Received by
B. Buchberger
1986 -06- 23

STANDARD BASES IN NON-COMMUTATIVE POLYNOMIAL RINGS

Teo Mora
Università di Genova

INTRODUCTION

This paper is a sequel of [MOR1], where I generalized the concept of Gröbner bases [BUC1,3] to non-commutative polynomial rings and discussed their main properties and semidecision procedures to compute them.

In the case of commutative polynomial rings and positive term orderings, there are different equivalent characterizations of Gröbner bases, the most important being the following:

F is a Gröbner basis of an ideal $I \subset K[X_1,\dots,X_n]$ if:

A the "maximal terms" of the basis elements generate the semigroup $M_T(I)$ of all maximal terms of elements in I

B every $f \in I$ can be represented as $f = \sum g_i f_i$, $f_i \in G$ so that the maximal term of f is not lower than every maximal term of $g_i f_i$.

C the terms which are not in $M_T(I)$ generate a K-vector space which is isomorphic to $K[X_1,\dots,X_n]/I$, and this isomorphism is computable.

D property B holds for a finite set of polynomials explicitly defined in terms of the basis elements.

(remark that B and C can be expressed in terms of the Buchberger reduction relation and then become respectively: each element in I can be reduced to 0; each element can be reduced to a unique irreducible element).

Properties immediately analogous to these still hold and are equivalent also in the case of non-commutative polynomial rings, so any of them can be chosen as a definition of Gröbner bases.

They are, however, no more equivalent in the other known generalizations of Gröbner bases; for instance when one consider polynomials over a ring (instead than over a field) [ZAC,SCH,KAK,MÖL,PAN] they lead to different concepts of basis.

In particular, when one still works on $P = K[X_1,\dots,X_n]$, but relaxes the condition of positiveness on the term ordering, so introducing the concept of standard bases [HIR,GAL,LAZ], not only examples suggest that it is difficult to find a statement analogous to C [MOR3], but A and B are equivalent only if stated in some extension R of the polynomial ring P (namely either the localization at the origin or the completion), and then B is verified not only by polynomials in I, but also by polynomials in $IR \cap P$, the contraction of the extension of I in R.

The results of Robbiano in his theory of graded structures [ROB1], which is a proposal of a generalization and unification of the known concepts of special bases (Gröbner, Macaulay, standard bases) together with other concepts related to the theories of graded and filtered rings, clearly show that in the general case, it is impossible to have equivalence between (the generalizations of) A and B.

In [MOR1] I gave a definition sufficiently general to allow for a common treatment also of standard bases in non-commutative polynomial rings. This was done choosing A as a definition of generalized Gröbner bases (which I called <u>d-sets</u>), and using (following [LAZ] and [ROB2]) a concept of term ordering more general than the one introduced by Buchberger [BUC1,3], i.e. relaxing the condition of positiveness for a term ordering.

While it was to be expected that A and B were no more equivalent for non-positive term orderings, it was possible to give a weaker analogon of B (each polynomial in I has a <u>d-representation</u>) which was equivalent to A, but which had some unexpected features:

1) the definition doesn't involve representations of polynomials in the ideal through the basis elements, with coefficients chosen in some extension ring are allowed;

2) the definition implies that a d-set is not necessarily a basis neither of the ideal (as it already happens for standard bases in the commutative case) nor of its extension in some extension ring.
However, as it will be shown in example 2 below, this analogon of B cannot be improved.

The aim of this note is then to give a possible interpretation of its unexpected features: it will come out that the problems are originated more by non-noetherianity than by non-commutativity; and that the analogon of B makes perfectly sense, once interpreted in terms of ring completions as follows:

> F is a d-set of I, if, denoting I^ the closure of I in the completion of the polynomial ring w.r.t. a topology naturally induced by a term ordering, each element in I^ can be obtained as a limit of a Couchy sequence of polynomials, each of them with a "good" representation in terms of F.

So a concept, more similar in nature to the one related to representations through Gröbner bases, can still be applied, but just to elements "approximating" the elements one has to represent.

This helps to understand the role of the formal power series ring in the definition of (commutative) standard bases, it stresses the fact (already suggested in [ROB1]) that Gröbner bases and their generalizations have a strong connections with ring topologies; it suggests also how to state a generalization of B which is still equivalent to (the generalization of) A in the general context of graded structures.

1.RECALLS

1.1 Let S denote a free semigroup generated by a finite alphabet A.
If m,n are in S, we will say m is a <u>multiple</u> of n (n <u>divides</u> m) iff there are l,r in S s.t. $m = l n r$.
$K[S]$, K a field, will denote the ring whose elements are finite linear combinations of elements of S:

$$K[S] := \Sigma_i c_i m_i : c_i \in K^*, m \in S,$$

with multiplication canonically defined in terms of the semigroup multiplication.

1.2 A <u>term ordering</u> $<$ on S is a total ordering s.t.:

i) for all m, m_1, m in S, $m_1 < m_2$ implies $m m_1 < m m_2$ and $m_1 m < m_2 m$.

ii) for all m in S, there exists no infinite decreasing sequence $m_1 > \ldots > m_i > \ldots$ s.t. for all i, $m_i > m$.

A term ordering will be called <u>positive</u> iff $1 \leq m$ for all m in S; a term ordering will be called <u>negative</u> iff $1 \geq m$ for all m in S or equivalently iff $m \geq m n$ and $m \geq n m$ for all m,n in S.

1.3 Let $<$ be a term ordering on S. If $f = \Sigma_{i=1,t} c_i m_i$, $c_i \in K^*, m_i \in S$, $m_1 > m_2 > \ldots > m_t$, define $M_T(f) := m_1$, $lc(f) = c_1$.
If $G \subset K[S]$, define $M_T(G) := \{ M_T(f) : f \in G^* \}$.
If I is a two-sided non-zero ideal of $K[S]$, $M_T(I)$ is a two-sided ideal of S.

1.4 A <u>distinguished set</u> (shortly a d-set) for I is a set $F \in I^*$ s.t. $M_T(F)$ generates $M_T(I)$.

1.5 We say that f in $K[S]$ has a <u>d-representation</u> in terms of a (possibly infinite) set $F \subset K[S]$ iff there is a sequence $g_1, \ldots, g_i, \ldots$ s.t. $g_1 = f$ and for all i:

1) $g_i \in K[S]$

2) if $g_i = 0$ then $g_{i+1} = 0$

3) if $g_i \neq 0$ then there are $l_i, r_i \in S$, $a_i \in K^*$, $f_i \in F$ s.t.

   i) $g_{i+1} = g_i - a_i l_i f_i r_i$

   ii) $M_T(g_i) = l_i M_T(f_i) r_i$

   iii) if $g_{i+1} \neq 0$ then $M_T(g_i) > M_T(g_{i+1})$

We say that f has a <u>finite d-representation</u> in terms of F iff

1) $f = \Sigma_{i=1,t} a_i l_i f_i r_i$, $a_i \in K^*$, $l_i, r_i \in S$, $f_i \in F$.

2) $M_T(f) = l_1 M_T(f_1) r_1 > l_i M_T(f_i) r_i \geq l_{i+1} M_T(f_{i+1}) r_{i+1}$ for all $i > 1$

Let us denote, for each m in S, $U(m)$ the K-vector space with basis $\{ n : n \in S, n < m \}$.
We say that f has a <u>mod. m</u> <u>d-representation</u> in terms of F iff there is g s.t. g has a finite d-representation in terms of F and $f-g$ is in $U(m)$, equivalently iff f has a finite d-representation in terms of $F \cup \{ n : n \in S, n < m \}$.

1.6 THEOREM The following conditions are equivalent:

1) F is a d-set for I

2) every f in I has a d-representation in terms of F

3) for all f in I, for all m in S, f has a mod. m d-representation in terms of F.

<u>Proof</u>:[MORI] Prop.2.2.

1.7 Given an ordered pair of terms, $(m_1,m_2) \in S^2$, the <u>set of matches</u> of (m_1,m_2), denoted by $M(m_1,m_2)$, is the finite set of all 4-tuples $(l_1,l_2,r_1,r_2) \in S^4$ s.t.either:

1) $l_1 = r_1 = 1$, $m_1 = l_2 m_2 r_2$

2) $l_2 = r_2 = 1$, $m_2 = l_1 m_1 r_1$

3) $l_2 = r_1 = 1$, $l_2 \neq 1$, $r_1 \neq 1$, there is $w \in S$ s.t. $w \neq 1$, $m_1 = l_2 w$, $m_2 = w r_1$

4) $l_2 = r_1 = 1$, $l_1 \neq 1$, $r_2 \neq 1$, there is $w \in S$ s.t. $w \neq 1$, $m_1 = w r_2$, $m_2 = l_1 w$.

1.8 LEMMA Let I be an ideal in $K[S]$, $F \subset I^*$ a basis of I, $m \in S$. The following are equivalent:

1) every $g \in I^*$ has a mod. m d-representation in terms of F

2) for all $f_1, f_2 \in F$, for all $(l_1,l_2,r_1,r_2) \in M(m_1,m_2)$, for all $l,r \in S$,

$$f := lc(f_2)\ l\ l_1\ f_1\ r_1\ r - lc(f_1)\ l\ l_2\ f_2\ r_2\ r$$

(if not zero) has a mod. m d-representation in terms of F.

<u>Proof</u>: [MORI]2.4.

1.9 COROLLARY With the same assumptions as in Lemma 1.8, if $<$ is negative, then the following are equivalent:

1) every $g \in I^*$ has a mod. m d-representation in terms of F

2) for all $f_1, f_2 \in F$, for all $(l_1,l_2,r_1,r_2) \in M(m_1,m_2)$,

$$f := lc(f_2) l_1 f_1 r_1 - lc(f_1) l_2 f_2 r_2$$

(if not zero) has a mod. m d-representation in terms of F.

<u>Proof</u>: 2)$\Rightarrow$1) We have just to prove that 1.8.2) holds.
Let then $f_1, f_2 \in F$, $(l_1,l_2,r_1,r_2) \in M(m_1,m_2)$, $f := lc(f_2)\ l_1 f_1 r_1 - lc(f_1)\ l_2 f_2 r_2$, and assume $f \neq 0$; let $l,r \in S$ and $g := l\ f\ r$.
By assumption we know f has a mod. m d-representation, i.e there is

$h \in U(m)$ s.t. $f - h = \Sigma_{i=1,t}\, a_i l_i f_i r_i$ is a finite d-representation. Then, since $<$ is negative, $l h r \in U(m)$ and $g - l h r = \Sigma_{i=1,t}\, a_i l l_i f_i r_i r$ is a finite d-representation.

2. AN EXAMPLE

2.1. The aim of the following example is to show that, accepting as definition of d-set the one given in 1.5 (i.e. a definition naturally involving "the ideal of maximal terms"), we cannot hope to improve on the concept of d-representation given in 1.5. We will show in fact that it is unavoidable to have not just a "series representation" involving infinitely many summands, but also infinitely many basis elements will be required in the representation.

2.2 Let $A := \{a,b,c,d,e\}$, S the free semigroup generated by A, $<$ any term ordering s.t. for all m,n in S, $\deg(m) > \deg(n)$ implies $m<n$ (e.g. the inverse of the graduated term ordering defined in [MOR1] 5.11).
Let $f_0 := bedc - cdc^3$, $f_i := ab^ic - ab^{i+2}e$ (for $i \ge 1$, so $M_T(f_0) = bedc$, $M_T(f_i) = ab^ic$ if $i \ge 1$.
Because of [MOR1] 2.4, $G := \{ f_i : i \in \mathbb{N} \}$ is a d-set for the ideal it generates.
Let $m_i := ab^icdc^{2i-1}$, $i \ge 1$, and $n_i := ab^{i+2}edc^{2i-1}$, $i \ge 1$.

2.3 It is then immediate that the following hold:

1) if $m_i - t = l f_j r$, $t,l,r \in S$, then $j = i$, $t = n_i$.
2) if $t - m_i = l f_j r$, $t,l,r \in S$, then $j=0$, $i>1$, $t = n_{i-1}$
3) if $n_i - t = l f_j r$, $t,l,r \in S$, then $j=0$, $t = m_{i+1}$
4) if $t - n_i = l f_j r$, $t,l,r \in S$, then $j = i$, $t = m_i$
5) $\{ t \in S : t - m_1 \in I \} = \{ m_i : i \in \mathbb{N} \} \cup \{ n_i : i \in \mathbb{N} \}$
6) m_1 is not in I; for all t in S, m_1 is in $I + U(t)$ and has a mod. t d-representation in terms of G:
for, let $d := \deg(t)$, s s.t. $d < 3s+2$, then
$$m_1 = \Sigma_{i=1,s-1}\, f_i dc^{2i-1} + (\Sigma_{i=1,s-1}\, ab^{i+1}) f_0 + m_s$$
is such a representation
7) the only d-representation of m_1 in terms of G is (using with some abuse of notation a "series" representation):
$$m_1 = \Sigma_{i=1,\infty}\, f_i dc^{2i-1} + (\Sigma_{i=1,\infty}\, ab^{i+1}) f_0.$$

2.4. It should then be clear that the concept of d-representation proposed in 1.5 cannot be improved and that no technique as in [MOR2,3]

to compute d-representations in finitely many steps can be applied.

3. POLYNOMIALS WITH d-REPRESENTATIONS

3.1 The example above shows another bad feature of d-representations: there are polynomials not in the ideal, which have d-representations in terms of a distinguished set of the ideal.
This parallels a situation which occurs also for standard bases in commutative polynomial rings: there, if I is a polynomial ideal, all polynomials which are in IA, A being either the localization or the completion of the polynomial ring, have a series representation in terms of a standard basis of I.
The aim of this section is to characterize the set of polynomials with d-representations in terms of a d-set of the ideal; we like to give a characterization given in terms of operations within the polynomial ring only; obviously such a characterization is possible also in the commutative case.

3.2 DEFINITION If I is an ideal of $K[S]$, denote $C(I) := \bigcap_{m \in S} (I + U(m))$.

3.3 REMARK If $<$ is positive, since $U(1) = 0$, $C(I) = I$, so the results below are trivial in this case.
If $<$ is not positive, there is $n \in S$, $n<1$. There is then an infinite decreasing sequence of terms $n_1,\dots,n_i,\dots$: one obtains such a sequence defining $n_i := n^i$. In the proofs below, we will freely make reference to this sequence.

3.4 PROPOSITION If I is an ideal of $K[S]$, $C(I)$ is an ideal of $K[S]$.
Proof: Remark that if $<$ is positive, $C(I) = I$, so we need a proof only in the case that there exists $n \in S$, $n<1$.
We have to prove that if $f \in C(I)^*$, $g \in K[S]^*$, then fg and gf are in $I + U(m)$ for every $m \in S$; we will proof just that, given $m \in S$, $fg \in I + U(m)$, since the other proof is symmetrical.
Let $n' := M_T(g)$; in the decreasing sequence $n'_1,\dots,n'_i,\dots$ where $n'_i := n_i n'$, there is i s.t. $n'_i < m$. Since $f \in I + U(n_i)$, there are $h' \in I, h'' \in U(n_i)$, s.t. $f = h' + h''$; so $fg = h'g + h''g$, with $h'g \in I$, $h''g \in U(n'_i) \subset U(m)$. So $fg \in I + U(m)$.

3.5 PROPOSITION The conditions of Theorem 1.6 are equivalent to:
4) $f \in C(I)$ iff f has a d-representation in terms of F.
Proof: 1)$\to$4): Assume $f \in K[S]^*$ has a d-representation in terms of F. Then (by implication 2$\to$3 of theorem 1.6) for each $m \in S$ there is g s.t. $f - g \in U(m)$ and g has a finite d-representation in terms of F. Then $g \in I$, so $f \in I + U(m)$ for each $m \in S$, and $f \in C(I)$.
Conversely, we want to show that for each $f \in C(I)^*$, f has a

d-representation in terms of F. Because of remark 3.3, we have to prove it only in the case $<$ is not positive, and because of Theorem 3.6 we can prove instead that F is a d-set for C(I).
So, let $f \in C(I)^*$, $m := M_T(f)$; since $f \in I + U(m)$, there is $g \in I$ s.t. $f - g \in U(m)$; then $M_T(g) = M_T(f)$, and since F is a d-set for I, $M_T(f)$ is in the ideal generated by $M_T(F)$.

4)$\Rightarrow$2): obviously if $f \in I^*$, $f \in C(I)^*$, so it has a d-representation in terms of F.

4. RING COMPLETIONS

4.1 We intend now to give an interpretation of d-representations in terms of ring completions. Therefore, we premit some recalls on basic concepts which will be useful in the following of the paper.

4.2 Let R be an associative ring, for each $m \in S$ let $U(m)$ be a subgroup of R.
We say $U := \{ U(m) : m \in S \}$ is an <u>S-filtration</u> of R if, for each $m, n \in S$, $U(m)U(n) \subset U(mn)$.
The S-filtration U induces a topological group structure on R (the one which is obtained considering U as a system of neighboroughs of zero), which is Hausdorff iff $\cap U(m) = 0$.
We say R is an <u>S-filtered ring</u> if, moreover, R is a topological ring w.r.t. the topology induced by U.

4.3 If R is an S-filtered ring, with U as filtration, a sequence $(f_i : i \in \mathbb{N})$ of elements of R is called a <u>Cauchy sequence</u> iff for every $m \in S$ there is $n \in \mathbb{N}$ s.t. for all $s, t \geq n$, $f_s - f_t \in U(m)$.
A sequence $(f_i : i \in \mathbb{N})$ <u>converges</u> to $f \in R$ (f is a <u>limit</u> of $(f_i : i \in \mathbb{N})$) iff for every $m \in S$ there is $n \in \mathbb{N}$ s.t. for all $s \geq n$, $f - f_s \in U(m)$.
Two Cauchy sequences (f_i) and (g_i) are called <u>equivalent</u> iff $(f_i - g_i)$ converges to 0.
R is called <u>complete</u> iff each Cauchy sequence of elements of R converges to an element of R.
Each S-filtered ring R has a <u>completion</u> R^ w.r.t. the topology induced by U, i.e. R^ is a topologically complete ring, s.t. R is topologically isomorphic to a dense subring of it (see e.g. [NUO]).

4.4 Clearly, $U := \{ U(m) : m \in S \}$ is an S-filtration on K[S], and the topology induced by it is Hausdorff, and moreover is discrete iff $<$ is positive. In this case, K[S] is a complete topological ring with respect to this topology.

Therefore, in the following, we will exclude this trivial case, while, obviously, the results below hold also in this case. So, throughout this section, we will assume $<$ is not positive; $n_1, \ldots, n_i, \ldots$ will denote the infinite decreasing sequence defined in Remark 3.3

4.5 LEMMA K[S] is an S-filtered ring with $U := \{ U(m) : m \in S \}$ as S-filtration.
<u>Proof</u>: We have just to prove that, for each $m \in S$, there are m', m'' in S, s.t. if $f \in U(m')$, $g \in U(m'')$, then $fg \in U(m)$.
To prove this, fix an arbitrary m' and let $n'_1, \ldots, n'_i, \ldots$ be the decreasing sequence defined by $n'_i := m'n_i$; there is i s.t. $n'_i < m$. Define then $m'' := n_i$.
Then $fg \in U(m'm'') \sim U(n'_i) \subset U(m)$.

4.6 We intend here to give a representation of K[S]^ which is different by the one recalled in 4.3.
Define K[[S,<]] to be the set of all applications $f: S \to K$ s.t. there is no increasing sequence (m_i) of elements of S with $f(m_i) \neq 0$ for all i.
K[[S,<]] is given a ring structure, defining:

$(f+g)(m) := f(m)+g(m)$

$(fg)(m) := \Sigma f(m')g(m'')$, where the sum runs on all pairs (which are finitely many) s.t. $m'm''=m$.

Since K[S] can be defined as the ring of those functions $f: S \to K$ which are zero a.e., K[S] can be canonically identified as a subring of K[[S,<]].
This definition naturally extends the definition of the (commutative) "formal power series" ring $K[[X_1, \ldots, X_n]]$, so we will (with the usual abuse of notations) use a "series representation" for the elements of K[[S,<]] which are not in K[S], denoting them as: $\Sigma_{i=1,\infty} c_i m_i$, $c_i \in K^*$, $m_i \in S$, $m_i > m_{i+1}$ for all i.
For every such element f, one can define $M_T(f) := m_1$, $lc(f) := c_1$.
One can also define $U(m)^\wedge := \{ f \in K[[S,<]], f=0 \text{ or } M_T(f) < m \}$.
One has then that $U^\wedge := \{ U(m)^\wedge : m \in S \}$ is an S-filtration inducing an S-filtered ring structure on K[[S,<]] and that $U(m) = U(m)^\wedge \cap K[S]$.

4.7 LEMMA K[[S,<]] is the completion of K[S].
<u>Proof</u>: i) <u>K[[S,<]] is complete</u>
Let (f_i) be a Cauchy sequence in K[[S,<]].
We intend to construct a (not necessarily infinite) decreasing sequence $m_1, \ldots, m_i, \ldots$ of elements of S and a sequence $c_1, \ldots, c_i, \ldots$ (indexed on the same set) of elements of K^*, s.t. (f_i) converges to $\Sigma c_j m_j$.
If one can extract from (f_i) an infinite subsequence (g_j) s.t. $M_T(g_j)$

form a decreasing sequence, then (f_i) converges to 0.
Otherwise there is N s.t. if $s \geq N$ then $lc(f_s)M_T(f_s)$ is constant.
Define then $m_1 := M_T(f_N)$, $c_1 := lc(f_N)$.
Remark that the Cauchy sequence (g_i) with $g_i := f_i - c_1 m_1$ for all i, is s.t. $M_T(g_i) < m_1$ for sufficiently large i.
Assume now we have defined $c_1, \dots, c_n$, $m_1, \dots, m_n$ s.t. the m_i's are a decreasing sequence and the Cauchy sequence (g_i) with $g_i := f_i - \Sigma_j c_j m_j$ for all i, is s.t. $M_T(g_i) < m_n$ for sufficiently large i.
Then, again, either one can extract from it an infinite subsequence (h_j) s.t. $M_T(h_j)$ form a decreasing sequence, in which case (g_i) converges to 0, and (f_i) to $\Sigma_j c_j m_j$; or there is N s.t. if $s \geq N$ then $lc(g_s)M_T(g_s)$ is constant, in which case one defines $m_{n+1} := M_T(f_N)$, $c_{n+1} := lc(f_N)$, and the procedure can be repeated.
If, in this way, one obtains an infinite decreasing sequence $m_1, \dots, m_i, \dots$ of elements of S and a corresponding sequence $c_1, \dots, c_i, \dots$ of elements of K^*, then clearly (f_i) converges to $g := \Sigma c_j m_j$, since for all $m \in S$ there is n s.t. $m_n < m$, and, if s is sufficiently large:

$$M_T(f_s - g) \leq M_T(f_s - \Sigma_{j=1,n} c_j m_j) < m_n < m.$$

2) <u>For each element of $K[[S,<]]$ there is a Cauchy sequence in $K[S]$ converging to it</u>
If $f \in K[S]$, then the thesis is obvious. Otherwise let $f =: \Sigma_{j=1,\infty} c_j m_j$; define $f_n := \Sigma_{j=1,n} c_j m_j$. Then clearly (f_n) converges to f.

5. RING COMPLETIONS AND d-REPRESENTATIONS

5.1 LEMMA Let $I^\wedge \subset K[[S,<]]$ be the ideal of all limits of Cauchy sequences in I. Then the following hold:

1) $M_T(I^\wedge) = M_T(I)$
2) $I^\wedge = \cap(I^\wedge + U(m)^\wedge)$
3) $C(I) = I^\wedge \cap K[S]$

<u>Proof</u>: 1): Let $f \in I^\wedge$, $f \neq 0$; (f_i) a Cauchy sequence of elements of I converging to it; by the argument in the proof of Prop.4.7.1), if s is sufficiently large, $M_T(f) = M_T(f_s)$. So the thesis.
2): Let $f \in \cap(I^\wedge + U(m)^\wedge)$; then for each n_i in the decreasing sequence of terms defined in 4.4, there are $f_i \in I^\wedge, g_i \in U(n_i)^\wedge$ s.t. $f = f_i + g_i$.
Since f_i is the limit of a Cauchy sequence of elements of I, there is $p_i \in I$ s.t. $f_i - p_i \in U(n_i)^\wedge$. Then (p_i) is a Cauchy sequence of elements of I converging to f, since, for each i, $f - p_i = g_i + (f_i - p_i) \in U(n_i)^\wedge$. Therefore $f \in I^\wedge$.
3): If $f \in I^\wedge \cap K[S]$, then, by the argument above, it is the limit of a Cauchy sequence (p_i) of elements of I. So for each m, if s is sufficiently large, $f - p_s \in U(m)^\wedge \cap K[S] = U(m)$; so for each m, $f = p_s + (f - p_s) \in I + U(m)$, therefore $f \in C(I)$.

5.2 LEMMA If $f \in K[S]$ has a d-representation in terms of F, then f is the limit of a Cauchy sequence (p_i) of elements of K[S], s.t. each p_i has a finite d-representation in terms of F.
<u>Proof</u>: Let g_i, a_i, l_i, f_i, r_i be as in 1.5.
For every n, define $p_n := g_1 - g_{n+1} = \Sigma_{i=1,n} a_i l_i f_i r_i$; then, for every n, p_n has a finite d-representation in terms of F.
We need to show that (p_n) is a Cauchy sequence converging to f; this is obvious if $g_n = 0$ for large n, so assume $g_n \neq 0$ for every n.
$(M_T(g_n))$ is then a decreasing sequence, so for each $m \in S$ there is n s.t. $M_T(g_n) < m$. Therefore for each $m \in S$, there is n s.t. if $s, t \geq n$, $p_t - p_s = g_{s+1} - g_{t+1} \in U(M_T(g_n)) \subset U(m)$, and $f - p_s = g_{s+1} \in U(M_T(g_n)) \subset U(m)$.
This completes the proof.

5.3 THEOREM The following conditions are equivalent:

1) F is d-set for I
5) $M_T(F)$ generates $M_T(I^\wedge)$
6) $f \in I^\wedge$ iff there is a Cauchy sequence (p_i) of elements of K[S] converging to f, s.t. each p_i has a finite d-representation in terms of F.

<u>Proof</u>: 1⇔5) : obvious from Lemma 5.1.1)
6)⇒5): Let $m \in M_T(I^\wedge)$, $f \in I^\wedge$ s.t. $m = M_T(f)$, (p_i) the Cauchy sequence of elements of K[S] converging to f, whose existence is implied by 6).
Then, if s is sufficiently large, $M_T(p_s) = m$, and if $\Sigma c_i l_i f_i r_i$ is the finite d-representation of p_s in terms of F, $M_T(f) = l_1 M_T(f_1) r_1$.
5)⇒6): If f is the limit of a Cauchy sequence (p_i) of elements of K[S], s.t. each p_i has a finite d-representation in terms of F, then for all i, $p_i \in (F) \subset I$, so $f \in I^\wedge$.
Conversely, if $g \in I^\wedge$, there are $f_1 \in F$, $l_1, r_1 \in S$, s.t. $M_T(g) = l_1 M_T(f_1) r_1$.
Then $g_2 := g_1 - l_1 f_1 r_1$ either is 0 or is s.t. $M_T(g_1) < M_T(g)$.
We can repeat the argument getting a sequence $g = g_0, \dots, g_n, \dots$ of elements of $I^\wedge$ s.t., for all i

1) if $g_i = 0$, then $g_{i+1} = 0$

2) if $g_i \neq 0$, then there are $a_i \in K^*$, $l_i, r_i \in S$, $f_i \in F$, s.t.:

i) $g_{i+1} = g_i - a_i\, l_i\, f_i\, r_i$

ii) $M_T(g_i) = l_i\, M_T(f_i)\, r_i$

iii) if $g_{i+1} \neq 0$, then $M_T(g_i) > M_T(g_{i+1})$.

Remark that this is a d-representation except that $g_i \notin K[S]$.

So as in the proof of Prop.5.2, defining $p_n := g_1 - g_{n+1} = \Sigma_{i=1,n}\, a_i l_i f_i r_i$, (p_n) is a Cauchy sequence of elements of $K[S]$ converging to f, s.t. each p_i has a finite d-representation in terms of F.

6.TRUNCATED STANDARD BASES

6.1 The interpretation of d-set provided by Th.5.3 shows that the following definition is a natural one, which extends in a sense the concept of truncated power series. An analogous concept has been recently introduced for the ring of convergent power series in [KFS].

6.2 DEFINITION If $m \in S$, we say F is a <u>m-truncated d-set</u> for an ideal I iff every $f \in I^\wedge$ has a mod. m d-representation in terms of F.

6.3 If < is a negative term ordering, a d-set will be called (as in the commutative case) a <u>standard basis</u>. In this case,every ideal I has a finite m-truncated standard basis for all $m \in S$.

It is obvious that,making use of Lemma 1.8, just minor modifications to Buchberger's algorithm provide an algorithm which,given a finite basis F of a finitely generated ideal I and $m \in S$, computes a finite m-truncated standard basis of I.

7.STANDARD BASES IN COMMUTATIVE POLYNOMIAL RINGS

7.1 Let **X** be a (either finite or enumerable) set of variables $\{X_1,\dots,X_n,\dots\}$, and let $K[\mathbf{X}]$ be the (commutative) polynomial ring in these variables.

The main definitions we have given throughout the paper are generalizations of the analogous definitions for the commutative polynomial ring.

In particular we can define a term ordering < on the commutative free semigroup T generated by **X** (whose elements, as usual, we will call <u>terms</u>) as a total ordering s.t.:

i) for all $m, m_1, m_2 \in T$, $m_1 < m_2$ implies $m\, m_1 < m\, m_2$.

ii) for every $m \in T$, there exists no infinite decreasing sequence $m_1 > \dots > m_i > \dots$ s.t. for all i, $m_i > m$.

(remark that this definition doesn't agree either with Buchberger's

[BUC1,2],which considers only positive term orderings, nor with Lazard's [LA2], which doesn't require condition ii)).

We can then define lc(f) and $M_T(f)$ for a polynomial f; $M_T(F)$ for a set F of polynomials, so that $M_T(I)$ is a semigroup ideal, if I is an ideal; $U(m)$ for every term m; $U := \{\, U(m) : m \in T \,\}$; $C(I)$ for every ideal I.

We can introduce also (with just the minor changes required by commutativity) the concepts of d-set, d-representation, finite d-representation, mod. m d-representation.

If we introduce also the concept of T-filtered ring, clearly $K[\mathbf{X}]$ is a T-filtered ring and its completion is $K[[\mathbf{X},<]]$, whose definition is the commutative analogon of the one given in 4.6.

Remark however that $K[[\mathbf{X},<]]$ is just a subring of the formal power series ring $K[[\mathbf{X}]]$, and coincides with it iff < is negative; otherwise, e.g., if $m > 1$ then $\Sigma_{i=1,\infty}\, m^i$ is in $K[[\mathbf{X}]]$ but not in $K[[\mathbf{X},<]]$.

We then have the following analogon of Theorem 1.5, Proposition 3.5 and Theorem 5.3:

7.2 THEOREM The following conditions are equivalent:

1) F is a d-set for I

2) every f in I has a d-representation in terms of F

3) for all f in I, for all term m, f has a mod. m d-representation in terms of F.

4) $f \in C(I)$ iff f has a d-representation in terms of F

5) $M_T(F)$ generates $M_T(I^\wedge)$

6) $f \in I^\wedge$ iff there is a Cauchy sequence (p_i) of elements of $K[\mathbf{X}]$ converging to f, s.t. each p_i has a finite d-representation in terms of F.

7.3 The following result, however, depends on commutativity; a non commutative counter-example is obtained taking S generated by {a,b}, $F := \{b - a\,b\,a\}$, $I := (F) \subset K[S]$, $g := b$.

7.4 THEOREM If $M_T(I)$ is finitely generated,(so in particular if $K[\mathbf{X}]$ is noetherian, i.e. **X** is finite) then the following conditions are equivalent:

1) F is a d-set for I

7) $g \in I^\wedge$ iff $g = \Sigma_{i=1,t}\, h_i f_i$, $h_i \in K[[\mathbf{X},<]]$, $f_i \in F$, and $M_T(g) \geq M_T(h_i)\, M_T(f_i)$ for all i.

<u>Proof</u>: 5)⇒7) Since $M_T(I)$ is finitely generated, w.l.o.g. we can assume F is finite.

As in the proof of 5)⇒6) (see 5.3), we can obtain an infinite sequence $g = g_0, \dots, g_n, \dots$ of elements of $I^\wedge$ s.t., for all i:

1) if $g_i = 0$, then $g_{i+1} = 0$

2) if $g_i \neq 0$, then there are $a_i \in K^*$, $m_i \in T$, $f_i \in F$, s.t.:

i) $g_{i+1} = g_i - a_i m_i f_i$

ii) $M_T(g_i) = m_i M_T(f_i)$

iii) if $g_{i+1} \neq 0$, then $M_T(g_i) > M_T(g_{i+1})$

If there is n s.t. $g_n = 0$, then there is nothing to prove.

So, assume $g_n \neq 0$ for all n. For every $f \in F$ define $p_0(f) := 0$; define then, for all $n \geq 1$, $p_n(f) := p_{n-1}(f)$ if $f_n \neq f$, $p_n(f) := p_{n-1}(f) + a_n m_n$ if $f_n = f$.

Clearly, for every f, ($p_n(f)$) is a Cauchy sequence; let p(f) be its limit; then $M_T(p(f))\, M_T(f) \leq m_i M_T(f_i) = M_T(g)$. Also, $g = \Sigma_{f \in F}\, p(f)\, f$, so the thesis.

7)⇒5) is obvious.

7.4 Also in the commutative case, if $M_T(I)$ is not finitely generated, we cannot improve the concept of d-representation as shown by the following example:

let X be infinite; let $I \subset K[X]$ be the ideal generated by $F := \{f_i : i \geq 1\}$, where $f_i := X_i - X_{i+1}$. Let $\omega : T \to \mathbb{N}$ be the unique semigroup morphism s.t. $\omega(X_i) = i$ and let < be a term ordering s.t. for every $m', m'' \in T$, $\omega(m') < \omega(m'')$ implies $m' > m''$, so < is negative and F is a standard basis of I.

Then $X_1 \in I^\wedge$ and X_1 is the limit of the Cauchy sequence (p_n) where for all n, $p_n := X_1 - X_{n+1} = \Sigma_{i=1,n} f_i$. It is easy to see that this gives the only d-representation of X_1 in terms of F, so F <u>is not a basis of</u> $I^\wedge$ <u>in</u> $K[[X,<]]$.

To show that a standard basis F of I may not be a basis of I in K[X], also with noetherianity assumptions, the following well-known example can be provided:

Let $X := \{X\}$, $I := (X)$, $f := X - X^2$, $F := \{f\}$, < the unique negative term ordering on T, then F is a standard basis of I, but, clearly $X \notin (F)$ and the only representation of X in terms of F satisfying the conditions of Th.7.4.7) is: $X = (\Sigma_{i=0,\infty} X^i)\, f$.

REFERENCES

[BUC1] B.BUCHBERGER Ein Algorithmus zum Auffinden der Basiselemente des Restklessenringes nach einem nulldimensionalen Polynomideal, Ph.D. Thesis, Innsbruck (1965)

[BUC2] B.BUCHBERGER A criterion for detecting unnecessary reductions in the constructions of Gröbner bases. Proc. EUROSAM 79, L. N. Comp. Sci. 72 (1979), 3-21

[BUC3] B.BUCHBERGER Gröbner bases: an algorithmic method in polynomial ideal theory, in N.K.BOSE Recent trends in multidimensional systems theory, Reidel (1985)

[GAL] A.GALLIGO A propos du theoreme de preparation de Weierstrass, L. N. Math. 409 (1974), 543-579

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

[KFS] H.KOBAYASHI, A.FURUKAWA, T.SASAKI Gröbner basis of ideal of convergent power series (1985)

[KRK] A.KANDRI-RODY, D.KAPUR An algorithm for computing the Gröbner basis of a polynomial ideal over a euclidean ring (1984)

[LAZ] D.LAZARD Gröbner bases, Gaussian elimination, and resolution of systems of algebraic equations, Proc. EUROCAL 83, L. N. Comp. Sci. 162 (1983), 146-156

[MÖL] H.M.MÖLLER On the computation of Gröbner bases in commutative rings (1985)

[MOR1] F.MORA Gröbner bases for non-commutative polynomial rings, Proc. AAECC3, L. N. Comp. Sci. (to appear) (1986)

[MOR2] F.MORA An algorithm to compute the equations of tangent cones, Proc. EUROCAM 82, L. N. Comp. Sci. 144 (1982), 158-165

[MOR3] F.MORA A constructive characterization of standard bases, Boll. U.M.I., Sez.D, 2 (1983), 41-50

[NVO] C.NASTASESCU, F. VAN OYSTAEYEN Graded Ring Theory, North-Holland (1982)

[PAN] L.PAN On the D-bases of ideals in polynomial rings over a principal ideal domain (1985)

[ROB1] L.ROBBIANO On the theory of graded structures, J. Symb. Comp. 2 (1986)

[ROB2] L.ROBBIANO Term orderings on the polynomial ring Proc. EUROCAL 85, L. N. Comp. Sci. 204 (1985), 513-517

[SCH] S.SCHALLER Algorithmic aspects of polynomial residue class rings, Ph.D. Thesis, Wisconsin Univ. (1979)

[ZAC] G.ZACHARIAS Generalized Gröbner bases in commutative polynomial rings, Bachelor Thesis, M.I.T. (1978)