leftrightarrow$ there exists $b \in B \setminus A$ such that the strict upper intervals $A_{>_b}$ and $B_{>_b}$ are either empty Here, $A_{>_b} = \{x \in A | x > b\}$ is the upper interval of b in A. Clearly, such element must be unique.

Theorem 9 . *With respect to this (strict) order $<$, the set F is well-ordered.*

Proof.
(1) It is easy to see that this is an order on F. Reflexivity is obtained in the usual way by reflexive completion of the given strict order $A \leq B \Leftrightarrow (A < B) \vee (A = B)$. Antisymmetry is obvious, since $A < B$ and $B < A$ leads to a contradiction. Now, let $A < B$ and $B < C$, and let $b = max(A\Delta B) \in B$ and $c = max(B\Delta C) \in C$. Then $c \notin B$ and therefore $c \neq b$. There are two possibilities:
either $b < c$ or $b > c$. In the first case, $c \notin A$ and $max(A\Delta C) = c$. In the second case, $b \in C$ and $max(A\Delta C) = b$. This proves transitivity. This is a total order since the maximal element in $A\Delta B \neq \phi$ has to be either in A or in B.
(2) Now, let us prove that this is a well-order i.e. it satisfies the (DCC) condition. Let

$$A_1 > A_2 > \cdots > A_n > \cdots$$

be a strictly descending chain in F. For $n \in \mathbb{N}$, define two sequences in X,

$$a_n = max(A_n \setminus A_{n+1}) \in A_n$$

and

$$p_n = max\{a_1, \cdots, a_n\}.$$

The last sequence is actually an ascending chain

$$p_1 \leq p_2 \leq \cdots \leq p_n \leq \cdots$$

Now notice that if there is a strict jump in the sequence i.e. if $p_n > p_{n-1}$, then $p_n = a_n \in A_i$ for all $i \leq n$. But A_1 is finite, so the number of

strict jumps is also finite, and the chain must be stationary. Let $p^{(1)}$ be its stationary value :

$$p_m = p_{m+1} = \cdots = p^{(1)},$$

which means that from that point on all subsets $A_{m+i} \cap \left\{x \in X | x \geq p^{(1)}\right\} = S \subset A_{m+i}$ coincide for all $i \geq 1$. The following easy fact will be used without proof.

Lemma 5 . (*"cut − off"*). *Let $A < B$, $max(A \Delta B) = b \in B \setminus A$ and let $S \subset A \cap B$. Denote $A^{(1)} = A \setminus S$ and $B^{(1)} = B \setminus S$. Then $A^{(1)} < B^{(1)}$ and $max\left(A^{(1)} \Delta B^{(1)}\right) = b$.*

Let $A_i^{(1)} = A_{m+i} \cap \left\{x \in X | x < p^{(1)}\right\} \subset A_{m+i}$ (we (*"cut − off"*) the set S i.e. all elements in the original chain which are $\geq p^{(1)}$). If $A_1^{(1)} \neq \phi$, then $A_i^{(1)}$ also form a strictly descending chain of finite sets

$$A_1^{(1)} > A_2^{(1)} > \cdots > A_n^{(1)} > \cdots$$

such that all corresponding maxima coincide: $a_i^{(1)} = a_{m+i}$. Now apply the same construction to this chain and obtain the stationary value $p^{(2)} < p^{(1)}$. In this way, we obtain a strictly descending chain

$$p^{(1)} > p^{(2)} > \cdots > p^{(k)}$$

in X which eventually must stop since X is well-ordered. This means that at this point $A_1^{(k)} = \phi$, the construction can not be continued and the original sequence must be finite. This proves the theorem. □
If we now apply this theorem to the sequence of finite sets of exponents of polynomials in the division algorithm, we obtain the previous theorem:
the fact that in the reduction process one can arbitrarily choose the term for the next reduction in the set $Supp_G(f)$. This leads to a conclusion that for certain special classes of polynomials one could try to find heuristics which could improve the calculation speed of Gröbner basis. This remark could open a quite new and broad area of research.

3.4 Monomial ideals and Hilbert basis theorem

In this section we will study the properties of monomial ideals, and we will see formally why divisibility is so important for finding an element of an ideal.

Definition 18 . *A monomial ideal is an ideal generated by a set of monomials. That is, I is a monomial ideal, if there is a subset $A \subset \mathbb{N}_0^n$ such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in K[x_1, \ldots, x_n]$. We write*

$$I = \langle x^\alpha | \alpha \in A \rangle$$

.

For example $I = \left\langle x^2y, xy^4, x^5y^3 \right\rangle \in K[x, y]$ is a monomial ideal with corresponding set $A = \{(2, 1), (1, 4), (5, 3)\}$. The least common multiple of two monomials x^α and x^β, $\alpha, \beta \in \mathbb{N}_0^n$ is:

$$LCM(x^\alpha, x^\beta) = x_1^{max(\alpha_1,\beta_1)} \ldots x_n^{max(\alpha_n,\beta_n)}$$

and their greatest common divisor is:

$$GCD(x^\alpha, x^\beta) = x_1^{min(\alpha_1,\beta_1)} \ldots x_n^{min(\alpha_n,\beta_n)}$$

Monomial ideals are easier to manipulate than arbitrary ideals. Consider, for instance, the ideal membership problem: If $I \subset K[x_1, \cdots, x_n]$ is a monomial ideal, given by monomial generators $m_1, \cdots, m_s$, a term is contained in I iff it is divisible by at least one of the m_i, an arbitrary polynomial $f \in K[x_1, \cdots, x_n]$ is contained in I iff all its terms are contained in I.

Lemma 6 *([7] ,p 70). Let $I = \langle x^\alpha | \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof. ($\Leftarrow$) Assume x^β is a multiple of x^α for some $\alpha \in A$. Then by the definition of an ideal it follows that $x^\beta \in I$.
($\Rightarrow$) Assume $x^\beta \in I$, and by the definition, $x^\beta = \sum_{i=1}^s h_i x^{\alpha_i}$ where $h_i \in K[x_1, \ldots, x_n]$ and $\alpha_i \in A$. Then we can write h_i as a linear combination of monomials as follows,

$$h_i = a_{p_i} x^{p_i} + a_{(p-1)_i} x^{(p-1)_i} + \ldots + a_{0_i}.$$

And

$$h_i x^{\alpha_i} = a_{p_i} x^{p_i+\alpha_i} + a_{(p-1)_i} x^{(p-1)_i+\alpha_i} + \ldots + a_{0_i} x^{\alpha_i}.$$

Thus we can see that every term of $\sum_{i=1}^s h_i x^{\alpha_i}$ must be divisible by some x^{α_i}. Since the sum of these terms is the monomial x^β, then each term must be divisible by same x^{α_i}. So x^β must also be divisible by some x^{α_i}. $\square$
The next lemma describes how we can characterize a polynomial that is in a given monomial ideal.

Lemma 7 *([7] p. 71). Let I be a monomial ideal, and let $f \in K[x_1, \ldots, x_n]$. Then the following are equivalet:*

1. *$f \in I$.*
2. *Every term of f lies in I.*
3. *f is a k-linear combination of the monomials in I.*

Proof. ($3 \Rightarrow 2$) Let f is a k-linear combination of the monomials *in* I. Then every term of f is a multiple of an element of I. Thus by definition, each term of f is in I. Since I is closed under addition, it follows that the sum of these terms f is also in I.
($2 \Rightarrow 1$) Assume every term of f lies in I. Then $f \in I$. since I is closed under addition.
($1 \Rightarrow 3$) Let $f \in I$ and suppose $I = \langle x^\alpha | \alpha \in A \rangle$. Then by definition, $f = \sum_{i=1}^{s} h_i x^{\alpha_i}$ where $h_i \in K[x_1, \ldots, x_n]$ and $\alpha_i \in A$. Let

$$h_i = a_{0_i} x^{m(i)} + a_{1_i} x^{m-1(i)} + \ldots + a_{m_i}.$$

Then

$$h_i x^{\alpha(i)} = a_{0_i} x^{q_i} x^{\alpha_i} + a_{1_i} x^{(q-1)_i} x^{\alpha_i} + \ldots + a_{q_i} x^{\alpha_i}.$$

Which means the terms of f are linear combinations of monomials x^{α_i} in I.
□
Now we can prove that any monomial ideal has a finite basis, by using the previous two lemmas, which will be the first step to show that every ideal has a finite generating set.

Lemma 8 . *(Dicksons Lemma) Let $I = \langle x^\alpha | \alpha \in A \rangle \subset k[x_1, \ldots, x_n]$ be a monomial ideal. Then I can be written in the form $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, where $\alpha_1, \ldots, \alpha_s \in A$. In particular, I has a finite basis*

For details of the proof, (see [7] p. 71-72).
Now we will use this fact to show that every ideal has a finite generating set. To do this, we have to introduce a monomial ideal that is generated by the leading terms of each polynomial in the ideal. Once we have a monomial ordering, each $f \in k[x_1, \ldots, x_n]$ has a unique leading term denoted $LT(f)$ and these leading terms generate a monomial ideal.

Definition 19 . *Let $I \subset k[x_1, \ldots, x_n]$ be a nonzero ideal.*

- *Let $LT(I)$ be the set of leading terms of I.*

$$LT(I) = \{ax^{\alpha} | there\ exists f \in I with LT(f) = ax^{\alpha}\}$$

- *We denote by $\langle LT(I)\rangle$ the ideal generated by the elements of $LT(I)$.*

So for example $\langle LT(I)\rangle$ is a monomial ideal. As we will see the ideals $\langle LT(I)\rangle$ and $\langle LT(g_1), \ldots, LT(g_s)\rangle$ where $g_1, \ldots, g_s$ are a finite generating set for I, are not always the same. Though we always have $\langle LT(g_1), \ldots, LT(g_s)\rangle \subset \langle LT(I)\rangle$, but the opposite does not hold. The following example explains this.

Example 7 . *Consider $I = \left\langle x^2 + 1, xy\right\rangle$ by use the lex ordering with $y < x$. Then $LT(x^2 + 1) = x^2$ and $LT(xy) = xy$. So, $\left\langle LT(x^2 + 1), LT(xy)\right\rangle = \left\langle x^2, xy\right\rangle$. Since,*

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

we know $y \in I$ and so $LT(y) \in \langle LT(I)\rangle$. However, $LT(y) = y \notin \left\langle x^2, xy\right\rangle$, since is not divisible by $LT(x^2 + 1)$ or $LT(xy)$. Therefor

$$\langle LT(I)\rangle \neq \left\langle LT(x^2 + 1), LT(xy)\right\rangle.$$

The next proposition will show that there is a set of polynomials in the ideal I for which they are the same.

Proposition 7 *([7] .p 76). Let $I \subset K[x_1, \ldots, x_n]$ be an ideal then:*

1. *$\langle LT(I)\rangle$ is a monomial ideal.*

2. *There are $g_1, \ldots, g_t \in I$ such that $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.*

Proof. Let $I \subset K[x_1, \ldots, x_n]$ be an ideal. We have to show that the above two Properties hold.
1. We know that the $LM(g)$ of elements $g \in I - \{0\}$ generate the monomial ideal $\langle LM(g) | g \in I - \{0\}\rangle$. Let $x^{\alpha_i} \in \langle LM(g) | g \in I - \{0\}\rangle$ be the leading monomial of g_i and a_{α_i} the leading coefficient of g_i. Then $a_{\alpha_i}.x^{\alpha_i} \in \langle LM(g) | g \in I - \{0\}\rangle$.
Let start with $a_{\alpha_j} g_j \in \langle LT(g) | g \in I - \{0\}\rangle$. Then $a_{\alpha_j}^{-1} \in K$, since K is a feild. So $a_{\alpha_j}^{-1}.a_{\alpha_j} g_j = g_j \in \langle LM(g) | g \in I - \{0\}\rangle$. Thus

$$\langle LM(g) | g \in I - \{0\}\rangle = \langle LT(g) | g \in I - \{0\}\rangle = \langle LT(I)\rangle$$

Therefore $\langle LT(I)\rangle$ is a monomial ideal.
2. By using Dicksons Lemma, then We have the monomial ideal $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$ for finitely many generated $g_1, \ldots, g_t \in I$. $\square$
The set of monomials $g_1, \ldots, g_t$ in the above proposition such that $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$ are in fact a finite generating set for ideal I and it is known as Gröbner basis, as we will see in the next chapter. We will fix a monomial ordering to use in the division algorithm and in computing leading terms.

Theorem 10 *(Hilbert Basis Theorem). Every ideal $I \subset K[x_1, \ldots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \ldots, g_t\rangle$ for some $g_1, \ldots, g_t \in I$.*

Proof.([7] p. 76) If $I = 0$, then our generating set is 0, which is finite. If I contains some nonzero polynomial, then by proposition (7), there are $g_1, \ldots, g_t \in I$ such that $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.
We want to show $I = \langle g_1, \ldots, g_t\rangle$.
($\supseteq$) $\langle g_1, \ldots, g_t\rangle \subset I$, because each $g_i \in I$.
($\subseteq$) Let $f \in I$ be any polynomial. By using the division algorithm we divide f by $\langle g_1, \ldots, g_t\rangle$, then we get an expression of the form

$$f = q_1 g_1 + \ldots + q_t g_t + r.$$

Where every term in r is not divisible by any $LT(g_i), \ldots, LT(g_t)$. We have to show that $r = 0$. Note that

$$r = f - q_1 g_1 - \ldots - q_t g_t \in I.$$

So, since $r \in I$, then $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Then by lemma(6) $LT(r)$ must be divisible by some $LT(g_i)$. But, except $r = 0$, this is contradiction which means that for r to be a remainder by the division algorithm. Thus,

$$f = q_1 g_1 + \ldots + q_t g_t + 0 \in \langle g_1, \ldots, g_t\rangle,$$

and so $f \in I$. Then $I \subset \langle g_1, \ldots, g_t\rangle$. $\square$

Corollary 2 . *If I_k are ideals, for $k \geq 1$ of $K[x_1, \ldots, x_n]$ with $I_1 \subset I_2 \subset I_3 \subset \cdots$ then there exist m such that $I_m = I_{m+1} = I_{m+2} = \ldots$*

The proof follow form Hilberts basis theorem.

3.5 The original proof of Hilbert basis theorem

Before we start with the details of the original Hilbert's proof, let us quickly review the historical development leading to the concept of Gröbner bases. In his paper of (1890) D. Hilbert [10] gave a proof of his famous Basis Theorem as well as of the structure and length of the sequence of syzygy modules of a polynomial system. Implicitly he also showed that the Hauptproblem (the main problem of the theory of polynomial ideals, according to B.L. van der Waerden), i.e. the problem whether $f \in I$ for a given polynomial f and polynomial ideal I, can be solved effectively. Hilberts solution of the Hauptproblem (and similar problems) was reinvestigated by G. Hermann [14] in (1926). She counted the field operations required in this effective procedure and arrived at a double exponential upper bound in the number of variables. In fact, Hermanns, or for that matter Hilberts, algorithm always actually achieves this worst case double exponential complexity. The next important step came when B. Buchberger, in his doctoral thesis [2] of (1965) advised by W. Gröbner, introduced the notion of a Gröbner basis (he did not call it this at that time) and also gave an algorithm for computing it. Gröbner bases are very special and useful bases for polynomial ideals. In subsequent publications Buchberger exhibited important additional applications of his Gröbner bases method, e.g. to the solution of systems of polynomial equations. In the worst case, Buchbergers Gröbner bases algorithm is also double exponential in the number of variables, but in practice there are many interesting examples which can be solved in reasonable time. But still, in the worst case, the double exponential behaviour is not avoided. And, in fact, it cannot be avoided by any algorithm capable of solving the Hauptproblem, as was shown by E.W. Mayr and A.R. Meyer in [11] (1982). When we are solving systems of polynomial (algebraic) equations such as, $f_1(x_1, \ldots, x_n) = \ldots = f_m(x_1, \ldots, x_n) = 0$,the important parameters are the number of variables n and the degree d of the polynomials $f_1, \ldots, f_m$. The Buchberger algorithm for constructing Gröbner bases is at the same time a generalization of Euclids algorithm for computing the greatest common divisor (GCD) of univariate polynomials (the case n = 1) and of Gauss triangularization algorithm for linear systems (the case d = 1). Both these algorithms are concerned with solving systems of polynomial equations, and they determine a canonical basis (either the GCD of the inputs or a triangularized form of the system) for the given polynomial system. Buchbergers algorithm can be seen as a generalization to the case of arbitrary n and d. Let us reproduce Hilbert's proof from [10].

Theorem 11 . *Let $F_1, F_2, F_3, \ldots,$ be an infinite series of forms of n variable $x_1, \ldots, x_n$. Then there are always a number m such that each form of that series can be expressed in the form :*

$$F = A_1F_1 + A_2F_2 + \ldots + A_mF_m,$$

where $A_1, \ldots, A_m$ are suitable forms of the same n variables.

Proof. Let $F_1, F_2, F_3, \ldots$ are the given number of forms of n variables $x_1, \ldots, x_n$. And let $F_1 \neq 0$, $deg(F_1) = r$. Then we determine first a liner change of the variables which has a nonzero determinant

$$y = A.x,$$

so, that the form F_1 transforms in a form G_1 of the variables $y_1, \ldots, y_n$, and the coefficient of y_n^r in the form G_1 is different from zero. By using this linear substitution, forms $F_2, F_3, \ldots$ respectively transform in $G_2, G_3, \ldots$. Now we consider the relation of the form

$$G_s = B_1G_1 + B_2G_2 + \ldots + B_mG_m,$$

where s is any index and $B_1, B_2, \ldots, B_m$ are forms of the variable $y_1, \ldots, y_n$, it will transform by using inverse linear change in a relation of the form

$$F_s = A_1F_1 + A_2F_2 + \ldots + A_mF_m,$$

where $A_1, \ldots, A_m$ are forms of the original variables $x_1, \ldots, x_n$.
Since the coefficient $y_n^r \neq 0$ in G_1, then the degree of each forms G_s of the given series with respect to the variable y_n is less than r. That multiplies G_1 with a suitable form B_s, and the obtained product is subtracted from G_s, for any $s = 1, 2, \ldots$

$$G_s = B_s.G_1 + g_{s1}y_n^{r-1} + g_{s2}y_n^{r-2} + \ldots + g_{sr},$$

where B_s is a form in n variables $y_1, \ldots, y_n$, while the forms $g_{s1}, \ldots, g_{sr}$ in the $n-1$ variables $y_1, \ldots, y_{n-1}$.
Now, we assume that our theorem for series of forms with $n-1$ variables is true, and apply the same to the first series of $g_{11}, g_{21}, g_{31}, \ldots$. Then there is a number μ, of the type that for each value of s,

$$g_{s1} = b_{s1}g_{11} + b_{s2}g_{21} + \ldots + b_{s\mu}g_{\mu 1} = l_s(g_{11}, g_{21}, \ldots, g_{\mu 1}).$$

Where $b_{s1}, b_{s2}, \ldots, b_{s\mu}$ are forms in $n-1$ variables $y_1, \ldots, y_{n-1}$.
Now we take the form

$$g_{st}^{(1)} = g_{st} - l_s\left(g_{1t}, g_{2t}, \ldots, g_{\mu t}\right) t = (1, 2, \ldots, r), \tag{3.1}$$

resulting in particular for $t = 1$ with

$$g_{s1}^{(1)} = 0$$

Apply the theorem for the first sequence, $g_{12}^{(1)}, g_{22}^{(1)}, g_{32}^{(1)}, \ldots$
According to this theorem, there is a number $\mu^{(1)}$ such that for each value of s there is a relation of the form

$$g_{s2}^{(1)} = b_{s1}^{(1)} g_{12}^{(1)} + b_{s2}^{(1)} g_{22}^{(1)} + \ldots + b_{s\mu^{(1)}}^{(1)} g_{\mu^{(1)}2}^{(1)} = l_s^{(1)}\left(g_{12}^{(1)}, g_{22}^{(1)}, \ldots, g_{\mu^{(1)}2}^{(1)}\right),$$

where $b_{s1}^{(1)}, b_{s2}^{(1)}, \ldots, b_{s\mu^{(1)}}^{(1)}$ are forms in $n-1$ variables $y_1, \ldots, y_{n-1}$. Now we take the form

$$g_{st}^{(2)} = g_{st}^{(1)} - l_s^{(1)}\left(g_{1t}^{(1)}, g_{2t}^{(1)}, \ldots, g_{\mu^{(1)}t}^{(1)}\right) t = (1, 2, \ldots, r). \tag{3.2}$$

The result for $t = 1, 2$ gives

$$g_{s1}^{(2)} = 0, g_{s2}^{(2)} = 0$$

Applying the theorem for the formal series $g_{13}^{(2)}, g_{23}^{(2)}, g_{33}^{(2)}, \ldots$, we have the relation

$$g_{s3}^{(2)} = l_s^{(2)}\left(g_{13}^{(2)}, g_{23}^{(2)}, \ldots, g_{\mu^{(2)}3}^{(2)}\right),$$

then we set

$$g_{st}^{(3)} = g_{st}^{21)} - l_s^{(2)}\left(g_{1t}^{(2)}, g_{2t}^{(2)}, \ldots, g_{\mu^{(2)}t}^{(2)}\right) t = (1, 2, \ldots, r). \tag{3.3}$$

Then it follows

$$g_{s1}^{(3)} = 0, g_{s2}^{(3)} = 0, g_{s3}^{(3)} = 0,$$

and after repeated application of this procedure, one obtains the relation

$$g_{st}^{(r-1)} = g_{st}^{r-2)} - l_s^{(r-2)}\left(g_{1t}^{(r-2)}, g_{2t}^{(r-2)}, \ldots, g_{\mu^{(r-2)}t}^{(r-2)}\right) t = (1, 2, \ldots, r), \tag{3.4}$$

and

$$g_{s1}^{(r-1)} = 0, g_{s2}^{(r-1)} = 0, \ldots, g_{s(r-1)}^{(r-1)} = 0.$$

Finally we obtain

$$g_{sr}^{(r-1)} = l_s^{(r-1)}\left(g_{1r}^{(r-1)}, g_{2r}^{(r-1)}, \ldots, g_{\mu^{(r-1)}r}^{(r-1)}\right),$$

so that

$$0 = g_{st}^{(r-1)} - l_s^{(r-1)}\left(g_{1t}^{(r-1)}, g_{2t}^{(r-1)}, \ldots, g_{\mu^{(r-1)}t}^{(r-1)}\right) t = (1, 2, \ldots, r). \qquad (3.5)$$

By adding the equations $(2.1), (2.2), (2.3), \ldots, (2.4), (2.5)$ we get
$g_{st} = l_s\left(g_{1t}, g_{2t}, \ldots, g_{\mu t}\right) + l_s^{(1)}\left(g_{1t}^{(1)}, g_{2t}^{(1)}, \ldots, g_{\mu^{(1)}t}^{(1)}\right) + \ldots$
$+ l_s^{(r-1)}\left(g_{1t}^{(r-1)}, g_{2t}^{(r-1)}, \ldots, g_{\mu^{(r-1)}t}^{(r-1)}\right)\ t = (1, 2, \ldots, r).$
On the right hand side of this formula, we can replace forms

$$g_{1t}^{(1)}, g_{2t}^{(1)}, \ldots, g_{\mu^{(1)}t}^{(1)}, \ldots, g_{1t}^{(r-1)}, g_{2t}^{(r-1)}, \ldots, g_{\mu^{(r-1)}t}^{(r-1)}.$$

As a result of repeated application of above equations by linear combinations of the form $g_{1t}, g_{2t}, \ldots, g_{mt}$, where $m = max(\mu, \mu^{(1)}, \ldots, \mu^{(r-1)})$, we get a system of equations of the form

$$g_{st} = c_{s1}g_{1t} + c_{s2}g_{2t} + \ldots + c_{sm}g_{mt} = k_s(g_{1t}, g_{2t}, \ldots, g_{mt})t = (1, 2, \ldots, r),$$

where $c_{s1}, c_{s2}, \ldots, c_{sm}$ again are forms in $n-1$ variables $y_1, \ldots, y_{n-1}$. If we multiply the last formula by y_n^{r-t} and add equations for $t = 1, 2, \ldots, r$ then

$$\begin{aligned}
G_s - B_sG_1 &= k_s(g_{11}, \ldots, g_{m1}).y_n^{r-1} + \ldots + k_s(g_{1r}, \ldots, g_{mr}).1 \\
&= \sum_{i=1}^{r} k_s(g_{1i}, \ldots, g_{mi}).y_n^{r-i} \\
&= \sum_{i=1}^{r}\left(\sum_{j=1}^{m} c_{sj}g_{ji}\right).y_n^{r-i} \\
&= \sum_{j=1}^{m}\sum_{i=1}^{r} c_{sj}g_{ji}y_n^{r-i} \\
&= \sum_{j=1}^{m} c_{sj}\sum_{i=1}^{r} g_{ji}y_n^{r-i} \\
&= \sum_{j=1}^{m} c_{sj}(G_j - B_jG_1) \\
&= k_s\left(G_1 - B_1G_1, G_2 - B_2G_1, \ldots, G_m - B_mG_1\right).
\end{aligned}$$

Or, if G_s denotes a form of n variables $y_1, \ldots, y_n$

$$\begin{aligned} G_s &= B_s G_1 + [c_{s1}(G_1 - B_1 G_1) + c_{s2}(G_2 - B_2 G_1) + \ldots + c_{sm}(G_m - B_m G_1) \\ &= (B_s + c_{s1} - c_{s1}B_1 - c_{s2}B_2 - \ldots - c_{sm}B_m)G_1 + c_{s2}G_2 + \ldots + c_{sm}G_m \\ &= l_s(G_1, G_2, \ldots, G_m) \end{aligned}$$

It is a constructive proof and not an existence proof, that means it gives an algorithm for how to find the expression. $\square$

CHAPTER 4

GRÖBNER BASIS

As we have seen, in general we do not obtain a uniquely determined remainder from the division algorithm. However, the subsequent definition of a Gröbner basis will have the quality that the division of f by G yields the same remainder, no matter how the elements of G are ordered in the division. Since we will show that every ideal I has a Gröbner basis, we are able to resolve the ideal membership problem with a necessary and sufficient condition for a polynomial f to be a member of an ideal I, namely that division of f by the Gröbner basis of I returns a remainder of 0.

4.1 Gröbner basis and Buchberger's algorithm

Definition 20 . *Let a monomial ordering on $K[x_1, \ldots, x_n]$ be fixed. A finite subset $G = \{g_1, \ldots, g_s\}$ of an ideal I is said to be a Gröbner basis of the ideal I if*

$$\langle LT(g_1), \ldots, LT(g_s)\rangle = \langle LT(I)\rangle .$$

As a corollary to the Hilbert Basis Theorem applied to $\langle LT(I)\rangle$ we have:

Corollary 3 *([7].p 77). Fix a monomial order $>$ on $K[x_1, \ldots, x_n]$, and let I be a non zero polynomial ideal. Then I has a Gröbner basis. Furthermore, any Gröbner basis of I is a basis of I.*

Proof. Let I be a nonzero ideal. Then the set $G = \{g_1, \cdots, g_s\}$ constructed in the proof of Hilbert Basis Theorem is a Gröbner basis by definition, and then every ideal has a Gröbner basis. For a Gröbner basis G note that if

$$\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle,$$

and so $I = \langle g_1, \cdots, g_s\rangle$ by the proof of Hilbert Basis Theorem. Therefore G is a basis for I. $\square$
Gröbner bases give some very useful algebraic results. Here is the first important result:

Corollary 4 . *let $I \subset K[x_1, \ldots, x_n]$ be a non zero polynomial ideal.*

1. *The ideal I has a Gröbner basis.*
2. *A Gröbner basis $G = \{g_1, \cdots, g_s\}$ of I generates I (as an ideal):*

$$\langle g_1, \cdots, g_s\rangle = I.$$

3. *If G is a Gröbner basis for I, then division by $g_1, \cdots, g_s$ leaves a uniqe remainder r independent of the order of the g_i. In fact, r is characterized as the unique polynomial such that.*
   (a) *$r = 0$ or no term of r is divisible by any of the leading terms of the $g_i (i = 1, \cdots, s)$.*
   (b) *$f - r \in I$ for $f \in G$.*

In a given Gröbner basis there may be elements of additional elements. For example, if $G = \{g_1, \cdots, g_s\}$ is a Gröbner basis for I and for $f \in G$ if $LT(f)$ is also contaoned in the ideal $\langle LT(G - \{f\})\rangle$, then $G - \{f\}$ is also a Gröbner basis for I. Given the definition of Gröbner basis, this is almost a trivality: Since $LT(f) \in \langle LT(G - \{f\})\rangle$, we find $\langle LT(G - \{f\})\rangle = \langle LT(G)\rangle = \langle LT(I)\rangle$. The resulting equality of the first and third term imply that $G - \{f\}$ is also a Gröbner basis.
The following definitions are intended to produce unique Gröbner bases in some sense.

Definition 21 . *A minimal Gröbner basis for an ideal is a Gröbner basis G for I satisfying:*

1. $LC(f) = 1$ *for all* $f \in G$;

2. $LT(f) \notin \langle LT(G - \{f\})\rangle$ *for all* $f \in G$.

A reduced Gröbner basis for an ideal I satisfies (1.) and the following condition which is stronger than (2):
No nonzero term of f is in $\langle LT(G - \{f\})\rangle$ for all $f \in G$.

Theorem 12 . *Every nonzero ideal* $I \subset K[x_1, \ldots, x_n]$ *has a unique reduced Gröbner basis (for a given monomial ordering).*

For the proof (see [7], [24]).
Once reduced Gröbner basis can be effectively computed, one has a method to decide whether two ideals are equal (they are equal if and only if they have the same reduced Gröbner basis).
As we have seen previously, the corollary (3) proves the existence of a Gröbner basis, its proof is not constructive and offers us little insight as to how to actually obtain one. We would like to obtain a generating set such that all that leading terms of the polynomials in the set generate the leading terms of the ideal I. This fails when there is a cancellation of leading terms of the kind in the previous example. To better determine when this cancellation occurs, Buchberger constructed a special polynomial that produces new leading terms.

Definition 22 . *Let* $f, g \in K\ [x_1, \ldots, x_n]$ *be nonzero polynomials of multidegree* α *and* β*, respectively, we define their S-polynomial as the polynomial*

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

where the monomial $x^\gamma = LCM(LT(f), LT(g))$.
Note that (S stands for "syzygy", from Latin syzygia "conjunction", or Greek $\sigma\zeta\upsilon\gamma o\varsigma$ *- syzygos, "yoked together")*

Example 8 . *Let* $f = x^3yz + xy^2z + x$ *and* $g = 2x^2y^2z + xy + xz$ *in* $\mathbb{Q}[x, y, z]$ *are ordered with respect to the lex order with* $x > y$. *Then* $\gamma = (3, 2, 1)$ *and we have:*

$$S(f, g) = \frac{x^3y^2z}{x^3yz} f - \frac{x^3y^2z}{2x^2y^2z} g = yf - \frac{1}{2}xg = -\frac{1}{2}x^2y - \frac{1}{2}x^2z + x^3yz + xy.$$

Notice that the cancellation of the leading terms according to the construction of the S-polynomial. Once a basis contains all the possible S-polynomials of polynomials in the ideal generating set, there are no extra polynomials in $\langle LT(I)\rangle$ that are not in $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$. This leads to the very important criterion.

Definition 23 *We write f^G for the remainder in the division of f by the (ordered) list of polynomials $G = \{g_1, \ldots, g_j\}$.*

Theorem 13 *(Buchberger's criterion). Let I be a polynomial ideal. Then a basis $G = \{g_1, \cdots, g_s\}$ for I is a Gröbner basis for I if and only if for all pairs $i \neq j$, we have*

$$S(f, g)^G = 0$$

(See [7] p.40-42 or [24] p.85-87)

Theorem 14 *(Buchberger's Algorithm). Let $I = \langle f_1, \ldots, f_s\rangle \neq (0)$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps.*

4.2 Computing Gröbner bases

The theory mentioned above formulates the algorithm criterion for computing Gröbner bases. And the next algorithm is the original algorithm presented by Buchberger in his PH.D.dissertation [2].
Algorithm:
Given: let the set $\{g_1, \cdots, g_s\}$ generating the ideal $I \subset K[x_1, \cdots, x_n]$ and a fixed monomial order $<$.
We compute: Gröbner basis of I with respect to $<$.

1. Take $G_0 = \{g_1, \cdots, g_s\}$, for $i := 0$.
2. If for all $f, g \in G_i$, with $S(f, g)^{G_i} = 0$ then G_i is a Gröbner basis and we will stop.
3. If there are $f, g \in G_i$ and $h := S(f, g)^{G_i} \neq 0$ then we take $G_{i+1} := G_i \cup \{h\}$, $i := i + 1$ and back to (2).

Proposition 8 . *This algorithm will terminates correctly*

Proof. When the algorithm terminates then G_i will be a Gröbner basis for I because:

- $G_i \subset I$ it generates I as it contains $g_1, \cdots, g_s$.
- According to the Theorem (13) then G_i is a Gröbner basis of the ideal it generates.

Now for termination consider the the ideals $J_i = \langle LM(g) | g \in G_i \rangle$. We claim that $G_i \subset G_{i+1} \Rightarrow J_i \subset J_{i+1}$. Actually $G_{i+1} = G_i \cup \{h\}$ and $LM(h)$ is not divisible by any $LM(g)$ for $g \in G_i$. Hence $LM(h) \notin J_i$ (Lemma 6). But $LM(h) \in J_{i+1}$ so $J_i \subset J_{i+1}$.
By Corollary (2), the algorithm must terminate. $\square$

Example 9 . *Let* $I = \langle f_1 = xyz - x, f_2 = x^2y - yz \rangle$ *with the deglex order with* $z < y < x$.
Let $G_0 = \{f_1, f_2\}$. *Since* $S(f_1, f_2) = xf_1 - zf_2 = -x^2y + yz^2$ *and* $S(f_1, f_2)^{G_0} = yz^2 - yz \neq 0$, *so we add* $f_3 := S(f_1, f_2)^{G_0} = yz^2 - yz$ *to* G_0 *as a new generator. And set*

$$G_1 = \{f_1, f_2, f_3\}.$$

Next compute
$S(f_1, f_3) = zf_1 - xf_3 = 0$, *and we get* $S(f_1, f_3)^{G_1} = 0$
$S(f_2, f_3) = z^2f_2 - x^2f_3 = x^2yz - yz^3$, *and we get* $S(f_2, f_3)^{G_1} = 0$
We have $S(f_i, f_j)^{G_1} = 0$ *for all* $1 \leq i \leq j \leq 3$. *By Buchberger's criterion, it follows that* $G_1 = \{f_1, f_2, f_3\} = \{xyz - x, x^2y - yz, yz^2 - yz\}$ *is a Gröbner basis for* I.

The Gröbner basis is determined by choice of a term order. C. Kollreider, in [5] (1978) showed the importance of the choice of the term order in the reduction process and influence at the complexity of the Buchberger's algorithm. First we have to select it, after that we can apply Buchberger's algorithm to obtain a Gröbner basis in that term order. Here are some examples of computing the Gröbner basis of an ideal with respect to different monomial orders.
Term orders that are close to one another will produces the same Gröbner basis.

Example 10 . *Let* $I = \langle x^2 + xy^2, x^2 - y^3, y^3 - y^2 \rangle$. *First, let* $<_{lex}$ *be the lexicographic order with* $y < x$ *as our term order. By using Buchberger's algorithm as follows:*
We have $G = \{x^2 + xy^2, x^2 - y^3, y^3 - y^2, xy^2 + y^2\}$. *Since* $S(g_1, g_2) = xy^2 + y^3$ *and* $S(g_1, g_2)^G = xy^2 + y^2 \neq 0$, *we add it to* G *as a new generator. Then we get* $G = \{x^2 + xy^2, x^2 - y^3, y^3 - y^2, xy^2 + y^2\}$. *Computing all S-polynomials we obtain* $S(g_i, g_j)^G = 0$, *for all* $1 \leq i \leq j \leq 4$.
We get a Gröbner basis for I, $G = \{x^2 + xy^2, x^2 - y^3, y^3 - y^2, xy^2 + y^2\}$ *in one step. Second, let* $<_{grlex}$ *be the graded lexicographic order. For the same* I *by using Buchberger's algorithm we get a different Gröbner basis* $G = \{xy^2 + x^2, -y^3 + x^2, y^3 - y^2, x^3 + x^2y, x^2y + xy^2, -x^2 + y^2\}$ *in three steps.*

Example 11 . *Let* $I = \langle xy + y^2, x^2y + xy^2 + x^2 \rangle$, *then the Gröbner basis of* I *with respect to the lex order with* $y < x$ *is* $G = \{xy + y^2, -x^2, -y^3\}$, *but the Gröbner bases with respect to the lex order with* $x < y$ *is* $G = \{y^2 + xy, -x^2\}$.

Note that we underline the leading terms of polynomials in I with respect to the term order $<$.

Example 12 . *Let* $I = \langle \underline{xy^3} - x^2, \underline{x^3y^2} - y \rangle$ *and let us use* 2^- *as our term order. We can use Buchberger's algorithm to calculate a Gröbner basis for* I.
Let $G = \{g_1 = xy^3 - x^2, g_2 = x^3y^2 - y\}$. *Since* $S(g_1, g_2) = -x^4 + y^2$ *and* $S(g_1, g_2)^G = -x^4 + y^2 \neq 0$, *we add* $S(g_1, g_2)^G$ *to* G *as new generator*

$$g_3 := \underline{-x^4} + y^2.$$

Now set $G = \{g_1, g_2, g_3\}$. *Computing S-polynomial we obtain:*
$S(g_1, g_3) = y^5 - x^5$ *and* $S(g_1, g_3)^G \neq 0$. *We must add* $g_4 = \underline{y^5} - x^5$ *to our generating set, letting* $G = \{g_1, g_2, g_3, g_4\}$.
Compute $S(g_1, g_2)^G = S(g_1, g_3)^G = 0$, *and* $S(g_2, g_3) = y^4 - xy$, $S(g_2, g_3)^G \neq 0$. *Then we add* $g_5 := \underline{y^4} - xy$ *to* G. *Letting*

$$G = \{g_1, g_2, g_3, g_4, g_5\},$$

compute: $S(g_2,g_3)^G = 0$, $S(g_1,g_4) = x^6 - x^2y^2$, $S(g_1,g_4)^G = 0$, $S(g_1,g_5) = S(g_1,g_5)^G = 0$, $S(g_2,g_4) = x^8 - y^4$, $S(g_2,g_4)^G = 0$. $S(g_2,g_5) = x^4y - y^3$, $S(g_2,g_5)^G = 0$, *and* $S(g_3,g_4) = -y^7 + x^9$, $S(g_3,g_4)^G = 0$, $S(g_3,g_5) = -y^6 + x^5y$, $S(g_3,g_5)^G = 0$, $S(g_4,g_5) = -x^5 + xy^2$, $S(g_4,g_5)^G = 0$.
We see that $S(g_i,g_j)^G = 0$ *for all* $1 \leq i \leq j \leq 5$, *and it follows that* $G = \{g_1,g_2,g_3,g_4,g_5\}$ *is a Gröbner basis for* I *with respect to* 2^-.

Theorem 15 . *Let* $I = \langle g_1,\ldots,g_m\rangle \subset K[x_1,\ldots,x_n]$ *be the ideal generated by the set* $G = \{g_1,\ldots,g_m\}$. *Then the following conditions are equivalent.*

1. $G = \{g_1,\ldots,g_m\}$ *is a Gröbner basis,*
2. *For all nonzero* $f \in I$, $LT(f) \in Supp_G(f)$,
3. *For all nonzero* $f \in I$, $Supp_G(f) \neq \phi$,
4. *The remainder* h *of a complete reduction process* $f \to_G h$ *with* $Supp_G(h) \neq \phi$ *is uniquely determined,*
5. *For all* $f \in I$, $f \to_G 0$,
6. *All syzygies* $S(g_i,g_j) \to_G 0$.

Proof. *Equivalences* (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5) $\Leftrightarrow$ (6) *are standard (see[7],[24]) And are stated here just for reasons of completeness. The proof is required only for the new equivalent condition* (3). *Obviously,* (2) $\Rightarrow$ (3). *Suppose that For all nonzero* $f \in I$, $Supp_G(f) \neq \phi$ *holds and let* $f \to_G h_1$ *and* $f \to_G h_2$. *Then* $h_1 - h_2 \in I$ *and* $Supp_G(h_1 - h_2) \neq \phi$ *which contradicts* (3). *Therefore,* (3) $\Rightarrow$ (4) *is proved.* $\square$

4.3 Gröbner fan

It is known how to obtain the Newton polygon and the corresponding fan of a given polynomial. But, we can not guess the Gröbner fan of an ideal I *from the fans of its generators. Rather, we should obtain the Gröbner basis* G *of* I, *for one monomial order* $<$. *The starting order* $<$ *and the members of the*

basis G determine one cone C_G of the Gröbner fan of I. Then, we cross the boundary of the cone C_G by choosing one of the neighboring orders $<_{new}$. There are two well known ways to compute the corresponding Gröbner basis. One, to apply Buchberger's algorithm for obtaining Gröbner basis to G, with the new monomial order. The other, to take the previous Gröbner basis G, to extract leading forms of polynomials in G with respect to boundary order $<_b$ and to compute (reduced) Gröbner basis H for the ideal they generate, with respect to the new order $<_{new}$. If we denote by f^G the reduced form of the polynomial f with respect to the starting order $\prec$ and with respect to G, then the Gröbner basis of I for the new order is $\{f - f^G | f \in H\}$. The use of the Newton polygon in the example follows Sturmfels [4].

Example 13 *. Let us consider the ideal $I = \langle xy^3 - x^2, x^3y^2 - y\rangle$. We want to describe the Gröbner fan of I. The idea is to determine boundaries of its cones starting from the slope 0^+ and moving in positive direction along the arc in the first quadrant.*

1) The first step. Let $<_1$ be the lexicographical order. Its weight vector is $(1, 0)$ with the slope 0^+. The corresponding matrix is

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

For more details (see [1], [8], [13]). Note that we underline the leading terms in $f_1 := xy^3 - \underline{x^2}$ and $f_2 := \underline{x^3y^2} - y$ from I. Then $S(f_1, f_2) = f_2 + xy^2 f_1 = -y + x^2y^5 = -y^5 f_1 + xy^8 - y = -y^5 f_1 + f_3$, where $f_3 := \underline{xy^8} - y$. From the former, we eliminate f_2. Now, $S(f_1, f_3) = y^8 f_1 + x f_3 = xy^{11} - xy = y^3 f_3 + y^4 - xy = y^3 f_3 + f_4$, where $f_4 := y^4 - \underline{xy}$. Then $S(f_1, f_4) = yf_1 - xf_4 = 0$, and $S(f_3, f_4) = f_3 + y^7 f_4 = \underline{y^{11}} - y =: f_5$. From that we can eliminate f_3. We now consider only f_1, f_4, f_5. Further, $S(f_1, f_5) = y^{11} f_1 + x^2 f_5 = xy^{14} - x^2 y = xy^3 f_5 + y f_1$, and $S(f_4, f_5) = y^{10} f_4 + x f_5 = y^{14} - xy = y^3 f_5 + f_4$. The basis $\{f_1, f_4, f_5\} = \{xy^3 - \underline{x^2}, y^4 - \underline{xy}, \underline{y^{11}} - y\}$ is a Gröbner basis of I with respect to $<_1$. We take the reduced Gröbner basis of I, $G_1 = \{\underline{x^2} - y^6, \underline{xy} - y^4, \underline{y^{11}} - y\}$. From the Newton polygon of

$y^6 - x^2$ *we read* $(2,0) - (0,6) = (2,-6) \perp (3,1)$. *Similarly, using* f_4 *we have* $(1,1) - (0,4) = (1,-3) \perp (3,1)$. *Therefore, the vector* $(3,1)$ *spans one-dimensional cone, the border between two-dimensional cones in the Gröbner fan of* I. *Then,* $C_1 := \mathbb{R}_{\geq 0} \cdot (1,0) + \mathbb{R}_{\geq 0} \cdot (3,1)$ *is the cone in the Gröbner fan of* I *that corresponds to the basis* G_1.

2) The second step. Assume that $<_2$ *is the monomial order with the slope* $\frac{1}{3}^+$. *Then, the corresponding matrix is*

$$M_2 = \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}.$$

Let $g_1 := \underline{y^6} - x^2$, $g_2 := \underline{y^4} - xy$, $g_3 := \underline{y^{11}} - y$ *from* G_1. *Then* $S(g_1, g_2) = g_1 - y^2 g_2 = \underline{xy^3} - x^2 =: g_4$. *This eliminates* g_1. $S(g_2, g_3) = g_3 - y^7 g_2 = xy^8 - y = x(g_2 + xy)^2 - y = x(g_2 + 2xy)g_2 + g_5$, *where* $g_5 := \underline{x^3 y^2} - y$. *We also eliminate* g_3. $S(g_2, g_4) = xg_2 - yg_4 = 0$, $S(g_4, g_5) = x^2 g_4 - yg_5 = y^2 - \underline{x^4} =: g_6$, $S(g_2, g_5) = x^3 g_2 - y^2 g_5 = -x^4 y + y^3 = yg_6$, $S(g_2, g_6) = x^4 g_2 + y^4 g_6 = -x^5 y + y^6 = y^2 g_2 + xyg_6$, $S(g_4, g_6) = x^3 g_4 + y^3 g_6 = -x^5 + y^5 = yg_2 + xg_6$, $S(g_5, g_6) = xg_5 + y^2 g_6 = -xy + y^4 = g_2$. *The set* $G_2 := \left\{\underline{y^4} - xy, \underline{xy^3} - x^2, \underline{x^3 y^2} - y, \underline{x^4} - y^2\right\}$ *is the reduced Gröbner basis with respect to* $<_2$. *From the Newton polygons of* g_2 *and* g_4 *we read* $(0,4) - (1,1) = (1,3) - (2,0) = (-1,3) \perp (3,1)$. *Similarly, using* g_6, *we have* $(4,0) - (0,2) = (4,-2) \perp (1,2)$. *Then,* $C_2 := \mathbb{R}_{\geq 0} \cdot (3,1) + \mathbb{R}_{\geq 0} \cdot (1,2)$ *is the cone in the Gröbner fan of* I *corresponding to the basis* G_2.

3) The third step. Assume that $<_3$ *is the monomial order with the slope* 2^+. *The corresponding matrix is*

$$M_3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

We mark $h_1 := \underline{y^4} - xy$, $h_2 := \underline{xy^3} - x^2$, $h_3 := \underline{x^3 y^2} - y$, $h_4 := \underline{y^2} - x^4$ *from* G_2. *Since the leading term of* h_4 *is* y^2 *and it divides all other leading terms, we will eliminate* h_1, h_2 *and* h_3, *by using syzygies.* $S(h_2, h_4) = h_2 - xyh_4 = \underline{x^5 y} - x^2 =: h_5$, $S(h_3, h_4) = h_3 - x^3 h_4 = \underline{x^7} - y =: h_6$, $S(h_1, h_4) = h_1 - y^2 h_4 = x^4 y^2 - xy = x^4 h_4 + x^8 - xy = x^4 h_4 + xh_6$. $S(h_4, h_5) =$

$x^5h_4 - yh_5 = -x^9 + x^2y = -x^2h_6$, $S(h_4, h_6) = x^7h_4 - y^2h_6 = -x^{11} + y^3 = -x^4h_6 + yh_4$, $S(h_5, h_6) = x^2h_5 - yh_6 = -x^4 + y^2 = h_4$. *The set* $G_3 := \{\underline{y^2} - x^4, \underline{x^5y} - x^2, \underline{x^7} - y\}$ *is the reduced Gröbner basis for* $<_3$. *From the Newton polygon of* h_4 *we read* $(4,0)-(0,2) = (4,-2)\perp(1,2)$. *Also, using* h_6, *we have* $(7,0) - (0,1) = (7,-1)\perp(1,7)$. *Therefore, the cone corresponding to the basis* G_3 *is* $C_3 := \mathbb{R}_{\geq 0} \cdot (1,2) + \mathbb{R}_{\geq 0} \cdot (1,7)$.

4) The fourth step. Assume that $<_4$ *is the monomial order with the slope* 7^+. *The corresponding matrix is*

$$M_4 = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}.$$

We mark $k_1 := \underline{y^2} - x^4$, $k_2 := \underline{x^5y} - x^2$, $k_3 := \underline{y} - x^7$ *from* G_3. *Since the leading term of* k_3 *is* y *and it divides all other leading terms, we will eliminate* k_1 *and* k_2 *by using syzygies.* $S(k_1, k_3) = k_1 - yk_3 = -x^4 + x^7y = x^2k_2$, $S(k_2, k_3) = k_2 - x^5k_3 = x^{12} - x^2 =: k_4$, $S(k_3, k_4) = yk_4 - x^{12}k_3 = -x^2y + x^{19} = x^4k_4 - x^2k_3$. *The set* $G_4 := \{\underline{y} - x^7, \underline{x^{12}} - x^2\}$ *is the reduced Gröbner basis with respect to* $<_4$. *We have* $(0,1) - (7,0) = (-7,1)\perp(1,7)$ *from the Newton polygon of* k_3. *Also, using* k_4, *we observe* $(12,0) - (2,0) = (10,0)\perp(0,1)$. *Then,* $C_4 := \mathbb{R}_{\geq 0}\cdot(1,7)+\mathbb{R}_{\geq 0}\cdot(0,1)$ *is the cone corresponding to the basis* G_4.

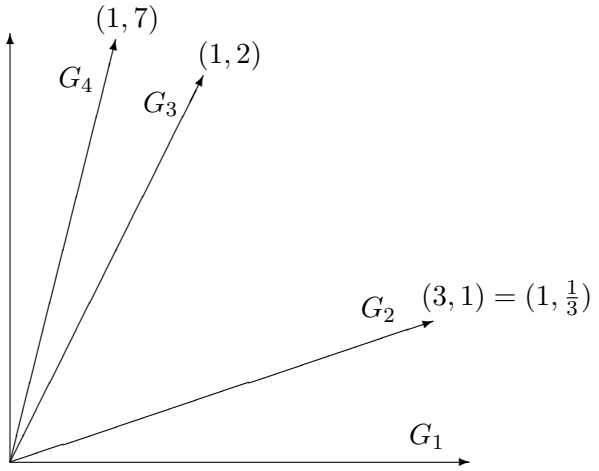

Figure 4.1: Gröbner fan for I

4.4 Bivariate Gröbner fan algorithm

In the case of two variables a precise algorithm can be given.

***Algorithm**:*

INPUT: An ideal $I = \langle f_1, \cdots, f_s \rangle$.

OUTPUT: The Gröbner fan of the ideal, $GF(I)$.

INTIALIZATION: $m = 0$, $GF(I) = \phi$.

WHILE: $m \geq 0$, $m \neq \infty$.

Compute the reduced Gröbner basis of I *with respect to* m^+, $G_{m^+} = \{g_{m_1}, g_{m_2}, \cdots, g_{m_t}\}$.

If there exist $g_{m_j} \in G_{m^+}$ *and* $k \in \mathbb{Q}$, $k > m$ *such that initial form* $in_k(g_{m_j})$ *is nonmonomial, take* n *to be the smallest* k *with that property. Otherwise , set* $n := \infty$.

$GF(I) := GF(I) \cup \{$*the cone from the slope* m *to the slope* $n\}$, $m := n$.

The above algorithm is illustrated in the Example (13).

BIBLIOGRAPHY

[1] *A. Ovchinnikov, A. Zobnin: Classification and application of monomial orderings and the properties of differential orderings. www.mayr.in.tum.de/konferenzen/CASC2002/CD/pdf/casc02.25.pdf.*

[2] *B. Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Dissertation, Univ. Innsbruck (1965)*

[3] *B. Buchberger: Introduction to Gröbner bases. (In: B. Buchberger, F. Winkler (editors): Gröbner bases and applications. Cambridge Univ Press, London Math Soc Lecture Notes 251, 1998, pp 3-31)*

[4] *B. Sturmfels: Gröbner bases and convex polytopes. University Lecture Series, Vol.8, AMS, Providence RI, 1996.*

[5] *C. Kollreider, Polynomial reduction: The Influence of the ordering of terms on a reduction algorithm, Camp. Linz. Bericht Nr. 124.(1978)*

[6] *C. Riquier: Les systèmes d'équations aux dérivées partielles, Gauthier-Villars, (1910)*

[7] *D. Cox, J. Little, D. O'Shea: Ideals, Varieties, and Algorithms. Springer, New York,1997.*

[8] *D. Pritchard: Walking Through The Gröbner Fan. citseerx.ist.psu.edu/viewdoc.*

[9] *D. W. Tarrant, JR.: Term Orders on the polynomial ring and the Gröbner Fan of an Ideal, thesis (2002)*

[10] *D.Hilbert: Über die Theorie der algebraischen Formen, Math. Annalen 36 (1890), 473-534 .*

[11] *E. Mayr, A. Meyer: The complexity of the word problem for commutative semigroups and polynomial ideals. Adv. in Math. 46 (1982), 305-329.*

[12] *E.R. Kolchin: Differential Algebra and Algebraic Groups. Academic Press, New York, (1973)*

[13] *G. Trevisan: Classificazione dei semplici ordinamenti di un gruppo libero commutativo con N generatori. Rend. Sem. Mat. univ. Padova 22 (1953) 143156.*

[14] *G.Hermann: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Annalen 95 (1926), 736-788.*

[15] *I. A. Ajwa, Z. Liu, P. S. Wang: Gröbner bases algorithm, ICM Technical Report ICM- 199502-00, 2003, 115.*

[16] *J. Freeke: Linking Gröbner Bases and Toric Varieties , masters project. people.bath.ac.uk/ac886/students/JaquelineFreeke.pdf.*

[17] *K. Fukuda, N. Jensen and R. Thomas: Computing Gröbner fans, math.AC/0509544*

[18] *L. Robbiano: Term orderings on the polynomial ring. EUROCAL 85 ,vol.2 (Linz,1985), Lecture Notes in Comput. Sci , Vol. 204, Springer, Berlin, (1985), pp. 513-517.*

[19] *M. Roczen: First steps with Gröbner bases, Preprint (www-irm.mathematik.hu-berlin.de/ roczen/papers/eforie.pdf).*

[20] *S. Collart, M. Kalkbrener and D. Mall: Converting Bases with the Gröbner Walk. J.Symbolic Computation (1997) 24,465-469.*

[21] *S. Zeada: Polynomial division and Gröbner basis. The Teaching of Mathematics, (2013), Vol. XVI, 1, pp. 22-28.*

[22] T. Mora, L. Robbiano: Gröbner Fan of an Ideal, J. symb. comp. 6 (1988) 183-208.

[23] W. Decker and F.O. Schreyer: Varieties, Gröbner Bases and Algebraic Curves. October 25, 2007. Springer. Berlin Heidelberg NewYork. HongKong ...

[24] W.W. Adams, P. Loustaunau: An Introduction to Gröbner Bases. Graduate Studies in Mathematics, Vol. 3, AMS, Providence RI, (1994).