Main purpose of these first talks is that of illustrating a theory which unifies various notions. In this way it will be easier to understand some fundamental concepts in Computer Algebra ,mostly that one of Gröbner bases. So let us start by recalling some of the main sources of our discussion.

§1 Standard bases, Macaulay bases, Gröbner bases.

A) Graded rings associated to ideals and standard bases

Let $(A,\mathfrak{m},k)$ be a local ring and let I be an ideal of A. If a is a non zero element of A, then the Krull Intersection Theorem guarantees the existence of a natural number n, such that $a \in I^n - I^{n+1}$. For technical reasons, which will be clear later on, let us denote by $v_I(a)$ the opposite of such number n. If we denote by $G = gr_I(A) = \oplus (I^n/I^{n+1})$, we immediately get two functions

$v : A - \{0\} \longrightarrow \mathbb{Z}$ defined by $v(a) = v_I(a)$

$F : A \longrightarrow G$ defined by $F(a) = \bar{a}$ in $I^{-v(a)} / I^{-v(a)+1}$ if $a \neq 0$ and $F(0) = 0$

Let us now consider a special situation , which nevertheless is of great importance: let $A = S/J$ where $S = k[X_1,\ldots,X_n]_{(X_1,\ldots,X_n)}$ $M = (X_1,\ldots,X_n)$ $\mathfrak{m} = M/J$, $I = \mathfrak{m}$: in this case one gets

$gr_M(S) \cong k[X_1,\ldots,X_n]$; $gr_I(A) \cong k[X_1,\ldots,X_n] / F(J)$,

where F(J) is the ideal generated by the initial forms of all the elements of J. However if $J = (f_1,\ldots f_r)$ then it is not necessarily true that $F(J) = (F(f_1),\ldots,F(f_r))$. This circumstance leeds naturally to the following

Definition An I-standard base of J is a finite set $\{f_1,\ldots,f_t\}$ of elements of J such that $F(J) = (F(f_1),\ldots,F(f_t))$.

Let us remark that the existence of standard bases is guaranteed by the fact that $gr_I(A)$ is noetherian (which is equivalent to the validity of the Artin-Rees lemma applied to the ideals M, J).

Therefore, in this situation, to "compute" G means to compute an M-standard base of J. The theory of the standard bases was initiated by Hironaka in his famous paper on the resolution of singularities **[Hironaka**, 1964] and it was developped from many other authors. For a systematic account and references on the standard bases see **[Robbiano-Valla**, 1983].

B) Compactification of affine schemes and homogeneization of ideals

Let $A = k[X_1,\dots,X_n]$ and let $\mathbf{X} \subset \mathbb{A}^n$ be an affine variety of ideal $J = I(\mathbf{X}) \subset \mathbb{A}^n$. We can embed $\mathbb{A}^n$ as the standard open set $X_0 \neq 0$ in $\mathbb{P} = \mathbb{P}(1,q_1,\dots,q_n)$, the weighted projective space with weights $1,q_1,\dots,q_n$ (For instance, when $q_1=\dots=q_n=1$, then $\mathbb{P}$ is the ordinary projective space). The projective closure $\overline{\mathbf{X}}$ of $\mathbf{X}$ in $\mathbb{P}$ is defined by the ideal $J(\overline{\mathbf{X}}) = {}^hJ$ of $k[X_0,\dots,X_n]$ where ${}^hJ$ denotes the homogeneization of J with respect to the homogenizing variable X_0 of weight 1.

Definition An H-base (Macaulay base) of J is a finite set $\{f_1,\dots,f_t\}$ of elements of J such that $H(J) = (H(f_1),\dots H(f_t))$, where $H(f_i)$ denotes the highest degree form in the expansion of f_i and $H(J)$ denotes the ideal generated by the highest degree forms of all the elements of J.

Proposition 1.1 If $\{f_1,\dots,f_t\}$ is an H-base of J, then ${}^hJ = ({}^hf_1,\dots,{}^hf_t)$.

Proof (Hint). One sees that ${}^hJ = ({}^hf_1,\dots,{}^hf_t) + X_0\,{}^hJ$ and then one concludes by using the graded Nakayama Lemma.■

(We observe that also the converse is true, and it is easy to prove it, but we do not need it in the following).

Therefore, in this situation, to "compute" $\overline{\mathbf{X}}$ means to compute a suitable H-base.

C) Computation of a "canonical" base of the k-vectorspace $k[X_1,\dots,X_n]/J$.

In his thesis [**Buchberger**, 1965] Buchberger solved the problem, posed by Gröbner, of determining a base of the k-vectorspace $k[X_1,\dots,X_n]/J$, by introducing the concept of the so called Gröbner-bases (G-bases) and by giving an explicit algorithm for their computation. Since, as we shall see, this concept plays a fundamental role in Computer Algebra, let us describe it.

Let $\mathbf{T}$ be the set of the terms in $k[X_1,\dots,X_n]$, where term means monomial with coefficient 1. Then $\mathbf{T}$ is a multiplicative semigroup with identity.
Let us denote by log the canonical injective homomorphism

$$\log : \mathbf{T} \longrightarrow \mathbb{Z}^n \quad \text{where} \quad \log(X_1^{t(1)}\cdots X_n^{t(n)}) = (t(1),\dots,t(n))$$

This homomorphism identifies $\mathbf{T}$ with $\mathbb{N}^n$.

§2 Graded structures and generalized standard bases.

In this section we are going to give some account on the theory of graded structures which was developed in [**Robbiano**, 1986], and which has, among its features,the property of giving some systematic and unifying treatment of the subjects mentioned in §1. We are not going to handle all the technicalities of the theory, but only to report loosely on its main achievements (see [**Robbiano**, 1986] and [**Robbiano**, 1985]) .

A) Graded structures

In every situation we have discussed so far, we always dealt with a composite object of type

$$\mathbb{A} = (A,\Gamma,v,G,F) \quad \text{where}$$

A is a commutative ring with 1,

$(\Gamma,<)$ is a totally ordered abelian group,

$v : A - \{0\} \longrightarrow \Gamma$ is a function, such that Γ is generated by $Im(v)$,

$F : A \longrightarrow G$ is a function,

and the five components of $\mathbb{A}$ are linked together by some suitable eight axioms (nine axioms if A is a k-algebra over a field k) .

For instance in the case of the theory which leeds to the notion of H-bases, A is $k[X_1,\ldots,X_n]$, Γ is $\mathbb{Z}$ with the usual ordering, G is $k[X_1,\ldots,X_n]$ with the graduation induced by the total degree with respect to some preassigned weights $q_1,\ldots,q_n$ of the variables, v is the function which sends a non zero polynomial to its degree, F is the function which sends 0 to 0 and a non zero polynomial to its maximum form with respect to the total degree.

Alternatively,we can say that in every situation we have discussed so far, we always dealt with a composite object of type

$$\mathbb{A}' = (A, \Gamma, F_A) \quad \text{where}$$

A is a commutative ring with 1,

$(\Gamma,<)$ is a totally ordered abelian group,

$F_A = (F^\gamma(A), \gamma\in\Gamma)$ is an increasing valued filtration in groups of A, i.e. an increasing filtration in groups of A, such that for every $a\neq 0$ there exists a minimum γ with $a\in F^\gamma(A)$.

We observe that, if we want to use increasing filtrations, we are induced to define $v_I(a)$ as the opposite of the usual $v_I(a)$, in the case of filtrations given

Definition A term-ordering on $A = k[X_1,\dots,X_n]$ is a total ordering $<$ on $\mathbb{Z}^n$ such that

1) $(\mathbb{Z}^n,<)$ is an ordered group
2) $\log(T) = \mathbb{N}^n \subset (\mathbb{Z}^n)^+$, where $(\mathbb{Z}^n)^+$ denotes the set of vectors of $\mathbb{Z}^n$, which are non negative with respect to $<$.

Given a term-ordering on A, to every polynomial f we may associate its maximum term, which we denote by $T(f)$, and to every ideal J in A we may associate the ideal $T(J)$ generated by the maximum terms of all the polynomials in J. Hence we get two functions

$v : A - \{0\} \longrightarrow \mathbb{Z}$ defined by $v(f) = \log(T(f))$

$F : A \longrightarrow G$ defined by $F(f) = T(f)$

Definition A G-base (Gröbner base) of J is a finite set $\{f_1,\dots,f_t\}$ of non zero elements of J such that equivalently

1) $T(J) = (T(f_1),\dots T(f_t))$
2) Every non zero element f of J can be represented as $f = \Sigma a_i f_i$ where $v(f) \geq v(a_i) + v(f_i)$ for every i such that $a_i \neq 0$.

The equivalence of these two properties will be discussed later (see Theorem 2.8)

Corollary 1.2 G-bases exist

Proof. It follows immediately from 1).∎

It should be remarked that in the literature sometimes G-bases are called standard bases.
In the next talks it will be shown that G-bases are the main tool for performing some basic operations on the ideals of A and for solving some fundamental computational problems in Commutative Algebra. Finally, since that topic will not be treated, let me remind that G-bases were applied to some questions of set-theoretic complete intersections (see [Robbiano-Valla, preprint]).

Proposition 2.5 Let A be a noetherian structure. Then $\Gamma^0(A)$ generates a finitely generated semigroup and Γ is isomorphic to $\mathbb{Z}^n$.

The proof relies on a result of [**Goto-Yamagishi**, 1982].■

Basic example Let $A = (A,\Gamma,v,G,F)$ be a graded structure and $M = (M,\Gamma,w,T,\Phi)$ an A-module. Let us choose $\{m_1,\dots,m_r\}$ to be a set of non zero elements of M; let A^r be the free module of rank r over A, whose canonical base we denote by $(e_1,\dots,e_r)$. Let $w_i = w(m_i)$ and let $w^+ : A^r-\{0\} \longrightarrow \Gamma$ be defined in the following way

$$w^+(a_1,\dots,a_r) = \max\{v(a_i)+w_i\} \quad a_i \neq 0$$

To w^+ we associate a filtration on A^r as we did in Proposition 2.1; this turns out to be a valued filtration. Then we get an associated graded G-module, which turns out to be $\oplus_i G(-w_i)$, $i=1,\dots,r$ and a map $F^+ : A^r \to \oplus_i G(-w_i)$ which is defined by $F^+(a_1,\dots,a_r) = (F'(a_1),\dots,F'(a_r))$ where

$$F'(a_i) = \begin{cases} 0 \text{ if } a_i=0 \text{ or } v(a_i)+w_i < w^+(a_1,\dots,a_r) \\ F(a_i) \text{ if } v(a_i)+w_i = w^+(a_1,\dots,a_r) \end{cases}$$

We denote by $L(w_1,\dots,w_r)$ or by $\oplus A(-w_i)$ the A-module $(A^r,\Gamma,w,\oplus_i G(-w_i), F^+)$. Then the A-homomorphism $\lambda : A^r \longrightarrow M$ defined by $\lambda(e_i) = m_i$ induces an A-morphism of $L(w_1,\dots,w_r)$ in M and the corresponding graded G-homomorphism $\Lambda : \oplus_i G(-w_i) \longrightarrow T$ is defined by $\Lambda(e_i) = \Phi(m_i)$ (here $(e_1,\dots,e_r)$ is the canonical base of $\oplus_i G(-w_i)$). This morphism $(\lambda,\Lambda) : L(w_1,\dots,w_r) \longrightarrow M$ is called the canonical morphism associated to $m_1,\dots,m_r$.

Definition An A-module L is said to be finite free if it is isomorphic to an A-module of type $L(w_1,\dots,w_r)$.

At this point the theory needs the introduction of a quite technical notion, which is essential for several purposes: it is the notion of Krull-module over a noetherian structure. The reader can check the paper [**Robbiano**, 1986] for the details. Let me only say that this notion is a suitable generalization of the Krull intersection property of finitely generated modules over local rings.

by powers of ideals.

Definition A quintuple $\mathbf{A} = (A,\Gamma,v,G,F)$, where the components satisfy the eight axioms, is termed a graded structure on A.
A triple $\mathbf{A}' = (A, \Gamma, F_A)$ where the components satisfy the properties described before is termed a v-filtered structure .

Proposition 2.1 To every graded structure $\mathbf{A} = (A,\Gamma,v,G,F)$ on A it is canonically associated a v-filtered structure $\mathbf{A}^* = (A, \Gamma, F_A)$ on A ,where F_A is the filtration defined by $F^\gamma(A) = \{ a\in A / v(a) \leq \gamma\} \cup \{0\}$.■

Proposition-Definition 2.2 $Im(v) = \{v\in\Gamma / G^\gamma \neq 0\}$
This set generates the group Γ and it is denoted by $\Gamma^*(\mathbf{A})$.■

The proof of these facts easily follows from the axioms.■

Proposition 2.3 If $\mathbf{A}$ is a graded or a v-filtered structure and $\Gamma^0(\mathbf{A}) \leq 0$ then $F^\gamma(A)$ is an ideal for every $\gamma\in\Gamma$.

The proof of this fact is again an immediate consequence of the axioms and it shows a first difference between the case of standard bases and the case of H-bases and G-bases.■

Over these "objects" $\mathbf{A}$, $\mathbf{A}^*$ it is possible to define "modules" $\mathbf{M}$, $\mathbf{M}^*$ and morphisms between them and one gets two categories "$\mathbf{A}$-modules" and "$\mathbf{A}^*$-modules ".
It turns out that the axioms are such that the following statement holds true

Theorem 2.4 Given a graded structure $\mathbf{A}$ and its associated v-filtered structure $\mathbf{A}^*$, the categories "$\mathbf{A}$-modules " and "$\mathbf{A}^*$-modules " are equivalent .■

This fact, whose proof is not too difficult, allows us to treat the two notions in some sense interchangeably. This is quite important for applications, and we feel free to use the symbols $\mathbf{A}$ and $\mathbf{M}$ both for graded and filtered structures and modules over them.

In the following when we say that $\mathbf{A}$ has a property, we mean that both rings A and G have that property and the same for $\mathbf{M}$.

And then we have the following main

Theorem 2.8 Let us consider the following conditions
a) $\{ m_1,\dots,m_r \}$ is a std-base of M .
b) $(\Phi(m_1),\dots,\Phi(m_r))$ is a base of T as a G-module .
Then a) $\Rightarrow$ b) and if M is a Krull A-module , then a) $\Leftarrow\Rightarrow$ b).■

Corollary 2.9 If A is a noetherian graded structure, then every finitely generated Krull A-module does have std-bases.■

The Krull condition plays also a fundamental role in the next theorems

Theorem 2.10 If A is a strong Krull structure and M is a finite Krull A-module , then M has a finite free resolution.

Theorem 2.11 Let A be a strong Krull structure. Let $M = (M,\Gamma,w,T,\Phi)$ be a finite Krull A-module and $m_1,\dots,m_r$ be non zero elements which generate M. Let $w_i = w(m_i)$, $i = 1,\dots,r$, and let (λ,Λ): $L(w_1,\dots,w_r) \longrightarrow M$ be the canonical morphism associated to $m_1,\dots,m_r$ (see the basic example at pag. 6). Then the following conditions are equivalent
1) (λ,Λ) is an epimorphism
2) Λ is surjective
3) For every homogeneous non zero element $\sigma \in \mathrm{Ker}(\Lambda)$, there exists an element $s \in \mathrm{Ker}(\lambda)$, such that $\Phi^+(s)=0$
4) There exists a homogeneous base $\{\sigma_1,\dots,\sigma_t\}$ of $\mathrm{Ker}(\Lambda)$ and elements $s_1,\dots,s_t \in \mathrm{Ker}(\lambda)$ such that $\Phi^+(s_i) = \sigma_i$.
5) $\{ m_1,\dots,m_r \}$ is a std-base of M.■

This theorem is a generalization of both a theorem of [**Robbiano-Valla**, 1983] on standard bases in local rings and a theorem of [**Buchberger**, 1976] on critical pairs and Gröbner bases

B) Morphisms of graded structures. Double structures.

It is possible to define morphisms between graded structures; however a lot of pathologies can occur. Therefore we skip the discussion of the general situation. We consider instead a special one, which is nevertheless suitable for many applications.

Definition A noetherian structure A such that every finite free A-module is a Krull A-module is termed a strong Krull structure .

For applications to the theory of Gröbner and Macaulay-bases , and also for the study of standard bases the following theorem is essential, because it implies that in these cases we can forget about the Krull condition. Namely we have

Theorem 2.6 a) Let A be a graded noetherian structure such that $\Gamma^0(A) \geq 0$. Then every finite A-module is a Krull-module; in particular A is a strong Krull-structure.
b) Let A be a graded structure over a local ring A, such that $\Gamma^0(A) = -\mathbb{N}$, $F_{-n}A = I^n$, where I is an ideal of A. Then A is a strong Krull structure.

The proof of part a) depends upon the description of the orderings on $\mathbb{Z}^n$, which will be discussed later.∎

The first achievement of the notion of Krull module is the following

Proposition 2.7 Let A be a noetherian structure, M a Krull A-module and let N be a submodule of M . Then
1) N is a Krull A-module .
2) The filtration induced on M/N is valued, hence M/N is an A-module and $\Gamma^0(M/N) \subset \Gamma^0(M)$.
3) M/N is a Krull A-module .
4) If A is a strong Krull structure and I is a submodule of A, then A/I is a strong Krull structure.∎

Now we come to one of the basic notions

Definition Let $M = (M,\Gamma,w,T,\Phi)$ be a finitely generated A-module, and let $m_1,\ldots,m_r$ be non zero elements of M. We say that $\{m_1,\ldots,m_r\}$ is a generalized standard base (std-base) of M if for every $m \in M$ we have
$m = \Sigma a_i m_i$ with $w(m) \geq v(a_i) + w(m_i)$ for every i such that $a_i \neq 0$.

§3 Orderings on $\mathbb{Z}^n$. An application to flat families.

In this section we report on some results of [**Robbiano**, 1985] and some other unpublished results, which give a description of the orderings on $\mathbb{Z}^n$. This is important for several reasons; namely special orderings (term-orderings) on $\mathbb{Z}^n$ are used to define Gröbner bases (see §1) and moreover $\mathbb{Z}^n$ equipped with an ordering came into play also in the general theory of graded structures (see §2). In the following, when we speak about an ordering $<$ on a commutative group G, we mean that $(G,<)$ is an ordered group i.e. the ordering $<$ is compatible with the sum in G.

Lemma 3.1 Every ordering $<$ on $\mathbb{Z}^n$ uniquely extends to an ordering $<$ on $\mathbb{Q}^n$.

Proof. Given $v = (q_1,\ldots,q_n) \in \mathbb{Q}^n$ let $m\in\mathbb{N}^+$ be such that $mv\in\mathbb{Z}^n$. Then $v>0$ iff $mv>0$.■

Let us now consider the subset V of $\mathbb{R}^n$ of the vectors v such that for every open nbh. U(v) of v in the euclidean topology, $U(v)\cap(\mathbb{Q}^n)^+$ and $U(v)\cap(\mathbb{Q}^n)^-$ are non-empty.

Lemma 3.2 V is a subvectorspace of $\mathbb{R}^n$ of dimension n-1.

Proof. To see that V is a subvectorspace is an easy exercise. By using the obvious map $\mathbb{R}^n\setminus V \longrightarrow \{-1,1\}$ with the discrete topology, we see that $\mathbb{R}^n\setminus V$ is disconnected ,if not empty. On the other hand $\mathbb{R}^n\setminus V$ cannot be empty since at least one "octant" of $\mathbb{R}^n$ is "positive". So the dimension of V has to be n-1.■

Definition Given a vector $v\in\mathbb{R}^n$ we denote by d(v) the dimension of the $\mathbb{Q}$-subvectorspace of $\mathbb{R}$ spanned by the coordinates of v.

Definition On $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{Z}^n$ we call lexicographic (lex) the ordering defined by: $(a_1,\ldots,a_n) > 0$ iff the first non zero coordinate from the left is positive.

So let $\mathbf{A}_\Gamma = (A,\Gamma,v,G(\Gamma),F_\Gamma) = (A, \Gamma, F(\Gamma)_A)$, $\mathbf{A}_\Delta = (A,\Delta,w,G(\Delta),F_\Delta) = (A, \Delta, F(\Delta)_A)$ be two graded structures on the same ring A, and let $\alpha : \Gamma \longrightarrow \Delta$ be an ordered homomorphism, such that $w(a) = \alpha(v(a))$ for every $a \neq 0$.

Definition The triple $\mathbf{A}_\alpha = (\mathbf{A}_\Gamma, \mathbf{A}_\Delta, \alpha)$ with the properties described above is termed a double structure on A .

Let now $\mathbf{M} = (\mathbf{M}_\Gamma, \mathbf{M}_\Delta)$, where $\mathbf{M}_\Gamma = (M,\Gamma,w_\Gamma,T(\Gamma),\mathfrak{F}_\Gamma)$, $\mathbf{M}_\Delta = (M,\Delta,w_\Delta,T(\Delta),\mathfrak{F}_\Delta)$ and α has the property that $\alpha(w_\Gamma(m)) = w_\Delta(m)$ for every $m \neq 0$; then we say that $\mathbf{M}$ is a module over $\mathbf{A}_\alpha$ and we define $G(\Gamma)_\Delta = \oplus_\delta G(\Gamma)_{\Delta,\delta}$ and $T(\Gamma)_\Delta = \oplus_\delta T(\Gamma)_{\Delta,\delta}$ where $G(\Gamma)_{\Delta,\delta} = \oplus G(\Gamma)_\gamma$ and $T(\Gamma)_{\Delta,\delta} = \oplus T(\Gamma)_\gamma$ and these direct sums are taken over all the γ's such that $\alpha(\gamma)=\delta$. So we are ready to state the following main

Theorem 2.12 Let $\mathbf{A}_\alpha$ be a noetherian double structure on A, and let $\mathbf{M}$ be a finitely generated $\mathbf{A}_\alpha$-module; let S be the semigroup generated by $\Gamma^0(\mathbf{A}_\Gamma)$ and assume that $\mathrm{Ker}(\alpha) \cap S = \{0\}$. Then

1) $G(\Gamma)_0 = G(\Delta)_0$ and we shall denote it by G_0 .

2) If [...] denotes the image in the Grothendieck group of finitely generated G_0-modules , then

$$[T(\Gamma)_{\Delta,\delta}] = [T(\Delta)_\delta] \text{ for every } \delta \in \Delta^0(\mathbf{M}_\Delta). \blacksquare$$

As a corollary we get a result, whose direct proof is anyhow much easier

Corollary 2.13 Let $A = k[X_1,\dots,X_n]$, I an ideal of A. Let T(I) denote the ideal generated by the maximal terms of the elements of I, with respect to an ordering on $\mathbb{Z}^n$, whose first vector is $u_1=(q_1,\dots,q_n)$ (this assumption will be clear a little later) and let F(I) denote the ideal generated by the forms of maximum degree of the elements of I, where $\deg(X_i)= q_i$.
Let A/T(I) and A/F(I) be considered as graded over $\mathbb{N}$ by the graduations induced by the graduation on A defined by the total degree, where $\deg(X_i)= q_i$.
Finally let H(A/T(I)), H(A/F(I)) be the Hilbert functions.
Then $H(A/T(I)) = H(A/F(I))$.

This a generalization of an old theorem of Macaulay (see [**Macaulay**, 1926]). $\blacksquare$

Remark We must be careful about the word "lexicographic"; it looks like reminding the order of the words in the dictionary. However in a dictionary one reeds a before aa and aab before ab and this relations are clearly incompatible. However, within a set of words having the same length, if we understand " > " as "precedes in the dictionary" then the ordering in the dictionary is the same as the lexicographic ordering induced by $a > b > c > \ldots$ as we described at the beginning of Example 1.

Example 2 Reverse lexicographic ordering (rev. lex).
The reverse lexicographic ordering on $\mathbb{Z}^n$ is defined by:
$(q_1,\ldots,q_n) > 0$ iff the first non zero coordinate from the right is negative.
Then it is clear that rev.lex = $(-e_n,\ldots,-e_1)$.
Then again $X_1 > X_2 > \ldots > X_n$ but $X_i < 1$ for each i and it is not a term-ordering.

Example 3 Degree-compatible orderings (see Corollary 2.13).
If a term-ordering is given such that $d_1 = 1$, then the first vector u_1 of $<$ can be chosen in such a way that $u_1=(q_1,\ldots,q_n)\in\mathbb{Z}^n$; then, given two terms M, N of $k[X_1,\ldots,X_n]$ we get $M<N$ if deg(M) < deg(N), where the degree is computed after endowing the variables $X_1,\ldots,X_n$ with the weights $q_1,\ldots,q_n$ respectively. Of course if deg(M) = deg(N) then we must look at the next vectors in the sequence characterizing $<$. For instance the term-ordering given by the following rule: M > N if either deg(M) > deg(N) (degree computed with respect to $\deg(X_i)=1$ for every i) or deg(M) = deg(N) and M > N in the lexicographic ordering generated by $X_1 > \ldots > X_n$, is given by the sequence of vectors $(u_1,\ldots,u_n)$ where $u_1 = (1,1,\ldots,1)$, $u_2 =(n-1,-1,\ldots,-1),\ldots\ldots$, $u_{n-1} = (0,\ldots,0,2,-1,-1)$, $u_n = (0,\ldots,0,1,-1)$, or by the sequence of vectors $(v_1,\ldots,v_n)$ where $v_1 = u_1$, $v_2 = (1,0,\ldots,0),\ldots,v_n = (0,\ldots0,1,0)$ (see the remark following Theorem 3.4).
For instance if n=3 and we denote X_1 by X, X_2 by Y, X_3 by Z we get
(*) $\quad 1 < Z < Y < X < Z^2 < YZ < Y^2 < XZ < XY < X^2$

Instead, the term-ordering given by the following rule: M > N if either deg(M) > deg(N) (degree computed with respect to $\deg(X_i)=1$ for every i) or deg(M) = deg(N) and M > N in the rev.lex ordering generated by $X_1 > \ldots > X_n$ is given by

A suitable use of Lemma 3.2 leeds to the following

Theorem 3.3 Given an ordering $<$ on $\mathbb{Q}^n$, then there exist an integer s with $1 \leq s \leq n$, and s orthogonal vectors $u_1,\ldots u_s$ such that $d(u_1)+\ldots d(u_s)=n$, and such that the map

$\alpha : (\mathbb{Q}^n,<) \longrightarrow (\mathbb{R}^s,\text{lex})$ given by $\alpha(v) = (v\cdot u_1,\ldots, v\cdot u_s)$

is an injective ordered homomorphism.■

If we denote by $s(<)$ the integer which arises in Theorem 3.3 we get

Theorem 3.4 The orderings $<$ on $\mathbb{Z}^n$ and on $\mathbb{Q}^n$ are classified by:
- an integer $s(<)$;
- a partition $(d_1,\ldots,d_s)$ of n;
- a sequence $(u_1,\ldots,u_s)$ of orthogonal unitary vectors of $\mathbb{R}^n$, such that $d(u_i)=d_i$ and such that u_i belongs to $G_{i-1}\otimes\mathbb{R}$, where G_{i-1} is the $\mathbb{Q}$-subvectorspace of $\mathbb{Q}^n$ of the vectors orthogonal to $(u_1,\ldots,u_{i-1})$ (here $G_{-1} = \mathbb{Q}^n$).

The extra condition that the first (from the left) non zero coordinate of $(v\cdot u_1,\ldots, v\cdot u_s)$ is positive for every $v\in\mathbb{N}^n\setminus\{0\}$ characterizes the term-orderings .■

Remark Elementary considerations show that also a sequence $(u_1,\ldots,u_s)$ of vectors which are not orthogonal can define an ordering: for, it is sufficient that the sequence $(\bar{u}_1,\ldots,\bar{u}_s)$, which is obtained from $(u_1,\ldots,u_s)$ by orthonormalizing , is one of the sequences described in Theorem 3.5.

Definition Given s vectors $u_1,\ldots,u_s$ which define an ordering $<$, we say that $< = (u_1,\ldots,u_s)$ and that $u_i = u_i(<)$

Example 1 Lexicographic ordering (lex.) .
We have already seen that the lexicographic ordering on $\mathbb{Z}^n$ is defined by : $(q_1,\ldots,q_n) > 0$ iff the first non zero coordinate from the left is positive.
Then it is clear that $\text{lex} = (e_1,\ldots,e_n)$ where $e_1 = (1,0,\ldots,0)$, $e_2 = (0,1,0,\ldots,0)$,....., $e_n = (0,\ldots,0,1)$.
This means that if we assume, as usual (see §1 C)), that $\log(X_1) = (1,0,\ldots,0),\ldots\ldots,\log(X_n) = (0,\ldots,0,1)$, then $X_1 > X_2 >\ldots> X_n$.
For instance if $n=3$ and we denote X_1 by X, X_2 by Y, X_3 by Z we get
$1 < Z < Z^2 < Z^3 < \ldots < Y < YZ < YZ^2 < YZ^3 < \ldots Y^2 < Y^2Z < Y^2Z^2 <\ldots< X < XZ$.

Corollary 3.6 Let U be a finite set of vectors of $\mathbb{Z}^n$, $<$ a total ordering on U. Then either the set of orderings on $\mathbb{Z}^n$, which induce $<$ on U, is empty, or its cone has dimension n.

Proof. Let $U = \{u_1,\dots,u_r\}$ and assume that $u_1<\dots<u_r$. Then let $E = \{u_2-u_1,\dots,u_n-u_{n-1}\}$ and apply the theorem 3.5.■

Remark We observe that the term-orderings are nothing but the orderings which are positive on $\{e_1,\dots,e_n\}$.

Corollary 3.7 Let E be a finite set of vectors and let $<$ be a term-ordering, which is positive on E. Then, if Σ denotes the set of the term-orderings positive on E, $C(\Sigma)$ is contained in the first "octant", and $\dim(C(\Sigma)) = n$. Therefore there are infinite sets of weights $(q_1,\dots,q_n)$, such that the hierarchy of inequalities induced by $<$ on E is the same as that one induced by the degrees of the elements of E computed with respect to the weights $(q_1,\dots,q_n)$ given to the variables.■

As a very important application of the preceding discussion, we prove the following Theorem (see [**Bayer**, 1982].

Theorem 3.8 Let k be a field, $A = k[X_1,\dots,X_n]$, I an ideal of A. Let $<$ be a termordering on A and let T(I) be the ideal generated by the maximum terms of the elements of I. Then A/T(I) is a special fiber of a flat family parametrized by k[t], where all the other fibers over closed points are isomorphic to I. In particular, if I is homogeneous with respect to a set of weights $(q_1,\dots,q_n)$ of the variables, and $u_1(<) = (q_1,\dots,q_n)$, then the Hilbert function is constant on the fibers (see Corollary 2.13).

Proof. Let $\{f_1,\dots,f_t\}$ be a G-base of I with respect to $<$ and let Σ denote the set of the term-orderings on A which yield the same hierarchy of inequalities as that induced by $<$ on all the terms of $f_1,\dots,f_t$. By Corollary 3.7 we get a set of weights $(q_1,\dots,q_n)$ such that the hierarchy is the same. Let us denote by σ an ordering having $q = (q_1,\dots,q_n)$ as first vector.
An easy consequence of the algorithm of Buchberger for computing G-bases is that $\{f_1,\dots,f_t\}$ is also a G-base of I with respect to σ.

the sequence of vectors $(u_1,\ldots,u_n)$ where $u_1 = (1,1,\ldots,1)$, $u_2 = (1,1,\ldots,1,-n+1),\ldots\ldots$, $u_{n-1} = (1,1,-2,0,\ldots,0)$, $u_n = (1,-1,0,\ldots 0)$, or by the sequence of vectors $(v_1,\ldots,v_n)$ where $v_1=u_1$, $v_2 = (0,0,\ldots,-1),\ldots$ $\ldots v_n = (0,-1,0,\ldots,0)$.
For instance if n=3 and we denote X_1 by X, X_2 by Y, X_3 by Z we get
$1 < Z < Y < X < Z^2 < YZ < \mathbf{XZ < Y^2} < XY < X^2$.

Example 4 Let us consider the ordering $<$ on $\mathbb{Z}^3$ given by (u_1,u_2,u_3) where $u_1 = (1,1,1)$, $u_2 = (4,2,1)$, $u_3 = (0,1,1)$. Then with respect to $<$ the relations given by (*) above hold.
However, while here $\mathbf{XZ^3 < Y^4}$, there $\mathbf{XZ^3 > Y^4}$.

Example 5 If u is the real vector $(\pi^n, \pi^{n-1},\ldots,\pi,1)$, then u defines an archimedean ordering on $\mathbb{Z}^n$ and $\mathbb{Q}^n$ such that $X_1 > X_2 > \ldots > X_n$.

Definition Given a set Σ of orderings on $\mathbb{Z}^n$, we may associate to it a cone, which is denoted by $C(\Sigma)$ and which is the cone generated by the first vectors of the orderings of Σ . These cones will be referred as "cones of orderings ".

Let now $E = \{v_1,\ldots,v_r\}$ be a finite set of vectors in $\mathbb{Z}^n$, and let Σ be the set of orderings positive on E. Let $C(\Sigma)$ be the cone of Σ, and let Γ be the dual cone of E, i.e. the cone $\{v \,/\, v\cdot v_i \geq 0$ for every $i = 1,\ldots,r\}$. An easy application of the theory of cones yields the following

Theorem 3.5 If Γ^0 denotes the interior of Γ, the following conditions hold true

a) $\Gamma^0 \subseteq C(\Sigma) \subseteq \Gamma$

b) $\dim(\Gamma) < n \Rightarrow \Sigma = \emptyset$

c) $\dim(\Gamma) = n \Rightarrow C(\Sigma) = \Gamma$. ∎

Example Let n=2 $E = \{e_1\}$ Then $\Gamma = \{(x,y) \,/\, x \geq 0\}$, $C(\Sigma) = \Gamma$.
On the "edge" of Γ we have 4 orderings; namely $<_1$, $<_2$, $<_3$, $<_4$, where $<_1 = (e_2,e_1)$, $<_2 = (-e_2,e_1)$, $<_3 = (e_2,-e_1)$, $<_4 = (-e_2,-e_1)$ and $<_1,<_2 \in C(\Sigma)$, while $<_3,<_4 \notin C(\Sigma)$.

§4 Characterizations of Gröbner bases

A) Characterizations related to semigroups

Let $A:=k[X_1,\dots,X_n]$ be a polynomial ring over a field k, let **T** denote the semigroup of terms (monic monomials), and let $<$ be a semigroup total ordering on **T**; let **M** be the semigroup of non-zero monomials, $\mathbf{M}:= k^*\times\mathbf{T}$. Then each polynomial $f\in A^*$ (we will use the following notation: if G is a subset of a ring we will denote $G^*:=\{ g\in G \,/\, g\neq 0 \}$) can be written in a unique way as:

$$f = \Sigma\, c_i m_i,\ c_i\in k^*,\ m_i\in\mathbf{T},\ m_1>m_2>\dots$$

Denote : $T(f) := m_1$, $\mathbf{lc}(f) := c_1$, $M(f) := c_1 m_1$.

If $F \subset A$, denote $T\{F\} := \{T(f) \,/\, f\in F^*\}$, $M\{F\} := \{M(f) \,/\, f\in F^*\}$, M(F) the ideal in A generated by M{F}.

We recall that if U is a subset of a commutative semigroup S, it is called a semigroup ideal if, for every $s\in S$, for every $u\in U$, $su\in U$.

Proposition 4.1 If $I\subset A$ is an ideal, and $F\subset I^*$, the following conditions are obviously equivalent:

A1: T{F} generates the semigroup ideal $T\{I\}\subset\mathbf{T}$

A2: M{F} generates the semigroup ideal $M\{I\}\subset\mathbf{M}$

A3: M(F) = M(I). ∎

(*cf.* the definition of G-base on page 3, where the first equivalent condition is **A3**)

All the definitions given above hold, however, also if A is the semigroup ring k[**T**], **T** a semigroup ordered by $<$, k an integral domain; in this context however the three conditions listed above are no more equivalent (**A2** and **A3** lead then to different generalizations of Gröbner bases, while **A1** is interesting only if k is a field, being then equivalent to **A2**) and only the implication **A2** ⇒ **A3** holds, as it is clearly shown by the following example in $\mathbb{Z}[X,Y]$:

$$F := \{3X,2Y\},\ G := \{3X,2Y,XY\},\ I := (F) = (G)$$

where F satisfies **A3** but not **A2**, while G satisfies both.

Let us now consider $A[t]$ and let us extend the term-ordering σ on A to the term-ordering τ on $A[t]$ defined by the following rule:
$t^{a_0}X_1^{a_1}\dots X_n^{a_n} > 0$ iff $\Sigma a_i > 0$ or $\Sigma a_i = 0$ and $X_1^{a_1}\dots X_n^{a_n} > 0$ according to σ (if $\log(t) = (1,0,\dots,0)$, $\log(X_1) = (0,1,0,\dots,0),\dots$ then as first two vectors of τ we may take $(1,q_1,\dots,q_n)$ and $(0, q_1,\dots,q_n)$).
Let us consider now the ideal ${}^hI$, i.e. the homogenized ideal of I with respect to the variable t, where $\deg(X_i) = q_i$ and obviously $\deg(t) = 1$.
CLAIM: $\{{}^hf_1,\dots,{}^hf_t\}$ is a G-base , hence a base of ${}^hI$ with respect to τ.
Namely $T({}^hI)$ is generated by $\{T({}^hf) \,/\, f\in I\}$ because of the definition of τ; but, for the same reason, $T({}^hf) = T(f)$. Therefore
$T({}^hI) = T(I)A[t] = (T(f_1),\dots,T(f_t))A[t] = (T({}^hf_1),\dots, T({}^hf_t))$.
Let us now consider the ring $F = A[t]/{}^hI$ and the homomorphism
φ: $k[t] \longrightarrow F$ This is the family that we are looking for.
Namely the fiber over the ideal (t) is $A[t]/({}^hI,t)$; but our choice of σ implies that $({}^hI,t) = ({}^hf_1,\dots,{}^hf_t,t) = (T({}^hf_1),\dots, T({}^hf_t),t) = (T(f_1),\dots,T(f_t),t) = (T(I),t)$; therefore the fiber over the origin is $A[t]/(T(I),t) \cong A/T(I)$.
The fiber over $(T-a)$, $a \neq 0$ is $F_a = A[t]/({}^hI,t-a)$.
The isomorphism $A[t] \longrightarrow A[t]$ given by $t \longrightarrow at$ induces an isomorphism $A[t]/({}^hI,t-a) \longrightarrow A[t]/({}^hI,t-1)$
But $A[t]/({}^hI,t-1)$ is clearly isomorphic to A/I.
CLAIM: The family φ is flat (see [**Bayer**, 1982]).
Indeed by standard arguments on base change of flatness (see [**Matsumura** , 1970]) we may assume that k is algebraically closed. Moreover since $k[t]$ is a principal ideal domain, flatness is equivalent to torsionfreeness. Of course torsonfreenes has to be checked only on irreducible elements: so we have to check only two cases:
1) $t\cdot f(t)=0 \bmod {}^hI$, hence $t\cdot f(t)\in {}^hI$, hence $f(t)\in {}^hI$ by the very definition of ${}^hI$
2) $(t-a)\cdot f(t) =0 \bmod {}^hI$; in this case we write $f(t) = \Sigma f_i(t)$ with f_i form of degree i; being ${}^hI$ homogeneous, we get
$-af_0(t)$, $tf_0(t)-af_1(t),\dots,tf_{r-1}(t)-af_r(t) \in {}^hI$ whence $f_i(t) \in {}^hI$ for every i, and we are done.
If moreover I is homogeneous with respect to a set of weights $(q_1,\dots,q_n)$ of the variables,and $u_1(<) = (q_1,\dots,q_n)$, then the flat family induces flat families parametrized by $k[t]$ on the finitely generated k-vectorspaces $(A/I)_n$ and $(A/(T(I))_n$ for every $n\in\mathbb{N}$, whence we get the constancy of the Hilbert functions along the fibers.∎

generated subsemigroup E of an ordered semigroup $(\mathbb{R}^s,lex)$,s.t. all its elements have non-negative coordinates. Let F be a non-void subset of E and let t be such that every element of F has the first t-1 coordinates zero, and at least one element of F has the t^{th} coordinate different from zero. Denoting π the projection from $\mathbb{R}^s$ to the t^{th} component, we have just to prove that $\pi(F)$ has a first element. Since $\pi(E)$ is a finitely generated non-negative subsemigroup of $\mathbb{R}$ with the usual ordering,which is archimedean, the result comes out from the fact that, if $r\in E$, the set $\{r'\in E \ / \ r'\leq r\}$ is finite. ∎

Proposition 4.4 $<$ is a term-ordering iff for every ideal I, for every set $F\subset I^*$, **A2** $\Rightarrow$**B1**.

Proof: $\Rightarrow$: Assume $<$ is a term-ordering. Let I be an ideal, $F\subset I^*$ s.t. **A2** holds, $g_1\in I^*$.

Since $g_1\in I^*$, $M(g_1)\in M(I)$, so there are $f_1\in F$, $m_1\in \mathbf{T}$, $a_1\in k^*$, s.t.

$$M(g_1) = a_1 m_1 M(f_1).$$

Define $g_2 := g_1 - a_1 m_1 f_1 \in I$. If $g_2\neq 0$, then $T(g_2)<T(g_1)$ and one can repeat the argument.

So one finds either a representation of g_1 as required by **B1** or one gets an infinite sequence of elements of I^*, $g_1,g_2,\ldots,g_i,\ldots$ s.t. for each i $T(g_i)>T(g_{i+1})$, against the assumption that $<$ is a well ordering.

$\Leftarrow$ Assume $<$ is not a term-ordering and let $n\in\mathbf{T}$ be s.t. $n<1$.Let $F:=\{n-n^2\}$, $I:=(n)$. Then F and I satisfy **A2** but don't satisfy **B1**. ∎

Proposition 4.5 $<$ is a term-ordering iff for every ideal I, for every set $F\subset I^*$, **A3** $\Rightarrow$**B3**. ∎

Lemma 4.3 holds for any ordered finitely generated commutative semigroup. Then propositions 4.4 and 4.5 hold in the more general context of a semigroup ring.

Conditions **B1,B2,B3** and **A3** can be stated in the more general context of graded structures; then **B3** coincides with the definition of generalized

B) Characterizations related to the graded ring structure

Proposition 4.2 Let us consider the following conditions on an ideal $I \subset A$ and a set $F \subset I^*$:

B1: every $f \in I^*$ can be represented:

$f = \Sigma a_i m_i f_i$, $a_i \in k^*$, $m_i \in \mathbf{T}$, $f_i \in F$,

$T(f) = T(m_1 f_1) > T(m_i f_i) > T(m_{i+1} f_{i+1})$ for every i

B2: every $f \in I^*$ can be represented:

$f = \Sigma a_i m_i f_i$, $a_i \in k^*$, $m_i \in \mathbf{T}$, $f_i \in F$,

$T(f) = T(m_1 f_1) > T(m_i f_i)$ for every i

B3: every $f \in I^*$ can be represented:

$f = \Sigma g_i f_i$, $g_i \in A^*$, $f_i \in F$, $T(g_i f_i) \leq T(f)$ for every i

Then the following implications hold trivially:

A2 ⇐ B1 ⇒ B2 ⇒ B3 ⇒ A3. ∎

(*cf.* the definition of G-base on page 3, where the second equivalent condition is **B3**).

Remark that in **B1,B2** one cannot assume that $f_i \neq f_j$ if $i \neq j$. We could, *but we don't*, assume such a condition in **B3**.

Recall that a total semigroup order $<$ on $\mathbf{T}$ is called a term-ordering iff $1 \leq m$ for every $m \in \mathbf{T}$.

Lemma 4.3 $<$ is a well-ordering iff $<$ is a term-ordering.

Proof: If there is $n \in \mathbf{T}$, $n < 1$, then defining $n_i := n^i$, one gets an infinite decreasing sequence.

Conversely assume $<$ is a term-ordering and not a well-ordering; then there is a infinite decreasing sequence $m_1 > \ldots > m_i > m_{i+1} > \ldots$ of elements of $\mathbf{T}$. By Dickson's Lemma, there are then m_i, m_j in the sequence, $n \in \mathbf{T}$, with $i < j$ and $m_i = m_j n$. Then $n < 1$.

An alternative proof is as follows ([**Robbiano**, 1986], Corollary 2.6): by the results of §3, $\mathbf{T}$ is isomorphic (as an ordered semigroup) to a finitely

$a:=c(h,t\ T(f))\neq 0$, $g = h - a/\mathbf{lc}(f)\ t\ f$.

Let then $m := t\ T(f)$, $b := c(p,m)$, and remark that $c(g,m)=0$. There are different cases:

i) $b = 0$: in this case clearly $h+p \gg g+p$.

ii) $b \neq 0$ and $a+b = 0$: in this case $h+p \ll g+p$, since $c(h+p,m)=0$ and $h+p = g + p - b/\mathbf{lc}(f)\ t\ f$

iii) $b \neq 0$ and $a+b \neq 0$: Let then

$q := h + p - (a+b)/\mathbf{lc}(f)\ t\ f = g + p - (b/\mathbf{lc}(f))\ t\ f$.

Then $c(q,m)=0$ and $h+p \gg q \ll g+p$. ∎

Also if $<$ is not a term-ordering, some relation $\rightarrow$ defined as above could still be noetherian (e.g. the relation defined by a finite set consisting of monomials). However if $<$ is not a term-ordering, let $m\in T$ s.t. $m<1$ and let $S:=\{m-m^2\}$; $\rightarrow$ is then non-noetherian since $m\rightarrow m^2\rightarrow\ldots\rightarrow m^i\rightarrow m^{i+1}\rightarrow\ldots$ (cf. Lemma 4.3)

Lemma 4.7 Let $g,h \in A$. Then $g-h \in (F) := I$ iff there are $h_0,\ldots,h_n\in A$ s.t. $g=h_0$, $h=h_n$, and for every i, either $h_{i-1}\rightarrow h_i$ or $h_i\rightarrow h_{i-1}$.

Proof: $\Rightarrow$: $g-h\in I$ iff $g=\Sigma_{i=1,n} m_i f_i + h$, $m_i\in\mathbf{M}$, $f_i\in F$ (the f_i's being not necessarily different). By induction on n.

If $n=1$, then $g=mf+h$, $m\in\mathbf{M}, f\in F$; since $mf\gg 0$, then (by R5) there is q s.t. $g\rightarrow q\leftarrow h$.

Inductively, let $g = \Sigma_{i=1,n+1} m_i f_i + h$ and let $g' := \Sigma_{i=1,n} m_i f_i + h$.

By inductive assumption and by the definition of $\rightarrow$, there are $h_0,\ldots,h_t\in A$ s.t. $g' = h_0$, $h=h_t$, and for every i, either $h_{i-1}\gg h_i$ or $h_i \ll h_{i-1}$.

Define $q_i := h_i + m_{n+1}f_{n+1}$ so that, in particular, $q_0 = g$. By R5 there are $p_1,\ldots,p_n$ s.t. $q_{i-1}\rightarrow p_i\leftarrow q_i$.

Also $m_{n+1}f_{n+1}\rightarrow 0$ so there is p_{t+1} s.t.

$q_t = h_t + m_{n+1}f_{n+1} \rightarrow p_{t+1} \leftarrow h_t = h$.

Since $g = g' + m_{n+1}f_{n+1} = h_0$, $h_t = h$, the sequence $q_0,p_1,q_1,\ldots,p_{t+1},h_t$ satisfies the requirement.

standard base and **A3** with condition b) of theorem 2.8. In this context proposition 4.4 holds and is the same as the first part of theorem 2.8.

C) Characterizations related to rewrite-rules

Let $<$ be a term ordering on A.
We will denote by c(f,m) the coefficient of the term m in the polynomial f, so that $f = \Sigma_T\ c(f,m)\ \ m$.
Let $F \subset A$ be a finite set. Define $\to$ as the reflexive-transitive closure of the relation $\gg$ defined as follows:

$h \gg g$ iff there is $f \in F$, $t \in T$, s.t. $a := c(h, t\ T(f)) \neq 0$,
$g = h - a/\mathbf{lc}(f)\ t\ f$.

Remark that if $h \gg g$, then g is obtained from h by substituting a term $t\ T(f)$ in it with terms less than $t\ T(f)$.
$h \in A$ is said irreducible iff $h \to g$ implies $g = h$.
$\to$ is said noetherian iff in every infinite sequence $h_1 \to \ldots \to h_i \to h_{i+1} \to \ldots$ there is N s.t. if $i > N$ then $h_i = h_{i+1}$. Remark that, if $<$ is noetherian, for every $h \in A$ there is an irreducible g s.t. $h \to g$.
It is said confluent if $g \leftarrow p \to h$ implies there is q s.t. $g \to q \leftarrow h$.

Lemma 4.6 $\to$ is a relation satisfying:

R1) $h \to h$
R2) $h \to g, g \to p$ imply $h \to p$
R3) $h \to g$ and $g \to h$ imply $h = g$
R4) $h \to g$ implies $mh \to mg$ for every $m \in \mathbf{M}$
R5) for every h,g,p s.t. $h \gg g$, there is q s.t. $h + p \to q \leftarrow g + p$
R6) 0 is irreducible

and which is noetherian if $<$ is a term-ordering.

Proof: $\to$ satisfies obviously R1,R2 and R6.
Since the effect of $\gg$ is to substitute a term with terms which are less than it w.r.t.$<$, then R3 is verified, and $\to$ is noetherian if $<$ is a term-ordering.
To verify R4, w.l.o.g. it is sufficient to show that $h \gg g$ implies $mh \gg mg$, which is trivial.
Let us verify R5: if $h \gg g$ there is $f \in F$, $t \in T$, s.t.

§4.

The following conditions are equivalent:

A1: $T(F)$ generates the semigroup ideal $T(I) \subset T$

A2: $M(F)$ generates the semigroup ideal $M(I) \subset M$

A3: $M(F) = M(I)$

B1: every $f \in I^*$ can be represented:

$$f = \Sigma a_i m_i f_i,\ a_i \in k^*,\ m_i \in T,\ f_i \in F,$$

$$T(f) = T(m_1 f_1) > T(m_i f_i) > T(m_{i+1} f_{i+1}) \text{ for every } i$$

B2: every $f \in I^*$ can be represented:

$$f = \Sigma a_i m_i f_i,\ a_i \in k^*,\ m_i \in T,\ f_i \in F,$$

$$T(f) = T(m_1 f_1) > T(m_i f_i) \text{ for every } i$$

B3: every $f \in I^*$ can be represented:

$$f = \Sigma g_i f_i,\ g_i \in A^*,\ f_i \in F,\ T(g_i f_i) \leq T(f) \text{ for every } i$$

C1: $h \in I$ implies $h \to 0$

C2: if h and g are irreducible: $h - g \in I$ implies $h = g$.

C3: for every $h \in A$ there exists a unique g irreducible s.t. $h \to g$

C4: $\to$ is confluent

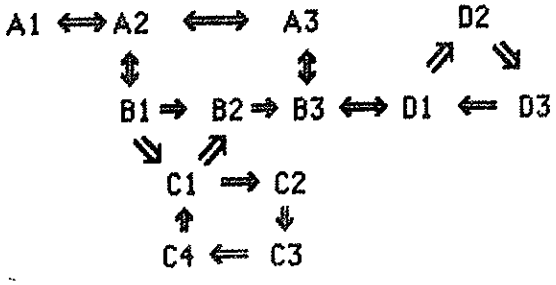
D1: Each homogeneous element of $\ker(s)$ b-extends to an element of $\ker(S)$

D2: If W is a base of $\ker(s)$ consisting of homogeneous elements, each element of W b-extends to an element of $\ker(S)$

D3: There is a base W of $\ker(s)$ consisting of homogeneous elements, s.t. each element of W b-extends to an element of $\ker(S)$

If F satisfies any of these conditions, it is called a Gröbner base of I (*cf.* the definition at page 3)

Proof: We sketch here the implications proved throughout these notes:



$u \in \ker(S)$ and w b-extends to u. ∎

Corollary 4.11 If $<$ is a term-ordering and $\{w_1,\ldots,w_t\}$ is a base of $\ker(s)$ consisting of homogeneous elements, and w_i b-extends to u_i, then $\{u_1,\ldots,u_t\}$ is a base of $\ker(S)$.

Proof: Let $u \in \ker(S)$, $w:=M(u)$, then $w=\Sigma m_i w_i$, $m_i \in \mathbf{M}$, $w_i \in W$, $T(m_i w_i)=T(w)$. Let $u_1:=u-\Sigma m_i u_i$; then $u_1 \in \ker(S)$ and, if $u_1 \neq 0$, then $T(u_1)<T(u)$.
The conclusion follows, since $<$ is a well ordering. ∎

Proposition 4.12 If $<$ is a term-ordering and F is a base of I, **B3** is equivalent with the conditions of proposition 4.2.

Proof: **B3 ⇒D1:** Let $w \in \ker(s)$, homogeneous, $w := \Sigma m_i e_i$; then $S(w) = \Sigma m_i f_i$, if not zero, is s.t. $T(S(w))<T(w)$. By assumption $S(w) = \Sigma g_i f_i$, with $T(g_i f_i) \leq T(S(w))<T(w)=T(m_i e_i)$. Then $u := \Sigma(m_i-g_i)e_i \in \ker(S)$ and $M(u)=w$.
D1 ⇒B3: Let $h \in I^*$ and let $h := \Sigma g_i f_i$ be any representation of h; let $u_1:=\Sigma g_i e_i$, so $S(u_1)=h$. If $T(u_1)=T(h)$ we are through, while if $T(u_1)>T(h)$ we will show how to obtain $u_2 \in A^t$ s.t. $S(u_2)=h$ and $T(u_2)<T(u_1)$. Since $<$ is a well ordering, this is sufficient to complete the proof.
Assume, therefore, $T(u_1)>T(h)$. Let $w := M(u_1)$, then $w \in \ker(s)$, so there exists $u \in \ker(S)$ s.t. $M(u) = w$. Let then $u_2 := u_1 - u$; u_2 satisfies the required conditions. ∎

The conditions **D1-3** can be stated in the more general context of graded structures; then conditions 3 and 4 of Theorem 2.11 respectively coincide with **D1** and **D3**.In that context, the theorems stated in this section still hold. Let us summarize the results proved in this paragraph in the following:

Characterization theorem 4.13 Let $<$ be a term-ordering on T, I an ideal of A, $F \subset I^*$ a base of I, $\rightarrow$ induced by F as in C), s and S defined as in

$T(h) = T(m_1f_1) > T(m_if_i) > T(m_{i+1}f_{i+1})$ for every i.

Define $h_t := \Sigma_{i=t,n} a_im_if_i$, $t=1,\ldots,n$. Then $h=h_1 \to \ldots \to h_t \to h_{t+1} \to \ldots \to h_n \to 0$.

C1⇒B2: if $h \in I^*$ then $h \to 0$ so $h = \Sigma a_im_if_i$, $a_i \in k^*$, $m_i \in T$, $f_i \in F$, and $T(h) \geq T(m_if_i)$ for every i, with equality holding just for one index.■

D) Characterizations related to syzygies

Let $f_1,\ldots,f_t \in P^*$, $F:=\{f_1,\ldots,f_t\}$.

Denote by $(e_1,\ldots,e_t)$ the canonical base of A^t.

The graduation induced by **T** on A extends obviously to A^t, defining $T(\Sigma g_ie_i):=\max(T(g_if_i):g_i\neq 0)$; define also $M(\Sigma g_ie_i):=\Sigma h_ie_i$, where

$h_i:=0$ iff $g_i=0$ or $T(g_if_i)<T(\Sigma g_ie_i)$

$h_i:=M(g_i)$ iff $T(g_if_i)=T(\Sigma g_ie_i)$.

$w := \Sigma g_ie_i$ is then said homogeneous if, for every $g_i \neq 0$, $g_i \in M$ and $T(g_if_i)=T(w)$.

Define $S : A^t \to A$ by $S(\Sigma g_ie_i) := \Sigma g_if_i$; $s : A^t \to A$ by $s(\Sigma g_ie_i) := \Sigma g_iM(f_i)$.

Remark that $T(S(u)) \leq T(u)$ and equality holds unless $M(u) \in \ker(s)$.

If w is a homogeneous element of ker(s), we say w b-extends to $u \in \ker(S)$ iff $M(u) = w$.

Remark that, if $u \in \ker(S)$, and $w = M(u)$, then $w \in \ker(s)$.

Proposition 4.10 If < is a term-ordering, the following conditions are equivalent:

D1: Each homogeneous element of ker(s) b-extends to an element of ker(S)

D2: If W is a base of ker(s) consisting of homogeneous elements, each element of W b-extends to an element of ker(S)

D3: There is a base W of ker(s) consisting of homogeneous elements, s.t. each element of W b-extends to an element of ker(S)

Proof: **D3 ⇒D1:** Let $w \in \ker(s)$, homogeneous; then $w=\Sigma m_iw_i$, $m_i \in M$, $w_i \in W$, $T(m_iw_i)=T(w)$. Let $u_i \in \ker(S)$ be s.t. w_i b-extends to u_i. Let $u := \Sigma m_iu_i$; then

$\Leftarrow$: The assumption implies there exist $f_1,\ldots,f_t \in F$, $m_1,\ldots,m_t \in \mathbf{M}$, $p_0,\ldots,p_t \in A$, s.t. $g-h = p_0 - p_t$, $p_{i-1} - p_i = m_i f_i \in I$ for every i.

The thesis is then obvious.■

Proposition 4.8 Let $F,\rightarrow,I$ be defined as above. If $\rightarrow$ is noetherian (e.g. if $<$ is a term-ordering), the following conditions are equivalent:

C1: $h \in I$ implies $h \rightarrow 0$

C2: if h and g are irreducible: $h-g \in I$ implies $h=g$.

C3: for every $h \in A$ there exists a unique g irreducible s.t. $h \rightarrow g$

C4: $\rightarrow$ is confluent.

Proof: **C1⇒C2:** If h and g are irreducible, then also h-g is such. Since, by **C1**, $h-g \rightarrow 0$, then $h-g=0$.

C2⇒C3: since $\rightarrow$ is noetherian we have just to prove uniqueness. However if g,p are irreducible elements s.t. $g \leftarrow h \rightarrow p$, then $g-p \in I$ and so $g=p$.

C3⇒C4: Let h,g,p be s.t. $g \leftarrow h \rightarrow p$ and let g',p' be irreducible elements s.t. $g \rightarrow g'$, $p \rightarrow p'$. Then $g' \leftarrow g \leftarrow h \rightarrow p \rightarrow p'$. So $g'=p'$ is the required element.

C4⇒C1: Since $h \in I$, by Lemma 4.7, there are $h_0,\ldots,h_{n-1} \in P^*$ s.t. $h=h_0$ and (defining $h_n:=0$) for every i, either $h_{i-1} \rightarrow h_i$ or $h_i \rightarrow h_{i-1}$.

Since 0 is irreducible, $h_{n-1} \rightarrow 0$. Therefore, either $h \rightarrow 0$ or there is $j<n-1$ s.t. $h_i \rightarrow 0$ if $i>j$, but it is false that $h_j \rightarrow 0$. Then $h_j \leftarrow h_{j+1} \rightarrow 0$. By confluence, however, there is g s.t. $h_j \rightarrow g \leftarrow 0$, and, since 0 is irreducible, $h_j \rightarrow g=0$, a contradiction.■

If for any ideal $I \subset A$, one is able to provide a set F which induces a confluent and noetherian relation $\rightarrow$, then one is able to decide ideal membership (by **C1**), ideal congruence (by **C2**), and to compute canonical representatives for elements in R/I (by **C3**).

Proposition 4.9 The following implications hold:

B1⇒C1⇒B2.

Proof: **B1⇒C1:** Let $h \in I^*$, $h = \Sigma_{i=1,n} a_i m_i f_i$, $a_i \in k^*$, $m_i \in T$, $f_i \in F$,

Lemma 5.2 If $S(i,j) \to 0$ then $s(i,j)$ b-extends to an element of $\ker(S)$

Proof: The assumption implies there is a representation $S(i,j) = \Sigma g_i f_i$ s.t. for each i, either $g_i = 0$ or $T(g_i f_i) \leq T(S(i,j)) < T(s(i,j))$.
So w b-extends to $u := s(i,j) - \Sigma g_i e_i$. ∎

Lemma 5.3 If $T(i,j) = T(i)T(j)$, then $s(i,j)$ b-extends to an element of $\ker(S)$.

Proof: $u := \mathbf{lc}(f_j)^{-1} f_j e_i - \mathbf{lc}(f_i)^{-1} f_i e_j \in \ker(S)$ and $M(u) = s(i,j)$. ∎

Lemma 5.4 $W_B := \{s(i,j) \,/\, \{i,j\} \in B\}$ is a base of $\ker(s)$. ∎

Impose on B a total ordering $\ll$ s.t.
if $\exists m \in \mathbf{T}$, $m > 1$, with $T(k,l) = m\, T(i,j)$, then $\{i,j\} \ll \{k,l\}$
We say $C \subset B$ is $\ll$-admissible if:
$\{i,j\} \notin C \Rightarrow \exists k$ s.t. $T(i,j) = T(i,j,k)$, $\{i,k\} \ll \{i,j\}$, $\{k,j\} \ll \{i,j\}$.

Lemma 5.5 If C is $\ll$-admissible, $W_C := \{s(i,j) \,/\, \{i,j\} \in C\}$ is a base of $\ker(s)$.

Proof: We show that if $\{i,j\} \notin C$, then $s(i,j)$ can be represented in terms of elements $s(k,l) \in B$, s.t. $\{k,l\} \ll \{i,j\}$.
Since $\{i,j\} \notin C$, then there is k s.t. $T(i,j) = T(i,j,k)$, $\{i,k\} \ll \{i,j\}$, $\{k,j\} \ll \{i,j\}$.
The following equality holds easily:

$$T(i,j,k)/T(i,j)\, s(i,j) - T(i,j,k)/T(i,k)\, s(i,k) + T(i,j,k)/T(j,k)\, s(j,k) = 0$$

i.e.

$$s(i,j) = T(i,j,k)/T(i,k)\, s(i,k) - T(i,j,k)/T(j,k)\, s(j,k).$$ ∎

The idea on which Buchberger algorithm is based is the following: let $F := \{f_1, \ldots, f_u\}$ be a base of I, and let C be a $\ll$-admissible subset of B.
If for each $\{i,j\} \in C$, s.t. $T(i,j) \neq T(i)T(j)$, $S(i,j) \to 0$ then, by lemmata 5.2, 5.3, and 5.5, **D3** is verified and F is a Gröbner base.

§5 Buchberger algorithm

A) An informal description of Buchberger algorithm

Let $A := k[X_1,\ldots,X_n]$, k a field, $<$ a term-ordering on **T**.

Let $f_1,\ldots,f_u \in A^*$, $F:=\{f_1,\ldots,f_u\}$, $I:=(F)$, $\rightarrow$ the relation induced by F.

Denote by $(e_1,\ldots,e_u)$ the canonical base of A^u. Let A^u be graded by **T**, as in §4, defining $T(\Sigma g_i e_i):=\max(T(g_i f_i): g_i \neq 0)$; define also $M(\Sigma g_i e_i)$ as in §4.

Define $S : A^u \rightarrow A$ by $S(\Sigma g_i e_i) := \Sigma g_i f_i$; $s : A^u \rightarrow A$ by $s(\Sigma g_i e_i) := \Sigma g_i M(f_i)$.

Let us recall the following definition: if w is a homogeneous element of ker(s), we say w b-extends to $u \in \ker(S)$ iff $M(u)=w$.
Let us also recall the following equivalent definitions of the concept of Gröbner base:

Proposition 5.1 F is a Gröbner base of I iff any of the following conditions is verified:

A3 $M(f) = M(I)$

C1 $f \in I$ iff $f \rightarrow 0$

D3 There is a base W of ker(s) consisting of homogeneous elements, s.t. each element of W b-extends to an element of ker(S). ∎

Since $\mathrm{im}(s)=(M(f_1),\ldots,M(f_u))$ is a monomial ideal, it is very easy to compute a base of ker(s), i.e. a base of the module of syzygies of M(I).
Denote:

$T(i) := T(f_i)$, $i=1\ldots u$;

$B:=\{\{i,j\} \mid 1\leq i<j\leq u\}$;

$T(i,j) :=$ **l.c.m.** $(T(i),T(j))$, $\{i,j\}\in B$;

$T(i,j,k) :=$ **l.c.m.** $(T(i),T(j),T(k))$, $1\leq i,j,k\leq u$;

$s(i,j) := \mathbf{lc}(f_i)^{-1}\, T(i,j)/T(i)\, e_i - \mathbf{lc}(f_j)^{-1}\, T(i,j)/T(j)\, e_j$, $1\leq i,j\leq u$;

$S(i,j) := S(s(i,j)) = \mathbf{lc}(f_i)^{-1}\, T(i,j)/T(i)\, f_i - \mathbf{lc}(f_i)^{-1}\, T(i,j)/T(j)\, f_j$, $1\leq i,j\leq u$,

the S-polynomial of f_i and f_j.

Remarks : 1) Buchberger proved that if $<$ is s.t. $\deg(m) < \deg(n) \Rightarrow m < n$, then an optimal choice is to choose $\{i,j\}$ s.t. $T(i,j)$ is minimal w.r.t. to $<$. This choice however can be very bad if $<$ is a lexicographical ordering.

2) Order $\{ \{i,j\} / 1 \le i < j \le u\}$ so that if $T(i,j) < T(k,l)$ then $\{i,j\} \ll \{k,l\}$, while pairs $\{i,j\}$, $\{k,l\}$ s.t. $T(i,j)=T(k,l)$ are sorted according to the order in which they are chosen by the algorithm.

The set $C := C_0 \cup \{\{i,j\} / T(i,j)=T(i)T(j)\}$ is then $\ll$-admissible so the set $\{s(i,j) / \{i,j\} \in C\}$ is a base of $\ker(s)$, $s : A^u \to A$ defined by $s(\Sigma g_i e_i) := \Sigma g_i M(f_i)$, whose elements b-extend to elements of $\ker(S)$, $S : A^u \to A$ defined by $S(\Sigma g_i e_i) := \Sigma g_i f_i$, so that G is a Gröbner base of I.

We present now two examples of Gröbner base computation; at any step in the computation in which a new element is added to the base, the following information will be presented:

1) a list of the base elements

2) a list of all pairs $\{i,j\}$, together with the list of the exponents of $T(i,j)$, and if $S(f_i,f_j)$ has been already treated by the algorithm:

- the symbol "P" to denote that $S(f_i,f_j)$ has not been computed because $T(i,j)=T(i)T(j)$.
- a number k, $i \neq k \neq j$, to denote that $S(f_i,f_j)$ has not been computed since $T(i,j)=T(i,j,k)$, $T(i,k) \neq T(i,j)$ or $\{i,k\} \notin B$, $T(k,j) \neq T(i,j)$ or $\{k,j\} \notin B$
- the symbol "$\to$" followed by a number l, to denote that $S(f_i,f_j)$ has been computed by the algorithm and there is $c \in k^*$ s.t. $S(f_i,f_j) \to c f_l$.

The pairs (i,j) will be ordered by $\ll$:

$(i,j) \ll (k,l)$ iff $T(i,j) < T(k,l)$
or $T(i,j)=T(k,l)$ and $j<l$
or $T(i,j)=T(k,l)$ and $j=l$ and $i<k$.

C) EXAMPLE

We compute here the Gröbner base of the ideal $I:=(X^3-Y, XY-Z) \subset \mathbb{Q}[X,Y,Z]$ w.r.t. the graduated rev-lex ordering on T generated by $Z>Y>X$, i.e. the

Otherwise if some $\{i,j\}\in C$ is found s.t. $S(i,j)\to g$, g irreducible, $g\neq 0$, **C1** doesn't hold and F is not a Gröbner base. In this case, one can force the condition $S(i,j)\to 0$ to be verified, just adding g (which is an element of I) to the base F; this leads to a necessary enlargement of B and of C and so requires to check $S(i,j)\to 0$ for several new pairs $\{i,j\}$.
Since the element g which has been added to the base F, being irreducible, is s.t. T(g) is not multiple of any element of T(F), it is impossible to add infinitely many elements to F,since this would contradict Dickson's Lemma. If one likes, the same can be proved using the noetherianity of A, because of the inclusion $(M(F))\subsetneq(M(F\cup\{g\}))$.

B) Buchberger algorithm

Algorithm Given $A,<, f_1,\ldots,f_t,F,I$ as above, compute a Gröbner base G of I.

$G := F$
$u := t$
$B := \{\{i,j\} / 1\le i<j\le u\}$
$[\![C_0 := \emptyset]\!]$
While $B\neq\emptyset$ **do**
  choose $\{i,j\}\in B$ [[see remark 1 below]]
  $B := B-\{\{i,j\}\}$
  If $T(i,j)\neq T(i)T(j)$ **or** (there is no k, $1\le k\le u, i\neq k\neq j$, s.t.
    $T(i,j)=T(i,j,k)$, $T(i,k)\neq T(i,j)$ or $\{i,k\}\notin B$, $T(k,j)\neq T(i,j)$ or
    $\{k,j\}\notin B$) [[see remark 2 below]] **then**
    $[\![C_0 := C_0\cup\{i,j\}]\!]$
    $f := S(i,j)$
    While $f\neq 0$ **and** $M(f)\in(M(G))$ **do**
      choose $m\in\mathbf{T}$, l, s.t. $M(f) = \mathbf{lc}(f)/\mathbf{lc}(f_l)\ m\ M(f_l)$
      $f := f - \mathbf{lc}(f)/\mathbf{lc}(f_l)\ m\ f_l$
    If $f\neq 0$ **then**
      $u := u+1$
      $f_u := f$
      $G := G\cup\{f_u\}$
      $B := B\cup\{\{i,u\} / 1<i<u\}$

		X Y Z
$f_1:=X^3-Y$	1 2	3 1 0 →3
$f_2:=XY-Z$	1 3	3 0 1 →0
$f_3:=X^2Z-Y^2$	2 3	2 1 1 →4
$f_4:=Y^3-XZ^2$	2 4	1 3 0 →0
	1 4	3 3 0 P
	3 4	2 3 1 P

So $\{f_1,f_2,f_3,f_4\}$ is a Gröbner base of I.

D) EXAMPLE

In this example we compute the Gröbner base of the ideal $I:=(T^3-X,T^4-Y)\subset\mathbb{Q}[X,Y,T]$ w.r.t. the lexicographical ordering induced by $X<Y<T$, i.e. the ordering characterized by $(0,0,1),(0,1,0),(1,0,0)$, if we denote X by X_1, Y by X_2, T by X_3.

		X Y T
$f_1:=T^3-X$	1 2	0 0 4
$f_2:=T^4-Y$		

$$\mathbf{S(f_1,f_2) = T\,f_1 - f_2 = Y - XT =: -f_3}$$

		X Y T
$f_1:=T^3-X$	1 3	1 0 3
$f_2:=T^4-Y$	1 2	0 0 4 →3
$f_3:=XT-Y$	2 3	1 0 4

$$\mathbf{S(f_1,f_3) = X\,f_1 - T^2\,f_3 = YT^2 - X^2 =: f_4}$$

ordering which is characterized by (1,1,1),(-2,1,1),(0,-1,1), if we denote X by X_1,Y by X_2, Z by X_3.

		X Y Z
$f_1 := X^3-Y$	1 2	3 1 0
$f_2 := XY-Z$		

$$S(f_1,f_2) = Y f_1 - X^2 f_2 = X^2Z - Y^2 =: f_3$$

		X Y Z
$f_1:=X^3-Y$	1 2	3 1 0 →3
$f_2:=XY-Z$	1 3	3 0 1
$f_3:=X^2Z-Y^2$	2 3	2 1 1

$$S(f_1,f_3) = Z f_1 - X f_3 = XY^2 - YZ \to 0$$

$$S(f_2,f_3) = XZ f_2 - Y f_3 = Y^3 - XZ^2 =: f_4$$

		X Y Z
$f_1:=X^3-Y$	1 2	3 1 0 →3
$f_2:=XY-Z$	1 3	3 0 1 →0
$f_3:=X^2Z-Y^2$	2 3	2 1 1 →4
$f_4:=Y^3-XZ^2$	2 4	1 3 0
	1 4	3 3 0
	3 4	2 3 1

$$S(f_2,f_4) = Y^2 f_2 - X f_4 = X^2Z^2 - Y^2Z \to 0$$

		X Y T
$f_1 := T^3 - X$	3 5	1 2 1 →6
$f_2 := T^4 - Y$	5 6	0 3 1
$f_3 := XT - Y$	3 6	1 3 1
$f_4 := YT^2 - X^2$	3 4	1 1 2 →5
$f_5 := Y^2T - X^3$	4 5	0 2 2
$f_6 := Y^3 - X^4$	4 6	0 3 2
	1 3	1 0 3 →4
	1 4	0 1 3
	1 5	0 2 3
	1 6	0 3 3
	1 2	0 0 4 →3
	2 3	1 0 4
	2 4	0 1 4
	2 5	0 2 4
	2 6	0 3 4

$$S(f_5,f_6) = Y f_5 - T f_6 = X^4T - X^3Y \to 0$$

$$S(f_4,f_5) = Y f_4 - T f_5 = X^3T - X^2Y \to 0$$

$$S(f_1,f_4) = Y f_1 - T f_4 = X^2T - XY \to 0$$

		X Y T	
$f_1 := T^3 - X$	3 4	1 1 2	
$f_2 := T^4 - Y$	1 3	1 0 3	→4
$f_3 := XT - Y$	1 4	0 1 3	
$f_4 := YT^2 - X^2$	1 2	0 0 4	→3
	2 3	1 0 4	
	2 4	0 1 4	

$$S(f_3, f_4) = YT\, f_3 - X\, f_4 = X^3 - Y^2T =: -f_5$$

		X Y T	
$f_1 := T^3 - X$	3 5	1 2 1	
$f_2 := T^4 - Y$	3 4	1 1 2	→5
$f_3 := XT - Y$	4 5	0 2 2	
$f_4 := YT^2 - X^2$	1 3	1 0 3	→4
$f_5 := Y^2T - X^3$	1 4	0 1 3	
	1 5	0 2 3	
	1 2	0 0 4	→3
	2 3	1 0 4	
	2 4	0 1 4	
	2 5	0 2 4	

$$S(f_3, f_5) = Y^2\, f_3 - X\, f_5 = X^4 - Y^3 =: -f_6$$

S 6. Applications not depending on term-ordering.

A) Canonical form of the elements of a quotient ring and Hilbert function.

Let $A = k[X_1,\dots,X_n]$ be a polynomial ring over a field and let $<$ be a term-ordering on A. Let us recall the following notations and definitions:

$T(A)$ is the set of the monic monomials of A;

if $f \in A$ is written as $\Sigma c_i m_i$ with $c_i = c(f,m_i) \in k^*$, $m_i \in T$ and $m_1 > m_2 > \dots$, then we put $T(f) = m_1$, $c(f) = c_1$, $M(f) = c_1 m_1$;

if $I \subset A$, we denote by $M(I)$ the ideal of A generated by $\{M(f) \mid f \in I\}$;

given a finite subset $G = \{g_1,\dots,g_s\}$ of A, an element $f = \Sigma c_i m_i$ of A is called irreducible with respect to G if no monomial of f belongs to the semigroup ideal of $T(A)$ generated by $\{M(g_1),\dots,M(g_s)\}$. An irreducible element f w.r.t. G is also said to be in normal form w.r.t. G.

Given a finite subset G of A, for every $f \in A$ it is possible to construct algorithmically an element $f' \in A$ such that:

i) f' is in normal form w.r.t. G;

ii) $f \equiv f'$ modulo the ideal generated by G.

Such an element f' is called a normal form of f (w.r.t. G).

Normal Form Algorithm

INPUT: $f \in A$, $G = \{g_1,\dots,g_s\} \subset A$.

OUTPUT: f' (a normal form of f), s polynomials $p_1,\dots,p_s$ s.t. $f = f' + \Sigma p_i g_i$ with $\deg(p_i g_i) \leq \deg(f)$.

```
f' = f ;
p_1 = ... = p_s = 0 ;
while f' is reducible do
    choose a monomial m_i of f', T(g_j) and u∈T(A) s.t. m_i = uT(g_j);
    γ = c(g_j)^{-1} c(f',m_i)
    f' = f' - γug_j ;
    p_j = p_j + γu .
```

		X Y T
$f_1 := T^3 - X$	3 5	1 2 1 →6
$f_2 := T^4 - Y$	5 6	0 3 1 →0
$f_3 := XT - Y$	3 6	1 3 1 P
$f_4 := YT^2 - X^2$	3 4	1 1 2 →5
$f_5 := Y^2T - X^3$	4 5	0 2 2 →0
$f_6 := Y^3 - X^4$	4 6	0 3 2 5
	1 3	1 0 3 →4
	1 4	0 1 3 →0
	1 5	0 2 3 4
	1 6	0 3 3 4
	1 2	0 0 4 →3
	2 3	1 0 4 1
	2 4	0 1 4 1
	2 5	0 2 4 1
	2 6	0 3 4 1

So $\{f_1,f_2,f_3,f_4,f_5,f_6\}$ is a Gröbner base of I; then $\{M(f_1),M(f_2),M(f_3),M(f_4),M(f_5),M(f_6)\}$ is a base of $(M(I))$; since $M(f_2) = TM(f_1)$, then $\{f_1,f_3,f_4,f_5,f_6\}$ is also a Gröbner base of I.

Corollary 6.3. Let I be a homogeneous ideal of A. Then

$$\mathbf{H}(A/I) = \mathbf{H}(A/M(I)) .$$

Proof. If $G = \{g_1,\ldots,g_s\}$ is a G-base of I, then $G' = \{M(g_1),\ldots,M(g_s)\}$ is a G-base of $M(I)$. So the set $\mathbf{B}$, defined in theorem 6.1, is the same for the G-base G of I and the G-base G' of $M(I)$. Let $\mathbf{B_d}$ be the part of degree d of $\mathbf{B}$. As a k-base of $(A/I)_d$ (resp. $(A/M(I))_d$) is given by the images in A/I (resp. in $A/M(I)$) of the elements of $\mathbf{B_d}$, we have: $\dim_k(A/I)_d = \dim_k(A/M(I))_d$ for all d. ∎

Corollary 6.4. If I is a homogeneous ideal of A, then the Hilbert function of $A/M(I)$ does not depend on the particular term-ordering on A. ∎

Algorithms to compute the Hilbert function of an ideal generated by monomials and, hence, of a homogeneous ideal are discussed in [**Möller-Mora**, 1983] and [**Möller-Mora**, 1986b]

B) Syzygies.

Given a finite subset $F = \{f_1,\ldots,f_r\}$ of A, the syzygy module of F is the sub A-module of A^r:

$$Syz(F) = \{(h_1,\ldots,h_r) \in A^r \;/\; \Sigma h_i f_i = 0\} .$$

In this section we want just describe how, using G-bases, we are able to find a system of generators for $Syz(F)$. Though not necessary in this context, it is suitable to worki with reduced G-bases.

Definition A G-base G is a reduced G-base if and only if each $g \in G$ has leading coefficient equal to 1 and is in normal form w.r.t. $G\backslash\{g\}$.

Remark . If G is a G-base, then each $f \in A$ has a unique normal form w.r.t. G (theorem 4.13, C3). We shall denote it by N(G,f) .

This result can be got, in a more constructive manner, as a corollary o the following theorem which gives an answer to the problem of a canonical representation of the elements of a quotient A/I of A . Note that its proof depends only on the characterizations C1 and C2 of the theorem 4.13.

From now on let $G = \{g_1,\dots,g_s\}$ denote a G-base of an ideal I with respect to some given term-ordering of A.

Theorem 6.1.([**Buchberger** ,1985]) Let $G = \{g_1,\dots,g_s\}$ be a G-base of an ideal I of A. Let **A** be the semigroup ideal of T(A) generated by $\{T(g_1),\dots,T(g_s)\}$ and let **B = T \ A** . Then the image $\bar{\mathbf{B}}$ of **B** is a k-base of A/I .

Proof. Note that the canonical map $\mathbf{B} \longrightarrow \bar{\mathbf{B}}$, $u \longmapsto \bar{u}$ is bijective.

Let $\bar{f} \in A/I$ and let f' be a normal form of f ; then $\bar{f} = \bar{f}'$ and f' is a linear combination of elements of **B** . So $\bar{\mathbf{B}}$ spans A/I .

If $\Sigma c_i \bar{u}_i = 0$ with $c_i \in k$, $u_i \in \mathbf{B}$, then $f = \Sigma c_i u_i \in I$, hence, by C1 of theorem 4.13 , 0 is a normal form of f . On the other hand, as $u_i \in \mathbf{B}$ for all i , the element f is already in normal form ; thus, by C2 of theorem 4.13, $f = 0$, that is $c_i = 0$ for all i and $\bar{\mathbf{B}}$ is a free set. ∎

Corollary 6.2. Let $f , g \in A$. Then:

i) $f \in I$ if and only if $N(G,f) = 0$;

ii) $\bar{f} = \bar{g}$ in A/I if and only if $N(G,f) = N(G,g)$.

Proof. It follows immediately from theorem 6.1 . ∎

In the next corollary we denote by **H**(R) the Hilbert function of a graded ring R .

compatible lexicographic ordering induced by $W > X > Y > Z$ i.e. the ordering which is characterized by (1,1,1,1), (1,0,0,0), (0,1,0,0), (0,1,0,0). We have:

$$h_{12} = S(f_1,f_2) = Y^2 f_1 - Z f_2 = -XY^3 + X^2Z^2 = X f_4$$

$$h_{13} = S(f_1,f_3) = WY f_1 - Z f_3 = -WXY^2 + X^3Z = -X f_2$$

$$h_{14} = S(f_1,f_4) = XZ f_1 - W f_4 = -X^2YZ + WY^3 = Y f_2$$

$$h_{23} = S(f_2,f_3) = W f_2 - Y f_3 = -WX^2Z + X^3Y = -X^2 f_1$$

$$h_{24} = S(f_2,f_4) = XZ^2 f_2 - WY^2 f_4 = -X^3Z^3 + WY^5 = Y^3 f_2 - X^2Z f_4$$

$$h_{34} = S(f_3,f_4) = XZ^2 f_3 - W^2Y f_4 = -X^4Z^2 + W^2Y^4 = Y^3 f_3 - X^3 f_4$$

so Syz(F) is generated by the rows of

$$\begin{vmatrix} -Y^2 & Z & 0 & X \\ -WY & -X & Z & 0 \\ -XZ & Y & 0 & W \\ -X^2 & -W & Y & 0 \\ 0 & Y^3 - XZ^2 & 0 & WY^2 - X^2Z \\ 0 & 0 & Y^3 - XZ^2 & W^2Y - X^3 \end{vmatrix}$$

Now let F be any finite subset of A. Let us write F as a row vector $(f_1,\ldots,f_r)$. We wish to find a matrix N, having r columns, such that the finitely many rows of N are a system of generators of Syz(F). For this purpose let us compute a (reduced) G-base $G = (g_1,\ldots,g_s)$ (row vector) of the ideal generated by F. Keeping track of how to write each g_i in terms of $f_1,\ldots,f_r$, we get an $r \times s$ matrix Q such that $G = FQ$. Applying the Normal Form Algorithm to $f_1,\ldots,f_r$, we can also construct an $s \times r$ matrix P such that $F = GP$.

It is easy to modify the algorithm of §5 in such a way its output is a reduced G-base. It suffices to add some instructions to reduce every elemen g of G in normal form w.r.t. G\{g} at the beginning and, also, each time a new polynomial is adjoined to the base.

Buchberger ([**Buchberger** ,1976b]) has showed that, fixed a term-ordering on A , for every ideal of A , there exists a unique reduced G-base.

First let us consider the syzygy module of a (reduced) G-base. We recal that theorem 2.11 and proposition 4.10 characterize G-bases by means of their syzygy module. Now, given a (reduced) G-base G , which we write as a row vector $(g_1,\ldots,g_s)$, we are going to show how to construct a matrix M with s columns such that $GM^t = 0$ (M^t is the transpose of M) and the finitely many rows of M are a system of generators for Syz(G). From lemma 5.4 and the characterizations of the G-bases related to syzygies (see §4), we get an algorithm ([**Spear**,1977], [**Zacharias** ,1978], [**Trinks** ,1978], [**Schreyer** ,1980], [**Möller-Mora** ,1986]) which constructs M and which we prefer describe informally as in [**Buchberger** ,1985].

- Start with the empty matrix M .
- For all pairs (i,j) $(1\le i<j\le s)$ let $h_{ij} = S(g_i,g_j) = u_i g_i - u_j g_j$ be the S-polynomial of g_i and g_j.
- Apply the Normal Form Algorithm to h and G to get the representation $h = p_1 g_1 + \ldots + p_s g_s$.
- Add

$$(p_1,\ldots,p_{i-1},p_i-u_i,p_{i+1},\ldots,p_{j-1},p_j-u_j,p_{j+1},\ldots,p_s)$$

as last row in M .

Example 6.5. In this example we compute the syzygies of the ideal I of the rational quartic curve. This ideal is generated by:

$$f_1 = WZ - XY \ , \ f_2 = WY^2 - X^2Z \ , \ f_3 = W^2Y - X^3 \ , \ f_4 = XZ^2 - Y^3$$

and these four elements are a reduced G-base of I w.r.t. the degree-

Proof. An r-uple H satisfying (*) can be constructed in this way: find a G-base G of I , represent f as GP and G as FQ , then H = QP . Each other r-uple is given by H + K where $K \in Syz(f_1,\dots,f_r)$. ∎

Corollary 6.9. Given a system of generators of an ideal I of A , it is possible to find a minimal one.

Proof. If $F = \{f_1,\dots,f_r\}$ is a system of generators of I , then $f_1 \in (f_2,\dots,f_r)$ if and only if there exists $(h_1,\dots,h_r) \in Syz(F)$ with $h_1 = 1$. ∎

Corollary 6.10. Given two ideal I and J of A , then $I \cap J$ can be computed .

Proof. Let $I = (f_1,\dots,f_r)$, $J = (f'_1,\dots,f'_t)$ and let S be a system of generators for $Syz(f_1,\dots,f_r,f'_1,\dots,f'_t)$. Let S' be the subset of the elements of S having not all the first r components and not all the last t components equal to zero. Then $I \cap J$ is generated by

$\{\Sigma h_i f_i \ / \ 1 \le i \le r$ and $(h_1,\dots,h_r, h'_1,\dots,h'_t) \in S$ for some $h'_1,\dots,h'_t\}$. ∎

Example 6.11. Let f_1, f_2, f_3, f_4 be the generators of the Macaulay's quartic curve as in the previous example. Then

$$(f_1, f_2) \cap (f_3, f_4) = (Yf_3, Zf_3, Xf_4, Wf_4) .$$

Remark Later on it will show how the intersection of two ideals of A can be computed without using syzygies.

Remark In general the system of generators for Syz(F) constructed in this way is not a minimal one. In the example 6.5 it is immediate to check that

$$R(5) = Y^2 R(3) - XZ R(1)$$

and

$$R(6) = -X^2 R(1) - XZ R(2) + WY R(3) + Y^2 R(4)$$

(here R(i) denotes the i-th row of M) .

However, one can use the theory of Gröbner bases for A-modules

Proposition 6.6 ([**Zacharias** ,1978]). The rows of the matrix

$$N = \begin{pmatrix} I - P^t Q^t \\ \hline M Q^t \end{pmatrix}$$

generates Syz(F) (I is the r×r unit matrix).

Proof. Let $H \in Syz(F)$, $H = (h_1,\dots,h_r)$. Then $FH^t = 0$, hence $GPH^t = 0$ and HP^t is a syzygy of G . As the rows of M generates Syz(G), there exists a vector K such that $HP^t = KM$. Our thesis follows multiplying on the right by Q^t and using the identity $H = HP^t Q^t + H(I - P^t Q^t)$. ■

Remark If $F \subset G$, then $P^t Q^t = I$, so Syz(F) is generated by MQ^t . In general, even if G is reduced, it can be $I \neq P^t Q^t$.

Example 6.7. Let $A = k[T,X,Y]$, where $\deg T = 1$, $\deg X = 3$, $\deg Y = 4$, and let us consider on A the degree- compatible reverse lex ordering induced by $Y > X > T$, i.e. the ordering which is characterized by (1,1,1), (-2,1,1), (0,-1,1). Let $F = \{ T^3 - X , Y - TX , T^2Y - X^2 \}$. Then the reduced G-base of the ideal generated by F is $G = \{ T^3 - X , T^4 - Y \}$. So we have

$$F = GP = G \begin{pmatrix} -1 & T & -X-T^3 \\ 0 & -1 & T^2 \end{pmatrix} \quad \text{and} \quad G = FQ = F \begin{pmatrix} -1 & -T \\ 0 & -1 \\ 0 & 0 \end{pmatrix}$$

Hence

$$I - P^t Q^t = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -X & T^2 & 0 \end{pmatrix}$$

So Syz(F) is generated by $(-X, T^2, 1)$ and, from the block MQ^t , $(-Y + TX, X - T^3, 0)$.

Corollary 6.8. Let $I = (f_1,\dots,f_r)$ an ideal of A and $f \in I$. Then it is possible to construct all the r-uples $(h_1,\dots,h_r)$ such that

$$(*) \qquad f = h_1 f_1 + \dots + h_r f_r \ .$$

S 7. Applications depending on term-ordering.

In this section we want to show how one can compute some special ideals by means of G-bases raising from a particular term-ordering.

A) Homogeneization and affinization.

The first question, which we speak of, is the behaviour of G-bases with respect to homogeneization and affinization processes. Though the homogeneization is already treated in the proof of theorem 3.8 , we wish to report it here for the sake of completeness.

Let $A = k[X_1,\dots,X_n]$ and $B = k[X_0,X_1,\dots,X_n]$ be two polynomial rings whose variables have respectively the weights $(q_1,\dots,q_n)$ and $(1,q_1,\dots,q_n)$. If $f \in A$, then ${}^hf$ denotes the homogeneous polynomial

$$X_0^{\partial f} f(X_1/X_0, \dots, X_n/X_0)$$

in B (∂f = degree of f) . For an ideal I of A we denote by ${}^hI$ the homogeneous ideal generated by the forms ${}^hf$ with $f \in I$.

If I(V) is the defining ideal of an affine algebraic variety V in $\mathbb{A}^n$, then ${}^hI(V)$ is the defining ideal of its projective closure $\bar{V}$ in the weighted projective space $\mathbb{P} = \mathbb{P}(1,q_1,\dots,q_n)$.

Given a polynomial $F \in B$, we denote by ${}^aF$ the polynomial

$$F(1,X_1,\dots,X_n)$$

of A ; if J is a homogeneous ideal of B generated by the forms $F_1,\dots,F_r$, then ${}^aJ$ is the ideal $({}^aF_1,\dots,{}^aF_r)$ of A .

When J is the defining ideal of a projective algebraic variety W , then ${}^aJ$ is the defining ideal of the affine subvariety of W contained in the standard open set $X_0 \neq 0$.

Let $<_A$ be a degree compatible term-ordering on A . Let us consider on B the induced term-ordering defined in the following way:

([**Bayer**,1985], [**Möller-Mora** ,1986]) having some results like the previous ones. In particular one can compute syzygies of syzygies, trim a system of generators to a minimal one (as in the corollary 6.7), and, repeating this, construct a minimal free resolution of an A-module.

C) Proper ideals.

The last problem having a trivial answer, not depending on the particular term-ordering, by means of G-bases, is checking whether an ideal of A is a proper ideal.

Proposition 6.12. Let I be an ideal of A and G a G-base of it. Then I = A if and only if G contains an invertible element.

Proof. Since G generates I , the implication ' $\Leftarrow$ ' is trivial. Viceversa, if I = A , then N(G,1) = 0 . Hence there exists g $\in$ G such that M(g) divides 1 . It follows that g $\in$ k .

Remark If G is a reduced G-base of I , then I = A if and only if 1 $\in$ G .

Corollary 7.2. ([**Robbiano-Valla**, preprint]). Let W be a projective variety in $\mathbb{P}^n$ and let V be an affine variety in $\mathbb{A}^n$ whose projective closure is W. If V is set-theoretic complete intersection of the hypersurfaces $f_1 = \ldots = f_r = 0$ and $\{f_1,\ldots,f_r\}$ is a G-base of the defining ideal $I(V)$ of V, then W is set-theoretic complete intersection of the hypersurfaces ${}^hf_1 = \ldots = {}^hf_r = 0$.

Proof. By hypothesis and theorem 7.1, it follows: $I(W) = {}^hI(V) = {}^h(\mathrm{rad}(f_1,\ldots,f_r)) = \mathrm{rad}({}^h(f_1,\ldots,f_r)) = \mathrm{rad}({}^hf_1,\ldots,{}^hf_r)$. ∎

Remarks. 1) In [**Robbiano-Valla**, preprint] it is showed that several classes of projective varieties, among which rational normal curves, rational ruled surfaces, elliptic normal curves, monomial curves in $\mathbb{P}^3$ which are arithmetically Cohen-Macaulay, are set-theoretic complete intersection. The main ingredients used there are the corollary 7.2 and the following lemma:

Lemma. Given $f_1,\ldots,f_r$ in A, $M(f_1),\ldots,M(f_r)$ is a regular sequence if and only if $\{f_1,\ldots,f_r\}$ is a regular sequence and a G-base. ∎

2) The theorem 7.1 is also used in [**Cavaliere-Niesi**, 1984b] to give a characterization of the monomial curves in $\mathbb{P}^n$ which are complete intersection and an algorithm to construct recursively all these curves.

Now we shall show it is possible to compute a G-base of an arbitrary ideal using homogeneous ideals. This fact has important theoretical applications as, for instance, to the problem of degree bounds for G-bases ([**Möller-Mora**, 1984]), but also practical ones: for instance, the Macintosh diskette "Macaulay", due to Bayer and Stillmann, which just compute G-bases, works, until today (February 1986), only on homogeneous ideals.

Let $<_A$ any term-ordering (not necessarily degree compatible) on A. Define then the following degree compatible term-ordering $<_B$ on B:

if $u , v \in T(B)$ and $\log(u) = (\alpha_0,\alpha_1,\ldots,\alpha_n)$, $\log(v) = (\beta_0,\beta_1,\ldots,\beta_n)$ we put $u <_B v$ if and only if $\Sigma\alpha_i < \Sigma\beta_i$ or $\Sigma\alpha_i = \Sigma\beta_i$ and ${}^a u <_A {}^a v$.

Theorem 7.1.([**Robbiano-Valla**, preprint]). Let $\{g_1,\ldots,g_s\}$ be a G-base of an ideal I w.r.t. a degree compatible term-ordering. Then $\{{}^h g_1,\ldots,{}^h g_s\}$ is a G-base of the ideal ${}^h I$ w.r.t. the induced term-ordering.

Proof. Since a homogeneous element in ${}^h I$ is of the type ${}^h f X_0^m$ and $M(f) = M({}^h f)$, we have $M({}^h f X_0^m) = M({}^h f)X_0^m = M(f)X_0^m$, hence $M({}^h I) \subset M(I)B = (M(g_1),\ldots,M(g_s))B = (M({}^h g_1),\ldots,M({}^h g_s))$.

The opposite inclusion being trivial, we get our thesis. ∎

Example (Macaulay's quartic curve) To find the projective closure of the curve given by $X = t$, $Y = t^3$, $Z = t^4$ whose ideal is $I = (X^3 - Y , XY - Z)$, we put $X < Y < Z$ and consider the degree-compatible given by $(1,1,1)$, $(-1,0,0)$, $(0,-1,0)$. Then the (reduced) G-base of I is

$$\{X^3 - Y , XY - Z , X^2Z - Y^2 , Y^3 - XZ^2\}$$

so ${}^h I$ is generated by

$$\{X^3 - YW^2 , XY - ZW , X^2Z - Y^2W , Y^3 - XZ^2\}.$$

Remark In the previous example, homogenizing the elements of G we get a minimal system of generators for ${}^h I$. In general it is not so - even if G is reduced. For instance, let us consider on $k[X,Y,Z,W]$ the ordering induced by $(1,1,1,1)$, $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$. Then the reduced G-base of the defining ideal of the monomial curve given by $X = t^4$, $Y = t^5$, $Z = t^6$, $W = t^7$ has 11 elements, but ${}^h I$ is minimally generated by 6 elements.

Ideals of monomial curves have been studied extensively; there are several specific algorithms to find a minimal system of generators: we remind here [**Herzog** ,1970] for monomial curves in $\mathbb{A}^3$, [**Bresinsky-Renschuch** ,1980] for those in $\mathbb{P}^3$, [**Elliahou** ,1983] for the general case in $\mathbb{A}^n$ and [**Cavaliere-Niesi** ,1984a] for that in $\mathbb{P}^n$.

Given a homogeneous ideal I, the <u>saturation</u> I^{sat} of I is the largest ideal $J \supset I$ such that $J_d = I_d$ for all $d \gg 0$.

Clearly I is saturated if and only if $I = I^{sat}$. The ideal I^{sat} is the largest ideal defining the same subscheme of $\mathbb{P}^n$ defined by I. I^{sat} can be obtained by taking a primary decomposition for I, and removing any primary ideals having the irrelevant ideal $(X_0,\dots,X_n)$ as associated prime.

Given $f \in B$, we put $(I:f^*) = \{ h \in B \,/\, f^t h \in I \text{ for some } t \}$.

Lemma 7.4. If $f \in (X_0,\dots,X_n)$ does not belong to any associated prime ideal of I, with the exception of $(X_0,\dots,X_n)$, then $(I:f^*) = I^{sat}$.

Proof. The ideal $(I:f^*)$ is saturated, because $(X_0,\dots,X_n)$ cannot be an associated prime of $(I:f^*)$. Let $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_t$ be a primary decomposition of I. Then $(I:f^*) = (\cap \mathfrak{q}_i : f^*) = \cap (\mathfrak{q}_i : f^*)$ and we have $(\mathfrak{q}_i:f^*) = (1)$ if the prime associated $\mathfrak{p}_i$ of $\mathfrak{q}_i$ contains f, and $(\mathfrak{q}_i:f^*) = \mathfrak{q}_i$ otherwise. ∎

Proposition 7.5. Consider on B the degree-compatible reverse lex term-ordering with $X_1 > \dots > X_n$. If $g_1 X_n^{a_1}, \dots, g_s X_n^{a_s}$ is a G-base for the ideal I, with none of $g_1,\dots,g_s$ divisible by X_n, then $\{ g_1,\dots,g_s \}$ is a G-base for $(I:X_n^*)$.

Note that the considered term-ordering has the following property:
(*) for each $f \in B$, X_n divides f if and only if X_n divides $M(f)$.

Proof. Let $u \in M((I:X_n^*))$. Then $u = M(f)$ for some $f \in (I:X_n^*)$, so $uX_n^m = M(f X_n^m) \in M(I)$. Thus uX_n^m is divisible by $M(g_i X_n^{a_i})$ for some i. Since g_i is not divisible by and (*) holds, $M(g_i)$ is not divisible by X_n.

if $u, v \in T(B)$, then $u <_B v$ if and only if $deg(u) < deg(v)$ or $deg(u) = deg(v)$ and ${}^a u <_A {}^a v$.

Theorem 7.3. ([**Möller-Mora**, 1984]). Let $\underline{f} = \{f_1, \ldots, f_m\}$ be a sequence of elements of A and let ${}^h\underline{f} = \{{}^h f_1, \ldots, {}^h f_m\}$. If $\{g_1, \ldots, g_s\}$ is a G-base of the ideal $({}^h\underline{f})$ of B w.r.t. $<_B$, then $\{{}^a g_1, \ldots, {}^a g_s\}$ is a G-base of the ideal $(\underline{f})$ of A w.r.t. $<_A$.

Proof. If $f \in I$, then there exists t such that $g = X_0^t {}^h f$ belongs to $({}^h f_1, \ldots, {}^h f_m)$. So $M(g) = X_0^t M({}^h f) = X_0^t M(f)$. On the other hand $M(g) = uM(g_i)$ for some $u \in T(B)$. Therefore
$M(f) = {}^a M(g) = {}^a u \, {}^a M(g_i) = {}^a u \, M({}^a g_i)$. ∎

Remark. Even if the G-base of $({}^h\underline{f})$ is reduced, that one of $(\underline{f})$ could be not such.

B) Saturation.

In this section we consider only homogeneous ideals. Here we wish to exhibit a Bayer's result [**Bayer**, 1985], which shows that the degree-compatible reverse lex ordering can be used for computing the saturation of an ideal.

Recall the following definitions:

Definition A homogeneous ideal I of $B = k[X_0, \ldots, X_n]$ is said to be saturated if, for all ideals $J \supset I$ such that $J_d = I_d$ for all $d \gg 0$, it results $I = J$.

S 8. Elimination and its applications

In this section we describe and give several examples of how to use G-bases in some problems which can be solved by elimination of variables.

Let $A = k[X_1,\dots,X_n]$ be a polynomial ring over a field k and let I be an ideal of A. The contraction $I \cap k[X_1,\dots,X_d]$ $(d < n)$ of I to the subring $k[X_1,\dots,X_d]$ of A is very easy to compute by means of G-bases related to a special class of term-orderings having the property "to separate" the eliminating variables $X_{d+1},\dots,X_n$ from the other ones.

From now on we denote the eliminating variables $X_{d+1},\dots,X_n$ by $Y_1,\dots,Y_{n-d}$. For shortness we shall write $\mathbf{X}$ for $X_1,\dots,X_d$ and $\mathbf{Y}$ for $Y_1,\dots,Y_{n-d}$; so we shall write for instance $A = k[\mathbf{X},\mathbf{Y}]$ and a monic monomial of A will be written as $X^A Y^B$.

Given two arbitrary term-orderings $<_x$, $<_y$ respectively on the set of the monic monomials $T(\mathbf{X})$, $T(\mathbf{Y})$ in the variables $\mathbf{X}$ and $\mathbf{Y}$, we define a term-ordering , called <u>elimination term-ordering</u>, on the set $T(A)$ of the monic monomials of A in the following way:

(*) $X^A Y^B < X^C Y^D$ if and only if $Y^B <_y Y^D$, or $Y^B = Y^D$ and $X^A <_x X^C$

The lexicographic ordering induced by $X_1 < X_2 < \dots < X_n$, i.e. the ordering described by the sequence of vectors $(e_n,\dots,e_1)$ where $e_1 = (1,0,\dots,0)$, $e_2 = (0,1,0,\dots,0),\dots, e_n = (0,\dots,0,1)$, is an elimination term-ordering.

Theorem 8.1. Let G be a G-base of I with respect to an elimination term-ordering. Then $G \cap k[\mathbf{X}]$ is a G-base of $I \cap k[\mathbf{X}]$ with respect to $<_x$.

<u>Proof</u>: Let $G \cap k[\mathbf{X}] = \{g_1,\dots, g_r\}$. From the definition of elimination term-ordering it follows that $M(f) \in k[\mathbf{X}]$ if and only if $f \in k[\mathbf{X}]$. Then $M(I \cap k[\mathbf{X}]) = M(I) \cap k[\mathbf{X}] = (M(g_1),\dots,M(g_r))$. ∎

Remark. A degree-compatible term-ordering is not an elimination term-ordering. Nevertheless if I is an homogeneous ideal for some graduation

Thus $M(g_i)$ divides u. Since each $g_i \in (I:X_n^*)$, $\{g_1,\ldots,g_s\}$ is a G-base for $(I:X_n^*)$. ∎

So, if X_n does not belong to any rilevant associated prime ideal of I, then the saturation of I can be computed using the degree-compatible reverse lex term ordering.

Remark If the field k is infinite, then there exists an element of degree 1, which does not belong to any non irrilevant associated prime ideal of I. But the choise of such an element is not deterministic.

c) Kernels

Proposition 8.2. Let $f_1,\dots,f_d \in k[T_1,\dots,T_m] = k[T]$ and let $\varphi: k[X] \longrightarrow k[T]$ be the ring homomorphism defined by $\varphi(X_i) = f_i$ for $i = 1,\dots,d$. Then we can compute $\operatorname{Ker}\varphi$.

Proof. We have $\varphi = \beta\alpha$ where $\alpha: k[X] \longrightarrow k[X,T]$ is the canonical embedding and $\beta: k[X,T] \longrightarrow k[T]$ is defined by $\beta(X_i) = f_i$, $\beta(T_i) = T_i$. Then $\operatorname{Ker}\varphi = \operatorname{Ker}\beta \cap k[X] = (X_1 - f_1,\dots, X_d - f_d)\,k[X,T] \cap k[X]$ can be computed using theorem 8.1. ∎

Corollary 8.3. a) Let φ as above and let J an ideal of $k[T]$. Then we can compute $\varphi^{-1}(J)$.

b) If $\psi: k[X] \longrightarrow k[T]/J$ is the ring homomorphism defined by $\psi(X_i) = \bar{f}_i$, then we can compute $\operatorname{Ker}\psi$.

Proof. In fact $\varphi^{-1}(J) = (J, X_1 - f_1,\dots, X_d - f_d)\,k[X,T] \cap k[X]$ and $\operatorname{Ker}\psi = \varphi^{-1}(J)$. ∎

d) Cartesian equations

If V is a variety given parametrically by $X_i = f_i(T_1,\dots,T_m)$, we can compute its cartesian equations by means of proposition 8.2. A G-base of the ideal $I(V)$ is the set of elements of a G-base of the ideal $(X_1 - f_1,\dots, X_d - f_d)\,k[X,T]$ which are in $k[X]$.

The following example shows that for a projective variety given parametrically we have an alternative method to find its ideal.

Example. Let $\mathbb{C}$ be the twisted cubic curve in $\mathbb{P}^3$ given parametrically by $X_0 = U^3$, $X_1 = TU^2$, $X_2 = T^2U$, $X_3 = T^3$.

A G-base of the ideal $J = (X_0 - U^3, X_1 - TU^2, X_2 - T^2U, X_3 - T^3) \subset k[X,T,U]$ with respect to the lexicographic order where $U > T > X_3 > \dots > X_0$, i.e. given by $(0,\dots,0,1)$, $\dots$, $(1,0,\dots,0)$, is $G = \{X_0 - U^3,\ X_1 - TU^2,\ X_2 - T^2U,\ X_3 - T^3,\ UX_2 - TX_1,\ UX_1 - TX_0,\ UX_3 - TX_2,\ X_2^2 - X_1X_3,\ X_0X_2 - X_1^2,\ X_0X_3 - X_1X_2\}$.

on A, then the previous theorem holds also for degree-compatible term-orderings satisfying (*) in any degree.

In fact we can repeat the proof in each degree n because the subspace $M(I_n)$ of A_n generated by the set of the leading monomials of elements of I_n is equal to the set $M(I)_n$ of degree n elements of $M(I)$.

Using elimination we are able to compute:

a) Projections

If I defines the subscheme S of $\mathbb{A}^n$ (or if an homogeneous ideal $J \subset A[X_0]$ defines the subscheme S' of $\mathbb{P}^n$) then $I \cap k[\mathbf{X}]$ (resp. $J \cap k[X_0,\mathbf{X}]$) defines the projection of S to $\mathbb{A}^d = \mathrm{Spec}\,(k[\mathbf{X}])$ (resp. of S' to $\mathbb{P}^d = \mathrm{Proj}\,(k[X_0,\mathbf{X}])$).

Example: Let $C \subset \mathbb{A}^3$ be the cubic curve defined by the equations $f = X^2 - Y = 0$, $g = XY - Z = 0$. The projection of C on the plane $Z = 0$ is defined by the ideal $(f,g) \cap k[X,Y]$. Since f,g are a G-base with respect to the lexicographic ordering where $X < Y < Z$, i.e. given by $(0,0,1)$, $(0,1,0)$, $(1,0,0)$, such projection is the curve defined by $X^2 - Y = 0$.

If we want the equation of the projection C' of C on the plane $X = 0$, we note that $f,g \notin k[Y,Z]$, but a G-base of the ideal (f,g) with respect to the lexicographic ordering where $X > Y > Z$, i.e. given by $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, is $G = \{X^2-Y, XY-Z, XZ-Y^2, Y^3-Z^2\}$. Then C' is defined by $Y^3-Z^2=0$.

b) Discriminant and resultant

We can compute the resultant of two polynomials f,g with respect to the variable X_1, in fact

$$\mathrm{result}_{X_1}(f,g) = (f,g) \cap k[X_2,\ldots,X_n].$$

Likewise the discriminant of a polynomial f with respect to the variable X_1 is

$$\mathrm{disc}_{X_1}(f) = (f, \partial f/\partial X_1) \cap k[X_2,\ldots,X_n].$$

As the form ring $G = \oplus_n J^n/J^{n+1}$ is isomorphic to $R'/(U)$, also G is computable.

f) The dimension of an ideal

It is very easy to check whether an ideal I of A is zero-dimensional by means of a G-base with respect to an arbitrary term-ordering. In fact we have:

Proposition 8.4. Let $G = \{ g_1, \ldots, g_s \}$ be a G-base of I. Then $\dim I = 0$ if and only if

(*) for each $i = 1, \ldots, n$ there exists $g_{ji} \in G$ such that $T(g_{ji}) = X_i^{m_i}$ for some $m_i \in \mathbb{N}$.

Proof. We have $\dim I = 0$ if and only if A/I is a k-vector space of finite dimension. By the theorem 6.1 a k-base $\bar{B}$ of A/I is the image in A/I of the set B of the terms which are not in the semigroup ideal S generated by $T(g_1), \ldots, T(g_s)$. Then B is finite if and only if for any i there exist e_i such that $X_i^{e_i} \in S$ and it is equivalent to condition (*). ∎

If $\dim I > 0$, we can compute it by means of the elimination, as shows the following proposition.

Proposition 8.5. $\dim I = \max \{ r \mid I \cap k[X_{i_1}, \ldots, X_{i_r}] = (0) \}$.

Proof. Let $m = \max \{ r \mid I \cap k[X_{i_1}, \ldots, X_{i_r}] = (0) \}$ and let $d = \dim I = \max \{ \dim \mathfrak{P} \mid \mathfrak{P} \supset I, \mathfrak{P} \text{ prime} \}$. Let $\mathfrak{P} \supset I$ such that $\dim \mathfrak{P} = d$. Since $A/\mathfrak{P}$ has trascendence degree d, d of the variables X_i are algebrically independent modulo $\mathfrak{P}$. In other words $\mathfrak{P} \cap k[X_{i_1}, \ldots, X_{i_d}] = (0)$ and $\mathfrak{P} \cap k[X_{i_1}, \ldots, X_{i_d}, X_j] \neq (0)$ for every $j \notin \{i_1, \ldots, i_d\}$. So $I \cap k[X_{i_1}, \ldots, X_{i_d}] = (0)$, that is $m \geq d$. Conversely we suppose that $I \cap k[X_{i_1}, \ldots, X_{i_m}] = (0)$ and $m > d$. Then, for every $\mathfrak{P} \supset I$ such that $\dim \mathfrak{P} = d$, it results $\mathfrak{P} \cap k[X_{i_1}, \ldots, X_{i_m}] \neq (0)$ and hence there exists $f \neq 0$ such that

Then $I(C) = J \cap k[X] = (X_2^2 - X_1X_3 , X_0X_2 - X_1^2 , X_0X_3 - X_1X_2)$.

Another way of computing $I(C)$, more efficient because it involves less parameters and less elements, is the following:

we consider the twisted cubic curve C' in $\mathbb{A}^3$ given by $X_1 = T$, $X_2 = T^2$, $X_3 = T^3$. Then C is the projective closure of C' .

We put on the monomials of $k[X,T]$ the term-ordering $X^A T^n < X^B T^m$ if and only if $n < m$, or $n = m$ and $X^A < X^B$ w.r.t. the degree compatible ordering with $X_1 < X_2 < X_3$ given by $(1,1,1)$, $(-1,0,0)$, $(0,-1,0)$.

So a G-base of the ideal $(X_1 - T , X_2 - T^2 , X_3 - T^3)$ is $G = \{ X_1 - T , X_2 - T^2 , X_3 - T^3, X_1^2 - X_2 , X_1X_2 - X_3 , X_2^2 - X_1X_3 \}$ and $G' = G \cap k[X] = \{ X_1^2 - X_2 , X_1X_2 - X_3 , X_2^2 - X_1X_3 \}$ is a G-base of $I(C')$ with respect to a degree compatible term-ordering.

Homogenizing the elements of G' we have a G-base of $I(C)$ (theorem 7.1).

e) Rees rings and form ring

Let I be an ideal of $k[X]$ and J an ideal of $k[X]/I$ generated by $\bar{f}_1, \ldots, \bar{f}_r$. The Rees ring of J is $R = \oplus_n J^n$ $(n \in \mathbb{N})$ and it results $R \cong (k[X]/I)[\bar{f}_1 T, \ldots, \bar{f}_r T] \subset (k[X]/I)[T]$.

Then $R \cong k[X,Y]/\mathrm{Ker}\ \psi$ where $\psi: k[X,Y] \longrightarrow (k[X]/I)[T]$ is the ring homomorphism defined by $\psi(X_i) = \bar{X}_i$, $\psi(Y_j) = \bar{f}_j T$.

So $\mathrm{Ker}\ \psi = (I, Y_1 - f_1T, \ldots, Y_r - f_rT)\, k[X,Y,T] \cap k[X,Y]$ can be computed by elimination.

Similarly the ring $R' = \oplus_n J^n$ $(n \in \mathbb{Z})$, also called Rees ring, is isomorphic to the ring $(k[X]/I)[\bar{f}_1 T, \ldots, \bar{f}_r T, T^{-1}] \cong k[X,Y,U]/\mathrm{Ker}\ \alpha$ where $\alpha: k[X,Y,U] \longrightarrow k[X,T,U]/(I, TU-1)$ is defined by $\alpha(X_i) = X_i$, $\alpha(U) = U$ and $\alpha(Y_i) = f_i T$, so $\mathrm{Ker}\ \alpha = (I, Y_1 - f_1T, \ldots, Y_r - f_rT, TU - 1)\, k[X,Y,U,T] \cap k[X,Y,U]$.

polynomial in $k[X_1]$. Then we can find the zeros of I by the following algoritm ([Buchberger ,1985]).

Algoritm 8.7.

INPUT G

OUTPUT $V(I)$

$p := G \cap k[X_1]$

$V_1 := \{ a \mid p(a) = 0 \}$

$i := 1$

While $i < n$ **do**

$V_{i+1} := \emptyset$

while $V_i \neq \emptyset$ **do**

choose $(a_1, \ldots, a_i) \in V_i$

$H := \{ g(a_1, \ldots, a_i, X_{i+1}) \mid g \in G \cap (k[X_1, \ldots, X_{i+1}] \setminus k[X_1, \ldots, X_i]) \}$

$p := G.C.D.(H)$

$V_{i+1} := V_{i+1} \cup \{ (a_1, \ldots, a_i, a) \mid p(a) = 0 \}$

$V_i := V_i \setminus \{ (a_1, \ldots, a_i) \}$

$V(I) := V_n$

Remarks.

To run the previous algoritm we need to know the zeros of polynomials in a single indeterminate with coefficients in the field k and in some algebraic extension of k .

Another subroutine required is a G.C.D. algoritm. Note that the G.C.D. of a finite set F of polynomials in a single variable is a reduced G- base of the ideal generated by F .

h) Operations on ideals

Several operations on ideals can be performed by means of the elimination process (cfr.[Gianni-Trager-Zacharias ,preprint]).

$f \in \cap_{\mathfrak{P}} (\mathfrak{P} \cap k[X_{i1},\ldots,X_{im}])$ $(\mathfrak{P} \supset I$, $\dim \mathfrak{P} = d)$. Then $f^n \neq 0$ and $f^n \in I$. This contradicts our assumption. ∎

Remark 8.6. Since the Hilbert functions $H(A/I)$ and $H(A/M(I))$ are equal (corollary 6.3), we have $\dim I = \dim M(I)$. Thus it suffices to be able to compute the dimension of monomial ideals.

Every system of generators of a monomial ideal J is trivially a G-base with respect to any term-ordering. Hence the computing of $\dim I$ is an easy matter.

The proposition 8.4 can be easily obtained as corollary of this result.

If $\mathfrak{P}$ is a prime ideal and we have found a particular d-uple $X_{i1},\ldots,X_{id}$ such that $\mathfrak{P} \cap k[X_{i1},\ldots,X_{id}] = (0)$ and $\mathfrak{P} \cap k[X_{i1},\ldots,X_{id},X_j] \neq (0)$ for any $j \notin \{i_1,\ldots,i_d\}$ we can conclude that $\dim \mathfrak{P} = d$. The following example shows that for an arbitrary ideal this is not sufficient.

Example. Let $I = (X_1^2, X_1X_3, X_1X_4, X_2X_3, X_2X_4) \subset k[X_1,\ldots,X_4]$. Then $I \cap k[X_2] = (0)$ and $I \cap k[X_2, X_i] \neq (0)$ for all $i \neq 2$, but $I \cap k[X_3, X_4] = (0)$ and $I \cap k[X_j, X_3, X_4] \neq (0)$ for $j = 1,2$. So $\dim I = 2$.

g) The zeros of a 0-dimensional ideal

Given an ideal I of A , by zero-locus $V(I)$ of I we mean the set of the zeros of all the elements of I in some algebraic extension of k . Of course it is enough to consider a finite system of generators $F = \{f_1,\ldots,f_m\}$ of I .

We have the following facts:

1. $V(I) \neq \emptyset$ if and only if $1 \notin I$, hence if and only if $1 \notin G$ for a reduced G-base G of I .

2. The set $V(I)$ is finite if and only if the ideal I is 0-dimensional.

3. Let I be a 0-dimensional ideal and let G be a reduced G-base of I with respect to the lex-ordering where $X_1 < X_2 < \ldots < X_n$, i.e. given by $(1,0,\ldots,0)$, $(0,1,0,\ldots,0),\ldots,$ $(0,\ldots,0,1)$. Then G contains exactly one

§ 9. Computation of some graded rings.

In this part we shall see how it is possible to compute some graded rings such as the Rees algebra, the form ring, the symmetric algebra.

a) Preliminaries

If I is an ideal of a ring A, we consider the family of ideals of A $\{I^n\}$, $n\in\mathbb{N}$ and we put $R_A(I)=\oplus_{n\geq 0} I^n$. In this A-module we define the following natural multiplication: if $x\in I^n$ and $y\in I^m$, then $xy\in I^{n+m}$.

Definition 9.1. The graded A-algebra $R_A(I)$ is termed the Rees algebra of the ideal I.

Consider now the abelian graded group $gr_I(A)=\oplus_{n\geq 0} I^n/I^{n+1}$ with the following multiplication: if $x\in I^n/I^{n+1}$ and $y\in I^m/I^{m+1}$, then $xy\in I^{n+m}/I^{n+m+1}$.

Definition 9.2. The graded ring $gr_I(A)$ is termed the form ring (or graded ring) associated to the ideal I (see also § 1).

In particular $gr_I(A)=R_A(I)/IR_A(I)$, hence the computation of $gr_I(A)$ is related to that of $R(I)$.

Now let M be an A-module, $T^n(M)$ the tensor product of n copies of M ($T^0(M)=A$) and define $T(M)=\oplus_{n\geq 0} T^n(M)$. It is possible to endow $T(M)$ with a structure of graded A-algebra since for any $p,q\in\mathbb{N}$ we have the A-linear canonical isomorphism $m_{pq}: T^p(M)\otimes_A T^q(M)\to T^{p+q}(M)$

Definition 9.3. The A-module $T(M)$ is termed the tensor algebra of M

Proposition 8.8. Let I, J be two ideals of A and let $f \in A$. Then:

1) The ideal $I \cap J$ is equal to $(TI, (T-1)J)A[T] \cap A$.

2) The ideal $(I:f^*) = IA_f \cap A$ is equal to $(I, Tf-1)A[T] \cap A$.

Proof. 1) We put $N = (TI, (T-1)J)A[T] \cap A$. Let $x \in I \cap J$, then $x = Tx - (T-1)x \in N$. Conversely let $f \in A$ such that $f = Tg + (T-1)h$ with $g \in IA[T]$, $h \in JA[T]$. Then g and h must have the same degree s in T. Let $g = \Sigma a_i T^i$, $h = \Sigma b_i T^i$, where $a_i \in I$, $b_i \in J$ for $i = 0,\dots,s$. It results $a_s = b_s$, $a_i = b_i - b_{i+1}$ for $i = 0,\dots,s-1$ and $f = -b_0$, thus $a_i, b_i \in I \cap J$ for all i and in particular $f \in I \cap J$.

2) We have $A_f \cong A[T]/(Tf-1)$. Let $\alpha: A \longrightarrow A[T]$ be the canonical embedding and let $\beta: A[T] \longrightarrow A[T]/(Tf-1)$ the canonical projection. Then $IA_f \cap A = (\beta\alpha)^{-1}(IA[T]/(Tf-1)) = \alpha^{-1}(I + \ker\beta) = (I, Tf-1)A[T] \cap A$. ∎

Corollary 8.9. Let I, f be as above. Then:

1) Let $G = \{g_1,\dots, g_r\}$ be a G-base of $I \cap (f)$ and let $H = \{h_1,\dots, h_r\}$ be such that $g_i = h_i f$, $i = 1,\dots,r$. Then H is a G-base of $(I : f)$.

2) $f \in \sqrt{I}$ if and only if $1 \in (I, Tf-1)A[T] \cap A$.

Proof. 1) Trivially $H \subset (I : f)$. Moreover for every $h \in (I : f)$ we have $hf \in I \cap (f)$, so $hf = \Sigma a_i g_i$ with $T(hf) \geq T(a_i g_i)$, $i = 1,\dots,r$, as G is a G-base of $I \cap (f)$ (theorem 4.13 (B3)).

But $T(hf) = T(h)T(f) \geq T(a_i h_i f) = T(a_i h_i)T(f)$, then $h = \Sigma a_i h_i$ and $T(h) \geq T(a_i h_i)$. This prove that H is a G-base of $(I : f)$.

2) $f \in \sqrt{I}$ if and only if $f^n \in I$ for some n, hence if and only if $1 \in (I : f^*)$. ∎

Remark 8.10. 1) If $J = (f_1,\dots, f_r)$ then $(I:J) = \cap (I : f_i)$ $i = 1,\dots,r$, so $(I : J)$ can be computed.

2) We can decide whether f is a zero-divisor modulo I. In fact f is a non zero-divisor modulo I if and only if $(I : f) = I$.

We are going to show how to reduce ourselves to the homogeneous case, even if we start from an inhomogeneous ideal.

Put $A = K[X_1,\dots,X_n]$, $B = A[X_0]$ and define the maps

$h: A \to B$, $a: B \to A$ as follows: if $f \in A$, $h(f) = {}^hf = X_0^{\deg f} f(X_1/X_0,\dots,X_n/X_0)$ and if $g \in B$, $a(g) = {}^ag = g(1,X_1,\dots,X_n)$ so that ${}^{ah}f = f$, while if f is a homogeneous polynomial in B then $f = X_0^t g$, $g \notin (X_0)$ and ${}^af = {}^ag$, ${}^{ha}f = g$.

If an ideal I of A is given through a system of generators $\{f_1,\dots,f_m\}$, let us denote by $\underline{f}$ the m-uple $f_1,\dots,f_m$, by $I = (\underline{f})$ the ideal generated by $\underline{f}$, by ${}^h\underline{f}$ the m-uple ${}^hf_1,\dots,{}^hf_m$ and by $({}^h\underline{f})$ the ideal generated by ${}^h\underline{f}$. Observe that if f is in I, then there is a t such that $X_0^t\,{}^hf$ is in $({}^h\underline{f})$ and if g is in $({}^h\underline{f})$, then ${}^ag$ is in I. Moreover if $\underline{g} = g_1,\dots,g_r$ is an r-uple of elements and we denote by $\underline{f}\,\underline{g}$ the mr-uple $(f_1g_1,\dots,f_mg_r)$, then $({}^h\underline{f})({}^h\underline{g}) = ({}^h(\underline{f}\,\underline{g}))$; in particular $({}^h\underline{f})^n = {}^h(I^n)$ for any $n \geq 0$.

Proposition 9.5. $R_A(I) \cong R_B(({}^h\underline{f}))/(X_0 - 1)R_B({}^h\underline{f})$

Proof. We consider the following morphism of groups $\varphi_n : ({}^hf)^n \to I^n$ which sends $f \in ({}^h\underline{f})^n$ in ${}^af$, and we note that if $f \in ({}^h\underline{f})^n$ then ${}^af$ is in I^n. Moreover if $f \in ({}^hf)^r$ and $g \in ({}^h\underline{f})^s$ with $r + s = n$, then $fg \in ({}^h\underline{f})^n$, $\varphi_n(fg) \in I^n$ and $\varphi_n(fg) = \varphi_r(f)\,\varphi_s(g)$ since ${}^a(fg) = {}^af\,{}^ag$.

It is clear that φ_n is an epimorphism, in fact if $F \in I^n$, then there is a t such that $X_0^t\,{}^hF \in ({}^h\underline{f})^n$ and $\varphi_n(X_0^t\,{}^hF) = F$. Let us prove now that $\operatorname{Ker}\varphi_n = (X_0 - 1)({}^h\underline{f})^n$; we have $(X_0 - 1)({}^h\underline{f})^n \subset \operatorname{Ker}\varphi_n$, conversely if $F \in ({}^h\underline{f})^n$, we can write $F = (X_0 - 1)H + d$ with $d \in A$.

It follows that $\varphi_n(F) = {}^aF = d = 0$. So it is induced an epimorphism of graded rings $\varphi : R_B(({}^h\underline{f})) \to R_A(I)$ whose kernel is the ideal $(X_0 - 1)R_B(({}^h\underline{f}))$ as required.

Definition 9.4. $S_A(M) = T(M)/J$ where J is the ideal of $T(M)$ generated by the elements $x \otimes y - y \otimes x$ with $x, y \in M$ is the symmetric algebra of M over A.

b) Computation of $R_A(I)$, $S_A(I)$ and $gr_I(I)$

If T is an indeterminate over A, we can identify the Rees algebra with the subring of $A[T]$ of the polynomials $\Sigma_r c_r T^r$, $r=0,\dots,p$, such that $c_r \in I^r$; in particular if $I = (f_1,\dots,f_m)$, then $R_A(I) = A[f_1T,\dots,f_mT]$.
If we consider the surjective map $g : A[T_1,\dots,T_m] \to R_A(I)$ which sends T_i in f_iT for $i=1,\dots,m$, we get $R_A(I) = A[T_1,\dots,T_m]/\operatorname{Ker} g$, where $\operatorname{Ker} g$ is the ideal of $A[T_1,\dots,T_m]$ generated by the homogeneous polynomials $F(T_1,\dots,T_m)$ such that $F(f_1,\dots,f_m)=0$.
Hence it is possible to find the generators of $\operatorname{Ker} g$ by using the "elimination", as it is described in § 8 e).
On the other hand if we consider the surjective map $k : A^m \to I$ which sends e_i in f_i, then it is defined the surjective map

$S(k) : S_A(A^m) = A[T_1,\dots,T_m] \to S_A(I)$ where $\operatorname{Ker} S(k)$ is the ideal of $A[T_1,\dots,T_m]$ generated by the linear forms $F(T_1,\dots,T_m)$ such that $F(f_1,\dots,f_m)=0$. It is then clear that $\operatorname{Ker} S(k) \subset \operatorname{Ker} g$ and in particular $\operatorname{Ker} S(k)$ is generated by the homogeneous part of degree one of $\operatorname{Ker} g$. Hence the computation of $S_A(I)$ and $gr_I(A)$ easily follows from that of $R_A(I)$.

We recall that if I is generated by a regular sequence $\{f_1,\dots,f_m\}$ in A, then $R_A(I) \cong S_A(I) \cong A[T_1,\dots,T_m]/(f_iT_j - f_jT_i)$ with $1 \le i < j \le m$ and $gr_I(A) = A/I[T_1,\dots,T_m]$.

Moreover if I is generated by homogeneous (or quasi-homogeneous) elements in $A=k[X_1,\dots,X_r]$, then an algorithm which computes $\operatorname{Ker} g$ has been implemented by Bayer and Stillman.

Observe that this algorithm has ending since the terms of f with same degree are a finite number.
What we are looking for is a set G of generators of I such that $\{ m_<(g) : g \in G \}$ generates $m_<(I)$ with respect to $<$ degree ordering.
Let "h" and "a" be the maps above defined, $I=(f_1,\dots,f_m)$ an ideal of A, $({}^hI) = ({}^hf_1,\dots,{}^hf_m)$ and $<_A$ a degree ordering.
We define the following degree term-ordering $<_B$ on $A[X_0]$:
$m_1 <_B m_2$ if $\deg(m_1)<\deg(m_2)$ or $\deg(m_1)=\deg(m_2)$ and ${}^am_1 >_A {}^am_2$.
So that if f is an homogeneous polynomials, then $m_{<_A}({}^af) = {}^aM_{<_B}(f)$.

Proposition 9.7. If $\{h_1,\dots,h_t\}$ is a Gröbner base for $({}^hI)$ with respect to $<_B$, then $\{{}^ah_1,\dots,{}^ah_t\}$ is a set of polynomials in I such that $\{m_{<_A}({}^ah_1),\dots, m_{<_A}({}^ah_t)\}$ generates $m_{<_A}(I)$.

Proof. If $f \in I$ we prove that $m_{<_A}(f) \in (m_{<_A}({}^ah_1),\dots, m_{<_A}({}^ah_t))$. There is $s \in \mathbb{N}$ such that $g=X_0^s\, {}^hf \in ({}^hI)$ and so $M_{<_B}(g) = X_0^s\, M_{<_B}({}^hf)$. Since $g \in ({}^hI)$, then $M_{<_B}(g) = m\, M_{<_B}(h_i)$ for some $i \le t$; it follows that ${}^a(X_0^s\, M_{<_B}({}^hf)) = {}^a(m\, M_{<_B}(h_i))$ and hence $m_{<_A}(f) = {}^am\ m_{<_A}({}^ah_i)$.

Remark 9.8. To find a $\mathfrak{m}$-standard base of an ideal I of $A=K[X_1,\dots,X_n]$, it is enough for example to find a Gröbner base of $({}^hI) \subset B=A[X_0]$ with respect to $<_B$ the usual degree ordering:
$1<X_1<\dots<X_n<X_0<X_1^2<X_1X_2<\dots<X_1X_n<\dots..$ and then to put $X_0=1$.

In the following A denotes a local ring with maximal ideal $\mathfrak{m}$ and I an ideal of A.

c) Lazard' s algorithm for the standard bases

We shall see that, in particular cases, to compute the Rees algebra and the form ring it is useful to introduce the notion of standard base (see also § 1).
If $A = K[X_1,\dots,X_n]$ and $f \in A$, we shall denote by $L(f)$ the homogeneous form of f of minimal degree and, if I is an ideal of A, $L(I)$ is the ideal of A generated by $\{ L(f) \ / \ f \in I \}$.
If $I = (f_1,\dots,f_m)$, then in general $L(I) \supseteq (L(f_1),\dots,L(f_m))$ and if $\mathfrak{m} = (X_1,\dots,X_n)$ we say that $\{f_1,\dots,f_m\}$ is a $\mathfrak{m}$ - standard base of I if $L(I) = (L(f_1),\dots,L(f_m))$.
The idea of [Lazard, 1983] is that every algorithm which computes Gröbner base can be used for standard bases by working with homogeneized polynomials.
Let $<$ be an ordering on the terms of A; we recall that, for any polynomial h of A, $m_<(h)$ (resp. $M_<(h)$) denotes the least (resp. greatest) term whose coefficient in h is not zero; if I is an ideal of A, $m_<(I)$ is the ideal generated by $\{ m_<(h) : h \in I \}$, while $M_<(I) = (\{ M_<(h) : h \in I \})$.
In [Mora, 1983] it is proved the following

Lemma 9.6. Let $<$ be any degree ordering; if G is a finite set of polynomials such that $\{ m_<(g) : g \in G \}$ generates $m_<(I)$, then G is a $\mathfrak{m}$ - standard base of I.

Proof. We shall prove that if $f \in I$, then $L(f) \in \{ L(g) : g \in G \}$. Since f is in I, $m_<(f) \in \{ m_<(g) : g \in G \}$; hence there is $g_1 \in G$ such that $m_<(f) = t_1 m_<(g_1)$ and then $f = t_1 g_1 + f_1$ with $f_1 \in I$, $m_<(f_1) > m_<(f)$.
If $\mathrm{mindeg}(f_1) > \mathrm{mindeg}(f)$, then $L(f) = t_1 L(g_1)$ and the result is proved.
Otherwise $L(f) = t_1 L(g_1) + L(f_1)$ and since $f_1 \in I$ there is $g_2 \in G$ such that $m_<(f_1) = t_2 m_<(g_2)$. In the same way we can write $f_1 = t_2 g_2 + f_2$ with $f_2 \in I$, $m_<(f_2) > m_<(f_1)$; if we repeat the same procedure, we find a representation of $L(f)$ in terms of $L(g)$ with $g \in G$.

$\{f_1,f_2,f_3\}$ is not a $\mathfrak{m}$-standard base of $\mathfrak{p}$ where $\mathfrak{m}=(x,y,z)$; in fact $G = y^4 - x^5 \in \mathfrak{p}$, but $L(G) \notin (L(f_1),L(f_2),L(f_3)) = (z^2,yz,xz)$. In this case $\{f_1,f_2,f_3,G\}$ is a $\mathfrak{m}$-standard base of $\mathfrak{p}$. Hence:

$$gr_{\mathfrak{m}/\mathfrak{p}}(R) = A/(z^2,yz,xz,y^4) \quad \text{and} \quad R_R(\mathfrak{m}/\mathfrak{p}) = A[T_1,T_2,T_3]/J$$

where $J = (xT_2-yT_1, xT_3-zT_1, yT_3-zT_2, x^3y^2 - z^2, x^3yT_2-zT_3, x^3T_2^2-T_3^2, yz-x^4, yT_3-x^3T_1, T_2T_3-x^2T_1^2, xz-y^3, xT_3-y^2T_2, T_1T_3-yT_2^2, y^4-x^5, y^3T_2-x^4T_1, y^2T_2^2-x^3T_1^2, yT_2^3-x^2T_1^3, T_2^4-xT_1^4)$.

To compute $S_{A/I}(\mathfrak{m}/I)$ it is easier. In fact if $\{f_1,\ldots,f_m\}$ is any system of generators of I and $\mathfrak{m}=(a_1,\ldots,a_n)$, then by Theorem 2.1 of [**Rossi**, 1979] $S_{A/I}(\mathfrak{m}/I) = A[a_1T,\ldots,a_nT]/(f_1,\ldots,f_m, f_1T,\ldots,f_mT)$.

d) Computation of $R_{A/I}(\mathfrak{m}/I)$, $gr_{\mathfrak{m}/I}(A/I)$ and $S_{A/I}(\mathfrak{m}/I)$

We consider the form ring $gr_{\mathfrak{m}/I}(A/I)=\oplus_{n\geq 0}(\mathfrak{m}/I)^n/(\mathfrak{m}/I)^{n+1}$ associated to $\mathfrak{m}/I$; the canonical epimorphism $\mathfrak{m} \to \mathfrak{m}/I$ induces the epimorphism $gr_{\mathfrak{m}}(A) \to gr_{\mathfrak{m}/I}(A/I)$ and we denote with I^* its kernel. Now if $A=K[X_1,\dots,X_n]$, then $gr_{\mathfrak{m}}(A)\simeq K[X_1,\dots,X_n]$ and $I^*=L(I)$. Hence if $\{f_1,\dots,f_m\}$ is a $\mathfrak{m}$-standard base of I, then $I^*=(L(f_1),\dots,L(f_m))$. We have already said that $R_A(\mathfrak{m}) \subset A[T]$, we denote with I' the homogeneous ideal $I\,A[T] \cap R_A(\mathfrak{m})$. It is clear that I' is the ideal of $R_A(\mathfrak{m})$ generated by the polynomials $\Sigma_r\, c_r T^r$, $r=0,\dots,p$, with $c_r \in I \cap \mathfrak{m}^r$, hence we have $R_{A/I}(\mathfrak{m}/I)=\oplus_{n\geq 0}(\mathfrak{m}/I)^n=\oplus_{n\geq 0}(\mathfrak{m}^n/\mathfrak{m}^n\cap I)=R_A(\mathfrak{m})/I'$. In [**Rossi**, 1979] I' is completely characterized through a $\mathfrak{m}$-standard base of I. First recall that if $f \in \mathfrak{m}$, we denote by $v_{\mathfrak{m}}(f)$ the greatest integer n such that $f \in \mathfrak{m}^n$.

Theorem 9.9. The following facts are equivalent :

i) $\{f_1,\dots,f_m\}$ is a $\mathfrak{m}$-standard base of I

ii) $I'=(f_1,f_1T,\dots,f_1T^{v_1},\dots\dots,f_m,f_mT,\dots,f_mT^{v_m})$ where $v_i=v_{\mathfrak{m}}(f_i)$

Remark 9.10. If $A=K[X_1,\dots,X_n]$, $\mathfrak{m}=(X_1,\dots,X_n)$, the epimorphism $g: A[T_1,\dots,T_n] \to R_A(\mathfrak{m})$ has as kernel the ideal $(X_iT_j - X_jT_i)$ $1\leq i<j\leq n$. If I is an ideal of A, $\{f_1,\dots,f_m\}$ a $\mathfrak{m}$-standard base of I with $v_r = \operatorname{mindeg}(f_r)$ and f_{rj} any element of $g^{-1}(f_rT^j)$, then

$$R_{A/I}(\mathfrak{m}/I)=A[T_1,\dots,T_m]/(X_iT_j - X_jT_i,\dots,f_r,f_{r1},\dots,f_{rv_r},\dots)$$ with $1\leq i<j\leq m$ and $r=1,\dots,m$.

Example 9.11. Let us compute the Rees algebra and the form ring associated to the maximal ideal of $R=K[t^4,t^5,t^{11}]$. It is known that $R=A/\mathfrak{p}$ where $A=K[x,y,z]$ and $\mathfrak{p}$ is the prime ideal of A generated by $f_1=x^3y^2-z^2$, $f_2=yz-x^4$, $f_3=xz-y^3$.

Möller H.M. - Mora F., (1983). The computation of the Hilbert function, Proc. EUROCAL 83 Springer L.N.C.S. 162, 157-167.

Möller H.M. - Mora F., (1984). Upper and lower bounds for the degree of Gröbner bases, Proc. EUROSAM 84 Springer L.N.C.S. 172-183.

Möller H.M. - Mora F. , (1986a). New constructive methods in classical ideal theory, J. Alg. 99.

Möller H.M. - Mora F. , (1986b). Computational aspects of reduction strategies to construct resolutions of monomial ideals, Proc. AAECC, Springer L.N.C.S.

Mora F., (1982). An algorithm to compute the equations of tangent cones, Proc. EUROCAM 82 Springer, L.N.C.S. 144 158-165.

Mora F., (1983). A constructive characterization of standard bases, Boll. U.M.I. Sez. D 2 41-50.

Robbiano L., (1985). Term orderings on the polynomial ring, Proc. EUROCAL 85,II Springer L.N.C.S. 204 513-517.

Robbiano L., (1986). On the theory of graded structures, J. Symb. Comp. 2.

Robbiano L. - Valla G.,(Preprint). On set theoretic complete intersections in the projective space, Preprint.

Robbiano L. - Valla G.,(1983). Free resolutions for special tangent cones, Commutative Algebra, Proc. of the Trento Conference, Lect. Notes in Pure and Appl. Math., 84, Marcel Dekker, New York.

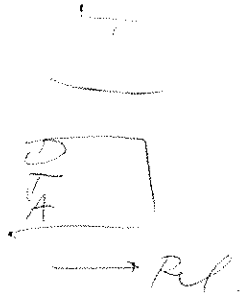
Rossi M.E.,(1979). Sulle algebre di Rees e simmetrica di un ideale, Le Matematiche, 34 107-119.

Schreyer F.O., (1980). Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrasschen Divisionsatz ... Diplomarbeit Hamburg.

Spear D., (1977). A constructive approach to commutative ring theory, Proc.MACSYMA Users' Conf. 369-376.

Trinks W., (1978). Über B.Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen, J.Number Th. 10 475-488.

Zacharias G., (1978). Generalized Gröbner bases in commutative polynomial rings, Bachelor Th. M.I.T.



References

Bayer D.A., (1982). The division algorithm and the Hilbert scheme, Ph.D.Thesis, Harvard.

Bayer D.A., (1985). An introduction to the division algorithm, Preprint.

Bayer D.A. - Stillman M., (1986). The design of Macaulay: A system for computing in algebraic geometry and commutative algebra, Preprint.

Bresinsky H. - Renschuch B., (1980). Basisbestimmung Veronesescher Projektionsideale mit allgemeiner Nullstelle $(t_0^m, t_0^{m-r}t_1^r, t_0^{m-s}t_1^s, t_1^m)$, Math. Nachr. 96 257-269.

Buchberger B., (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D.Thesis, Innsbruck.

Buchberger B., (1976a). A theoretical basis for the reduction of polynomials to canonical form, ACM SIGSAM Bull. 10-3,19-29.

Buchberger B., (1976b). Some properties of Gröbner bases for polynomial ideals, ACM SIGSAM Bull. 10-4,19-24.

Buchberger B., (1985). Gröbner bases:an algorithmic method in polynomial ideal theory. Recent trends in multidimensional systems theory (Bose N.K. Ed.), Reidel.

Cavaliere M.P. - Niesi G., (1984a). Sulle equazioni di una curva monomiale proiettiva, Ann. Univ. Ferrara, Sez. VII, Sc. Mat. 30.

Cavaliere M.P. - Niesi G., (1984b). Sulle curve monomiali proiettive intersezione completa, Boll. U.M.I., Algebra e Geometria, Serie VI, 3-D.

Ellahou S., (1983). Courbes monomiales et algèbre de Rees symbolique, Thèse n. 2080, Université de Genève.

Gianni P. - Trager B. - Zacharias G., (1984). Gröbner bases and primary decomposition of polynomial ideals, Preprint.

Goto S. - Yamagishi K., (1983). Finite generation of noetherian graded rings, Proc. Amer. Math. Soc. 98, 41-44.

Herzog J., (1970). Generators and relations of Abelian semigroups and semigroup rings. Manuscripta Math. 3.

Hironaka H., (1964). Resolution of singularities of an algebraic variety over a field of characteristic zero, Ann.Math. 79 109-326.

Lazard D., (1983). Gröbner bases,Gaussian elimination, and resolution of systems of algebraic equations, Proc.EUROCAL 83 Springer, L.N.C.S. 162 146-156.

Macaulay F.S., (1927). Some properties of enumeration in the theory of modular systems, Proc. London Math. Soc. 26 531-555.

Matsumura H. (1970). Commutative Algebra, Benjamin, New York.

Möller H.M., (1985). On the computation of Gröbner bases in commutative rings, Preprint.