LA QUESTE DEL SAINT GR_a(AL): A COMPUTATIONAL APPROACH TO LOCAL ALGEBRA

Teo MORA
Dipartimento di Matematica
Università
Via L. Alberti 4
I 16132 Genova ITALIE

Mesire Gauvain esgarde le vaissel, si le prise plus que rien qu'il eust veue, mais il ne puet savoir de quoi il est, kar de fust n'est il pas ne de nule maniere de metal, ne de pierre ne rest il mie de cor ne d'os, et de ceu est il tos esbahis. Apres regarde la pucele, si se merveille plus asses de sa bialté que del vaissel, kar onques mes ne vit il feme qui de bialté s'apareillast a ceste: si muse a li si durement qu'a autre rien ne pense. Et ensi com la damoisele passe par devant le dois, si s'agenoille chescuns devant le saint vaissel et tantost sont les tables replenies de tos les bials mengiers que l'en porroit deviser; et li palés fu raemplis de si bones odors com se totes les espieces terrienes i fuissent espandues.

Quant la damoisele fu une fois alee par devant le dois, si s'en retorne et entre en la chambre dont ele vint. Et mesire Gauvain le convoie des iex tant com il puet et quant il ne la voit mes, si regarde devant lui a la table ou il seoit, mes il ne voit chose qu'il puisse mengier, ains est la table vuide devant lui, et il n'i a nus qui n'ait autresi grant plenté de viande comme s'ele sorsist. Quant il voit ce, si en est si esbahis qu'il ne set qu'il doie dire ne que fere, kar bien set qu'il a mespris en aucune chose, por quoi il n'a eu a mengier ausi come li autres.

Lancelot, LXVI, 13-14, Ed. Micha, Geneve, Droz, 1978

INTRODUCTION

Many properties and invariants of ideals in a polynomial ring can be effectively and efficiently obtained once a Gröbner basis of the ideal has been computed by means of Buchberger Algorithm. This has made feasible a computational algebraic approach to the global study of varieties in the complex affine and projective spaces.

As polynomial ideals provide an algebraic setting for the global study of varieties, the study of local properties of a variety finds an algebraic intepretation in local algebra (i.e. the theory of local rings). In this setting an exact counterpart of the notion of Gröbner bases has been long since defined under the name of standard bases; standard bases however don't share the same good computational properties, since Buchberger's Algorithm often fails to terminate when applied to this situation.

While a general algorithm for standard basis computations is still lacking (for instance in the ring of formal power series, also under suitable notions of computability), there are situations in which a simple variant of Buchberger's Algorithm, the Tangent Cone Algorithm [1], is sufficent for the computation of standard bases. While the Tangent Cone Algorithm properly applies only to the case of the localization of a polynomial ring to the origin, elementary algebraic manipulations allow to apply it at least in the following two situations:

1) the localization at a prime ideal of a coordinate ring

2) the ring of algebraic formal power series

Both cases have important geometrical interpretations:

1) let $I_1 \subset I_2 \subset I_3 \subset k[X_1,\ldots,X_n]$ be prime ideals; let $B := k[X_1,\ldots,X_n]/I_1$, $\mathfrak{p} \subset B$ the image of I_3 and let A be the localisation of B at $\mathfrak{p}$; let I be the prime ideal in A, which is the extension of the image of I_2 (each prime ideal in A is such for a suitable $I_2 \subset k[X_1,\ldots,X_n]$, with $I_1 \subset I_2 \subset I_3$).

The geometrical meaning of this situation can be roughly described as follows: we have three affine varieties $V_3 \subset V_2 \subset V_1$ (V_i being defined by I_i); A describes a neighborhood of V_3 in V_1; I defines the variety V_2 "locally", i.e. in such a neighborhood; by studying I we are attempting a description of the local behaviour of V_2.

2) The study of algebraic formal power series is related instead with the study of analytically irreducible branches at the origin of an algebraic variety and comes out naturally when studying singular points of algebraic varieties: for instance in Newton-Puiseux algorithm [***] for determining the analytic branches of a curve at a singular point and, more generally, in the study of analytic components of a complex algebraic variety.

The Tangent Cone Algorithm can therefore be used as a computational tool for local algebra, at least in the two cases discussed above. The aim of this paper is to give a survey of such an approach.

We start with a discussion of the local description of a variety at a point (§1), thus producing a first example of computational problems to which the Tangent Cone Algorithm can be successfully applied.

In Section 2 we will recall the basic notions and the basic results realted with the Tangent Cone Algorithm. Then (§3) we will show how it can be used to effectively solve the problems posed in § 1.

§4 will describe a computational model for rings of algebraic formal power series based on the Implicit Function Theorem and on the Tangent Cone Algorithm, which has been recently introduced and which allows to give effective versions of classical theorems from Weierstrass Preparation Theorem to Noether Normalization Lemma and which gives an algorithm for computing elimination ideals in a ring of algebraic power series

Then we will enter local algebra proper: after a recall of the basic notions from local algebra we will need (§5), we will give a computational model for localizations of cooordinate rings at prime ideals, based on the Tangent Cone Algorithm, which gives an effective description of the topological notions involved and allows for standard basis computations (§6).

In particular the associated graded ring is explicitly presented as a polynomial ring modulo a homogeneous ideal given by a Gröbner basis. Because of this, algorithms relying on Gröbner bases can be applied and the classical "method of associated graded rings" is turned into a computational tool (§7).

Finall we briefly discuss the applications of the Tangent Cone Algorithm to the theory of isolated singularities, proposed by Luengo, Pfister and Schönemann (§8).

None of the results presented in the paper is original [2], but we hope to have improved their presentation with respect to the original research contributions and to provide an updated survey of the applications of standard basis techniques in computational local algebra.

1 AN INTRODUCTORY PROBLEM

Let P denote the polynomial ring $k[X_1,\ldots,X_n]$ with coefficients in a field k.

If $f \in P - \{0\}$, it can be uniquely written as a finite sum of non-zero homogeneous polynomials:

$$f = \Sigma_{i=1\ldots t} f_i \text{ , } f_i \text{ homogeneous and non-zero, } \deg(f_1) < \ldots < \deg(f_i) < \deg(f_{i+1}) < \ldots$$

To the polynomial f we can associate its *order*, $\mathrm{ord}(f) := \deg(f_1)$ and its *initial form*, $\mathrm{in}(f) := f_1$.

The order of f is the infinitesimal order at the origin of f as an analytic function; its initial form is the lowest order non-zero Taylor approximation of f at the origin.

If $I \subset P = k[X_1,\ldots,X_n]$ is an ideal, we define $in(I) := (in(f) : f \in P)$, the *initial form ideal* of I, to be the homogeneous ideal in P generated by the initial forms of the elements in I. Geometrically, (when the base field k is C) it is the ideal which defines the cone of the tangents at the origin (counted with the correct multiplicity) to the variety in C^n defined by I [3]: we are clearly assuming that the origin is in V, i.e. $I \subset (X_1,\ldots,X_n)$; otherwise in(I) is the polynomial ring and the cone of tangents is void (as it should be).

It gives therefore a kind of "lowest order approximation" to such variety.

Let V be the variety in C^n defined by the radical ideal I. Let $f \in P$; if $g \in P$ is s.t. $f - g \in I$, then f and g define the same polynomial function $f(x_1,\ldots,x_n) = g(x_1,\ldots,x_n)$ on V. What are the infinitesimal order at the origin and a lowest order non-zero Taylor approximation at the origin of the polynomial function $f(x_1,\ldots,x_n)$?

LEMMA 1 Consider the set $R_f := \{g \in P : g - f \in I\}$. Assume there is $g \in R_f$ s.t. $in(g) \notin in(I)$ and let $n := ord(g)$.

Then the following hold:

i) if $h \in R_f$, $ord(h) < n$, then $in(h) \in in(I)$.

ii) if $h \in R_f$, $ord(h) \geq n$, then $ord(h) = n$, $in(g) - in(h) \in in(I)$.

Proof: i) since $ord(h) < ord(g)$, $in(h - g) = in(h)$; since $h - g \in I$, $in(h) = in(h - g) \in in(I)$.

ii) If $ord(h) > n$, then $in(h - g) = in(g) \notin in(I)$; since $h - g \in I$, $in(g) = in(h - g) \in in(I)$, a contradiction.

Then if $ord(h) \geq n$, necessarily $ord(h) = n$, $in(h - g) = in(h) - in(g)$; then, since $h - g \in I$, $in(h) - in(g) = in(h - g) \in in(I)$.

It is then clear that the answer to the questions above is: ord(g) and the residue class of in(g) mod. in(I).

However there are cases in which a g as required by the Lemma doesn't exist.

In fact consider $P := C[X,Y]$, $f = X$, I the ideal generated by $X - X^2$, V the variety defined by I, which is the union of the two lines $x = 0$, $x = 1$.

The polynomial function $f(x,y) = x$ vanishes identically in any point of V which is sufficiently near to the origin, so it actually coincides locally with the polynomial function $g(x,y) = 0$.

This is reflected by the fact that in the set R_f there is no g s.t. $in(g) \notin in(I) = (X)$: in fact if $g - f \in I$, then $g - X = h\,(X - X^2)$ for some polynomial h, so $g = X + h\,(X - X^2) = X\,(1 + h\,(1 - X))$ and in(g) is a multiple of X. However $X \notin I$.

Remark however that the vanishing of the polynomial function x is reflected by the fact that $X = (1 - X)^{-1}\,(X - X^2)$ so X belongs to the ideal generated by $X - X^2$ in any ring containing the inverse of $(1 - X)$; introducing the inverse of $(1 - X)$ makes sense, since "near the origin" $1 - X$ never vanishes so it is an invertible function.

In fact we can actually find a natural solution to our problem by considering the "local" nature of both our problem (infinitesimal orders, lowest order approximations at a point) and of our data (functions defined

near a point) and so by carrying on the machinery we have developed to the larger ring of the rational functions which are defined in 0,

$Loc(P) := \{(1+g)^{-1} f : f, g \in P, g(0) = 0\} \subset k(X_1,\ldots,X_n)$

where we define, for $h = (1+g)^{-1} f$, and for an ideal $I \subset Loc(P)$:

$in(h) := in(f)$, $ord(h) := ord(f)$, $in(I) := (in(h) : h \in I) \subset P$

preserving the geometrical meaning of these notions.

As we will establish later, the following holds:

FACT If $I \subset Loc(P)$ is an ideal and $h \in Loc(P)$, then there is $h_0 \in Loc(P)$ s.t.

i) either $h_0 = 0$ or $in(h_0) \notin in(I)$

ii) $h - h_0 \in I$

As a consequence we have:

PROPOSITION 1 Let $I \subset Loc(P)$ be an ideal. Let $F \subset I$ be s.t. $in(F) = in(I)$. Let $h \in Loc(P)$. Let $h_0 \in Loc(P)$ be s.t. $h - h_0 \in I$ and either $h_0 = 0$ or $in(h_0) \notin in(I)$ (whose existence is guaranteed by the above Fact)

Then:

i) $h \in I$ if and only if $h_0 = 0$

ii) if $h_0 \neq 0$, $g - h \in I$ and $ord(g) < ord(h_0)$, then $in(g) \in in(I)$.

iii) if $h_0 \neq 0$, $g - h \in I$ and $ord(g) \geq ord(h_0)$, then $ord(g) = ord(h_0)$, $in(g) - in(h_0) \in in(I)$.

Proof: i) If $h_0 = 0$, then $h = h - h_0 \in I$. If $h_0 \neq 0$, then $h_0 \notin I$, otherwise $in(h_0) \in in(I)$; so $h - h_0 \in I$ implies $h \notin I$.

ii) and iii): The proof is the same as for Lemma 1.

As a consequence, the infinitesimal order at the origin of the rational function $h(x_1,\ldots,x_n)$ is $ord(h_0)$, its lowest order Taylor approximation at the origin is the residue class of $in(h_0)$ in $P/in(I)$.

To go back to the example we are discussing, in Loc(P) we have $X = (1 - X)^{-1} (X - X^2) \in (X - X^2)$, so $h_0 = 0$, reflecting the fact that x vanishes identically in any point of V which is sufficiently near to the origin.

In the same way we could have considered $P^{\wedge} := k[[X_1,\ldots,X_n]]$. It is clear that all the notions and the considerations we have carried out for P and Loc(P) could have been developped for formal power series too.

In fact any $f \in P^{\wedge} - \{0\}$, it can be uniquely written as a (perhaps infinite) sum of non-zero homogeneous polynomials:

$f = \Sigma_{i=1\ldots t} f_i$, f_i homogeneous and non-zero, $deg(f_1) < \ldots < deg(f_i) < deg(f_{i+1}) < \ldots$

and so we can associate to it its *order*, $ord(f) := deg(f_1)$ and its *initial form*, $in(f) := f_1$; also to an ideal $I \subset P^{\wedge}$, we can associate the homogeneous ideal $in(I) := (in(f) : f \in I) \subset P$; all these concepts have the same analytical meaning as in the polynomial case [4].

So now we are considering an ideal $I = (g_1,\ldots,g_r) \subset P^\wedge$, s.t. $I \subset (X_1,\ldots,X_n)$, some neighbourhood U of the origin where the analytic functions $g_1(x_1,\ldots,x_n),\ldots,g_r(x_1,\ldots,x_n)$ are defined and the set $V := \{(x_1,\ldots,x_n) \in U : g_i(x_1,\ldots,x_n) = 0\}$. Then we consider $f \in P^\wedge$, some neighbourhood W of the origin s.t. the analytical function $f(x_1,\ldots,x_n)$ is defined in W and we would like to speak of the infinitesimal order at the origin and a lowest order non-zero Taylor approximation at the origin of the analytical function $f(x_1,\ldots,x_n)$ on $V \cap W$

By extending Prop. 2 to ideals in $P^\wedge$ (having earlier extended also the corresponding Fact), we obtained that there is $h_0 \in P^\wedge$ s.t. $h - h_0 \in I$, and either $h_0 = 0$ or $in(h_0) \notin in(I)$. Then the infinitesimal order at the origin of the analytical function $f(x_1,\ldots,x_n)$ on $V \cap W$ is $ord(h_0)$ and a lowest order non-zero Taylor approximation is the residue class of $in(h_0)$ mod. in(I).

2 RECALLS: THE TANGENT CONE ALGORITHM [5]

The discussion above should have made clear the interest of being able to explicitly compute a set $F \subset I \subset Loc(P)$ (or $P^\wedge$) s.t. $in(F) = in(I)$ and for each $h \in Loc(P)$ (resp. $P^\wedge$) an element h_0 s.t. $h - h_0 \in I$ and either $h_0 = 0$ or $in(h_0) \notin in(I)$.

We remark immediately that the existence of such an algorithm in $P^\wedge$ is at present an open problem [6], but there is a solution, based on the tangent cone algorithm, both for Loc(P) and for rings of algebraic formal power series [AMR1, AMR2].

We are going therefore to introduce the tangent cone algorithm, which will be our main tool for such computations.

Let $P := k[X_1,\ldots,X_n]$ be a polynomial ring over a field, let $T = \langle X_1,\ldots,X_n\rangle$ denote the free commutative semigroup generated by $\{X_1,\ldots,X_n\}$, let $<$ be a semigroup total ordering on T.

Then each polynomial $f \in P - \{0\}$ can be written in a unique way as:

$$f = \Sigma_{i=1\ldots t}\, c_i\, m_i,\ c_i \in k^*,\ m_i \in T,\ m_1 > m_2 > \ldots > m_t.$$

Denote : $T(f) := m_1$, $M(f) := c_1\, m_1$.

T(f) is the maximal term, M(f) the maximal monomial of f.

When we need to specify the ordering $<$ on which the definitions above depend, we will use either the notation $T_<$, $M_<$, or $<_\sigma$, T_σ, M_σ.

If $F \subset P$, denote $M\{F\} := \{M(f) : f \in F - \{0\}\}$, M(F) the ideal generated by M{F}. Therefore if I is an ideal, M(I) is the monomial ideal generated by the maximal monomials of the elements in I.

We say $f \in P-\{0\}$ has a *Gröbner representation* in terms of $F \subset P - \{0\}$ if and only if it can be represented:

$$f = \Sigma\, g_i\, f_i,\ g_i \in P - \{0\},\ f_i \in F,\ T(g_i)\, T(f_i) \leq T(f) \text{ for every } i$$

(such a representation will be called a Gröbner representation).

Given $f \in P - \{0\}$, $F \subset P - \{0\}$, an element $h \in P$ s.t. $f - h \in (F)$ and either $h = 0$ or $M(h) \notin M(F)$ will be called a *normal form* of f w.r.t. F.

Let $NF(f,F) := \{h \in P : h \text{ is a normal form of } f \text{ w.r.t. } F\}$.

In case $<$ is a well-ordering, the result below is well-known and gives a definition of Gröbner bases; we just recall that an algorithm (Buchberger algorithm) is known to compute Gröbner bases, whose termination is proved using, in an essential way, the fact that $<$ is a well-ordering.

THEOREM 1 If $I \subset P$ is an ideal, and $F \subset I - \{0\}$, the following conditions are equivalent:

1) $M\{F\}$ generates the ideal $M(I)$

2) $f \in I - \{0\}$ if and only if it has a Gröbner representation in terms of F

3) for each $f \in P - \{0\}$:

i) if $f \in I$, then $NF(f,F) = \{0\}$

ii) if $f \notin I$, then $NF(f,F) \neq \emptyset$ and $\forall h \in NF(f,F)$, $h \neq 0$.

DEFINITION 1 A set $F \subset I - \{0\}$ is called a *Gröbner basis* for the ideal I if and only if it satisfies the equivalent conditions of Theorem 1.

We recall here an important property related to Gröbner bases (more exactly to the ideal $M(I)$) which we will use later:

LEMMA 2 Let $B := \{t \in T : t \notin M(I)\}$ and let $k[B]$ denote the k-vector space with basis B.
Then $\forall h \in P$, there is a unique $g \in k[B]$ s.t. $h - g \in I$.
Such a g is called a *canonical form* of the residue class of h mod. I and denoted $Can(h,I)$.
Moreover $Can(h,I) = 0$ if and only if $h \in I$, $Can(h_0,I) = Can(h_1,I)$ if and only if $h_0 - h_1 \in I$.
Also $Can(h,I)$ can be computed if a Gröbner basis of I is known.

For our applications, we must however consider a larger class of orderings, the "tangent cone orderings", which don't cover all possible orderings but a class sufficient for most applications. We don't give here the definition (for which cf. [MPT]) but we limit to explicitly present those tangent cone orderings we will need in the applications discussed in this paper:
if $<$ is an ordering on T, the variables can be divided in two classes and renamed, denoting by

$\{Z_1,\ldots,Z_m\}$ the set of variables s.t. $Z_i > 1$

$\{Y_1,\ldots,Y_d\}$ the set of variables s.t. $Y_j < 1$;

each term $m \in T$ is then the product $m = m_Z\, m_Y$ of a term m_Z in the Z's only and of a term m_Y in the Y's only (one can consider also the case in which $\{Z_1,\ldots,Z_m\}$ is empty [7]).
The restriction $<_Z$ of $<$ to $<Z_1,\ldots,Z_m>$ is a well-ordering; for the restriction $<_Y$ of $<$ to $<Y_1,\ldots,Y_d>$ we require that a semigroup morphism $w: <Y_1,\ldots,Y_d> \rightarrow \mathbf{Z}$ is given s.t.

i) $w(m) < 0$ if $m \neq 1$

ii) $w(m_1) < w(m_2)$ implies $m_1 <_Y m_2$.

Moreover we require that:

$m < m'$ if and only if $m_Y < m'_Y$ or ($m_Y = m'_Y$ and $m_Z < m'_Z$)

From now on $<$ will be a tangent cone ordering.

Denote by Loc(P) the following subring of $k(X_1,\ldots,X_n)$:

$$Loc(P) := \{(1 + g)^{-1} f, \text{ s.t. } T(g) < 1\}.$$

We can define for $h = (1 + g)^{-1} f$ and for an ideal $I \subset Loc(P)$:

$$T(h) := T(f),\ M(h) := M(f),\ M(I) := (M(h) : h \in I) \subset P$$

DEFINITION 2 Given $f \in Loc(P) - \{0\}$, $F \subset Loc(P) - \{0\}$, an element $h \in Loc(P)$ is called a *normal form* of f w.r.t. F if

$$f - h = \Sigma g_i f_i,\ g_i \in Loc(P) - \{0\},\ f_i \in F$$

either $h = 0$ or $M(h) \notin M(F)$.

Nf(f,F) will denote the set $\{h \in Loc(P)$: h is a normal form of f w.r.t. F$\}$

DEFINITION 3 We say $h \in Loc(P)-\{0\}$ has a *standard representation* in terms of $F \subset Loc(P) - \{0\}$ if and only if it can be represented:

$$f = \Sigma g_i f_i,\ g_i \in Loc(P) - \{0\},\ f_i \in F,\ T(g_i)\,T(f_i) \leq T(f) \text{ for every } i$$

(such a representation will be called a standard representation).

DEFINITION 4 A set $F \subset I - \{0\}$ is called a *standard basis* for the ideal $I \subset Loc(P)$ if and only if $M\{F\}$ generates the ideal M(I).

THEOREM 2 The following conditions are equivalent:

1) F is a standard basis of I

2) $f \in I$ if and only if f has a standard representation in terms of F

3) for each $f \in Loc(P) - \{0\}$:

i) if $f \in I$, then $NF(f,F) = \{0\}$

ii) if $f \notin I$, then $NF(f,F) \neq \emptyset$ and $\forall h \in NF(f,F),\ h \neq 0$.

PROPOSITION 2 Let F be a standard basis for the ideal $I \subset Loc(P)$, then:

1) let $h \in NF(g,F)$; then:

if $h = 0$, then $g \in I$

if $h \neq 0$, $g \notin I$

2) if $h \in NF(g,F)$, $h \neq 0$, then $T(h) = \min\{T(g') : g' - g \in I\}$

3) if $g, g' \in Loc(P) - I$ are s.t. $g - g' \in I$, then $M(h) = M(h')$ for each $h \in NF(g,F)$ and $h' \in NF(g',F)$.

A variant of Buchberger algorithm, the Tangent Cone Algorithm [8], allows to compute standard sets of ideals. More precisely:

THEOREM 3 Given $g, f_1,\ldots,f_r \in Loc(P)$, there is an algorithm (the **Tangent Cone Algorithm**) which computes polynomials u, h such that

u is a unit in Loc(P)

$u^{-1}h$ is a normal form of g in terms of $\{f_1,...,f_r\}$

As a consequence, it is possible, given $g, f_1,...,f_r \in Loc(P)$:

1) to compute polynomials $g_1,...,g_s$ such that $\{g_1,...,g_s\}$ is a standard basis for $(f_1,...,f_r)$.

2) to decide whether $g \in (f_1,...,f_r)$.

The notion of standard bases can be extended to submodules of $Loc(P)^t$ in two different ways [9], where $<$ is a fixed ordering on T for which it is possible to apply the tangent cone algorithm.

First of all, for any arbitrary choice of t terms $m_1,...,m_t \in T$, we can define for each $\phi := (f_1,..., f_t) \in Loc(P)^t$:

$T(\phi) := \max\{T(f_i) + m_i\}$

$M(\phi) := (p_1,..., p_t) \in P^t$, where $p_i := M(f_i)$ if $T(f_i) + m_i = T(\phi)$, $p_i := 0$ otherwise.

If $\Phi \subset Loc(P)^t$, let us denote $M\{\Phi\} := \{M(\phi) : \phi \in \Phi - \{0\}\} \subset P^t$, $M(\Phi)$ the submodule of P^t generated by $M\{\Phi\}$.

If U is a submodule of $Loc(P)^t$, we say $\Phi \subset U$ is a *T-standard basis* for U if $M(\Phi) = M(U)$.

This notion ([G-Z]) is more suitable from an algebraic point of view but not from a computational one, however a suitable generalization of the tangent cone algorithm allows to compute T-standard bases.

We can also consider ([P-S], [G-Z]) the set of terms T_t of P^t to be the set of elements $(p_1,...,p_t) \in P^t$ s.t. there is j with $p_j \in T$, $p_i = 0$ if $i \neq j$ and impose an ordering $<_t$ on T_t s.t.

for $t, t' \in T, \phi, \phi' \in T_t$, $t \leq t'$ and $\phi \leq_t \phi'$ implies $t\,\phi \leq t'\,\phi'$.

Then each $\phi \in P^t - \{0\}$ can be written in a unique way as:

$\phi = \Sigma_{i=1...s}\, c_i\, \phi_i$, $c_i \in k^*$, $\phi_i \in T_t$, $\phi_1 > \phi_2 > ... > \phi_s$.

Denote : $Hterm(\phi) := \phi_1$, $Hmon(\phi) := c_1\, \phi_1$.

The two functions can be obviously extended to $Loc(P)^t$.

If $\Phi \subset Loc(P)^t$, denote $Hmon\{\Phi\} := \{Hmon(\phi) : \phi \in \Phi - \{0\}\}$, $Hmon(\Phi)$ the ideal generated by $Hmon\{\Phi\}$.

If U is a submodule of $Loc(P)^t$, we say Φ is a *standard basis* for U if $Hmon(\Phi) = Hmon(U)$.

A generalization of the Tangent Cone Algorithm allows to compute standard sets of submodules of $Loc(P)^t$ at least in the following two cases [10]:

1) $t_1\, e_i <_t t_2\, e_j$ if and only if $i < j$ or $(i = j$ and $t_1 < t_2)$ [P-S]

2) For given $m_1,..., m_t \in T$, $t_1\, e_i <_t t_2\, e_j$ if and only if $t_1\, m_i < t_2\, m_j$ or $(t_1\, m_i = t_2\, m_j$ and $i < j)$ [G-Z].

We will refer only to the second case, in which case we will say that $<_t$ is compatible with $<$ and $m_1,...,m_t$.

We remark that in this case a standard basis is a T-standard basis too.

Let us now restrict to an ordering s.t. for each i $X_i < 1$.

Each $f \in P^{\wedge} - \{0\}$ can be uniquely written as an ordered (possibly infinite) sum of monomials:

$f = \Sigma\, m_i$, $c_i \in k\text{-}\{0\}$, $m_i \in T$, $m_1 > m_2 > ... > m_i > m_{i+1} > ...$

We can extend our definitions, denoting:

$T(f) := m_1$, $M(f) := c_1\, m_1$

and remarking that the definitions agree with the one previously given for elements in $Loc(P) \subset P^{\wedge}$: in fact $(1 + g)^{-1} f$ has the power series expansion $\Sigma_{i \geq 0} g^i f$ and it is easy to verify that $M((1 + g)^{-1} f) = M(f) = M(\Sigma g^i f)$.

Also if $F \subset P^{\wedge}$, we denote $M\{F\} := \{M(f) : f \in F - \{0\}\}$, M(F) the ideal generated by $M\{F\}$.

Then the generalizations of defs. 2-4, Th. 2 and Prop.2 hold for $P^{\wedge}$ too.

However no algorithm is presently known to actually compute a standard basis of a given ideal I, also under suitable computational restrictions, unless I is 0-dimensional [FKS,MPT].

3 AN INTRODUCTORY SOLUTION

We started the previous section with the remark that it was interesting to explicitly compute a set $F \subset I \subset Loc(P)$ s.t. in(F) = in(I) and for each $h \in Loc(P)$ an element h_0 s.t. $h - h_0 \in I$ and either $h_0 = 0$ or $in(h_0) \notin in(I)$. Here is a solution:

Let $<$ be a semigroup ordering on T s.t.

for $m_1, m_2 \in T$, $deg(m_1) < deg(m_2) \Rightarrow m_1 > m_2$.

This is equivalent to say that the function $w: T \rightarrow Z$ defined by $w(m) = -deg(m)$ is s.t.

$w(m_1) < w(m_2) \Rightarrow m_1 < m_2$

so $<$ is in the class of orderings we are considering.

We will consider also the well-ordering $<_w$ on T which agrees with $<$ on terms of the same degree, but is compatible (instead of anticompatible) with the degree, i.e.

$m_1 <_w m_2$ if and only if $deg(m_1) < deg(m_2)$ or $(deg(m_1) = deg(m_2)$ and $m_1 < m_2)$

Finally remark that the definition of Loc(P) we gave (w.r.t. $<$ in §2) and the one we gave in §1 agree, since w.r.t. $<$, $T(g) < 1$ if and only if $g \in (X_1,\ldots,X_n)$ if and only if $g(0) = 0$.

PROPOSITION 3 Let $I \subset Loc(P)$ be an ideal. Let $F \subset I$ be a standard basis of I.

Let $h \in Loc(P)$ and let $h_0 \in Loc(P)$ be a normal form of h.

Then:

i) $\{in(f) : f \in F\}$ generates in(I).

ii) $\{in(f) : f \in F\}$ is a Gröbner basis of in(I) w.r.t. the well-ordering $<_w$.

iii) if $h_0 = 0$, then $h \in I$

iv) if $h_0 \neq 0$, $in(h_0) \notin in(I)$

v) if $h_0 \neq 0$, $g - h \in I$ and $ord(g) < ord(h_0)$, then $in(g) \in in(I)$.

vi) if $h_0 \neq 0$, $g - h \in I$ and $ord(g) \geq ord(h_0)$, then $ord(g) = ord(h_0)$, $in(g) - in(h_0) \in in(I)$.

vii) $Can(h_0,in(I))$ is a canonical form

Proof: i) and ii): Since $\forall h \in Loc(P)$, $M(h) = M(in(h))$, we can easily conclude that both $M(I) = M(in(I))$ and $M(F) = M(in(F))$, so that $M(in(F)) = M(in(I))$.

Also, if f is a homogeneous element of P, $M(f) = M_w(f)$. Therefore $M_w(in(F)) = M(in(F)) = M(in(I)) = M_w(in(I))$.

So $\{in(f) : f \in F\}$ is a Gröbner basis, and therefore a basis, of I.

iii) It is obvious

iv) If $in(h_0) \in in(I)$, then $M(h_0) = M(in(h_0)) \in M(in(I)) = M(I)$

v) and vi): The proof is the same as for Lemma 1.

This solves completely the problem we posed, since we are able to compute standard bases and normal forms in Loc(P) by means of the Tangent Cone Algorithm.
We just make the further remark that the residue class of h_0 mod. in(I) (i.e. the least non-zero approximation of $f(x_1,\ldots,x_n)$) can be represented by $Can(h_0, in(I)) \subset k[\mathbf{B}]$.

We are going now to show that it is possible to do the same, and more, also in the ring of algebraic formal power series.

4 COMPUTING WITH ALGEBRAIC SERIES

In two joint recent papers ([AMR1], [AMR2]) with M.E. Alonso and M. Raimondo, a computational model for algebraic formal power series has been proposed which relies on a symbolic codification of the series by means of the Implicit Function Theorem, introduced in [ALR] and on the Tangent Cone Algorithm. What follows is a short summary of the main results which can be obtained.
We will use the following notation: for a ring B s.t. $k[Z_1,\ldots,Z_r] \subset B \subset k[[Z_1,\ldots,Z_r]]$, denote $B_{loc} := \{f\, g^{-1} : f, g \in B, g \text{ invertible in } k[[Z_1,\ldots,Z_r]]\}$, and remark that for $B = k[Z_1,\ldots,Z_r]$, and for each ordering $<$ s.t. $m \leq 1\ \forall m$, $B_{loc} = Loc(B)$. We will also use "$\underline{Z}$" as a shorthand for "$Z_1,\ldots,Z_r$"

Let k be a computable field; $k[[X_1,\ldots,X_n]]_{alg}$ denotes the ring of algebraic formal power series (i.e. the ring of algebraic functions vanishing and developpable in Taylor series at the origin).
Let us fix an ordering $<$ on the semigroup $T = \langle X_1,\ldots,X_n\rangle$ s.t.

for $m_1, m_2 \in T$, $\deg(m_1) < \deg(m_2) \Rightarrow m_1 > m_2$. (11)

Let us consider polynomials $F_1,\ldots, F_r \in k[X_1,\ldots,X_n, Y_1,\ldots,Y_r]$ vanishing at the origin and s.t. the Jacobian of the F_i's with respect to the Y_j's at the origin is a lower triangular non singular matrix. Under this assumption, by the Implicit Function Theorem, there are unique $f_1,\ldots, f_r \in k[[X_1,\ldots,X_n]]_{alg}$ s.t. $f_j(0) = 0\ \forall j$, and $F_i(\underline{X},f_1,\ldots,f_r) = 0\ \forall i$.

DEFINITION 5 $(F_1,\ldots, F_r)$ is called a locally smooth system (LSS) defining $f_1,\ldots, f_r \in k[[X_1,\ldots,X_n]]_{alg}$ if:

the Jacobian of the F_i's with respect to the Y_j's at the origin is a lower triangular non singular matrix.

$f_1,\ldots, f_r$ are the unique solutions of $F_1 = 0,\ldots, F_r = 0$ which vanish at the origin.

Given the LSS $F := (F_1,\ldots,F_r)$ defining $f_1,\ldots, f_r$, let $P := k[X_1, \ldots, X_n, Y_1, \ldots, Y_r]$, $k[\underline{X},F]_{loc} := k[\underline{X}, f_1,\ldots, f_r]_{loc} \subset k[[\underline{X}]]_{alg}$. To compute in it, we consider the evaluation map $\sigma_F : Loc(P) \rightarrow k[\underline{X},F]_{loc}$ defined by $\sigma_F(Y_i) = f_i$, for which $Ker(\sigma_F) = (F_1,\ldots,F_r)\, Loc(P)$, so that $k[\underline{X},F]_{loc} \approx Loc(P)/(F_1,\ldots,F_r)$.

If an algebraic series g is given by assigning a polynomial $G(\underline{X},T)$ s.t. $G(\underline{X},g) = 0$ and an algorithm to compute any truncation of g, it is possible to compute a LSS F s.t. $g \in k[\underline{X},F]_{loc}$ (cf. [A-M]).

It is possible to show that, for suitable orderings $<_u$ on P which restricts to $<$ on T, a locally smooth system $(F_1,\ldots,F_r)$ is a standard basis in Loc(P) for the ideal it generates and $M_u(F_1,\ldots,F_r) = (Y_1,\ldots,Y_r)$; therefore, by normal form computations it is possible to modify the LSS defining the f_i's so that it satisfies the following assumptions, for an explicitly obtained ordering $<_\sigma$:

1) $\mathbf{F} = (F_1,\ldots,F_r)$ is a LSS for $f_1,\ldots,f_r$

2) $f_i \neq 0\ \forall i$

3) $F_i = Y_i\ (1+Q_i) - R_i$ with $Q_i, R_i \in (\underline{X},\underline{Y})$, $R_i \in k[\underline{X},Y_1,\ldots,Y_{i-1},Y_{i+1},\ldots,Y_r]$ and $M_\sigma(R_i) = M(f_i)$

4) $\{F_1,\ldots,F_r\}$ is a standard basis for the ideal it generates in Loc(P) w.r.t. $<_\sigma$ and $M_\sigma(F_i) = Y_i$

5) $<_\sigma$ restricts to $<$ on $<\underline{X}>$

Such an F is called a *standard locally smooth system* (SLSS) over $<$.

By applying the tangent cone algorithm w.r.t. $<_\sigma$ in Loc(P), given $G_0,\ldots,G_s \in$ Loc(P) and denoting $g_i := \sigma(G_i)\forall i$, it is then possible:

1) to compute $H \in$ Loc(P) which is a normal form of G_0 w.r.t. $\{F_1,\ldots,F_r\}$; such an H is s.t. $H = 0$ if and only if $g_0 = 0$ and, if $H \neq 0$ then $\sigma(H) = g_0$, $M_\sigma(H) \in k[\underline{X}]$, $M_\sigma(H) = M(g_0)$; H is called a *representation* of g_0

2) therefore to decide whether $g_0 = 0$, and, if $g_0 \neq 0$, to compute $T(g_0)$, $M(g_0)$ and $in(g_0)$

3) to compute a representation of a normal form of g_0 w.r.t. $\{g_1,\ldots,g_s\}$

4) to compute $H_1,\ldots,H_t$ s.t. H_i is a representation of $h_i := \sigma(H_i)$ and $\{h_1,\ldots,h_t\}$ is a standard basis for $I := (g_1,\ldots,g_s)$ w.r.t. $<$.

5) as a consequence $\{in(h_1),\ldots,in(h_t)\}$ are a Gröbner basis of in(I) w.r.t. $<_w$

6) also, if H_0 is a representation of a normal form h_0 of g_0 w.r.t. $\{h_1,\ldots,h_t\}$, then the residue class of $in(h_0)$ mod. in(I) (which has the analytical meaning discussed in §1) can be explicitly obtained.

By applying the above techniques, one can moreover give computational versions of classical theorems:

THEOREM 4 Given a local smooth system $G := (G_1,\ldots, G_r) \subset k[\underline{X}, Z, \underline{Y}] =: P$ defining $f_1,\ldots, f_r \in k[[\underline{X}, Z]]_{alg}$ and $G_0 \in$ Loc(P) s.t., denoting $g := \sigma_G(G_0)$, $g(0,\ldots,0, Z) \neq 0$, then:

(Weierstrass Preparation Th.)

it is possible to compute:

1) an ordering $<$ on $<\underline{X}, Z>$ s.t. $T(g) = Z^d$, whiose restriction to $<\underline{X}>$ we denote $<'$

2) a SLSS $F := (F_1,\ldots, F_r)$ over $<$ defining $f_1,\ldots, f_r$ s.t. $k[\underline{X}, Z, F]_{loc} = k[\underline{X}, Z, G]_{loc}$ and a representation $G \in$ Loc(P) of g

3) a SLSS $H \subset K[\underline{X}, \underline{Y}, U_0,\ldots,U_{d-1},U_{10},\ldots,U_{1d-1},\ldots,U_{r0},\ldots,U_{rd-1}] =: Q$ over $<'$, defining h_j, $h_{ij} \in K[[\underline{X}]]_{alg}$, $i=1\ldots r$, $j = 0\ldots d-1$

4) $V, V_i \in Loc(Q)$, V a unit s.t.

a) $W := (H,F)$ is a SLSS over <

b) $Wei(g) := g\ \sigma_W(V) = \Sigma_{j=0...d-1}\ h_j Z^j = \Sigma_{j=0...d-1}\ \sigma_H(U_j) Z^j \in K[\underline{X},H]_{loc}[X_n]$

c) $f_i = \sigma_W(V_i)\ g + \Sigma_{j=0...d-1}\ h_{ij} Z^j$.

(Weierstrass Division Th.)

If moreover $B \in P$ [12] is given such that $\sigma_G(B) =: b \neq 0$, then it is possible to compute $A \in Loc(Q)$, and polynomials $A_j \in k[\underline{X}, \underline{U}]$, $j = 0...d-1$, s.t.

1) $b = Wei(g) + \Sigma_{j=0...d-1}\ \sigma_H(A_j) Z^j$

2) $\Sigma_{j=0...d-1}\ \sigma_H(A_j) Z^j$ is the canonical form of b w.r.t. (g) in $k[[\underline{X},Z]]$ [13]

3) $\sigma_W(A)$, $\sigma_H(A_j)$ are unique

THEOREM 5 Given a local smooth system $G := (G_1,..., G_r) \subset k[\underline{X}, \underline{Y}] =: P$ defining $f_1,..., f_r \in k[[\underline{X}, Z]]_{alg}$ and $H_1,...,H_s \in Loc(P)$ and denoting $h_i := \sigma_G(H_i)$, $I = (h_1,...,h_s) \subset k[[\underline{X}]]_{alg}$,

then:

(Noether Normalization Lemma)

it is possible to compute:

1) a linear change of coordinates $C: k[[\underline{X}]]_{alg} \rightarrow k[[\underline{X}]]_{alg}$

2) $d = \dim(I)$

3) a SLSS H defining algebraic series in $k[[X_1,...,X_d]]_{alg}$

4) $B_1,...,B_{n-d}, A_1,..., A_t \in k[X_1,...,X_d,H]_{loc}[X_{d+1},...,X_n]$

s.t. denoting, with a slight abuse of notation σ_H: $k[X_1,...,X_d,H]_{loc}[X_{d+1},...,X_n] \rightarrow k[[\underline{X}]]_{alg}$ the extension of the evaluation morphism σ_H, $b_i := \sigma_H(B_i)$, $a_j := \sigma_H(A_j)$, one has:

a) $C(I) \cap k[[X_1,...,X_d]]_{alg} = (0)$

b) $\forall i\ B_i \in k[X_1,...,X_d,H]_{loc}[X_{d+1},...,X_{d+i-1}][X_{d+i}]$ is a monic polynomial in X_{d+i} whose coefficients (in $k[X_1,...,X_d,H]_{loc}[X_{d+1},...,X_{d+i-1}]$) belong to $(X_1,...,X_{d+i-1}, Y_1,...,Y_r)$

c) $(b_1,...,b_{n-d}, a_1,..., a_t)\ k[[\underline{X}]]_{alg} = C(I)$

so that:

d) $k[[\underline{X}]]_{alg}/C(I)$ is an integral extension of $k[[X_1,...,X_p]]_{alg}$

(Algebraic Series Elimination)

Moreover for each j, it is possible to compute:

1) a linear change of coordinates $C: k[[\underline{X}]]_{alg} \rightarrow k[[\underline{X}]]_{alg}$

2) a SLSS H defining algebraic series in $k[[X_1,...,X_j]]_{alg}$

3) $A_1,..., A_t \in k[X_1,...,X_j,H]_{loc}$

s.t. denoting $J := (A_1,..., A_t)\ k[[X_1,...,X_j]]_{alg}$ one has:

$J = C(I)\ K[[\underline{X}]]_{alg} \cap K[[X_1,...,X_j]]_{alg}$

5 RECALLS: LOCAL ALGEBRA

The analytical notions we have discussed in §1 and §3 can be stated and interpreted in algebro-topological terms; also they can generalized in order to allow a local study of the ring of rational functions defined on

a variety V "near" a subvariety V'. The aim of this section is to briefly review the algebraic bases for the local study of an algebraic variety (14).

Let A be a commutative ring (noetherian and with identity), $L \subset A$ be an ideal s.t. $\cap L^n = (0)$.
For each $a \in A - \{0\}$, there is n s.t. $a \in L^n - L^{n+1}$. We then define $v_L(a) := n$.
The function $v_L : A - \{0\} \to N$, the *order function*, satisfies, $\forall a,b \in A - \{0\}$ (15):

$v(a+b) \geq \min(v(a), v(b))$

$v(a\,b) \geq v(a) + v(b)$

Let us consider the direct sum $Gr_L(A) := \oplus_{n=0\ldots\infty} L^n / L^{n+1}$, which is an abelian group, and a graded one if we consider the elements of L^n / L^{n+1} to be the homogeneous elements of degree n.
$Gr_L(A)$ is turned into a graded ring by the following multiplication:
if $a \in L^n / L^{n+1}$, $b \in L^m / L^{m+1}$, then there are $a_1 \in L^n$, $b_1 \in L^m$ s.t. a (resp. b) is the residue class of a_1 (resp. b_1) mod. L^{n+1} (resp. L^{m+1}). Therefore $a_1 b_1 \in L^{m+n}$. Define $a\,b \in L^{m+n}/L^{m+n+1}$ to be the residue class of $a_1 b_1$ mod. L^{m+n+1}.
It is straightforward to verify that the above definition doesn't depend on the choice of a_1 and b_1 and that, with this definition of multiplication, $Gr_L(A)$ is a (commutative, noetherian, with identity) graded ring.
Let us define, for $a \in A - \{0\}$, $in_L(a) \in gr_L(A)$ to be the residue class of a mod. L^{n+1}, where $n = v_L(a)$; and let us define $in_L(0) := 0$.
The function $in_L : A \to Gr_L(A)$, the *initial form function*, satisfies $\forall a,b \in A - \{0\}$:

$in(a + b) = in(a)$ if $v(a) < v(b)$

$= in(b)$ if $v(a) > v(b)$

$= in(a) + in(b)$ if $v(a) = v(b)$ and $in(a) + in(b) \neq 0$

$v(a + b) > \min(v(a),v(b))$ if and only if $v(a) = v(b)$, $in(a) + in(b) = 0$

$in(a\,b) = in(a)\,in(b)$ unless $in(a)\,in(b) = 0$

$v(a\,b) > v(a) + v(b)$ if and only if $in(a)\,in(b) = 0$

If we choose the set $\{L^n : n \in N\}$ as a basis of neighbourhoods of 0, then we obtain a ring topology on A, the L-*adic topology*, which is Hausdorff (since $\cap L^n = (0)$).
Under this topology the *closure* of an ideal I (the set of elements of A which are limits of Cauchy sequences of elements in I) is $cl(I) := \cap (I + L^n)$, which is an ideal too.
A is *complete* if each Cauchy sequence of elements of A has a limit in A. By standard topological techniques, we can obtain $A^\wedge$, the *completion* of A, which is a topological ring under the $L^\wedge$-adic topology, where $L^\wedge = L\,A^\wedge = \{a \in A^\wedge$: there is a Cauchy sequence $(a_n : n \in N) \subset L$ converging to a$\}$.
Since $\cap L^{\wedge n} = (0)$, we have the associated graded ring $Gr_{L^\wedge}(A^\wedge)$ and the functions $v_{L^\wedge}$, $in_{L^\wedge}$; quite straightforwardly one proves that $Gr_{L^\wedge}(A^\wedge) \approx Gr_L(A)$, and, having identified the two rings, that $v_{L^\wedge}$ and $in_{L^\wedge}$ coincide on A with v_L and in_L.
For an ideal $I \subset A$, the completion of I is the ideal $\{a \in A^\wedge$: there is a Cauchy sequence $(a_n : n \in N) \subset I$ converging to a$\}$; it is easy to prove that

$cl(I) = I^\wedge \cap A$, $\quad I^\wedge = I\,A^\wedge = cl(I)\,A^\wedge$.

Notwithstanding the obvious importance of completions, they are not an easy object to deal with computationally, because they are rings of series unless the L-adic topology is discrete ($L^n = (0)$ for some n).

A more suitable (at least for computational purposes) overring of A is the *Zariskification* A_{1+L} of A, i.e. the localization of A at the multiplicative closed system $1+L = \{1 + g : g \in L\}$ (16).

A_{1+L} is the ring of "formal fractions" $(1+g)^{-1} h$, $h \in A$, $g \in L$, with the usual identification:

$(1+g)^{-1} h = (1+g_1)^{-1} h_1$ if and only if $(1+g_1) h = (1+g) h_1$ (17).

It can be identified with a subring of $A^\wedge$, since in $A^\wedge$, for each $g \in L$, (1-g) has as its inverse the limit of the Cauchy sequence $\Sigma_{i=0\ldots n} g^i$.

Moreover $L^e = L A_{1+L} = L^\wedge \cap A_{1+L}$ induces a topology on A_{1+L}, whose restriction to A is the L-adic topology; the completion of A_{1+L} for this topology is again $A^\wedge$.

Also, it is straightforward to verify that that $Gr_L{}^e(A_{1+L}) \approx Gr_{L^\wedge}(A^\wedge) \approx Gr_L(A)$, and, having identified the three rings, that $v_L{}^e$ and $in_L{}^e$ are the restrictions of $v_{L^\wedge}$ and $in_{L^\wedge}$ and so coincide on A with v_L and in_L.

A_{1+L} is a *Zariski ring*, i.e. it has the following properties:

a) every ideal is closed for the L^e-adic topology

b) for each ideal $I \subset A_{1+L}$, $I A^\wedge \cap A_{1+L} = I$

so that for each ideal $I \subset A$, $cl(I) = I A_{1+L} \cap A$.

Moreover it is the smallest extension of A in $A^\wedge$ which is a Zariski ring (18).

To each ideal $I \subset A$, the homogeneous ideal $in_L(I) := (in_L(a) : a \in I) \subset gr_L(A)$ is associated.

Clearly $in(I) = in(cl(I)) = in(I A_{1+L}) = in(I^\wedge)$.

An L-*standard basis* of I is a finite set $\{g_1,\ldots, g_s\} \subset I$ s.t. $in_L(I) = (in_L(g_1),\ldots, in_L(g_s))$ (19).

Example 1 Let $A := k[X_1,\ldots,X_n]$, $L := (X_1,\ldots,X_n)$. Then $Gr_L(A) \approx A$, with the usual grading; $v_L(f)$ is the order of f; $in_L(f)$ is its initial form, $in_L(I) = in(I)$ is the ideal defining the cone of the tangents at the origin of the variety defined by the ideal I; we reobtain therefore the notions of §1, so that the L-adic topology on A is, very roughly speaking, the algebraic setting for the analytical notion of "infinitesimal order".

We remark thathe completion $A^\wedge$ of A is the formal power series ring $k[[X_1,\ldots,X_n]]$, while its Zariskification A_{1+L} is the local ring at the origin Loc(A), which stresses in this first example the computational advantage of the latter on the former.

Prime ideals in A correspond to irreducible algebraic varieties in the affine space k^n; prime ideals in $A^\wedge$ correspond to (germs of) analytic irreducible varieties passing through the origin; prime ideals in A_{1+L} to irreducible algebraic varieties passing through the origin, and can be obtained by extending to A_{1+L} ideals of varieties in k^n which are not irreducible but have a single and irreducible component passing through the origin.

So all the notions above, in this simplest case, are related to the "local" behaviour of a variety "near" the origin; we can also appreciate a major difference betwenn the completion and the Zariskification: e.g. $I := ((Y^2 - X^2 + X^3)(1 + X)) \subset A$ is not prime while $J = (Y^2 - X^2 + X^3)$ is such; in A_{1+L}, $I A_{1+L} = J A_{1+L} = (Y^2 - X^2 + X^3)$ is a prime ideal, since $(1 + X)$ is invertible (corresponding to a variety not through the

origin); however in $A^\wedge$ we have the factorization $Y^2 - X^2 + X^3 = (Y + X\,g(X))\,(Y - X\,g(X))$ where $g(X) \in k[[X]]$ is the formal power series corresponding to the Taylor expansion of the analytical function $g(x) := \sqrt{(1-x)}$.

Example 2 This leads to a second important case we have already treated (in §4), which is related [20] with the analytic study of singular points of algebraic varieties, for instance in Newton-Puiseux algorithm for determining the analytic branches of a curve at a singular point and more generally when studying analytic components of a complex algebraic variety. We have $A := k[[X_1,\ldots,X_n]]_{alg}$, the ring of algebraic formal power series (i.e. the ring of algebraic functions which vanish and can be developed into Taylor series at the origin), $L := (X_1,\ldots,X_n)$.

Again $A^\wedge = k[[X_1,\ldots,X_n]]$, while, A being local with maximal ideal L, $A_{1+L} = A$.

The geometrical interpretation is essentially as in the example above, prime ideals in Q corresponding to analytically irreducible branches at the origin of an algebraic variety.

Before introducing the next two examples we need the following:

LEMMA 3 Let Q be a ring; let $H \subset J \subset Q$ be two ideals, with $\cap J^n = (0)$. Let $A := Q/H$, $\pi : Q \to A$ the canonical projection, $L := \pi(J)$. The following conditions are equivalent [21]:

1) $H = \cap (H + J^n)$, i.e. $H = cl(H)$

2) $\cap L^n = (0)$

4) J contains all associated primes to H

3) L contains all zero-divisors of A

Proof: cf. [Z-S] V.I, Ch.IV, Theorems 12 and 12'

Example 3 Let $Q := k[Z_1,\ldots,Z_m]$; let $H \subset J \subset Q$ be two ideals. Let $A := Q/H$, $\pi : Q \to A$ the canonical projection, $L := \pi(J)$.

Let us moreover assume that J is prime and that $\cap L^n = (0)$.

Under this assumption we can localize A at L, obtaining the local ring A_L; we are interested in the topology on A_L induced by its maximal ideal $\mathfrak{a} := L\,A_L$. Remark that, A_L being local, it coincides with its Zariskification.

Let V be the variety defined by H (assuming H is radical) and W the subvariety of V defined by J; then A is the ring of polynomial functions on V, while the ring of rational functions on V is obtained by inverting those elements of A which are not zero-divisors, i.e. it is the ring of formal fractions $g^{-1} f$, $f \in A$, $g \in A$ g not zero-divisor with the usual identification

$g^{-1} f = g_1^{-1} f_1$ if and only if $g f_1 - g_1 f = 0$

and the resulting arithmetics mimicking the one in Q.

A polynomial function $f \in A$ identically vanishes on W if and only if $f \in L$ [22], therefore a rational function $g^{-1} f$ is defined on W if and only if it has a representative $g_1^{-1} f_1$ with $g_1 \notin L$. So we have obtained that A_L is exactly the ring of those rational functions on V which are defined at each point of W, while $\mathfrak{a}$ is the ideal of those rational functions on V defined and vanishing on W.

The prime ideals of A_L canonically correspond to those prime ideals of A which contain H and are contained in J; so (again if H is radical) they describe those irreducible algebraic varieties which are contained in V and which pass through the subvariety W.

The notions related to the a-adic topology are, in a very rough sense, a generalization of the concepts involving the "infinitesimal order" (see Ex.1) in a "neighborhood" of W, for "germs of rational functions" over the topological space Spec(A) of all prime ideals (irreducible algebraic varieties) of A with the Zariski topology.

Example 4 More in general, we can avoid requiring that J is prime, so: let $Q := k[Z_1,\ldots,Z_m]$, $H \subset J \subset Q$ be two ideals, $H = \cap (H + J^n)$, $A := Q/H$, $\pi : Q \to A$ the canonical projection, $L := \pi(J)$.

We can study the L-adic topology of A; in this case the Zariskification will be given by A_{1+L}. If, as it is the case in applications (related to normalization), J is the radical of H, then A_{1+L} is semilocal (i.e. it has finitely many maximal ideals $\mathfrak{m}_i$, in which case $A_{1+L} = \oplus A_{\mathfrak{m}_i}$).

It is important to remark, for the applications below, that if L is maximal, then $A_{1+L} = A_L$ [23].

If H is not closed for the J-adic topology, one should substitute cl(H) to H in the above setting: the algorithm we are going to discuss in the next section applies this substitution automatically.

6 STANDARD BASIS COMPUTATION IN LOCAL RINGS

In §3 we have seen that by using standard bases it is possible to explicitly obtain ord(a), in(a) for $a \in$ Loc(P), in(I) for $I \subset$ Loc(P) and also to compute the order and the initial form of the residue class of a mod.I (which are resp. the order and the canonical representative.in k[B] of any normal form of a w.r.t. to a standard basis of I), so covering the situation discussed in Ex.1. In §4 we have extended this to $k[[X_1,\ldots,X_n]]_{alg}$ (Example 2).

We intend here to show that the same technique can be used to cover the situation discussed in Example 3; we will do so by solving the more general but easier case presented in Example 4.

First of all we remark that if we are able to compute $v_L(a)$ and $in_L(a)$ for $a \in A$, we have solved also the problem of computing "order" and "initial form" of elements modulo an ideal, because of the following result:

PROPOSITION 4 Let A be a commutative ring (noetherian and with identity), $L \subset A$ be an ideal s.t. $\cap L^n = (0)$.

Let $I \subset A$, $\mathfrak{I} := cl(I) = \cap (I + L^n)$, $R := A/\mathfrak{I}$, $\pi : A \to R$ the canonical projection, $J := \pi(L)$. Let $a \in A$, $b := \pi(a) \neq 0$.

Then:

1) $Gr_J(R) \simeq Gr_L(A)/in_L(I)$

2) there is c s.t. $\pi(c) = b$ and $in_L(c) \notin in_L(I)$. For such a c

$v_J(b) = v_L(c)$

$in_J(b)$ is the residue class of $in_L(c)$ mod. $in_L(I)$

3) $v_J(b) = \min\{v_L(c) : \pi(c) = b\}$

Proof: 1) We explicitly define a homogeneous morphism $\Pi : Gr_L(A) \to Gr_J(R)$ whose kernel is $in_L(I)$. It is sufficient to define $\Pi(\alpha)$ for a homogeneous $\alpha \in Gr_L(A)$ of some degree n; so α is the residue class mod. L^{n+1} of some $a \in L^n - L^{n+1}$. Then $b := \pi(a) \in J^n$; let β be the residue class of b mod. J^{n+1}; we define $\Pi(\alpha) := \beta$.

It is clear that the definition doesn't depend on the choice of a (since $\pi(L^{n+1}) \subset J^{n+1}$) and that the application is a morphism.

We are left to prove that $Ker(\Pi) = in_L(I) = in_L(\mathfrak{I})$.

In fact if $\alpha \in in_L(\mathfrak{I})$ is homogeneous of degree n, then there is $a \in (\mathfrak{I} \cap L^n) - L^{n+1}$ so that $\alpha = in_L(a)$, but then $\pi(a) = 0$.

Conversely let $\alpha \in Gr_L(A)$, homogeneous of degree n be s.t. $\Pi(\alpha) = 0$, and let $a \in L^n - L^{n+1}$ be s.t. $\alpha = in_L(a)$; since $\Pi(\alpha) = 0$, then $b := \pi(a) \in J^{n+1}$; since $\pi^{-1}(J^{n+1}) = L^{n+1} + \mathfrak{I}$, there are $c \in L^{n+1}$, $d \in \mathfrak{I}$ s.t. $a = c + d$, but then $in_L(c) \leq n+1 < n = in_L(a)$, implies $\alpha = in_L(a) = in_L(d) \in in_L(\mathfrak{I})$.

2) Since $\pi(a) \neq 0$, $a \notin \mathfrak{I} = \cap (I + L^n)$, so there is n s.t. $a \in I + L^n$ and $a \notin I + L^{n+1}$; by the first implication we have $a = d + c$ with $c \in L^n$, $d \in I$, so $\pi(c) = b$; if $in_L(c) \in in_L(I)$, there is $d_1 \in I$ s.t. $in_L(c) = in_L(d_1)$; but then $c_1 := c - d_1 \in L^{n+1}$, $a = (d + d_1) + c \in I + L^{n+1}$.

Since $in_L(c) \notin in_L(\mathfrak{I})$, $c \notin \mathfrak{I} + L^{n+1} = \pi^{-1}(J^{n+1})$; so $b \in J^n - J^{n+1}$, $v_J(b) = n = v_L(c)$. Since $c \in L^n - L^{n+1}$, by the definition above $\Pi(in_L(c)) = in_J(\pi(c)) = in_J(b)$.

3) Let c as above so that $in_L(c) \notin in_L(\mathfrak{I})$, and assume there is d s.t. $\pi(d) = b$ and $v_L(d) < v_L(c)$; then $c - d \in \mathfrak{I}$ and $in_L(c) = in_L(c - d) \in in_L(\mathfrak{I})$, a contradiction.

On the other hand we should be able to give a representation of the associated graded ring which is suitable for computations. Now if we are given a ring R and an ideal J, then we know that $Gr_J(R) = \oplus J^n/J^{n+1}$, which is clearly not a representation very suitable for computational purposes. But since J has a finite basis $(b_1,\ldots,b_t)$, $Gr_J(R)$ is generated as an algebra over R/J by the residue classes $\beta_1,\ldots,\beta_t$ of $b_1,\ldots,b_t$, and so it is isomorphic to the quotient of a polynomial ring $(R/J)[X_1,\ldots,X_t]$ modulo a homogeneous ideal L. Clearly a representation of $Gr_J(R)$ obtained by explicitly giving R/J, $X_1,\ldots,X_t$, and the homogenous ideal L is quite suitable for computations.

If moreover if J is maximal and R is a finitely generated k-algebra, then R/J is a field K, which is an algebraic extension of k and can be effectively given by means of a Gröbner basis of J; in this case we could like that the homogeneous ideal L is explicitly given by means of a Gröbner basis.

We intend to describe in this section how, by means of standard bases and of the tangent cone algorithm, it is possible to obtain such an effective a representation for $Gr_J(R)$ when $R = A_L$, $J = a$ (A and L as in Example 3) or $R = A_{1+L}$, $J = L^e$ as in Example 4; and also to effectively compute $v_J(a)$ and $in_J(a)$ for each $a \in R$, $in_J(I)$ for each $I \subset R$.

First of all, we discuss a very trivial generalization of Example 1, which will however be our main tool for solving the general problem.

Let $P := k[Z_1,\ldots,Z_m,Y_1,\ldots,Y_s]$, let $\wp := (Y_1,\ldots,Y_s) \subset P$; remark that $gr_\wp(P) \simeq P$, graded by $deg_Y : P \to N$, where $deg_Y(Z_i) = 0$, $deg_Y(Y_j) = 1$.

We impose a well-ordering $<_Z$ on $<Z_1,\ldots,Z_m>$ and an ordering $<_Y$ on $<Y_1,\ldots,Y_s>$ which is anticompatible with the degree i.e.

$\deg(m_1) > \deg(m_2)$ implies $m_1 <_Y m_2$

and we order T, the semigroup of terms in P, by the tangent cone ordering < s.t.:

$m < m'$ if and only if $m_Y < m'_Y$ or ($m_Y = m'_Y$ and $m_Z < m'_Z$)

We will consider also the well-ordering $<_w$ on T defined by:

$m <_w n$ if and only if $\deg_Y(m) < \deg_Y(n)$ or ($\deg_Y(m) = \deg_Y(n)$ and $m < n$).

Remark that under <, for $f \in P$ one has $T(f) < 1$ if and only if $f \in \wp$, so that $\mathrm{Loc}(P) = P_{1+\wp}$.

Clearly if $f \in P$, we can write it uniquely as:

$f = \Sigma_{i=1\ldots t} f_i$, f_i homogeneous (w.r.t. $\deg_Y$) and non-zero, $\deg_Y(f_1) < \ldots < \deg_Y(f_i) < \deg_Y(f_{i+1}) <\ldots$;

then $v_\wp(f) = \deg_Y(f_1)$, $in_\wp(f) = f_1$. Also:

LEMMA 4 If G is a standard basis for $I \subset \mathrm{Loc}(P)$ w.r.t. <, then it is a $\wp$-standard basis for I and $\{in_\wp(f) : f \in G\}$ is a Gröbner basis for $in_\wp(I)$ w.r.t. $<_w$.

Proof: the proof of Prop.3 can be applied verbatim

Let now (cf. Ex.4) $Q := k[Z_1,\ldots,Z_m]$; let $H_0 \subset J \subset Q$ be two ideals, with $H_0 := (h_1,\ldots, h_t)$, $J := (f_1,\ldots,f_s)$, let $H = \mathrm{cl}(H_0) = \cap (H_0 + J^m)$.

Let $R := Q/H$, $\pi : Q \to R$ the canonical projection. Let P and $\wp$ be as above.

Define $p : P \to Q$ by $p(Z_i) = Z_i$, $p(Y_j) = f_j$ and let $q : P \to R$ be the composition $q = \pi\, p$; let $A = R_{1+\pi(J)}$, $L := \pi(J)\, A$.

LEMMA 6 q induces a surjective morphism (which we will still denote by q) $q: \mathrm{Loc}(P) = P_{1+\wp} \to A$, so that

$\mathrm{Ker}(q) = (h_1,\ldots, h_t, f_1 - Y_1,\ldots, f_m - Y_m) =: \Im$

$q(\wp) = (\pi(f_1),\ldots,\pi(f_s)) = \pi(J)\, A = L$

Proof: $q: \mathrm{Loc}(P) \to A$ is the composition of the extensions of $p : \mathrm{Loc}(P) \to Q_{1+J}$ and $\pi : Q_{1+J} \to A$. The thesis follows since $\{h_1,\ldots,h_t\}$ is a basis of $H_0\, Q_{1+J} = H\, Q_{1+J} = \mathrm{Ker}(\pi)$.

Then, as a consequence of Proposition 4, since $\mathrm{gr}_L(A) \simeq \mathrm{gr}_\wp(P_{1+\wp}) / in_\wp(\Im) \simeq P / in_\wp(\Im)$, after a standard set G of $\Im$ is computed, $\mathrm{gr}_L(A)$ is explicitly given as a polynomial ring modulo a homogeneous ideal, which is given through a Gröbner basis.

More exactly we have:

$\mathrm{gr}_L(A) \simeq k[Z_1,\ldots,Z_m,Y_1,\ldots,Y_s]/in_\wp(\Im)$

Moreover, since we have a Gröbner basis of $in_\wp(\Im)$, we know the set $B := \{t \in T : t \notin M_w(in_\wp(\Im))\} = \{t \in T : t \notin M(\Im)\}$.

The vector space isomorphism between $k[Z_1,\ldots,Z_m,Y_1,\ldots,Y_s]/in_\wp(\Im)$ and k[B] can be used to impose on the latter vector-space a product which makes it isomorphic to $k[Z_1,\ldots,Z_m,Y_1,\ldots,Y_s]/in_\wp(\Im)$ and in

turn to $gr_L(A)$. It is immediate to verify that this isomorphism is degree preserving if we just assign to each $b \in B$ its degree $deg_Y(b)$ in P. We can therefore identify $gr_L(A)$ with k[B].

Also the projection Π: P → k[B] (cf. Prop. 4) can be easily computed by computing the canonical representative of an element modulo $in_{\wp}(\Im)$.

Therefore we have:

PROPOSITION 5 Let $a \in Q - \{0\} \subset P$, and let us compute $b \in P$ and a unit u s.t. $u^{-1} b$ is a local normal form of a w.r.t. G.

Let $I \supset \Im$ be an ideal in P, F a standard set for I w.r.t. <.

Then:

$v_L(q(a)) = v_{\wp}(b) = deg_Y(M(b))$.

$in_L(q(a)) = \Pi(in_{\wp}(b))$

$\{q(f) : f \in F\}$ is a L-standard basis of q(I).

Example 5 Let $Q := k[X,Y,Z]$, $H := (Y^2 - XZ)$, $J := (Y^2 - XZ, X^3 - YZ, X^2Y - Z^2)$; since H is prime and contained in the prime ideal J, then H = cl(H).

Let $R := Q/H = k[x,y,z]$, $A := R_{1+\pi(J)}$, $L := \pi(J)$ $A = (x^3 - yz, x^2y - z^2)$, $P := k[X,Y,Z,V,T,U]$. Then $\Im$ $= Ker(q) = (Y^2 - XZ, Y^2 - XZ - V, X^3 - YZ - U, X^2Y - Z^2 - T)$, $\wp := (V,T,U) \subset Loc(P)$.

A standard basis of $\Im$ is given by $G := \{Y^2 - XZ, X^3 - YZ - U, X^2Y - Z^2 - T, V, YU - XT, ZU - YT\}$ so that

$in_{\wp}(\Im) = (Y^2 - XZ,\ X^3 - YZ, X^2Y - Z^2, V, YU - XT, ZU - YT)$

$gr_L(A) = K[X,Y,Z]/J\ [T,U,V]/(V, YU - XT, ZU - YT) \approx K[X,Y,Z]/J\ [T,U]/(YU - XT, ZU - YT)$

If $f := x^4 - y^3 \in A$, a normal form of $X^4 - Y^3$ w.r.t. G is XU, so $v_L(f) = 1$ and $in_L(f) = xu$.

A standard basis of $(XU, \Im)$ is

$G \cup \{XU, X^2T, XYT, YZT + TU, XZT + U^2, Z^2T + T^2, U^3\}$

so that a L-standard basis of (f) is $\{xu, x^2t, xyt, yzt + tu, xzt + u^2, z^2t + t^2, u^3\}$ and

$in_L(\ (f)\ ) := (xu, x^2t, xyt, yzt, xzt, z^2t, u^3)$

Let us now assume, moreover, that J is prime (cf. Ex. 3). Then denoting, as in Ex. 3, a the maximal ideal of $A_L = R_{\pi(J)}$:

LEMMA 7 Let K be the field of fractions of Q/J; $p : Q \to Q/J \approx R/\pi(J) \approx A/L$ denote the canonical projection; σ: $P \to Q/J\ [Y_1,\ldots,Y_S] \subset K[Y_1,\ldots,Y_S]$ denote the morphism which coincides with p on Q and s.t. $\sigma(Y_i) = Y_i$. Then:

1) $J = in_{\wp}(\Im) \cap Q$

2) if F is a Gröbner basis of $in_{\wp}(\Im)$ w.r.t. $<_W$, then $F \cap Q$ is a Gröbner basis of J w.r.t. $<_Z$ and p(F) is a Gröbner basis for $p(in_{\wp}(\Im))$ w.r.t. the restriction of $<_W$ to the terms of $K[Y_1,\ldots,Y_S]$

3) $Gr_L(A) \approx P / in_{\wp}(\Im) \approx (A / J)\ [Y_1,\ldots,Y_S] / p(in_{\wp}(\Im))$

4) $Gr_a(A_L) \approx K[Y_1,\ldots,Y_S] / p(in_{\wp}(\Im))$

5) let $I \subset A_L$ be an ideal: if G is a L-standard basis for $I \cap A$, then it is a a-standard basis for I.

Proof: 1) $\forall$ i, $f_i = in_{\wp}(f_i - Y_i)$, so $J \subset in_{\wp}(\Im) \cap Q$. Conversely assume $a \in in_{\wp}(\Im) \cap Q$. Then there is $b \in \Im \cap P$ s.t. $in_{\wp}(b) = a$, i.e. $b = a + c$ with $c \in (Y_1,\ldots,Y_s)$; since $a + c = b = \Sigma\, g_i\,(f_i - Y_i)$, by evaluating at $Y_1 = \ldots = Y_t = 0$ we obtain $a = \Sigma\, g'_i\, f_i$ so $a \in J$.

2) both facts are well-known properties of Gröbner bases (cf. [GTZ])

3) is trivial

4) $V = \{in_L(f) : f \notin L\}$ is a multiplicative closed system, for if $a_1, a_2 \in V$, $f_1, f_2 \notin L$ are such that $in(f_i) = a_i$, then $f_1\, f_2 \notin L$, since L is prime, and $a_1\, a_2 = in(f_1\, f_2) \in V$.

Clearly $V^{-1}\, Gr_L(A) \approx K[Y_1,\ldots,Y_s] / p(in_{\wp}(\Im))$, so we have to prove that $Gr_a(A_L) \approx V^{-1}\, Gr_L(A)$.

In fact we obtain such an isomorphism in the following way: if $a \in A_L$, $a = b^{-1}\, c$ with $b \notin L$, we associate $in_a(a)$ with $in_L(b)^{-1}\, in_L(c)$. It is easy to verify that the definition doesn't depend on the choice of a nor on the choice of its representation and that the resulting application is bijective and a morphism.

5) if $a \in I$, $a = b^{-1}\, c$ with $b \notin L$, then $c = b\, a \in I \cap A$, so $in_L(c) \in (in_L(g) : g \in G) \subset Gr_L(A)$ and $in_a(a) = in_L(b)^{-1}\, in_L(c) \in (in_L(g) : g \in G) \subset V^{-1}\, Gr_L(A)$.

By means of Lemma 5 we obtain an explicit representation of $Gr_a(A_L)$; in order to get computational results from it, we need some more insight on the way we present K.

Let us consider $B_0 := \{b \in B : deg_Y(b) = 0\} \subset Q$. Because $F \cap Q$ is a Gröbner basis of J w.r.t. $<_Z$ we have a k-vector space isomorphism between A/J and $k[B_0]$, which by Gröbner basis techniques allows to define a domain structure on $k[B_0]$ isomorphic to A/J and therefore to define a field structure isomorphic to K on the set of formal fractions $\{f^{-1}\, g : f, g \in k[B], f \neq 0\}$, so that we can identify K with the latter set.

Let us now consider $B_1 := \{b \in B \cap k[Y_1,\ldots,Y_s]\}$. Since p(F) is a Gröbner basis for $p(in_{\wp}(\Im))$ w.r.t. the restriction of $<_W$ to the terms of $K[Y_1,\ldots,Y_s]$, it is easy to prove that $B_1 = \{b \in T : b \notin M(p(in_{\wp}(\Im)))\}$, so, again, we have a K-vector space isomorphism between $Gr_a(A_L) \approx K[Y_1,\ldots,Y_s] / p(in_{\wp}(\Im))$ and $K[B_1]$ and so a ring structure on the latter isomorphic to the one of $Gr_a(A_L)$. As a consequence:

COROLLARY 1 Let $a_0, a_1 \in Q - \{0\} \subset P$, $a_1 \notin \Im$, and let us compute $b_0, b_1 \in P$ and units u_0, u_1 s.t. $u_i^{-1}\, b_i$ is a local form of a_i w.r.t. to a standard basis G of $\Im$.

Let $I \supset \Im$ be an ideal in Loc(P), F a standard basis for I w.r.t. $<$.

Then:

$v_a(\pi(a_0)^{-1}\, \pi(a_1)) = v_{\wp}(b_1) = deg_Y(M(b))$.

$in_a(\pi(a_0)^{-1}\, \pi(a_1)) = \Pi(in_{\wp}(b_0))^{-1}\, \Pi(in_{\wp}(b_1))$

$\{q(f) : f \in F\}$ is an a-standard basis of $q(I)\, A_L$.

Example 5 (cont.) Actually J is a prime ideal and one can easily remark that $J = in_{\wp}(\Im) \cap Q$, $A/L = Q/J = k[X,Y,Z]/(Y^2 - XZ, X^3 - YZ, X^2Y - Z^2)$ so that $K = k(\xi,\eta,\zeta)$ where $\eta^2 - \xi\zeta = \xi^3 - \eta\zeta = \xi^2\eta - \zeta^2 = 0$.

Since $Gr_L(A) = K[X,Y,Z]/J\,[T,U]/(YU - XT, ZU - YT)$ one has

$Gr_a(A_L) = K[T,U]/(\eta U - \xi T, \zeta U - \eta T) \simeq K[T]$ by identifying U with ξ/η $T = \eta/\zeta$ T, since $\eta^2 - \xi\zeta = 0$.

Since a L-standard basis of (f) is $\{xu, x^2t, xyt, yzt + tu, xzt + u^2, z^2t + t^2, u^3\}$, an a-standard basis of (f) A_L is $\{T\}$.

Already in this easy example, we must remark that L-standard bases can be quite complex also if a-standard bases are easy, and, especially, that the arithmetics of K, under this presentation, can be easily become unfeasible for the lack of canonical representatives for elements, which require to perform arithmetics mod. J (and so normal form computations) just for testing equality.

If however J is a maximal ideal, then K = Q/J and is isomorphic to $k[B_0]$. Also $A_L = A$, $v_a = v_L$, $in_a = in_L$, $Gr_a(A_L) = gr_L(A)$ so we are reduced to the easier case of Proposition 5.

Moreover if $<_Z$ is a lexicographical ordering, the (reduced) Gröbner basis of J is given by $\{g_1,\ldots, g_m\}$ where each g_i is the minimal polynomial of the class of Z_i mod. J, over the field $K[Z_1,\ldots,Z_{i-1}]/(f_1,\ldots,f_{i-1})$. So k[B] is just the canonical presentation of the algebraic extension K over k.

Moreover (in case k is of char. 0), if we are willing to perform a random linear changement of coordinates substituting Z_1 with $Z_1 - \Sigma c_i Z_i$ ($c_i \in Q$), the reduced Gröbner basis of J becomes (probabilistically) $\{g_1(Z_1), Z_2 - g_2(Z_1), \ldots, Z_m - g_m(Z_1)\}$, so that K[B] is the canonical presentation of the simple algebraic extension K over k.

The interesting fact is that a bit more of algebra allows to show that one can effectively reduce oneself to this case.

For that we must first compute a Gröbner basis of the prime ideal J.

From it ([CAR, K-W, LOG, G-T]), we can easily obtain a maximal subset $\{Z_{i_1},\ldots,Z_{i_d}\}$ of algebraically independent variables mod. J. Let us further relabel our variables denoting $\{U_1,\ldots,U_d\}$ the algebraically independent ones, and $\{V_1,\ldots, V_r\}$ the remaining ones.

PRIMBASISSATZ ([GRÖ]) Under the assumptions and with the notation above, there are polynomials $g_1,\ldots, g_r, g, g_i \in k[U_1,\ldots,U_d,V_1,\ldots, V_{i-1}][V_i]$ with leading coefficient in $k[U_1,\ldots,U_d]$, $g \in k[U_1,\ldots, U_d]$ s.t. denoting $Q^0 := k(U_1,\ldots,U_s)[V_1,\ldots,V_r]$

i) each g_i is irreducible over $k[U_1,\ldots,U_d,V_1,\ldots, V_{i-1}]/(g_1,\ldots,g_{i-1})$

ii) $(g_1,\ldots,g_r) : g = J$

iii) $J^0 := (g_1,\ldots, g_r)\, Q^0$ is a maximal ideal and $K \simeq Q^0/J^0$

iv) $(g_1,\ldots,g_r)$ are a reduced Gröbner basis of J^0.

v) $Q^0{}_{J^0} = Q_J$

PROPOSITION 6 Denote $H^0 := H\, Q^0$, $R^0 := Q^0/H^0$, $\pi^0 : Q^0 \to R^0$ the canonical projection. Then $\pi^0(J^0)$ is a maximal ideal in R^0 and $R^0{}_{\pi^0(J^0)} = A_L$.

Proof: Both rings are the quotient of $Q^0{}_{J^0} = Q_J$ by the extension of H in $Q^0{}_{J^0} = Q_J$.

Example 5 (cont.) A lexicographical Gröbner basis of J is $\{YZ - X^3, Z^2 - X^2Y, XZ - Y^2, Y^3 - X^4\}$, from which we know that a maximal set of alg. ind. variables is $\{X\}$.

So $Q^0 = k(X)[Y,Z]$, $H^0 := (Z - 1/X\ Y^2)$, $J^0 := (Z - 1/X\ Y^2, Y^3 - X^4)$, $R^0 := Q^0/H^0 = k(X)[y,z]$, $\pi^0(J^0) = (z - 1/X\ y^2, y^3 - X^4)$.

So $K = Q^0/J^0 = k(X)[\eta,\zeta]$ with $\eta^3 = X^4$, $\zeta = 1/X\ \eta^2$.

So we take $P := k(X)[Y,Z,U,V]$, $\Im = (Z - 1/X\ Y^2, Z - 1/X\ Y^2 - U, Y^3 - X^4 - V)$, $\wp := (U,V)$.

A standard basis of $\Im$ is given by $G := \{Z - 1/X\ Y^2, U, Y^3 - X^4 - V\}$ so that

$$in_\wp(\Im) = (Z - 1/X\ Y^2, U, Y^3 - X^4)$$

$$gr_a(A_L) \simeq K(X)[Y,Z]/J^0\,[U,V]/(U) \simeq K[V].$$

If $f := yz - X^3 \in Q^0$, a normal form of $YZ - X^3$ w.r.t. G is $1/X\ V$, so $v_a(f) = 1$ and $in_a(f) = 1/X\ V$.

A standard set of $(1/X\ V, \Im)$ is

$$G \cup \{V\}$$

so that a a-standard basis of (f) is $\{V\}$.

7 THE EFFECTIVE METHOD OF THE ASSOCIATED GRADED RINGS

The chapter on Local Algebra of the classical treatise [Z-S] begins with a section headed "The method of associated graded rings". The basic idea is as follows: even in the most general setting we presented in §5, $Gr_L(A)$ is the quotient of a polynomial ring over A/L modulo a homogeneous ideal. Since the structure of such a ring is more easy to handle, one can hope to get informations on A and its L-adic topology, by solving related questions on $Gr_L(A)$.

In the setting we discussed in the previous section, we have something more, namely an explicit presentation of $Gr_L(A)$ as a polynomial ring modulo a homogeneous ideal, which is given through a Gröbner basis.

So, at least in principle, the method of associated graded rings is turned into a computational tool, since, because of this presentation of $Gr_L(A)$, Gröbner basis techniques can be used to find explicit solutions to a variety of questions on it.

In what follows, we will mostly restrict to the case of a local ring AL and to the topology of its maximal ideal a, assuming that $Gr_a(AL)$ is explicitly given as a polynomial ring P over $K := AL/a$, modulo a homogeneous ideal H given through a Gröbner basis:

$$Gr_a(AL) = K[y_1,\ldots,y_s] = K[Y_1,\ldots,Y_s]/H$$

and that we know elements $f_1,\ldots,f_n \in AL$ s.t. $y_i = in_a(f_i)$.

In the easiest case of Ex.1, $AL = Loc(P)/J$, $a = (X_1,\ldots,X_n)$ we have $(s = n)$ and:

$$Gr_a(AL) = K[y_1,\ldots,y_n] = K[Y_1,\ldots,Y_n]/H \text{ with } H = in(J) \text{ and } y_i = in(X_i)$$

In the case $A = k[[X_1,\ldots,X_n]]_{alg}/J$ (§4) we have:

$$Gr_a(AL) = K[y_1,\ldots,y_n] = K[Y_1,\ldots,Y_n]/H \text{ with } H = in(J) \text{ and } y_i = in(X_i)$$

In the case of Ex.3 (with notation of Prop. 4) we have:

$$Gr_a(A_L) = K[y_1,\ldots,y_s] = K[Y_1,\ldots,Y_s]/H \text{ with } H = p(in_\wp(\Im)), \text{ and } y_i = in_L(q(f_i)).$$

3.1 DIMENSION

It is a classical result that $\dim(AL) = \dim(Gr_a(AL))$.

Moreover if **H** is an ideal in the polynomial ring $P = K[Y_1,\ldots,Y_s]$ and a Gröbner basis of **H** is known, $\dim(P/H) = \dim(P/M(H))$ and there are several algorithms [CAR, K-W, LOG, G-T] to compute $\dim(P/M(H))$.

One can remark that the computation of the dimension is easier if one starts with a lexicographical Gröbner basis, but very often to compute the lexicographical Gröbner basis is very hard.

3.2 SYSTEMS OF PARAMETERS

Most of the algorithms for computing the dimension of **P/H** (and all the ones quoted above) do so by producing a maximal subset of variables which are algebraically independent mod. I.

A system of parameters in the local ring AL, $\dim(AL) = \delta$, is a set $\{a_1,\ldots,a_\delta\}$ of elements of AL which generate a primary ideal for the maximal ideal **a**. It is easy to show that if $\{a_1,\ldots,a_\delta\}$ are such that $\{in(a_1),\ldots, in(a_\delta)\}$ are a maximal set of algebraically independent homogeneous elements of degree 1 in $Gr_a(AL)$, then $\{a_1,\ldots,a_\delta\}$ is a system of parameters.

So if $\{Y_{i_1},\ldots,Y_{i_\delta}\}$ is a maximal set of algebraically independent variables mod. **H**, then $\{f_{i_1},\ldots,f_{i_\delta}\}$ is a system of parameters.

Also, checking if a given set is a system of parameters can be easily done, checking algebraic independence of their initial forms.

3.3 HILBERT FUNCTION

If I is a homogeneous ideal in the polynomial ring $P = K[Y_1,\ldots,Y_s]$, the Hilbert function of I, $\mathbf{Hilb_P}(I) : \mathbf{N} \rightarrow \mathbf{N}$ is defined by letting $\mathbf{Hilb_P}(I,n)$ to be the dimension as a **K**-vector space of the degree n component of the graded module **P/H**. It clearly coincides with the Hilbert function of M(I), which can be computed by combinatorial techniques ([M-M],[B-S],[PON]) and it is a polynomial for sufficiently large n.

If AL is a local ring with maximal ideal **a** and J an ideal in AL, the Hilbert function $H_{AL}(J) : \mathbf{N} \rightarrow \mathbf{N}$ is defined by $\mathbf{Hilb}_{AL}(J,n) = \text{length}(AL / (J+a^n))$, where the length of an AL-module M is the length r of a maximal strictly descending chain of AL-modules $M = M_0 \supset M_1 \supset \ldots \supset M_r = (0)$.

It can be easily proved that $\mathbf{Hilb}_{AL}(J,n) = \Sigma_{i=0\ldots n}\, \mathbf{Hilb_P}(in_a(J) + H,i)$. So the Hilbert function (and of the Hilbert polynomial) of an ideal in a local ring is reduced to the same problem on polynomial rings.

Many interesting invariants (like the dimension, which is the dimension of the corresponding quotient ring and the multiplicity) of the ideal $J \subset AL$ can be directly read off from the Hilbert polynomial.

A more general situation has been studied with similar techniques in [SPA].

3.4 REGULARITY

A local ring is called regular whenever its associated graded ring is isomorphic to a polynomial ring. The geometrical meaning (in the case of Ex. 3) is quite easy; with the notation of example 3, this means that the variety defined by J is a regular subvariety of the one defined by H.

In the representation we obtain for $Gr_a(AL)$ this doesn't necessarily mean that the ideal H is the zero ideal; it just mean that it is generated by linear elements. This can be however easily checked and, if the ring is regular, it is immediate to modify the presentation of $Gr_a(AL)$ in order to present it as a polynomial ring.

3.5 RESOLUTIONS

Two algorithms to compute (the initial modules of) a free resolution of an ideal I in a local ring A_L (as in Ex.3) are presented in [G-Z].

The first algorithm makes use of the fact that (like Buchberger algorithm) the Tangent Cone Algorithm, while computing a standard basis $(g_1,\ldots,g_t)$ of an ideal in Loc(P), produces also a basis of the module of syzygies among the g_i's (which is a submodule of $Loc(P)^t$). By the extension of the algorithm to modules (case 2) the same result holds.

So each module of syzygies can be iteratively computed each module of syzygies by computing a standard basis of the previous one.

The second is a constructive version of the following theorem in [ROB1]:

THEOREM Each graded $Gr_a(A_L)$-free resolution of $in_a(I)$ lifts to an A_L-free resolution of I

which is obtained by adapting the techniques proposed in [M-M] and uses the notion of T-standard bases.

8 ISOLATED SINGULARITIES

The Tangent Cone Algorithm for modules (case 1) has been applied in [L-P] and [P-S] to the study of isolated singularities.

Let C be a variety in C^n with an isolated singularity at the origin; two important invariants of the singularity are the Milnor number μ and the Tjurina number τ of the singularity, the first being a topological invarient and the second an analytic invariant of the singularity.

In case C is a complete intersection variety with an isolated singularity, both numbers have an easy characterization as dimensions of C-vector spaces; namely let C be a complete intersection variety in C^n with an isolated singularity at the origin; in particular C is given by equations $f_1 = \ldots = f_m = 0$, where $f_i \in C[X_1,\ldots,X_n]$ (24), $f(0) = 0$.

Let I_μ be the ideal in $C[[X_1,\ldots,X_n]]$ generated by the maximal minors of the Jacobian matrix of $f_1,\ldots, f_m$; I_τ the ideal in $C[[X_1,\ldots,X_n]]$ generated by the maximal minors of the Jacobian matrix of $f_1,\ldots, f_m$ and by $f_1,\ldots,f_m$.

Since 0 is an isolated singularity of C, both ideals are 0 dimensional so that $C[[X_1,\ldots,X_n]]/I_\mu$ and $C[[X_1,\ldots,X_n]]/I_\tau$ are finitely dimensional C-vector spaces.

Because of the following easy:

LEMMA 7 Let $\{f_1,\ldots,f_t\} \in k[X_1,\ldots,X_n] =: P$, denote by I the ideal they generate in $k[X_1,\ldots,X_n]$, by J the ideal they generate in $k[[X_1,\ldots,X_n]]$, by Loc(I) := I Loc(P). If J is a 0-dimensional ideal, then:

$$\dim_k k[[X_1,\ldots,X_n]]/J = \dim_k Loc(P)/Loc(I) = \dim_k P/M_<(I)$$

where $<$ is any total semigroup ordering on T s.t. $w_<(X_i) < 0$ for each i

both μ and τ can be computed easily by means of the tangent cone algorithm.
Other invariants (related to the Poincaré complex of the singularity) for isolated singularities can be described in terms of the finite dimension as C-vector spaces of modules $C[[X_1,...,X_n]]^r/U$, U a submodule explicitly given through a basis.
By the generalization of the tangent cone algorithm to modules, such invariants have been extensively computed and used to derive theoretical results ([L-P],[P-S]) on isolated singularities of curves in C^2 and complete intersection curves in C^3.

ACKNOWLEDGEMENTS

I like to thank Alain Poli and the Organizing Committee of AAECC 7 for their invitation to present these results.
This paper has grown out from the lecture notes of a cycle of talks I gave while visiting the Universdidad Complutense of Madrid in 1988 and I was able to complete it only thanks to an invitation at Rennes University: I would thank Maria Emilia Alonso, Marie Françoise Roy and all the friends in Madrid and in Rennes for their nice hospitality.
My thanks also to Mario Raimondo which patiently discussed with me the presentation of the geometrical aspects.

REFERENCES

[ALR] M.E.Alonso, I.Luengo, M.Raimondo, *An Algorithm on Quasi-Ordinary Polynomials*, Proc. AAECC6, L.N.Comp.Sci. 356 (1989)

[A-M] M.Artin, B. Mazur, *On periodic points*, Ann. Math. 81 (1965), 82-99

[AMR1] M.E.Alonso, T.Mora, M.Raimondo, *Computing with algebraic series*, Proc. ISSAC 89 (1989)

[AMR2] M.E.Alonso, T.Mora, M.Raimondo, *A computational model for algebraic power series*, submited to J. Pure Appl. Alg.

[B-S] D. Bayer, Communication at COCOAII (1989)

[CAR] G. Carrà,

[FKS] A.Furukawa, H. Kobayashi, T. Sasaki, *Gröbner bases of ideals of convergent power series* (1985)

[G-T] A. Galligo, C. Traverso

[GTZ] P.Gianni, B.Trager, G.Zacharias,

[G-Z] M.Grieco, B.Zucchetti, Communication at AAECC-7 (1989)

[GRÖ] W. Gröbner

[K-W] Kredel, Weispfenning

[LOG] A. Logar

[L-P] I. Luengo, G. Pfister, *Normal forms and moduli spaces of curve singularities with semigroup $<2p, 2q, 2pq + d>$*, Preprint Univ. Compl. Madrid (1988)

[M-M] H.M. Möller, F. Mora, *New constructive methods in classical ideal theory*, J. Alg. 100 (1986)

[MOR1] F. Mora, *An algorithm to compute the equations of tangent cones*, Proc. EUROCAM 82, Lect.N.Comp.Sci. 144 (1982), 158-165

[MOR2] F. Mora, *A constructive characterization of standard bases*, Boll. Unione Matematica Italiana ,Sez. D, 2 (1983), 41-50 .

[MOR3] F. Mora, *An algorithmic approach to local rings*, Proc. EUROCAL 85, Lect. N. Comp. Sci. 204 (1985), 518-525.

[MPT] T. Mora, G. Pfister, C.Traverso *An introduction to the tangent cone algorithm*, submitted to C.Hoffman Ed. *Issues in non-linear geometry and robotics*, JAI Press

[P-S] G. Pfister, H.Schönemann, *Singularities with exact Poincaré complex but not quasihomogeneous*, Preprint 147, Humboldt Univ., Dept. Math. (1988)

[PON] Ponkratjev, to appear in Proc. Eurocal '87, L.N.C.S.

[ROB1] L.Robbiano, *Coni tangenti a singolarità razionali*, Atti Conv. Geom. Alg. Firenze (1981)

[ROB2] L.Robbiano, *On the theory of graded structures*, J. Symb. Comp. 2 (1986) 139-170

[SPA] W. Spangher, *On the computation of the Hilbert-Samuel series and multiplicity*, Proc. AAECC6, L. N. Comp. sci. 357 (1989), 407-414

[Z-S] O.Zariski, P.Samuel, *Commutative Algebra*, Van Nostrand (1958)

---

[1] If I'm allowed a trivial historical remark, the birth date of the Tangent Cone Algorithm is known, being the night of January 12, 1981. The birth place is however less precisely known, since the author got the crucial idea on a night train from Genoa to Antwerpen in a neighborhhod of the Swiss-German border.

[2] To the references quoted in the text one should add [MOR1], [MOR2] which contain the original presentation of the tangent cone algorithm and [MOR3], with its application to localizations of coordinate rings at prime ideals.
Moreover the pioneering work [GAL] is rich in applications of standard basis techniques to ideals of power series.

[3] To be precise in order that this geometrical notion makes sense, we should restrict ourselves to radical ideals.

[4] Again, to be precise, in order that the analytical notions make sense, we should restrict to convergent series, but the algebraic formulation can be performed with no restriction.

[5] For a detailed introduction to the tangent cone algorithm, the reader can consult the recent survey [MPT].

[6] An important exception is when I is 0-dimensional (for that case sf. [FKS] and [MPT].
One clearly must introduce computability restrictions (if one allows a single power series whose coefficients are given by a semirecursive function, then standard basis computation becomes undecidable), but otherwise I'm unable to figure a general obstruction against the existence of a standard basis algorithm for power series; for that matter however I'm unable to figure how such an algorithm should work.

[7] If $\{Y_1,\ldots,Y_d\}$ is empty then we have a well-ordering and there is no need of the tangent cone algorithm, which actually in such instance reduces to Buchberger algorithm

[8] For the purposes of this paper, it is not crucial to know how it works. The interested reader can consult the survey [MPT], where improved versions are presented. There are available implementations: a MODULA-2 one running under MS-DOS by G.Pfister and H. Schönemann (Humboldt Univ. Berlin); a Common Lisp one in the ALPI system by C. Traverso (Pisa). The algorithm is actually under implementation in the MacIntosh system CoCoA by A. Giovini and G. Niesi (Genova).
Standard bases can also be computed (by Lazard's Homogeneization Technique) on any system with a Buchberger algorithm.

[9] Both ways generalize a corresponding way of defining Gröbner bases for submodules of P^t; for a presentation of them and a comparison of their respective merits cf. [M-M], where they are called T-baseds and G-bases respectively.

[10] where $(e_1,\ldots,e_t)$ denotes the canonical basis of $Loc(P)^t$ i.e. $\Sigma f_i e_i := (f_1,\ldots,f_t)$

[11] The original result is more general, covering those orderings for which there exists a semigroup morphism $w : T \to Z$ s.t. $w(m) < 0$ iff $m \neq 1$ and $w(m_1) < w(m_2)$ implies $m_1 < m_2$.

[12] B must belong to P, not to Loc(P) in order that the construction holds

[13] i.e. it is in the residue class of b mod. (g) and no terms with non-zero coefficients in its expansion are multiple of T(g)

[14] This section is essentially an abstract from the classical treatise [Z-S], Chap. VIII.

[15] We will often omit the subscript L

[16] There are no zero-divisors in 1+L, in fact if $g \in L$, $h \in A$ are s.t. $(1-g)\,h = 0$, then $h = g^n h \in L^n\ \forall n$, so $h = 0$.

[17] So A_{1+L} is effective, whenever A is such; The same doesn't hold for $A^\wedge$ which is a ring of series.

[18] Because in such a Zariski ring the elements of 1 + L must be invertible.

[19] The definitions and the constructions leading to the concepts of Gröbner and standard bases can be interepreted in topological terms so that they are a generalization of the notions realted to L-adic topologies. For such a topological theory unifying the notions of Gröbner bases, standard bases and L-standard bases, one can consult [ROB2].

[20] not as easily as the example above could induce to believe

[21] Their geometrical meaning in case H and J are radical ideals is that the variety defined by J is contained in each irreducible component of the variety defined by H.

[22] since this is equivalent to say that $\forall g \in Q$ s.t. $\pi(g) = f$, $g \in J$

[23] Since L is maximal, if $a \notin L$, then the ideal generated by a and L is the whole ring, so $1 = s\,a + b$ for some $s \in A$, $b \in L$, then $(1 - b)^{-1}\,s\,a = 1$ in A_{1+L}, so a is invertible in A_{1+L} and $A_L \subset A_{1+L}$. Since if $a \in A$ can be written 1 + b with $b \in L$, then $a \notin L$ (otherwise $1 \in L$), the converse inclusion is obvious.

[24] Actually one should require the f_i to be convergent power series; the (non essential) restriction is due to computability reasons.