



Bases of subalgebras of $K[[x]]$ and $K[x]$

Abdallah Assi, Pedro A. García-Sánchez, Vincenzo Micale

► To cite this version:

Abdallah Assi, Pedro A. García-Sánchez, Vincenzo Micale. Bases of subalgebras of $K[[x]]$ and $K[x]$. MEGA'2015 (Special Issue), Jun 2016, Trento, Italy. hal-01094629v3

HAL Id: hal-01094629

<https://hal.science/hal-01094629v3>

Submitted on 29 Aug 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

BASES OF SUBALGEBRAS OF $\mathbb{K}[[x]]$ AND $\mathbb{K}[x]$

A. ASSI, P. A. GARCÍA-SÁNCHEZ, AND V. MICALE

ABSTRACT. Let f_1, \dots, f_s be formal power series (respectively polynomials) in the variable x . We study the semigroup of orders of the formal series in the algebra $K[[f_1, \dots, f_s]] \subseteq K[[x]]$ (respectively the semigroup of degrees of polynomials in $K[f_1, \dots, f_s] \subseteq K[x]$). We give procedures to compute these semigroups and several applications. We prove in particular that the space curve parametrized by f_1, \dots, f_s has a flat deformation into a monomial curve.

1. INTRODUCTION

Let \mathbb{K} be a field and let $\mathbb{K}[[x]]$ be the ring of formal power series over \mathbb{K} . Let $f_1(x), \dots, f_s(x)$ be s elements of $\mathbb{K}[[x]]$ and let $R = \mathbb{K}[[f_1, \dots, f_s]]$ be the subalgebra of $\mathbb{K}[[x]]$ generated by f_1, \dots, f_s . Given $f \in R$, let $\text{o}(f)$ the order of f . The set $\text{o}(R) = \{\text{o}(f) \mid f \in R\}$ is a submonoid of \mathbb{N} , and the knowledge of a system of generators of this monoid is important for the understanding of the subalgebra R . When furthermore $\mathbb{K}[[x]]$ is an R -module of finite length, then $\text{o}(R)$ is a numerical semigroup.

A similar construction can be made in the ring of polynomials $\mathbb{K}[x]$. More precisely let $f_1(x), \dots, f_s(x)$ be s elements of $\mathbb{K}[x]$ and let $A = \mathbb{K}[f_1, \dots, f_s]$ be the subalgebra of $\mathbb{K}[x]$ generated by f_1, \dots, f_s . Given $f \in A$, let $\text{d}(f)$ the degree of f . The set $\text{d}(A) = \{\text{d}(f) \mid f \in A\}$ is a submonoid $\text{d}(A)$ of \mathbb{N} , and the knowledge of a system of generators of this monoid is important for the understanding of the subalgebra A . When furthermore $\mathbb{K}[x]$ is an A -module of finite length, then $\text{d}(A)$ is a numerical semigroup.

A numerical semigroup S is a submonoid of the set of nonnegative integers under addition such that the $\mathbb{N} \setminus S$ is finite, or equivalently, $\text{gcd}(S) = 1$ (the greatest common divisor of the elements of S), see for instance [16]. In this case, there exists a minimum $c \in S$ such that $c + \mathbb{N} \subseteq S$. We call this element the *conductor* of S , and denote it by $c(S)$ (the motivation of this name and others coming from Algebraic Geometry is explained in [3, 8]).

Assume that f_i is a monomial x^{a_i} for every $i \in \{1, \dots, s\}$. Then $\text{o}(R)$ (respectively $\text{d}(A)$) is generated by a_1, \dots, a_s . In this case, $R \simeq \mathbb{K}[[X_1, \dots, X_s]]/T$ (respectively $A \simeq \mathbb{K}[X_1, \dots, X_s]/T$), where T is a prime binomial ideal and, thus, $V(T)$ is a toric variety.

Given a subalgebra $R = \mathbb{K}[[f_1, \dots, f_s]]$ (respectively $A = \mathbb{K}[f_1, \dots, f_s]$), the main objective of this paper is to describe an algorithm that calculates a generating system of $\text{o}(R)$ (respectively $\text{d}(A)$). The algorithm we present here allows us, by using the technique of homogenization, to construct a flat $\mathbb{K}[[u]]$ -module (respectively $\mathbb{K}[u]$ -module) which is a deformation of R (respectively A) to a binomial ideal. This technique is well known when $R = \mathbb{K}[[f_1, f_2]]$ and \mathbb{K} is algebraically closed field of characteristic zero (see [11] and [19]). It turns out that the same holds wherever we can associate a semigroup to the local subalgebra, and also that the same technique can be adapted to the global setting. As a particular case we prove that a plane polynomial curve has a deformation into a complete intersection monomial space curve.

The paper is organized as follows. In Section 2 we focus on the local case, namely the case of a subalgebra R of $\mathbb{K}[[x]]$. We introduce the notion of basis of R and we show how to construct such a basis. We also show that if $\text{o}(R)$ is a numerical semigroup, then every element of a reduced basis is a polynomial. In Section 3 we show how to construct a deformation from R to a toric ideal (or a formal toric variety) by using the technique of homogenization. In Section 4 we focus on the case when $R = \mathbb{K}[[f(x), g(x)]]$ and \mathbb{K} is an algebraically closed field of characteristic zero. The existence in this case of the theory of Newton-Puiseux allows us to precise the results of Sections 2 and 3. The difference with the procedure

The first author is partially supported by the project GDR CNRS 2945 and a GENIL-SSV 2014 grant.

The second author is supported by the projects MTM2014-55367-P, FQM-343, FQM-5849, and FEDER funds.

presented in Section 2 is that it does not rely in the computation of successive kernels. Then in Sections 5 and 6 we adapt the local results to the case of a subalgebra A of $\mathbb{K}[x]$. When $A = \mathbb{K}[f(x), g(x)]$ and \mathbb{K} is algebraically closed field of characteristic zero, a basis of A can be obtained by using the theory of approximate roots of the resultant of $X - f(x), Y - g(x)$, which is a polynomial with one place at infinity.

The procedures presented here have been implemented in **GAP** ([10]) and will be part of the forthcoming stable release of the package **numericalsgps** ([7]).

1.1. Some notation. We denote by $\langle A \rangle$ the monoid generated by A , $A \subseteq \mathbb{N}$, that is, the set $\{n_1x_1 + \dots + n_mx_m \mid m \in \mathbb{N}, n_i \in \mathbb{N}, x_i \in A \text{ for all } i \in \{1, \dots, m\}\}$.

Associated to each numerical semigroup S we can define a natural partial ordering \leq_S , where for two elements s and r in S we have $s \leq_S r$ if there exists $u \in S$ such that $r = s + u$. The set g_i of minimal elements in $S \setminus \{0\}$ with this ordering is called a *minimal set of generators* for S . The set of minimal generators is finite since for any $s \in S \setminus \{0\}$, we have $x \not\equiv y \pmod{s}$ if $x \neq y$ are minimal elements with respect to \leq_S . The cardinality of the minimal generating system is known as the *embedding dimension* of S .

2. SEMIGROUP OF A FORMAL SPACE CURVE

Let \mathbb{K} be a field. In this section we will consider rings R that are subalgebras of $\mathbb{K}[[x]]$ and such that, if we denote the integral closure of R in its quotient field by \bar{R} , then $\bar{R} = \mathbb{K}[[x]]$ and $\lambda_R(\bar{R}/R) < \infty$ where $\lambda_R(\cdot)$ is the length as R -module. Part of the results of this section are inspired in [15] and in [14]. An alternative procedure (implemented in Maple) is provided in [5]. The main difference with our approach is that we do not rely on the multiplicity sequence, and thus we do not need to perform blow-ups. Also we take intrinsic advantage in our implementation of the **GAP** package **numericalsgps** ([10, 7]).

Let $f = \sum_i c_i x^i \in \bar{R}^* = \bar{R} \setminus \{0\}$. Define $\text{supp}(f) = \{i, c_i \neq 0\}$. We call $\min \text{supp}(f)$ the *order* of f and we denote it by $\text{o}(f)$. We also set $M_o(f) = c_{\text{o}(f)} x^{\text{o}(f)}$. If $M_o(f) = x^{\text{o}(f)}$, then we shall say, by abuse of notation, that f is *monic*. We set $\text{o}(0) = +\infty$.

We denote by $\text{o}(R)$ the set of orders of elements in $R^* = R \setminus \{0\}$, that is, $\text{o}(R) = \{\text{o}(f) \mid f \in R^*\}$. We finally set $M_o(R) = \mathbb{K}[M_o(f) \mid f \in R^*]$.

Proposition 2.1. *Let f_1, f_2 be elements of \bar{R}^* and let $a = \min\{\text{o}(f_1), \text{o}(f_2)\}$.*

- (i) $a \leq \text{o}(f_1 + f_2)$.
- (ii) If $\text{o}(f_1) \neq \text{o}(f_2)$ then $a = \text{o}(f_1 + f_2)$.
- (iii) $\text{o}(f_1 f_2) = \text{o}(f_1) + \text{o}(f_2)$.

Proof. This follows easily from the definition of order. □

Proposition 2.2. [13, Lemma 3, p.486] *Let R_1 and R_2 be rings of our type such that $R_1 \subseteq R_2$ and $\text{o}(R_1) = \text{o}(R_2)$. Then $R_1 = R_2$.*

Proposition 2.3. [13, Proposition 1, p.488] *Let R be a ring of our type. Then $\lambda_R(\bar{R}/R) = |\mathbb{N} \setminus \text{o}(R)|$.*

The following two results appear in [15], and since this paper is very hard to find, we include the proofs for sake of completeness.

Proposition 2.4. [15] *Let R be a ring of our type. Then $\text{o}(R)$ is a numerical semigroup.*

Proof. Since R is a ring and by (iii) of Proposition 2.1, we have that $\text{o}(R)$ is a subsemigroup of \mathbb{N} . By $\lambda_R(\bar{R}/R) < \infty$ and Proposition 2.3, we have the proof. □

Proposition 2.5. [15] *Let R be a ring of our type. Then R contains every element $f \in \mathbb{K}[[x]]$ of order $\text{o}(f) \geq c(\text{o}(R))$.*

Proof. Use Proposition 2.2 with $R_1 = R$ and $R_2 = R + x^{c(\text{o}(R))} \mathbb{K}[[x]]$. □

This later result allows to work with polynomials instead of series.

Let f_1, \dots, f_s be in \bar{R}^* . Let $R = \mathbb{K}[[f_1, \dots, f_s]]$ be a subalgebra of $\mathbb{K}[[x]]$ as above, that is, the integral closure of R in its quotient field is $\bar{R} = \mathbb{K}[[x]]$ and $\lambda_R(\bar{R}/R) < \infty$.

Under these hypotheses on R , we have that $\mathfrak{o}(R)$ is a numerical semigroup (Proposition 2.4).

We say that the set $\{f_1, \dots, f_s\} \subset R^*$ is a *basis* of R if $\mathfrak{o}(R) = \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$. The set $\{f_1, \dots, f_s\}$ is a basis of R if and only if $M_{\mathfrak{o}}(R) = \mathbb{K}[M_{\mathfrak{o}}(f_1), \dots, M_{\mathfrak{o}}(f_s)]$.

Proposition 2.6. *Let the notations be as above. Given $f(x) \in \mathbb{K}[[x]]$, there exist $g(x) \in R$ and $r(x) \in \mathbb{K}[[x]]$ such that the following conditions hold.*

- (i) $f(x) = g(x) + r(x) = \sum_{\alpha} c_{\alpha} f_1^{\alpha_1} \dots f_s^{\alpha_s} + r(x)$.
- (ii) If $g(x) \neq 0$ (respectively $r(x) \neq 0$), then $\mathfrak{o}(g) \geq \mathfrak{o}(f)$ (respectively $\mathfrak{o}(r) \geq \mathfrak{o}(f)$).
- (iii) Either $r(x) = 0$ or $\text{supp}(r(x)) \subseteq \mathbb{N} \setminus \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$.

Proof. The assertion is clear if $f \in \mathbb{K}$. Suppose that $f \notin \mathbb{K}$ and let $f(x) = \sum_{i \geq p} c_i x^i$ with $p = \mathfrak{o}(f) \geq 0$.

- (1) If $p \notin \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$, then we set $g^1 = 0$, $r^1 = c_p x^p$ and $f^1 = f - c_p x^p$.
- (2) If $p \in \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$, then $c_p x^p = c_{\theta} M_0(f_1)^{\theta_1} \dots M_0(f_s)^{\theta_s}$. We set $g^1 = c_{\theta} f_1^{\theta_1} \dots f_s^{\theta_s}$, $r^1 = 0$ and $f^1 = f - g^1$.

In such a way that $f = f^1 + g^1 + r^1$, $g^1 \in R$, either $r^1 = 0$ or $\text{supp}(r^1) \subseteq \mathbb{N} \setminus \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$, and if $f^1 \neq 0$, then $\mathfrak{o}(f^1) > \mathfrak{o}(f) = p$. Then we restart with f^1 . We construct in this way sequences $(f^k)_{k \geq 1}, (g^k)_{k \geq 1}, (r^k)_{k \geq 1}$ such that for all $k \geq 1$, $f = f^k + \sum_{i=1}^k g^i + \sum_{i=1}^k r^i$, and $\mathfrak{o}(f) < \mathfrak{o}(f^1) < \dots < \mathfrak{o}(f^k)$, $\sum_{i=1}^k g^i \in R$, $\text{supp}(\sum_{i=1}^k r^i) \subseteq \mathbb{N} \setminus \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$ and for all $i < j \leq k$, if $g^i \neq 0 \neq g^j$ (respectively $r^i \neq 0 \neq r^j$), then $\mathfrak{o}(f) \leq \mathfrak{o}(g^i) < \mathfrak{o}(g^j)$ (respectively $\mathfrak{o}(f) \leq \mathfrak{o}(r^i) < \mathfrak{o}(r^j)$). Clearly $\lim_{k \rightarrow +\infty} f^k = 0$. Hence, if $g = \lim_{k \rightarrow +\infty} \sum_{i=1}^k g^i$ and $r = \lim_{k \rightarrow +\infty} \sum_{i=1}^k r^i$, then $f = g + r$ and g, r satisfy the conditions above. \square

We denote the series $r(x)$ of the proposition above by $R_{\mathfrak{o}}(f, \{f_1, \dots, f_s\})$. This series depend strongly on step (2) of the proof of Proposition 2.6. Let for example $f_1 = x^6, f_2 = x^4 + x^5, f_3 = x^2 + x^5$, and let $f = x^4$. We have $f = f_2 - x^5 = f_3^2 - f_1 f_2 - 2x^7 + x^{11}$. We shall see that $r(x)$ becomes unique if f_1, \dots, f_s is a basis of R (see Proposition 2.8).

Proposition 2.7. *The set $\{f_1, \dots, f_s\}$ is a basis of R if and only if $R_{\mathfrak{o}}(f, \{f_1, \dots, f_s\}) = 0$ for all $f \in R$.*

Proof. Suppose that $\{f_1, \dots, f_s\}$ is a basis of R and let $f \in R$. Let $r(x) = R_{\mathfrak{o}}(f, \{f_1, \dots, f_s\})$. Then $r(x) \in R$. If $r \neq 0$, then $\mathfrak{o}(r) \in \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$, which is a contradiction.

Conversely, suppose that $\{f_1, \dots, f_s\}$ is not a basis of R and let $0 \neq f \in R$ such that $\mathfrak{o}(f) \notin \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$. We have $R_{\mathfrak{o}}(f, \{f_1, \dots, f_s\}) \neq 0$, which contradicts the hypothesis. \square

Proposition 2.8. *If $\{f_1, \dots, f_s\}$ is a basis of R then for all $f \in \mathbb{K}[[x]]$, $R_{\mathfrak{o}}(f, \{f_1, \dots, f_s\})$ is unique.*

Proof. Suppose that $f = g_1(x) + r_1(x) = g_2(x) + r_2(x)$ where $g_1(x), g_2(x), r_1(x), r_2(x)$ satisfy conditions (i), (ii), (iii) of Proposition 2.6. We have $r_1(x) - r_2(x) = g_2(x) - g_1(x) \in R$. If $r_1(x) - r_2(x) \neq 0$ then $\mathfrak{o}(r_1(x) - r_2(x)) \notin \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$. This contradicts the hypothesis. \square

Let, as above, $R = \mathbb{K}[[f_1, \dots, f_s]]$. We shall suppose that f_i is monic for all $1 \leq i \leq s$. Define

$$\phi : \mathbb{K}[X_1, \dots, X_s] \longrightarrow \mathbb{K}[x], \quad \phi(X_i) = M_{\mathfrak{o}}(f_i) \text{ for all } i \in \{1, \dots, s\}.$$

Let $\{F_1, \dots, F_r\}$ be a generating system of the kernel of ϕ . We can choose all of them to be binomials. If $F_i = X_1^{\alpha_1^i} \dots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \dots X_s^{\beta_s^i}$, we set $S_i = f_1^{\alpha_1^i} \dots f_s^{\alpha_s^i} - f_1^{\beta_1^i} \dots f_s^{\beta_s^i}$. Note that if $p = \sum_{k=1}^s \alpha_k^i \mathfrak{o}(f_k) = \sum_{k=1}^s \beta_k^i \mathfrak{o}(f_k)$, then $\mathfrak{o}(S_i) > p$.

Theorem 2.9. *The system $\{f_1, \dots, f_s\}$ is a basis of R if and only if $R_{\mathfrak{o}}(S_i, \{f_1, \dots, f_s\}) = 0$ for all $i \in \{1, \dots, r\}$.*

Proof. Suppose that $\{f_1, \dots, f_s\}$ is a basis of R . Since $S_i \in R$ for all $i \in \{1, \dots, r\}$, then, by Proposition 2.7, $R_{\mathfrak{o}}(S_i, \{f_1, \dots, f_s\}) = 0$.

For the sufficiency assume to the contrary that $\{f_1, \dots, f_s\}$ is not a basis of R . Then there exists $f \in R$ such that $\mathfrak{o}(f) \notin \langle \mathfrak{o}(f_1), \dots, \mathfrak{o}(f_s) \rangle$. Write

$$f = \sum_{\theta} c_{\theta} f_1^{\theta_1} \dots f_s^{\theta_s}.$$

For all $\underline{\theta}$, if $c_{\underline{\theta}} \neq 0$, we set $p_{\underline{\theta}} = \sum_{i=1}^s \theta_i o(f_i) = o(f_1^{\theta_1} \cdots f_s^{\theta_s})$. Let $p = \min\{p_{\underline{\theta}} \mid c_{\underline{\theta}} \neq 0\}$ and let $\{\underline{\theta}^1, \dots, \underline{\theta}^l\}$ be such that $p = o(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i})$ for all $i \in \{1, \dots, l\}$ (such a set is clearly finite). Also $p \leq o(f) < \infty$.

If $\sum_{i=1}^l c_{\underline{\theta}^i} M_o(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}) \neq 0$, then $p = o(f) \in \langle o(f_1), \dots, o(f_s) \rangle$. But this is impossible. Hence, $\sum_{i=1}^l c_{\underline{\theta}^i} M_o(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}) = 0$, and then $\sum_{i=1}^l c_{\underline{\theta}^i} X_1^{\theta_1^i} \cdots X_s^{\theta_s^i} \in \ker(\phi)$. Hence

$$\sum_{i=1}^l c_{\underline{\theta}^i} X_1^{\theta_1^i} \cdots X_s^{\theta_s^i} = \sum_{k=1}^r \lambda_k F_k$$

with $\lambda_k \in \mathbb{K}[X_1, \dots, X_s]$ for all $k \in \{1, \dots, r\}$ (recall that F_1, \dots, F_r are binomials generating $\ker(\phi)$). This implies that

$$\sum_{i=1}^l c_{\underline{\theta}^i} f_1^{\theta_1^i} \cdots f_s^{\theta_s^i} = \sum_{k=1}^r \lambda_k(f_1, \dots, f_s) S_k.$$

From the hypothesis $R_o(S_k, \{f_1, \dots, f_s\}) = 0$. Hence there is an expression of S_k of the form $S_k = \sum_{\underline{\beta}^k} c_{\underline{\beta}^k} f_1^{\beta_1^k} \cdots f_s^{\beta_s^k}$ with $o(f_1^{\beta_1^k} \cdots f_s^{\beta_s^k}) \geq o(S_k)$.

So by replacing $\sum_{i=1}^l c_{\underline{\theta}^i} f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}$ with $\sum_{k=1}^r \lambda_k(f_1, \dots, f_s) \sum_{\underline{\beta}^k} c_{\underline{\beta}^k} f_1^{\beta_1^k} \cdots f_s^{\beta_s^k}$ in the expression of f , we can rewrite f as $f = \sum_{\underline{\theta}'} c_{\underline{\theta}'} f_1^{\theta_1'} \cdots f_s^{\theta_s'}$ with $\min\{o(f_1^{\theta_1'} \cdots f_s^{\theta_s'}) \mid c_{\underline{\theta}'} \neq 0\} > p$.

Since $o(f) < +\infty$, this process will stop, yielding a contradiction. \square

Algorithm 2.10. Let the notations be as above.

1. If $R_o(S_k, \{f_1, \dots, f_s\}) = 0$ for all $k \in \{1, \dots, r\}$, then $\{f_1, \dots, f_s\}$ is a basis of R .
2. If $r(x) = R_o(S_k, \{f_1, \dots, f_s\}) \neq 0$ for some $k \in \{1, \dots, r\}$, and if $M_o(r(x)) = ax^q$, then we set $f_{s+1} = \frac{1}{a}r(x)$, and we restart with $\{f_1, \dots, f_{s+1}\}$. Note that in this case,

$$\langle o(f_1), \dots, o(f_s) \rangle \subsetneq \langle o(f_1), \dots, o(f_s), o(f_{s+1}) \rangle \subseteq o(R).$$

This process will stop, giving a basis of R , because the complement of $o(R)$ in \mathbb{N} is finite.

Observe that $r(x)$ is not in general a polynomial. So we must use a trick to compute it, or at least the relevant part of it. This is accomplished by using Proposition 2.5. If in the current step of the algorithm $\langle o(f_1), \dots, o(f_s) \rangle$ is a numerical semigroup, then we compute its conductor, say c . Then $c \geq c(o(R))$. To compute $R_o(f, \{f_1, \dots, f_s\})$ we do the following. Let $p = o(f)$.

1. If $p \geq c$, then return 0. We implicitly assume that x^a is in our generating set for $a \in c + \mathbb{N}$ (though we do not store them).
2. If $p \in \langle o(f_1), \dots, o(f_s) \rangle$, then $M_o(f) = \sum_{\underline{\theta}} c_{\underline{\theta}} M_o(f_1)^{\theta_1} \cdots M_o(f_s)^{\theta_s}$. Set $f = f - \sum_{\underline{\theta}} c_{\underline{\theta}} f_1^{\theta_1} \cdots f_s^{\theta_s}$, and call recursively $R_o(f, \{f_1, \dots, f_s\})$ (the process will stop because the order of the new f is larger, and eventually will become bigger than c after a finite number of steps).
3. If $p \notin \langle o(f_1), \dots, o(f_s) \rangle$, then return f .

If $\langle o(f_1), \dots, o(f_s) \rangle$ is not a numerical semigroup, let d be its greatest common divisor. Set $c = dc(\langle o(f_1), \dots, o(f_s) \rangle / d)$. In this case we proceed as follows.

1. If $p \geq c$, then return f . We cannot ensure here that f will be reduced to zero, so we add it just in case.
2. If $p \in \langle o(f_1), \dots, o(f_s) \rangle$, then $M_o(f) = \sum_{\underline{\theta}} c_{\underline{\theta}} M_o(f_1)^{\theta_1} \cdots M_o(f_s)^{\theta_s}$. Set $f = f - \sum_{\underline{\theta}} c_{\underline{\theta}} f_1^{\theta_1} \cdots f_s^{\theta_s}$, and call recursively $R_o(f, \{f_1, \dots, f_s\})$.
3. If $p \notin \langle o(f_1), \dots, o(f_s) \rangle$, then return f . One might check first if d does not divide p , because in this case for sure $p \notin \langle o(f_1), \dots, o(f_s) \rangle$.

Observe that by adding the conditions $p \geq c$, we are avoiding entering in an eventual infinite loop.

Suppose that $\{f_1, \dots, f_s\}$ is a basis of R . Also suppose that for all $i \in \{1, \dots, s\}$, f_i is monic. We say that $\{f_1, \dots, f_s\}$ is a *minimal basis* of R if $o(f_1), \dots, o(f_s)$ generate minimally the semigroup $o(R)$. We say that $\{f_1, \dots, f_s\}$ is a *reduced basis* of R if $\text{supp}(f_i(x) - M_0(f_i)) \subseteq \mathbb{N} \setminus o(R)$. Let $i \in \{1, \dots, s\}$. If $o(f_i) \in \langle o(f_1), \dots, o(f_{i-1}), o(f_{i+1}), \dots, o(f_s) \rangle$, then $\{f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_s\}$ is also a basis of R . Furthermore,

by applying the division process of Proposition 2.6 to $f_i - M_o(f_i)$, we can always construct a reduced basis of R .

Corollary 2.11. *The algebra R has a unique minimal reduced basis.*

Proof. Let $\{f_1, \dots, f_s\}$ and $\{g_1, \dots, g_{s'}\}$ be two minimal reduced bases of R . Hence s is the embedding dimension of $\mathfrak{o}(R)$, and the same holds for s' ; whence they are equal. Let $i = 1$. There exists j_1 such that $\mathfrak{o}(f_1) = \mathfrak{o}(g_{j_1})$, because minimal generating systems of numerical semigroups are unique. If $f_1 - g_{j_1} \neq 0$, then $\mathfrak{o}(f_1 - g_{j_1}) \notin \mathfrak{o}(R)$ (the basis is reduced), which is a contradiction because $f_1 - g_{j_1} \in R$. The same argument shows that $\{f_1, \dots, f_s\} = \{g_1, \dots, g_{s'}\}$ \square

Remark 2.12. Let $R = \mathbb{K}[[f_1, \dots, f_s]]$ and assume that f_i is monic for all $1 \leq i \leq s$. Also assume that $\mathfrak{o}(f_1) \leq \mathfrak{o}(f_2) \leq \dots \leq \mathfrak{o}(f_s)$. Set $n = \mathfrak{o}(f_1)$ and let $f_1 = x^n + \sum_{i>n} c_i^1 x^i$. By an analytic change of variables, we may assume that $f_1 = x^n$, hence, up to an analytic isomorphism, we may assume that $R = \mathbb{K}[[x^n, f_2, \dots, f_s]]$. In particular, we may assume that R has a minimal reduced basis of the form $x^n, g_2(x), \dots, g_{s'}(x)$.

Example 2.13. Let $R = \mathbb{K}[[x^4 + x^5, x^6, x^{15} + x^{16} + \sum_{n \geq 20} x^n]]$, with \mathbb{K} a field of characteristic zero. Then R is a one-dimensional ring. Since the conductor of $\langle 4, 6, 15 \rangle$ is 18, we have that $\lambda_R(\mathbb{K}[[X]]/R) < \infty$ and we know by Proposition 2.5 that $R = \mathbb{K}[[x^4 + x^5, x^6, x^{15} + x^{16}]]$. Let us denote $x^4 + x^5$ by f_1 , x^6 by f_2 and $x^{15} + x^{16}$ by f_3 . The kernel of $\phi : \mathbb{K}[X_1, X_2, X_3] \rightarrow \mathbb{K}[x]$, $\phi(X_1) = x^4$, $\phi(X_2) = x^6$ and $\phi(X_3) = x^{15}$ is generated by $X_1^3 - X_2^2, X_3^2 - X_2^5$, hence we get $S_1 = x^{13} + x^{14} + \frac{1}{3}x^{15}$ and $S_2 = x^{31} + \frac{1}{2}x^{32}$. As $13 \notin \langle 4, 6, 15 \rangle$, we add it as $f_4 = S_1$. We do not care about S_2 , because the conductor of $\langle 4, 6, 15 \rangle$ is 18.

Now, the conductor of $\langle 4, 6, 13, 15 \rangle$ is 12. If we compute a system of generators of the kernel of $\phi : \mathbb{K}[X_1, X_2, X_3, X_4] \rightarrow \mathbb{K}[x]$, $\phi(X_1) = x^4$, $\phi(X_2) = x^6$, $\phi(X_3) = x^{15}$ and $\phi(X_4) = x^{13}$, then all the elements S_i have orders greater than 12, and so the algorithm ends. We conclude that $\mathfrak{o}(R) = \langle 4, 6, 13, 15 \rangle$.

We have implemented this algorithm in the **numericalsgps** ([7]) **GAP** ([10]) package. Next we illustrate how to compute this semigroup with the functions we have implemented (that will be available in the next release of the package).

```
gap> x:=X(Rationals,"x");;
gap> l:=[x^4+x^5,x^6,x^15+x^16];;
gap> s:=SemigroupOfValuesOfCurve_Local(l);;
gap> MinimalGeneratingSystem(s);
[ 4, 6, 13, 15 ]
gap> SemigroupOfValuesOfCurve_Local(l,13);
x^13
```

Remark 2.14. It is known (cf. [3, Section II.1]) that there exist relations between algebraic characteristics and invariants of the semigroup $\mathfrak{o}(R)$ and the ring R . Hence, in the Example 2.13, from $\mathfrak{o}(R) = \langle 4, 6, 13, 15 \rangle = \{0, 4, 6, 8, 10, 12, \dots\}$, we deduce that the conductor of $\mathfrak{o}(R)$ is 12. The conductor of R in \bar{R} is precisely $(x^{c(\mathfrak{o}(R))})$ ([3]). We have that $\lambda_R(\bar{R}/R) = |[0, c(\mathfrak{o}(R)) - 1] \cap (\mathbb{N} \setminus \mathfrak{o}(R))| = 7$ counts the number of gaps of $\mathfrak{o}(R)$ ([13, Proposition 1]). The integer $\lambda_R(\bar{R}/R)$ is the degree of singularity of R , and this is why the genus of $\mathfrak{o}(R)$ is called by some authors the degree of singularity of the semigroup (see [3, 13]). In the setting of Weierstrass numerical semigroups the genus coincides with the geometrical genus of the curve used to define the semigroup ([6]).

The number of sporadic elements of $\mathfrak{o}(R)$ is $\lambda_R(R/(R : \bar{R})) = |[0, c(\mathfrak{o}(R)) - 1] \cap \mathfrak{o}(R)| = 5$.

The ring R is Cohen-Macaulay and its type is less than or equal to $\#T(\mathfrak{o}(R)) = 3$, where for a numerical semigroup Γ , $T(\Gamma) = \{x \in \mathbb{Z} \setminus \Gamma \mid x + \Gamma^* \subseteq \Gamma\}$ ([3, Proposition II.1.16]). According also to [3, Proposition II.1.16], equality holds if and only if $\mathfrak{o}(R : \mathfrak{m}) = T(\mathfrak{o}(R))$. However $T(\mathfrak{o}(R)) = \{2, 9, 11\}$ and $2 \notin \mathfrak{o}(R : \mathfrak{m})$. So in our example we get an strict inequality.

Example 2.15. Let $R = \mathbb{K}[[x^4, x^6 + x^7, x^{13} + a_{14}x^{14} + a_{15}x^{15} + \dots]]$ with \mathbb{K} a field. Using the same argument as in the Example 2.13, we find that if $\text{char } \mathbb{K} \neq 2$, we have that if $a_{15} - a_{14} + 1/2 = 0$, then $\{x^4, x^6 + x^7, x^{13}\}$ is the reduced basis of R . Furthermore, since $\langle 4, 6, 13 \rangle$ is a symmetric numerical semigroup (the number of nonnegative integers not in the semigroup equals the conductor divided by

two), then, by [12], R is Gorenstein. Finally $\lambda_R(\bar{R}/R) = 8$. Otherwise if $a_{15} - a_{14} + 1/2 \neq 0$, then $\{x^4, x^6 + x^7, x^{13}, x^{15}\}$ is the reduced basis of R with R a non Gorenstein ring. Furthermore $\lambda_R(\bar{R}/R) = 7$.

Otherwise, if $\text{char } \mathbb{K} = 2$, then the reduced basis of R is $\{x^4, x^6 + x^7, x^{13}, x^{15}\}$ and R is not a Gorenstein ring. Here, $\lambda_R(\bar{R}/R) = 7$.

Example 2.16. Let $R = \mathbb{K}[[x^8, x^{12} + x^{14} + x^{15}]]$, with \mathbb{K} a field of characteristic zero. Using the same argument as in the Example 2.13, we have that

$$\{x^8, x^{12} + x^{14} + x^{15}, x^{26} + x^{27} + x^{29} - \frac{1}{2}x^{31}, \\ x^{53} + \frac{1}{2}x^{55} - \frac{1}{2}x^{57} - \frac{1}{8}x^{63} + \frac{25}{8}x^{67} - \frac{95}{32}x^{71} - \frac{15}{16}x^{75} - \frac{135}{32}x^{83}\}$$

is the reduced basis of the Gorenstein ring R . Furthermore, we have $\lambda_R(\bar{R}/R) = 42$.

```
gap> l:=[x^8,x^12+x^14+x^15];;
gap> SemigroupOfValuesOfCurve_Local(1,"basis");
[ x^8, x^15+x^14+x^12, -1/2*x^31+x^29+x^27+x^26,
-135/32*x^83-15/16*x^75-95/32*x^71+25/8*x^67-1/8*x^63-1/2*x^57+1/2*x^55+x^53 ]
```

Example 2.17. The following battery of examples was provided by Lance Bryant as a test for our algorithm.

```
gap> l:=[ [ x^6,x^8+x^9,x^19], [x^7,x^9+x^10,x^19,x^31], [x^7,x^21+x^28+x^33],
[x^4,x^6+x^7,x^13], [x^6,x^8+x^11,x^10+2*x^13,x^21], [x^5,-x^18-x^21,-x^23,-x^26],
[x^5,-x^18-x^21,-x^26], [x^5,-x^18-x^21,x^23-x^26], [x^6,x^9+x^10,x^19],
[x^7,x^9+x^10,x^19], [x^8,x^9+x^10,x^19], [x^7,x^9+x^10,x^17,x^19] ];;
gap> List(1, i->MinimalGeneratingSystem(SemigroupOfValuesOfCurve_Local(i)));
[ [ 6, 8, 19, 29 ], [ 7, 9, 19, 29, 31 ], [ 7, 33 ], [ 4, 6, 13, 15 ],
[ 6, 8, 10, 21, 23, 25 ], [ 5, 18, 26, 39, 47 ], [ 5, 18, 26, 39, 47 ],
[ 5, 18, 26, 39, 47 ], [ 6, 9, 19, 20 ], [ 7, 9, 19, 29 ], [ 8, 9, 19, 30 ],
[ 7, 9, 17, 19, 29 ] ]
```

Remark 2.18. We do not know a priori if $\bar{R} \neq \mathbb{K}[[x]]$ and we do not have a general procedure to check it. If the algorithm is called with such an R , it will eventually not stop.

3. DEFORMATION TO A TORIC IDEAL

Let the notations be as in Section 2. Given $f(x) = \sum_{i \geq p} c_i x^i \in \mathbb{K}[[x]]$, we set $H_f(u, x) = \sum_{i \geq p} c_i u^{i-p} x^i$. In particular, if we consider the linear form $L : \mathbb{N}^2 \rightarrow \mathbb{N}, L(a, b) = b - a$, then H_f is L -homogeneous of order p , that is, $L(i - p, i) = p$ for all $i \in \text{supp}(f)$. We set $H_R = \mathbb{K}[[u, H_f \mid f \in R]]$. With these notations we have the following.

Proposition 3.1. *The set $\{f_1, \dots, f_s\}$ is a basis of R if and only if $H_R = \mathbb{K}[[u, H_{f_1}, \dots, H_{f_s}]]$.*

Proof. Note first that if $H_g \in H_R$ for some $g \in \mathbb{K}[[x]]$, then $g \in R$. Suppose that $\{f_1, \dots, f_s\}$ is a basis of R and let $f(x) \in R$. Write $H_f(u, x) = \sum_{i \geq p} c_i u^{i-p} x^i$. We have $M_o(f) = c_p x^p = c_p \prod_{i=1}^s M_o(f_i)^{p_i^k}$, hence

$$H_f - c_p \prod_{i=1}^s H_{f_i}^{p_i^k} = u^q H_{f^1}$$

with $f^1 \in R$ and either $f^1 = 0$, or $\text{o}(f^1) > p$. In the second case we restart with f^1 . A similar argument as in Proposition 2.6 proves our assertion.

Conversely, suppose that $H_R = \mathbb{K}[[u, H_{f_1}, \dots, H_{f_s}]]$ and let $f \in R$. Let $P(X_0, X_1, \dots, X_s) \in \mathbb{K}[[X_0, X_1, \dots, X_s]]$ such that $H_f = P(u, H_{f_1}, \dots, H_{f_s})$. Setting $u = 0$, we get that $M_o(f) = P(M_o(f_1), \dots, M_o(f_s)) \in \mathbb{K}[[M_o(f_1), \dots, M_o(f_s)]]$. Hence $M_o(f) \in \mathbb{K}[[M_o(f_1), \dots, M_o(f_s)]]$. \square

Suppose that $\{f_1, \dots, f_s\}$ is a basis of R . Then $T = \mathbb{K}[[u]][H_{f_1}, \dots, H_{f_s}]$ is a $\mathbb{K}[[u]]$ -module. When $u = 1$ (respectively $u = 0$), we get $T|_{u=1} = R$ (respectively $T|_{u=0} = \mathbb{K}[[M(f_1), \dots, M(f_s)]]$). Hence we get a deformation from R to $\mathbb{K}[[M_o(f_1), \dots, M_o(f_s)]]$. More precisely let

$$\psi : \mathbb{K}[[X_1, \dots, X_s]] \longrightarrow R = \mathbb{K}[[f_1, \dots, f_s]]$$

and

$$H_\psi : \mathbb{K}[[u]][X_1, \dots, X_s] \longrightarrow T = \mathbb{K}[[u]][H_{f_1}, \dots, H_{f_s}]$$

be the morphisms of rings such that $H_\psi(u) = u$, $\psi(X_i) = f_i$ and $H_\psi(X_i) = H_{f_i}$ for all $i \in \{1, \dots, s\}$. Let, as in Section 2,

$$S_i = f_1^{\alpha_1^i} \dots f_s^{\alpha_s^i} - f_1^{\beta_1^i} \dots f_s^{\beta_s^i} = \sum_{\underline{\theta}^i} c_{\underline{\theta}^i}^i f_1^{\theta_1^i} \dots f_s^{\theta_s^i}, 1 \leq i \leq r$$

with $o(f_1^{\theta_1^i} \dots f_s^{\theta_s^i}) = D_{\underline{\theta}^i}^i > \sum_{k=1}^s \alpha_k^i o(f_k) = \sum_{k=1}^s \beta_k^i o(f_k) = p_i$. Let I (respectively J) be the ideal generated by $(G_i = X_1^{\alpha_1^i} \dots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \dots X_s^{\beta_s^i} - \sum_{\underline{\theta}^i} c_{\underline{\theta}^i}^i X_1^{\theta_1^i} \dots X_s^{\theta_s^i})_{1 \leq i \leq r}$ (respectively $(H_i = X_1^{\alpha_1^i} \dots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \dots X_s^{\beta_s^i} - \sum_{\underline{\theta}^i} u^{D_{\underline{\theta}^i}^i - p_i} c_{\underline{\theta}^i}^i X_1^{\theta_1^i} \dots X_s^{\theta_s^i})_{1 \leq i \leq r}$) in $\mathbb{K}[[X_1, \dots, X_s]]$ (respectively $\mathbb{K}[[u]][X_1, \dots, X_s]$).

We shall consider on \mathbb{N}^s (respectively, \mathbb{N}^{s+1}) the linear form

$$O(\theta_1, \dots, \theta_s) = \sum_{i=1}^s \theta_i o(f_i)$$

(respectively $O_h(\theta_0, \theta_1, \dots, \theta_s) = -\theta_0 + \sum_{i=1}^s \theta_i o(f_i)$).

Given a monomial $X_1^{\theta_1} \dots X_s^{\theta_s}$ (respectively $u^{\theta_0} X_1^{\theta_1} \dots X_s^{\theta_s}$), we set $O(X_1^{\theta_1} \dots X_s^{\theta_s}) = O(\theta_1, \dots, \theta_s)$ (respectively $O_h(u^{\theta_0} X_1^{\theta_1} \dots X_s^{\theta_s}) = O_h(\theta_0, \theta_1, \dots, \theta_s)$).

For $G = \sum_{\underline{\theta}} c_{\underline{\theta}} X_1^{\theta_1} \dots X_s^{\theta_s}$ (respectively $H = \sum_{\underline{\theta}} c_{\underline{\theta}} u^{\theta_0} X_1^{\theta_1} \dots X_s^{\theta_s}$), we say that G (respectively H) is O -homogeneous of order a (respectively O_h -homogeneous of order b) if $O(\theta_1, \dots, \theta_s) = a$ (respectively $O_h(\theta_0, \theta_1, \dots, \theta_s) = b$) for all $(\theta_1, \dots, \theta_s)$ (respectively $(\theta_0, \theta_1, \dots, \theta_s)$) such that $c_{\underline{\theta}} \neq 0$. More generally let $G = \sum_{k \geq 0} G_{p_k}$ where $p_0 < p_1 < \dots$ and G_{p_k} is O -homogeneous of order p_k . We set $O(G) = p_0$. We also set $\text{in}(G) = G_{p_0}$ and we call it the *initial form* of G .

We finally set $O(0) = +\infty$, and we recall that $O(G) = +\infty$ if and only if $G = 0$.

Lemma 3.2. *With the standing notations and hypothesis, the kernel of ψ is generated by I .*

Proof. Let, as in Section 2, F_1, \dots, F_r be a generating system of the kernel of the morphism

$$\phi : \mathbb{K}[[X_1, \dots, X_s]] \longrightarrow \mathbb{K}[[x]], \quad \phi(X_i) = M_o(f_i)$$

for all $i \in \{1, \dots, s\}$. In particular F_i is O -homogeneous of order $o(f_i)$ for all $i \in \{1, \dots, s\}$, and $\mathbb{K}[[X_1, \dots, X_s]]/(F_1, \dots, F_r) \simeq \mathbb{K}[[M_o(f_1), \dots, M_o(f_s)]]$.

For all $i \in \{1, \dots, r\}$, $\psi(G_i) = 0$. Hence $I \subseteq \ker(\psi)$.

For the other inclusion, let $G = \sum_{\underline{\theta}} c_{\underline{\theta}} X_1^{\theta_1} \dots X_s^{\theta_s} \in \ker(\psi)$. Write $G = \sum_{k \geq 0} c_{\theta^k} X_1^{\theta_1^k} \dots X_s^{\theta_s^k}$ where $O(\theta_1^0, \dots, \theta_s^0) \leq O(\theta_1^1, \dots, \theta_s^1) \leq \dots$. Since $\psi(G) = 0$, we have that

$$\sum_{k \geq 0} c_{\theta^k} f_1^{\theta_1^k} \dots f_s^{\theta_s^k} = 0.$$

In particular $\sum_{k, O(\theta^k) = O(\theta^0)} c_{\theta^k} M_o(f_1)^{\theta_1^k} \dots M_o(f_s)^{\theta_s^k} = 0$, and consequently $\sum_{k, O(\theta^k) = O(\theta^0)} c_{\theta^k} X_1^{\theta_1^k} \dots X_s^{\theta_s^k} \in \ker(\phi)$. This implies that

$$\sum_{k, O(\theta^k) = O(\theta^0)} c_{\theta^k} X_1^{\theta_1^k} \dots X_s^{\theta_s^k} = \sum_{i=1}^r \lambda_i^0 F_i$$

for some $\lambda_i^0 \in \mathbb{K}[[X_1, \dots, X_s]]$, $i \in \{1, \dots, r\}$, with λ_i^0 is O -homogeneous of order $O(G) - O(F_i)$. Hence

$$\sum_{k, O(\theta^k) = O(\theta^0)} c_{\theta^k} f_1^{\theta_1^k} \dots f_s^{\theta_s^k} = \sum_{i=1}^r \lambda_i^0(f_1, \dots, f_s) S_i.$$

Let $G^1 = G - \sum_{i=1}^r \lambda_i^0 G_i$. We have $G^1 \in \ker(\psi)$. If $G^1 \neq 0$, then $O(G) < O(G^1)$. Then we restart with G^1 . We construct in the same way G^2 , and $\lambda_1^1, \dots, \lambda_r^1$ such that $G^1 = G^2 + \sum_{j=1}^r \lambda_j^1 G_j$ with $O(G) < O(G^1) < O(G^2)$, λ_i^1 O -homogeneous and $O(\lambda_i^0) < O(\lambda_i^1)$ for all $i \in \{1, \dots, r\}$. If we continue in this way, we get that for all $k \geq 0$,

$$G = G^{k+1} + \sum_{i=1}^r (\lambda_i^0 + \lambda_i^1 + \dots + \lambda_i^k) G_i,$$

with $O(G) < O(G^1) < \dots < O(G^{k+1})$, λ_i^j O -homogeneous, and $O(\lambda_i^0) < O(\lambda_i^1) < \dots < O(\lambda_i^k)$ for all $i \in \{1, \dots, r\}$ and for all $j \in \{1, \dots, k\}$. If $G^k = 0$ for some k , then we are done. Otherwise, let $\lambda_i = \sum_{k=0}^{\infty} \lambda_i^k$, and let $\bar{G} = \lim_{k \rightarrow \infty} G^k$. We have $\bar{G} = 0$ and $G = \sum_{i=1}^r \lambda_i G_i$. This proves our assertion. \square

Let the notations be as above. Let $G = \sum_{\theta} c_{\theta} X_1^{\theta_1} \dots X_s^{\theta_s} \in \mathbb{K}[[X_1, \dots, X_s]]$ and write $G = \sum_{i \geq 0} G_{p_i}$ with $p_0 < p_1 < \dots$ and G_{p_i} O -homogeneous. We set $H_G = \sum_{i \geq 0} u^{p_i - p_0} G_{p_i}$, in such a way that H_G is O_h -homogeneous of order p_0 . Given an ideal S of $\mathbb{K}[[X_1, \dots, X_s]]$, we set $\text{in}(S) = (\text{in}(G) \mid G \in S \setminus \{0\})$. We also denote by $H_S = (H_G \mid G \in S \setminus \{0\})\mathbb{K}[[u, X_1, \dots, X_s]]$. With these notations we have $\text{in}(S_i) = F_i$ and $H_{G_i} = H_i$ for all $i \in \{1, \dots, r\}$.

Lemma 3.3. *Let the notations be as above. We have $\text{in}(I) = (F_1, \dots, F_r)$, and $H_I = (H_1, \dots, H_r) = J$.*

Proof. The first assertion follows from the proof of Lemma 3.2. To prove the second assertion, let $H \in H_I$ and assume that H is O_h -homogeneous. We have $G = H(1, X_1, \dots, X_s) \in I$. Furthermore, $H = u^e H_G$ for some $e \geq 0$. Write $H_G = \text{in}(G) + H^1$ where $H^1(0, X_1, \dots, X_s) = 0$. We have $\text{in}(G) = \sum_{i=1}^r \lambda_i F_i$ where λ_i is O -homogeneous of order $p_0 - O(F_i)$. Let $H_{G^1} = H_G - \sum_{i=1}^r \lambda_i H_{G_i} = H_G - \sum_{i=1}^r \lambda_i H_i$. Then $H_{G^1} \in H_I$ is O_h -homogeneous and $O_h(H_G) < O_h(H_{G^1})$. Now we restart with H_{G^1} . We prove in this way that $H \in (H_1, \dots, H_r)$. \square

Let $H = \sum_{\theta} c_{\theta} u^{\theta} X_1^{\theta_1} \dots X_s^{\theta_s} \in \ker(H_{\psi})$. Write $H = \sum_k H^k$, where H^k is O_h -homogeneous. For all k , we have $H_{\psi}(H^k) = 0$. Setting $G_k = H^k(1, X_1, \dots, X_s)$, we have $\psi(G_k) = 0$. This implies that $G_k \in I$. Hence $H_{G_k} \in (H_1, \dots, H_r)$ by Lemma 3.3. But $H^k = u^{e_k} H_{G_k}$ for some $e_k \in \mathbb{N}$. Consequently $H^k \in (H_1, \dots, H_r)$. Finally $H \in (H_1, \dots, H_r)$, which proves that $\ker(H_{\psi}) \subseteq J$. As the inclusion $J \subseteq \ker(H_{\psi})$ is obvious, we conclude that $J = \ker(H_{\psi})$.

Now the morphism

$$\mathbb{K}[[u]] \longrightarrow \mathbb{K}[[u]][[X_1, \dots, X_s]]/J$$

is flat because u is not a zero divisor. Hence we get a family of formal space curves parametrized by u that gives us a deformation from $\mathbb{K}[[X_1, \dots, X_r]]/I$ to $\mathbb{K}[[X_1, \dots, X_r]]/(F_1, \dots, F_r)$.

In particular we get the following.

Theorem 3.4. *Every formal space curve of \mathbb{K}^l , parametrized by $Y_1 = g_1(x), \dots, Y_l = g_l(x)$ has a deformation into a formal monomial curve of \mathbb{K}^r for some positive integer r .*

4. BASIS OF $\mathbb{K}[[f(x), g(x)]]$

In this section we study the particular case of a subalgebra R of $\mathbb{K}[[x]]$ generated by two elements, and see that a different approach can be considered to study $\mathfrak{o}(R)$, with some interesting applications.

Let $f(x) = \sum_{i \geq n} a_i x^i$ and $g(x) = \sum_{j \geq m} b_j x^j$ be two elements of $\mathbb{K}[[x]]$ and suppose, without loss of generality, that the following conditions hold:

- (1) $a_n = b_m = 1$,
- (2) $n \leq m$,
- (3) the greatest common divisor of $\text{supp}(f(x)) \cup \text{supp}(g(x))$ is equal to 1 (in particular for all $d > 1$, $f(x), g(x) \notin \mathbb{K}[[x^d]]$).

Let the notations be as in Section 2, in particular $R = \mathbb{K}[[f, g]]$. By the analytic change of variables $f(x) = \tilde{x}^n$, we may assume that $R = \mathbb{K}[[x^n, g(x)]]$. Let $F(X, Y)$ be the x -resultant of $X - x^n, Y - g(x)$, that is, $F(X, Y)$ is the generator of the kernel of the map $\rho : \mathbb{K}[[X, Y]] \longrightarrow \mathbb{K}[[x]]$, $\rho(X) = x^n$ and $\rho(Y) = g(x)$.

Since $\mathbb{K}[[f, g]] = \mathbb{K}[[f, g - f^k]]$ for all $k \geq 1$, then we shall assume that $n < m$ and also that n does not divide m . Given a nonzero element $G(X, Y) \notin (F(X, Y))\mathbb{K}[[X, Y]]$, we set $\text{int}(F, G) = \text{o}(G(f(x), g(x)))$. Condition (3) implies that the set of $\text{int}(F, G), G(X, Y) \notin (F(X, Y))\mathbb{K}[[X, Y]]$, is a numerical semigroup. We denote it by $\Gamma(F)$. We have the following.

Proposition 4.1. $\text{o}(R) = \Gamma(F)$.

Proof. We have $a \in \Gamma(F)$ if and only if $a = \text{o}(G(f(x), g(x)))$ for some $G(X, Y) \in \mathbb{K}[[X, Y]]$ if and only if $a \in \text{o}(R)$. \square

Suppose that \mathbb{K} is algebraically closed with characteristic zero, and let $d_1 = n$, $m_1 = \inf\{i \in \text{supp}(g) \mid d_1 \nmid i\}$, that is, $m_1 = m$, and $d_2 = \gcd(n, m_1)$. For all $k \geq 2$ we set $m_k = \inf\{i \in \text{supp}(g) \mid d_k \nmid i\}$ and $d_{k+1} = \gcd(d_k, m_k)$. It follows that there exists $h \geq 1$ such that $d_{h+1} = 1$. The set $\{m_1, \dots, m_h\}$ is called the *set of Newton-Puiseux exponents* of $F(X, Y)$. Let $e_k = \frac{d_k}{d_{k+1}}$ for all $1 \leq k \leq h$ and define the sequence $(r_k)_{0 \leq k \leq h}$ as follows: $r_0 = n, r_1 = m$, and for all $2 \leq k \leq h, r_k = r_{k-1}e_{k-1} + m_k - m_{k-1}$. With these notations we have the following (see [1]).

- (1) $\Gamma(F) = \text{o}(R)$ is generated by $\{r_0, r_1, \dots, r_h\}$.
- (2) $r_k d_k < r_{k+1} d_{k+1}$ for all $k \in \{1, \dots, h-1\}$.
- (3) $\Gamma(F) = \text{o}(R)$ is free with respect to the arrangement (r_0, \dots, r_h) . More precisely, let $e_k = \frac{d_k}{d_{k+1}}$ for all $k \in \{1, \dots, h\}$. Then $e_k r_k \in \langle r_0, \dots, r_{k-1} \rangle$.
- (4) $C = \sum_{k=1}^h (e_k - 1)r_k - n + 1$ is the conductor of $\Gamma(F) = \text{o}(R)$.

Example 4.2. Let $f = x^7$ and $g = x^4 + x^2$. The above resultant is then $F = y^7 - 7x^2y^3 - x^4 - 14x^2y^2 - 7x^2y - x^2$. Then $\Gamma(F) = \text{o}(R) = \langle 2, 7 \rangle$.

```
gap> Resultant(x-t^7, y-t^4-t^2,t);
y^7-7*x^2*y^3-x^4-14*x^2*y^2-7*x^2*y-x^2
gap> s:=SemigroupOfValuesOfCurve_Local([t^7,t^4+t^2]);
<Modular numerical semigroup satisfying 7x mod 14 <= x >
gap> MinimalGeneratingSystem(last);
[ 2, 7 ]
gap> IsFreeNumericalSemigroup(s);
true
```

Let the notations be as above. For all $k \geq 2$, let $G_k(X, Y) \in \mathbb{K}[[X, Y]]$ such that $\text{o}(G_k(x^n, g(x))) = r_k$. It follows from [1] that $\deg_Y G_k = \frac{n}{d_k}$. If $g_k(x) = G_k(x^n, g(x))$, then we have the following.

Proposition 4.3. *The set $\{x^n, g, g_2, \dots, g_h\}$ is a basis of R , that is, $R = \mathbb{K}[[x^n, g, g_2, \dots, g_h]]$ and $M_o(R) = \mathbb{K}[[x^n, x^m, x^{r_2}, \dots, x^{r_h}]]$.*

Note that, by a similar argument as in Section 2, we may assume that $f = x^n, g = x^m + \sum_{i \in G(\Gamma(F))} c_i^1 x^i$, and for all $k \geq 2, g_k = x^{r_k} + \sum_{i \in G(\Gamma(F))} c_i^k x^i$, where $G(\Gamma(F)) = \{j \in \mathbb{N} \mid j \notin \Gamma(F)\}$ is the set of gaps of $\Gamma(F)$.

Let the notations be as in Section 3. The morphism

$$D : \mathbb{K}[[u]] \longrightarrow T = \mathbb{K}[[u]][[H_f, H_g, H_{g_2}, \dots, H_{g_h}]]$$

gives us a deformation of $T|_{u=1} = R = \mathbb{K}[[f(x), g(x), g_2(x), \dots, g_h(x)]]$ to $T|_{u=0} = \mathbb{K}[[x^n, x^m, x^{r_2}, \dots, x^{r_h}]]$. Note that, since $\langle n, m, r_2, \dots, r_h \rangle$ is free with respect to the given arrangement, then it is a complete intersection (see for instance [16]). For all $k \in \{1, \dots, h\}$, write $e_k r_k = \sum_{i=0}^{k-1} \theta_i^k r_i$ with $0 \leq \theta_i^k < e_i$ for all $i \in \{1, \dots, k-1\}$. If B is the ideal of $\mathbb{K}[X_0, X_1, \dots, X_h]$ generated by

$$\{X_1^{e_2} - X_0^{\frac{m}{d_2}}, X_2^{e_2} - X_0^{\theta_0^2} X_1^{\theta_1^2}, \dots, X_h^{e_h} - X_0^{\theta_0^h} X_1^{\theta_1^h} \dots X_{h-1}^{\theta_{h-1}^h}\}$$

then

$$\mathbb{K}[[x^n, x^m, x^{r_2}, \dots, x^{r_h}]] \simeq \mathbb{K}[[X_0, X_1, \dots, X_h]]/B.$$

Let $\bar{F}(X, Y)$ be the x -resultant of $X - x^n, y - g(x)$. By hypothesis, $\bar{F}(X, Y)$ is a polynomial. Furthermore, $\bar{F}(X, Y) = Y^n + a_1(X)Y^{n-1} + \dots + a_n(X)$ with $\text{o}(a_i(X)) > i$ for all $2 \leq i \leq n$. Set $G_{h+1} = \bar{F}$ and for all $k \geq 1$, let

$$G_{k+1} = G_k^{e_k} - X^{\theta_0^k} \prod_{i=1}^{k-1} G_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k X^{\alpha_0^k} G_1^{\alpha_1^k} \dots G_k^{\alpha_k^k},$$

where the following conditions hold:

- (1) for all $i \in \{1, \dots, k-1\}$, $0 \leq \theta_i^k < e_i$;
- (2) for all $\underline{\alpha}^k$, if $c_{\underline{\alpha}^k}^k \neq 0$, then for all $i \in \{1, \dots, k\}$, $0 \leq \alpha_i^k < e_i$;
- (3) for all $\underline{\alpha}^k$, if $c_{\underline{\alpha}^k}^k \neq 0$, then $\alpha_0^k n + \sum_{i=1}^k \alpha_i^k r_i = D_i^k > e_k r_k = \theta_0^k r_0 + \sum_{i=1}^{k-1} \theta_i^k r_i$.

It follows from Section 3. that if I (respectively J) is the ideal generated by

$$(X_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} X_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k X_0^{\alpha_0^k} X_1^{\alpha_1^k} \dots X_k^{\alpha_k^k})_{1 \leq k \leq h}$$

(respectively $(X_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} X_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k u^{D_i^k - e_k r_k} X_0^{\alpha_0^k} X_1^{\alpha_1^k} \dots X_k^{\alpha_k^k})_{1 \leq k \leq h}$) in $\mathbb{K}[[X_0, \dots, X_h]]$ (respectively $\mathbb{K}[[u]][[X_0, \dots, X_h]]$), then

$$R = \mathbb{K}[[x^n, g(x), g_2(x), \dots, g_h(x)]] \simeq \mathbb{K}[[X_0, X_1, \dots, X_h]]/I$$

and

$$\mathbb{K}[[u]][[x^n, H_g, H_{g_2}, \dots, H_{g_h}]] \simeq \mathbb{K}[[u]][[X_0, X_1, \dots, X_h]]/J.$$

Furthermore, $\mathbb{K}[[u]][[X_0, X_1, \dots, X_h]]/J$ is a flat $\mathbb{K}[[u]]$ -module. This gives us a family of formal space curves parametrized by u which is a deformation from $\mathbb{K}[[X_0, X_1, \dots, X_h]]/I$ to the formal toric variety $\mathbb{K}[[X_0, X_1, \dots, X_h]]/B$. The later being a complete intersection, we get the following.

Theorem 4.4. *Every irreducible singularity of a plane curve $X = f(x), Y = g(x)$ of \mathbb{K}^2 has a deformation into a formal monomial complete intersection curve of \mathbb{K}^{h+1} for some $h \geq 1$.*

Example 4.5. Let $f(x) = x^4, g(x) = x^6 + x^7$. The minimal polynomial of $(f(x), g(x))$ is given by:

$$F(X, Y) = Y^4 - 2X^3Y^2 + X^6 - 4X^5Y - X^7 = (Y^2 - X^3)^2 - 4X^5Y - X^7$$

Let $r_0 = 4 = d_1, r_1 = 6 = m_1$ and $G_1 = Y$. We have $d_2 = \gcd(6, 4) = 2$, hence $m_2 = 7$. It follows that $r_2 = 13$. Note that if $G_2 = Y^2 - X^3$, then $g_2(x) = G_2(f(x), g(x)) = 2x^{13} + x^{14}$. Hence $\Gamma(F) = \text{o}(R) = \langle 4, 6, 13 \rangle$ and $\{f(x), g(x), g_2(x)\}$ is a basis of R . Let us double check it.

```
gap> SemigroupOfValuesOfCurve_Local([x^4, x^6+x^7], "basis");
[ x^4, x^7+x^6, -1/2*x^15+x^13 ]
```

(Observe that the output is different, since this is a reduced basis: we change $2x^{13} + x^{14}$ with $x^{13} + \frac{1}{2}x^{14}$, and then using that $14 = 2 \times 4 + 6$, we replace this last polynomial with $x^{13} - \frac{1}{2}x^{15}$.)

Consequently, $H_R = \mathbb{K}[[u, x^4, x^6 + ux^7, 2x^{13} + ux^{14}]]$. With the notations above, $e_1 = 3, e_2 = 2$, hence $\mathbb{K}[[x^4, x^6, x^{13}]] \simeq T = \mathbb{K}[[X_0, X_1, X_2]]/(X_1^2 - X_0^3, X_2^2 - X_0^5X_1)$, and

$$\mathbb{K}[[u]] \longrightarrow \mathbb{K}[[u]][[X_0, X_1, X_2]]/(X_1^2 - X_0^3, X_2^2 - 4X_0^5X_1 - u^2X_0^7)$$

gives us a deformation from R to T (we can also change X_2 with $\frac{1}{2}X_2$, and then $B = (X_1^2 - X_0^3, X_2^2 - 4X_0^4X_1)$).

5. SEMIGROUP OF A POLYNOMIAL CURVE

Let \mathbb{K} be a field and let $f_1(x), \dots, f_s(x)$ be s polynomials of $\mathbb{K}[x]$. Let $A = \mathbb{K}[f_1, \dots, f_s]$ be a subalgebra of $\mathbb{K}[x]$, and assume, without loss of generality, that f_i is monic for all $i \in \{1, \dots, s\}$. Given $f(x) = \sum_{i=0}^p c_i x^i \in A$, with $c_p \neq 0$, we set $d(f) = p$ and $M(f) = c_p x^p$, the *degree* and *leading monomial*, respectively. We also define $\text{supp}(f) = \{i \mid c_i \neq 0\}$. The set $d(A) = \{d(f) \mid f \in A\}$ is a submonoid of \mathbb{N} . We shall assume that $\lambda_A(\mathbb{K}[x]/A) < \infty$. In particular $d(A)$ is a numerical semigroup. We say that $\{f_1, \dots, f_s\}$ is a *basis* of A if $\{d(f_1), \dots, d(f_s)\}$ generates $d(A)$. Clearly, $\{f_1, \dots, f_s\}$ is a basis of A if

and only if $\mathbb{K}[M(f), f \in A] = \mathbb{K}[M(f_1), \dots, M(f_s)]$. For several variables, these basis are known in the literature as SAGBI basis ([17, 4]). Since there are already algorithms in the literature to calculate a basis of A , we will not include the procedure here.

We would like just mention that if we follow a similar argument to the one used in Section 2, the sequences of degrees decrease, and thus the finiteness conditions are easier to deduce. In this setting a basis for A is unique up to constants.

6. DEFORMATION TO A TORIC IDEAL

Let the notations be as in Section 5. Given $f(x) = \sum_{i=0}^p c_i x^i \in \mathbb{K}[x]$, we set $h_f(u, x) = \sum_{i=0}^p c_i u^{p-i} x^i$, in particular, if we consider the linear form $L_h : \mathbb{N}^2 \rightarrow \mathbb{N}, L(a, b) = a + b$, then h_f is L_h -homogeneous of degree p , that is, $L_h(i, p-i) = p$ for all $i \in \text{Supp}(f)$. We set $h_A = \mathbb{K}[u, h_f \mid f \in A]$. With these notations we have the following result, and its proof is similar to that of Proposition 3.1.

Proposition 6.1. *The set $\{f_1, \dots, f_r\}$ is a basis of A if and only if $h_A = \mathbb{K}[u, h_{f_1}, \dots, h_{f_s}]$.*

Suppose that $\{f_1, \dots, f_s\}$ is a basis of A . By the inclusion morphism of rings $D : \mathbb{K}[u] \rightarrow B = \mathbb{K}[u, h_{f_1}, \dots, h_{f_s}]$, B is a $\mathbb{K}[u]$ -module. When $u = 1$ (respectively $u = 0$), we get $B|_{u=1} = A$ (respectively $B|_{u=0} = \mathbb{K}[M(f_1), \dots, M(f_s)]$). Hence we get a deformation from A to $\mathbb{K}[M(f_1), \dots, M(f_s)]$. More precisely let

$$\psi : \mathbb{K}[X_1, \dots, X_s] \rightarrow \mathbb{K}[f_1, \dots, f_s]$$

and

$$h_\psi : \mathbb{K}[u][X_1, \dots, X_s] \rightarrow \mathbb{K}[u][h_{f_1}, \dots, h_{f_s}]$$

be the morphisms of rings such that $h_\psi(u) = u$, $\psi(X_i) = f_i$ and $h_\psi(X_i) = h_{f_i}$ for all $i = 1, \dots, s$. For all $i = 1, \dots, r$, let

$$S_i = f_1^{\alpha_1^i} \dots f_s^{\alpha_s^i} - f_1^{\beta_1^i} \dots f_s^{\beta_s^i} = \sum_{\underline{\theta}^i} c_{\underline{\theta}^i}^i f_1^{\theta_1^i} \dots f_s^{\theta_s^i}$$

with $d(f_1^{\theta_1^i} \dots f_s^{\theta_s^i}) = D_{\underline{\theta}^i}^i > \sum_{k=1}^s \alpha_k^i d(f_k) = \sum_{k=1}^s \beta_k^i d(f_k) = p_i$. Let I (respectively J) be the ideal generated by $(G_i = X_1^{\alpha_1^i} \dots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \dots X_s^{\beta_s^i} - \sum_{\underline{\theta}^i} c_{\underline{\theta}^i}^i X_1^{\theta_1^i} \dots X_s^{\theta_s^i})_{1 \leq i \leq r}$ (respectively $(H_i = X_1^{\alpha_1^i} \dots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \dots X_s^{\beta_s^i} - \sum_{\underline{\theta}^i} u^{p_i - D_{\underline{\theta}^i}^i} c_{\underline{\theta}^i}^i X_1^{\theta_1^i} \dots X_s^{\theta_s^i})_{1 \leq i \leq r}$) in $\mathbb{K}[X_1, \dots, X_s]$ (respectively $\mathbb{K}[u][X_1, \dots, X_s]$).

We shall consider on \mathbb{N}^s (respectively, \mathbb{N}^{s+1}) the linear form

$$D(\theta_1, \dots, \theta_s) = \sum_{i=1}^s \theta_i d(f_i)$$

(respectively $D_h(\theta_0, \theta_1, \dots, \theta_s) = \theta_0 + \sum_{i=1}^s \theta_i d(f_i)$).

Given a monomial $X_1^{\theta_1} \dots X_s^{\theta_s}$ (respectively $u^{\theta_0} X_1^{\theta_1} \dots X_s^{\theta_s}$), we set $D(X_1^{\theta_1} \dots X_s^{\theta_s}) = D(\theta_1, \dots, \theta_s)$ (respectively $D_h(u^{\theta_0} X_1^{\theta_1} \dots X_s^{\theta_s}) = D_h(\theta_0, \theta_1, \dots, \theta_s)$).

For $G = \sum_{\theta} c_{\theta} X_1^{\theta_1} \dots X_s^{\theta_s}$ (respectively $H = \sum_{\theta} c_{\theta} u^{\theta_0} X_1^{\theta_1} \dots X_s^{\theta_s}$), we say that G (respectively H) is D -homogeneous of degree a (respectively D_h -homogeneous of degree b) if $D(\theta_1, \dots, \theta_s) = a$ (respectively $D_h(\theta_0, \theta_1, \dots, \theta_s) = b$) for all $(\theta_1, \dots, \theta_s)$ (respectively $(\theta_0, \theta_1, \dots, \theta_s)$) such that $c_{\theta} \neq 0$. More generally let $G = \sum_{k=0}^m G_{p_k}$ where $p_0 > p_1 > \dots > p_m$ and G_{p_k} is D -homogeneous of degree p_k . We set $D(G) = p_0$. We also set $\text{In}(G) = G_{p_0}$ and we call it the *initial form* of G .

Lemma 6.2. *With the standing notations and hypothesis, the kernel of ψ is generated by I .*

Proof. Let F_1, \dots, F_r be a generating system of the kernel of the morphism

$$\phi : \mathbb{K}[X_1, \dots, X_s] \rightarrow \mathbb{K}[x], \phi(X_i) = M(f_i)$$

for all $i \in \{1, \dots, s\}$. In particular F_i is D -homogeneous of degree $d(f_i)$ for all $i \in \{1, \dots, s\}$, and $\mathbb{K}[X_1, \dots, X_s]/(F_1, \dots, F_r) \simeq \mathbb{K}[M(f_1), \dots, M(f_s)]$.

For all $i \in \{1, \dots, r\}$, $\psi(G_i) = 0$. Hence $I \subseteq \ker(\psi)$. For the other inclusion, let $G = \sum_{\theta} c_{\theta} X_1^{\theta_1} \cdots X_s^{\theta_s} \in \ker(\psi)$. Write $G = \sum_{k=0}^m c_{\theta^k} X_1^{\theta_1^k} \cdots X_s^{\theta_s^k}$ where $D(\theta^0) \geq D(\theta^1) \geq \dots > D(\theta^m)$. Since $\psi(G) = 0$, we have that

$$\sum_{k=0}^m c_{\theta^k} f_1^{\theta_1^k} \cdots f_s^{\theta_s^k} = 0.$$

In particular, $\sum_{k, D(\theta^k)=D(\theta^0)} c_{\theta^k} M(f_1)^{\theta_1^k} \cdots M(f_s)^{\theta_s^k} = 0$, and consequently $\sum_{k, D(\theta^k)=D(\theta^0)} c_{\theta^k} X_1^{\theta_1^k} \cdots X_s^{\theta_s^k} \in \ker(\phi)$. This implies that

$$\sum_{k, D(\theta^k)=D(\theta^0)} c_{\theta^k} X_1^{\theta_1^k} \cdots X_s^{\theta_s^k} = \sum_{i=1}^r \lambda_i^0 F_i$$

for some $\lambda_i^0 \in \mathbb{K}[X_1, \dots, X_s]$, $i \in \{1, \dots, r\}$, with λ_i^0 is D -homogeneous of degree $D(G) - D(F_i)$. Hence

$$\sum_{k, D(\theta^k)=D(\theta^0)} c_{\theta^k} f_1^{\theta_1^k} \cdots f_s^{\theta_s^k} = \sum_{i=1}^r \lambda_i^0(f_1, \dots, f_s) S_i.$$

Let $G^1 = G - \sum_{i=1}^r \lambda_i^0 G_i$. It follows that $G^1 \in \ker(\psi)$. If $G^1 \neq 0$, then $D(G) > D(G^1)$. Then we restart with G^1 . We construct in the same way G^2 , and $\lambda_1^1, \dots, \lambda_r^1$ such that $G^1 = G^2 + \sum_{j=1}^r \lambda_j^1 G_j$ with $D(G) > D(G^1) > D(G^2)$, λ_i^1 D -homogeneous and $D(\lambda_i^0) > D(\lambda_i^1)$ for all $i \in \{1, \dots, r\}$. If we continue in this way, we get that for all $k \geq 0$,

$$G = G^{k+1} + \sum_{i=1}^r (\lambda_i^0 + \lambda_i^1 + \dots + \lambda_i^k) G_i,$$

with $D(G) > D(G^1) > \dots > D(G^{k+1})$, λ_i^j D -homogeneous, and $D(\lambda_i^0) > D(\lambda_i^1) > \dots > D(\lambda_i^k)$ for all $i \in \{1, \dots, r\}$ and for all $j \in \{1, \dots, k\}$. Thus, there exists l such that $G^{l+1} = 0$. Hence $G = \sum_{i=1}^r (\lambda_i^0 + \lambda_i^1 + \dots + \lambda_i^l) G_i$. This proves our assertion. \square

Let the notations be as above. Let $G = \sum_{\theta} c_{\theta} X_1^{\theta_1} \cdots X_s^{\theta_s} \in \mathbb{K}[X_1, \dots, X_s]$ and write $G = \sum_{i=0}^m G_{p_i}$ with $p_0 > p_1 > \dots > p_m$ and G_{p_i} D_h -homogeneous. We set $H_G = \sum_{i=0}^m u^{p_0-p_i} G_{p_i}$, in such a way that H_G is D_h -homogeneous of degree p_0 . Given an ideal S of $\mathbb{K}[X_1, \dots, X_s]$, we set $\text{In}(S) = (\text{In}(G) \mid G \in S \setminus \{0\})$. We also denote by $H_S = (H_G \mid G \in S \setminus \{0\}) \mathbb{K}[u, X_1, \dots, X_s]$. With these notations we have $\text{In}(S_i) = F_i$ and $H_{G_i} = H_i$ for all $i \in \{1, \dots, r\}$.

Lemma 6.3. *Let the notations be as above. We have $\text{In}(I) = (F_1, \dots, F_r)$, and $H_I = (H_1, \dots, H_r) = J$.*

Proof. The first assertion follows from the proof of Lemma 6.2.

To prove the second assertion, let $H \in H_I$ and assume that H is D_h -homogeneous. We have $G = H(1, X_1, \dots, X_s) \in I$. Furthermore, $H = u^e H_G$ for some $e \geq 0$. Write $H_G = \text{In}(G) + H^1$ where $H^1(0, X_1, \dots, X_s) = 0$. We have $\text{In}(G) = \sum_{i=1}^r \lambda_i F_i$ where λ_i is D -homogeneous of degree $D(G) - D(F_i)$. Let $H_{G^1} = H_G - \sum_{i=1}^r \lambda_i H_{G_i} = H_G - \sum_{i=1}^r \lambda_i H_i$. Then $H_{G^1} \in H_I$ is D_h -homogeneous and $D_h(H_G) > D_h(H_{G^1})$. Now we restart with H_{G^1} . In this way we show that $H \in (H_1, \dots, H_r)$. \square

Let $H = \sum_{\theta} c_{\theta} u^{\theta} X_1^{\theta_1} \cdots X_s^{\theta_s} \in \ker(h_{\psi})$. Write $H = \sum_{k=0}^n H^k$ where H^k is D_h -homogeneous. For all k , we have $h_{\psi}(H^k) = 0$. Setting $G_k = H^k(1, X_1, \dots, X_s)$, we have $\psi(G_k) = 0$. This implies that $G_k \in I$, and thus $H_{G_k} \in (H_1, \dots, H_r)$ by Proposition 6.3. But $H^k = u^{e_k} H_{G_k}$ for some $e_k \in \mathbb{N}$, whence $H^k \in (H_1, \dots, H_r)$. Finally $H \in (H_1, \dots, H_r)$, which proves that $\ker(h_{\psi}) \subseteq J$. The inclusion $J \subseteq \ker(h_{\psi})$ is obvious, and we can conclude that $J = \ker(h_{\psi})$.

Now the morphism

$$\mathbb{K}[u] \longrightarrow \mathbb{K}[u][X_1, \dots, X_r]/J$$

is flat (because $p(u)$ is not a zero divisor for all $p(u) \in \mathbb{K}[u]$). Hence we get a family of polynomial space curves parametrized by u which gives us a deformation from $\mathbb{K}[X_1, \dots, X_r]/I$ to $\mathbb{K}[X_1, \dots, X_r]/(F_1, \dots, F_r)$.

In particular, we get the following analogue to Theorem 3.4, which can be seen as a geometric reinterpretation of [18, Corollary 11.6] (also [4, Corollary 6.1]).

Theorem 6.4. *Every polynomial space curve of \mathbb{K}^l , parametrized by $Y_1 = g_1(x), \dots, Y_l = g_l(x)$ has a deformation into a monomial curve of \mathbb{K}^r for some positive integer r .*

7. BASIS OF $K[f(x), g(x)]$

In [20], the case when a subalgebra A of $\mathbb{K}[x]$ has a (SAGBI) basis with two elements is treated. Here we study subalgebras generated by two elements of $\mathbb{K}[x]$, and see how a basis can be obtained by using a different approach to that of the general case, as we already did for $\mathbb{K}[[x]]$ in Section 4.

Let $f(x) = \sum_{i=1}^n a_i x^i$ and $g(x) = \sum_{j=1}^m b_j x^j$ be two polynomials of $\mathbb{K}[x]$ and suppose, without loss of generality, that the following conditions hold:

- (1) $a_n = b_m = 1$,
- (2) $n \geq m$,
- (3) the greatest common divisor of $\text{supp}(f(x)) \cup \text{supp}(g(x))$ is equal to 1 (in particular for all $d > 1$, $f(x), g(x) \notin \mathbb{K}[x^d]$).

Let the notations be as in Section 5, in particular $A = \mathbb{K}[f, g]$. Let also $F(X, Y)$ be the x -resultant of $X - f(x), Y - g(x)$, that is, $F(X, Y)$ is the generator of the kernel of the map $\psi : \mathbb{K}[X, Y] \rightarrow \mathbb{K}[x], \psi(X) = f(x)$ and $\psi(Y) = g(x)$. Since $\mathbb{K}[f, g] = \mathbb{K}[f, g - f]$, then we shall assume that $n > m$. Write $F(X, Y) = Y^n + c_1(X)Y^{n-1} + \dots + c_n(X)$. Given a polynomial $G(X, Y) \notin (F(X, Y))\mathbb{K}[X, Y]$, we set $\text{int}(F, G) = \deg_x G(f(x), g(x))$. Assume that \mathbb{K} is algebraically closed with characteristic zero. Let d be a divisor of n , and let G be a monic polynomial in $\mathbb{K}[X][Y]$ of degree $\frac{n}{d}$ in Y . Write $F = G^d + \alpha_1(X, Y)G^{d-1} + \dots + \alpha_d(X, Y)$ where for all $k \in \{1, \dots, d\}$, if $\alpha_k \neq 0$, then $\deg_Y \alpha_k < \frac{n}{d}$. We say that G is a d th *approximate root* of F if $\alpha_1 = 0$. There is a unique d th approximate root of F . We denote it by $\text{App}(F, d)$. The following results can be found in [1].

Theorem 7.1. *Under the standing hypothesis.*

- (1) $F(X, Y)$ has one place at infinity, that is the affine curve $F(X, Y) = 0$ has one point at infinity, and the projective closure of this curve in $\mathbb{P}_{\mathbb{K}}^2$ is analytically irreducible at this point.
- (2) $\{\text{int}(F, G) \mid G \in \mathbb{K}[X, Y] \setminus (F)\}$ is a numerical semigroup.
- (3) Let $D(n)$ be the set of divisors of n . The set $\{\text{int}(F, \text{App}(F, d)) \mid d \in D(n)\}$ generates $\Gamma(F)$.

We call $\{\text{int}(F, G) \mid G \in \mathbb{K}[X, Y] \setminus (F)\}$ the semigroup of F , and we denote it by $\Gamma(F)$.

Corollary 7.2. *Let the notations be as above. We have $d(A) = \Gamma(F)$.*

Proof. In fact, $h(x) \in A$ if and only if $h(x) = P(f(x), g(x))$ for some $P(X, Y) \in \mathbb{K}[X, Y]$. Hence $a \in d(A)$ if and only if $a = \text{int}(F, P)$, $P \in \mathbb{K}[X, Y]$ which means that $a \in \Gamma(F)$. \square

Let $F(X, Y) = Y^n + c_1(X)Y^{n-1} + \dots + c_n(X)$ be as above, and assume, after a possible change of variables $X' = X, Y' = Y + \frac{c_1}{n}$, that $c_1(X, Y) = 0$ (note that this does not change A). In particular $\text{App}(F, n) = Y$. A system of generators of $\Gamma(F)$ can be found algorithmically in the following way.

Let $r_0 = d_1 = n = \text{int}(F, X), r_1 = \deg_X a_n(X) = \text{int}(F, \text{App}(F, n))$, and $d_2 = \gcd(r_0, r_1)$. We set $G_2 = \text{App}(F, d_2), r_2 = \text{int}(F, G_2) = \deg_X G_2(f(x), g(x))$, and $d_3 = \gcd(r_2, d_2)$, and so on... With these notations we have the following:

- (1) $d_1 > d_2 > \dots$ and there exists $h \geq 1$ such that $d_{h+1} = 1$;
- (2) $\Gamma(F) = d(A)$ is generated by $\{r_0, r_1, \dots, r_h\}$;
- (3) $r_k d_k > r_{k-1} d_{k-1}$ for all $k \in \{1, \dots, h\}$;
- (4) $\Gamma(F) = d(A)$ is free with respect to the arrangement (r_0, \dots, r_h) . More precisely, let $e_k = \frac{d_k}{d_{k+1}}$ for all $k \in \{1, \dots, h\}$. Then $e_k r_k \in \langle r_0, \dots, r_{k-1} \rangle$;
- (5) $C = \sum_{k=1}^h (e_k - 1)r_k - n + 1$ is the conductor of $\Gamma(F) = d(A)$.

Lemma 7.3. *If $A = \mathbb{K}[x]$, then $r_k = d_{k+1}$ for all $k = 1, \dots, h$. In particular $\deg_x G_h(f(x), g(x)) = 1$ and m divides n .*

Proof. If $A = \mathbb{K}[x]$ then $C = 0$, hence $\sum_{k=1}^h (e_k - 1)r_k = n - 1$. Since $r_k \geq d_{k+1}$, then $\sum_{k=1}^h (e_k - 1)r_k \geq n - 1$ with equality if and only if $r_k = d_{k+1}$ for all $k = 1, \dots, h$. Since $m = r_1 = d_2 = \gcd(n, m)$, then m divides n . \square

Lemma 7.4. [20, Theorem 2] *If $\gcd(n, m) = 1$, then $\{f(x), g(x)\}$ is a basis of A .*

Proof. If $\gcd(n, m) = 1$, then $\Gamma(F) = d(A) = \langle n, m \rangle$. Hence $\{f(x), g(x)\}$ is a basis of A . \square

Lemma 7.5. *Suppose that $\gcd(n, m) = p_1 \cdots p_l$ where p_i is a positive prime number for all $i \in \{1, \dots, l\}$ (and the p_i 's are not necessarily distinct). The set $\{f(x), g(x)\}$ is not a basis of A . Furthermore, if c is the cardinality of a basis of A , then $2 \leq c \leq l + 2$. In particular, if $\gcd(n, m)$ is a prime number $p > 1$, then a basis of A has either two or three elements.*

Proof. Since $\gcd(n, m) > 1$, then the first assertion is clear. On the other hand, since $d_2 = \gcd(n, m) = p_1 \cdots p_r$, we have $A \neq \mathbb{K}[x]$, and $h \leq l + 1$. Hence $\Gamma(F) = d(A)$ has at most $l + 2$ generators. The result now follows. \square

Remark 7.6. Let $\underline{r} = (r_0 = n, r_1 = m, r_2, \dots, r_h)$ be a sequence of integers and for all $k \geq 1$, let $d_k = \gcd(r_0, \dots, r_{k-1})$ and $e_k = \frac{d_k}{d_{k+1}}$. Assume that the following conditions hold:

- (1) $d_1 > d_2 > \dots > d_{h+1} = 1$;
- (2) $r_k d_k > r_{k-1} d_{k-1}$ for all $k \in \{1, \dots, h\}$;
- (3) $e_k r_k \in \langle r_0, \dots, r_{k-1} \rangle$ for all $k = 1, \dots, h$.

Such a sequence is called a δ -sequence and it is well known (see [1]) that there exists a polynomial $\tilde{F}(X, Y)$ with one place at infinity such that the semigroup $\{\text{rank}_{\mathbb{K}} \mathbb{K}[X, Y]/(\tilde{F}, G), G \notin (F)\}$ is generated by \underline{r} .

It follows from Theorem 7.1. that a polynomial curve has one place at infinity. The converse is not true in general. Abhyankar asked whether every semigroup generated by a δ -sequence (hence the semigroup of a curve with one place at infinity) is the semigroup of a polynomial curve (for example, the δ -sequence $(10, 4, 5)$ generates the semigroup $\langle 4, 5 \rangle$ which is the semigroup of the polynomial curve $A = \mathbb{K}[x^4, x^5]$). It has been proved recently that the answer is no ([9]). It would be nice to see which supplementary conditions a δ -sequence should satisfy in order to generate the semigroup of a polynomial curve.

Remark 7.7. Let $f(x)$ and $g(x)$ be as above, and let $A = \mathbb{K}[f(x), g(x)]$. Let also $F(X, Y)$ be the x -resultant of $X - f(x)$ and $Y - g(x)$. Let $r_0 = n, r_1 = m, r_2, \dots, r_h$ be the generators of $\Gamma(F)$ calculated as above. Let $1 \leq k \leq h$ and let $G_k(X, Y) = \text{App}(F, d_k)$. We have $d(G_k(f(x), g(x))) = r_k$, but G_k is not the unique polynomial with this condition (for example, $d((G_k + \lambda)(f(x), g(x))) = r_k$ for all $\lambda \neq 0$). Hence it is natural to ask the following: is there a polynomial $G(X, Y)$ (of degree $< n$ in Y) such that G is parametrized by polynomials in x such that $d(G(f(x), g(x))) = r_k$? Such a polynomial, if it exists, should be of degree $\frac{n}{d_k}$ and should have the contact with F at a characteristic exponent of F (see [1] for the definition of the characteristic exponents of a curve with one place at infinity and the notion of contact). Hence the existence of such a polynomial implies that a polynomial curve can be approximated by polynomial curves.

Let the notations be as above, in particular $F(X, Y) = Y^n + c_1(X)Y^{n-1} + \dots + c_n(X)$ is the x -resultant of $(X - f(x), Y - g(x))$. Let $G_1 = Y, G_2, \dots, G_h$ be the set of approximate roots of $F(X, Y)$ constructed algorithmically as above. In particular $r_0 = n, r_1 = m, r_2 = \text{int}(F, G_2), \dots, r_h = \text{int}(F, G_h)$ generate $d(A)$. For all $k = 2, \dots, h$, let $g_k(x) = G_k(f(x), g(x))$ and let $M(g_k) = b_{r_k} x^{r_k}$. We have $A = \mathbb{K}[f(x), g(x), g_2(x), \dots, g_h(x)]$. Furthermore, the map

$$D : \mathbb{K}[u] \longrightarrow B = \mathbb{K}[u][h_f, h_g, h_{g_2}, \dots, h_{g_h}]$$

introduced in Section 6. gives us a deformation of the polynomial curve $B|_{u=1} = A$ into $B|_{u=0} = \mathbb{K}[t^n, t^m, t^{r_2}, \dots, t^{r_h}]$. Note that, since $\langle n, m, r_2, \dots, r_h \rangle$ is free with respect to the given arrangement, then it is a complete intersection. For all $k \in \{1, \dots, h\}$, write $e_k r_k = \sum_{i=0}^{k-1} \theta_i^k r_i$ with $0 \leq \theta_i^k < e_i$ for every $i \in \{1, \dots, k-1\}$. With the notations above, if T is the ideal of $\mathbb{K}[X_0, X_1, \dots, X_h]$ generated by

$$\{X_1^{e_2} - X_0^{\frac{m}{d_2}}, X_2^{e_2} - X_0^{\theta_0^2} X_1^{\theta_1^2}, \dots, X_h^{e_h} - X_0^{\theta_0^h} X_1^{\theta_1^h} \dots X_{h-1}^{\theta_{h-1}^h}\},$$

then

$$\mathbb{K}[x^n, x^m, x^{r_2}, \dots, x^{r_h}] \simeq \mathbb{K}[X_0, X_1, \dots, X_h]/T.$$

Set $G_{h+1} = F$ and for all $k \geq 1$, let

$$G_{k+1} = G_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} G_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k X_0^{\alpha_0^k} G_1^{\alpha_1^k} \cdots G_k^{\alpha_k^k},$$

where the following conditions hold:

- (1) for all $i \in \{1, \dots, k-1\}$, $0 \leq \theta_i^k < e_i$;
- (2) for all $\underline{\alpha}^k$, if $c_{\underline{\alpha}^k}^k \neq 0$, then for all $i \in \{1, \dots, k\}$, $0 \leq \alpha_i^k < e_i$,
- (3) for all $\underline{\alpha}^k$, if $c_{\underline{\alpha}^k}^k \neq 0$, then $\alpha_0^k n + \sum_{i=1}^k \alpha_i^k r_i = D_i^k < e_k r_k = \theta_0^k r_0 + \sum_{i=1}^{k-1} \theta_i^k r_i$.

It follows from Section 6 that if I (respectively J) is the ideal generated by $(X_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} X_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k X_0^{\alpha_0^k} X_1^{\alpha_1^k} \cdots X_k^{\alpha_k^k})_{1 \leq k \leq h}$ (respectively $(X_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} X_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k u^{e_k r_k - D_i^k} X_0^{\alpha_0^k} X_1^{\alpha_1^k} \cdots X_k^{\alpha_k^k})_{1 \leq k \leq h}$) in $\mathbb{K}[X_0, \dots, X_h]$ (respectively $\mathbb{K}[u][X_0, \dots, X_h]$), then

$$A = \mathbb{K}[x^n, g(x), g_2(x), \dots, g_h(x)] \simeq \mathbb{K}[X_0, X_1, \dots, X_h]/I$$

and

$$\mathbb{K}[u][x^n, h_{g(x)}, h_{g_2(x)}, \dots, h_{g_h(x)}] \simeq \mathbb{K}[u][X_0, X_1, \dots, X_h]/J.$$

Furthermore, $\mathbb{K}[u][X_0, X_1, \dots, X_h]/J$ is a flat $\mathbb{K}[u]$ -module. This gives us a family of space curves parametrized by u which is a deformation from $\mathbb{K}[X_0, X_1, \dots, X_h]/I$ to the toric variety $\mathbb{K}[X_0, X_1, \dots, X_h]/T$. The later being a complete intersection, we get the following result.

Theorem 7.8. *Every polynomial curve $X = f(x), Y = g(x)$ of \mathbb{K}^2 has a deformation into a monomial complete intersection curve of \mathbb{K}^{h+1} for some positive integer h .*

Example 7.9. Let $f(x) = x^6 + x^3, g(x) = x^4$. The minimal polynomial of $(f(x), g(x))$ is given by:

$$F(X, Y) = Y^6 - 2X^2Y^3 - 4XY^3 - Y^3 + X^4.$$

Let $r_0 = 6 = d_1, r_1 = 4$ and $G_1 = Y$. We have $d_2 = \gcd(6, 4) = 2$, and $G_2 = \text{App}(F, 2) = Y^3 - X^2 - 2X - \frac{1}{2}$. Since $g_2(x) = G_2(f(x), g(x)) = -2x^9 - 3x^6 - 2x^3 - \frac{1}{2}$, then $r_2 = 9$ and $d_3 = 1$, hence $\Gamma(F) = d(A) = \langle 6, 4, 9 \rangle$ and $\{f(x), g(x), -g_2(x)\}$ is a basis of A . Consequently, $h_A = \mathbb{K}[u, x^6 + u^3x^3, x^4, 2x^9 + 3u^3x^6 + 2u^6x^3 + \frac{1}{2}u^9]$. Note that, with the notations above, $e_1 = 3, e_2 = 2$, hence $\mathbb{K}[x^6, x^4, 2x^9] \simeq \mathbb{K}[X_0, X_1, X_2]/(X_1^3 - X_0^2, X_2^2 - 4X_0^3) = \mathbb{K}[X_0, X_1, X_2]/T$, $\mathbb{K}[x^6 + x^3, x^4, 2x^9 - 3x^6 - 2x^3 - \frac{1}{2}] \simeq \mathbb{K}[X_0, X_1, X_2]/(X_1^3 - X_0^2 - 2X_0 - \frac{1}{2}, X_2^2 - 4X_0^3 - 5X_0^2 - 2X_0 - \frac{1}{4})$, and

$$\mathbb{K}[u] \longrightarrow \mathbb{K}[u][X_0, X_1, X_2]/(X_1^3 - X_0^2 - 2u^6X_0 - \frac{1}{2}u^9, X_2^2 - 4X_0^3 - 5u^6X_0^2 - 2u^{12}X_0 - \frac{1}{4}u^{18})$$

gives us a deformation from A to $\mathbb{K}[X_0, X_1, X_2]/T$.

The computation of the approximate roots and of $\Gamma(F)$ can be performed with the algorithm presented in [2].

```
gap> f:=y^6-2*x^2*y^3-4*x*y^3-y^3+x^4;;
gap> SemigroupOfValuesOfPlaneCurveWithSinglePlaceAtInfinity(f);
<Numerical semigroup with 3 generators>
gap> MinimalGeneratingSystem(last);
[ 4, 6, 9 ]
gap> SemigroupOfValuesOfPlaneCurveWithSinglePlaceAtInfinity(f);
[ [ 6, 4, 9 ], [ y, y^3-x^2-2*x-1/2 ] ]
```

Example 7.10. Let $f(x) = x^6 + x, g(x) = x^4$. The minimal polynomial of $(f(x), g(x))$ is given by:

$$F(X, Y) = Y^6 - 2X^2Y^3 - 4XY^2 - Y + X^4.$$

Let $r_0 = 6 = d_1, r_1 = 4$ and $G_1 = Y$. We have $d_2 = \gcd(6, 4) = 2$, and $G_2 = \text{App}(F, 2) = Y^3 - X^2$. Since $g_2(x) = G_2(f(x), g(x)) = -2x^7 - x^2$, then $r_2 = 7$ and $d_3 = 1$, hence $\Gamma(F) = d(A) = \langle 6, 4, 7 \rangle$ and $\{f(x), g(x), -g_2(x)\}$ is a basis of A . Consequently, $h_A = \mathbb{K}[u, x^6 + u^5x, x^4, 2x^7 + u^5x^2]$. Note that,

with the notations above, $e_1 = 3, e_2 = 2$, hence $\mathbb{K}[x^6, x^4, x^7] \simeq \mathbb{K}[X_0, X_1, X_2]/(X_1^3 - X_0^2, X_2^2 - X_0X_1^2) = \mathbb{K}[X_0, X_1, X_2]/T$, and

$$\mathbb{K}[u] \longrightarrow \mathbb{K}[u][X_0, X_1, X_2]/(X_1^3 - X_0^2, X_2^2 - 4X_0X_1^2 - u^{10}X_1)$$

gives us a deformation from A to $\mathbb{K}[X_0, X_1, X_2]/T$ (we can also change X_2 with $\frac{1}{2}X_2$, and then we get $(X_1^3 - X_0^2, X_2^2 - X_0X_1^2 - \frac{1}{4}u^{10}X_1)$ instead).

Acknowledgements

The authors would also like to thank Lance Bryant for providing plenty of examples for testing our algorithms, as well as suggesting us to implement new functionalities, that are now given as an extra argument of the function `SemigroupOfValuesOfCurveLocal`.

A communication with the contents of this manuscript was presented by the third author at MEGA'2015. We would like to thank the anonymous referees assigned by the organization of this meeting for their comments and suggestions. All of them were taken into account in the current version of this manuscript.

REFERENCES

- [1] S.S. Abhyankar, On the semigroup of a meromorphic plane curve, Part I, in Proceedings of International Symposium on Algebraic Geometry (1977), 240–414.
- [2] A. Assi, P. A. García-Sánchez, Algorithms for curves with one place at infinity, *J. Symb. Comp.* **74**, (2016), 475–492.
- [3] V. Barucci, D. E. Dobbs, M. Fontana, Properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains, *Mem. Amer. Math. Soc.* vol 125, **598** (1997).
- [4] A. Bravo, Some facts about canonical subalgebra bases, *Trends in Commutative Algebra*, **51**, (2004), 247–254.
- [5] A. Castellanos, J. Castellanos, Algorithm for the Semigroup of a Space Curve Singularity, *Semigroup Forum* **70** (2005) 44–60.
- [6] A. Del Centina, Weierstrass points and their impact in the study of algebraic curves: a historical account from the “Lückensatz” to the 1970s. *Ann. Univ. Ferrara Sez. VII Sci. Mat.* **54** (2008), 37–59.
- [7] M. Delgado, P. A. García-Sánchez, J. Morais, “NumericalSgps”, A GAP package for numerical semigroups. Available via <http://www.gap-system.org>.
- [8] R. Fröberg-C. Gottlieb-R. Häggkvist, On numerical semigroups, *Semigroup forum* **35** (1987), 63–83.
- [9] M. Fujimoto, M. Suzuki, K. Yokoyama, On polynomial curves in the affine plane. *Osaka J. Math.* **43** (2006), no. 3, 597–608.
- [10] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.5; 2014, <http://www.gap-system.org>.
- [11] R. Goldin, B. Teissier, Resolving singularities of plane analytic branches with one toric morphism. *Resolution of singularities (Oberurgl, 1997)*, *Progr. Math.*, **181**, Birkhauser, Basel, 2000, 315–340.
- [12] E. Kunz, The value-semigroup of a one-dimensional Gorenstein ring, *Proc. Amer. Math. Soc.* **25** (1970), 748–751.
- [13] T. Matsuoka, On the degree of singularity of one-dimensional analytically irreducible noetherian local rings, *J. Math. Kyoto Univ.*, **11-3** (1971), 485–494.
- [14] V. Micale, Order bases of subalgebras of power series rings, *Comm. Algebra* **31** (2003), no. 3, 1359–1375.
- [15] V. Micale, G. Molica, B. Torrisi, Order bases of subalgebras of $k[[X]]$, *Commutative rings*, 193–199, Nova Sci. Publ., Hauppauge, NY, 2002.
- [16] J. C. Rosales, P. A. García-Sánchez, Numerical semigroups, *Developments in Mathematics*, 20. Springer, New York, 2009.
- [17] L. Robbiano and M. Sweedler, Subalgebra bases, pp. 61–87 in *Commutative Algebra (Salvador, 1988)*, edited by W. Bruns and A. Simis, *Lecture Notes in Math.* **1430**, Springer, Berlin, 1990.
- [18] B. Sturmfels, Gröbner bases and convex polytopes, *University Lecture Series* **8**, Amer. Math. Soc., Providence, 1996.
- [19] B. Teissier, “Appendice”, pp. 145–199 in *Le problème des pour les branches planes*, by O. Zariski, Centre de Mathématiques de l’Ecole Polytechnique, Paris, 1975. Second edition, Hermann, 1986.
- [20] A. Torstensson, Canonical bases for subalgebras on two generators in the univariate polynomial ring. *Beiträge Algebra Geom.* **43** (2002), 565–577.

UNIVERSITÉ D’ANGERS, MATHÉMATIQUES, 49045 ANGERS CEDED 01, FRANCE
E-mail address: `assi@univ-angers.fr`

IE MATH-GR AND DEPARTAMENTO DE ÁLGEBRA, UNIVERSIDAD DE GRANADA, E-18071 GRANADA, ESPAÑA
E-mail address: `pedro@ugr.es`

DIPARTIMENTO DI MATEMATICA E INFORMATICA, VIALE A. DORIA, 6 - I 95125 CATANIA, ITALIA
E-mail address: `vmicale@dmf.unict.it`