NOTAS DE TRABAJO

9. QUANTUM GROEBNER BASES

Pascual Jara Martínez

Departamento de Álgebra
Universidad de Granada

Granada, 1996/98

Primera redacción: Abril 1996
Segunda redacción: Mayo 1998

Pascual Jara
Departamento de Álgebra
Facultad de Ciencias
Universidad de Granada
18071–Granada. ESPAÑA

Partially supported by DGICYT(PB94–0791), (PB97–0837)

ISBN 84–605–8962–5 Depósito Legal: GR–695/99

Introduction.

In this pamphlet we develop a non–commutative version of Groebner bases; we no not establish a general theory of non–commutative Groebner bases but a very special case, hence the reader may find more general frameworks for non–commutative Groebner bases. See for example [10, 12].

Our development is justified mainly in our study of $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$, the quantum polynomial ring in n indeterminates and its cofinite prime ideals. We will do that in the forthcomming paper [9]. The study of Groebner bases in this context is similar to the developed on commutative polynomial rings and, in some sense, it may be considered as a simple classroom exercise. The only difficulties appear when we are proving that certain families of elements are system of generators; in these cases the proofs are built using strongly the arithmetic of $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$.

We may consider this work as an attempt to unify and collect some results to be applied in near works.

Let us give a justification of the theory. In algebraic geometry, over an algebraically closed field, the affine space is parameterize by the polynomial ring $\mathrm{K}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$; then the study of geometrical objects is realized through algebraically objects, i.e., ideals in $\mathrm{K}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$. Now to manipulate ideals a useful tool are Groebner bases. If we introduce some deformation in the affine space, i. e., we try to study some physical phenomenon as for example heat, then the coordinate ring also reveals this deformation. The simplest example is provided if we consider the following commutation rules for the indeterminates:

$$X_j X_i = q_{i,j} X_i X_j, \quad 1 \leq i < j \leq n, \quad 0 \neq q_{i,j} \in K. \tag{1}$$

Thus we obtain the quantum polynomial ring; the justification of this name can found in [11]. The elements in this new ring are the same than in $\mathrm{K}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$, but the multiplication is different; in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ the multiplication is defined using the relationships given in (1).

With this framework the following question arise naturally: is it possible to develop a arithmetic in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ similar to the arithmetic in

$\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}]$? It is well known that the answer is yes. To develop this arithmetic we devote the first chapter. The basis to this development will be a division theorem. In order to establish the uniqueness of the remainder in the division we need to introduce Groebner bases. Finally we obtain uniqueness of certain special kinds of Groebner bases to left ideals.

At this point we remark that the theory has been developed to left ideals, and that a similar theory may be established to right ideals or even to two–sided ideals, see [10].

Chapter one finishes with applications of Groebner bases of left ideals. Let us cite the problem of deciding if an element of $\mathrm{K}_\mathrm{q}[\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}]$ belongs to a left ideal I and the problem of deciding when two left ideals are equal.

An extension of this theory is realized in chapter two. We study the application of Groebner bases to finitely generated left modules over the ring $\mathbf{R} = \mathrm{K}_\mathrm{q}[\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}]$. It is clear that it is enough to study submodules of finitely generated free modules. Thus the theory of Groebner bases for modules runs parallel to the same theory for left ideals of $\mathbf{R}$.

We finish this chapter studying the solutions of systems of equations or equivalently the syzygies modules. Let us remark that if $g_1, \ldots, g_t \in \mathbf{R}^m$ is a non–empty family, then a system of generators for $\mathrm{Syz}(g_1, \ldots, g_t)$ can be easily built. An special case is obtained if $g_1, \ldots, g_t$ is a Groebner basis for a submodule of $\mathbf{R}^m$; in this case the built system of generators is a Groebner basis for a submodule of $\mathbf{R}^t$ (even though it is necessary to define a special monomial order in $\mathbf{R}^t$ induced by $g_1, \ldots, g_t$.) This situation allows us to compute a free resolution of a finitely generated $\mathbf{R}$–module in knowning a Groebner basis for the relationships module of M, i.e., the kernel of a finitely generated free presentation of M. This theory will be used in the paper [9] to compute certain Ext groups.

The following are the references mainly used through this work:
- Adams–Loustaunau [1],
- Becker–Weispfenning [2],
- Bueso–Castro–Jara [4],
- Castro [5],
- Cox–Little–O'Shea [6],
- Kandri-Rodi–Weispfenning [10].

Finally we point out that our main reference to orders and admissible orders was [2], whereas [1] was our reference to Groebner bases of modules.

We would like to thank the following people their careful reading of earlier versions of this notes: J. L. Bueso, J. M. García, J. Gómez, J. Jódar, L. Merino, E. Santos.

Contents

P. Jara

Chapter 1

Groebner bases.

1.1. Orders and admissible orders.

Let $\mathbb{N}^n$ be the product of n copies of $\mathbb{N}$. It is well known that $\mathbb{N}^n$ has structure of commutative monoid if we consider the addition component–wise.

Let $\preceq$ be a *partial order* in $\mathbb{N}^n$, i. e., a binary relation in $\mathbb{N}^n$ satisfying the reflective, anti–symmetric and transitive properties. If $\preceq$ only satisfies the reflective and transitive properties, we call it a *preorder*. A partial order is a *total order* if for any $\alpha, \beta \in \mathbb{N}^n$ we have either $\alpha \preceq \beta$ or $\beta \preceq \alpha$; in the same way we define *total preorder*.

Let $\preceq$ be a preorder in $\mathbb{N}^n$, we write $a \prec b$ to express that $a \preceq b$ and $a \not\preceq b$.

Let $\preceq$ be a preorder in $\mathbb{N}^n$, and $S \subseteq \mathbb{N}^n$ be a non–empty set; an element $\alpha \in S$ is *minimal* (resp. *maximal*) in S if it does not exist $\beta \in S$ such that $\beta \prec \alpha$ (resp. $\alpha \prec \beta$). A preorder $\preceq$ is called *artinian* (resp. *noetherian*) if any non–empty subset $S \subseteq \mathbb{N}^n$ has a minimal (resp. maximal) element. A total artinian order is called a *well order*.

Let $\preceq_1$ and $\preceq_2$ be two preorders in $\mathbb{N}^n$, we say that $\preceq_2$ *extends* $\preceq_1$ if $\alpha \preceq_1 \beta$ implies $\alpha \preceq_2 \beta$ for any $\alpha, \beta \in \mathbb{N}^n$.

Let $\preceq$ be a preorder in $\mathbb{N}^n$. Let $S \subseteq \mathbb{N}^n$ be a non–empty subset; a *Dickson basis* of S is a finite subset $F \subseteq S$ such that for any $\alpha \in S$ there exists $\beta \in F$ with $\beta \preceq \alpha$. A preorder $\preceq$ is said to *satisfy the Dickson property* if any non–empty subset $S \subseteq \mathbb{N}^n$ has a Dickson basis. Orders and preorders satisfying the Dickson property are studied and characterized in [2].

Let $\preceq_1$ and $\preceq_2$ be preorders in $\mathbb{N}^{n_1}$ and $\mathbb{N}^{n_2}$, respectively. We define their *product* in $\mathbb{N}^{n_1+n_2}$ as:

$$(\alpha_1,\alpha_2) \preceq (\beta_1,\beta_2) \text{ if } \begin{cases} \alpha_1 \preceq_1 \beta_1 \text{ and} \\ \alpha_2 \preceq_2 \beta_2, \end{cases}$$

and their *lexicographical product* in $\mathbb{N}^{n_1+n_2}$ as:

$$(\alpha_1,\alpha_2) \preceq (\beta_1,\beta_2) \text{ if } \begin{cases} \alpha_1 \prec_1 \beta_1 \text{ or} \\ \alpha_1 \preceq_1 \beta_1,\ \beta_1 \preceq_1 \alpha_1 \text{ and } \alpha_2 \preceq_2 \beta_2. \end{cases}$$

We may iterate these products of preorders. If $\preceq_1$ and $\preceq_2$ are total orders, then their product is a partial order and their lexicographical product is a total order. We denote by $\leq$ the product order, in $\mathbb{N}^n$, of the usual order in $\mathbb{N}$ and call it the *usual order* in $\mathbb{N}^n$.

A total order $\preceq$ in $\mathbb{N}^n$ is called *admissible* if it satisfies:
(1) $0 \preceq \alpha$ for any $\alpha \in \mathbb{N}^n$;
(2) $\alpha \prec \beta$ implies $\alpha+\gamma \prec \beta+\gamma$ for any $\alpha, \beta, \gamma \in \mathbb{N}^n$.

Condition (2) may be also expressed as:
(2′) $\alpha \preceq \beta$ implies $\alpha+\gamma \preceq \beta+\gamma$ for any $\alpha, \beta, \gamma \in \mathbb{N}^n$.

(1.1.1) Proposition.
Any admissible order in $\mathbb{N}^n$ extends the usual order.

To get a proof of this and related facts on admissible orders the reader may see the book of Becker–Weispfenning, [2].

1.2. Monomial orders.

A noncommutative framework of Groebner bases was early developed, see Bergman [3], Gateva–Ivanova [7] or Ufnarovski [13] et al. Also in the case of differential operators rings it has been studied, see Castro [5], Pauer [8] et al. The main aim of this part is to be available, with consistent notation, the results we will use.

We may develop the theory in the case of iterated Ore extensions of a field K, with commutativity relations of the type:

$$X_jX_i = q_{i,j}X_iX_j + r_{i,j}, \quad i<j, \quad 0 \neq q_{i,j} \in K,$$

where $r_{i,j} \in K[X_1,\ldots,X_{j-1}]$. But this implies to use only very particular monomial orders. Hence, in order the get a more compact exposition,

we drop the terms $r_{i,j}$. In any case, the general theory is a simple exercise from the situation we will discuss here, as this is from the commutative case.

We call $\mathbf{R} = \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ the polynomial ring in non commutative indeterminates satisfying the following relationships:

$$X_j X_i = q_{i,j} X_i X_j, \quad 1 \leq i < j \leq n,\ 0 \neq q_{i,j} \in K.$$

Any polynomial $F \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ has a uniquely determined expression in the following form:

$$F = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha,$$

where $a_\alpha \in K$, for any $\alpha \in \mathbb{N}^n$, are almost all zero and $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ if $\alpha = (\alpha_1, \ldots, \alpha_n)$.

Given $F \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ we call any $a_\alpha X^\alpha$ in the above expression, with $a_\alpha \neq 0$, a *term* of F, and X^α a *monomial*. There exists a bijection from the set of all monomial to the set $\mathbb{N}^n$. This bijection provides, given an admissible order $\preceq$ in $\mathbb{N}^n$, a total order $\preceq$ in the set of all monomial in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ in the following way:

$$X^\alpha \preceq X^\beta \text{ if } \alpha \preceq \beta$$

There exists a big difference with the commutative case: now the product of two monomials is not necessarily a monomial but a term. For that reason we must extend the above order on monomials to a preorder on terms as follows:

$$aX^\alpha \prec bX^\beta \text{ if } 0 \neq a, b \in K \text{ and } \alpha \prec \beta.$$

Now this preorder is compatible with the product in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ in the following sense; it satisfies

(1) $1 \preceq bX^\beta$ for any $0 \neq bX^\beta \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$;

(2) $aX^\alpha \prec bX^\beta$ implies $acX^\alpha X^\gamma \prec bcX^\beta X^\gamma$ for any $0 \neq aX^\alpha$, bX^β, $cX^\gamma \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$.

We must first to compute the commutativity rules in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$, in order to prove that $X^\alpha X^\beta$ is a term, and after that show that the relationships in (2) are true.

We call $\mathbf{q} = (q_{i,j})_{i<j}$ and define

$$\mathbf{q}^{(\alpha,\beta)} = \prod_{i<j} q_{i,j}^{\alpha_i\beta_j}, \quad \alpha, \beta \in \mathbb{N}^n.$$

It is clear that we obtain:

$$X^\beta X^\alpha = \mathbf{q}^{(\alpha,\beta)} X^{\alpha+\beta}, \quad \alpha, \beta \in \mathbb{N}^n.$$

The arithmetic of $\mathbf{q}^{(\alpha,\beta)}$ follows the following relationships:

$$\begin{array}{l} \mathbf{q}^{(\alpha+\alpha',\beta+\beta')} = \mathbf{q}^{(\alpha,\beta)} \cdot \mathbf{q}^{(\alpha,\beta')} \cdot \mathbf{q}^{(\alpha',\beta)} \cdot \mathbf{q}^{(\alpha',\beta')}; \\ \mathbf{q}^{-(\alpha,\beta)} = \mathbf{q}^{(-\alpha,\beta)} = \mathbf{q}^{(\alpha,-\beta)}, \end{array}$$

where the negative exponents are defined using $q_{i,j}^{-1}$.

With these results we have a total order on non–zero monomials and a total preorder on non–zero terms, associated to an admissible order in $\mathbb{N}^n$. We refer them as a *monomial order* and a *term preorder* respectively.

1.3. Division algorithm.

In the following, let $\preceq$ be a fixed, but arbitrary, admissible order in $\mathbb{N}^n$ and we consider indifferently either the associated monomial order or the term preorder on $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$.

(1.3.1) Lemma.
Every non–zero polynomial $F \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ can be written, in a uniquely way, as $F = \sum_{i=1}^t a_{\alpha^i} X^{\alpha^i}$, where

$$\alpha^1 \succ \ldots \succ \alpha^t, \quad 0 \neq a_{\alpha^i} \in K, i = 1, \ldots, t.$$

To fix notation let us define some elements associated to a non–zero polynomial $0 \neq F \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ written as in Lemma (1.3.1).

(i) The *Newton diagram* of F is:

$$\mathcal{N}(F) = \{\alpha \in \mathbb{N}^n \colon\ a_\alpha \neq 0\};$$

(ii) If $F \neq 0$, the *exponent* of F is:

$$\exp(F) = \max\{\alpha \in \mathbb{N}^n \colon\ \alpha \in \mathcal{N}(F)\};$$

(iii) The *degree* of F is:

$$\mathrm{grad}(F) = \max\{\alpha_1 + \cdots + \alpha_n\colon\ \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathcal{N}(F)\};$$

(iv) The *leader coefficient* of F is: $\mathrm{lc}(F) = a_{\exp(F)}$;

(v) The *leader term* of F is: $\mathrm{lt}(F) = a_{\exp(F)} X^{\exp(F)}$;

(vi) The *leader monomial* of F is: $\mathrm{lm}(F) = X^{\exp(F)}$.

To extend these definitions to any polynomial, we may define for $F = 0$ in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ the elements $\mathcal{N}(F) = \varnothing$, $\mathrm{lt}(F) = 0$ and $\mathrm{lc}(F) = 0$.

(1.3.2) Lemma.
$\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ *is an integral domain and if* $0 \neq F, G \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$, *then* $\exp(FG) = \exp(F) + \exp(G)$.

PROOF. Let $0 \neq F, G \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$, then $\mathrm{lt}(F), \mathrm{lt}(G) \neq 0$ and we have $\mathrm{lt}(FG) = \mathrm{lt}(F)\,\mathrm{lt}(G)$. Hence the exponent is $\exp(F) + \exp(G)$, and the leader coefficient is $\mathrm{lc}(F)\,\mathrm{lc}(G)\mathbf{q}^{(\exp(F), \exp(G))} \neq 0$. □

The following result is also immediate.

(1.3.3) Lemma.
Let $0 \neq F, G \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ *then the following statements are true:*

(1) If $F + G \neq 0$, *then* $\exp(F + G) \preceq \max\{\exp(F), \exp(G)\}$;

(2) If $\exp(F) \prec \exp(G)$, *then* $\exp(F + G) = \exp(G)$.

Let us introduce some extra terminology. If $\alpha^1, \ldots, \alpha^t \in \mathbb{N}^n$ is a list of elements in $\mathbb{N}^n$, we define:

$$\begin{aligned}
\Delta^1 &= \mathbb{N}^n + \alpha^1,\\
\Delta^2 &= (\mathbb{N}^n + \alpha^2) \setminus \Delta^1,\\
&\vdots\\
\Delta^t &= (\mathbb{N}^n + \alpha^t) \setminus \cup_{i<t}\Delta^i,\\
\overline{\Delta} &= \mathbb{N}^n \setminus \cup_{i\leq t}\Delta^i.
\end{aligned}$$

We think there is no confusion with the notation α^i for an element in $\mathbb{N}^n$, as we will not use the powers of elements in $\mathbb{N}^n$.

(1.3.4) Lemma.
Let $\alpha^1, \ldots, \alpha^t$ be a list of elements in $\mathbb{N}^n$, we have that $\{\Delta^1, \Delta^2, \ldots, \Delta^t, \overline{\Delta}\}$ is a partition of $\mathbb{N}^n$.

As a consequence we have the division algorithm in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$.

(1.3.5) Theorem. (Division algorithm.)
Given an admissible order in $\mathbb{N}^n$, for any finite list of non zero polynomials

$$G_1, \ldots, G_t \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}],$$

we consider the partition of $\mathbb{N}^n$ determined by the list of elements of $\mathbb{N}^n$

$$\exp(G_1), \ldots, \exp(G_t).$$

Then we have that for any $0 \neq F \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ there exist unique polynomials $Q_1, \ldots, Q_t, R \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ satisfying the following conditions:

(1) $F = \sum_{i=1}^{t} Q_i G_i + R$;

(2) $R = 0$ or $\mathcal{N}(R) \subseteq \overline{\Delta}$;

(3) For any index i we have: $\mathcal{N}(Q_i)\exp(G_i) \subseteq \Delta^i$.

As a consequence, if $Q_i G_i \neq 0$, then $\exp(Q_i G_i) \preceq \exp(F)$ and if $R \neq 0$, then $\exp(R) \preceq \exp(F)$.

PROOF. Existence.

We do induction on $\exp(F)$. If $\exp(F) = 0$, then there are two possibilities:

(i) $\exp(F) = (0, \ldots, 0) \in \Delta^i$, for some index i or

(ii) $\exp(F) = (0, \ldots, 0) \in \overline{\Delta}$.

(i) In this case $\exp(F) = \gamma + \exp(G_i)$, for some $\gamma \in \mathbb{N}^n$, then $\exp(G_i) = (0, \ldots, 0)$ and $G_i \in K$. We can take:

$$\begin{cases} Q_j = 0, & \text{if } j \neq i; \\ Q_i = F_i/G_i; \\ R = 0 \end{cases}$$

(ii) In this case $\exp(F) \in \overline{\Delta}$, and we can take:

$$\begin{cases} Q_i = 0, & \text{if } i = 1, \dots, t; \\ R = F \end{cases}$$

Let us assume now that the result is true for all the polynomials G with $\exp(G) \prec \exp(F)$. As before, there are two possibilities:

(i) $\exp(F) \in \Delta^i$, for some index i or

(ii) $\exp(F) \in \overline{\Delta}$.

(i) In this case $\exp(F) = \gamma + \exp(G_i)$, for some $\gamma \in \mathbb{N}^n$. If we define $H = X^\gamma G_i$ then $F - \frac{\mathrm{lc}(F)}{\mathrm{lc}(H)} X^\gamma G_i$ is a polynomial with exponent strictly less than exponent of F. Applying the induction hypothesis we have:

$$F - \frac{\mathrm{lc}(F)}{\mathrm{lc}(H)} X^\gamma G_i = \sum_i Q'_i G_i + R',$$

where $Q'_1, \dots, Q'_t, R$ satisfying the conditions in the theorem. Then we have an expression:

$$F = \sum_i Q_i G_i + R,$$

where

$$\begin{cases} Q_j = Q'_j, & \text{if } j \neq i; \\ Q_i = Q'_i + \frac{\mathrm{lc}(F)}{\mathrm{lc}(H)} X^\gamma; \\ R = R' \end{cases}$$

To prove that we have the conditions of the theorem, we observe the following inclusions:

$$\begin{aligned} \exp(G_i) + \mathcal{N}(Q_i) &\subseteq \{\mathcal{N}(Q'_i) \cup \{\gamma\}\} + \exp(G_i) \\ &= (\mathcal{N}(Q'_i) + \exp(G_i)) \cup \{\gamma\}\}) \cup \{\gamma + \exp(G_i)\} \\ &\subseteq \Delta^i. \end{aligned}$$

(ii) In this case $\exp(F) \in \overline{\Delta}$, then $F - \mathrm{lt}(F)$ is a polynomial with exponent strictly less than the exponent of F. Hence by the induction hypothesis we have:

$$F - \mathrm{lt}(F) = \sum_i Q'_i G_i + R'$$

where $Q'_1, \ldots, Q'_t, R'$ satisfying the conditions in the theorem. Then we have the following expression of F:

$$F = \sum_i Q_i G_i + R,$$

where

$$\begin{cases} Q_i = Q'_i, & \text{if } i = 1, \ldots, t; \\ R = R' + \mathrm{lt}(F) \end{cases}$$

To prove that we have the conditions of the theorem, if $R \neq 0$, then since $\mathcal{N}(0) = \varnothing$, we have:

$$\mathcal{N}(R) = \mathcal{N}(R' + \mathrm{lt}(F)) \subseteq \mathcal{N}(R') \cup \{\exp(F)\} \subseteq \overline{\Delta}.$$

Uniqueness.

Let

$$F = \sum_i Q_i G_i + R = \sum_i Q'_i G_i + R'$$

be two expressions of F satisfying the conditions of the theorem. Then we have:

$$0 = \sum_i (Q_i - Q'_i) G_i + (R - R').$$

Let us analyze the exponents of the different summands in this sum:

$$\exp(R - R') \in \mathcal{N}(R - R') \subseteq \mathcal{N}(R) \cup \mathcal{N}(R') \subseteq \overline{\Delta}.$$

$$\begin{aligned} \exp((Q_i - Q'_i)G_i) &= \exp(Q_i - Q'_i) + \exp(G_i) \\ &\subseteq \mathcal{N}(Q_i - Q'_i) + \exp(G_i) \\ &= (\mathcal{N}(Q_i) + \exp(G_i)) \cup (\mathcal{N}(Q'_i) + \exp(G_i)) \\ &\subseteq \Delta^i. \end{aligned}$$

Now, as $\Delta^1, \ldots, \Delta^t, \overline{\Delta}$ is a partition of $\mathbb{N}^n$, each summand must be zero. So, as $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ is a domain, we have $Q_i = Q'_i$, for any index i, and $R = R'$. □

We call $Q_1, \ldots, Q_t$ the *left quotients* and R the *left remainder* of F relative to $\{G_1, \ldots, G_t\}$. The left remainder R may be also represented by $R_l(F; \{G_1, \ldots, G_t\})$, and if there is no confusion simply by $R(F; \{G_1, \ldots, G_t\})$.

In an analogous way we may define right quotients and right remainder of F relative to $\{G_1, \ldots, G_t\}$.

The ordering of the polynomials $G_1, \ldots, G_t$ is determinant to the computation of the left remainder, i. e., it can be happen that:

$$R(F; \{G_1, \ldots, G_i, \ldots, G_j, \ldots, G_t\}) \neq R(F; \{G_1, \ldots, G_j, \ldots, G_i, \ldots, G_t\}),$$

if $i \neq j$.

1.4. Groebner bases.

If I is a left ideal of $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$, we define

$$\mathrm{Exp}(I) = \{\exp(F)\colon\ F \in I\}.$$

(1.4.1) Lemma.
$\mathrm{Exp}(I)$ *is a monoideal of* $\mathbb{N}^n$*, i.e.,* $\mathbb{N}^n + \mathrm{Exp}(I) \subseteq \mathrm{Exp}(I)$.

Since the usual order in $\mathbb{N}^n$ satisfies the Dickson property, see Becker–Weispfenning [2], then for any non empty monoideal M there exists a finite subset $\{a^1, \ldots, a^t\} \subseteq M$ such that

$$M = \mathbb{N}^n + \{a^1, \ldots, a^t\}.$$

In particular this is true for $\mathrm{Exp}(I)$ being I any left ideal in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$.

(1.4.2) Lemma.
Let I *be a non zero left ideal of* $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$*. If* A *is a finite system of generators of* $\mathrm{Exp}(I)$*, then any set of polynomials* $\{F_\alpha\colon\ \alpha \in A\} \subseteq I$ *such that* $\exp(F_\alpha) = \alpha$ *for any* $\alpha \in A$ *is a systems of generators of* I *as left ideal.*

PROOF. Since A is finite, we can assume that $\{F_\alpha\colon\ \alpha \in A\} = \{G_1, \ldots, G_t\}$. For any $0 \neq F \in I$ we apply the division algorithm for the sequence $G_1, \ldots, G_t$. Hence we have an expression $F = \sum_i Q_i G_i + R$. If the remainder R is non–zero, then $\mathcal{N}(R) \subseteq \overline{\Delta}$. On the other hand, $R = F - \sum_i Q_i G_i \in I$, so we have $\exp(R) \in \mathrm{Exp}(I) = \mathbb{N}^n + A = \cup_i \Delta^i$, which is a contradiction. □

If I is a left ideal of $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$, a *Groebner basis* of I is a finite set of non zero elements $\mathbb{G} = \{G_1, \ldots, G_t\} \subseteq I$ satisfying

$$\mathrm{Exp}(I) = \mathbb{N}^n + \{\exp(G_1), \ldots, \exp(G_t)\}.$$

(1.4.3) Corollary.
(1) Every non zero left ideal of $\mathrm{K_q}[\mathrm{X_1},\dots,\mathrm{X_n}]$ *has a Groebner basis;*

(2) Every Groebner basis of a non zero left ideal is a system of generators.

(1.4.4) Proposition.
Let I be a non zero left ideal of $\mathrm{K_q}[\mathrm{X_1},\dots,\mathrm{X_n}]$ *and $\mathbb{G}$, $\mathbb{G}'$ two Groebner bases of I, then for any $0 \neq F \in \mathrm{K_q}[\mathrm{X_1},\dots,\mathrm{X_n}]$ we have:*

$$R(F;\mathbb{G}) = R(F;\mathbb{G}').$$

PROOF. Let us assume that, after applying the division algorithm for $\mathbb{G}$ and $\mathbb{G}'$, we have two expressions:

$$F = \sum_{G_i \in \mathbb{G}} Q_i G_i + R = \sum_{G'_j \in \mathbb{G}'} Q'_j G'_j + R',$$

respectively. If $R \neq R'$, since $R - R' \in I$, then

$$\exp(R - R') \in \mathrm{Exp}(I) = \cup_i \Delta^i = \cup_j (\Delta')^j.$$

But

$$\exp(R - R') \in \mathcal{N}(R - R') \subseteq \mathcal{N}(R) \cup \mathcal{N}(R') \subseteq \overline{\Delta} = \overline{\Delta'},$$

which is a contradiction. □

As a consequence the remainder in the division of an element F by a Groebner basis $\mathbb{G}$ do not depends of the ordering of $\mathbb{G}$.

Now we will try to get a uniquely determined Groebner basis for any non zero left ideal I. The following Lemma is almost trivial.

(1.4.5) Lemma.
Let I be a non zero left ideal of $\mathrm{K_q}[\mathrm{X_1},\dots,\mathrm{X_n}]$ *and $\mathbb{G} = \{G_1,\dots,G_t\}$ a Groebner basis of I. Let $F \in \mathbb{G}$ a polynomial satisfying:*

$$\exp(F) \in \mathbb{N}^n + \{\exp(G):\ F \neq G \in \mathbb{G}\},$$

then $\mathbb{G} \setminus \{F\}$ is a Groebner basis of I.

A Groebner basis $\mathbb{G}$ of a non zero left ideal I of $\mathrm{K_q[X_1,\dots,X_n]}$ is called *minimal* if it satisfies:

(i) $\mathrm{lc}(F) = 1$ for any $F \in \mathbb{G}$;

(ii) $\exp(F) \notin \mathbb{N}^n + \{\exp(G)\colon\ F \neq G \in \mathbb{G}\}$ for any $F \in \mathbb{G}$.

It is very simple to prove the following proposition.

(1.4.6) Proposition.
Every non zero left ideal I of $\mathrm{K_q[X_1,\dots,X_n]}$ has a minimal Groebner basis.

A non zero left ideal may have different minimal Groebner bases. In order to provide uniqueness we introduce a new kind of Groebner bases. A Groebner basis $\mathbb{G}$ of a non zero left ideal I is called *reduced* if it satisfies:

(i) $\mathrm{lc}(F) = 1$ for any $F \in \mathbb{G}$;

(ii) $\mathcal{N}(F) \cap (\mathbb{N}^n + \{\exp(G)\colon\ F \neq G \in \mathbb{G}\}) = \varnothing$.

It is clear that every reduced Groebner basis of a non zero left ideal is a minimal Groebner basis.

(1.4.7) Theorem.
Every non zero left ideal I of $\mathrm{K_q[X_1,\dots,X_n]}$ has a unique reduced Groebner basis.

PROOF. If $\mathbb{G}$ is a minimal Groebner basis, a polynomial $F \in \mathbb{G}$ is called *reduced* if

$$\mathcal{N}(F) \cap (\mathbb{N}^n + \{\exp(G)\colon\ F \neq G \in \mathbb{G}\}) = \varnothing.$$

It is obvious that if $F \in \mathbb{G}$ is reduced, then it is reduced in every minimal Groebner basis $\mathbb{G}'$ such that $F \in \mathbb{G}'$ and

$$\{\exp(G)\colon\ G \in \mathbb{G}\} = \{\exp(G)\colon\ G \in \mathbb{G}'\}.$$

We define for any $F \in \mathbb{G}$ the following elements:

$$\begin{aligned} F' &= R(F, \mathbb{G} \setminus \{F\}); \\ \mathbb{G}' &= (\mathbb{G} \setminus \{F\}) \cup \{F'\}. \end{aligned}$$

We claim $\mathbb{G}'$ is also a Groebner basis of I. If $\exp(F) \neq \exp(F')$, then we obtain from the relations:

$$F = \sum_{F \neq G \in \mathbb{G}} Q_G G + R(F; \mathbb{G} \setminus \{F\}) = \sum_{F \neq G \in \mathbb{G}} Q_G G + F'$$

and

$$\exp(F) = \max\{\{\exp(Q_G G):\ F \neq G \in \mathbb{G}\} \cup \{\exp(F')\}\},$$

and from the fact that all the exponents are different, that there exists $G \in \mathbb{G} \setminus \{F\}$ such that $\exp(F) = \exp(Q_G G)$, which is a contradiction with the fact that $\mathbb{G}$ is a minimal Groebner basis.

Then we have that $\mathbb{G}'$ is a Groebner basis and also that F' is reduced. Applying this process to each polynomial in $\mathbb{G}$, we obtain a reduced Groebner basis.

In order to prove the uniqueness, if $\mathbb{G}$ and $\mathbb{G}'$ are reduced Groebner bases, then

$$\mathrm{Exp}(I) = \mathbb{N}^n + \mathrm{Exp}(\mathbb{G}) = \mathbb{N}^n + \mathrm{Exp}(\mathbb{G}').$$

If $F \in \mathbb{G}$ then we have the following relations:

$$\begin{array}{ll} \exp(F) = \gamma + \exp(G'), & G' \in \mathbb{G}',\ \gamma \in \mathbb{N}^n; \\ \exp(G') = \gamma' + \exp(G), & G \in \mathbb{G},\ \gamma' \in \mathbb{N}^n; \end{array}$$

so we have $\exp(F) = \gamma' + \gamma + \exp(G)$. Since $\mathbb{G}$ is minimal, then $\gamma = 0 = \gamma'$. Then $\exp(F) = \exp(G')$ and we have the equality:

$$\exp(\mathbb{G}) = \exp(\mathbb{G}').$$

For any $F \in \mathbb{G}$, there exists $G' \in \mathbb{G}'$ such that $\exp(F) = \exp(G')$. Then $F - G'$ has all its terms less than $\exp(F)$. Since $F - G' \in I$ then we have $R(F - G'; \mathbb{G}) = 0$. Now $\mathbb{G}$ and $\mathbb{G}'$ are reduced and $\exp(\mathbb{G}) = \exp(\mathbb{G}')$, then

$$\mathcal{N}(F - G') \subseteq \overline{\Delta} = \mathbb{N}^n \setminus \mathrm{Exp}(I),$$

To prove this inclusion let us consider the following development:

$$\begin{array}{l} \mathcal{N}(F - G') \cap (\mathbb{N}^n + \exp(\mathbb{G})) \\ = \mathcal{N}(F - G') \cap (\cup\{\mathbb{N}^n + \exp(L):\ L \in \mathbb{G}\}) \\ = \cup\{\mathcal{N}(F - G') \cap (\mathbb{N}^n + \exp(L)):\ L \in \mathbb{G}\} \\ = \cup\{\mathcal{N}(F - G') \cap (\mathbb{N}^n + \exp(L)):\ F \neq L \in \mathbb{G}\} \\ = \mathcal{N}(F - G') \cap (\mathbb{N}^n + \{\exp(L):\ F \neq L \in \mathbb{G}\}) \\ \subseteq (\mathcal{N}(F) \cap (\mathbb{N}^n + \{\exp(L):\ F \neq L \in \mathbb{G}\})) \cup \\ (\mathcal{N}(G') \cap (\mathbb{N}^n + \{\exp(L):\ G' \neq L \in \mathbb{G}'\})) = \varnothing \end{array}$$

Then $R(F - G'; \mathbb{G}) = F - G'$, and $F = G'$. □

This uniqueness will be useful to study equality of left ideals in $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$.

1.5. Buchberger algorithm.

We are now interested in characterizing and computing Groebner bases.

(1.5.1) Proposition.
Let I be a non zero left ideal of $\mathrm{K_q[X_1,\dots,X_n]}$ and $\mathbb{G} = \{G_1,\dots,G_t\}$ be a finite family of polynomials in I. Then the following statements are equivalent:

(a) $\mathbb{G}$ is a Groebner basis of I;

(b) For any $0 \neq F \in I$ we have $R(F;\mathbb{G}) = 0$.

PROOF. (a)⇒(b). If $R(F,\mathbb{G}) \neq 0$, then $\exp(R(F,\mathbb{G})) \in \mathrm{Exp}(I) \cap \overline{\Delta} = \varnothing$, which is a contradiction.

(b)⇒(a). Let $0 \neq F \in I$, by the division algorithm, with respect to $\mathbb{G}$, there exist $Q_1,\dots,Q_t, R \in \mathrm{K_q[X_1,\dots,X_n]}$ such that:

$$F = \textstyle\sum_i Q_i G_i, \text{ and}$$

$$\exp(G_i) + \mathcal{N}(Q_i) \subseteq \Delta^i.$$

As a consequence, $\exp(Q_iG_i) \neq \exp(Q_jG_j)$ if $i \neq j$. So $\exp(F)$ is the maximum of the exponents of the summands Q_iG_i. Therefore there exists an index i such that

$$\exp(F) = \exp(Q_iG_i) \in \Delta^i \subseteq \exp(G_i) + \mathbb{N}^n,$$

and $\exp(F) \in \{\exp(G_1),\dots,\exp(G_t)\} + \mathbb{N}^n$. □

Since this characterization of Groebner bases involves all the polynomials in the left ideal, it is not very practical. Our goal now is to look for more practical criterion to characterize Groebner bases.

Using the arithmetical rules in the quantum polynomial ring $\mathrm{K_q[X_1,\dots,X_n]}$ we will define the *minimum common multiple* of a pair of monomials. Let X^α and X^β be monomials in $\mathrm{K_q[X_1,\dots,X_n]}$, we define

$$\gamma_i = \max\{\alpha_i,\beta_i\}, \qquad 1 \leq i \leq n.$$

Let $\gamma = (\gamma_1,\dots,\gamma_n) \in \mathbb{N}^n$, then we call $X^\gamma = \mathrm{mcm}\{X^\alpha, X^\beta\}$ the *minimum common multiple* of X^α and X^β. We have that X^γ is really a multiple in $\mathrm{K_q[X_1,\dots,X_n]}$ of X^α and X^β; it satisfies:

$$X^\gamma = \mathbf{q}^{-(\alpha,\gamma-\alpha)} X^{\gamma-\alpha} X^\alpha = \mathbf{q}^{-(\beta,\gamma-\beta)} X^{\gamma-\beta} X^\beta.$$

With this baggage we may define the *semisyzygies* or *s–polynomials* in the ring $\mathrm{K_q}[\mathrm{X_1},\dots,\mathrm{X_n}]$. Given $0 \neq F$, $G \in \mathrm{K_q}[\mathrm{X_1},\dots,\mathrm{X_n}]$, with $\exp(F) = X^\alpha$ and $\exp(G) = X^\beta$, the s–polynomial defined by F and G is:

$$S(F,G) = \frac{\mathbf{q}^{-(\alpha,\gamma-\alpha)}}{\mathrm{lc}(F)} X^{\gamma-\alpha} F - \frac{\mathbf{q}^{-(\beta,\gamma-\beta)}}{\mathrm{lc}(G)} X^{\gamma-\beta} G.$$

(1.5.2) Lemma.
Let $\sum_{i=1}^{t} c_i X^{\alpha^i} F_i$ be an expression, where F_i are polynomials in $\mathrm{K_q}[\mathrm{X_1},\dots,\mathrm{X_n}]$, $c_i \in K$ and $\alpha^i \in \mathbb{N}^n$, satisfying:

$$\exp(\sum_i c_i X^{\alpha^i} F_i) \prec \delta, \text{ where } \delta = \exp(X^{\alpha^i} F_i), \text{ for any index } i.$$

Then there exist elements $c_{jk} \in K$ such that:

$$\sum_i c_i X^{\alpha^i} F_i = \sum_{jk} c_{jk} X^{\delta-\gamma^{jk}} S(F_j,F_k), \quad \text{and } \exp(X^{\delta-\gamma^{jk}} S(F_j,F_k)) < \delta,$$

where $X^{\gamma^{jk}} = \mathrm{mcm}\{X^{\exp(F_j)}, X^{\exp(F_k)}\}$.

PROOF. Let us assume that $\exp(F_i) = \beta^i$, then $\alpha^i + \beta^i = \delta$. We do the following development:

$$\sum_i c_i X^{\alpha^i} F_i = \sum_i c_i \,\mathrm{lc}(F_i) \frac{X^{\alpha^i} F_i}{\mathrm{lc}(F_i)} = \sum_i c_i \,\mathrm{lc}(F_i) \mathbf{q}^{(\beta^i,\alpha^i)} H_i,$$

where we define H_i by satisfying the equation $\frac{X^{\alpha^i} F_i}{\mathrm{lc}(F_i)} = \mathbf{q}^{(\beta^i,\alpha^i)} H_i$ We may complete this development in the following way:

$$\sum_i c_i X^{\alpha^i} F_i = \sum_i c_i \,\mathrm{lc}(F_i) \mathbf{q}^{(\beta^i,\alpha^i)} H_i =$$

$$= c_1 \,\mathrm{lc}(F_1)\mathbf{q}^{(\beta^1,\alpha^1)}(H_1-H_2)+(c_1 \,\mathrm{lc}(F_1)\mathbf{q}^{(\beta^1,\alpha^1)}+c_2 \,\mathrm{lc}(F_2)\mathbf{q}^{(\beta^2,\alpha^2)})(H_2-H_3)+\cdots$$
$$\cdots+(c_1 \,\mathrm{lc}(F_1)\mathbf{q}^{(\beta^1,\alpha^1)}+\cdots+c_{t-1} \,\mathrm{lc}(F_{t-1})\mathbf{q}^{(\beta^{t-1},\alpha^{t-1})})(H_{t-1}-H_t)+$$
$$+(c_1 \,\mathrm{lc}(F_1)\mathbf{q}^{(\beta^1,\alpha^1)}+\cdots+c_t \,\mathrm{lc}(F_t)\mathbf{q}^{(\beta^t,\alpha^t)})H_t.$$

Let us consider now the product $X^{\delta-\gamma^{jk}} S(F_j,F_k)$. We will develop it and obtain a multiple of $H_j - H_k$.

$$X^{\delta-\gamma^{jk}} S(F_j,F_k) =$$

$$= X^{\delta-\gamma^{jk}}\left(\frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(F_j)}X^{\gamma^{jk}-\beta^j}F_j - \frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(F_k)}X^{\gamma^{jk}-\beta^k}F_k\right) =$$

$$= \frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(F_j)}X^{\delta-\gamma^{jk}}X^{\gamma^{jk}-\beta^j}F_j - \frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(F_k)}X^{\delta-\gamma^{jk}}X^{\gamma^{jk}-\beta^k}F_k =$$

$$= \frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)}}{\mathrm{lc}(F_j)}\mathbf{q}^{(\gamma^{jk}-\beta^j,\delta-\gamma^{jk})}X^{\delta-\beta^j}F_j - \frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)}}{\mathrm{lc}(F_k)}\mathbf{q}^{(\gamma^{jk}-\beta^k,\delta-\gamma^{jk})}X^{\delta-\beta^k}F_k =$$

$$= \frac{\mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)+(\gamma^{jk}-\beta^j,\delta-\gamma^{jk})}}{\mathrm{lc}(F_j)}X^{\delta-\beta^j}F_j - \frac{\mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)+(\gamma^{jk}-\beta^k,\delta-\gamma^{jk})}}{\mathrm{lc}(F_k)}X^{\delta-\beta^k}F_k =$$

$$= \mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)+(\gamma^{jk}-\beta^j,\delta-\gamma^{jk})}\frac{X^{\alpha^j}F_j}{\mathrm{lc}(F_j)} - \mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)+(\gamma^{jk}-\beta^k,\delta-\gamma^{jk})}\frac{X^{\alpha^k}F_k}{\mathrm{lc}(F_k)} =$$

$$= \mathbf{q}^{-(\beta^j,\gamma^{jk}-\beta^j)+(\gamma^{jk}-\beta_j,\delta-\gamma^{jk})+(\beta^j,\alpha^j)}H_j - \mathbf{q}^{-(\beta^k,\gamma^{jk}-\beta^k)+(\gamma^{jk}-\beta_k,\delta-\gamma^{jk})+(\beta^j,\alpha^j)}H_k =$$

$$= \mathbf{q}^{(\gamma^{jk},\delta-\gamma^{jk})}(H_j - H_k).$$

Then we have:

$$\mathbf{q}^{-(\gamma^{jk},\delta-\gamma^{jk})}X^{\delta-\gamma^{jk}}S(F_j,F_k) = H_j - H_k.$$

Now since $\sum_i c_i\,\mathrm{lc}(F_i)\mathbf{q}^{(\beta^i,\alpha^i)} = 0$ as $\exp(\sum C_i X^{\alpha^i}F_i \prec \delta$, we have:

$$\sum_i c_i X^{\alpha^i}F_i =$$

$$c_1\,\mathrm{lc}(F_1)\mathbf{q}^{(\beta^1,\alpha^1)}\mathbf{q}^{-(\gamma^{12},\delta-\gamma^{12})}X^{\delta-\gamma^{12}}S(F_1,F_2)+$$
$$+(c_1\,\mathrm{lc}(F_1)\mathbf{q}^{(\beta^1,\alpha^1)} + c_2\,\mathrm{lc}(F_2)\mathbf{q}^{(\beta^2,\alpha^2)})\mathbf{q}^{-(\gamma^{23},\delta-\gamma^{23})}X^{\delta-\gamma^{23}}S(F_2,F_3) + \cdots$$
$$\cdots + (c_1\,\mathrm{lc}(F_1)\mathbf{q}^{(\beta^1,\alpha^1)} + \cdots + c_{t-1}\,\mathrm{lc}(F_{t-1})\mathbf{q}^{(\beta^{t-1},\alpha^{t-1})})$$
$$\mathbf{q}^{-(\gamma^{t-1,t},\delta-\gamma^{t-1,t})}X^{\delta-\gamma^{t-1,t}}S(F_{t-1},F_t).$$

Therefore we have the first part of the theorem. To get the second part we take into account that every H_i is a monic polynomial with $\exp(H_i) = \delta$, so $\exp(H_i - H_j) < \delta$ and the result holds. □

(1.5.3) Theorem. (Buchberger)
Let I be a non zero left ideal of $\mathrm{K_q[X_1,\ldots,X_n]}$ and $\mathbb{G}$ a finite system of generators of I. Then the following statements are equivalent:

(a) $\mathbb{G}$ is a Groebner basis of I;

(b) Fixed an ordering in $\mathbb{G}$*, for any* $i \neq j$ *we have:* $R(S(G_i, G_j); \mathbb{G}) = 0$.

PROOF. (a)⇒(b). It is obvious.

(b)⇒(a). Let $0 \neq F \in I$, then $F = \sum Q_i G_i$ and we have:

$$\exp(F) \leq \max\{\exp(Q_i G_i):\ i = 1, \dots, t\}.$$

We will see that it is possible to reach the equality. Let us call

$$\begin{aligned} &\delta = \max\{\exp(Q_i G_i):\ i = 1, \dots, t\}, \\ &\delta^i = \exp(Q_i G_i). \end{aligned}$$

If $\exp(F) \prec \delta$, we decompose F in the following way:

$$\begin{aligned} F &= \textstyle\sum_i Q_i G_i = \\ &= \textstyle\sum_{\delta^i = \delta} Q_i G_i + \sum_{\delta^i < \delta} Q_i G_i = \\ &= \textstyle\sum_{\delta^i = \delta} \mathrm{lt}(Q_i) G_i + \sum_{\delta^i = \delta} (Q_i - \mathrm{lt}(Q_i)) G_i + \sum_{\delta^i < \delta} Q_i G_i. \end{aligned}$$

the two last sums are negligible; its exponent is less than δ. Thereof we can change $\sum_{\delta^i = \delta} \mathrm{lt}(Q_i) G_i$ by another expression. Using Lemma (1.5.2) we have:

$$\sum_{\delta^i = \delta} \mathrm{lt}(Q_i) G_i = \sum_{jk} c_{jk} X^{\delta - \gamma^{jk}} S(G_j, G_k),$$

with $\exp(X^{\delta - \gamma^{jk}} S(G_j, G_k)) \prec \delta$. The remainders of the division of $S(G_j, G_k)$ by $G_1, \dots, G_t$ are null, so we have:

$$S(G_j, G_k) = \sum_i Q_{jki} G_i, \qquad \text{with } Q_{jki} \in \mathrm{K_q}[\mathrm{X_1}, \dots, \mathrm{X_n}],$$

and, by the division algorithm, we have:

$$\exp(Q_{jki} G_i) \preceq \exp(S(G_j, G_k)).$$

Therefore we find an expression of the following type:

$$F = \sum_i Q'_i G_i, \quad \text{with } \exp(Q' G_i) \prec \delta.$$

Repeating the process as many times as it would be necessary, we get an expression like

$$F = \sum_i Q_i G_i,$$

where $\exp(F) = \max\{\exp(Q_iG_i)\colon\ i = 1, \dots, t\}$, so $\exp(F) = \exp(Q_iG_i)$ for some index *i*, i. e.:

$$\exp(F) = \exp(Q_iG_i) = \exp(Q_i) + \exp(G_i) \in \mathbb{N}^n + \{\exp(G_1), \dots, \exp(G_t\}.$$

and $\mathbb{G}$ is a Groebner basis. □

We are now looking for a method to compute a Groebner basis of any non zero left ideal I of $\mathrm{K_q}[\mathrm{X_1}, \dots, \mathrm{X_n}]$.

(1.5.4) Theorem. (Buchberger algorithm.)
Let I be a non zero left ideal of $\mathrm{K_q}[\mathrm{X_1}, \dots, \mathrm{X_n}]$ and let $\{G_1, \dots, G_t\}$ be a system of generators. It is possible to build a Groebner basis of I if we follow the following steps:

(1) First we define $\mathbb{G}_0 = \{G_1, \dots, G_t\}$;

(2) Second we define $\mathbb{G}_{n+1} = \mathbb{G}_n \cup \{R(S(F,G); \mathbb{G}_n) \neq 0\colon\ F, G \in \mathbb{G}_n\}$ for any $n \in \mathbb{N}$.

Then there exists an index i such that $\mathbb{G}_i = \mathbb{G}_{i+1}$ and we have that $\mathbb{G}_i$ is a Groebner basis of I.

PROOF. Let $\mathbb{G}_0 = \{G_1, \dots, G_t\}$, if $R(S(F,G); \mathbb{G}_0) = 0$ for any pair $F, G \in \mathbb{G}_0$, then we have a Groebner basis. In the contrary, there exist F, $G \in \mathbb{G}_0$ such that $R(S(F,G); \mathbb{G}_0) \neq 0$. If we call $G_{t+1} = R(S(F,G); \mathbb{G})$, then $\mathcal{N}(G_{t+1}) \subseteq \overline{\Delta}$. If we define:

$$\mathbb{G}_{(1)} = \{G_1, \dots, G_t, G_{t+1}\},$$

then we get a partition

$$\Delta^1, \dots, \Delta^t, \Delta^{t+1}, \overline{\Delta^{(1)}},$$

where $\Delta^{t+1} \cup \overline{\Delta^{(1)}} = \overline{\Delta}$. Hence if $R(F; \mathbb{G}_0) = 0$, for $F \in \mathrm{K_q}[\mathrm{X_1}, \dots, \mathrm{X_n}]$, then $R(F; \mathbb{G}_{(1)}) = 0$. If $R(S(G_i, G_j), \mathbb{G}_0) = 0$ we also have $R(S(G_i, G_j), \mathbb{G}_{(1)}) = 0$.

If for any F, $G \in \mathbb{G}_{(1)}$ we have $R(S(F,G); \mathbb{G}_{(1)}) = 0$, then we have a Groebner basis. In the contrary there exists a new $G_{t+2} = R(S(F,G); \mathbb{G}_{(1)}) \neq 0$. We define $\mathbb{G}_{(2)} = \{G_1, \dots, G_{t+1}, G_{t+2}\}$ and have $\mathcal{N}(G_{t+2}) \subseteq \overline{\Delta^{(1)}}$.

If in some step we obtain a Groebner basis, the process finishes. In the contrary we obtain an infinite strictly ascending chain of systems of generators:

$$\mathbb{G}_0 \subset \mathbb{G}_{(1)} \subset \cdots$$

Associated with this chain we have an strictly ascending chain of monoideals:

$$\mathbb{N}^n + \exp(\mathbb{G}_0) \subset \mathbb{N}^n + \exp(\mathbb{G}_{(1)}) \subset \cdots$$

As a consequence of Dickson's lemma this chain must stabilize. So there exists an index n such that

$$\exp(\mathbb{G}_{(n)}) + \mathbb{N}^n = \exp(\mathbb{G}_{(n+1)}) + \mathbb{N}^n,$$

and we have:

$$\exp(G_{t+n+1}) \in \exp(\mathbb{G}_{(n)}) + \mathbb{N}^n = \mathbb{N}^n \setminus \overline{\Delta^{(n)}},$$

but $\exp(G_{t+n+1}) \in \overline{\Delta^{(n)}}$, which is a contradiction. □

In the above process we obtain a system of generators of I which is a Groebner basis, and perhaps it has too many polynomials. Now we are going to optimize the process to obtain a Groebner basis. Following Theorem (1.4.7), it is possible to get a reduced Groebner basis.

1.6. Application of Groebner bases.

(1.6.1) Remark. (Membership problem.)
Let I be a non zero left ideal of $\mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ and let $\{F_1, \ldots, F_r\}$ be a system of generators of I; given $F \in \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$, the problem is to determine if $F \in I$.

To solve this problem we compute a Groebner basis $\mathbb{G} = \{G_1, \ldots, G_t\}$ of I; then we have $F \in I$ if and only if $R(F; \mathbb{G}) = 0$.

It is possible to obtain an expression of F as a K–linear combination of the original generators $F_1, \ldots, F_r$ of I. To do that we only need to take into account that, by the division algorithm, there exists an expression

$$F = Q_1 G_1 + \cdots + Q_t G_t,$$

where the polynomials G_i are s–polynomials obtained from the polynomials F_j, so the desired expression can be computed.

(1.6.2) Remark. (Equality of ideals.)
Let I_1 and I_2 be non zero left ideals of $\mathrm{K_q}[\mathrm{X_1},\ldots,\mathrm{X_n}]$ with systems of generators $\{F_1,\ldots,F_r\}$ and $\{H_1,\ldots,H_s\}$, respectively. The problem is to determine when $I_1 = I_2$. .

To solve this problem we compute reduced Groebner bases $\mathbb{G}_1$ and $\mathbb{G}_2$ of I_1 and I_2, respectively. By the uniqueness of reduced Groebner bases we have $I_1 = I_2$ if and only if $\mathbb{G}_1 = \mathbb{G}_2$.

Cofinite left ideals.

We study now cofinite left ideals, i. e., left ideals I such that $\mathrm{K_q}[\mathrm{X_1},\ldots,\mathrm{X_n}]/I$ is finitely dimensional K–vector space.

(1.6.3) Remark. (A $\mathbb{C}$–basis of the quotient.)
A method to compute a basis of $\mathrm{K_q}[\mathrm{X_1},\ldots,\mathrm{X_n}]/I$.

Given an element $F+I$ of $\mathrm{K_q}[\mathrm{X_1},\ldots,\mathrm{X_n}]/I$, with respect to a given Groebner basis of I we have a representative R such that $\mathcal{N}(R) \subseteq \mathbb{N}^n \setminus \mathrm{Exp}(I)$. So we can write down R in the following way:

$$R = \sum_{\alpha} c_\alpha X^\alpha,$$

where $\alpha \notin \mathbb{N}^n + \{\exp(G)\colon\ G \in \mathbb{G}\} = \mathrm{Exp}(I)$ and $c_\alpha \in \mathbb{C}$. Hence we have that $\{X^\beta\colon\ \beta \in \mathbb{N}^n \setminus \mathrm{Exp}(I)\}$ is a linearly independent system of generators of $\mathrm{K_q}[\mathrm{X_1},\ldots,\mathrm{X_n}]/I$.

As a byproduct it is possible to determine when a left ideal is cofinite: a left ideal I is cofinite if and only if the cardinal of $\mathbb{N}^n \setminus \mathrm{Exp}(I)$ is finite.

This result will be extended when we study the Gelfand–Kirillov dimension of a quotient $\mathrm{K_q}[\mathrm{X_1},\ldots,\mathrm{X_n}]/I$.

As we know a non zero left ideal I is cofinite if and only if $\mathbb{N}^n \setminus \mathrm{Exp}(I)$ is finite. We are now looking for a simpler characterization.

(1.6.4) Proposition. (Characterization of cofinite left ideals.)
Let I be a non zero left ideal of $\mathrm{K_q}[\mathrm{X_1},\ldots,\mathrm{X_n}]$ and $\mathbb{G}$ a reduced Groebner basis of I. Then the following statements are equivalent:

(a) I is cofinite;

(b) For any indeterminate X_i there exists $G_j \in \mathbb{G}$ and $\nu_i \in \mathbb{N}$ such that $\mathrm{lt}(G_j) = X_i^{\nu_i}$.

PROOF. (a)⇒(b). Since I is cofinite, given X_i there exists $\nu_i \in \mathbb{N}$ such that $X_i^{\nu_i}$ is the leader term of a polynomial in I. Hence $(0,\dots,\nu_i,\dots,0) \in \mathrm{Exp}(I) = \exp(\mathbb{G}) + \mathbb{N}^n$. Let us call $\alpha^j = \exp(G_j)$ for any $G_j \in \mathbb{G}$. There exist $j \in \{1,\dots,t\}$ and $\gamma \in \mathbb{N}^n$ such that

$$(0,\dots,\nu_i,\dots,0) = \alpha^j + \gamma,$$

then $\alpha^j_h = 0 = \gamma_h$ if $h \neq i$. Therefore $\exp(G_j) = (0\dots,\mu_i,\dots,0)$ for some $\mu_i \in \mathbb{N}$, i. e., $\mathrm{lm}(G_j) = X_i^m$ for some $m \in \mathbb{N}$.
(b)⇒(a). Let us consider $\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(I)$. By the hypothesis, for any X_i there exists G_j such that $\mathrm{lt}(G_j) = X_i^{\nu_i}$. If $\alpha_i \geq \nu_i$, then we have an expression of the following type:

$$\alpha = (0,\dots,\nu_i,\dots,0) + (\alpha_1,\dots,\alpha_i - \nu_i,\dots,\alpha_n) \in \exp(G_j) + \mathbb{N}^n \subseteq \mathrm{Exp}(I),$$

which is a contradiction, so for any index i we have $\alpha_i < \nu_i$. As a consequence there exist finitely many elements $\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(I)$ and I is cofinite. □

Chapter 2

Groebner bases of modules.

The theory of Groebner bases for modules may be reduced to the theory of Groebner bases for polynomial rings, see Adams–Loustaunau [1]. Let us introduce here some notation and results on this theory. Their proofs are easily from similar proofs in the case of polynomial rings, hence most of them will be omitted.

2.1. Division algorithm.

Let us represent $\mathrm{K_q}[\mathrm{X}_1,\ldots,\mathrm{X_n}]$ by **R**, and consider **M** the free **R**–module of rank s, i. e., $\mathbf{M}\cong\mathbf{R}^s$. If $\{e_1,\ldots,e_s\}$ is a **R**–basis of $\mathbf{R}^s$, then every element of $\mathbf{R}^s$ can be uniquely written as:

$$\sum_{i=1}^{s} R_i e_i,$$

where $R_i\in\mathbf{R}$ for any index $i=1,\ldots,s$. Given an admissible order in $\mathbb{N}^n$ or equivalently a monomial order in **R**, every element R_i may be written uniquely as a sum of multiples of monomials

$$R_i=\sum_{j=1}^{t_i} c_{ij}M_{ij},\ \text{with}\ \exp(M_{i1})\succ\cdots\succ\exp(M_{it_i}),\ 0\neq c_{ij}\in K$$

Joining both results we obtain an expression:

$$\sum_{i=1}^{s}\sum_{j=1}^{t_i} c_{ij}M_{ij}e_i$$

As a consequence, it is natural to consider the elements $c_{ij}M_{ij}e_i$ as the atoms of $\mathbf{R}^s$, where M_{ij} is a monomial of $\mathbf{R}$ and $e_1, \ldots, e_s$ is a basis of $\mathbf{R}^s$. We call these elements *terms* in $\mathbf{R}^s$. We call a *monomial* in $\mathbf{R}^s$ an expression $X^\alpha e_i$, $\alpha \in \mathbb{N}^n$. They may be parameterize by the set $\mathbb{N}^n \times \{1, \ldots, s\}$; we will denote this set by $\mathbb{N}_s^n$, their elements are represented by (α, i), being $\alpha \in \mathbb{N}^n$ and $i \in \{1, \ldots, s\}$. If $s = 1$, then $\mathbb{N}_1^n = \mathbb{N}^n$.

For any admissible order in $\mathbb{N}^n$ we obtain two orders in $\mathbb{N}_s^n$; they are the lexicographical and reverse lexicographical order of the admissible order given in $\mathbb{N}^n$ and the usual order in $\{1, \ldots, s\}$, and call them the associated TOP, "*term over position*", and POT, "*position over term*", orders.

TOP:

$$(\alpha, i) \prec (\beta, j) \text{ if } \begin{cases} \alpha \prec \beta \text{ or} \\ \alpha = \beta \text{ and } i < j \end{cases}$$

POT:

$$(\alpha, i) \prec (\beta, j) \text{ if } \begin{cases} i < j \text{ or} \\ i = j \text{ and } \alpha \prec \beta \end{cases}$$

The POT and TOP orders satisfies the following properties:

(1) They are total orders in $\mathbb{N}_s^n$;

(2) There exists an action of $\mathbb{N}^n$ over $\mathbb{N}_s^n$ defined by:

$$\mathbb{N}^n \times \mathbb{N}_s^n \xrightarrow{\theta} \mathbb{N}_s^n, \quad \theta(\alpha, (\beta, i)) = (\alpha + \beta, i).$$

We denote $\theta(\alpha, (\beta, i)) = \alpha + (\beta, i)$. This action satisfies:

(a) $0 \neq \alpha \in \mathbb{N}^n$ and $(\beta, i) \in \mathbb{N}_r^n$ implies $(\beta, i) \prec (\alpha + \beta, i)$;

(b) $(\beta^1, i_1) \prec (\beta^2, i_2)$ implies $(\alpha+\beta_1, i_1) \prec (\alpha+\beta_2, i_2)$ for any (β_1, i_1), $(\beta_2, i_2) \in \mathbb{N}_s^n$ and $\alpha \in \mathbb{N}^n$;

As a consequence $(0, i) \preceq (\alpha, i)$ for any $i \in \{1, \ldots, r\}$ and $\alpha \in \mathbb{N}^n$. A total order in $\mathbb{N}_s^n$ satisfying these properties is called an *admissible order* in $\mathbb{N}_s^n$ and associate to it we have a monomial order in $\mathbf{R}^s$.

An admissible order in $\mathbb{N}_s^n$ is *lying over* an admissible order in $\mathbb{N}^n$ if, in addition, it satisfies:

(c) $\alpha^1 \prec \alpha^2$ in $\mathbb{N}^n$ implies $(\alpha^1+\beta,i) \prec (\alpha^2+\beta,i)$ in $\mathbb{N}_s^n$ for any $(\beta,i)\in\mathbb{N}_s^n$.

In fact we will only consider admissible orders in $\mathbb{N}_r^n$ lying over a fixed, but arbitrary admissible order in $\mathbb{N}^n$; we call them only admissible orders in $\mathbb{N}_r^n$.

(2.1.1) Lemma.
For any admissible order in $\mathbb{N}^n$ we have that the POT and the TOP are admissible orders in $\mathbb{N}_s^n$.

There exists a map

$$\log:\{\text{non zero terms in } \mathbf{R}^s\}\to\mathbb{N}_s^n,\quad \log(aX^\alpha e_i)=(\alpha,e_i).$$

This map satisfies the following property:

$$\log((bX^\beta)(aX^\alpha e_i))=\log(bX^\beta)+\log(aX^\alpha e_i)$$

We may define then a *preorder* in the set of all non zero terms

$$aX^\alpha e_i \preceq bX^\beta e_j \text{ if } \log(aX^\alpha e_i)\preceq\log(bX^\beta e_j).$$

This preorder satisfies the following properties:

(1) It is a total preorder;

(2) $e_i \preceq aX^\alpha e_i$ for any $0\neq a\in K$, $\alpha\in\mathbb{N}^n$ and $i\in\{1,\dots,s\}$;

(3) $aX^\alpha e_i \preceq bX^\beta e_j$ implies $cX^\gamma aX^\alpha e_i \preceq cX^\gamma bX^\beta e_j$ for any non–zero $aX^\alpha e_i$, $bX^\beta e_j$, cX^γ;

(4) $aX^\alpha \preceq bX^\beta$ implies $aX^\alpha cX^\gamma e_i \preceq bX^\beta cX^\gamma e_j$ for any non–zero aX^α, bX^β, $cX^\gamma e_i$.

(2.1.2) Lemma.
Let $x\in\mathbf{R}^s$ be a non zero element, then x may be written, in a uniquely way, as:

$$x=\sum_{j=1}^t a_{(\alpha^j,i_j)}X^{\alpha^j}e_{i_j},\ 0\neq a_{(\alpha^j,i_j)}\in K,\ j=1,\dots,t,\ (\alpha^1,i_1)\succ\cdots\succ(\alpha^t,i_t),$$

where $(\alpha^j,i_j)\in\mathbb{N}_s^n$.

Then we may define for any $0 \neq x \in \mathbf{R}^s$ the following elements:

(i) The *Newton diagram* of x is:

$$\mathcal{N}(x) = \{(\alpha, i) \in \mathbb{N}_s^n : \ a_{(\alpha,i)} \neq 0\};$$

(ii) If $x \neq 0$, the *exponent* of x is:

$$\exp(x) = \max\{(\alpha, i) \in \mathbb{N}_s^n : \ (\alpha, i) \in \mathcal{N}(F)\};$$

(iii) The *leader coefficient* of x is: $\mathrm{lc}(x) = a_{\exp(x)}$;

(iv) The *leader term* of x is: $\mathrm{lt}(x) = a_{\exp(x)} X^{\alpha} e_i$, where $\exp(x) = (\alpha, i)$;

(v) The *leader monomial* of x is: $\mathrm{lm}(x) = X^{\alpha} e_i$, where $\exp(x) = (\alpha, i)$.

As in the polynomial case we define $\mathcal{N}(0) = \varnothing$, $\mathrm{lc}(0) = 0$ and $\mathrm{lt}(x) = 0$.

(2.1.3) Proposition.
Let $0 \neq x, x' \in \mathbf{R}^s$ and $0 \neq F \in \mathbf{R}$, then the following statements holds:

(1) $\exp(Fx) = \exp(F) + \exp(x)$*;*

(2) If $x + x' \neq 0$, then $\exp(x + x') \leq \max\{\exp(x), \exp(x')\}$*;*

(3) If $\exp(x) < \exp(x')$*, then* $\exp(x + x') = \exp(x')$*.*

Given a list $(\alpha^1, i_1), \ldots, (\alpha_t, i_t)$ of elements in $\mathbb{N}_s^n$, we define

$$\begin{aligned}
&\Delta^1 = \mathbb{N}_s^n + (\alpha^1, i_1),\\
&\Delta^2 = (\mathbb{N}_s^n + (\alpha^2, i_2)) \setminus \Delta^1,\\
&\vdots\\
&\Delta^t = (\mathbb{N}_s^n + (\alpha^t, i_t)) \setminus \cup_{i<t} \Delta^i,\\
&\overline{\Delta} \ = \mathbb{N}_s^n \setminus \cup_{i \leq t} \Delta^i.
\end{aligned}$$

(2.1.4) Lemma.
With the above notation, for any list $(\alpha^1, i_1), \ldots, (\alpha_t, i_t)$ of elements in $\mathbb{N}_s^n$ we have that $\Delta^1, \ldots, \Delta^t, \overline{\Delta}$ is a partition of $\mathbb{N}_s^n$.

(2.1.5) Theorem. (Division algorithm in $\mathbf{R}^s$)
Given an admissible order in $\mathbb{N}_s^n$, for any list $m_1, \ldots, m_t$ of non zero elements in $\mathbf{R}^s$ we consider the list $\exp(m_1), \ldots, \exp(m_t)$ of elements in $\mathbb{N}_s^m$. then for any $0 \neq m \in \mathbf{R}^s$ there exist polynomials $Q_1, \ldots, Q_t \in \mathbf{R}$ and $r \in \mathbf{R}^s$, uniquely determined, satisfying the following statements:

(1) $m = \sum_{i=1}^{t} Q_i m_i + r$*;*

(2) $r = 0$ *or* $\mathcal{N}(r) \subseteq \overline{\Delta}$*;*

(3) For any index i *we have* $\mathcal{N}(Q_i) + \exp(m_i) \subseteq \Delta^i$

As a consequence, if $Q_i m_i \neq 0$*, then* $\exp(Q_i m_i) \leq \exp(m)$*, and* $r \neq 0$ *implies* $\exp(r) \leq \exp(m)$*.*

The polynomials $Q_1, \ldots, Q_t$ are called the *quotients* of m with respect to $m_1, \ldots, m_t$, and r is called the *remainder* . We represent this remainder by $r(m; \{m_1, \ldots, m_t\})$.

2.2. Groebner bases.

Let us consider in $\mathbb{N}_s^n$ a fixed, but arbitrary, admissible order. For any non zero submodule $\mathbf{N} \subseteq \mathbf{R}^s$ we define

$$\mathrm{Exp}(\mathbf{N}) = \{\exp(n):\ 0 \neq n \in \mathbf{N}\}.$$

A non–empty subset $Y \subseteq \mathbb{N}_s^n$ is called *stable* if it satisfies:

$$\mathbb{N}^n + Y \subseteq Y$$

(2.2.1) Lemma.
For any non zero submodule $\mathbf{N}$ *of* $\mathbf{R}^s$ *the set* $\mathrm{Exp}(\mathbf{N})$ *is stable.*

PROOF. Given $n \in \mathbf{N}$ and $\alpha \in \mathbb{N}^n$. We have $X^\alpha n \in \mathbf{N}$ and $\exp(X^\alpha n) = \exp(X^\alpha) + \exp(n) = \alpha + \exp(n)$. Hence $\mathrm{Exp}(\mathbf{N})$ is stable. □

(2.2.2) Proposition.
For any non zero submodule $\mathbf{N}$ *of* $\mathbf{R}^s$ *there exist finitely many elements* $(\alpha^1, i_1), \ldots, (\alpha^t, i_t) \in \mathrm{Exp}(\mathbf{N})$ *such that*

$$\mathrm{Exp}(\mathbf{N}) = \mathbb{N}^n + \{(\alpha^1, i_1), \ldots, (\alpha^t, i_t)\}.$$

PROOF. We call $Y_i = \{\alpha \in \mathbb{N}^n:\ (\alpha, i) \in \mathrm{Exp}(\mathbf{N})\}$. Since each Y_i is an non empty subset of $\mathbb{N}^n$, it has a Dickson basis with respect to the usual order in $\mathbb{N}^n$. Let $\alpha^{i_1}, \ldots, \alpha^{i_{t_i}}$ a Dickson basis of Y_i. Then the set

$$Y = \{(\alpha^{i_1}, i), \ldots, (\alpha^{i_{t_i}}, i):\ i = 1, \ldots, s\}$$

is a Dickson basis with respect to either TOP or POT order induced in $\mathbb{N}_s^n$ by the usual order in $\mathbb{N}^n$. In particular we obtain:

$$\mathrm{Exp}(\mathbf{N}) = \mathbb{N}^n + Y.$$

□

Let $\mathbf{N} \subseteq \mathbf{R}^s$ be a non zero submodule. We call a *Groebner basis* of $\mathbf{N}$ any non empty subset $\{m_1, \ldots, m_t\} \subseteq \mathbf{N}$ such that $\mathbb{N}^n + \{\exp(m_1), \ldots, \exp(m_t)\} = \mathrm{Exp}(\mathbf{N})$.

(2.2.3) Lemma.
Let $\mathbf{N} \subseteq \mathbf{R}^s$ be a non zero submodule, any Groebner basis of $\mathbf{N}$ is a system of generator.

PROOF. Given $m \in \mathbf{N}$ and $\mathbb{G} = \{m_1, \ldots, m_t\}$ be a Groebner basis, by the division algorithm, we have:

$$m = Q_1 m_1 + \cdots, Q_t m_t + r.$$

If $r \neq 0$, then $\mathcal{N}(r) \in \overline{\Delta} = \mathbb{N}_s^n \setminus \cup_{i=1}^t \Delta^i = \mathbb{N}_s^n \setminus \mathrm{Exp}(\mathbf{N})$. On the other hand, since $r \in \mathbf{N}$, then $\exp(r) = \mathrm{Exp}(\mathbf{N})$; which is a contradiction. □

(2.2.4) Corollary.
Any non zero submodule of $\mathbf{R}^s$ has a Groebner basis.

(2.2.5) Proposition.
Let $\mathbf{N} \subseteq \mathbf{R}^s$ be a non zero submodule and $\mathbb{G}$ and $\mathbb{G}'$ Groebner bases of $\mathbf{N}$, then for any $m \in \mathbf{R}^s$ we have:

$$r(m; \mathbb{G}) = r(m; \mathbb{G}').$$

PROOF. Let $0 \neq m \in \mathbf{R}^s$, by the division algorithm we have:

$$m = \sum_{m_i \in \mathbb{G}} Q_i m_i + r(m; \mathbb{G}) = \sum_{m_j \in \mathbb{G}'} Q_j m_j + r(m; \mathbb{G}')$$

If $r(m; \mathbb{G}) \neq r(m; \mathbb{G}')$, then $x = r(m; \mathbb{G}) - r(m; \mathbb{G}') \in \mathbf{N}$, hence $\exp(x) \in \mathrm{Exp}(\mathbf{N})$. On the other hand, we have:

$$\exp(x) \in \mathcal{N}(x) \subseteq \mathcal{N}(r(m; \mathbb{G})) \cup \mathcal{N}(r(m; \mathbb{G}') \subseteq \overline{\Delta} = \overline{\Delta'} = \mathbb{N}_s^n \setminus \mathrm{Exp}(\mathbf{N}),$$

which is a contradiction. □

We will introduce some special Groebner bases in order to prove their uniqueness.

(2.2.6) Lemma.
Let $\mathbf{N} \subseteq \mathbf{R}^s$ *be a non zero submodule and* $\mathbb{G}$ *a Groebner basis. If* $x \in \mathbb{G}$ *satisfies:* $\exp(x) \in \mathbb{N}^n + \{\exp(m)\colon\ x \neq m \in \mathbb{G}\}$*, then* $\mathbb{G} \setminus \{x\}$ *is a Groebner basis of* $\mathbf{N}$*.*

Let $\mathbf{N} \subseteq \mathbf{R}^s$ be a non zero submodule and $\mathbb{G}$ a Groebner basis of $\mathbf{N}$, we say that $\mathbb{G}$ is *minimal* if it satisfies:

(i) $\mathrm{lc}(m) = 1$ for any $m \in \mathbb{G}$;

(ii) $\exp(x) \notin \mathbb{N}^n + \{\exp(m)\colon\ x \neq m \in \mathbb{G}\}$ for any $x \in \mathbb{G}$.

(2.2.7) Proposition.
Any non zero submodule of $\mathbf{R}^s$ *has a minimal Groebner basis.*

Let $\mathbf{N} \subseteq \mathbf{R}^s$ be a non zero submodule and $\mathbb{G}$ a Groebner basis, we say that $\mathbb{G}$ is *reduced* is it satisfies:

(i) $\mathrm{lc}(m) = 1$ for any $m \in \mathbb{G}$;

(ii) $\mathcal{N}(x) \cap \mathbb{N}^n + \{\exp(m)\colon\ x \neq m \in \mathbb{G}\} \neq \varnothing$ for any $x \in \mathbb{G}$.

(2.2.8) Proposition.
Any non zero submodule of $\mathbf{R}^s$ *has a reduced Groebner basis.*

Groebner bases may be easily characterized as follows:

(2.2.9) Proposition.
Let $\mathbf{N} \subseteq \mathbf{R}^s$ *be a non zero submodule and* $\mathbb{G} \subseteq \mathbf{N}$ *a finite family, then the following statements are equivalent:*

(a) $\mathbb{G}$ *is a Groebner basis;*

(b) $r(m;\mathbb{G}) = 0$ *for any* $0 \neq m \in \mathbf{N}$*;*

(c) For any $m \in \mathbf{N}$ *there exists an expression* $m = \sum_{m_i \in \mathbb{G}} Q_i m_i$ *such that* $\exp(m) = \max\{\exp(Q_i m_i)\colon\ m_i \in \mathbb{G}\}$*.*

Given terms $X^\alpha e_i$ and $X^\beta e_j$ in $\mathbf{R}^s$ we define their minimum common multiple as $X^\gamma \delta_{ij} e_i$, where X^γ is the minimum common multiple of X^α and X^β in $\mathbf{R}$.

Let m, $n \in \mathbf{R}^s$, the s–*polynomial* or *semisyzygy* of m and n is defined as:

$$S(m,n) = \mathbf{q}^{-(\alpha,\gamma-\alpha)} X^{\gamma-\alpha} \delta_{ij} \frac{1}{\mathrm{lc}(m)} m - \mathbf{q}^{-(\beta,\gamma-\beta)} X^{\gamma-\beta} \delta_{ij} \frac{1}{\mathrm{lc}(n)} n,$$

being $\exp(m) = (\alpha, i)$ and $\exp(n) = (\beta, j)$.

(2.2.10) Theorem. (Buchberger theorem)
Let $\mathbf{N} \subseteq \mathbf{R}^s$ *be a non zero submodule and* $\mathbb{G} = \{m_1, \ldots, m_t\}$ *a finite system of generators of* $\mathbf{N}$*, then the following statements are equivalent:*

(a) $\mathbb{G}$ *is a Groebner basis of* $\mathbf{N}$*;*

(b) For any $i \neq j$ *we have* $r(S(m_i, m_j); \mathbb{G}) = 0$.

(2.2.11) Theorem. (Buchberger algorithm)
Let $\mathbf{N} \subseteq \mathbf{R}^s$ *be a non zero submodule and* $\{m_1, \ldots, m_t\}$ *a system of generators. A Groebner basis of* $\mathbf{N}$ *can be reached as follows:*

$$\begin{aligned} &\mathbb{G}_0 = \{m_1, \ldots, m_t\}; \\ &\vdots \\ &\mathbb{G}_{n+1} = \mathbb{G}_n \cup \{r(S(m,n):\ m,n \in \mathbb{G}_n\} \end{aligned}$$

Then there exists an index n *such that* $\mathbb{G}_n = \mathbb{G}_{n+1}$*, in this case* $\mathbb{G}_n$ *is a Groebner basis of* $\mathbf{N}$.

2.3. Applications.

(2.3.1) Remark. (Membership problem.)
Let $\mathbf{N} \subseteq \mathbf{R}^s$ be a non zero submodule and $\{n_1, \ldots, n_l\}$ a system of generators, given $m \in \mathbf{R}^s$, the problem is to decide if $m \in \mathbf{N}$. To solve this problem we compute a Groebner basis $\mathbb{G} = \{m_1, \ldots, m_t\}$ of $\mathbf{N}$ then we have $m \in \mathbf{N}$ if and only if $r(m; \mathbb{G}) = 0$.

In addition, since the elements m_i are $\mathbf{R}$–linear combination of $\{n_1, \ldots, n_l\}$, it is possible to obtain an expression

$$m = Q_1 n_1 + \cdots + Q_l n_l$$

in the case in which $m \in \mathbf{N}$.

(2.3.2) Remark. (Equality of submodules.)
Let $\mathbf{N}_1$ and $\mathbf{N}_2$ be non zero submodules of $\mathbf{R}^s$ with systems of generators $\{n_1, \ldots, n_l\}$ and $\{h_1, \ldots, h_k\}$ respectively. The problem is to determine when $\mathbf{N}_1 = \mathbf{N}_2$.

To solve this problem we compute reduced Groebner bases $\mathbb{G}_1$ and $\mathbb{G}_2$ of $\mathbf{N}_1$ and $\mathbf{N}_2$ respectively. By the uniqueness of reduced Groebner bases we have $\mathbf{N}_1 = \mathbf{N}_2$ if and only if $\mathbb{G}_1 = \mathbb{G}_2$.

(2.3.3) Remark. (Cofinite submodules.)
As in the case of ideals, a K–basis of $\mathbf{R}^s/\mathbf{N}$ is indexed in the set $\mathbb{N}_s^n \setminus \mathrm{Exp}(\mathbf{N})$. In addition, a finiteness criterion can be done: for any indeterminate X_j and any index i there exists a $m \in \mathbf{N}$ such that $\mathrm{lm}(m) = X_j^n e_i$ for some $n \in \mathbb{N}$.

More applications.

Let us consider $\mathbf{R} = \mathrm{K_q}[\mathrm{X_1}, \ldots, \mathrm{X_n}]$ and new indeterminates $Y_1, \ldots, Y_m$. Let $\mathbf{N} \subseteq \mathbf{R}[Y_1, \ldots, Y_m]^t$ be a submodule, we are interested in an elimination theorem in order to determine a Groebner basis of $\mathbf{N} \cap \mathbf{R}^t$ when a Groebner basis of $\mathbf{N}$ is known.

(2.3.4) Theorem.
Let $\mathbb{G}$ be a Groebner basis of $\mathbf{N} \subseteq \mathbf{R}[Y_1, \ldots, Y_m]^t$ with respect to a TOP monomial order and the lexicographical order in $\mathbf{R}[Y_1, \ldots, Y_m]$, being Y_j's bigger than X_i's. Then $\mathbb{G} \cap \mathbf{R}^t$ is a Groebner basis of $\mathbf{N} \cap \mathbf{R}^t$.

PROOF. We always have the inclusion $\mathbb{G} \cap \mathbf{R}^t \subseteq \mathbf{N} \cap \mathbf{R}^t$. On the other hand, given $0 \neq m \in \mathbf{N} \cap \mathbf{R}^t$, there exists $g \in \mathbb{G}$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(m)$. Since m has only indeterminates $X_1, \ldots, X_n$, then the same holds for $\mathrm{lm}(m)$, the coordinate of g in which appears $\mathrm{lm}(g)$, and since the monomial order is TOP, in the coordinates of g only appear indeterminates $X_1, \ldots, X_n$. As a consequence $g \in \mathbb{G} \cap \mathbf{R}^t$. □

As a direct application let us show how to compute a Groebner basis of an intersection of submodules.

(2.3.5) Proposition. (Intersection of submodules.)
Let $\mathbf{N}_1$ and $\mathbf{N}_2$ be non–zero submodules of $\mathbf{R}^s$ with generators $f_1, \ldots, f_h$ and $g_1, \ldots, g_k$ respectively. Let Y a new indeterminate, commuting with $\mathbf{R}$, and let us define

$$\mathbf{L} = \mathbf{R}(Yf_1, \ldots, Yf_h, (1-Y)g_1, \ldots, (1-Y)g_k) \subseteq \mathbf{R}[Y]^s,$$

then $\mathbf{N}_1 \cap \mathbf{N}_2 = \mathbf{L} \cap \mathbf{R}^s$.

PROOF. Let $m \in \mathbf{N}_1 \cap \mathbf{N}_2$, then $m = Ym + (1-Y)m \in \mathbf{L} \cap \mathbf{R}^s$. Conversely, let $m \in \mathbf{L} \cap \mathbf{R}^s$, then $m = \sum_i Yf_i + \sum_j (1-Y)g_j$. If we evaluate Y in 1 then we obtain $m = \sum_i f_i \in \mathbf{N}_1$; and evaluating in 0 then $m = \sum_j g_j \in \mathbf{N}_2$. □

(2.3.6) Remark. (Annihilator of an element.)
As a consequence, to get a Groebner basis of $\mathbf{N}_1 \cap \mathbf{N}_2$ it is enough to compute a Groebner basis $\mathbb{G}$ of $\mathbf{L}$ in $\mathbf{R}[Y]^s$ with respect to a TOP monomial order in which Y is biggest that each X_i lexicographically. Then a Groebner basis of $\mathbf{N}_1 \cap \mathbf{N}_2$ is $\mathbb{G} \cap \mathbf{R}^s$.

Another useful application involve the computation of the annihilator of elements in $\mathbf{R}^s$.

(2.3.7) Proposition.
Let $\mathbf{N}$ *be a non–zero submodule of a* $\mathbf{R}^s$ *and* $0 \neq m \in \mathbf{R}^s$, *then*

$$(\mathbf{N} : m) = \{Q \in \mathbf{R} :\ Qm \in \mathbf{N} \cap \mathbf{R}m\}.$$

PROOF. Easy. □

(2.3.8) Remark.
As a consequence to compute a system of generator of $(\mathbf{N} : m)$ it is enough to compute a system of generator of $\mathbf{N} \cap \mathbf{R}m$ and divide each element by m. Hence the quotients produce a system of generators of $(\mathbf{N} : m)$. Indeed, let $Q \in (\mathbf{N} : m)$ and $x_1, \ldots, x_l$ a system of generators of $\mathbf{N} \cap \mathbf{R}m$; let $x_i = H_i m$, $H_i \in \mathbf{R}$, $i = 1, \ldots, l$. We may write $Qm = \sum_i C_i x_i = \sum_i C_i H_i m$, being $C_i \in \mathbf{R}$. At least one of the coordinates of m is non–zero as m is non zero. Hence $Q = \sum_i C_i H_i$ as $\mathbf{R}$ is a domain.

2.4. Syzygy modules.

Let us consider a linear map $f\colon \mathbf{R}^t \to \mathbf{R}^m$. Then, fixed bases $\{e_1, \ldots, e_t\}$ in $\mathbf{R}^t$ and $\{l_1, \ldots, l_m\}$ in $\mathbf{R}^m$ respectively, f is determined by a matrix with coefficients in $\mathbf{R}$. Let

$$f(e_i) = \sum_{j=1}^{m} a_{ij} l_j, \quad i = 1, \ldots, t$$

then the matrix of f is $A(f) = \begin{pmatrix} a_{11} \cdots a_{im} \\ \vdots \quad\quad \vdots \\ a_{t1} \cdots a_{tm} \end{pmatrix}$.

We call the kernel of $A(f)$ the *syzygy module* of f, and represent it by $\mathrm{Syz}(f)$. Hence we have:

$$\mathrm{Syz}(f) = \{(b_i)_i \in \mathbf{R}^t \colon\ (b_i)_i (a_{ij})_{ij} = 0\}$$

$$\begin{cases} b_1 a_{11} + \cdots + b_t a_{t1} = 0 \\ \vdots \\ b_1 a_{1m} + \cdots + b_t a_{tm} = 0 \end{cases} \tag{2.1}$$

i.e., $\mathrm{Syz}(f)$ is the set of all solutions to the system of linear equations (2.1).

The problem, we are interested, is to determine a system of generators of $\mathrm{Syz}(f)$.

First case.

Let us consider $f\colon \mathbf{R}^t \to \mathbf{R}$ defined by

$$f(e_i) = c_i X^{\alpha^i}, \quad 0 \neq c_i \in K, \quad \alpha^i \in \mathbb{N}^n, \quad i = 1, \ldots, t.$$

(2.4.1) Proposition.
For any $i \neq j \in \{1, \ldots, t\}$ we define $X_{ij} = \mathrm{mcm}\{X^{\alpha^i}, X^{\alpha^j}\} = X^{\gamma^{ij}}$, then

$$\{\mathbf{q}^{-(\alpha^i, \gamma^{ij} - \alpha^i)} X^{\gamma^{ij} - \alpha^i} e_i - \{\mathbf{q}^{-(\alpha^j, \gamma^{ij} - \alpha^j)} X^{\gamma^{ij} - \alpha^j} e_i \colon\ 1 \leq i < j \leq t\}$$

is a system of generators of Syz$(c_1 X^{\alpha^1}, \ldots, c_t X^{\alpha^t})$.

PROOF. First we prove that each element is a syzygy:

$$\mathbf{q}^{-(\alpha^i, \gamma^{ij} - \alpha^i)} X^{\gamma^{ij} - \alpha^i} c_i X^{\alpha^i} - \mathbf{q}^{-(\alpha^j, \gamma^{ij} - \alpha^j)} X^{\gamma^{ij} - \alpha^j} c_j X^{\alpha^j} = X^{\gamma} - X^{\gamma} = 0$$

To prove that it is a system of generators, let $(H_1, \ldots, H_t) \in \mathrm{Syz}(c_1 X^{\alpha^1}, \ldots, c_t X^{\alpha^t})$, then

$$H_1 c_1 X^{\alpha^1} + \cdots + H_t c_t x^{\alpha^t} = 0$$

For any $\alpha \in \mathbb{N}^n$ the coefficient of X^α must be zero, hence we may assume that each H_i has the following form: $H_i = c_i' X^{\beta^i}$, being either $c_i' = 0$ or $\beta^i + \alpha^i = \alpha$.

Let $c'_{i_1},\dots,c'_{i_s}$ the only non–zero coefficients and assume that $\beta^{i_1}\prec\cdots\prec\beta^{i_s}$. then we have:

$$
\begin{aligned}
&\textstyle\sum_{i=1}^{t} H_i e_i\\
&=\textstyle\sum_{i=1}^{t} c'_i X^{\beta^i} e_i\\
&=\textstyle\sum_{j=1}^{s} c'_{i_j} X^{\beta^{i_j}} e_{i_j}\\
&= c'_{i_1}\mathbf{q}^{-(\gamma^{12}-\alpha^{i_1},\alpha-\gamma^{12})} X^{\alpha-\gamma^{12}} X^{\gamma^{12}-\alpha^{i_1}} e_{i_1}+\cdots\\
&\ +c'_{i_{s-1}}\mathbf{q}^{-(\gamma^{s-1s}-\alpha^{i_{s-1}},\alpha-\gamma^{s-1s})} X^{\alpha-\gamma^{s-1s}} X^{\gamma^{s-1s}-\alpha^{i_s}} e_{i_{s-1}}+c'_{i_s}X^{\beta^{i_s}}e_{i_s}\\
&= c'_{i_1}c_{i_1}\mathbf{q}^{-(\gamma^{12}-\alpha^{i_1},\alpha-\gamma^{12})+(\alpha^{i_1},\gamma^{12}-\alpha^{i_1})} X^{\alpha-\gamma^{12}}\frac{\mathbf{q}^{-(\alpha^{i_1},\gamma^{12}-\alpha^{i_1})}}{c_{i_1}} X^{\gamma^{12}-\alpha^{i_1}} e_{i_1}\\
&\ +c'_{i_2}c_{i_2}\mathbf{q}^{-(\gamma^{23}-\alpha^{i_2},\alpha-\gamma^{23})+(\alpha^{i_2},\gamma^{23}-\alpha^{i_2})} X^{\alpha-\gamma^{23}}\frac{\mathbf{q}^{-(\alpha^{i_2},\gamma^{23}-\alpha^{i_2})}}{c_{i_2}} X^{\gamma^{23}-\alpha^{i_2}} e_{i_2}\\
&\ +\cdots+c'_{i_s}X^{\beta^{i_s}}e_{i_s}\\
&= c'_{i_1}c_{i_1}\mathbf{q}^{-(\gamma^{12},\alpha-\gamma^{12})+(\alpha^{i_1},\alpha-\alpha^{i_1})} X^{\alpha-\gamma^{12}}\frac{\mathbf{q}^{-(\alpha^{i_1},\gamma^{12}-\alpha^{i_1})}}{c_{i_1}} X^{\gamma^{12}-\alpha^{i_1}} e_{i_1}\\
&\ +c'_{i_2}c_{i_2}\mathbf{q}^{-(\gamma^{23},\alpha-\gamma^{23})+(\alpha^{i_2},\alpha-\alpha^{i_2})} X^{\alpha-\gamma^{23}}\frac{\mathbf{q}^{-(\alpha^{i_2},\gamma^{23}-\alpha^{i_2})}}{c_{i_2}} X^{\gamma^{23}-\alpha^{i_2}} e_{i_2}\ +\cdots+c'_{i_s}X^{\beta^{i_s}}e_{i_s}\\
&= c'_{i_1}c_{i_1}\mathbf{q}^{-(\gamma^{12},\alpha-\gamma^{12})+(\alpha^{i_1},\alpha-\alpha^{i_1})} X^{\alpha-\gamma^{12}}\\
&\ \left(\frac{\mathbf{q}^{-(\alpha^{i_1},\gamma^{12}-\alpha^{i_1})}}{c_{i_1}} X^{\gamma^{12}-\alpha^{i_1}} e_{i_1}+\frac{\mathbf{q}^{-(\alpha^{i_2},\gamma^{12}-\alpha^{i_2})}}{c_{i_2}} X^{\gamma^{12}-\alpha^{i_2}} e_{i_2}\right)\\
&\ +\left(c'_{i_1}c_{i_1}\mathbf{q}^{-(\gamma^{12},\alpha-\gamma^{12})+(\alpha^{i_1},\alpha-\alpha^{i_1})} X^{\alpha-\gamma^{12}}\frac{\mathbf{q}^{-(\alpha^{i_2},\gamma^{12}-\alpha^{i_2})}}{c_{i_2}} X^{\gamma^{12}-\alpha^{i_2}}\right.\\
&\ \left.+\ c'_{i_2}c_{i_2}\mathbf{q}^{-(\gamma^{23},\alpha-\gamma^{23})+(\alpha^{i_2},\alpha-\alpha^{i_2})} X^{\alpha-\gamma^{23}}\frac{\mathbf{q}^{-(\alpha^{i_2},\gamma^{23}-\alpha^{i_2})}}{c_{i_2}} X^{\gamma^{23}-\alpha^{i_2}}\right) e_{i_2}\\
&\ +\cdots+c'_{i_s}X^{\beta^{i_s}}e_{i_s}\\
&=\cdots+\left(c'_{i_1}c_{i_1}\mathbf{q}^{-(\gamma^{23},\alpha-\gamma^{23})+(\alpha^{i_1},\alpha-\alpha^{i_1})} X^{\alpha-\gamma^{23}}\right.\\
&\ \left.+\ c'_{i_2}c_{i_2}\mathbf{q}^{-(\gamma^{23},\alpha-\gamma^{23})+(\alpha^{i_2},\alpha,\alpha^{i_2})} x^{\alpha-\gamma^{23}}\right)\frac{\mathbf{q}^{-(\alpha^{i_2},\gamma^{23}-\alpha^{i_2})}}{c_{i_2}} X^{\gamma^{23}-\alpha^{i_2}} e_{i_2}\\
&\ +\cdots+c'_{i_s}X^{\beta^{i_s}}e_{i_s}\\
&=\cdots+\left(\left(c'_{i_1}c_{i_1}\mathbf{q}^{(\alpha^{i_1},\alpha-\alpha^{i-1})}+\cdots+c'_{i_{s-1}}c_{i_{s-1}}\mathbf{q}^{(\alpha^{i_{s-1}},\alpha-\alpha^{i_{s-1}})}\right)\right.\\
&\ \left.\mathbf{q}^{-(\gamma^{s-1s},\alpha-\gamma^{s-1s})} X^{\alpha-\gamma^{s-1s}}\frac{\mathbf{q}^{-(\alpha^{i_s},\gamma^{s-1s}-\alpha^{i_s})}}{c_{i_s}} X^{\gamma^{s-1s}-\alpha^{i_s}}+c'_{i_s}X^{\alpha-\alpha^{i_s}}\right) e_{i_s}\\
&=\cdots+\left(\left(c'_{i_1}c_{i_1}\mathbf{q}^{(\alpha^{i_1},\alpha-\alpha^{i-1})}+\cdots+c'_{i_{s-1}}c_{i_{s-1}}\mathbf{q}^{(\alpha^{i_{s-1}},\alpha-\alpha^{i_{s-1}})}\right)\right.\\
&\ \left.\mathbf{q}^{-(\alpha^{i_s},\alpha-\alpha^{i_s})}\frac{1}{c_{i_s}} X^{\alpha-\alpha^{i_s}}+c'_{i_s}X^{\alpha-\alpha^{i_s}}\right) e_{i_s}\\
&=\cdots+\left(c'_{i_1}c_{i_1}\mathbf{q}^{(\alpha^{i_1},\alpha-\alpha^{i-1})}+\cdots+c'_{i_{s-1}}c_{i_{s-1}}\mathbf{q}^{(\alpha^{i_{s-1}},\alpha-\alpha^{i_{s-1}})}+c'_{i_s}c_{i_s}\mathbf{q}^{(\alpha^{i_s},\alpha-\alpha^{i_s})}\right)\\
&\ \mathbf{q}^{-(\alpha^{i_s},\alpha-\alpha^{i_s})}\frac{1}{c_{i_s}} X^{\alpha-\alpha^{i_s}} e_{i_s}.
\end{aligned}
$$

The sum in the parenthesis is zero as

$$\begin{aligned}
&H_1 c_1 X^{\alpha^1} + \cdots + H_t c_t X^{\alpha^t} = 0\\
&H_{i_1} c_{i_1} X^{\alpha^{i_1}} + \cdots + H_{i_s} c_{i_s} X^{\alpha^{i_s}} = 0\\
&c'_{i_1} X^{\alpha-\alpha^{i_1}} c_{i_1} X^{\alpha^{i_1}} + \cdots + c'_{i_s} X^{\alpha-\alpha^{i_s}} c_{i_s} X^{\alpha^{i_s}} = 0\\
&\left(c'_{i_1} c_{i_1} \mathbf{q}^{(\alpha^{i_1},\alpha-\alpha^{i_1})} + \cdots + c'_{i_s} c_{i_s} \mathbf{q}^{(\alpha^{i_s},\alpha-\alpha^{i_s})} \right) X^{\alpha} = 0
\end{aligned}$$

and $c'_{i_1} c_{i_1} \mathbf{q}^{(\alpha^{i_1},\alpha-\alpha^{i_1})} + \cdots + c'_{i_s} c_{i_s} \mathbf{q}^{(\alpha^{i_s},\alpha-\alpha^{i_s})} = 0$ □

Second case.

Let us consider $f\colon \mathbf{R}^t \to \mathbf{R}$ defined by

$$f(e_i) = G_i, \quad 0 \neq G_i \in \mathbf{R}, \quad i = 1, \ldots, t,$$

being $\{G_1, \ldots, G_t\}$ a Groebner basis in $\mathbf{R}$ and $\mathrm{lc}(G_i) = 1$ for any index i. Let $\mathrm{lm}(G_i) = X^{\alpha^i}$, $i = 1, \ldots, t$.

In this case we call $X^{\gamma^{ij}}$ the minimum common multiple of X^{α^i} and X^{α^j} and define the s–polynomials of G^i and G_j, $i < j$, as usual:

$$S(G_i, G_j) = \mathbf{q}^{-(\alpha^i,\gamma^{ij}-\alpha^i)} X^{\gamma^{ij}-\alpha^i} G_i - \mathbf{q}^{-(\alpha^j,\gamma^{ij}-\alpha^j)} X^{\gamma^{ij}-\alpha^j} G_j$$

Since $\{G_1, \ldots, G_t\}$ is a Groebner basis, by the division algorithm there exists an expression of $S(G_i, G_j)$ as follows:

$$\begin{aligned}
&S(G_i, G_j) = \textstyle\sum_{h=1}^{t} Q_{ijh} G_h, \quad Q_{ijh} \in \mathbf{R}\\
&\mathrm{lm}(S(G_i, G_j)) = \max\{\mathrm{lm}(Q_{ijh} G_h)\colon\ 1 \leq h \leq t\} \prec X^{\gamma^{ij}}
\end{aligned}$$

Hence we define new elements

$$s_{ij} = \mathbf{q}^{-(\alpha^i,\gamma^{ij}-\alpha^i)} X^{\gamma^{ij}-\alpha^i} e_i - \mathbf{q}^{-(\alpha^j,\gamma^{ij}-\alpha^j)} X^{\gamma^{ij}-\alpha^j} e_j - \sum_{h=1}^{t} Q_{ijh} e_h \in \mathbf{R}^t$$

It is clear that s_{ij} is a syzygy of $G_1, \ldots, G_t$ as

$$\mathbf{q}^{-(\alpha^i,\gamma^{ij}-\alpha^i)} X^{\gamma^{ij}-\alpha^i} G_i - \mathbf{q}^{-(\alpha^j,\gamma^{ij}-\alpha^j)} X^{\gamma^{ij}-\alpha^j} G_j - \sum_{h=1}^{t} Q_{ijh} G_h = 0$$

(2.4.2) Theorem.
The family $\{s_{ij}\colon\ 1 \leq i < j \leq t\}$ *is a system of generators of* $\mathrm{Syz}(G_1, \ldots, G_t)$.

PROOF. Let $h = \sum_{i=1}^{t} H_i e_i \in \mathrm{Syz}(G_1, \ldots, G_t)$ which is not generated by the set $\{s_{ij}\colon\ 1 \leq i < j \leq t\}$. We may take h such that

$$X^{\alpha} = \max\{\mathrm{lm}(H_i G_i\colon\ 1 \leq i \leq t\} \text{ is minimal}$$

Let us call $S = \{i \in \{1, \ldots, t\}\colon\ \mathrm{lm}(H_i G_i) = X^{\alpha}\}$ and for any $i \in \{1, \ldots, t\}$ we define

$$H_i' = \begin{cases} H_i & \text{if } i \notin S; \\ H_i - \mathrm{lm}(H_i) & \text{if } i \in S. \end{cases}$$

Let us call $\mathrm{lm}(H_i) = c_i X^{\beta^i}$, $0 \neq c_i \in K$, $i \in S$. Since h is a syzygy it satisfies:

$$\sum_{i \in S} c_i X^{\beta^i} X^{\alpha^i} = 0, \quad \beta^i + \alpha^i = \alpha.$$

Hence

$$\sum_{i \in S} c_i X^{\beta^i} e_i \in \mathrm{Syz}(X^{\alpha^i}\colon\ i \in S).$$

As a consequence

$$\sum_{i \in S} c_i X^{\beta^i} e_i = \sum_{\substack{i < j \\ i,j \in S}} Q_{ij} \left(\mathbf{q}^{-(\alpha^i, \gamma^{ij} - \alpha^i)} X^{\gamma^{ij} - \alpha^i} e_i - \mathbf{q}^{-(\alpha^j, \gamma^{ij} - \alpha^j)} X^{\gamma^{ij} - \alpha^j} e_j \right)$$

being $Q_{ij} \in \mathbf{R}$. Each coordinate in the left part is homogeneous and satisfies $\beta^i + \alpha^i = \alpha$. Then we may consider each Q_{ij} homogeneous and a K–multiple of $X^{\alpha - \gamma^{ij}}$. Therefore we obtain:

$$\begin{aligned} h &= \textstyle\sum_{i=1}^{t} = \sum_{i \in S} c_i X^{\beta^i} e_i + \sum_{i=1}^{t} H_i' e_i \\ &= \sum_{\substack{i < j \\ i,j \in S}} Q_{ij} \left(\mathbf{q}^{-(\alpha^i, \gamma^{ij} - \alpha^i)} X^{\gamma^{ij} - \alpha^i} e_i - \mathbf{q}^{-(\alpha^j, \gamma^{ij} - \alpha^j)} X^{\gamma^{ij} - \alpha^j} e_j \right) + \textstyle\sum_{i=1}^{t} H_i' e_i \\ &= \sum_{\substack{i < j \\ i,j \in S}} Q_{ij} s_{ij} + \textstyle\sum_{i=1}^{t} H_i' e_i + \sum_{\substack{i < j \\ i,j \in S}} Q_{ij} (\textstyle\sum_{h=1}^{t} Q_{ijh} e_h). \end{aligned}$$

If we define

$$p = \sum_{i=1}^{t} P_i e_i = \sum_{i=1}^{t} H'_i e_i + \sum_{\substack{i<j \\ i,j \in S}} Q_{ij}(\sum_{h=1}^{t} Q_{ijh} e_h)$$

then $p \in \mathrm{Syz}(G_1, \ldots, G_t)$ and it is not an $\mathbf{R}$–linear combination of $\{s_{ij}\colon\ 1 \leq i < j \leq t\}$. We reach to a contradiction if we prove that

$$\max\{\mathrm{lm}(P_i G_i)\colon\ 1 \leq i < j \leq t\} \prec X^{\alpha}$$

For any $l \in \{1, \ldots, t\}$ we have:

$$\begin{aligned} &\mathrm{lm}(P_l G_l) \\ &= \mathrm{lm}(H'_l X^{\alpha^l} - \sum_{\substack{i<j \\ i,j \in S}} Q_{ij} Q_{ijl} X^{\alpha^l}) \\ &\preceq \max\{\mathrm{lm}(H'_l X^{\alpha^l}), \mathrm{lm}(\sum_{\substack{i<j \\ i,j \in S}} Q_{ij} Q_{ijl} X^{\alpha^l})\} \end{aligned}$$

We have $\mathrm{lm}(H'_l X^{\alpha^l}) \prec X^{\alpha^l}$ by the definition of H'_l. Also, by construction, Q_{ij} is a K–multiple of $X^{\alpha-\gamma^{ij}}$, then

$$\mathrm{lm}(Q_{ij} Q_{ijl} X^{\alpha^l}) \preceq \mathrm{lm}(Q_{ij} S(G_i, G_j)) \prec \mathrm{lm}(X^{\alpha-\gamma^{ij}} X^{\gamma^{ij}}) = X^{\alpha}.$$

As a consequence $\mathrm{lm}(P_l G_l) \prec X^{\alpha}$, which is a contradiction with the election of h. □

Third case.

Let us consider $f\colon \mathbf{R}^s \to \mathbf{R}$ defined by

$$f(e_j) = F_j, \quad 0 \neq F_j \in \mathbf{R}, \quad j = 1, \ldots, s.$$

In this case we compute a Groebner basis for the left ideal of $\mathbf{R}$ generates by $F_1, \ldots, F_s$. Let $\{G_1, \ldots, G_t\}$ such a Groebner basis in $\mathbf{R}$, we may assume $\mathrm{lc}(G_i) = 1$ for any index i.

There exist expressions

$$G_i = \textstyle\sum_{j=1}^{s} A_{ij} F_j, \quad i = 1, \ldots, t, \quad A_{ij} \in \mathbf{R} \text{ and}$$

$$F_j = \textstyle\sum_{i=1}^{t} B_{ji} G_i, \quad j = 1, \ldots, s, \quad B_{ji} \in \mathbf{R}.$$

Now we may define matrices $A = \begin{pmatrix} A_{11} \cdots A_{1s} \\ \vdots \quad \vdots \\ A_{t1} \cdots A_{ts} \end{pmatrix}$ and $B = \begin{pmatrix} B_{11} \cdots B_{1t} \\ \vdots \quad \vdots \\ B_{s1} \cdots B_{st} \end{pmatrix}$ and obtain matrix identities

$$\begin{pmatrix} G_1 \\ \vdots \\ G_t \end{pmatrix} = \begin{pmatrix} A_{11} \cdots A_{1s} \\ \vdots \quad \vdots \\ A_{t1} \cdots A_{ts} \end{pmatrix} \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix} = \begin{pmatrix} B_{11} \cdots B_{1t} \\ \vdots \quad \vdots \\ B_{s1} \cdots B_{st} \end{pmatrix} \begin{pmatrix} G_1 \\ \vdots \\ G_t \end{pmatrix}$$

If we consider the linear map $g\colon \mathbf{R}^t \to \mathbf{R}$ defined by

$$g(e_i) = G_i, \quad i = 1, \ldots, t,$$

and compute a system of generators $\{g_1, \ldots, g_l\}$ of $\mathrm{Syz}(G_1, \ldots, G_t\}$, using the second case. To get a system of generators of $\mathrm{Syz}(F_1, \ldots, F_s)$ we proceed as follows:

Let $h \in \mathrm{Syz}(G_1, \ldots, G_t)$, if $h = \sum_{i=1}^{t} H_i e_i$, we have the following matrix equation:

$$0 = (H_1 \cdots H_t) \begin{pmatrix} G_1 \\ \vdots \\ G_t \end{pmatrix} = (H_1 \cdots H_t) \begin{pmatrix} A_{11} \cdots A_{1s} \\ \vdots \quad \vdots \\ A_{t1} \cdots A_{ts} \end{pmatrix} \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix}.$$

Hence $(H_1 \cdots H_t) \begin{pmatrix} A_{11} \cdots A_{1s} \\ \vdots \quad \vdots \\ A_{t1} \cdots A_{ts} \end{pmatrix}$ is a syzygy for $F_1, \ldots, F_s$.

On the other hand, let us consider the following expression:

$$(1_s - BA) \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix} = \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix} - BA \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix} = \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix} - B \begin{pmatrix} G_1 \\ \vdots \\ G_t \end{pmatrix} = 0$$

Hence the rows $f_1, \ldots, f_s$ of the matrix $1_s - BA$ are syzygies for $F_1, \ldots, F_s$.

(2.4.3) Theorem.
With the above notation the family $\{g_1 A, \ldots, g_l A, f_1, \ldots, f_s\}$ *is a system of generators of* $\mathrm{Syz}(F_1, \ldots, F_s)$.

PROOF. Given $h \in \mathrm{Syz}(F_1, \ldots, F_s)$, $h = \sum_{j=1}^{s} H_j e_j$, we have

$$0 = (H_1, \ldots, H_s) \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix} = (H_1, \ldots, H_s) B \begin{pmatrix} G_1 \\ \vdots \\ G_t \end{pmatrix}$$

Hence $(H_1,\dots,H_s)B \in \mathrm{Syz}(G_1,\dots,G_t)$. As a consequence

$$(H_1,\dots,H_s)B = (Q_1,\dots,Q_l)\begin{pmatrix} g_1 \\ \vdots \\ g_l \end{pmatrix}$$

and

$$(H_1,\dots,H_s)BA = (Q_1,\dots,Q_l)\begin{pmatrix} g_1 \\ \vdots \\ g_l \end{pmatrix} A$$

Then we have:

$$\begin{aligned}(H_1,\dots,H_s) &= (H_1,\dots,H_s) - (H_1,\dots,H_s)BA + (H_1,\dots,H_s)BA \\ &= (H_1,\dots,H_s)(1_s - BA) - (H_1,\dots,H_s)BA \\ &= H_1,\dots,H_s)\begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix} + (Q_1,\dots,Q_l)\begin{pmatrix} g_1 \\ \vdots \\ g_l \end{pmatrix} A\end{aligned}$$

and the result follows. □

Four case.

Let us consider $f\colon \mathbf{R}^t \to \mathbf{R}^m$ defined by

$$f(e_i) = g_i, \quad 0 \neq g_i \in \mathbf{R}^m \quad i = 1,\dots,t,$$

being $\{g_1,\dots,g_t\}$ a Groebner basis in $\mathbf{R}^m$ and $\mathrm{lc}(g_i) = 1$ for any index i. Let $\mathrm{lm}(g_i) = X^{\alpha^i} l_{d_i} = X^{(\alpha^i,d_i)}$, $i = 1,\dots,t$, and define $X^{\gamma^{ij}}\delta_{d_i d_j}$ the minimum common multiple of $\mathrm{lm}(g_i)$ and $\mathrm{lm}(g_j)$. the s–polynomial of g_i and g_j is:

$$S(g_i,g_j) = \mathbf{q}^{-(\alpha^i,\gamma^{ij}-\alpha^i)} X^{\gamma^{ij}-\alpha^i}\delta_{d_i d_j} g_i - \mathbf{q}^{-(\alpha^j,\gamma^{ij}-\alpha^j)} X^{\gamma^{ij}-\alpha^j}\delta_{d_i d_j} g_j$$

Since $\{g_1,\dots,g_t\}$ is a Groebner basis, in the division of $S(g_i,g_j)$ we obtain:

$$\begin{aligned}&S(g_i,g_j) = \textstyle\sum_{h=1}^t Q_{ijh} g_h, \quad Q_{ijh} \in \mathbf{R} \\ &\mathrm{lm}(S(g_i,g_j)) = \max\{\mathrm{lm}(Q_{ijh} g_h):\ 1 \le h \le t\}\end{aligned}$$

and define

$$s_{ij} = \mathbf{q}^{-(\alpha^i,\gamma^{ij}-\alpha^i)} X^{\gamma^{ij}-\alpha^i}\delta_{d_i d_j} e_i - \mathbf{q}^{-(\alpha^j,\gamma^{ij}-\alpha^j)} X^{\gamma^{ij}-\alpha^j}\delta_{d_i d_j} e_j - \sum_{h=1}^t Q_{ijh} e_h;$$

it is clear that $s_{ij} \in \mathrm{Syz}(g_1,\dots,g_t)$.

(2.4.4) Proposition.
The set $\{\mathbf{q}^{-(\alpha^i,\gamma^{ij}-\alpha^i)}X^{\gamma^{ij}-\alpha^i}\delta_{d_id_j}e_{d_i}-\mathbf{q}^{-(\alpha^j,\gamma^{ij}-\alpha^j)}X^{\gamma^{ij}-\alpha^j}\delta_{d_id_j}e_{d_j}\colon\ 1\leq i<j\leq t\}$ *is a system of generators of* $\mathrm{Syz}(X^{(\alpha^i,d_i)}\colon\ 1\leq i\leq t)$.

PROOF. It is clear that each element is that set is a syzygy, as if $d_i\neq d_j$, then $\delta_{d_id_j}=0$, and if $d_i=d_j$, then

$$\mathbf{q}^{-(\alpha^i,\gamma^{ij}-\alpha^i)}X^{\gamma^{ij}-\alpha^i}e_{d_i}-\mathbf{q}^{-(\alpha^j,\gamma^{ij}-\alpha^j)}X^{\gamma^{ij}-\alpha^j}e_{d_i}=X^{\gamma^{ij}}e_{d_i}-X\gamma^{ij}e_{d_i}=0.$$

On the other hand, let $h=(H_1,\ldots,H_t)\,\mathrm{Syz}(X^{(\alpha^i,d_i)}\colon\ 1\leq i\leq t\}$. We have:

$$H_1X^{\alpha^1}l_{d_i}+\cdots+H_tX^{\alpha^t}l_{d_t}=0$$

We may assume that every H_i is homogeneous and it has the following form: $H_ic_iX^{\beta^i}$. Since $\{l_1,\ldots,l_m\}$ is a $\mathbf{R}$–basis, if we consider the $d_{i_1},\ldots,d_{i_s}$ such that $l_{d_{i_1}}=\cdots=l_{d_{i_s}}$, then we obtain a syzygy of $\{X^{\alpha^{i_1}},\ldots,X^{\alpha^{i_s}}\}$. Applying the first case we have that $\sum_{j=1}^s H_{i_j}e_{i_j}$ is generated by

$$\{\mathbf{q}^{-(\alpha^{i_j},\gamma^{jh}-\alpha^{i_j})}X^{\gamma^{jh}-\alpha^{i_j}}e_{i_j}-\mathbf{q}^{-(\alpha^{i_h},\gamma^{jh}-\alpha^{i_h})}X^{\gamma^{jh}-\alpha^{i_h}}e_{i_h}\colon\ 1\leq j<h\leq s\}.$$

We may repeat the process and finally we get the result. □

As a consequence we obtain

(2.4.5) Theorem.
With the above notation we have that $\{s_{ij}\colon\ 1\leq i<j\leq t\}$ *is a system of generators of* $\mathrm{Syz}(g_1,\ldots,g_t)$.

Fifth case.

Let us consider $f\colon\mathbf{R}^s\to\mathbf{R}^m$ defined by

$$f(e_j)=f_j,\quad 0\neq f_j\in\mathbf{R}^m,\quad j=1,\ldots,s.$$

In this case we compute a Groebner basis for the submodule of $\mathbf{R}^m$ generates by $f_1,\ldots,f_s$. Let $\{g_1,\ldots,g_t\}$ such a Groebner basis. As usual we may assume that $\mathrm{lm}(g_i)=1$ for any index *i*.

There exist matrices $A=(A_{ij})_{ij}$ and $B=(B_{ji})_{ji}$ with coefficient in $\mathbf{R}$ such that

$$\begin{pmatrix}g_1\\ \vdots\\ g_t\end{pmatrix}=\begin{pmatrix}A_{11}\cdots A_{1s}\\ \vdots\quad\ \vdots\\ A_{t1}\cdots A_{ts}\end{pmatrix}\begin{pmatrix}f_1\\ \vdots\\ f_s\end{pmatrix}\quad\text{and}\quad\begin{pmatrix}f_1\\ \vdots\\ f_s\end{pmatrix}=\begin{pmatrix}B_{11}\cdots B_{1t}\\ \vdots\quad\ \vdots\\ B_{s1}\cdots B_{st}\end{pmatrix}\begin{pmatrix}g_1\\ \vdots\\ g_t\end{pmatrix}$$

Let $x_1, \ldots, x_l$ be a system of generators of $\mathrm{Syz}(g_1, \ldots, g_t)$, then, as in the third case, for any index j we have that $x_j A$ is a syzygy of $f_1, \ldots, f_s$. Also the rows $y_1, \ldots, y_s$ of the matrix $1_s - BA$ are sysygies.

(2.4.6) Theorem.
With the above notation the set $\{x_1A, \ldots, x_lA, y_1, \ldots, y_s\}$ *is a system of generators of* $\mathrm{Syz}(f_1, \ldots, f_s)$.

Groebner bases for syzygies.

(2.4.7) Proposition. (Schreyer–1980)
Let $g_1, \ldots, g_s \in \mathbf{R}^t$ *and* $\preceq$ *be a monomial order in* $\mathbf{R}^t$. *We define a new order on monomial in* $\mathbf{R}^s$ *as follows:*

$$X^\alpha e_i \prec X^\beta e_j \text{ if } \begin{cases} \mathrm{lm}(X^\alpha g_i) \prec \mathrm{lm}(X^\beta g_j) \text{ or} \\ \mathrm{lm}(X^\alpha g_i) = \mathrm{lm}(X^\beta g_j) \text{ and } j < i \end{cases}$$

Then $\preceq$ *is a monomial order in* $\mathbf{R}^s$.

PROOF. It is clear that $\preceq$ is a total order on monomials in $\mathbf{R}^s$. To prove that it is a monomial order we proceed as follows:
(1) Given $0 \neq \alpha \in \mathbb{N}^n$ and $(\beta, i) \in \mathbb{N}^n_s$, then $\mathrm{lm}(X^\alpha X^\beta g_i) \succ \mathrm{lm}(X^\beta g_i$, hence $(\beta, i) \prec (\alpha + \beta, i)$.
(2) Given $\alpha \in \mathbb{N}^n$ and $(\beta^1, i_1) \prec (\beta^2, i_2) \in \mathbb{N}^n_s$, then
(2–a) If $\mathrm{lm}(X^{\beta^1} g_{i_1}) \prec \mathrm{lm}(X^{\beta^2} g_{i_2})$, then $\mathrm{lm}(X^\alpha X^{\beta^1} g_{i_1}) \prec \mathrm{lm}(X^\alpha X^{\beta^2} g_{i_2})$. Therefore $(\alpha + \beta^1, i_1) \prec (\alpha + \beta^2, i_2)$.
(2–b) If $\mathrm{lm}(X^{\beta^1} g_{i_1}) = \mathrm{lm}(X^{\beta^2} g_{i_2})$, then $\mathrm{lm}(X^\alpha X^{\beta^1} g_{i_1}) = \mathrm{lm}(X^\alpha X^{\beta^2} g_{i_2})$ and $i_2 < i_1$, therefore $(\alpha + \beta^1, i_1) \prec (\alpha + \beta^2, i_2)$.
(3) Given $\alpha \prec \beta \in \mathbb{N}^n$, for any index i we have $\mathrm{lm}(X^\alpha g_i) \prec \mathrm{lm}(X^\beta g_i)$. Therefore $(\alpha, i) \prec (\beta, i)$. □

The monomial order defined in the above Proposition is called the *monomial order induced* by $g_1, \ldots, g_s$ in $\mathbf{R}^s$.

(2.4.8) Theorem.
Let $\mathbb{G} = \{g_1, \ldots, g_t\}$ *be a Groebner basis in* $\mathbf{R}^m$, *then the system of generators* $\{s_{ij}\colon\ 1 \leq i < j \leq t\}$ *of* $\mathrm{Syz}(g_1, \ldots, g_t)$, *defined in Theorem (2.4.5) is a Groebner basis of* $\mathrm{Syz}(g_1, \ldots, g_t)$ *with respect to the monomial order in* $\mathbf{R}^t$ *induced by* $g_1, \ldots, g_t$. *In addition we have:*

$$\mathrm{lm}(s_{ij}) = X^{\gamma^{ij} - \alpha^i} e_i, \quad 1 \leq i < j \leq t, \quad \text{being } \mathrm{lm}(g_i) = X^{\alpha^i}.$$

PROOF. First we prove that $\mathrm{lm}(s_{ij}) = X^{\gamma^{ij}-\alpha^i}e_i$. Since

$$\mathrm{lm}(X^{\gamma^{ij}-\alpha^i}g_i) = \mathrm{lm}(X^{\gamma^{ij}-\alpha^j}g_j = X^{\gamma^{ij}},$$

and $i < j$, then we have $X^{\gamma^{ij}-\alpha^j}e_j \prec X^{\gamma^{ij}-\alpha^i}e_i$. Let X^α a monomial in a summand $Q_{ijh}e_h$, then we have:

$$\mathrm{lm}(X^\alpha g_h) \prec \mathrm{lm}(S(g_i,g_j)) \prec \mathrm{lm}(X^{\gamma^{ij}-\alpha^i}g_i).$$

Hence $X^\alpha e_h \prec X^{\gamma^{ij}-\alpha^i}e_i$.

Second we prove that in fact we obtain a Groebner basis. Let $h \in \mathrm{Syz}(g_1,\dots,g_t)$ defined by $h = \sum_{l=1}^t H_l e_l$, $H_l \in \mathbf{R}$ and let $\mathrm{lt}(H_l) = c_{\alpha^l}X^{\alpha^l}$, then $\mathrm{lm}(h) = X^{\alpha^i}e_i$ for some index i. We define

$$S = \{l \in \{1,\dots,t\}\colon\ \mathrm{lm}(X^{\alpha^l}g_l) = \mathrm{lm}(X^{\alpha^i}g_i)\}$$

For any $l \in S$ we have $l \geq i$. We define a new element in $\mathbf{R}^t$ as follows:

$$h' = \sum_{l\in S} c_l X^{\alpha^l}e_l$$

Since h is a syzygy then $\sum_{l\in S} c_l X^{\alpha^l}\mathrm{lt}(g_l) = 0$. Hence h' is a syzygy of $\{\mathrm{lt}(g_l)\colon\ l \in S\}$, in fact it is a syzygy of $\{\mathrm{lt}(g_1),\dots,\mathrm{lt}(g_t)\}$. We obtain that h' is generated by the set

$$\{\mathbf{q}^{-(\alpha^l,\gamma^{lh}-\alpha^l)}X^{\gamma^{lh}-\alpha^l}e_l - \mathbf{q}^{-(\alpha^h,\gamma^{lh}-\alpha^h)}X^{\gamma^{lh}-\alpha^h}e_h\colon\ l,h \in S,\ l < h\}$$

Let $h' = \sum_{lh} Q_{lh}\mathbf{q}^{-(\alpha^l,\gamma^{lh}-\alpha^l)}X^{\gamma^{lh}-\alpha^l}e_l - \mathbf{q}^{-(\alpha^h,\gamma^{lh}-\alpha^h)}X^{\gamma^{lh}-\alpha^h}e_h)$, $Q_{lh} \in \mathbf{R}$.

Since $\mathrm{lm}(h') = \mathrm{lm}(h) = X^{\alpha^i}e_i$, this term appears in the right side in the expression of h'. We obtain this term using the leader terms of Q_{lh}, hence we have:

$$\begin{aligned} &c_i X^{\alpha^i}e_i = \textstyle\sum_h \mathrm{lt}(Q_{ih})X^{\gamma^{ih}-\alpha^i}e_i,\\ &h \in S, \quad h > i, \quad X^{\alpha^i} = \mathrm{lm}(\mathrm{lt}(Q_{ih})X^{\gamma^{ih}-\alpha^i}) \end{aligned}$$

Therefore, there exists a summand, hence an index h, such that $\mathrm{lm}(s_i h) = X^{\gamma^{ih}\alpha^i}e_i$. As a consequence $\mathrm{lm}(s_{ih})$ divides $\mathrm{lm}(h)$, hence $\{s_{ij}\colon\ 1 \leq i < j \leq t\}$ is a Groebner basis. □

Bibliography

[1] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, 3, American Mathematical Society, 1994.

[2] T. Becker and V. Weispfenning, *Gröbner bases. A computational approach to commutative algebra*, Graduate texts in Mathematics, 141, Springer–Verlag, 1993.

[3] G. Bergman, *The diamond lemma for ring theory*, Adv. in Math. **29** (1978), 178–218.

[4] J. L. Bueso, F. Castro, and P. Jara, *Effective computation of the Gelfand–Kirillov dimension*, Proc. Edinburgh Math. Soc. (1997), 8 pp.

[5] F. Castro, *Calculs effectifs pour les ideaux d'opérateurs differentiels*, Géométrie Algébrique et Applications. Vol III, Hermann, 1987, pp. 1–20.

[6] D. Cox, J. J. Little, and D. O'Shea, *Ideals, varieties and algorithms*, Undergraduate Texts in Math., Springer–Verlag, 1992.

[7] T. Gateva-Ivanova and V. Latyshev, *On the recognizable properties of associative algebras*, J. Symb. Comput. **6** (1988), 371–388.

[8] M. Insa and F. Pauer, *Gröbner bases in rings of differential operators*, Gröbner Bases and Applications, London Math. Soc. Lect. Notes Series No. 251, 1998, pp. 259–280.

[9] P. Jara and J. Jódar, *An example of bernstein duality*, To appear in Advances in Math. Granada, 1998.

[10] A. Kandri-Rodi and V. Weispfenning, *Non–commutative Gröbner bases in algebras of solvable type*, J. Symb. Comp. **9** (1990), 1–26.

[11] S. P. Smith, *Quantum groups: An introduction and Survey for ring theorists*, Non Commutative Rings, S. Montgomery, L. Small (Editors). Mathematical Sciences Research Institute Publ., 24, 1991, pp. 131–178.

[12] V. Ufnarovski, *Combinatorial and asymptotic methods af algebra*, Algebra VI.(Encycl. Math. Sci., vol 57), Springer–Verlag, 1995.

[13] _____, *Introduction to noncommutative gröbner bases theory*, Gröbner Bases and Applications, London Math. Soc. Lect. Notes Series No. 251, 1998, pp. 259–280.

Index