



HAL
open science

Canonical bases of modules over one dimensional k-algebras

A A Abbas, A A Assi, Pedro A García-Sánchez

► **To cite this version:**

A A Abbas, A A Assi, Pedro A García-Sánchez. Canonical bases of modules over one dimensional k-algebras. 2017. hal-01485009v2

HAL Id: hal-01485009

<https://hal.science/hal-01485009v2>

Preprint submitted on 9 Mar 2017

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.

CANONICAL BASES OF MODULES OVER ONE DIMENSIONAL K-ALGEBRAS

A. ABBAS, A. ASSI, AND P. A. GARCÍA-SÁNCHEZ

ABSTRACT. Let \mathbf{K} be a field and denote by $\mathbf{K}[t]$, the polynomial ring with coefficients in \mathbf{K} . Set $\mathbf{A} = \mathbf{K}[f_1, \dots, f_s]$, with $f_1, \dots, f_s \in \mathbf{K}[t]$. We give a procedure to calculate the monoid of degrees of the \mathbf{K} algebra $\mathbf{M} = F_1\mathbf{A} + \dots + F_r\mathbf{A}$ with $F_1, \dots, F_r \in \mathbf{K}[t]$. We show some applications to the problem of the classification of plane polynomial curves (that is, plane algebraic curves parametrized by polynomials) with respect to some of their invariants, using the module of Kähler differentials.

1. INTRODUCTION

Let \mathbf{K} be a field of characteristic zero and let $f(X, Y)$ be a nonzero irreducible element of $\mathbf{K}[X, Y]$. Let $C = \{(x, y) \in \mathbf{K}^2 \mid f(x, y) = 0\}$ be the plane algebraic curve defined by f . There are some important invariants that can be associated with C : the Milnor number, $\mu(f)$, which is the rank of $\mathbf{K}[X, Y]/(f_X, f_Y)$, and the Turina number, $\nu(f)$, which is the rank of $\mathbf{K}[X, Y]/(f, f_X, f_Y)$ (where f_X, f_Y denote the partial derivatives of f). The first one tells us how singular is the family of curves $C_\lambda = \{(x, y) \mid f(x, y) - \lambda = 0\}$, and the second one tells us how singular is the curve C . Suppose that C is parametrized by two polynomials $X(t), Y(t) \in \mathbf{K}[t]$. In this case, we can associate to f a semigroup, denoted $\Gamma(f)$ and defined by $\Gamma(f) = \{d(g(X(t), Y(t)) \mid g(X, Y) \in \mathbf{K}[X, Y] \setminus (f)\}$, where $d(g(X(t), Y(t)))$ denotes the degree in t of $g(X(t), Y(t))$.

Let $\mathbf{A} = \mathbf{K}[X(t), Y(t)]$ be the \mathbf{K} -algebra generated by $X(t), Y(t)$. Then \mathbf{A} is the ring of coordinates of C . If $\lambda(\mathbf{K}[t]/\mathbf{A}) < +\infty$, then $\Gamma(f)$ is a numerical semigroup, and $\mu(f)$ coincides with the conductor of $\Gamma(f)$. Let $\mathbf{M} = X'(t)\mathbf{A} + Y'(t)\mathbf{A}$ be the \mathbf{A} -module generated by the derivatives of $X(t), Y(t)$. The set of degrees in t of elements of \mathbf{M} , denoted $d(\mathbf{M})$, defines an ideal of $\Gamma(f)$, and from the definition it follows that for all $s \in \Gamma(f)$, the element $s - 1$ is in $d(\mathbf{M})$. Such an element is called exact. In general, $d(\mathbf{M})$ contains elements that are non exact, and the cardinality of the set of these elements is bounded by the genus of $\Gamma(f)$. Furthermore, this cardinality is nothing but the difference $\mu - \nu$. Hence the numerical semigroup $\Gamma(f)$ and the ideal $d(\mathbf{M})$ offer a good computational approach to the study of these invariants.

This paper has two main goals. Given a \mathbf{K} -algebra $\mathbf{A} = \mathbf{K}[f_1(t), \dots, f_s(t)]$, we first describe an algorithm that computes a system of generators of the ideal consisting of degrees in t of elements of the module $\mathbf{M} = F_1(t)\mathbf{A} + \dots + F_r(t)\mathbf{A}$ (where $f_1(t), \dots, f_s(t), F_1(t), \dots, F_r(t) \in \mathbf{K}[t]$). This algorithm uses the one given in [5] in order to compute the semigroup consisting of degrees in t of elements of \mathbf{A} . Then we consider the case where $\mathbf{A} = \mathbf{K}[X(t), Y(t)]$ is the ring of coordinates of the algebraic plane curve parametrized by $X(t), Y(t)$, and \mathbf{K} is an algebraically closed field of characteristic zero. It turns out that the curve has one place at infinity, and if $f(X, Y)$ is a generator of the curve in $\mathbf{K}[X, Y]$, then the semigroup $\Gamma(f)$ introduced above, which is the same as the semigroup associated with \mathbf{A} , can be calculated from the Abhyankar-Moh theory (see [4]). Using this fact and some techniques introduced in Section 6, we characterize the semigroup of polynomial curves when $\mu - \nu \in \{0, 1, 2\}$.

Date: March 9, 2017.

2000 Mathematics Subject Classification. 14H20, 14H50, 05E15.

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

2. NUMERICAL SEMIGROUPS AND IDEALS

2.1. Numerical semigroups. Let S be a subset of \mathbb{N} . The set S is a submonoid of \mathbb{N} if the following holds:

- (1) $0 \in S$,
- (2) If $a, b \in S$ then $a + b \in S$.

Clearly, $\{0\}$ and \mathbb{N} are submonoids of \mathbb{N} . Also, if S contains a nonzero element a , then $da \in S$ for all $d \in \mathbb{N}$, and in particular, S is an infinite set.

Let S be a submonoid of \mathbb{N} and let G be the subgroup of \mathbb{Z} generated by S (that is, $G = \{\sum_{i=1}^s \lambda_i a_i \mid \lambda_i \in \mathbb{Z}, a_i \in S\}$). If $1 \in G$, then we say that S is a *numerical semigroup*. This is equivalent to the condition that $\mathbb{N} \setminus S$ is a finite set.

We set $G(S) = \mathbb{N} \setminus S$ and we call it the set of *gaps* of S . We denote by $g(S)$ the cardinality of $G(S)$, and we call $g(S)$ the *genus* of S . We set $F(S) = \max(G(S))$ and we call it the *Frobenius number* of S . We also define $C(S) = F(S) + 1$ and we call it the *conductor* of S . The least positive integer of S , $m(S) = \inf(S \setminus \{0\})$ is known as the *multiplicity* of S .

Even though any numerical semigroup has infinitely many elements, it can be described by means of finitely many of them. The rest can be obtained as linear combinations with nonnegative integer coefficients from these finitely many.

Let S be a numerical semigroup and let $A \subseteq S$. We say that S is generated by A and we write $S = \langle A \rangle$ if for all $s \in S$, there exist $a_1, \dots, a_r \in A$ and $\lambda_1, \dots, \lambda_r \in \mathbb{N}$ such that $s = \sum_{i=1}^r \lambda_i a_i$. Every numerical semigroup S is finitely generated, that is, $S = \langle A \rangle$ with $A \subseteq S$ and A is a finite set.

Let $n \in S^*$. We define the *Apéry set* of S with respect to n , denoted $\text{Ap}(S, n)$, to be the set

$$\text{Ap}(S, n) = \{s \in S \mid s - n \notin S\}.$$

Let S be a numerical semigroup and let $n \in S^*$. For all $i \in \{1, \dots, n\}$, let $w(i)$ be the smallest element of S such that $w(i) \equiv i \pmod{n}$. Then

$$\text{Ap}(S, n) = \{0, w(1), \dots, w(n-1)\}.$$

Furthermore, $S = \langle n, w(1), \dots, w(n-1) \rangle$.

We will be interested in a special class of numerical semigroups, namely free numerical semigroups. The definition is as follows.

Definition 2.1. Let $S = \langle r_0, r_1, \dots, r_h \rangle$ be a numerical semigroup, and let $d_{i+1} = \gcd(r_0, r_1, \dots, r_i)$ for all $i \in \{0, \dots, h\}$ (in particular $d_1 = r_0$ and $d_{h+1} = 1$) and $e_i = \frac{d_i}{d_{i+1}}$ for all $i \in \{1, \dots, h\}$. We say that S is free for the arrangement (r_0, \dots, r_h) if the following conditions hold:

- (1) $d_1 > d_2 > \dots > d_{h+1} = 1$,
- (2) $e_i r_i \in \langle r_0, \dots, r_{i-1} \rangle$ for all $i \in \{1, \dots, h\}$.

Note that the notion of freeness depends on the arrangement of the generators. For example, $S = \langle 4, 6, 13 \rangle$ is free for the arrangement $(4, 6, 13)$ but it is not free for the arrangement $(13, 4, 6)$. Note also that if $S = \langle r_0, r_1, \dots, r_h \rangle$ is free with respect to the arrangement (r_0, \dots, r_h) , then $g(S) = \frac{C(S)}{2}$.

Let $S = \langle r_0, r_1, \dots, r_h \rangle$ and suppose that S is free with respect to the arrangement (r_0, \dots, r_h) . Let the notations be as above, given $s \in \mathbb{Z}$, there exist $\lambda_0, \lambda_1, \dots, \lambda_h \in \mathbb{Z}$ such that

$$s = \sum_{i=0}^h \lambda_i r_i \text{ and } 0 \leq \lambda_i < e_i, \quad i \in \{1, \dots, h\}.$$

Such a representation is unique. We call it the *standard representation* of s . We have $s \in S$ if and only if $\lambda_0 \geq 0$. Also any free semigroup has the following properties.

Proposition 2.2. *Let $S = \langle r_0, \dots, r_h \rangle$ be a free numerical semigroup with respect to the arrangement (r_0, \dots, r_h) .*

- i) $F(S) = \sum_{i=1}^h (e_i - 1)r_i - r_0$.
- ii) *For all $a, b \in \mathbb{Z}$, if $a + b = F(S)$, then $a \in S$ if and only if $b \notin S$. In other words, S is a symmetric numerical semigroup.*
- iii) $\text{Ap}(S, r_0) = \left\{ \sum_{i=1}^h \lambda_i r_i \mid 0 \leq \lambda_i < e_i \text{ for all } i \in \{1, \dots, h\} \right\}$.

2.2. Ideals of numerical semigroups. Let S be a numerical semigroup of \mathbb{N} and let I be a nonempty set of \mathbb{N} . We say that I is a *relative ideal* of S if for all $(a, s) \in I \times S$, $a + S \in I$ ($I + S \subseteq I$ for short) and there exists $d \in \mathbb{Z}$ such that $d + I \subseteq S$. This second condition is equivalent to saying that I has a minimum.

Define the following order on \mathbb{Z} : $n_1 \leq_S n_2$ if $n_2 - n_1 \in S$. Let $E \subset \mathbb{N}$. We say that $n \in E$ is a minimal element of E with respect to \leq_S if for all $s \in E$, the condition $s \leq_S n$ implies $n = s$. We denote by $\text{Minimals}_{\leq_S}(E)$ the set of minimal elements of E with respect to \leq_S .

If I is an ideal of S , then there exist a set $\{a_1, \dots, a_l\} \subseteq I$ such that $I = \bigcup_{i=1}^l (a_i + S)$. We say that $\{a_1, \dots, a_l\}$ is a *system of generators* of I . If furthermore $a_k \notin \bigcup_{i \neq k} (a_i + S)$, then we say that $\{a_1, \dots, a_l\}$ is a *minimal set of generators* of I . Observe that all minimal generators are incongruent modulo $m(S)$, and thus a minimal set of generators of I has at most $m(S)$ elements. This set coincides with $\text{Minimals}_{\leq_S}(I)$.

Intersection of two relative ideals is again a relative ideal. In particular, given $a, b \in \mathbb{N}$, $(a + S) \cap (b + S)$ is a relative ideal. Assume that $\{a_1, \dots, a_r\}$ is the set of minimal generators of $(a + S) \cap (b + S)$. We set

$$R(a, b) = \{(a_k - a, a_k - b), k \in \{1, \dots, r\}\}.$$

Example 2.3. *Let $S = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, \rightarrow\}$ and let $a = 3$, $b = 5$. We have $3 + S = \{3, 6, 7, 9, 10, \rightarrow\}$ and $5 + S = \{5, 8, 9, 11, 12, \rightarrow\}$. Hence $(3 + S) \cap (5 + S) = \{9, 11, 12, \rightarrow\} = (9 + S) \cup (11 + S)$. Note that $\{9, 11\}$ is the set of minimal elements of $(3 + S) \cap (5 + S)$ with respect to \leq_S and that $R(3, 5) = \{(6, 4), (8, 6)\}$.*

3. RELATORS FOR MONOMIAL SUBALGEBRAS

Let $S = \langle s_1, \dots, s_n \rangle$ be a numerical semigroup and let I be a relative ideal of S . Let $\{a_1, \dots, a_r\}$ be a minimal system of generators of I . Let \mathbf{K} be a field and consider the algebra $\mathbf{A} = \mathbf{K}[t^{s_1}, \dots, t^{s_n}] = \mathbf{K}[S]$. Let $\mathbf{M} = t^{a_1} \mathbf{A} + \dots + t^{a_r} \mathbf{A}$ and let

$$\phi : \mathbf{A}^r \rightarrow \mathbf{M}, \quad \phi(f_1, \dots, f_r) = t^{a_1} f_1 + \dots + t^{a_r} f_r.$$

The kernel $\ker(\phi)$ is a submodule of \mathbf{A}^r . The following result gives explicitly a generating system for $\ker(\phi)$.

Theorem 3.1. *Let S be a numerical semigroup and let I be a relative ideal of S minimally generated by $\{a_1, \dots, a_r\}$. Let φ be the morphism*

$$\phi : \mathbf{A}^r \rightarrow t^{a_1} \mathbf{A} + \dots + t^{a_r} \mathbf{A}, \quad \phi(f_1, \dots, f_r) = t^{a_1} f_1 + \dots + t^{a_r} f_r.$$

Then $\ker(\phi)$ is generated by

$$\left\{ t^\alpha \mathbf{e}_i - t^\beta \mathbf{e}_j \mid i, j \in \{1, \dots, r\}, i \neq j, (\alpha, \beta) \in R(a_i, a_j) \right\},$$

where $\{\mathbf{e}_1, \dots, \mathbf{e}_r\}$ denotes the canonical basis of \mathbf{A}^r .

Proof. Let $B = \{t^\alpha \mathbf{e}_i - t^\beta \mathbf{e}_j \mid i, j \in \{1, \dots, r\}, i \neq j, (\alpha, \beta) \in R(a_i, a_j)\}$. Clearly, $B \subset \ker(\varphi)$.

Let $\mathbf{f} = (f_1, \dots, f_r) \in \ker(\phi)$. We have $\sum_{i=1}^r t^{a_i} f_i = 0$. Let d_i be the degree of f_i , and assume that $c_i t^{d_i}$ is the leading term of f_i , $i \in \{1, \dots, r\}$. As $\sum_{i=1}^r t^{a_i} f_i = 0$, there must be $i \in \{2, \dots, r\}$ and a monomial kt^s of f_i such that $a_1 + d_1 = a_i + s$ ($s \in S$). Without loss of generality, we may

think that $i = 2$. Thus $a_1 + d_1 = a_2 + s \in (a_1 + S) \cap (a_2 + S)$, whence $a_1 + d_1 = a_2 + s = \gamma + s_{12}$ with γ a minimal generator of $(a_1 + S) \cap (a_2 + S)$ and $s_{12} \in S$. Hence $(d_1, s) = (\gamma - a_1 + s_{12}, \gamma - a_2 + s_{12})$. Set $(\alpha, \beta) = (\gamma - a_1, \gamma - a_2)$. Then $(\alpha, \beta) \in R(a_1, a_2)$ and $(d_1, s) = (\alpha + s_{12}, \beta + s_{12})$.

We can write $\mathbf{f} = (f_1, \dots, f_r) = c_1 t^{s_{12}} (t^\alpha \mathbf{e}_1 - t^\beta \mathbf{e}_2) + \mathbf{f}'$, with $\mathbf{f}' = (f'_1, f'_2, f_3, \dots, f_r)$, $f'_1 = f_1 - c_1 t^{d_1}$ and $f'_2 = f_2 + c_1 t^{d_1}$. In this way, we have killed the leading term of f_1 , and \mathbf{f}' is again in $\ker(\varphi)$. We continue with \mathbf{f}' until the first component is zero. After that we focus on the second component and so on. We will end up with an expression of the form $\mathbf{f}^{(n)} = (0, \dots, 0, f_r^{(n)}) \in \ker(\varphi)$. But this leads to $f_r^{(n)} = 0$, since otherwise $t^{ar} f_r^{(n)}$ would not be zero. This concludes the proof. \square

Example 3.2. Let $S = \langle 3, 4 \rangle$ and let $I = (3 + S) \cup (5 + S)$. Let

$$\phi : \mathbf{A}^2 \rightarrow t^3 \mathbf{K}[t^3, t^4] + t^5 \mathbf{K}[t^3, t^4], \quad \phi(f_1, f_2) = t^3 f_1 + t^5 f_2.$$

Then $\ker(\phi)$ is generated by $\{(t^6, -t^4), (t^8, -t^6)\}$.

In light of Theorem 3.1, we can use the following code in GAP (by using the `numericalsgps` package) to calculate the kernel of φ .

GAP CODE 1. R and ker functions

```

1  R:=function(a,b,s)
2  local i, mg;
3  i:=IntersectionIdealsOfNumericalSemigroup(a+s,b+s);
4  mg:=MinimalGenerators(i);
5  return List(mg, m->[m-a,m-b]);
6  end;
7
8  ker:=function(I)
9  local mg, s, r, i, j, n;
10 s:=AmbientNumericalSemigroupOfIdeal(I);
11 mg:=MinimalGenerators(I);
12 r:=[];
13 n:=Length(mg);
14 for i in [1..n] do
15   for j in [i+1..n] do
16     r:=Union(r,R(mg[i],mg[j],s));
17   od;
18 od;
19 return r;
20 end;
```

Example 3.2, can be calculated as follows.

```

gap> s:=NumericalSemigroup(3,4);
<Numerical semigroup with 2 generators>
gap> I:=[3,5]+s;
<Ideal of numerical semigroup>
gap> ker(I);
[ [ 6, 4 ], [ 8, 6 ] ]
```

4. BASIS OF A \mathbf{K} -ALGEBRA

Let \mathbf{K} be a field and let $f_1(t), \dots, f_s(t) \in \mathbf{K}[t]$. Let $\mathbf{A} = \mathbf{K}[f_1, \dots, f_s]$, which is a subalgebra of $\mathbf{K}[t]$. Assume, without loss of generality, that f_i is monic for all $i \in \{1, \dots, s\}$. Given $f(t) =$

$\sum_{i=0}^p c_i t^i \in \mathbf{A}$, with $c_p \neq 0$, we set $d(f) = p$ and $M(f) = c_p t^p$, the *degree* and *leading monomial* of f , respectively. We also define $\text{supp}(f) = \{i \mid c_i \neq 0\}$, the *support* of f .

The set $d(\mathbf{A}) = \{d(f) \mid f \in \mathbf{A}\}$ is a submonoid of \mathbb{N} . We shall assume that $\lambda_{\mathbf{A}}(\mathbf{K}[t]/\mathbf{A}) < \infty$. This implies that $d(\mathbf{A})$ is a numerical semigroup. We say that $\{f_1, \dots, f_s\}$ is a *basis* of \mathbf{A} if $\{d(f_1), \dots, d(f_s)\}$ generates $d(\mathbf{A})$. Clearly, $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} if and only if $\mathbf{K}[M(f) \mid f \in \mathbf{A}] = \mathbf{K}[M(f_1), \dots, M(f_s)]$.

Proposition 4.1. *Given $f(t) \in \mathbf{K}[t]$, there exist $g(t) \in \mathbf{A}$ and $r(t) \in \mathbf{K}[t]$ such that the following conditions hold:*

- (1) $f(t) = g(t) + r(t)$,
- (2) if $g(t) \neq 0$ (respectively $r(t) \neq 0$), then $d(g) \leq d(f)$ (respectively $d(r) \leq d(f)$),
- (3) If $r(t) \neq 0$, then $\text{supp}(r(t)) \subseteq \mathbb{N} \setminus \langle d(f_1), \dots, d(f_s) \rangle$.

Proof. The assertion is clear if $f \in \mathbf{K}$. Suppose that $f \notin \mathbf{K}$ and let $f(t) = \sum_{i=0}^p c_i t^i$ with $p = d(f) > 0$.

- (1) If $p \notin \langle d(f_1), \dots, d(f_s) \rangle$, then we set $g^1 = 0, r^1 = c_p t^p$ and $f^1 = f - c_p t^p$.
- (2) If $p \in \langle d(f_1), \dots, d(f_s) \rangle$, then $t^p = M(f_1)^{\theta_1} \dots M(f_s)^{\theta_s}$, for some $(\theta_1, \dots, \theta_s) \in \mathbb{N}^s$ (this expression is not necessarily unique). We set $g^1 = c_p f_1^{\theta_1} \dots f_s^{\theta_s}, r^1 = 0$ and $f^1 = f - g^1$.

With this choice of g^1 and r^1 , we have $f = f^1 + g^1 + r^1, g^1 \in \mathbf{A}, r^1 \in \mathbf{K}[t]$, and the following conditions hold:

- (1) If $r^1 \neq 0$, then $\text{supp}(r^1) \subseteq \mathbb{N} \setminus \langle d(f_1), \dots, d(f_s) \rangle$.
- (2) If $f^1 \notin \mathbf{K}$, then $d(f^1) < d(f) = p$.

Then we restart with f^1 . Clearly there is $k \geq 1$ such that $f^k \in \mathbf{K}$. We set $g = g^1 + \dots + g^k + f^k$ and $r = r^1 + \dots + r^k$. \square

We denote the polynomial $r(t)$ of Proposition 4.1 by $R(f, \{f_1, \dots, f_s\})$. Note that this polynomial is not unique.

Proposition 4.2. *The set $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} if and only if $R(f, \{f_1, \dots, f_s\}) = 0$ for all $f \in \mathbf{A}$.*

Proof. Suppose that $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} and let $f \in \mathbf{A}$. Let $r(t) = R(f, \{f_1, \dots, f_s\})$. Then $r(t) \in \mathbf{A}$. If $r \neq 0$, then $d(r) \in \langle d(f_1), \dots, d(f_s) \rangle$, because $\{f_1, \dots, f_s\}$ is a basis, and this is a contradiction.

Conversely, given $0 \neq f \in \mathbf{A}$, if $d(f) \notin \langle d(f_1), \dots, d(f_s) \rangle$, then $R(f, \{f_1, \dots, f_s\}) \neq 0$, which is a contradiction. \square

Remark 4.3. Suppose that $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} . For all $f \in \mathbf{K}[t]$, $R(f, \{f_1, \dots, f_s\})$ is unique. Write $f = g_1 + r_1 = g_2 + r_2$, and suppose that $g_i, r_i, i \in \{1, 2\}$ satisfy conditions (1), (2) and (3) of Proposition 4.1. We have $g_1 - g_2 = r_2 - r_1 \in \mathbf{A}$. Hence $d(r_2 - r_1) \in d(\mathbf{A})$, because $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} . If $r_1 \neq r_2$, then $d(r_2 - r_1) \in \text{supp}(r_1) \cup \text{supp}(r_2)$. Thus by Proposition 4.1, $d(r_2 - r_1) \in \mathbb{N} \setminus \langle d(f_1), \dots, d(f_s) \rangle = \mathbb{N} \setminus d(\mathbf{A})$, which is a contradiction.

Let the notations be as above and let

$$\phi : \mathbf{K}[X_1, \dots, X_s] \longrightarrow \mathbf{K}[t], \quad \phi(X_i) = M(f_i), \quad \text{for all } i \in \{1, \dots, s\}.$$

Let $\{F_1, \dots, F_r\}$ be a generating system of the kernel of ϕ . We can choose F_i to be a binomial for all $i \in \{1, \dots, r\}$. If $F_i = X_1^{\alpha_1} \dots X_s^{\alpha_s} - X_1^{\beta_1} \dots X_s^{\beta_s}$, we set $S_i = f_1^{\alpha_1} \dots f_s^{\alpha_s} - f_1^{\beta_1} \dots f_s^{\beta_s}$. Observe that if $d = \sum_{k=1}^s \alpha_k^i d(f_k) = \sum_{k=1}^s \beta_k^i d(f_k)$, then $d(S_i) < d$.

Theorem 4.4. *The set $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} if and only if $R(S_i, \{f_1, \dots, f_s\}) = 0$ for all $i \in \{1, \dots, r\}$.*

Proof. Suppose that $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} . Since $S_i \in \mathbf{A}$ for all $i \in \{1, \dots, r\}$, we trivially obtain $R(S_i, \{f_1, \dots, f_s\}) = 0$.

For the sufficiency, assume that there is $f \in \mathbf{A}$ such that $d(f) \notin \langle d(f_1), \dots, d(f_s) \rangle$, and write

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

For all $\underline{\theta}$, if $c_{\underline{\theta}} \neq 0$, we set $p_{\underline{\theta}} = \sum_{i=1}^s \theta_i d(f_i) = d(f_1^{\theta_1} \cdots f_s^{\theta_s})$. Take $p = \max\{p_{\underline{\theta}} \mid c_{\underline{\theta}} \neq 0\}$ and let $\{\underline{\theta}^1, \dots, \underline{\theta}^l\}$ be the set of elements such that $p = d(f_1^{\theta_i^1} \cdots f_s^{\theta_i^s})$ for all $i \in \{1, \dots, l\}$. If $\sum_{i=1}^l c_{\underline{\theta}^i} M(f_1^{\theta_i^1} \cdots f_s^{\theta_i^s}) \neq 0$, then $p = d(f) \in \langle d(f_1), \dots, d(f_s) \rangle$, which by assumption is impossible. Hence $\sum_{i=1}^l c_{\underline{\theta}^i} M(f_1^{\theta_i^1} \cdots f_s^{\theta_i^s}) = 0$, which implies that $\sum_{i=1}^l c_{\underline{\theta}^i} X_1^{\theta_i^1} \cdots X_s^{\theta_i^s} \in \ker(\phi)$. Thus

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

with $\lambda_k \in \mathbf{K}[X_1, \dots, X_s]$ for all $k \in \{1, \dots, r\}$. This implies that

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

By hypothesis, $R(S_k, \{f_1, \dots, f_s\}) = 0$. So there exists an expression $S_k = \sum_{\underline{\beta}^k} c_{\underline{\beta}^k} f_1^{\beta_1^k} \cdots f_s^{\beta_s^k}$ with $d(f_1^{\beta_1^k} \cdots f_s^{\beta_s^k}) \leq d(S_k)$ for all $\underline{\beta}^k$ such that $c_{\underline{\beta}^k} \neq 0$. Finally we can write $f = \sum_{\underline{\theta}'} c_{\underline{\theta}'} f_1^{\theta_1'} \cdots f_s^{\theta_s'}$ with $\max\{d(f_1^{\theta_1'} \cdots f_s^{\theta_s'}) \mid c_{\underline{\theta}'} \neq 0\} < p$.

We now restart with the new expression of f . This process will stop, yielding a contradiction. \square

Algorithm 4.5. *Let the notations be as above.*

- (1) *If $R(S_k, \{f_1, \dots, f_s\}, \{f_1, \dots, f_s\}) = 0$ for all $k \in \{1, \dots, r\}$, then $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} .*
- (2) *If $r(t) = R(S_k, \{f_1, \dots, f_s\}, \{f_1, \dots, f_s\}) \neq 0$ for some $k \in \{1, \dots, r\}$, then we set $f_{s+1} = r(t)$, and we restart with $\{f_1, \dots, f_{s+1}\}$.*

Note that in this case, $\langle d(f_1), \dots, d(f_s) \rangle \subsetneq \langle d(f_1), \dots, d(f_s), d(f_{s+1}) \rangle$.

This process will stop, giving a basis of \mathbf{A} .

Suppose that $\{f_1, \dots, f_s\}$ is a basis of \mathbf{A} . We say that $\{f_1, \dots, f_s\}$ is a *minimal basis* of \mathbf{A} if $\{d(f_1), \dots, d(f_s)\}$ minimally generates the semigroup $d(\mathbf{A})$. We say that $\{f_1, \dots, f_s\}$ is a *reduced basis* of \mathbf{A} if $\text{supp}(f_i - M(f_i)) \in \mathbb{N} \setminus d(\mathbf{A})$ and f_i is monic for all $i \in \{1, \dots, s\}$.

Let $i \in \{1, \dots, s\}$. If $d(f_i)$ is in $\langle d(f_1), \dots, d(f_{i-1}), d(f_{i+1}), \dots, d(f_s) \rangle$, then the set obtained by removing f_i , $\{f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_s\}$, is also a basis of \mathbf{A} . Furthermore, by applying the division process of Proposition 4.1 to $f_i - M(f_i)$, we can always construct a reduced basis of \mathbf{A} .

Corollary 4.6. *Up to constants, the algebra \mathbf{A} 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 \mathbf{A} . Clearly $s = s'$, and equals the embedding dimension of $d(\mathbf{A})$. Let $i = 1$. There exists j_1 such that $d(f_1) = d(g_{j_1})$, because minimal generating systems of a numerical semigroup are unique.

Observe that $\text{supp}(f_1 - g_{j_1}) \subseteq \text{supp}(f_1 - M(g_{j_1})) = \text{supp}(f_1 - M(f_1)) \subseteq \mathbb{N} \setminus d(\mathbf{A})$. Thus, if $f_1 - g_{j_1} \notin \mathbf{K} \setminus \{0\}$, then $d(f_1 - g_{j_1}) \notin d(\mathbf{A})$, which is a contradiction because $f_1 - g_{j_1} \in \mathbf{A}$. The same argument shows that for all $i \geq 2$, there exists j_i such that $f_i - g_{j_i} \in \mathbf{K}$. \square

Corollary 4.7. *Let $\{f_1, \dots, f_s\}$ be a reduced basis of A . For all $i \in \{1, \dots, s\}$, $\text{supp}(f_i - M(f_i)) \subseteq G(d(\mathbf{A}))$.*

Example 4.8. We compute $d(\mathbf{A})$ for $\mathbf{A} = \mathbf{K}[t^6 + t, t^4]$; $f_1 = t^6 + t$ and $f_2 = t^4$. We start by computing the kernel of $\phi : \mathbf{K}[X_1, X_2] \rightarrow \mathbf{K}[t]$, with $\phi(X_1) = t^6$ and $\phi(X_2) = t^4$. This kernel is generated by $F_1 = X_2^3 - X_1^2$. Hence $S_1 = 2t^7 + t^2$. Since $7 \notin \langle 4, 6 \rangle$, then we add $f_3 = 2t^7 + t^2$ to our generating set.

In the next step $\phi : \mathbf{K}[X_1, X_2, X_3] \rightarrow \mathbf{K}[t]$, with $\phi(X_1) = t^6$, $\phi(X_2) = t^4$ and $\phi(X_3) = 2t^7$; $\ker \phi = (X_2^3 - X_1^2, X_3^2 - 4X_1X_2^2)$, whence $S_1 = f_3$ and $S_2 = f_3^2 - 4f_1f_2^2 = t^4 = f_2$. It turns out that $\mathbf{R}(S_1, \{f_1, f_2, f_3\}) = 0 = \mathbf{R}(S_2, \{f_1, f_2, f_3\})$, and consequently $\{f_1, f_2, f_3\}$ is a (reduced minimal) basis of \mathbf{A} . Also $d(\mathbf{A}) = \langle 4, 6, 7 \rangle$.

These computations can be performed with the numericalsgps GAP package.

```
gap> SemigroupOfValuesOfCurve_Global([t^6+t, t^4], "basis");
[ t^4, t^6+t, t^7+1/2*t^2 ]
```

Or if we just want to calculate $d(\mathbf{A})$:

```
gap> s:=SemigroupOfValuesOfCurve_Global([t^6+t, t^4]);;
gap> MinimalGenerators(s);
[ 4, 6, 7 ]
```

5. MODULES OVER \mathbf{K} -ALGEBRAS

Let the notations be as in Section 4. In particular $\{f_1, \dots, f_s\}$ is a set of polynomials of $\mathbf{K}[t]$ and $\mathbf{A} = \mathbf{K}[f_1, \dots, f_s]$. Let $\{F_1, \dots, F_r\}$ be a set of nonzero elements of $\mathbf{K}[t]$, and let $\mathbf{M} = \sum_{i=1}^r F_i \mathbf{A}$ be the \mathbf{A} -module generated by F_1, \dots, F_r . We set $d(\mathbf{M}) = \{d(F), F \in \mathbf{M} \setminus 0\}$.

If $F \in \mathbf{M}$ and $g \in \mathbf{A}$ then $gF \in \mathbf{M}$, hence $d(\mathbf{M})$ is a relative ideal of $d(\mathbf{A})$.

Definition 5.1. We say that $\{F_1, \dots, F_r\}$ is a basis of \mathbf{M} if and only if $d(\mathbf{M}) = \bigcup_{i=1}^r (d(F_i) + d(\mathbf{A}))$. Equivalently, $\{F_1, \dots, F_r\}$ is a basis of \mathbf{M} if and only if $\{d(F_1), \dots, d(F_r)\}$ is a basis of the ideal $d(\mathbf{M})$ of $d(\mathbf{A})$.

Theorem 5.2. Let $\{f_1, \dots, f_s, F_1, \dots, F_r\}$ be a set of nonzero polynomials of $\mathbf{K}[t]$. Let $\mathbf{A} = \mathbf{K}[f_1, \dots, f_s]$ and \mathbf{M} be the \mathbf{A} -module generated by $\{F_1, \dots, F_r\}$. Given $F \in \mathbf{K}[t]$, $F \neq 0$, there exist $g_1, \dots, g_r \in \mathbf{A}$ and $R \in \mathbf{K}[t]$ such that the following conditions hold.

- (1) $F = \sum_{i=1}^r g_i F_i + R$.
- (2) For all $i \in \{1, \dots, r\}$, if $g_i \neq 0$, then $d(g_i) + d(F_i) \leq d(F)$.
- (3) If $R \neq 0$, then $d(R) \leq d(F)$ and $d(R) \in \mathbb{N} \setminus \bigcup_{i=1}^r (d(F_i) + d(\mathbf{A}))$.

Proof. The assertion is clear if $F \in \mathbf{K}$. Suppose that $F \notin \mathbf{K}$ and let $F(t) = \sum_{i=0}^p c_i t^i$ with $p = d(f) > 0$.

In order to simplify notation, set $S = d(\mathbf{A})$ and $I = \bigcup_{i=1}^r (d(F_i) + S)$.

- (i) If $p \notin I$, then we set $g^1 = \dots = g^r = 0$, $R^1 = c_p t^p$ and $F^1 = F - R^1$.
- (ii) If $p \in I$, then $c_p t^p = c_{\theta_i} t^{s_i} M(F_i)$ for some $s_i \in S$ and some $i \in \{1, \dots, r\}$. Let $g \in \mathbf{A}$ such that $M(g) = c_{\theta_i} t^{s_i}$. We set $g_i^1 = g$, $g_j^1 = 0$ for all $j \neq i$, $R^1 = 0$ and $F^1 = F - gF_i$.

In this way, $F = F^1 + \sum_{i=1}^r g_i^1 F_i + R^1$, and the following conditions hold:

- (1) $g_i^1 \in \mathbf{A}$ for all $i \in \{1, \dots, r\}$.
- (2) If $R^1 \neq 0$, then $\text{supp}(R^1) \subseteq \mathbb{N} \setminus I$.
- (3) If $F^1 \notin \mathbf{K}$, then $d(F^1) < d(F) = p$.

Then we restart with F^1 . Clearly there is $k \geq 1$ such that $F^k \in \mathbf{K}$. We set $g_i = g_i^1 + \dots + g_i^k$ for all $i \in \{1, \dots, r\}$, and $R = R^1 + \dots + R^k + F^k$. \square

We denote the polynomial R of Theorem 5.2 by $R_{\mathbf{A}}(F, \{F_1, \dots, F_r\})$.

The following GAP code can compute $R_{\mathbf{A}}(f, \{F_1, \dots, F_r\})$. Here \mathbf{A} contains a basis of the algebra \mathbf{A} , and \mathbf{M} is $\{F_1, \dots, F_r\}$.


```

                                GAP CODE 2. reduce function
1  reduce:=function(A,M,f)
2    local gens,geni,cand,d, fact, c, r, s,a;
3    gens:=List(A, DegreeOfLaurentPolynomial);
4    s:=NumericalSemigroup(gens);
5    geni:=List(M,DegreeOfLaurentPolynomial);
6    if IsZero(f) then
7      return f;
8    fi;
9    d:=DegreeOfLaurentPolynomial(f);
10   c:=First([1..Length(geni)], i->d-geni[i] in s);
11   r:=f;
12   while c<>fail do
13     fact:=FactorizationsIntegerWRTList(d-geni[c],gens);
14     a:=M[c]*Product(List([1..Length(gens)],i->A[i]^fact[1][i]));
15     r:=r-LeadingCoefficient(r)*a/LeadingCoefficient(a);
16     if IsZero(r) then
17       return r;
18     fi;
19     d:=DegreeOfLaurentPolynomial(r);
20     c:=First([1..Length(geni)], i->d-geni[i] in s);
21   od;
22   return r/LeadingCoefficient(r);
23 end;

```

Proposition 5.3. *Let the notations be as in Theorem 5.2. The following conditions are equivalent:*

- (1) $\{F_1, \dots, F_r\}$ is a basis of \mathbf{M} .
- (2) For all $F \in \mathbf{M}$, $R_{\mathbf{A}}(F, \{F_1, \dots, F_r\}) = 0$.

Proof. Suppose that $\{F_1, \dots, F_r\}$ is a basis of \mathbf{M} and let $F \in \mathbf{M}$. If $R = R_{\mathbf{A}}(F, \{F_1, \dots, F_r\}) \neq 0$, then $d(R) \in \mathbb{N} \setminus \bigcup_{i=1}^r (d(F_i) + d(\mathbf{A})) = \mathbb{N} \setminus d(\mathbf{M})$. But $R \in \mathbf{M}$. This is a contradiction.

Conversely suppose that $R_{\mathbf{A}}(F, \{F_1, \dots, F_r\}) = 0$ for all $F \in \mathbf{M}$. Take $F \in \mathbf{M}$. If $d(F) \in \mathbb{N} \setminus \bigcup_{i=1}^r (d(F_i) + d(\mathbf{A}))$, then by construction, $R_{\mathbf{A}}(F, \{F_1, \dots, F_r\}) \neq 0$, which is a contradiction. \square

Let $F_1, \dots, F_r \in \mathbf{K}[t]$ and assume, without loss of generality, that F_1, \dots, F_r are monic. Assume also that $\{f_1, \dots, f_s\}$ is a reduced basis for \mathbf{A} . Let a_i be such that $M(F_i) = t^{a_i}$ for all $i \in \{1, \dots, r\}$. Let $(s_i, s_j) \in R(a_i, a_j)$. Then $s_i, s_j \in d(\mathbf{A})$. Then $s_i = \sum_{l=1}^s e_{il} d(f_l)$ and $s_j = \sum_{l=1}^s e_{jl} d(f_l)$, for some $e_{il}, e_{jl} \in \mathbb{N}$. Let $g_i = \prod_{l=1}^s f_l^{e_{il}}$, $g_j = \prod_{l=1}^s f_l^{e_{jl}} \in \mathbf{A}$. Note that these polynomials may not be unique, there are as many as factorizations of s_i and s_j , but this amount is finite. Then $d(g_i) = s_i$ and $d(g_j) = s_j$, and also $M(g_i) = t^{s_i}$ and $M(g_j) = t^{s_j}$ (recall that f_l is monic for all l). We have $t^{s_i} M(F_i) - t^{s_j} M(F_j) = 0$, whence $t^{s_i} \mathbf{e}_i - t^{s_j} \mathbf{e}_j \in \ker(\phi)$ with $\phi : \mathbf{A}^r \rightarrow \mathbf{M}$, $\phi(p_1, \dots, p_r) = \sum_{i=1}^r p_i M(F_i)$. If

$$F = g_i F_i - g_j F_j,$$

then $d(F) < a_i + s_i = a_j + s_j$. We call F an S -polynomial of (F_1, \dots, F_r) . Every element of $\ker(\phi)$ gives rise to an S -polynomial. Let $\text{SP}(F_1, \dots, F_r)$ be the set of S -polynomials of (F_1, \dots, F_r) constructed this way. The set $\text{SP}(F_1, \dots, F_r)$ has finitely many elements, though for our purposes it will be enough to choose a finite subset of $\text{SP}(F_1, \dots, F_r)$.

Let $n \in d(\mathbf{A})$. The set $\mathbf{Z}(n) = \{(n_1, \dots, n_s) \in \mathbb{N}^s \mid n = \sum_{i=1}^s n_i d(g_i)\}$ has finitely many elements (usually known as the set of factorizations of n). Let \preceq_{lex} denote the lexicographical ordering in \mathbb{N}^s .

We will consider $\text{MinSP}(F_1, \dots, F_r)$ the set of all elements $g_i F_i - g_j F_j \in \text{SP}(F_1, \dots, F_r)$ such that, with the above notation, $g_i = \prod_{l=1}^s f_l^{e_{il}}$ and $g_j = \prod_{l=1}^s f_l^{c_{jl}}$ with $(e_{i_1}, \dots, e_{i_s}) = \min_{\preceq_{\text{lex}}}(\mathbf{Z}(d(g_i)))$ and $(e_{j_1}, \dots, e_{j_s}) = \min_{\preceq_{\text{lex}}}(\mathbf{Z}(d(g_j)))$.

In Theorem 5.4 we give a characterization for a set $\{F_1, \dots, F_r\}$ of \mathbf{M} to be a basis of \mathbf{M} in terms of $\text{MinSP}(F_1, \dots, F_r)$.

Theorem 5.4. *Let $\{f_1, \dots, f_s, F_1, \dots, F_r\}$ be a set of nonzero polynomials of $\mathbf{K}[t]$. Let $\mathbf{A} = \mathbf{K}[f_1, \dots, f_s]$ and \mathbf{M} be the \mathbf{A} -module generated by $\{F_1, \dots, F_r\}$. The following conditions are equivalent:*

- (1) $\{F_1, \dots, F_r\}$ is a basis of \mathbf{M} ,
- (2) For all $F \in \text{MinSP}(F_1, \dots, F_r)$, $R_{\mathbf{A}}(F, \{F_1, \dots, F_r\}) = 0$.

Proof. In order to simplify notation, set $a_i = d(F_i)$ for all $i \in \{1, \dots, r\}$, and $S = d(\mathbf{A})$.

(1) implies (2) follows from Proposition 5.3.

For the other implication, we are going to show that for each $R \in \mathbf{M}$, $d(R) \in \bigcup_{i=1}^r (a_i + S)$.

Take $R \in \mathbf{M}$. If $R = 0$, we are done. Otherwise, we can find an expression of the form $R = g_1 F_1 + \dots + g_r F_r$ with $g_1, \dots, g_r \in \mathbf{A}$. Assume that $d(R) \in \mathbb{N} \setminus \bigcup_{i=1}^r (a_i + S)$. Set

$$p = \max_{i, g_i \neq 0} (a_i + \alpha_i).$$

Where $\alpha_i = d(g_i)$, $i \in \{1, \dots, r\}$. Then $p > d(R)$. We shall prove that there exists another expression of R , say $R = g'_1 F_1 + \dots + g'_r F_r$ with $p > p' = \max_{i, g'_i \neq 0} (a_i + d(g'_i))$. And this eventually leads to a contradiction, since the interval $\{d(R) + 1, \dots, p\}$ has finitely many elements.

Suppose, without loss of generality, that $p = \alpha_i + a_i$, $i \in \{1, \dots, l\}$ and $p > \alpha_i + a_i \in \{l+1, \dots, r\}$. Clearly $l \geq 2$. We prove by induction on l that we can rewrite R as $R = g'_1 F_1 + \dots + g'_r F_r$ with $p > p' = \max_{i, g'_i \neq 0} (d(g'_i) + a_i)$.

- (i) We first suppose that $l = 2$ and let $M(g_1) = c_{g_1} t^{\alpha_1}$, $M(g_2) = c_{g_2} t^{\alpha_2}$. It follows from the hypothesis that $c_{g_2} = -c_{g_1}$, and also that $\alpha_1 = s + s_1$, $\alpha_2 = s + s_2$ with $(s_1, s_2) \in R(a_1, a_2)$. Hence we have

$$c_{g_1} t^{\alpha_1} t^{a_1} + c_{g_2} t^{\alpha_2} t^{a_2} = c_{g_1} t^s (t^{s_1} t^{a_1} - t^{s_2} t^{a_2}).$$

Let $\tilde{g}_1, \tilde{g}_2 \in \mathbf{A}$ such that $M(\tilde{g}_1) = t^{s_1}$, $M(\tilde{g}_2) = t^{s_2}$, and $\tilde{g}_1 F_1 - \tilde{g}_2 F_2$ is a minimal S -polynomial. We have $d(\tilde{g}_1 F_1 - \tilde{g}_2 F_2) < s_1 + a_1 = \alpha_1 - s + a_1 = p - s$. By hypothesis, $R_{\mathbf{A}}(\tilde{g}_1 F_1 - \tilde{g}_2 F_2, \{F_1, \dots, F_r\}) = 0$, and thus

$$\tilde{g}_1 F_1 - \tilde{g}_2 F_2 = \bar{g}_1 F_1 + \bar{g}_2 F_2 + \dots + \bar{g}_r F_r,$$

with $d(\bar{g}_i F_i) \leq d(\tilde{g}_1 F_1 - \tilde{g}_2 F_2) < p - s$ for all $i \in \{1, \dots, r\}$. We can then rewrite R as

$$\begin{aligned} R &= (g_1 - c_{g_1} t^s \tilde{g}_1) F_1 + (g_2 - c_{g_2} t^s \tilde{g}_2) F_2 + c_{g_1} t^s \bar{g}_1 F_1 + c_{g_2} t^s \bar{g}_2 F_2 + \sum_{i \geq 3} g_i F_i \\ &= \sum_{i=1}^r g'_i F_i, \end{aligned}$$

with $d(g'_i F_i) < p$ for all $i \in \{1, \dots, r\}$.

- (ii) Now let $l > 2$ and let $M(g_i) = c_{g_i} t^{s_i}$ for all $i \in \{1, \dots, r\}$. We have $R = \sum_{i=1}^r g_i F_i = g_1 F_1 - \frac{c_{g_1}}{c_{g_2}} g_2 F_2 + (\frac{c_{g_1}}{c_{g_2}} + 1) g_2 F_2 + \sum_{i=3}^r g_i F_i$. It follows from (i) that $g_1 F_1 - \frac{c_{g_1}}{c_{g_2}} g_2 F_2 = \bar{g}_1 F_1 + \dots + \bar{g}_r F_r$ with $\max_{i, \bar{g}_i \neq 0} d(\bar{g}_i F_i) < p$. Hence $R = \tilde{g}_1 F_1 + \dots + \tilde{g}_r F_r$ with

- $\tilde{g}_1 = \bar{g}_1$,
- $\tilde{g}_2 = \bar{g}_2 + (\frac{c_{g_1}}{c_{g_2}} + 1) g_2$,
- $\tilde{g}_i = \bar{g}_i + g_i$ for $i \in \{3, \dots, r\}$.

In particular, the set $\{i \mid d(\tilde{g}_i F_i) = p\}$ has at most $l - 1$ elements, and it follows from the induction hypothesis that $R = g'_1 F_1 + \dots + g'_r F_r$ with $p > p' = \max_{i, g'_i \neq 0} (d(g'_i) + d(F_i))$. \square

Algorithm 5.5. Let $\mathbf{M} = \sum_{i=1}^r F_i \mathbf{A}$.

- (1) If for all $F \in \text{MinSP}(F_1, \dots, F_r)$, $R_{\mathbf{A}}(F, \{F_1, \dots, F_r\}) = 0$ then, by Theorem 5.4, $\{F_1, \dots, F_r\}$ is a basis of \mathbf{M} . Return $\{F_1, \dots, F_r\}$.
- (2) If $R_{\mathbf{A}}(F, \{F_1, \dots, F_r\}) \neq 0$ for some $F \in \text{SP}(F_1, \dots, F_r)$, then we set $F_{r+1} = R_{\mathbf{A}}(F, \{F_1, \dots, F_r\})$ and we restart with $\{F_1, \dots, F_{r+1}\}$.

Since $\mathbb{N} \setminus \bigcup_{i=1}^r (d(F_i) + S)$ has finitely many elements, then the procedure stops after a finite number of steps, returning a basis of \mathbf{M} .

GAP CODE 3. generatorsModule

```

1  generatorsModule:=function(A,M,t)
2    local S, gens, gM, a, b, da, db, i, j, rs, rd, rel, fcta, fctb, C,
3      pair, reduction, n;
4
5    gens:=List(A, DegreeOfLaurentPolynomial);
6    n:=Length(A);
7    S:=NumericalSemigroup(gens);
8
9    gM:=ShallowCopy(M);
10   C:=[];
11   for i in [1..Length(gM)] do
12     for j in [i+1..Length(gM)] do
13       Add(C, [gM[i], gM[j]]);
14     od;
15   od;
16   while C<>[] do
17     pair:=Remove(C, 1);
18     a:=pair[1];
19     b:=pair[2];
20     da:=DegreeOfLaurentPolynomial(a);
21     db:=DegreeOfLaurentPolynomial(b);
22     rs:=R(da, db, S);
23     reduction:=true;
24     for rel in rs do
25       fcta:=FactorizationsIntegerWRTList(rel[1], gens)[1];
26       fctb:=FactorizationsIntegerWRTList(rel[2], gens)[1];
27       rd:=reduce(A, gM,
28         a*Product(List([1..n], i->A[i]^fcta[i]))-
29         b*Product(List([1..n], i->A[i]^fctb[i])));
30       if not(IsZero(rd)) then
31         C:=Union(C, List(gM, x->[x, rd]));
32         Add(gM, rd);
33       fi;
34     od;
35   od;
36
37   reduction:=false;
38   while not reduction do
39     reduction:=true;

```

```

40   a:=First(gM, x->x<>reduce(A,Difference(gM,[x]),x));
41   if a<>fail then
42     rd:=reduce(A,Difference(gM,[a]),a);
43     if IsZero(rd) then
44       gM:=Difference(gM,[a]);
45     else
46       gM:=Union(Difference(gM,[a]),[rd]);
47     fi;
48     reduction:=false;
49   fi;
50 od;
51 return gM;
52 end;

```

Example 5.6. Let $\mathbf{A} = \mathbf{K}[t^6 + t, t^4]$ be as in Example 4.8, and recall that $\{f_1 = t^6 + t, f_2 = t^4, f_3 = t^7 + \frac{1}{2}t^2\}$ is a basis of $d(\mathbf{A})$. Let $\mathbf{M} = F_1\mathbf{A} + F_2\mathbf{A}$ with $F_1 = t^3$ and $F_2 = t^4$. We have $(3 + d(\mathbf{A})) \cap (4 + d(\mathbf{A})) = \{10, 11\} + d(\mathbf{A})$. Thus $R(3, 4) = \{(7, 6), (8, 7)\}$.

For $(7, 6)$, $7 = d(f_3)$ and $6 = d(f_1)$ (and these are the only factorizations of 7 and 6 in terms of the generators of $d(\mathbf{A})$). We have the S -polynomial

$$f_3F_1 - f_1F_2 = \left(t^7 + \frac{1}{2}t^2\right)t^3 - (t^6 + t)t^4 = -\frac{1}{2}t^5.$$

We take $F_3 = t^5$, and as $5 \notin \{3, 4\} + d(\mathbf{A})$, we add it to our system of generators, obtaining $\{F_1, F_2, F_3\}$.

Now for $(8, 7)$ we have the S -polynomial

$$f_2^2F_1 - f_3F_2 = t^8t^3 - \left(t^7 + \frac{1}{2}t^2\right)t^4 = -\frac{1}{2}t^6.$$

Set $F_4 = t^6$. As $6 \notin \{3, 4, 5\} + d(\mathbf{A})$, we add it to our generating set: $\{F_1, F_2, F_3, F_4\}$. One can show that any other S -polynomial with respect to this new generating system reduces to zero, and thus $\{F_1, F_2, F_3, F_4\}$ is a basis for $d(\mathbf{M})$.

```

gap> A:=SemigroupOfValuesOfCurve_Global([t^6+t,t^4],"basis");
[ t^4, t^6+t, t^7+1/2*t^2 ]
gap> M:=[t^3,t^4];;
gap> generatorsModule(A,M,t);
[ t^3, t^4, t^5, t^6 ]
gap> SetInfoLevel(InfoNumSgps,2);
gap> generatorsModule(A,M,t);
#I new generator t^5 of degreee 5
#I new generator t^6 of degreee 6
#I Reducing...
[ t^3, t^4, t^5, t^6 ]

```

6. MODULE OF KÄHLER DIFFERENTIALS

Let $\{f_1, \dots, f_r\}$ be a set of polynomials of $\mathbf{K}[t]$ and $\mathbf{A} = \mathbf{K}[f_1, \dots, f_r]$. We shall assume that $\mathbb{N} \setminus d(\mathbf{A})$ is a finite set, in particular $d(\mathbf{A})$ is a numerical semigroup. We shall denote it by S . Let $F_i = f_i'(t)$ for all $i \in \{1, \dots, r\}$, and let $\mathbf{M} = F_1\mathbf{A} + \dots + F_r\mathbf{A}$. We know that the set $I = d(\mathbf{M}) = \{d(F) \mid F \in \mathbf{M}\}$ is a relative ideal of S .

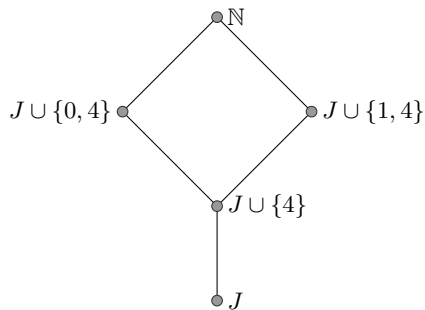
Given $g \in \mathbf{A}$, we have $g'(t) \in \mathbf{M}$. In particular, if $s \in S$, then $s - 1 \in I$. We say that $s - 1$ is an *exact degree*. We call the other elements of I *non exact degrees* of \mathbf{M} . We denote by $\text{NE}(\mathbf{M})$ the set of non exact degrees, that is

$$\text{NE}(\mathbf{M}) = \{i \in I \mid i + 1 \notin S\}.$$

Let $\text{ne}(\mathbf{M})$ be the cardinality of $\text{NE}(\mathbf{M})$. It follows that $\text{ne}(\mathbf{M}) \leq g(S)$, the genus of S .

Example 6.1. Let $x(t)$ and $y(t)$ be polynomials of degree 3 and 4 respectively. As $\gcd(3, 4) = 1$, $\{x(t), y(t)\}$ is a basis for $\mathbf{A} = \mathbb{K}[x(t), y(t)]$ and $S = d(\mathbf{A}) = \langle 3, 4 \rangle$. Set $\mathbf{M} = x'(t)\mathbf{A} + y'(t)\mathbf{A}$. Then $I = d(\mathbf{M})$ contains the ideal $J = (2, 3) + S$. The lattice of ideals of S containing J is the following.

```
gap> s:=NumericalSemigroup(3,4);;
gap> oi:=overIdeals([2,3]+s);
[ <Ideal of numerical semigroup>, <Ideal of numerical semigroup>,
<Ideal of numerical semigroup>, <Ideal of numerical semigroup>,
<Ideal of numerical semigroup> ]
gap> List(oi,MinimalGenerators);
[ [ 2, 3 ], [ 0, 1, 2 ], [ 0, 2 ], [ 1, 2, 3 ], [ 2, 3, 4 ] ]
```



The set of non exact elements for each ideal is:

```
gap> List(oi,non exactElements);
[ [ ], [ 0, 1, 4 ], [ 0, 4 ], [ 1, 4 ], [ 4 ] ]
```

And all these ideals can be realized as $d(M)$ for some $x(t), y(t)$.

- $J = (2, 3) + S = I$ for $(x(t), y(t)) = (t^3, t^4)$.
- $J \cup \{4\} = (2, 3, 4) + S = I$ for $(x(t), y(t)) = (t^3 + t^2, t^4)$.
- $J \cup \{0, 4\} = (0, 2) + S = I$ for $(x(t), y(t)) = (t^3, t^4 + t)$.
- $J \cup \{1, 4\} = (1, 2, 3) + S = I$ for $(x(t), y(t)) = (t^3, t^4 + t^2)$.
- $N = J \cup \{0, 1, 4\} = (0, 1, 2) + S = I$ for $(x(t), y(t)) = (t^3 + t, t^4)$.

```
gap> A:=[t^3,t^4];;
gap> generatorsKhalerDifferentials(A,t);
[ t^2, t^3 ]
gap> A:=[t^3+t^2,t^4];;
gap> generatorsKhalerDifferentials(A,t);
[ t^2+2/3*t, t^3, t^4 ]
gap> A:=[t^3,t^4+t];;
gap> generatorsKhalerDifferentials(A,t);
[ 1, t^2 ]
gap> A:=[t^3,t^4+t^2];;
gap> generatorsKhalerDifferentials(A,t);
[ t, t^2, t^3 ]
gap> A:=[t^3+t,t^4];;
gap> generatorsKhalerDifferentials(A,t);
```

[1, t, t^2]

Proposition 6.2. *Let the notations be as above. If S is symmetric, then $\text{ne}(\mathbf{M}) \leq \frac{F(S)}{2}$.*

Proof. In fact, the cardinality of $\{s \mid s+1 \notin S\}$ is, in this case, $\frac{F(S)}{2}$ (see for instance [11, Chapter 3]). \square

In the following we shall suppose that $r = 2$, and that \mathbf{K} is an algebraically closed field of characteristic zero. We shall also use the notation $X(t), Y(t)$ for $f_1(t), f_2(t)$ and we recall that $\lambda_{\mathbf{A}}(\mathbf{K}[t]/\mathbf{K}[X(t), Y(t)]) < +\infty$. Let $f(X, Y)$ be the monic generator of the kernel of the map $\psi : \mathbf{K}[X, Y] \rightarrow \mathbf{K}[t], \psi(X) = X(t), \psi(Y) = Y(t)$. Then f has one place at infinity (see [1]).

We shall denote $S = d(\mathbf{A})$ by $\Gamma(f)$. Given a nonzero polynomial $g(X, Y) \in \mathbf{K}[X, Y]$, the element $\text{deg}_t g(X(t), Y(t))$ of $\Gamma(f)$ coincides with the rank over \mathbf{K} of the \mathbf{K} -vector space $\frac{\mathbf{K}[X, Y]}{(f, g)}$ (see for instance [4, Chapter 4]).

Let f_X, f_Y denote the partial derivatives of f and let $(f - \lambda)_{\lambda \in \mathbf{K}}$ be the family of translates of f . Let $\lambda \in \mathbf{K}$ and let $V(f - \lambda) = \{P \in \mathbf{K}^2 \mid (f - \lambda)(P) = 0\}$ be the curve of \mathbf{K}^2 defined by $f - \lambda$. Given $P = (a, b) \in V(f - \lambda)$, we denote by μ_P^λ the *local Milnor number* of $(f - \lambda)$ at P (if $\mathfrak{m}_P = (X - a, Y - b)$, then μ_P^λ is defined to be the rank of the \mathbf{K} -vector space $\mathbf{K}[X, Y]_{\mathfrak{m}_P} / (f, g)\mathbf{K}[X, Y]_{\mathfrak{m}_P}$). We say that $f - \lambda$ is *singular* at P if $\mu_P^\lambda > 0$, otherwise, P is a *smooth point* of $f - \lambda$. We say that $f - \lambda$ is *singular* if $f - \lambda$ has at least one singular point. In our setting, if $f - \lambda$ is singular, then it has a finite number of singular points. Furthermore, there is a finite number of translates of f which are singular. Let $\mu(f) = \dim_{\mathbf{K}} \frac{\mathbf{K}[X, Y]}{(f_X, f_Y)}$, then

$$\mu(f) = \sum_{\lambda \in \mathbf{K}} \sum_{P \in V(f - \lambda)} \mu_P^\lambda,$$

that is, $\mu(f)$ is the sum of local Milnor numbers at the singular points of the translates of f .

Write

$$X(t) = t^n + \alpha_1 t^{n-1} + \cdots + \alpha_n$$

and

$$Y(t) = t^m + \beta_1 t^{m-1} + \cdots + \beta_m$$

and suppose, without loss of generality, that $m < n$ and also (by taking the change of variables $t_1 = t + \frac{\beta_1}{m}$) that $\beta_1 = 0$. We can express $f(X, Y)$ as $f(X, Y) = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$. Clearly $n, m \in \Gamma(f)$. Let d be a divisor of n and let $g(X, Y)$ be a Y -monic polynomial of degree $\frac{n}{d}$ in Y . Let

$$f = g^d + c_1(X, Y)g^{d-1} + \cdots + c_d(X, Y)$$

with $\text{deg}_Y c_i(X, Y) < \frac{n}{d}$ for all $i \in \{1, \dots, d\}$, the expansion of f with respect to g . We say that g is a *dth approximate root* of f if $c_1(X, Y) = 0$. It is well known that a *dth approximate root* of f exists and it is unique. We denote it by $\text{App}(f, d)$. With these notations we have the following algorithm that computes a set of generators of $\Gamma(f)$ (see for instance [3]).

Algorithm 6.3. *Let $r_0 = m = d_1$ and let $r_1 = n$. Let $d_2 = \text{gcd}(r_0, r_1) = \text{gcd}(r_1, d_1)$ and let $g_2 = \text{App}(f, d_2)$. We set $r_2 = d(g_2(X(t), Y(t)))$ and $d_3 = \text{gcd}(r_2, d_2)$ and so on.*

It follows from [1] that there exists $h > 1$ such that $d_{h+1} = 1$, and also that $\Gamma(f) = \langle r_0, r_1, \dots, r_h \rangle$.

We set $e_k = \frac{d_k}{d_{k+1}}$ for all $k \in \{1, \dots, h\}$.

The following Proposition gives the main properties of $\Gamma(f)$.

Proposition 6.4. *Let f, r_i, d_i , and e_i be defined as above. We have the following:*

- (1) $\Gamma(f)$ is free with respect to the arrangement (r_0, r_1, \dots, r_h) .
- (2) $r_k d_k > r_{k+1} d_{k+1}$ for all $k \in \{1, \dots, h\}$.

- (3) $d(f_y(x(t), y(t))) = \sum_{i=1}^h (e_i - 1)r_i$.
(4) $C(\Gamma(f)) = \mu(f) = d(f_y(x(t), y(t))) - n + 1$.

Proof. See [4]. □

Let $\mathbf{B} = \frac{\mathbf{K}[X, Y]}{(f)}$ and let x, y be the images of X, Y in \mathbf{B} . Let $\mathbf{N} = \mathbf{B}dx + \mathbf{B}dy$ be the \mathbf{B} -module generated by $\{dx, dy\}$, and let $\bar{\mathbf{B}}$ be the integral closure of \mathbf{B} . Let $\tilde{\mathbf{N}} = \bar{\mathbf{B}}dx + \bar{\mathbf{B}}dy$. Let $\nu(f) = \dim_{\mathbf{K}} \frac{\mathbf{K}[X, Y]}{(f, f_X, f_Y)} = \dim_{\mathbf{K}} \frac{\mathbf{B}}{(f_X, f_Y)}$. If we denote by $\ell(\cdot)$ the length of the module, then we have the following property.

Proposition 6.5. [6, Corollary 2] *Let f be defined as above.*

$$\nu(f) = \ell\left(\tilde{\mathbf{N}}/\mathbf{N}\right) + \frac{\mu(f)}{2}.$$

In our setting, $\mathbf{B} \simeq \mathbf{K}[X(t), Y(t)] = \mathbf{A}$, hence $\bar{\mathbf{B}} \simeq \bar{\mathbf{A}} = \mathbf{K}[t]$, where $\bar{\mathbf{A}}$ is the integral closure of \mathbf{A} . It follows that \mathbf{N} is isomorphic to $\mathbf{M} = x'(t)\mathbf{A} + y'(t)\mathbf{A}$ and also that $\tilde{\mathbf{N}}$ is isomorphic to $\tilde{\mathbf{M}} = x'(t)\mathbf{K}[t] + y'(t)\mathbf{K}[t] = \{g'(t), g(t) \in \mathbf{K}[t]\}$.

Note that if $g(X, Y) \in \mathbf{K}[X, Y]$, then $\frac{d}{dt}g(X(t), Y(t)) \in \mathbf{M}$, whence $d(\frac{d}{dt}g(X(t), Y(t))) \in I = d(\mathbf{M})$. It follows that $\{s - 1 \mid s \in \Gamma(f)\} \subseteq I$ and $d(\frac{d}{dt}g(X(t), Y(t)))$ is an exact element. In particular, $\ell(\frac{\tilde{\mathbf{N}}}{\mathbf{N}})$ is the cardinality of the set $\{s \in G(\Gamma(f)) \mid s - 1 \notin S\}$. This cardinality is nothing but $g(\Gamma(f)) - \text{ne}(\mathbf{M}) = \frac{\mu(f)}{2} - \text{ne}(\mathbf{M})$, and it follows that:

- (1) $\nu(f) = \mu(f) = C(\Gamma(f))$ if and only if $\text{ne}(\mathbf{M}) = 0$, that is, every element of I is exact;
- (2) $\nu(f) = \frac{\mu(f)}{2}$ if and only if $\text{ne}(\mathbf{M}) = g(\Gamma(f))$.

In the following, we shall introduce the notion of characteristic exponents of f . Then we shall prove that, after possibly a change of variables, the curve $V(f)$ has a parametrization in one of the following forms:

- (1) $X(\tau) = \tau^n, Y(\tau) = \tau^m$ (hence the equation of the curve is of the form $W^n - Z^m$),
- (2) $X(\tau) = \tau^n + c_\lambda \tau^\lambda + \dots, Y(\tau) = \tau^n$ and $m + \lambda \notin \Gamma(f)$ (hence the degree of $mX'(\tau)Y(\tau) - nX(\tau)Y'(\tau)$ is a non exact element of I).

We will need to this end this technical Lemma.

Lemma 6.6. *Let $q(t) = t + \sum_{i \geq 1} c_i t^{-i} \in \mathbf{K}((t))$ and define the map $l : \mathbf{K}((T)) \rightarrow \mathbf{K}((t))$, $\alpha(T) \mapsto \alpha(q(t))$. In particular, $l(T) = q(t)$. Then l is an isomorphism.*

Proof. We clearly have $l(\alpha(T) + \beta(T)) = l(\alpha(T)) + l(\beta(T))$ and $l(\alpha(T)\beta(T)) = l(\alpha(T))l(\beta(T))$ for all $\alpha(T), \beta(T) \in \mathbf{K}((T))$. Furthermore, $l(1) = 1$ and $\ker(l) = \{0\}$. We shall now construct the inverse of l by proving that $t = T + b_1 T^{-1} + b_2 T^{-2} + \dots$ for some $b_i \in \mathbf{K}$. We shall do this by induction on $k \geq 1$. More precisely we shall prove that for all $k \geq 1$, there exist $b_k \in \mathbf{K}$ such that $\deg_t(t - l(T + b_1 T^{-1} + \dots + b_k T^{-k})) \leq -k - 1$. We shall use the fact that for all $k \in \mathbb{Z}$, we can write

$$l((q(t))^k) = t^k + \sum_{i \geq 1} c_i^{(k)} t^{k-i-1}$$

for some $c_i^{(k)} \in \mathbf{K}$. If $k = 1$, then we set $b_1 = -c_1$. We have $t - l(T) - b_1 l(T^{-1}) = (-c_1 - b_1)T^{-1} - \sum_{i \geq 2} c_i^{(1)} t^{-i} = \sum_{i \geq 2} -c_i^{(1)} t^{-i}$. Hence the assertion is clear. Suppose that the assertion is true for k and let us prove it for $k + 1$. By hypothesis we have

$$t = l(T + b_1 T^{-1} + \dots + b_k T^{-k}) + \sum_{i \geq 1} c_i^{(k)} t^{-k-i}.$$

Then we set $b_{k+1} = c_1^{(k)}$. But $l(c_1^{(k)}(q(t))^{-k-1}) = c_1 t^{-k-1} + \sum_{i \geq 1} c_i^{(k+1)} t^{-k-2-i}$. Hence $t = l(T + b_1 T^{-1} + \dots + b_{k+1} T^{-k-1}) + \sum_{i \geq 1} c_i^{(k+1)} t^{-k-1-i}$. This proves the assertion for $k + 1$.

Let $q_1(T) = T + \sum_{k \geq 1} b_k T^{-k}$ and set $l_1(\gamma(t)) = \gamma(q_1(T))$ (in particular $l_1(t) = q_1(T)$). Since $\deg_t(t - l(q_1(T))) \leq -k$ for all $k \geq 0$, then $t = l(q_1(T))$. This proves that l is surjective, hence an isomorphism. Note that $l_1 = l^{-1}$ because $l(l_1(t)) = t$. \square

Let us make the following change of variables

$$T = t(1 + \beta_2 t^{-2} + \dots + \beta_m t^{-m})^{\frac{1}{m}} = t \left(1 + \frac{1}{m} \beta_2 t^{-2} + \dots \right) = q(t).$$

This change of variables defines a map $l : \mathbf{K}((T)) \rightarrow \mathbf{K}((t))$, $l(T) = q(t)$. It follows from Lemma 6.6 that l is an isomorphism. Let $X_1(T) = X(l^{-1}(t))$ and $Y_1(T) = Y(l^{-1}(t))$. We have

$$Y_1(T) = T^m \text{ and } X_1(T) = T^n + \sum_{p < n} c_p T^p,$$

for some $c_p \in \mathbf{K}$, and we can easily verify that for all $g(X, Y) \in \mathbf{K}[X, Y]$, $d(g(X(t), Y(t)))$ is also the degree in T of $g(X_1(T), Y_1(T))$. Furthermore, $\frac{d}{dt}(g(X(t), Y(t))) = \frac{d}{dT}(g(X_1(T), Y_1(T))) \frac{dT}{dt}$.

Recall that the Newton-Puiseux exponents of f are defined as follows: let $m_1 = -n$ and let $D_2 = \gcd(m, n) = d_2$. For all $i \geq 2$ define $-m_i = \max\{p \mid D_i \nmid p\}$ and $D_{i+1} = \gcd(D_i, m_i)$. We have $D_{h+1} = d_{h+1} = 1$ and $D_i = d_i$ for all $i \in \{1, \dots, h\}$ (the d_i where defined in Algorithm 6.3).

The Newton-Puiseux exponents are related to the sequence r_0, \dots, r_h by the following relation: $r_0 = m$, $r_1 = n$, and for all $k \geq 1$, $-r_{k+1} = -r_k e_k + (m_{k+1} - m_k)$ where we recall that $e_k = \frac{d_k}{d_{k+1}}$ for all $k \in \{1, \dots, h\}$. In particular, $r_2 = r_1 e_1 + m_2 - m_1 = r_1 e_1 - m_2 - r_1 = (e_1 - 1)r_1 - m_2$. Hence $-m_2 < r_2$.

Let $\lambda = \max\{p \mid p < n, c_p \neq 0\}$ and suppose that $\lambda > -\infty$. We have:

$$X_1(T) = T^n + c_\lambda T^\lambda + \dots \text{ and } Y_1(T) = T^m.$$

The hypothesis on λ implies that $c_\lambda \neq 0$. Let

$$W(T) = mX_1'(T)Y_1(T) - nY_1'(T)X_1(T).$$

We have $W(T) = (m\lambda - nm)c_\lambda T^{m+\lambda-1} + \dots$. If $m + \lambda \notin \Gamma(f)$, then $m + \lambda - 1$ is a non exact degree. Suppose that $m + \lambda \in \Gamma(f)$. We have then the following two possibilities.

- (1) $\lambda > -m_2$. In this case, $d_2 \mid \lambda$. Hence λ is in the group generated by n, m . Then $m + \lambda = an + bm$ for some $a, b \in \mathbb{N}$.
- (2) $\lambda = -m_2$. In this case, $m + \lambda = m - m_2 = an + bm + cr_2$ for some $a, b, c \in \mathbb{N}, c \neq 0$. But $m - m_2 = m + r_2 - (e_1 - 1)r_1$. Thus, $m + r_2 - (e_1 - 1)r_1 = an + bm + cr_2$. If $c \geq 1$, then $m - (e_1 - 1)r_1 = an + bm + (c - 1)r_2$, which is a contradiction because $m - (e_1 - 1)r_1 = m - (e_1 - 1)n < 0$. It follows that $c = 0$, whence $m + r_2 - (e_1 - 1)r_1 = an + bm$, and $r_2 = (a + e_1 - 1)n + (b - 1)m$, but $d_2 = \gcd(n, m)$ does not divide r_2 . This is again a contradiction.

It follows that $\lambda < -m_2$ and $m + \lambda = an + bm$ for some $a, b \in \mathbb{N}$. Since $n > m > \lambda$ then $a \leq 1$. Furthermore, if $a = 1$, then $b = 0$. Hence one of the following conditions holds.

- (1) $m + \lambda = n$. Let in this case $Y_2 = Y_1 + \alpha, \alpha \in \mathbf{K}^*$. We have

$$\bar{W}(T) = mX_1'(T)Y_2(T) - nY_2'(T)X_1(T) = [(m\lambda - nm)c_\lambda - \alpha mn]T^{n-1} + \dots$$

Hence, if $\alpha = \frac{\lambda - n}{n}c_\lambda = -\frac{m}{n}c_\lambda$, then $\bar{W}(T)$ has degree strictly less than $n - 1$. As an example of this case, let $X(t) = t^9 + t^5, Y(t) = t^4$. We have $W(t) = 16t^8$ and $8 + 1 = 9 \in d(\mathbf{A})$. If $\bar{Y} = t^4 + \frac{4}{9}$, then $\bar{W}(t) = mX'(t)\bar{Y}(t) - n\bar{Y}'(t)X(t) = \frac{-80}{9}t^4$ and $4 + 1 \notin d(\mathbf{A})$.

- (2) $m + \lambda = \theta m$. In this case, $\lambda = (\theta - 1)m$. The change of variables $X_2 = X_1 - Y_1^{\theta-1}, Y_2 = Y_1$ is such that either $(X_2, Y_2) = (T^n, T^m)$ or $X_2 = T^n + c_{\lambda_1} T^{\lambda_1} + \dots, Y_2 = T^m$ with $\lambda_1 < \lambda$. As an example of this case, let $X(t) = t^7, Y(t) = t^4 + t$. We have $W(t) = -21t^7$ and $7 + 1 = 8 = 2.4 \in d(\mathbf{A})$. Let $Y_1 = T^4$. Then $T^4 = t^4 + t, T = t(t^{-3} + 1)^{\frac{1}{4}}$, and

$X_1(T) = T^7 - \frac{1}{4}T^4 + \frac{7}{16}T + \dots$. If $X_2 = X_1 + \frac{1}{4}Y_1, Y_2 = Y_1$, then $X_2 = T^7 + \frac{7}{16}T + \dots, Y_2 = T^4$ and $mX_2'(T)Y_2(T) - nY_2'(T)X_2(T) = \frac{21}{2}T^4 + \dots$, with $4 + 1 = 5 \notin d(\mathbf{A})$.

We shall prove that these two processes will eventually stop. This is clear for the first case since we are constructing a strictly increasing sequence of nonnegative integers. In the second case, if $h \geq 2$ then this is clear since the set of integers in the interval $[\lambda, -m_2]$ is finite. Suppose that $h = 1$, that is, $\gcd(m, n) = 1$. If the process is infinite, then after a finite number of steps we will obtain a new parametrization of the curve of the form $\tilde{X} = T^n + \alpha T^{-l} + \dots, \tilde{Y} = T^m$ with $l > nm$, which is a contradiction.

It follows that either we get a parametrization (τ^n, τ^m) of the curve $V(f)$ (which means that the equation of this curve is $W^n - Z^m$ with $\mathbf{K}[X, Y] \simeq \mathbf{K}[Z, W]$ and $\gcd(n, m) = 1$), or we get a new parametrization $Z(t) = t^n + a_1 t^{\alpha_1} + \dots + a_n, W(t) = t^m + b_1 t^{\beta_1} + \dots + b_m$ such that the degree of $W(t) = mZ'(t)W(t) - nW'(t)Z(t)$ is a non exact element of I .

We then get the following result.

Theorem 6.7. (see also [2]) *Let $X(t) = t^n + a_1 t^{n-1} + \dots + a_n, Y(t) = t^m + b_1 t^{m-1} + \dots + b_m$ be the equations of a polynomial curve in \mathbf{K}^2 and let $f(X, Y)$ be the minimal polynomial of $X(t), Y(t)$, that is, $f(X, Y)$ is the resultant in t of $(X - X(t), Y - Y(t))$. Let $\mathbf{M} = X'(t)\mathbf{A} + Y'(t)\mathbf{A}$ be the \mathbf{A} -module generated by $X'(t), Y'(t)$. The following conditions are equivalent.*

- i) *The equality $\mu(f) = \nu(f)$ holds.*
- ii) *Every element of the ideal $I = d(\mathbf{M})$ is exact.*
- iii) *The integers n and m are coprime and there exist an isomorphism $\mathbf{K}[X, Y] \rightarrow \mathbf{K}[Z, W]$ such that the image of $f(X, Y)$ is $W^n - Z^m$.*

Proof. i) \iff ii) is clear and ii) \implies iii) results from the calculations above. Finally iii) \implies i) because $W^n - Z^m \in (W^{n-1}, Z^{m-1})$. \square

Let the notations be as above and let $W(t) = mX'(t)Y(t) - nY'(t)X(t)$.

If $W(t) = 0$, then $mX'(t)Y(t) = nY'(t)X(t)$. Hence $Y(t)^n - X(t)^m = 0$. In particular, $f(X, Y) = Y^n - X^m$.

If $W(t) \neq 0$ and $W(t)$ is exact, then similar calculations as above show that there exists a change of variables in such a way that the new W is either 0 or its degree is a non exact element. Assume that $f(X, Y)$ is not equivalent to a quasi-homogeneous polynomial, in particular we may assume that $W(t)$ is not exact. In the following we shall give a bound for the number of non exact elements of I .

Proposition 6.8. *Let the notations be as above. If $\text{ne}(\mathbf{M}) > 0$ then $\text{ne}(\mathbf{M}) \geq 2^{h-1}$.*

Proof. Consider as above the parametrization $X(T) = T^n + c_\lambda T^\lambda + \dots, Y(T) = T^m$ and let $d(W) = m + \lambda - 1$. We have $m + \lambda \notin \Gamma(f)$. Furthermore, $\lambda \geq -m_2$. Let $g_i(X, Y) = \text{App}(f, d_i)$ for all $i \in \{1, \dots, h\}$. We have two cases.

- (1) $\lambda > -m_2$. We have $m + \lambda = -am + bn$ with $a, b \in \mathbb{N}, a > 0, 0 \leq b \leq e_1$. Hence, for all $(\alpha_2, \dots, \alpha_h) \in \mathbb{N}^{h-1}$, if $\alpha_i < e_i$, then for every $i \in \{2, \dots, h\}$, the degree of $g_2^{\alpha_2} \cdots g_h^{\alpha_h} W$ is not exact, hence $\text{ne}(\mathbf{M}) \geq 2^{h-1}$.
- (2) $\lambda = -m_2$. We have $m + \lambda = m - m_2 = -am + bn + cr_2$ with $a, b, c \in \mathbb{N}, a > 0, 0 \leq b < e_1, 0 \leq c < e_2$. But $-m_2 = r_2 - (e_1 - 1)r_1$. Thus $m + r_2 - (e_1 - 1)r_1 = -am + bn + cr_2$, and since $(c - 1)r_2$ is not divisible by d_2 , we get $c = 1$, whence $(a + 1)m = (e_1 - 1 + b)r_1 = (e_1 - 1 + b)n$. If $b = 0$, then $(e_1 - 1)n$ is divisible by m , which is a contradiction. Hence $e - 1 - 1 + b \geq 2$, which implies that $a \geq 2$. Finally $m + \lambda = -am + bn + r_2$ with $a \geq 2$. Note that $d(YW) = -(a - 1)m + bn + r_2$, and thus $d(YW)$ is not exact. Furthermore, for all $(\alpha_3, \dots, \alpha_h) \in \mathbb{N}^{h-2}$, if $\alpha_i < e_i$ for all $i \in \{3, \dots, h\}$, then the degree of $Y g_3^{\alpha_3} \cdots g_h^{\alpha_h} W$ is not exact. It follows that $\text{ne}(\mathbf{M}) \geq 2^{h-1}$. \square

Corollary 6.9. *With the notations above. We have the following.*

- (1) If $\text{ne}(\mathbf{M}) = 1$, then $h = 1$, that is, $S = \langle m, n \rangle$ with $\gcd(m, n) = 1$. Furthermore, $\text{NE}(\mathbf{M}) = \{\mathbf{F}(\Gamma(f)) - 1\}$.
- (2) If $\text{ne}(\mathbf{M}) = 2$, then $h \in \{1, 2\}$, that is, either $\Gamma(f) = \langle m, n \rangle$ with $\gcd(m, n) = 1$ or $\Gamma(f) = \langle m, n, r_2 \rangle$ with $d_3 = 1$. Furthermore, if $h = 1$ (respectively $h = 2$), then $\text{NE}(\mathbf{M})$ is either $\{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - m - 1\}$ or $\{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - n - 1\}$ (respectively $\text{NE}(\mathbf{M})$ is either $\{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - n - 1\}$ or $\{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - m - 1\}$ or $\{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - r_2 - 1\}$).

Proof. (1) The first assertion results from Proposition 6.8, and obviously $\text{NE}(\mathbf{M}) = \{m + \lambda - 1\}$. If $m + \lambda < \mathbf{F}(\Gamma(f))$ then $m + \lambda = -am + bn$ with $a \geq 1$ and $b \leq m - 1$. If $a > 1$ then XW is not exact and $XW \neq W$. This is a contradiction. If $a = 1$ then $b < m - 1$ (otherwise $m + \lambda = -a + (m - 1)n = \mathbf{F}(\Gamma(f))$ which contradicts the hypothesis). But YW is not exact and $YW \neq W$. This is again a contradiction.

(2) The first assertion results from Proposition 6.8. To prove the second assertion, let W_1 have a non exact degree with $d(W_1) < \mathbf{F}(\Gamma(f)) - 1$ and $d(W_1)$ is minimal in $\text{ne}(\mathbf{M})$. Suppose first that $h = 1$. We have $d(W_1) + 1 = -am + bn$ with $a \geq 1$ and $0 \leq b \leq m - 1$. If $a \geq 2$ and $b < m - 1$, then XW_1, YW_1 have also non exact degrees, and thus $\text{ne}(\mathbf{M}) \geq 3$, which is a contradiction. Consequently either $a = 1$ or $b = m - 1$. If $a = 1$, then $b < m - 1$, whence $YW_1, \dots, Y^{m-1-b}W_1$ have also non exact degrees. This forces b to be equal to $m - 2$. Consequently $\text{NE}(\mathbf{M}) = \{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - 1 - n\}$. If $b = m - 1$, then we prove in a similar way that $\text{NE}(\mathbf{M}) = \{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - 1 - m\}$.

Suppose now that $h = 2$. Then $d(W_1) + 1 = -an + bm + cr_2$ with $a \geq 1$, $0 \leq b \leq e_1 - 1$, $0 \leq c \leq e_2 - 1$, and $(a, b, c) \neq (-1, e_1 - 1, e_2 - 1)$ (otherwise $d(W_1) + 1 = d(\mathbf{F}(\Gamma(f)))$). This forces $\text{ne}(\mathbf{M})$ to be equal to 1 by the minimality of $d(W_1)$. On the other hand, $\text{ne}(\mathbf{M}) = 2$ forces (a, b, c) to be either $(-1, e_1 - 2, e_2 - 1)$ (and thus $\text{NE}(\mathbf{M}) = \{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - m - 1\}$) or $(-2, e_1 - 1, e_2 - 1)$ (hence $\text{NE}(\mathbf{M}) = \{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - n - 1\}$) or $(-1, e_1 - 1, e_2 - 2)$ (in this case $\text{NE}(\mathbf{M}) = \{\mathbf{F}(\Gamma(f)) - 1, \mathbf{F}(\Gamma(f)) - r_2 - 1\}$). \square

In the following we shall give more precise information when $\text{ne}(\mathbf{M}) \in \{1, 2\}$.

The case of one non exact element. In this case $h = 1$, $\Gamma(f) = \langle m, n \rangle$ with $m < n$ and $\gcd(m, n) = 1$. Furthermore, $m + \lambda = \mathbf{F}(\Gamma(f)) = -m + (m - 1)n < m + n$ because $\lambda < n$. This implies that $(m - 2)n < 2m < 2n$. In particular, $m < 4$. If $m = 2$, then $n = 2p + 1$ for some $p \geq 1$. If $m = 3$, then $n < 2m = 6$ and $n > m = 3$ implies that either $n = 4$ or $n = 5$.

The case of two non exact elements and $h = 1$. In this case, $\Gamma(f) = \langle m, n \rangle$ with $m < n$ and $\gcd(m, n) = 1$. Furthermore, By Corollary 6.9, $m + \lambda \in \{\mathbf{F}(\Gamma(f)) - n, \mathbf{F}(\Gamma(f)) - m\}$.

- (1) If $m + \lambda = \mathbf{F}(\Gamma(f)) - m = -2m + (m - 1)n$, then we get, using the fact that $\lambda < n$, $6 > (n - 3)(m - 2)$. Hence (m, n) is either $(2, 2p + 1), p \geq 1$ or $(3, 4)$ or $(3, 5)$ or $(4, 5)$.
- (2) If $m + \lambda = \mathbf{F}(\Gamma(f)) - n = -m + (m - 2)n$, then we get that $4 > (n - 2)(m - 3)$. In particular, (m, n) is either $(2, 2p + 1)$ with $p \geq 1$, or $(3, n)$ with $n \geq 4$ and $\gcd(3, n) = 1$, or $(4, 5)$.

The case of two non exact elements and $h = 2$. Let $\Gamma(f) = \langle m, n, r_2 \rangle$ and let the notations be as above. Since $\mathbf{F}(\Gamma(f)) - 1$ is a non exact element of I , we have $m + \lambda \in \{\mathbf{F}(\Gamma(f)), \mathbf{F}(\Gamma(f)) - m, \mathbf{F}(\Gamma(f)) - n, \mathbf{F}(\Gamma(f)) - r_2\}$.

- (1) If $m + \lambda = \mathbf{F}(\Gamma(f)) - m = -m + (e_1 - 1)n + (e_2 - 1)r_2$, then $\lambda = -m_2 = r_2 - (e_1 - 1)n$ (because otherwise $\lambda > -m_2$, whence d_2 divides λ and consequently $m + \lambda$ is in $d_2\mathbb{Z}$, which is a contradiction). This implies that $m + r_2 - (e_1 - 1)n = -m + (e_1 - 1)n + (e_2 - 1)r_2$. Since $d_2 = \gcd(m, n)$ does not divide ir_2 for all $1 \leq i \leq e_2 - 1$, we deduce that $e_2 = 2$. This implies that $m - (e_1 - 1)n = 0$, which is a contradiction since $m < n$.
- (2) Suppose that $m + \lambda = \mathbf{F}(\Gamma(f)) - r_2 = -m + (e_1 - 1)n + (e_2 - 2)r_2$. If $e_2 \neq 2$, then by the same argument as in (1), $\lambda = -m_2 = r_2 - (e_1 - 1)n$. Hence $m + r_2 - (e_1 - 1)n = -m + (e_1 - 1)n + (e_2 - 2)r_2$. Since d_2 does not divide ir_2 for all $1 \leq i \leq e_2 - 1$, we obtain $e_2 = 3$, but $m - (e_1 - 1)n = 0$, which is a contradiction. It follows that $e_2 = 2$, whence $d_2 = 2$ and $\lambda > -m_2$ (because $\lambda = -2m + (e_1 - 1)n$ and m_2 is not divisible by d_2). But

$m + \lambda = F(\Gamma(f)) - r_2 = -m + (e_1 - 1)n < m + n$, and thus

$$-2m + \left(\frac{m}{2} - 1\right)n < n.$$

Let $a = \frac{m}{2}$ and $b = \frac{n}{2}$. Since $\gcd(m, n) = 2$, a and b are coprime. The equality above implies that $2a > (a - 2)b$. But $a < b$. Hence $2b > (a - 2)b$, that is, $a < 4$. Note that $a > 1$ because $h = 2$. If $a = 2$, then $b = 2p + 1$ for some $p \in \mathbb{N}$. If $a = 3$, then $b < 6$, and consequently $b \in \{4, 5\}$. This implies that (m, n, r_2) satisfies one of the following conditions:

- (a) $m = 4, n = 4p + 2, r_2 = 2q + 1$ and $8p + 4 > 2q + 1$.
 - (b) $m = 6, n = 8, r_2 = 2p + 1$ and $24 > 2p + 1$.
 - (c) $m = 6, n = 10, r_2 = 2p + 1$ and $30 > 2p + 1$.
- (3) If $m + \lambda = F(\Gamma(f)) - m = -2m + (e_1 - 1)r_1 + (e_2 - 1)r_2$, then $\lambda = -m_2 = r_2 - (e_1 - 1)n$, which implies that $m + r_2 - (e_1 - 1)n = -2m + (e_1 - 1)r_1 + (e_2 - 1)r_2$. Hence $e_2 = d_2 = 2$ and $3m = 2(e_1 - 1)n = 2\left(\frac{m}{2} - 1\right)n$. Consequently $3\left(\frac{m}{2} - 1\right) + 3 = \left(\frac{m}{2} - 1\right)n$. Finally, $(n - 3)\left(\frac{m}{2} - 1\right) = 3$. The only solution is $m = 4, n = 6$. Hence $r_2 = 2p + 1$ with $12 > r_2$.
- (4) If $m + \lambda = F(\Gamma(f)) - n = -m + (e_1 - 2)r_1 + (e_2 - 1)r_2$ then $\lambda = -m_2 = r_2 - (e_1 - 1)n$, which implies that $m + r_2 - (e_1 - 1)n = -m + (e_1 - 2)r_1 + (e_2 - 1)r_2$. Thus $e_2 = d_2 = 2$ and $2m = (2e_1 - 3)n = (m - 3)n$. This yields $6 = (m - 3)(n - 2)$. All possible cases lead to a contradiction.

These results can be summarized into the following theorem.

Theorem 6.10. *Let $X(t) = t^n + a_1t^{n-1} + \dots + a_n$, $Y(t) = t^m + b_1t^{m-1} + \dots + b_m$, and assume that $m < n$ and $\gcd(m, n) < m$. Let $f(X, Y)$ be the monic irreducible polynomial of $\mathbf{K}[X, Y]$ such that $f(X(t), Y(t)) = 0$, and let $\Gamma(f)$ be the semigroup associated with f . Assume that $\Gamma(f)$ is a numerical semigroup and let $\Gamma(f) = \langle m = r_0, n = r_1, r_2, \dots, r_h \rangle$ where r_2, \dots, r_h are constructed as in Algorithm 6.3. Let $\mu(f) = \dim_{\mathbf{K}} \mathbf{K}[X, Y]/(f_X, f_Y)$ and $\nu(f) = \dim_{\mathbf{K}} \mathbf{K}[X, Y]/(f, f_X, f_Y)$. Assume that $\mu(f) > \nu(f)$.*

- i) If $\mu(f) = \nu(f) + 1$, then $h = 1$.
- ii) If $\mu(f) = \nu(f) + 2$, then $h \in \{1, 2\}$.

Moreover, the following also holds.

- (1) If $\mu(f) = \nu(f) + 2$, then $\Gamma(f) = \langle m, n \rangle$ and one of the following conditions holds:
 - $(m, n) = (2, 2p + 1), p \geq 1$,
 - $(m, n) = (3, 4)$,
 - $(m, n) = (3, 5)$.
- (2) If $\mu(f) = \nu(f) + 2$ and $h = 1$, then $\Gamma(f) = \langle m, n \rangle$ and one of the following conditions holds:
 - $(m, n) = (2, 2p + 1), p \geq 1$,
 - $(m, n) = (3, 4)$,
 - $(m, n) = (3, 5)$,
 - $(m, n) = (4, 5)$,
 - $(m, n) = (3, n)$, with $\gcd(3, n) = 1$.
- (3) If $\mu(f) = \nu(f) + 1$ and $h = 2m$ then $\Gamma(f) = \langle m, n, r_2 \rangle$ and one of the following conditions holds:
 - $(m, n, r_2) = (4, 4p + 2, 2q + 1)$, $p \geq 1$ and $8p + 4 > 2q + 1$,
 - $(m, n, r_2) = (6, 8, 2p + 1)$, $p \leq 11$,
 - $(m, n, r_2) = (6, 10, 2p + 1)$, $p \leq 14$,
 - $(m, n, r_2) = (4, 6, 2p + 1)$, $p \leq 5$.

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, A. Sathaye, On quasi-homogeneous curves, Affine Algebraic Geometry, Osaka Univ. Press, Osaka (2007), 33–56.

- [3] A. Assi, P. A. García-Sánchez, Algorithms for curves with one place at infinity, *J. Symb. Comp.*, **74** (2016), 475–492.
- [4] A. Assi, P. A. García-Sánchez, Numerical Semigroups and Applications, RSME Springer Series I, 2016.
- [5] A. Assi, P. A. García-Sánchez, V. Micale, Bases of subalgebras of $K[[x]]$ and $K[x]$, avec Pedro A. Garca Snchez et Vincenzo Micale, *J. of Symb. Comp.*, **79** (2017), 4–22.
- [6] R. Berger, Differentialmoduln eindimensionaler lokaler Ringe, *Math. Z.* **81** (1963), 326–354.
- [7] M. Delgado, P. A. García-Sánchez, J. Morais, “NumericalSgps”, A GAP package for numerical semigroups. Available via <http://www.gap-system.org>.
- [8] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.5; 2014, <http://www.gap-system.org>.
- [9] V. Micale, Order bases of subalgebras of power series rings, *Comm. Algebra* **31** (2003), no. 3, 1359–1375.
- [10] V. Micale, G. Molica, B. Torrisi, Order bases of subalgebras of $k[[X]]$, *Commutative rings*, 193–199, Nova Sci. Publ., Hauppauge, NY, 2002.
- [11] J. C. Rosales, P. A. García-Sánchez, Numerical semigroups, *Developments in Mathematics*, 20. Springer, New York, 2009.
- [12] 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.
- [13] O. Zariski, Characterization of plane algebroid curves whose module of differentials has maximum torsion, *Proceedings of the National Academy of Sciences of the United States of America*, **56**, No. 3 (1966), pp. 781–786

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

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

DEPARTAMENTO DE ÁLGEBRA AND IEMATH-GR, UNIVERSIDAD DE GRANADA, E-18071 GRANADA, ESPAÑA
E-mail address: pedro@ugr.es
URL: www.ugr.es/local/pedro