Local zero estimates and effective division in rings of algebraic power series

Guillaume Rond

LOCAL ZERO ESTIMATES AND EFFECTIVE DIVISION IN RINGS OF ALGEBRAIC POWER SERIES

GUILLAUME ROND

Abstract. We characterize finite modules over the ring of formal power series which are completion of modules defined over the ring of algebraic power series. This characterization is made in terms of local zero estimates. To prove this characterization we show an effective Weierstrass Division Theorem and an effective solution to the Ideal Membership Problem in rings of algebraic power series. Finally we apply these results to prove a gap theorem for power series which are remainder of the Grauert-Hironaka-Galligo Division Theorem.

1. Introduction

The goal of this paper is to give a characterization in term of local zero estimates for a finite module defined over the ring of formal power series to be the completion of a module defined over the ring of algebraic power series. Finding conditions for the algebraicity of such modules is a long-standing problem (see [Sa56] or [Ar66] for instance). Let us recall that an algebraic power series over a field $\Bbbk$ in the variables x_1,..., x_n is a formal power series $f(x) \in \Bbbk[\![x]\!]$ (from now on we denote the tuple $(x_1, \cdots, x_n)$ by x) such that

$$P(x, f(x)) = 0$$

for a non-zero polynomial $P(x, Z) \in \Bbbk[x, Z]$. The set of algebraic power series is a subring of $\Bbbk[\![x]\!]$ denoted by $\Bbbk\langle x\rangle$.
For an algebraic power series f, we define the height of f, $\mathrm{H}(f)$, to be the maximum of the degrees of the coefficient of the minimal polynomial of f (see Definition 3.2). If f is a polynomial its height is equal to its degree as a polynomial.
Let M be a $\Bbbk[\![x]\!]$-module The order function ord_M is defined as follows:

$$\mathrm{ord}_M(m) := \sup\{c \in \mathbb{N} \ / \ m \in (x)^c M\} \ \ \forall m \in M\backslash\{0\}.$$

Let $p \in \Bbbk[x]^s$ (resp. $\Bbbk\langle x\rangle^s$). The *degree* (resp. *height*) of p is the maximum of the degrees (resp. heights) of its components. Then our main result is the following:

Theorem 1.1. *Let $\Bbbk$ be any field and let M be a finite $\Bbbk[\![x]\!]$-module,*

$$M = \frac{\Bbbk[\![x]\!]^s}{N}$$

for some integer s and some $\Bbbk[\![x]\!]$-sub-module N of $\Bbbk[\![x]\!]^s$. Then the following conditions are equivalent:

i) *The sub-module N is generated by a sub-module of $\Bbbk\langle x\rangle^s$.*

2010 *Mathematics Subject Classification.* Primary : 13J05, Secondary : 13P10, 11G50, 11J82.
The author was partially supported by ANR projects STAAVF (ANR-2011 BS01 009) and SUSI (ANR-12-JS01-0002-01).

ii) *There exists a constant C such that*

$$ord_M(p) \leq C \cdot deg\,(p) \quad \forall p \in \Bbbk[x]^s \backslash N.$$

iii) *There exists a function*

$$C : \mathbb{N} \longrightarrow \mathbb{R}_{>0}$$

such that

$$ord_M(f) \leq C(Deg(f)) \cdot H(f) \quad \forall f \in \Bbbk\langle x\rangle^s \backslash N.$$

Here $Deg(f)$ denotes the degree of the field extension $\Bbbk(x) \longrightarrow \Bbbk(x, f)$. Moreover when $char\,(\Bbbk) = 0$ then C depends polynomially on $Deg(f)$.

Our result is a generalization of a previous result of S. Izumi (see [Iz92a], [Iz92b], [Iz98] where he proved (i)$\Longleftrightarrow$(ii) when $\mathrm{char}\,(\Bbbk) = 0$, $s = 1$ and N is a prime ideal of $\Bbbk[\![x]\!]$).
Since $\mathrm{H}(p) = \deg(p)$ and $\mathrm{Deg}(p) = 1$ for any polynomial p we have (iii)$\Longrightarrow$(ii). The proof of (ii)$\Longrightarrow$(i) is quite straightforward using Hilbert-Samuel functions and is essentially the same as in [Iz92b]. The difficulty in Theorem 1.1 is (i)$\Longrightarrow$(iii). In fact the first difficulty occurs already when $s = 1$ and N is an ideal of $\Bbbk[\![x]\!]$ which is not prime. The case of a prime ideal (in the case of (ii)$\Longrightarrow$(ii)) has been proved by S. Izumi in [Iz92a] in the complex analytic case using resolution of singularities of Moishezon spaces and for any field of characteristic zero using basic field theory. But when N is not prime his proof does not adapt at all and the general case cannot be reduced to the case proved by S. Izumi.

The proof we give here is done by induction on s and n by solving linear equations with coefficients in $\Bbbk\langle x\rangle$. For doing this we need to prove two effective division results in the rings of algebraic power series which may be of general interest. These are the followings:

i) In the case of the Weierstrass Division of an algebraic power series f by another algebraic power series it is proved by J.-P. Lafon that the remainder and the quotient of the division are algebraic power series [La65]. The problem solved here is to bound the complexity of the division, i.e. bound the complexity of the quotient and the remainder of the division in function of the complexity of the input data. This is Theorem 4.5 and is the main tool to solve the next division problem.

ii) Bounding the complexity of the Ideal Membership Problem in the ring of algebraic power series, i.e. if an algebraic power series f is in the ideal generated by algebraic power series g_1,..., g_p, bound the complexity of algebraic power series a_1,..., a_p such that

$$f = a_1 g_1 + \cdots + a_p g_p.$$

This is Theorem 6.1.

The complexity invariants associated to an algebraic power series f are its degree and its height. The first one is the degree of the field extension $\Bbbk(x) \longrightarrow \Bbbk(x, f)$ and the second one has been defined above. In particular we will prove that the previous complexity problems admit a solution which is linear with respect to the height of f (but it is not linear which respect to the other data). This is exactly what we need to prove Theorem 1.1.

Finally we apply our main theorem to give a partial answer to a question of H. Hironaka. When f, g_1,..., g_s are formal power series, we can write

$$f = a_1 g_1 + \cdots + a_s g_s + r$$

where the non-zero monomials in the Taylor expansion of r are not divisible by the initial terms of the g_i (see Section 8 for precise definitions). When the power series f and the g_i are convergent then r is also convergent. This result has been proved by H. Grauert in order to study versal deformations of isolated singularities of analytic hypersurfaces [Gr72] and then by H. Hironaka to study resolution of singularities [Hi64]. But when f and the g_i are algebraic power series, then r is not an algebraic power series in general and H. Hironaka raised the problem of characterizing such power series r (see [Hi77]). In this case we prove that such power series r are not too transcendental (see Theorem 10.2). More precisely if we write r as $r = \sum_{k=0}^{\infty} r_{n(k)}$ where $r_{n(k)}$ is a non-zero homogeneous polynomial of degree $n(k)$ and the sequence $(n(k))_k$ is strictly increasing, we show that

$$\limsup_{k \longrightarrow \infty} \frac{n(k+1)}{n(k)} < \infty.$$

Let us mention that this division problem appears also in combinatorics: the generating series of walks confined in the first quadrant are solutions of such division but are nor algebraic nor D-finite in general (see [HK08] or [KK12]).

Let us mention that estimates of the kind ii) in Theorem 1.1, i.e. estimates of the form

$$\mathrm{ord}_M p \leq \gamma(\deg(p))$$

where $\gamma : \mathbb{N} \longrightarrow \mathbb{N}$ is an increasing function, $s = 1$ and N is an ideal of analytic functions are called *zero estimates* in the literature. Finding such estimates for particular classes of functions is an important subject of research in transcendence theory, in particular when the ideal N is generated by analytic functions of the form

$$x_k - f_k(x_1, \cdots, x_{k-1}), \cdots, x_n - f_n(x_1, \cdots, x_{k-1})$$

for some $k < n$ and f_k, ..., f_n solutions of differential equations (see [Sh59], [BB85], [Ne87] for instance) or functional equations (q-difference equations or Mahler functions - see [Ni90] for instance).

The paper is organized as follows: After giving the list of notations used in the paper in Section 2, we define the height of an algebraic power series in Section 3 and give the first properties of it. In Section 4 we prove an effective Weierstrass Division Theorem (see Theorem 4.5). In Section 5 we give some results about the Ideal Membership Problem in rings which are localizations of rings of polynomials (see Theorem 5.2) and in Section 6 we give an effective Ideal Membership theorem for algebraic power series rings (see Theorem 6.1). Then Section 7 is devoted to the proof of Theorem 1.1. The next three sections concern the Grauert-Hironaka-Galligo Division Theorem: in Section 8 we state this theorem and give the example of Gabber and Kashiwara showing that the remainder of such division of an algebraic power series by another one is not algebraic in general. We show in Section

9 that the example of Gabber-Kashiwara is generic in some sense, i.e. in general the division of an algebraic power series by another one does not have an algebraic remainder (see Proposition 9.2). Finally we prove in Section 10 our gap theorem for remainders of such division (see Theorem 10.2).

Remark 1.2. We show in Example 8.3 that the bound in Theorem 1.1 ii) is sharp. For iii) it is not clear if such bound is sharp. Indeed, let f be an algebraic power series and $M = \Bbbk[\![x]\!]/I$ where I is an ideal generated by algebraic power series. Let

$$a_d(x)T^d + a_{d-1}(x)T^{d-1} + \cdots + a_0(x)$$

be the minimal polynomial of f. Then we have

$$(a_d f^{d-1} + a_{d-1}f^{d-2} + \cdots + a_1)f = -a_0.$$

We set $g := a_d f^{d-1} + a_{d-1}f^{d-2} + \cdots + a_1$. If $a_0 \notin I$, then

$$\mathrm{ord}_M(f) \leq \mathrm{ord}_M(gf) = \mathrm{ord}_M(a_0) \leq C\,\mathrm{H}(f)$$

where C is the constant of ii) in Theorem 1.1 since $a_0(x)$ is a polynomial of degree $\leq \mathrm{H}(f)$. This shows that in general the function C of iii) can be chosen to be independent of $\mathrm{Deg}(f)$ except maybe when $a_0(x) \equiv 0$ in M.

Acknowledgment. The author would like to thank Paco Castro-Jiménez and Herwig Hauser for the discussions they had about the Weierstrass division Theorem in the algebraic case.

2. Notations

In the whole paper $\Bbbk$ denotes a field of any characteristic. Let n be a non-negative integer and set

$$x := (x_1, ..., x_n) \text{ and } x' := (x_1, ..., x_{n-1}).$$

The ring of polynomials in n variables over $\Bbbk$ will be denoted by $\Bbbk[x]$ and its field of fractions by $\Bbbk(x)$. The ring of formal power series in n variables over $\Bbbk$ is denoted by $\Bbbk[\![x]\!]$ and its field of fractions by $\Bbbk((x))$. An algebraic power series is a power series $f(x) \in \Bbbk[\![x]\!]$ such that

$$P(x, f(x)) = 0$$

for some non-zero polynomial $P(x, y) \in \Bbbk[x, y]$ where y is a single indeterminate. The set of algebraic power series is a local subring of $\Bbbk[\![x]\!]$ denoted by $\Bbbk\langle x\rangle$.
When $\Bbbk$ is a valued field we denote by $\Bbbk\{x\}$ the ring of convergent power series in n variables over $\Bbbk$. We have

$$\Bbbk[x] \subset \Bbbk\langle x\rangle \subset \Bbbk\{x\} \subset \Bbbk[\![x]\!].$$

For a polynomial $p \in \Bbbk[x]$ we denote by $\deg(p)$ its total degree in the variables x_1,..., x_n. If $y := (y_1, ..., y_m)$ is a new set of indeterminates and $p \in \Bbbk[x, y]$ we denote by

$$\deg_{(y_1,...,y_m)}(p)$$

the degree of p seen as a polynomial in $\mathbb{K}[y]$ where $\mathbb{K} := \Bbbk(x)$. When $p \in \Bbbk[x]^s$ for some s, we denote by $\deg(p)$ the maximum of the degrees of the components of p.

For an algebraic power series $f \in \Bbbk\langle x\rangle$, the height of f is the maximum of the degrees of the coefficients of the minimal polynomial of f (see Definition 3.2). The height of a vector of algebraic power series is the maximum of the heights of its

components.

When $(A, \mathfrak{m})$ is a local ring we set

$$\mathrm{ord}_A(x) := \sup\{k \in \mathbb{N} \ / \ x \in \mathfrak{m}^k\} \in \mathbb{N} \cup \{\infty\} \quad \forall x \in A.$$

If M is a finite A-module we set

$$\mathrm{ord}_M(m) := \sup\{k \in \mathbb{N} \ / \ m \in \mathfrak{m}^k M\} \quad \forall m \in M.$$

When $A = \Bbbk[\![x]\!]$ we write ord instead of $\mathrm{ord}_{\Bbbk[\![x]\!]}$. For an ideal of $\Bbbk[\![x]\!]$ generated by g_1,..., g_p we define

$$\mathrm{ord}_{g_1,\cdots,g_p}(f) := \sup\{n \in \mathbb{N} \ / \ f \in (g_1, \cdots, g_p)^n\} \in \mathbb{N} \cup \{\infty\}.$$

If $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$ we set

$$|\alpha| := \alpha_1 + \cdots + \alpha_n.$$

If λ_1,..., λ_n are positive integers we define

$$\nu_\lambda(f) := \min\{\lambda_1\alpha_1 + \cdots \lambda_n\alpha_n \ / \ f_\alpha \neq 0 \text{ if } f = \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha\}$$

for any non-zero $f \in \Bbbk[\![x]\!]$ and $\nu_\lambda(0) = \infty$. This function satisfies

$$\nu_\lambda(fg) = \nu_\lambda(f) + \nu_\lambda(g) \quad \forall f, g \in \Bbbk[\![x]\!]$$
$$\nu_\lambda(f+g) \geq \min\{\nu_\lambda(f), \nu_\lambda(g)\} \quad \forall f, g \in \Bbbk[\![x]\!].$$

For any ideal I of $\Bbbk[\![x]\!]$, this function induces a function on $\Bbbk[\![x]\!]/I$, denoted by $\nu_{\lambda,\Bbbk[\![x]\!]/I}$, and defined by

$$\nu_{\lambda,\Bbbk[\![x]\!]/I}(f) := \sup\{\nu_\lambda(g) \ / \ g \in \Bbbk[\![x]\!] \text{ and } g \equiv f \text{ mod. } I\}.$$

It satisfies

$$\nu_{\lambda,\Bbbk[\![x]\!]/I}(fg) \geq \nu_\lambda(f) + \nu_\lambda(g) \quad \forall f, g \in \Bbbk[\![x]\!]/I$$
$$\nu_{\lambda,\Bbbk[\![x]\!]/I}(f+g) \geq \min\{\nu_\lambda(f), \nu_\lambda(g)\} \quad \forall f, g \in \Bbbk[\![x]\!]/I.$$

3. Height and degree of algebraic power series

In this part $\Bbbk$ denotes a field of any characteristic.

Definition 3.1. Let $f \in \Bbbk\langle x\rangle$ be an algebraic power series. The morphism $\Bbbk[x,T] \longrightarrow \Bbbk\langle x\rangle$ defined by sending $P(x,T)$ onto $P(x,f)$ is not injective and its kernel is a height one prime ideal of $\Bbbk[x,T]$. Thus it is generated by one polynomial. If $P(x,T)$ is a such a generator then any other generator of this ideal is equal to $P(x,T)$ times a non-zero element of $\Bbbk$. Such a generator is call a minimal polynomial of f. By abuse of language we will often refer to such an element by *the* minimal polynomial of f.

Definition 3.2. [AB13] Let $P(T) \in \Bbbk[x][T]$. The height of P is the maximum of the degrees of the coefficients of $P(T)$ seen as a polynomial in T.
Let α be an algebraic element over $\Bbbk(x)$. The height of α is the height of its minimal polynomial and is denoted by $\mathrm{H}(\alpha)$. Its degree is the degree of its minimal polynomial or, equivalently, the degree of the field extension $\Bbbk(x) \longrightarrow \Bbbk(x,\alpha)$ and is denoted by $\mathrm{Deg}(\alpha)$.

Example 3.3. Let f be a polynomial in $\Bbbk[x]$, then $\mathrm{H}(f) = \deg(f)$ and $\mathrm{Deg}(f) = 1$. Let f/g be a rational function in $\Bbbk(x)$. Then $\mathrm{H}(f/g) = \max\{\deg(f), \deg(g)\}$ and $\mathrm{Deg}(f/g) = 1$.
If α is algebraic over $\Bbbk(x)$, then $1/\alpha$ also and $\mathrm{H}(1/\alpha) = \mathrm{H}(\alpha)$ and $\mathrm{Deg}(1/\alpha) = \mathrm{Deg}(\alpha)$.
If $f(x)$ is an algebraic power series and $M \in \mathrm{Gl}_n(\Bbbk)$ then $f(Mx)$ is also algebraic and $\mathrm{H}(f(Mx)) = \mathrm{H}(f(x))$ and $\mathrm{Deg}(f(Mx)) = \mathrm{Deg}(f(x))$.

Remark 3.4. There is another measure of the complexity of an algebraic power series f. This one is defined to be the total degree of the minimal polynomial of f and denoted by $\mathrm{c}(f)$ (cf. [Ra89] or [AMR91]). Thus we have

$$\frac{\mathrm{H}(f) + \mathrm{Deg}(f)}{2} \leq \max\{\mathrm{H}(f), \mathrm{Deg}(f)\} \leq \mathrm{c}(f) \leq \mathrm{H}(f) + \mathrm{Deg}(f).$$

This shows that $\mathrm{c}(f)$ is equivalent to $\mathrm{H}(f) + \mathrm{Deg}(f)$. Moreover these bounds are sharp. Indeed let $P_n(T) := (1+x^n)T^n - 1$ (where x is a single variable and $n \in \mathbb{N}$). Then $P_n(T)$ is irreducible and has a root f_n in $\Bbbk\langle x\rangle$. Thus $\mathrm{H}(f_n) = \mathrm{Deg}(f_n) = n$ and $c(f_n) = 2n$. On the other hand the polynomial $Q_n(T) := T^n - (1 + x^n)$ is irreducible and has a root g_n in $\Bbbk\langle x\rangle$. Thus $\mathrm{H}(g_n) = \mathrm{Deg}(g_n) = c(g_n) = n$.
We choose to use $\mathrm{H}(f)$ instead of $\mathrm{c}(f)$ since the complexity of the Weierstrass Division Theorem is linear in $\mathrm{H}(f)$ but not in $\mathrm{c}(f)$ (it is not linear in $\mathrm{Deg}(f)$ - see Theorem 4.5). Indeed we need to prove the existence of a bound in (iii) of Theorem 1.1 which is linear in $\mathrm{H}(f)$.

Lemma 3.5. *(*[AB13] *Lemma 4.1) Let α_1,..., α_p be algebraic elements over $\Bbbk(x)$ and a_1,..., $a_p \in \Bbbk(x)$. Then we have:*

$$\begin{gathered}
Deg(a_1\alpha_1 + \cdots + a_p\alpha_p) \leq Deg(\alpha_1)\cdots Deg(\alpha_p),\\
H(a_1\alpha_1 \cdots + a_p\alpha_p) \leq p \cdot Deg(\alpha_1)\cdots Deg(\alpha_p)(\max_i\{H(\alpha_i)\} + \max_j\{H(a_j)\}),\\
H(a_1 + \alpha_1) \leq H(\alpha_1) + Deg(\alpha_1)H(a_1),\\
Deg(\alpha_1\cdots\alpha_p) \leq Deg(\alpha_1)\cdots Deg(\alpha_p),\\
H(\alpha_1\cdots\alpha_p) \leq p \cdot Deg(\alpha_1)\cdots Deg(\alpha_p)\max_i\{H(\alpha_i)\}.
\end{gathered}$$

Proof. All these inequalities are proved in [AB13] except the third one that we prove here. Let $P(x,T)$ be the minimal polynomial of α_1 and let us write $a_1(x) = b(x)/c(x)$ for some polynomials $b(x)$ and $c(x)$. Then

$$Q(x,T) := c(x)^{\deg_T(P)}P(x, T - a_1)$$

is a polynomial vanishing at $\alpha_1 + a_1$. Thus

$$\mathrm{H}(\alpha_1 + a_1) \leq \deg_x(Q(x,T)) \leq \mathrm{H}(\alpha_1) + \mathrm{Deg}(\alpha_1)\mathrm{H}(a_1).$$

□

Lemma 3.6. *For an algebraic power series f we have:*

$$ord(f) \leq H(f).$$

Moreover for any integer $1 \leq i \leq n$ we have:

$$ord_{x_i,\cdots,x_n}(f(0,\cdots,0,x_i,\cdots,x_n)) \leq H(f).$$

Proof. Let $P(T) = a_dT^d + \cdots + a_1T + a_0$ be the minimal polynomial of f. Since $P(f) = 0$ there is two integers $0 \leq i < j \leq d$ such that $\mathrm{ord}(a_if^i) = \mathrm{ord}(a_jf^j)$. Thus

$$\mathrm{ord}(f) = \frac{\mathrm{ord}(a_i) - \mathrm{ord}(a_j)}{j-i} \leq \mathrm{ord}(a_i) \leq \deg(a_i).$$

This proves the first inequality. The second one is proven by noticing that if $P(x_1, \cdots x_n, f(x_1 \cdots, x_n)) = 0$, then $P(0, x_2, \cdots, x_n, f(0, x_2, \cdots, x_n)) = 0$. Since P is the minimal polynomial of f, then P is not divisible by x_1, thus

$$P(0, x_2, \cdots, x_n, T) \not\equiv 0.$$

This proves that $f(0, x_2, \cdots, x_n)$ is an algebraic power series and its minimal polynomial divides $P(0, x_2, \cdots, x_n, T)$, hence

$$\mathrm{H}(f(0, x_2, x \cdots, x_n)) \leq \mathrm{H}(f).$$

The first inequality implies

$$\mathrm{ord}_{x_2,\cdots,x_n}(f(0, x_2, \cdots, x_n)) \leq \mathrm{H}(f).$$

Hence the second inequality is proved by induction on i. □

Remark-Definition 3.7. Let $\mathbb{K}$ be an algebraic closure of $\Bbbk((x'))$ where $x' := (x_1, \cdots, x_{n-1})$. The (x')-valuation $\mathrm{ord}_{x'}$ defined on $\Bbbk((x'))$ extends uniquely to $\mathbb{K}$ and is still denoted by $\mathrm{ord}_{x'}$. The completion of $\mathbb{K}$ for the $\mathrm{ord}_{x'}$ valuation is denoted by $\widehat{\mathbb{K}}$. Let $\alpha \in \widehat{\mathbb{K}}$ such that $\mathrm{ord}_{x'}(\alpha) > 0$ and f be a power series. Then $f(x', \alpha)$ is well defined in $\widehat{\mathbb{K}}$. If $f(x', \alpha) = 0$ we call α a *root* of f.
If f is an algebraic power series and $P(x, T)$ is the minimal polynomial of f, then $P(x', \alpha, 0) = 0$ thus α is algebraic over $\Bbbk(x')$.

Let f be a power series which is x_n-regular of order d, i.e. $f(0, ..., 0, x_n) = u(x_n)x_n^d$ with $u(0) \neq 0$. Then, by the Weierstrass Preparation Theorem, there exist a unit v and a Weierstrass polynomial $P = x_n^d + a_1(x')x_n^{d-1} + \cdots + a_d(x')$ such that $f = vP$. The polynomial P is called the *Weierstrass polynomial of* f. Let $\alpha \in \mathbb{K}$ be a root of P. Since $\mathrm{ord}(a_i(x')) > 0$ for any i we have $\mathrm{ord}_{x'}(\alpha) > 0$. Thus $f(x', \alpha)$ and $v(x', \alpha)$ are well defined in $\widehat{\mathbb{K}}$ and $f(x', \alpha) = 0$. On the other hand if $\alpha \in \mathbb{K}$ is a root of f, since $\mathrm{ord}_{x'}(\alpha) > 0$ then $v(x', \alpha) \neq 0$ in $\widehat{\mathbb{K}}$, thus $P(x', \alpha) = 0$. This proves that the roots of f are exactly the roots (in the usual sense) of P seen as a polynomial in x_n and are elements of an algebraic closure of $\Bbbk((x'))$.

Lemma 3.8. *Let $\alpha \in \mathbb{K}$ be a root of an algebraic power series f. Then α is algebraic over $\Bbbk(x)$ and*

$$H(\alpha) \leq H(f) \quad \textit{and} \quad Deg(\alpha) \leq H(f).$$

Moreover if α_1,..., α_d are distinct roots of f, then

$$[\Bbbk(x', \alpha_1, \cdots, \alpha_d) : \Bbbk(x')] \leq H(f)!$$

Proof. Let $P(x, T)$ be the minimal polynomial of f. Since $f(x', \alpha) = 0$ we have

$$P(x', \alpha, 0) = 0.$$

Thus $P(x', T, 0)$ is a non-zero polynomial vanishing at α, proving that α is algebraic, hence

$$\mathrm{H}(\alpha) \leq \deg_{x'}(P(x', T, 0)) \leq \deg_{(x', x_n)}(P(x', x_n, T)) = \mathrm{H}(f)$$

and

$$\mathrm{Deg}(\alpha) \leq \deg_T(P(x', T, 0)) \leq \deg_{x_n}(P(x', x_n, T)) \leq \mathrm{H}(f).$$

Moreover $P(x', T, 0)$ is a polynomial having α_1,..., α_d as roots. Thus a splitting field of $P(x', T, 0)$ over $\Bbbk(x')$ contains these roots, thus

$$[\Bbbk(x', \alpha_1, \cdots, \alpha_d) : \Bbbk(x')] \leq \deg_T(P(x', T, 0))!$$

□

Lemma 3.9. *Let α be algebraic over $\Bbbk(x)$ with ord$(\alpha) > 0$. Let $g(x, y)$ be an algebraic power series where y is a single variable. Then $g(x, \alpha)$ is algebraic over $\Bbbk(x)$ and*

$$H(g(x, \alpha)) \leq H(g) \cdot (H(\alpha) + Deg(\alpha))$$
$$Deg(g(x, \alpha)) \leq Deg(\alpha) \cdot Deg(g).$$

Proof. Let $P(x, y, Z) \in \Bbbk[x, y, Z]$ be the minimal polynomial of g and $Q(x, Z) \in \Bbbk[x, Z]$ be the minimal polynomial of α. Then

$$P(x, \alpha, g(x, \alpha)) = 0$$

and $P(x, \alpha, T) \not\equiv 0$ otherwise $P(x, y, T)$ is divisible by $Q(x, y)$ which is impossible since P is assumed to be irreducible. Thus $g(x, \alpha)$ is algebraic over $\Bbbk(x, \alpha)$, hence over $\Bbbk(x)$, and

$$R(x, Z) := \mathrm{Res}_T(P(x, T, Z), Q(x, T)) \neq 0$$

is a polynomial of $\Bbbk[x][Z]$ vanishing at $g(x, \alpha)$. We can write

$$P(x, T, Z) = a_0(x, Z) + a_1(x, Z)T + \cdots + a_h(x, Z)T^h$$

where $h \leq \mathrm{H}(g)$, $\deg(a_i) \leq \mathrm{H}(g) + \mathrm{Deg}(g)$, $\deg_x(a_i) \leq \mathrm{H}(g)$ and $\deg_Z(a_i) \leq \mathrm{Deg}(g)$. We write

$$Q(x, T) = b_0(x) + b_1(x)T + \cdots + b_e(x)T^e$$

with $e = \mathrm{Deg}(\alpha)$ and $\deg(b_i) \leq \mathrm{H}(\alpha)$ for all i. Since $R(Z)$ is homogeneous of degree h in b_0,..., b_e and homogeneous of degree e in a_0,..., a_h, we see that

$$\deg_Z(R(Z)) \leq e \cdot \mathrm{Deg}(g) = \mathrm{Deg}(\alpha) \cdot \mathrm{Deg}(g)$$

and

$$\mathrm{H}(R(Z)) \leq h \cdot \mathrm{H}(\alpha) + e \cdot \mathrm{H}(g).$$

This proves the lemma. □

Remark 3.10. Let $g(x, y)$ be an algebraic power series where $y = (y_1, ..., y_m)$ and let $a_1(x)$,..., $a_m(x)$ be algebraic power series vanishing at 0. If $P(x, y, T)$ is the minimal polynomial of g, then

$$P(x, a(x), g(x, a(x))) = 0$$

but it may happen that

$$P(x, a(x), T) = 0.$$

Hence the previous proof does not extend directly to this case. For example let

$$P_1(x, y_1) := y_1^2 - (1 + x)$$
$$P_2(x, y_2) := y_2^2 - (1 + x)$$

where x is a single variable. Then P_1 and P_2 have a root in $\Bbbk\langle x\rangle$, say $a(x)$. Let

$$P(x, y, T) := (P_1 + P_2)T^2 + P_1T + P_2.$$

the discriminant of P is equal to

$$\Delta := P_1^2 - 4P_2 = y_1^4 - 2(1+x)y_1^2 - 4y_2^2 + x^2 - 2x - 3$$

and is not a square in $\Bbbk[x, y_1, y_2]$, thus P is irreducible in $\Bbbk[x, y, T]$. But Δ is unit in $\Bbbk\langle x, y\rangle$ and $P_1 + P_2$ also. So Δ has a root square in $\Bbbk\langle x\rangle$ if $\mathrm{char}\,(\Bbbk) \neq 2$ and 3 is a square in $\Bbbk$. Thus in this case $P(x, y, T)$ has two roots in $\Bbbk\langle x, y\rangle$. But here

$$P(x, a(x), a(x), T) = 0.$$

Lemma 3.11. *Let $g(x, y)$ be an algebraic power series where $y = (y_1, ..., y_m)$ and let $a_1(x)$,..., $a_m(x)$ be algebraic power series vanishing at 0. Then*

$$H(g(x, a(x))) \leq \left(\prod_{i=1}^{m}(H(a_i) + Deg(a_i))\right) \cdot H(g),$$

$$Deg(g(x, a(x))) \leq \left(\prod_{i=1}^{m} Deg(a_i)\right) \cdot Deg(g).$$

Proof. Let us set

$$g_1(x, y_2, ..., y_m) := g(x, a_1(x), y_2, ..., y_m),$$
$$g_2(x, y_1, ..., y_{m-2}) := g_1(x, a_2(x), y_3, ..., y_m),$$
$$\cdots\cdots$$
$$g_m(x) = g_{m-1}(x, a_m(x)) = g(x, a(x)).$$

Then by Lemma 3.9, we have

$$\mathrm{H}(g_i) \leq \mathrm{Deg}(a_i) \cdot \mathrm{Deg}(g_{i-1}),$$
$$\mathrm{Deg}(g_i) \leq \mathrm{H}(g_{i-1})(\mathrm{H}(a_i) + \mathrm{Deg}(a_i)).$$

This proves the lemma.

□

Lemma 3.12. *Let f be an algebraic power series. Then $\frac{\partial f}{\partial x_n}$ is an algebraic power series and*

$$H\left(\frac{\partial f}{\partial x_n}\right) \leq 2Deg(f)^{2Deg(f)+3}H(f),$$

$$Deg\left(\frac{\partial f}{\partial x_n}\right) \leq Deg(f).$$

Proof. Let $P(x, T)$ be the minimal polynomial of f. Since $P(x, f) = 0$ we have

$$\frac{\partial P}{\partial x_n}(x, f(x)) + \frac{\partial f}{\partial x_n}(x)\frac{\partial P}{\partial T}(x, f(x)) = 0.$$

Since f is separable over $\Bbbk(x)$, then $\frac{\partial P}{\partial T} \neq 0$ and since P is the minimal polynomial of f then $\frac{\partial P}{\partial T}(x, f(x)) \neq 0$. Thus $\frac{\partial f}{\partial x_n}(x)$ is an algebraic power series and

$$\frac{\partial f}{\partial x_n}(x) = -\frac{\partial P}{\partial x_n}(x, f(x))/\frac{\partial P}{\partial T}(x, f(x)) \in \Bbbk(x, f).$$

So we obtain

$$\mathrm{Deg}\left(\frac{\partial f}{\partial x_n}(x)\right) \leq \mathrm{Deg}(f)$$

and

$$\mathrm{H}\left(\frac{\partial f}{\partial x_n}(x)\right) \leq 2\mathrm{Deg}(f)^2 \max\left\{\mathrm{H}\left(\frac{\partial P}{\partial x_n}(x,f(x))\right), \mathrm{H}\left(\frac{\partial P}{\partial T}(x,f(x))\right)\right\}.$$

We have

$$\frac{\partial P}{\partial T}(x,f(x)) = \sum_{i=0}^{\mathrm{Deg}(f)-1} a_i(x) f(x)^i$$

for some polynomials $a_i(x)$ with $\mathrm{Deg}(a_i) \leq \mathrm{H}(f)$. Thus

$$\mathrm{H}\left(\frac{\partial P}{\partial T}(x,f(x))\right) \leq \mathrm{Deg}(f)^{2\mathrm{Deg}(f)+1}\mathrm{H}(f).$$

In the same way we also have

$$\mathrm{H}\left(\frac{\partial x_n}{\partial T}(x,f(x))\right) \leq \mathrm{Deg}(f)^{2\mathrm{Deg}(f)+1}\mathrm{H}(f).$$

This proves the lemma. □

Lemma 3.13. *Let $f(x,y)$ be an algebraic power series where y is a single variable and q be a positive integer. Let us write $q = rp^e$ where $p = char(\Bbbk)$, $e \in \mathbb{N}$ and $\gcd(r,p) = 1$ (we set $e = 0$ when $char(\Bbbk) = 0$ and by convention $q = r$). Let us write*

$$f(x,y) = f_0(x,y^q) + f_1(x,y^q)y + \cdots + f_{q-1}(x,y^q)y^{q-1}.$$

Then the power series $f_i(x,y^q)$ are algebraic and for any $0 \leq i \leq q-1$ we have

$$H(f_i(x,y^q)) \leq q2^q Deg(f)^{2qDeg(f)+4q}\left(H(f) + \frac{q(q-1)}{2}\right)$$

$$Deg(f_i(x,y^q)) \leq Deg(f)^r.$$

Proof. We need to consider different cases:

(1) If $e = 0$ i.e. $\gcd(q,p) = 1$. By taking a finite extension of $\Bbbk$ we may assume that $\Bbbk$ contain a primitive q-th root of unity. Let ξ be such a primitive root of unity. Then

$$f(x,\xi^l y) = \sum_{k=0}^{q-1} f_k(x,y^q)\xi^{lk}y^k \quad \forall\ k,l.$$

Thus we have

$$\widetilde{f} = V(\xi)F(x,y^q)$$

where $\widetilde{f}$ is the vector with entries $f(x,\xi^l y)$, $1 \leq l \leq q$, $F(x,y^q)$ is the vector with entries $f_0(x,y^q)$, $yf_1(x,y^q)$,..., $y^{q-1}f_{q-1}(x,y^q)$ and $V(\xi)$ is the Vandermonde matrix

$$\begin{pmatrix} 1 & \xi & \xi^2 & \cdots & \xi^{q-1} \\ 1 & \xi^2 & \xi^4 & \cdots & \xi^{2(q-1)} \\ 1 & \xi^3 & \xi^6 & \cdots & \xi^{3(q-1)} \\ \vdots & \vdots & \vdots & \ddots & \cdots \\ 1 & \xi^q & \xi^{2q} & \cdots & \xi^{(q-1)q} \end{pmatrix}.$$

Thus

$$F(x,y^q) = V(\xi)^{-1}\widetilde{f}$$

Since the coefficients of $V(\xi)^{-1}$ are in $\Bbbk$ and $\mathrm{H}(f(x,\xi^l y)) = \mathrm{H}(f(x,y))$, by Lemma 3.5 we have

$$\mathrm{H}(F(x,y^q)) \leq q\mathrm{H}(f)$$
$$\mathrm{Deg}(F(x,y^q)) \leq \mathrm{Deg}(f)^q.$$

Thus

$$\mathrm{H}(f_k(x,y^q)) \leq q\mathrm{H}(f) + q - 1,$$
$$\mathrm{Deg}(f_k(x,y^q)) \leq \mathrm{Deg}(f)^q \quad \forall k.$$

(2) If $q = p$, then we have

$$\frac{\partial f}{\partial y} = f_1 + 2f_2 y + \cdots + (p-1)f_{p-1}y^{p-2},$$
$$\cdots\cdots\cdots$$
$$\frac{\partial^{p-1} f}{\partial y^{p-1}} = (p-1)!f_{p-1}.$$

Thus we have

$$\Delta f = M\widetilde{f}$$

where Δf is the vector of entries $\frac{\partial^k f}{\partial y^k}$, for $0 \leq k \leq p-1$, $\widetilde{f}$ is the vector with entries $f_l(x,y^p)$, for $0 \leq l \leq p-1$, and M is a upper triangular matrix with coefficients in $\Bbbk[y]$ and whose determinant is in $\Bbbk$. The height of the coefficients of M^{-1} is less than $\frac{p(p-1)}{2}$. Since

$$\widetilde{f} = M^{-1}\Delta f,$$

by Lemma 3.5 we obtain

$$\mathrm{H}(f_k(x,y^p)) \leq p\mathrm{Deg}(f)\mathrm{Deg}\left(\frac{\partial f}{\partial y}\right)\cdots\mathrm{Deg}\left(\frac{\partial^{p-1} f}{\partial y^{p-1}}\right)\left(\mathrm{H}\left(\frac{\partial^{p-1} f}{\partial y^{p-1}}\right) + \frac{p(p-1)}{2}\right)$$
$$\leq p2^{p-1}\mathrm{Deg}(f)^{2(p-1)\mathrm{Deg}(f)+4p-3}\left(\mathrm{H}(f) + \frac{p(p-1)}{2}\right).$$

Moreover, still by Lemma 3.12 we have

$$\mathrm{Deg}(f_k(x,y^p)) \leq \mathrm{Deg}(f) \quad \forall k.$$

(3) If $q = rp^e$ where $\gcd(r,p) = 1$, we write

$$f = \widetilde{f_0}(x,y^p) + \widetilde{f_1}(x,y^p)y + \cdots + \widetilde{f_{p-1}}(x,y^p)y^{p-1}.$$

Then

$$\widetilde{f_0} = f_0 + f_p y^p + \cdots + f_{q-p}y^{q-p},$$
$$\widetilde{f_1} = f_1 + f_{p+1}y^p + \cdots + f_{q-p+1}y^{q-p},$$
$$\cdots\cdots\cdots$$
$$\widetilde{f_{p-1}} = f_{p-1} + f_{2p-1}y^p + \cdots + f_{q-1}y^{q-p}.$$

Thus, by induction, we deduce from the previous cases

$$\mathrm{Deg}(f_i) \leq \mathrm{Deg}(f)^r,$$
$$\mathrm{H}(f_i) \leq q2^{p^e-1}\mathrm{Deg}(f)^{r+2(p-1)e\mathrm{Deg}(f)+(4p-3)e}\left(\mathrm{H}(f) + \frac{r(r-1)}{2}\right)$$
$$\leq q2^q\mathrm{Deg}(f)^{2q\mathrm{Deg}(f)+4q}\left(\mathrm{H}(f) + \frac{q(q-1)}{2}\right).$$

□

4. Effective Weierstrass Division Theorem

In this part we prove an effective Weierstrass Division Theorem. The proof (thus the complexity) is more complicated in the positive characteristic case since the Weierstrass polynomial associated to the divisor f may have irreducible factors that are not separable.

Lemma 4.1. *Let $\Bbbk$ be any field. Let f be an algebraic power series which is x_n-regular of order d. Then there exist a unit $u \in \Bbbk\langle x\rangle$ and a Weierstrass polynomal $P \in \Bbbk\langle x'\rangle[x_n]$ such that*

$$f = u \cdot P$$

and

$$Deg(P) \leq H(f)!,$$

$$H(P) \leq 2dH(f)^{d+1}.$$

Proof. The existence of u and P comes from the Weierstrass Preparation Theorem for formal power series
Let α_1,..., $\alpha_d \in \mathbb{K}$ be the roots of $P(x_n)$ counted with multiplicities. Then we have $P = \prod_{i=1}^{d}(x_n - \alpha_i)$. By Remark 3.7 the roots of $P(x_n)$ are the roots of f thus, by Lemma 3.8, P is an algebraic power series. Hence u is also an algebraic power series.
By Lemma 3.5 $\mathrm{H}(x_n - \alpha_i) \leq \mathrm{H}(\alpha_i) + \mathrm{Deg}(\alpha_i)$ and $\mathrm{Deg}(x_n - \alpha_i) = \mathrm{Deg}(\alpha_i) \leq \mathrm{H}(f)$ for all i by Lemma 3.8. Thus, by Lemma 3.5,

$$\mathrm{H}(P) \leq d \cdot \mathrm{Deg}(\alpha_1) \cdots \mathrm{Deg}(\alpha_d) \cdot \max_i\{\mathrm{H}(\alpha_i) + \mathrm{Deg}(\alpha_i)\} \leq d\mathrm{H}(f)^d(\mathrm{H}(f) + \mathrm{H}(f)).$$

Moreover $P \in \Bbbk(x, \alpha_1, \cdots, \alpha_d)$. But $[\Bbbk(x, \alpha_1, ..., \alpha_d) : \Bbbk(x)] \leq \mathrm{H}(f)!$ by Lemma 3.8 hence

$$\mathrm{Deg}(P) \leq \mathrm{H}(f)!$$

□

Lemma 4.2. *Let f be an algebraic power series which is x_n-regular of order d and let us assume that f has d distinct roots in $\mathbb{K}$. Let g be any algebraic power series. Then there exist unique algebraic power series q and r such that $r \in \Bbbk\langle x'\rangle[x_n]$ is of degree $< d$ in x_n and*

$$g = fq + r.$$

Moreover, if $r = r_0 + r_1x_n + \cdots + r_{d-1}x_n^{d-1}$, we have

$$H(r_i) \leq 4d(H(f)!)^{d+1}H(f)^2Deg(g)\max\left\{d!\frac{d(d-1)}{2}H(f)^{\frac{d(d-1)}{2}}(H(f)!)^{d!+2}, H(g)\right\}$$

$$\leq 2^{2^{O(H(f)^2)}}Deg(g)(H(g)+1) \quad \forall i,$$

$$H(r) \leq d\left(H(f)!H(f)^dDeg(g)^d\right)^d(\max_i\{H(r_i)\} + d - 1).$$

$$Deg(r_j),\ Deg(r) \leq H(f)!H(f)^dDeg(g)^d.$$

Proof. The Weierstrass Division Theorem for formal power series gives the existence and unicity of q and r. We just need to prove that q and r are algebraic and the inequalities on heights and degrees. Let α_1,..., $\alpha_d \in \mathbb{K}$ be the roots of f. Then we have

$$g(x', \alpha_i) = r(x', \alpha_i) \quad \forall i.$$

By writing $r = r_0 + r_1 x_n + \cdots + r_{d-1} x_n^{d-1}$ with $r_j \in \Bbbk\langle x' \rangle$ for all j, we obtain:

$$V(\alpha_i)\widetilde{r} = \widetilde{g}(\alpha_j)$$

where $V(\alpha_i)$ is the $d \times d$ Vandermonde matrix of the α_i:

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{d-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_d & \alpha_d^2 & \cdots & \alpha_d^{d-1} \end{pmatrix},$$

$\widetilde{r}$ is the $d \times 1$ column vector with entries r_k, and $\widetilde{g}(\alpha_j)$ is the $d \times 1$ column vector with entries $g(x', \alpha_j)$. Since the α_i are distinct $V(\alpha_i)$ is invertible and we obtain

$$\widetilde{r} = V(\alpha_i)^{-1}\widetilde{g}(\alpha_j). \tag{1}$$

By Lemmas 3.8 and 3.9 we see that the r_i and r are algebraic power series, thus q is also an algebraic power series. Still by Lemmas 3.8 and 3.9 we have:

$$\mathrm{H}(g(x', \alpha_i)) \leq 2\mathrm{H}(g) \cdot \mathrm{H}(f)$$
$$\mathrm{Deg}(g(x', \alpha_i)) \leq \mathrm{H}(f) \cdot \mathrm{Deg}(g).$$

The determinant of $V(\alpha_i)$ is the sum of $d!$ elements of the form

$$\alpha_{\sigma(1)}\alpha_{\sigma(2)}^2 \cdots \alpha_{\sigma(d-1)}^{d-1},$$

where σ is a permutation of $\{0, \cdots, d-1\}$. Each of these elements belongs to $\Bbbk(x', \alpha_1, ..., \alpha_d)$ so their degree is bounded $\mathrm{H}(f)!$ by Lemma 3.8. Thus the degree of any element of $\Bbbk(x', \alpha_1, ..., \alpha_d)$ is $\leq \mathrm{H}(f)!$. Thus by Lemma 3.5

$$\mathrm{H}(\det(V(\alpha_i))) \leq d!\frac{d(d-1)}{2}\mathrm{H}(f)^{\frac{d(d-1)}{2}+1}(\mathrm{H}(f)!)^{d!}.$$

Since the coefficients of $V(\alpha_i)^{-1}$ are $(d-1) \times (d-1)$ minors of $V(\alpha_i)$ divided by $\det(V(\alpha_i))$, the height of them is bounded by

$$H_V := 2d!(\mathrm{H}(f)!)^2(\mathrm{H}(f)!)^{d!}\frac{d(d-1)}{2}H(f)^{\frac{d(d-1)}{2}+1} =$$
$$= 2d!\frac{d(d-1)}{2}\mathrm{H}(f)^{\frac{d(d-1)}{2}+1}(\mathrm{H}(f)!)^{d!+2}.$$

Moreover their degree is bounded by $\mathrm{H}(f)!$ since they belong to $\Bbbk(x, \alpha_1, ..., \alpha_d)$. Since r_j is of the form $v_1 g(x', \alpha_1) + \cdots + v_d g(x', \alpha_d)$ where v_1,..., v_d are coefficients of $V(\alpha_i)^{-1}$ (by Equation (1)) we obtain:

$$\mathrm{H}(r_j) \leq d(\mathrm{H}(f)!)^d \max_i \{2\mathrm{H}(f)!\mathrm{Deg}(g(x', \alpha_i)) \max\{H_V, \mathrm{H}(g(x', \alpha_i))\}\}$$

$$\leq 4d(\mathrm{H}(f)!)^{d+1}\mathrm{H}(f)\mathrm{Deg}(g)\max\left\{d!\frac{d(d-1)}{2}\mathrm{H}(f)^{\frac{d(d-1)}{2}+1}(\mathrm{H}(f)!)^{d!+2}, \mathrm{H}(f)\mathrm{H}(g)\right\}$$

$$= 4d(\mathrm{H}(f)!)^{d+1}\mathrm{H}(f)^2\mathrm{Deg}(g)\max\left\{d!\frac{d(d-1)}{2}\mathrm{H}(f)^{\frac{d(d-1)}{2}}(\mathrm{H}(f)!)^{d!+2}, \mathrm{H}(g)\right\}.$$

Moreover r_j and $r \in \Bbbk(x', \alpha_1, \cdots, \alpha_d, g(x', \alpha_1), \cdots, g(x', \alpha_d))$, hence we have (by Lemmas 3.8 and 3.9):

$$\mathrm{Deg}(r_j) \leq \mathrm{H}(f)!\mathrm{H}(f)^d\mathrm{Deg}(g)^d, \quad \mathrm{Deg}(r) \leq \mathrm{H}(f)!\mathrm{H}(f)^d\mathrm{Deg}(g)^d.$$

Since

$$r = r_0 + x_n r_n + \cdots + x_n^{d-1} r_{d-1},$$

$$H(r) \leq d\left(\mathrm{H}(f)!\mathrm{H}(f)^d\mathrm{Deg}(g)^d\right)^d (\max_i\{\mathrm{H}(r_i)\} + d - 1).$$

□

Lemma 4.3. *Let assume that $\Bbbk$ is field of characteristic $p > 0$. Let f be an irreducible algebraic power series which is x_n-regular of order d and let us assume that its Weierstrass polynomial is not separable. Let g be any algebraic power series. Then there exist unique algebraic power series q and r such that $r \in \Bbbk\langle x'\rangle[x_n]$ is of degree $< d$ in x_n and*

$$g = fq + r.$$

Moreover, if $r = r_0 + r_1 x_n + \cdots + r_{d-1}x_n^{d-1}$, we have

$$H(r_i) \leq d^{d^{O(d)}} Deg(g)^{2d(Deg(g)+2)}(H(g)+1) \quad \forall i,$$

$$H(r) \leq d^{d^{O(d)}} Deg(g)^{O(d\,Deg(g))}(H(g)+1)i,$$

$$Deg(r_j),\ Deg(r) \leq Deg(r) \leq H(f)!H(f)^d Deg(g_i)^d \quad \forall i.$$

Proof. Let P denote the Weierstrass polynomial of f. Then we have

$$P = \prod_{k=1}^{D} (x_n - \alpha_i)^{p^e}$$

where α_1,..., α_D are the distinct roots of $P(x_n)$ in $\mathbb{K}$. Thus $P \in \Bbbk\langle x'\rangle[x_n^{p^e}]$ by Lemma 4.1 and $d = Dp^e$. By the Weierstrass Division Theorem for formal power series we have

$$g = Pq + r$$

where

$$r = r_0 + r_1 x_n + \cdots + r_{d-1}x_n^{d-1}$$

and $r_i \in \Bbbk[\![x']\!]$. Let us write

$$g = g_0(x', x_n^{p^e}) + g_1(x', x_n^{p^e})x_n + \cdots + g_{p^e-1}(x', x_n^{p^e})x_n^{p^e-1}$$

where $g_i := g_i(x', x_n^{p^e}) \in \Bbbk[\![x', x_n^{p^e}]\!]$ for all i.
We define $\widetilde{P}$ by

$$\widetilde{P}(x', x_n^{p^e}) = P(x', x_n).$$

Then $\widetilde{P}$ is an algebraic power series and $\mathrm{H}(\widetilde{P}) \leq \mathrm{H}(P)$ (if $R(x', x_n^{p^e}, T)$ is the minimal polynomial of P, the $R(x, x_n, T)$ is a non-zero polynomial vanishing at $\widetilde{P}$). Let us perform the Weierstrass Division of $g_i(x', x_n)$ by $\widetilde{P}$:

$$g_i(x', x_n) = \widetilde{P}q_i + \sum_{j=0}^{D-1} r_{i,j}(x')x_n^j.$$

By Lemma 4.2 the $r_{i,j}(x')$ are algebraic power series and

$$\mathrm{H}(r_{i,j}) \leq 4d(\mathrm{H}(P)!)^{d+1}\mathrm{H}(P)^2\mathrm{Deg}(g_i(x',x_n)) \tag{2}$$
$$\max\left\{d!\frac{d(d-1)}{2}\mathrm{H}(P)^{\frac{d(d-1)}{2}}(\mathrm{H}(P)!)^{d!+2}, \mathrm{H}(g_i(x',x_n))\right\}.$$

$$\leq 4d((2d\mathrm{H}(f)^{d+1})!)^{d+1}(2d\mathrm{H}(f)^{d+1})^2\mathrm{Deg}(g)\times \tag{3}$$

$$\times \max\left\{d!\frac{d(d-1)}{2}\,(2d\mathrm{H}(f)^{d+1}))^{\frac{d(d-1)}{2}}((2d\mathrm{H}(f)^{d+1})!)^{d!+2},\right.$$
$$\left. p^e 2^{p^e}\mathrm{Deg}(g)^{2p^e\mathrm{Deg}(g)+4p^e}\left(\mathrm{H}(g)+\frac{p^e(p^e-1)}{2}\right)\right\}$$
$$\leq d^{d^{O(d)}}\mathrm{Deg}(g)^{2d(\mathrm{Deg}(g)+2)}(\mathrm{H}(g)+1)$$

since $\mathrm{Deg}(g_i(x',x_n)) = \mathrm{Deg}(g(x',x_n^{p^e}))$ and $\mathrm{H}(g_i(x',x_n)) = \mathrm{H}(g(x',x_n^{p^e}))$. Finally, since

$$g_i(x',x_n^{p^e}) = P\,q_i(x',x_n^{p^e}) + \sum_{j=0}^{D-1} r_{i,j}(x')x_n^{jp^e}$$

and

$$r = \sum_{i=0}^{p^e-1}\sum_{j=0}^{D-1} r_{i,j}(x')x_n^{jp^e+i}$$

by unicity of the remainder in the Weierstrass division, we obtain

$$\mathrm{H}(r) \leq d^{d^{O(d)}}\mathrm{Deg}(g)^{O(d\,\mathrm{Deg}(g))}(\mathrm{H}(g)+1).$$

Moreover

$$\mathrm{Deg}(r_{i,j}), \mathrm{Deg}(r) \leq \mathrm{H}(f)!\mathrm{H}(f)^D\mathrm{Deg}(g_i)^D \quad \forall i,j$$

since $r_{i,j}$ and $r \in \Bbbk(x',\alpha_1,...,\alpha_D, g_i(x',\alpha_1),....,g_i(x',\alpha_D))$ (as shown in the proof of Lemma 4.2). □

Lemma 4.4. *For an integer d we have*

$$d^{d^{O(d)}} = 2^{2^{O(d^2)}}.$$

Proof. For d large enough there exists a constant $C > 0$ such that

$$d\ln(d) + \ln(\ln(d)) \leq Cd^2 + \ln(\ln(2)) + \ln(2).$$

Thus

$$d^d\ln(d) \leq \ln(2)2^{Cd^2}$$

and

$$d^{d^d} \leq 2^{2^{Cd^2}}$$

□

Theorem 4.5. *Let $\Bbbk$ be any field. Let f be an algebraic power series which is x_n-regular of order d. Let g be any algebraic power series. Then there exist unique algebraic power series q and r such that $r \in \Bbbk\langle x'\rangle[x_n]$ is of degree $< d$ in x_n and*

$$g = fq + r.$$

Moreover we have the following bounds:

i) *if* $char(\Bbbk) = 0$*:*

$$H(r) \leq 2^{2^{O(H(f)^2)}} Deg(g)^{5d^2}(H(g)+1),$$
$$H(q) \leq 2^{2^{O(H(f)^2)}} Deg(g)^{5d^2+2d+3} Deg(f)(H(g)+1).$$

ii) *if* $char(\Bbbk) > 0$*:*

$$H(r) \leq 2^{2^{O(H(f)^2)}} Deg(g)^{10d^3(Deg(g)+2)}(H(g)+1),$$
$$H(q) \leq 2^{2^{O(H(f)^2)}} Deg(g)^{10d^3(Deg(g)+2)+2d+3} Deg(f)(H(g)+1).$$

In both cases we have

$$Deg(r) \leq H(f)!H(f)^d Deg(g)^d,$$
$$Deg(q) \leq H(f)!H(f)^d Deg(g)^{d+1}.$$

Proof. Let us write $f = u.P$ where u is a unit and P a Weierstrass polynomial in x_n. Let us decompose P into the product of irreducible Weierstrass polynomials

$$P = P_1 ... P_s.$$

Let us consider the following Weierstrass divisions:

$$g = P_1 Q_1 + R_1$$
$$Q_1 = P_2 Q_2 + R_2$$
$$\cdots\cdots$$
$$Q_{s-1} = P_s Q_s + R_s.$$

Then

$$g = P_1 ... P_s Q_s + R_1 + P_1 R_2 + P_1 P_2 R_3 + \cdots + P_1 \cdots P_{s-1} R_s$$

and

$$r := R_1 + P_1 R_2 + P_1 P_2 R_3 + \cdots + P_1 \cdots P_{s-1} R_s$$

is the remainder of the division of g by P by unicity of the Weierstrass division. Here $s \leq d$ since P is monic of degree d in x_n. Let d_i be the degree in x_n of the polynomial P_i for $1 \leq i \leq s$. Let us choose $1 \leq i \leq s$ and let us denote by α_1,..., $\alpha_{d_i} \in \mathbb{K}$ the roots of P_i.
First let us prove the Lemma when $\mathrm{char}(\Bbbk) = 0$. In this case these roots are distinct. Then

$$P_i = \prod_{i=1}^{d_i} (x_n - \alpha_i).$$

Since $\mathrm{H}(x_n - \alpha_i) \leq \mathrm{H}(\alpha_i) + \mathrm{Deg}(\alpha_i) \leq 2\mathrm{H}(f)$ (by Lemma 3.5) and $\mathrm{Deg}(x_n - \alpha_i) = \mathrm{Deg}(\alpha_i) \leq \mathrm{H}(f)$ then

$$\mathrm{H}(P_i) \leq 2\mathrm{H}(f)^{\mathrm{H}(f)+2}$$

and

$$\mathrm{Deg}(P_i) \leq \mathrm{H}(f)!$$

since P_i is in the extension of $\Bbbk(x)$ generated by the roots of f.
By Lemma 4.2, the height of R_1 is bounded by

$$2^{2^{O(d_1^2)}} \cdot \mathrm{H}(P_1) \cdot \mathrm{Deg}(g) \cdot (\mathrm{H}(g)+1) \leq 2^{2^{O(d^2)}} \mathrm{H}(f)^{\mathrm{H}(f)+2} \cdot \mathrm{Deg}(g) \cdot (\mathrm{H}(g)+1)$$

and $\mathrm{Deg}(R_1) \leq \mathrm{H}(f)!\mathrm{H}(f)^d\mathrm{Deg}(g)^d$. So

$$\begin{aligned}\mathrm{H}(Q_1) = \mathrm{H}\left(\frac{g-R_1}{P_1}\right) &\leq 2\mathrm{Deg}(P_1)\mathrm{Deg}(g-R_1)\times \\ &\times \max\{\mathrm{H}(P_1), 2\mathrm{Deg}(g)\mathrm{Deg}(R_1)\max\{\mathrm{H}(g),\mathrm{H}(R_1)\}\} \\ &\leq 8\mathrm{H}(f)!\mathrm{Deg}(g)^2\mathrm{Deg}(R_1)^2\max\{\mathrm{H}(g),\mathrm{H}(R_1)\}. \\ &\leq 2^{2^{O(d)}}(\mathrm{H}(f)!)^3\mathrm{H}(f)^{\mathrm{H}(f)+2d+2}\mathrm{Deg}(g)^{2d+3}(\mathrm{H}(g)+1).\end{aligned}$$

Still by Lemma 4.2 we have

$$\mathrm{H}(R_i) \leq 2^{2^{O(d^2)}}\mathrm{H}(f)^{\mathrm{H}(f)+2}\mathrm{Deg}(Q_{i-1})(\mathrm{H}(Q_{i-1})+1),$$

$$\begin{aligned}\mathrm{H}(Q_i) &\leq 2\mathrm{Deg}(P_i)\mathrm{Deg}(Q_{i-1}-R_i)\times \\ &\times \max\{\mathrm{H}(P_i), 2\mathrm{Deg}(R_i)\mathrm{Deg}(Q_{i-1})\max\{\mathrm{H}(R_i),\mathrm{H}(Q_{i-1})\}\} \\ &\leq 8\mathrm{Deg}(P_i)\mathrm{Deg}(Q_{i-1})^2\mathrm{Deg}(R_i)^2\mathrm{H}(R_i).\end{aligned}$$

Exactly as in the proof of Lemma 4.2 we have

$$R_i \in \Bbbk(x, \alpha_1, ..., \alpha_d, Q_{i-1}(x', \alpha_1), ..., Q_{i-1}(x', \alpha_d)).$$

Since $Q_{i-1} = \frac{Q_{i-2}-R_{i-1}}{P_{i-1}}$ we obtain, by induction,

$$Q_{i-1}(x', a_k) \in \Bbbk(x', \alpha_1, ..., \alpha_d, Q_{i-2}(x', \alpha_1), ..., Q_{i-2}(x', \alpha_d))$$

thus

$$R_i, Q_i \in \Bbbk(x, \alpha_1, ..., \alpha_d, g(x', \alpha_1), ..., g(x', \alpha_d)) \quad \forall i$$

and

$$\mathrm{Deg}(R_i), \mathrm{Deg}(Q_i) \leq \mathrm{H}(f)!\mathrm{H}(f)^d\mathrm{Deg}(g)^d \quad \forall i.$$

Thus

$$\mathrm{H}(Q_i) \leq 16\mathrm{H}(f)^{\mathrm{H}(f)+2}\left(\mathrm{H}(f)!\mathrm{H}(f)^d\mathrm{Deg}(g)^d\right)^4\mathrm{H}(R_i)$$

Thus

$$\mathrm{H}(R_i) \leq 2^{2^{O(d^2)}}(\mathrm{H}(f)!)^5\mathrm{H}(f)^{2\mathrm{H}(f)+4d+4}\mathrm{Deg}(g)^{5d}(\mathrm{H}(R_{i-1})+1)$$

Since $d \leq \mathrm{H}(f)$ and $s \leq d$, by induction we obtain

$$\mathrm{H}(R_i) \leq 2^{2^{O(\mathrm{H}(f)^2)}}\mathrm{Deg}(g)^{5d^2}(\mathrm{H}(g)+1).$$

Thus

$$\mathrm{H}(r) \leq 2^{2^{O(\mathrm{H}(f)^2)}}\mathrm{Deg}(g)^{5d^2}(\mathrm{H}(g)+1)$$

and

$$\mathrm{Deg}(r) \leq \mathrm{H}(f)!\mathrm{H}(f)^d\mathrm{Deg}(g)^d.$$

Since $q = \frac{g-r}{f}$,

$$\mathrm{H}(q) \leq 4\mathrm{Deg}(f)\mathrm{Deg}(g-r)\max\{\mathrm{H}(g-r),\mathrm{H}(f)\}.$$

Since f and $g - r \in \Bbbk(x, \alpha_1, ..., \alpha_d, g(x', \alpha_1), ..., g(x', \alpha_d), g(x))$, we have

$$\mathrm{Deg}(g-r), \mathrm{Deg}(q) \leq \mathrm{H}(f)!\mathrm{H}(f)^d\mathrm{Deg}(g)^{d+1}.$$

Thus

$$\begin{aligned}\mathrm{H}(q) &\leq 8(\mathrm{H}(f)!)^2\mathrm{H}(f)^{2d}\mathrm{Deg}(g)^{2d+3}\mathrm{Deg}(f)\mathrm{H}(r) \\ &\leq 2^{2^{O(\mathrm{H}(f)^2)}}\mathrm{Deg}(g)^{5d^2+2d+3}\mathrm{Deg}(f)(\mathrm{H}(g)+1).\end{aligned}$$

In the case $\mathrm{char}\,(\Bbbk) = p > 0$ the proof is completely similar using Lemma 4.3 so we skip the details. □

5. Ideal membership problem in localizations of polynomial rings

Before bounding the complexity of the Ideal Membership Problem in the ring of algebraic power series we review this problem in the ring of polynomials and give extensions to localizations of the ring of polynomials that may be of independent interest.

Let $\Bbbk$ be a field and $x := (x_1, ..., x_n)$. The following theorem is well known (it is attributed to G. Hermann [He26] but a modern and correct proof is given in the appendix of [MM82]):

Theorem 5.1. [He26][MM82] *Let $\Bbbk$ be a infinite field. Let M be a submodule of $\Bbbk[x]^q$ generated by vectors f_1,..., f_p whose components are polynomials of degrees less than d. Let $f \in \Bbbk[x]^q$. Then $f \in M$ if and only if there exist a_1,..., $a_p \in \Bbbk[x]$ of degrees $\leq \deg(f) + (pd)^{2^n}$ such that*

$$f = a_1 f_1 + \cdots + a_p f_p.$$

If we work over the local ring $\Bbbk[x]_{(x)}$ the situation is a bit different. Saying that $f \in \Bbbk[x]^q$ is in $\Bbbk[x]_{(x)}M$ is equivalent to say that there exist polynomials a_1,..., a_p and u, $u \notin (x)$, such that

$$uf = a_1 f_1 + \cdots + a_p f_p. \tag{4}$$

There exists an analogue of Buchberger algorithm to compute Gröbner basis in local rings introduced by T. Mora [Mo82] but it does not give effective bounds on the degrees of the a_i. We can also do the following:
Saying that (4) is satisfied is equivalent to say that there exist polynomials a_1,..., a_p, b_1,.., b_n such that

$$f = a_1 f_1 + \cdots + a_p f_p + b_1 x_1 f + \cdots + b_n x_n f.$$

In this case $u = 1 - \sum_i x_i b_i$.
Thus by applying Theorem 5.1, we see that $f \in \Bbbk[x]_{(x)}M$ if and only if (4) is satisfied for polynomials u, a_1,...,a_p of degrees $\leq \deg(f) + ((p+n)\max\{d, \deg(f)+1\})^{2^n}$. But this bound is not linear in $\deg(f)$ any more, which may be interesting if f_1,..., f_p are fixed and f varies.
Nevertheless we can prove the following result:

Theorem 5.2. *For any n, q and $d \in \mathbb{N}$ there exists an integer $\gamma(n,q,d)$ such that $\gamma(n,q,d) = (2d)^{2^{O(n+q)}}$ and satisfying the following property:*
Let $\Bbbk$ be an infinite field, M be a submodule of $\Bbbk[x_1, \cdots, x_n]^q$ generated by vectors f_1,..., f_p of degree $\leq d$ and let $f \in \Bbbk[x]^q$. Let P be a prime ideal of $\Bbbk[x]$. Then $f \in \Bbbk[x]_P M$ if and only if there exist polynomials a_1,..., a_p of degrees $\leq \deg(f) + \gamma(n,q,d)$ and u, $u \notin P$, of degree $\leq \gamma(n,d)$ such that

$$uf = a_1 f_1 + \cdots + a_p f_p.$$

Proof. Let S be the ring defined as follows (this is the idealization of M - see [Na62]): S is equal to $\Bbbk[x] \times \Bbbk[x]^q$ and we define:

$$(p, f) + (p', f') := (p + p', f + f')$$

$$(p,f).(p',f') := (pp', pf' + p'f) \quad \forall (p,f),(p',f') \in \Bbbk[x] \times \Bbbk[x]^q.$$

Let $I := \{0\} \times M \subset S$. Then I is an ideal of S and it is generated by $(0, f_1)$,..., $(0, f_q)$.
Moreover S is isomorphic to the ring

$$S' := \frac{\Bbbk[x_1, ..., x_n, y_1, ..., y_q]}{(y_1, ..., y_q)^2}$$

and the isomorphism $\sigma : S \longrightarrow S'$ is defined as follows:
If $(p, f) \in S$, $f := (f^{(1)}, \cdots, f^{(q)})$, then $\sigma(p, f)$ is the image of $r + f^{(1)}y_1 + \cdots + f^{(q)}y_q$ in S'.
Thus, by identifying S and S', we have the following equivalences:

$$f \in M \Longleftrightarrow (0, f) \in I \Longleftrightarrow f^{(1)}(x)y_1 + \cdots + f^{(q)}(x)y_q \in I + (y)^2.$$

Let us assume that the theorem is proved when M is an ideal of $\Bbbk[x]$. If we write $f_i = (f_{i,1}, \cdots, f_{i,q})$ for $1 \leq i \leq p$ then $I + (y)^2$ is generated by $\widetilde{f_1} := \sum_{j=1}^q f_{1,j}y_1$,..., $\widetilde{f_p} := \sum_{j=1}^q f_{p,j}y_q$ and the y_iy_j for $1 \leq i \leq j \leq q$, whose degrees are less than $d+2$. Thus, by assumption, there exists $a_1(x, y)$,..., $a_p(x, y)$, $a_{i,j}(x, y)$ for $1 \leq i \leq j \leq$ such that

$$f^{(1)}(x)y_1 + \cdots + f^{(q)}(x)y_q = \sum_{i=1}^p a_i\widetilde{f_i} + \sum_{1 \leq i \leq j \leq q} a_{i,j}y_iy_j$$

and

$$\deg(a_k),\ \deg(a_{i,j}) \leq \deg(f) + \gamma(n + q, d + 2)$$

where $\gamma(n + q, d + 2) \leq (2d)^{2^{O(n+q)}}$. Since

$$f(x) = \sum_{i=1}^p a_i(x, 0)f_i(x)$$

this proves the theorem. Thus we only need to prove the theorem when $M = I$ is an ideal of $\Bbbk[x]$.
Let $I = Q_1 \cap \cdots \cap Q_s$ be an irredundant primary decomposition of I in $\Bbbk[x]$. Let us assume that Q_1,..., $Q_r \subset P$ and $Q_i \not\subset P$ for $i > r$. Then

$$I\Bbbk[x]_P = Q_1\Bbbk[x]_P \cap \cdots \cap Q_r\Bbbk[x]_P$$

is an irredundant primary decomposition of $I\Bbbk[x]_P$ in $\Bbbk[x]_P$ (see Theorem 17, Chap. 4 [ZS58]). Let J be the ideal of $\Bbbk[x]$ defined by $J = Q_1 \cap \cdots \cap Q_r$. Obviously $I\Bbbk[x]_P = J\Bbbk[x]_P$ and moreover for any $f \in \Bbbk[x]$, $f \in J\Bbbk[x]_P$ if and only if $f \in J$. Indeed, $f \in J\Bbbk[x]_P$ if and only if there exists $u \notin P$ such that $uf \in Q_i$ for $i = 1, ..., r$, but since $u \notin P$ and $Q_i \subset P$, then $f \in Q_i$ for all $1 \leq i \leq r$ and $f \in J$.

Each ideal Q_i may be generated by polynomials of degree $\leq (2d)^{2^{O(n)}}$ and this bound depends only on n and d (see Statements 63, 64 and 64 [Se74]). By Statement 56 of [Se74], the ideal J is generated by polynomials of degrees $\leq (2d)^{2^{O(n)}}$ and once more this bound depends only on n and d. Let g_1,..., g_t be such generators of J. Since $\deg(g_i) \leq (2d)^{2^{O(n)}}$ for any i, then t will be bounded by the number of monomials in x_1,..., x_n of degree $\leq (2d)^{2^{O(n)}}$, thus $t \leq \binom{(2d)^{2^{O(n)}} + n + 1}{n} \leq (2d)^{2^{O(n)}}$ also.

If $f \in I\Bbbk[x]_P$, then $f \in J$ and by Theorem 5.1, there exist polynomials c_1,..., c_t such that

$$f = c_1 g_1 + \cdots + c_t g_t$$

where $\deg(c_i) \leq \deg(f) + (td)^{2^n} \leq \deg(f) + (2d)^{2^{O(n)}}$ for any i.
Let J' be the ideal of $\Bbbk[x]$ equal to $Q_{r+1} \cap \cdots \cap Q_s$. Then as for J, J' is generated by polynomials of degrees $\leq (2d)^{2^{O(n)}}$. Since $J' \not\subset P$, one of these generators is not in P. Let u be such a polynomial. Then we have $ug_i \in J \cap J' = I$ for any i. Thus there exist polynomials $b_{i,j}$, for $1 \leq i \leq t$ and $1 \leq j \leq p$, such that

$$ug_i = \sum_j b_{i,j} f_j.$$

Still by Theorem 5.1, we may choose the $b_{i,j}$ such that $\deg(b_{i,j}) \leq (2d)^{2^{O(n)}}$. Hence

$$uf = \sum_j \left(\sum_i c_i b_{i,j} \right) f_j.$$

Then the result follows since $\deg(u) \leq (2d)^{2^{O(n)}}$ and

$$\deg\left(\sum_i c_i b_{i,j} \right) \leq \deg(f) + (2d)^{2^{O(n)}}.$$

□

Remark 5.3. Let S be a multiplicative closed subset of $\Bbbk[x]$. The previous proof does not apply to the ring $S^{-1}\Bbbk[x]$ if $\Bbbk[x]\backslash S$ is not an ideal. The only problem in the proof occurs when we look for a polynomial $u \in J' \cap S$. Saying that $J' \cap S \neq \emptyset$ is not equivalent to say that for any system of generators of J' one of these generators is in S (since the complement of S is not an ideal). Thus we have no bound on the degree of such a u. Nevertheless, by choosing $u \in J' \cap S$ independently on f, this gives the following result:

Proposition 5.4. *Let $\Bbbk$ be an infinite field. Let M be a submodule of $\Bbbk[x_1, ..., x_n]^q$ generated by the vectors f_1,..., f_p and S be a multiplicative closed subset of $\Bbbk[x]$. Then there exists a constant $C > 0$ (depending only on M) such that the following holds:*
For any $f \in \Bbbk[x]^q$, $f \in S^{-1}M$ if and only if there exist polynomials a_1,..., a_p of degrees $\leq deg(f) + C$ and u, $u \in S$, of degree $\leq C$ such that

$$uf = a_1 f_1 + \cdots + a_p f_p.$$

6. Ideal membership in rings of algebraic power series

Theorem 6.1. *Let $\Bbbk$ be any infinite field. Then there exists an effective function $C(n, q, p, H_1, D_1, D_2)$ such that the following holds:*
Let $f = (f_1, \cdots, f_q)$ and $g_1 = (g_{1,1}, \cdots, g_{1,q})$,..., $g_p = (g_{p,1}, \cdots, g_{p,q})$ be vectors of $\Bbbk\langle x_1, \cdots, x_n\rangle^q$ with

$$H(g_i) \leq H_1 \text{ for all } i,\ H(f) \leq H_2,$$
$$[\Bbbk(x, g_{i,j})_{1\leq j\leq p,\ 1\leq i\leq q} : \Bbbk(x)] \leq D_1,$$
$$[\Bbbk(x, f_i)_{1\leq i\leq q} : \Bbbk(x)] \leq D_2$$

Let us assume that f is one the $\Bbbk\langle x\rangle$-module generated by the vectors g_j. Then there exist algebraic power series a_j such that

$$f_i = \sum_{j=1}^{p} a_j g_{i,j}, \qquad 1 \leq i \leq q \tag{5}$$

and

$$H(a_j) \leq C\,(n, q, p, H_1, D_1, D_2) \cdot (H_2 + 1) \quad \forall j.$$

Proof. We set $H_g := \max_{i,j} \mathrm{H}(g_{i,j})$, $D_g := \max_{i,j} \mathrm{Deg}(g_{i,j})$, $H_f := \max_i \mathrm{H}(f_i)$ and $D_f := \max_i \mathrm{Deg}(f_i)$. Let G be the $p \times q$ matrix whose entries are the $g_{i,j}$. We assume that the rank of G is $q \leq p$ (either the system has no solution or some equations may be removed) and that the first q columns are linearly independent. Let Δ be the determinant of these first q columns. By a linear change of coordinates me may assume that Δ is x_n-regular of degree $d \leq \mathrm{H}(\Delta) \leq q!qD_g^{2q}H_g$ by Lemma 3.5 since $\Bbbk$ is infinite. By Lemma 4.1 we can write $\Delta = u \cdot P$ where P is a unit and P a Weierstrass polynomial of degree d with

$$\mathrm{H}(P) \leq 2d\mathrm{H}(\Delta)^{d+1} \leq 2\mathrm{H}(\Delta)^{\mathrm{H}(\Delta)+2} \leq 2\left(q!qD_g^{2q}H_g\right)^{q!qD_g^{2q}H_g+2}.$$

Set

$$F_i(x, A) := \sum_{j=1}^{p} g_{i,j}(x)A_j - f_i(x) \quad \forall i$$

where A_1,..., A_p are new variables. Let $a_{i,k}(x')$ be algebraic power series of $\Bbbk\langle x'\rangle$ for $1 \leq i \leq p$ and $0 \leq k \leq d-1$. Then let us set

$$a_i^* := \sum_{k=0}^{d-1} a_{i,k}(x')x_n^k \quad \text{for } 1 \leq i \leq p,$$

$$a^* := (a_1^*, ..., a_p^*).$$

Let $A_{i,k}$, $1 \leq i \leq p$, $0 \leq k \leq d-1$, be new variables and let us set

$$A_i^* := \sum_{k=0}^{d-1} A_{i,k}x_n^k, \qquad 1 \leq i \leq p$$

and

$$A^* := (A_1^*, ..., A_p^*).$$

Let us consider the Weierstrass division of $F_i(x, A^*)$ by Δ:

$$F_i(x, A^*) = \Delta.Q_i(x, A^*) + \sum_{l=0}^{d-1} R_{i,l}(x', A^*)x_n^l = \Delta.Q_i(x, A^*) + R_i.$$

Let us consider the Weierstrass divisions:

$$g_{i,j}(x)x_n^k = \Delta.Q_{i,j,k}(x) + \sum_{l=0}^{d-1} R_{i,j,k,l}(x')x_n^l = \Delta.Q_{i,j,k}(x) + R_{g_{i,j}},$$

$$f_i(x) = \Delta.Q_i'(x) + \sum_{l=0}^{d-1} R_{i,l}'(x')x_n^l = \Delta.Q_i'(x) + R_{f_i}.$$

By unicity of the remainder and the quotient of the Weierstrass division we obtain:

$$Q_i(x,A^*)=\sum_{j=1}^{p}\sum_{k=0}^{d-1}Q_{i,j,k}(x)A_{j,k}-Q'_i(x),$$

$$R_{i,l}(x',A^*)=\sum_{j=1}^{p}\sum_{k=0}^{d-1}R_{i,j,k,l}(x')A_{j,k}-R'_{i,l}(x'),$$

Hence $Q_i(x',A^*)$ and $R_{i,l}(x',A^*)$ are linear with respect to the variables $A_{i,j}$.
If $R_{i,l}(x',a^*)=0$ for all i and l, then $F_i(x,a^*)\in(\Delta)\ \forall i$. This means that there exists a vector of $\mathbb{k}\langle x\rangle^q$, denoted by $b(x)$, such that

$$G(x).a^*(x)-f(x)=\Delta(x).b(x) \tag{6}$$

where $G(x)$ is the $q\times p$ matrix with entries $g_{i,j}$ and $f(x)$ is the vector with entries $f_i(x)$. In fact we can choose the vector of entries $Q_i(x,a^*)$ for $b(x)$.
Let $G'(x)$ be the adjoint matrix of the $q\times q$ matrix built from $G(x)$ by taking only the first q columns. Then

$$G'(x).G(x)=\begin{pmatrix}\Delta(x).\mathbb{1}_q & ?\end{pmatrix}.$$

Thus, by multiplying (6) by $G'(x)$ on the left side, we have

$$\begin{pmatrix}\Delta(x)a_1^*(x)+P_1(a_{q+1}^*(x),\cdots,a_p^*(x))\\ \Delta(x)a_2^*(x)+P_2(a_{q+1}^*(x),\cdots,a_p^*(x)\\ \vdots\\ \Delta(x)a_q^*(x)+P_q(a_{q+1}^*(x),\cdots,a_p^*(x))\end{pmatrix}-G'(x).f(x)=\Delta(x).G'(x).b(x)$$

for some P_i depending linearly on $a_{q+1}^*(x),\cdots,a_p^*(x)$. Then we set

$$a_i(x):=a_i^*(x)-c_i(x)\ \text{ for } 1\leq i\leq q,$$

$$a_i(x):=a_i^*(x)\ \text{ for } q<i\leq p$$

where $c(x)$ is the vector $G'(x).b(x)$. Since $G'(x)$ has rank q, this shows that

$$G(x).a(x)-f(x)=0$$

i.e. $a(x)$ is a solution of (5).

For simplicity we will bound the height and the degree of $a(x)$ when $\mathrm{char}\,(\mathbb{k})=0$. The bounds in positive characteristic are similar. By theorem 4.5 we have

$$\mathrm{H}(R_{i,j,k,l}(x'))\leq 2^{2^{O(\mathrm{H}(\Delta)^2)}}D_g^{5d^2}(D_gH_g+1)\leq 2^{2^{O(q^{2q}D_g^{4q}H_g^2)}},$$

$$\mathrm{H}(R'_{i,l}(x'))\leq 2^{2^{O(\mathrm{H}(\Delta)^2)}}D_f^{5d^2}(H_f+1)\leq 2^{2^{O(q^qD_g^{2q}H_g)}}D_f^{5d^2}(H_f+1),$$

$$\mathrm{H}(Q_{i,j,k}(x))\leq 2^{2^{O(q^{2q}D_g^{4q}H_g^2)}}D_g^{5d^2+2d+3}\mathrm{Deg}(\Delta)(D_gH_g+1)\leq 2^{2^{O(q^{2q}D_g^{4q}H_g^2)}},$$

$$\begin{aligned}\mathrm{H}(Q'_i(x))\leq 2^{2^{O(q^{2q}D_g^{4q}H_g^2)}}&D_f^{5d^2+2d+3}\mathrm{Deg}(\Delta)(H_f+1)\\ &\leq 2^{2^{O(q^{2q}D_g^{4q}H_g^2)}}D_f^{5d^2+2d+3}(H_f+1).\end{aligned}$$

$$\begin{aligned}\mathrm{Deg}(R_{i,j,k,l}(x'))\leq \mathrm{H}(\Delta)!\mathrm{H}(\Delta)^{\mathrm{H}(\Delta)}&D_g^{\mathrm{H}(\Delta)}\\ &\leq((q!q)^2D_g^{4q+1}H_g^2)^{q!qD_g^{2q}H_g}\leq 2^{2^{O(q^{2q}D_g^{4q}H_g^2)}}\end{aligned}$$

$$\mathrm{Deg}(R'_{i,l}(x')) \leq \mathrm{H}(\Delta)!\mathrm{H}(\Delta)^{\mathrm{H}(\Delta)} D_f^{\mathrm{H}(\Delta)} \leq ((q!q)^2 D_g^{4q} D_f H_g^2)^{q!qD_g^{2q}H_g}$$
$$\leq (2D_f)^{2^{O(q^{2q} D_g^{4q} H_g^2)}}$$
$$\mathrm{Deg}(Q_{i,j,k}(x)) \leq ((q!q)^2 D_g^{4q+1} H_g^2)^{q!qD_g^{2q}H_g} D_g \leq 2^{2^{O(q^q D_g^{2q} H_g)}}$$
$$\mathrm{Deg}(Q'_i(x)) \leq ((q!q)^2 D_g^{4q} D_f H_g^2)^{q!qD_g^{2q}H_g} D_f \leq (2D_f)^{2^{O(q^q D_g^{2q} H_g)}}$$

So we obtain

$$\mathrm{H}(b(x)) \leq 2(\mathrm{Deg}(Q_{i,j,k}(x))D_{a^*})^{pd}\mathrm{Deg}(Q'_i(x))\times$$
$$\times \max\left\{2pd(\mathrm{Deg}(Q_{i,j,k}(x))D_{a^*})^{pd+1} \max\{\mathrm{H}(Q_{i,j,k}(x)), H_{a^*}\}, \mathrm{H}(Q'_i(x))\}\right\}$$
$$\leq (2D_f + 2^p)^{2^{O(q^{2q} D_g^{4q} H_g^2)}} D_{a^*}^{2H_g p+1} H_{a^*}(H_f+1)$$
$$\mathrm{Deg}(b(x)) \leq (2D_f)^{2^{O(q^q D_g^{2q} H_g)}} D_{a^*}.$$

We have

$$\mathrm{H}(\det(G(x))) \leq q.q!D_g^{q!+q}H_g.$$

The height of the coefficients of $G'(x)$ is less than

$$(q-1)(q-1)!D_g^{(q-1)!+(q-1)}H_g$$

Thus the height of the coefficients of $G'(x)$ is less than

$$2q!qD_g^{q!+q+2}H_g.$$
$$\mathrm{H}(G'(x).b(x)) \leq 2q(\mathrm{Deg}(G'(x))\mathrm{Deg}(b(x))^{q+1} \max\{\mathrm{H}(G'(x)), \mathrm{H}(b(x))\}$$
$$\leq 2D_g(2D_f)^{2^{O(q^q D_g^{2q} H_g)}} D_{a^*}(2D_f+2^p)^{2^{O(q^{2q} D_g^{4q} H_g^2)}} D_{a^*}^{2H_g p+1} H_{a^*}(H_f+1)$$
$$\leq (2D_f + 2^p)^{2^{O(q^{2q} D_g^{4q} H_g^2)}} D_{a^*}^{2H_g p+2} H_{a^*}(H_f+1)$$

Hence

$$\mathrm{H}(a(x)) \leq (2D_f + 2^p)^{2^{O(q^{2q} D_g^{4q} H_g^2)}} D_{a^*}^{2H_g p+3} H_{a^*}(H_f+1).$$

Moreover

$$\mathrm{Deg}(a(x)) \leq D_{a^*}\mathrm{Deg}(b(x)) \leq (2D_f)^{2^{O(q^q D_g^{2q} H_g)}} D_{a^*}^2.$$

Let

$$\Lambda_H(n,p,q,D_f,D_g,H_f,H_g)$$

be a uniform bound on the height of the a_i and

$$\Lambda_D(n,p,q,D_f,D_g,H_f,H_g)$$

be a uniform bound on the degree of the a_i. Thus we have

$$\Lambda_H(n,p,q,D_f,D_g,H_f,H_g) \leq (2D_f+2^p)^{2^{O(\Phi^2)}}\times$$
$$\times\Lambda_D\left(n-1, pd, qd, (2D_f)^{2^{O(\Phi^2)}},\ 2^{2^{O(\Phi^2)}}, 2^{2^{O(\Phi^2)}}, 2^{2^{O(\Phi^2)}}\right)^{2H_g p+3}\times$$
$$\times\Lambda_H\left(n-1, pd, qd, (2D_f)^{2^{O(\Phi^2)}},\ 2^{2^{O(\Phi^2)}}, 2^{2^{O(\Phi^2)}}, 2^{2^{O(\Phi^2)}}\right)(H_f+1)$$

and

$$\Lambda_D(n,p,q,D_f,D_g,H_f,H_g) \leq (2D_f)^{2^{O(\Phi)}}\times$$
$$\times\Lambda_D\left(n-1, pd, qd, (2D_f)^{2^{O(\Phi^2)}}, 2^{2^{O(\Phi^2)}}, 2^{2^{O(\Phi^2)}}, 2^{2^{O(\Phi^2)}}\right)^2$$

where

$$d \leq \Phi := q^q D_g^{2q} H_g$$

Since linear equations with coefficients in a field $\Bbbk$ which have solutions have solution in $\Bbbk$ we see that:

$$\Lambda_H(0,p,q,D_f,D_g,H_f,H_g) = 0,$$
$$\Lambda_D(0,p,q,D_f,D_g,H_f,H_g) \leq 1.$$

Then the result is proved by induction on n. □

Remark 6.2. The proof of this result does not give a nice bound on the functions $C(n,q,p,H_1,D_1,D_2)$ or $\Lambda_D(n,p,q,D_f,D_g,H_f,H_g)$. One can check that $\Lambda_D(n,p,q,D_f,D_g,H_f,H_g)$ is bounded by a tower of exponential of length $3n$ of the form

$$(2D_f)^{2^{2^{\cdot^{\cdot^{\cdot^{O(qD_gH_g)}}}}}}.$$

For $C(n,q,p,H_1,D_1,D_2)$ we obtain the same kind of bound.
In positive characteristic, the bounds are more complicated and are not polynomial in D_f since the bounds on the complexity of the Weierstrass Division are not polynomial in D_f.

7. Proof of Theorem 1.1

7.1. **Proof of (i)⟹(iii).** We will denote by R_n the ring of algebraic power series in n variables over a field $\Bbbk$ and $\widehat{R}_n$ its $(x_1,..,x_n)$-adic completion. If $\Bbbk$ is a finite field we replace $\Bbbk$ by $\Bbbk(t)$ where t is transcendental over $\Bbbk$ - this does not change the problem. Thus we may assume that $\Bbbk$ is infinite.

For any $\Bbbk\langle x\rangle$-module M, we have $\mathrm{ord}_M(m) = \mathrm{ord}_{\widehat{M}}(m)$ for all $m \in M$, thus we may assume M is equal to R_n^s/N for some R_n-submodule N of R_n^s.
We set $e := (e_1,...,e_s)$ where the e_1,..., e_s is the canonical basis of R_n^s. Let us assume that N is generated by $L_1(e)$,..., $L_l(e)$ and let us set $L(e) := (L_1(e),...,L_l(e))$. Let us write

$$L_i(e) = \sum_{j=1}^{s} l_{i,j} e_j \quad \text{for } 1 \leq i \leq l$$

and let H (resp. D) be a bound on the height (resp. the degree) of the $l_{i,j}$.
The proof is done by a double induction on s and k. Let

$$f = f_1 e_1 + \cdots + f_s e_s \in R_n^s.$$

We consider the following cases:

- (1) If $s = 1$ and $N = (0)$, then $M = R_n$ and in this case

$$\mathrm{ord}_M(f) = \mathrm{ord}_{R_n}(f) \leq \mathrm{H}(f)$$

for any algebraic power series f by Lemma 3.6.

- (2) If $s = 1$ and $N \neq (0)$, then $M = \frac{R_n}{I}$ for some ideal I of R_n. After a linear change of variables there exists a Weierstrass polynomial $q(x) \in I$ with respect to x_n, whose coefficients are in R_{n-1}, of degree d in x_n. Then M is isomorphic to R_{n-1}^d/N' for some sub-module N' of R_{n-1}^d. If $f(x) \in R_n$, then the remainder r of the division of f by q (with respect to x_n) has height less than $C_1(\mathrm{H}(f)+1)$ for

some $C_1 > 0$ depending only on $q(x)$ and $\mathrm{Deg}(f)$ (by Theorem 4.5 - moreover C_1 is polynomial in $\mathrm{Deg}(f)$ when $\mathrm{char}\,(\Bbbk) = 0$) and f and r have the same image in M. If $r = r_0 + r_1 x_n + \cdots + r_{d-1} x_n^{d-1}$, with $r_i \in R_{k-1}$ for all i, then the image of r (or f) in R_{k-1}^d/N is the element $(r_0, r_1, ..., r_{d-1})$ whose height is less that $C_1 \cdot (\mathrm{H}(f) + 1)$ still by Theorem 4.5. Moreover $\mathrm{ord}_M(f) = \mathrm{ord}_M(r)$. Since x_n is finite over R_n, there exists a constant $a > 0$ such that $x_n^a \in (x')$, with $x' = (x_1, ..., x_{k-1})$. Thus $(x)^{ac} \subset (x')^c$ for any integer c. So we have:

$$\mathrm{ord}_{R_{k-1}^d/N'}(r) = \sup\{c \in \mathbb{N} \ / \ r \in (x')^c R_{k-1}^d/N'\} \geq \frac{1}{a+1}\mathrm{ord}_M(r).$$

By the induction hypothesis on k there exists $C > 0$ such that

$$\mathrm{ord}_{R_{k-1}^d/N'}(r) \leq C \cdot \mathrm{H}(r) \quad \forall r \in R_{k-1}^d.$$

Thus we have

$$\mathrm{ord}_M(f) = \mathrm{ord}_M(r) \leq (a+1)\mathrm{ord}_{R_{k-1}^d/N}(r) \leq (a+1)C\,\mathrm{H}(r) \leq (a+1)CC_1\,(\mathrm{H}(f)+1).$$

If $\mathrm{char}\,(\Bbbk) = 0$ and C is assumed to depend polynomially on $\mathrm{Deg}(r)$, then $(a+1)CC_1$ depends polynomially on $\mathrm{Deg}(f)$ by Theorem 4.5.

- (3) If f_s is in the ideal of R_n generated by $l_{1,s}$,..., $l_{l,s}$.
Then we can write

$$f_s = a_1 l_{1,s} + \cdots + a_l l_{l,s}$$

where the a_i are algebraic power series with $\mathrm{H}(a_i) \leq C_2(\mathrm{H}(f_s) + 1)$ for all i where $C_2 > 0$ depends only on the $l_{i,s}$ and $\mathrm{Deg}(f_s)$ (by Theorem 6.1). Moreover, when $\mathrm{char}\,(\Bbbk) = 0$, C_2 depends polynomially on $\mathrm{Deg}(f_s) \leq \deg(f)$ by Remark 6.2. Let us set

$$f' := f - \sum_{i=1}^{l} a_i L_i(e).$$

We set $N' = N \cap R_n^{s-1} \times \{0\}$. We denote by M' the sub-module of M equal to

$$\frac{R_n^{s-1} \times \{0\}}{N'}.$$

By the Artin-Rees Lemma there exists a constant $c_0 > 0$ such that

$$(x)^{c+c_0} M \cap M' \subset (x)^c M' \quad \forall c \in \mathbb{N}.$$

Hence we have:

$$\mathrm{ord}_M(f) = \mathrm{ord}_M(f) = \mathrm{ord}_M(f') \leq \mathrm{ord}_{M'}(f') + c_0.$$

By the induction hypothesis on s, there exists $C' > 0$ depending on $\mathrm{Deg}(f')$ (thus on $\mathrm{Deg}(f)$ by Theorem 6.1) such that

$$\mathrm{ord}_{M'}(f') \leq C' \cdot \mathrm{H}(f').$$

If $\mathrm{char}\,(\Bbbk) = 0$ and we assume that C' depends polynomially on $\mathrm{Deg}(f')$, then C' depends polynomially on $\mathrm{Deg}(f)$ by Remark 6.2. Hence

$$\mathrm{ord}_M(f) \leq \mathrm{ord}_{M'}(f') + c_0 \leq C' \cdot \mathrm{H}(f') + c_0 \leq A \cdot \mathrm{H}(f) + B$$

for some constants A and B depending only on the $l_{i,j}$ and $\mathrm{Deg}(f)$. Moreover A and B depend polynomially on $\mathrm{Deg}(f)$ when $\mathrm{char}\,(\Bbbk) = 0$.

- (4) If f_s is not in the ideal of R_n generated by $l_{1,s}$,..., $l_{l,s}$.
Then by the induction hypothesis on k, there exists $C > 0$ depending only on the l_i, s and $\mathrm{Deg}(f_n)$ such that

$$\mathrm{ord}_{R_n}(f_n + a_1 l_{1,s} + \cdots + a_l l_{l,s}) \leq C \cdot \mathrm{H}(f_n)$$

for any $a_i \in R_n$. Moreover C depends polynomially on $\mathrm{Deg}(f_n) \leq \mathrm{Deg}(f)$ when $\mathrm{char}\,(\Bbbk) = 0$. Thus

$$\mathrm{ord}_M(f) = \sup_{a_1,\ldots,a_l \in R_n} \left\{\mathrm{ord}_{R_n^s}(f + a_1 L_1(e) + \cdots + a_l L_l(e))\right\} \leq C \cdot \mathrm{H}(f_n) \leq C \cdot \mathrm{H}(f).$$

7.2. **Proof of (ii)$\Longrightarrow$(i).** Let M be a finite $\widehat{R}_n$-module, $M = \widehat{R}_n^s/N$. As we did before in the proof of Theorem 5.2 we define the ring S as follows: S is equal to $\widehat{R}_n \times M$ and we define:

$$(r, m) + (r', m') := (r + r', m + m')$$
$$(r, m).(r', m') := (rr', rm' + r'm) \quad \forall (r, m), (r', m') \in S.$$

In this case M is seen as an ideal of S by identifying any element $m \in M$ to $(0, m)$. Let L_1,..., L_l be generators of N. Let $y := (y_1, ..., y_s)$ be a vector of new indeterminates. Then S is isomorphic to the following ring:

$$S' := \frac{\widehat{R}_n[y_1, ..., y_s]}{(L_1(y), ..., L_l(y)) + (y)^2}$$

and the isomorphism $\sigma : S \longrightarrow S'$ is defined as follows:
If $(r, p) \in S$, $p := p_1 m_1 + \cdots + p_s m_s$, then $\sigma(r, p)$ is the image of $r + p_1 y_1 + \cdots + p_s y_s$ in S'.

Lemma 7.1. *For any $p \in M$ we have*

$$ord_M(p) + 1 \leq ord_{S'}(\sigma(0, p))$$

where $ord_{S'}$ is the (x, y)-adic order of S'.

Proof. Let us assume that $f \in (x)^c M$. Thus there exist q_1,...,$q_s \in (x)^c \widehat{R}_n$ and a_1,..., $a_l \in \widehat{R}_n$ such that

$$(p_1 - q_1)m_1 + \cdots + (p_s - q_s)m_s = a_1 L_1 + \cdots + a_l L_l.$$

Thus

$$(p_1 - q_1)y_1 + \cdots + (p_s - q_s)y_s = a_1 L_1(y) + \cdots + a_l L_l(y).$$

Thus $\sigma(0, p) \in (x)^c(y)S$. □

Since the order function of S' is the same as the order function of

$$\widehat{S}' = \frac{\Bbbk[\![x_1, ..., x_n, y_1, ..., y_s]\!]}{(L_1(y), ..., L_l(y)) + (y)^2},$$

then M satisfies (ii) of Theorem 1.1 if and only if $\widehat{S}'$ does. Moreover we see that N is generated by algebraic power series if and only if $(L_1(y), ..., L_l(y)) + (y)^2$ is generated by algebraic power series. Thus we may assume that M is a complete local ring, say $M = \widehat{R}_n/I$ for some ideal I.

We set $J := I \cap \Bbbk[x]$ and

$$J_d := \{p \in J \ / \ \deg(p) \leq d\} \quad \forall d \in \mathbb{N}.$$

Then I is generated by algebraic power series if and only if $\mathrm{ht}(I) = \mathrm{ht}(J)$, otherwise $\mathrm{ht}(I) > \mathrm{ht}(J)$. Let $\Bbbk[x]_d$ be the set of polynomials of degree $\leq d$. We set

$$\Phi(d) := \dim_{\Bbbk}\left(\frac{\Bbbk[x]_d}{J_d}\right).$$

Then $d \longmapsto \Phi(d)$ is a polynomial map of degree $p := \dim\left(\frac{\Bbbk[x]}{J}\right)$ for d large enough. Then we define

$$\Psi(d) := \dim_{\Bbbk}\left(\frac{M}{(x)^d}\right).$$

Then $d \longmapsto \Psi(d)$ is a polynomial map of degree $q := \dim(M)$ for d large enough. Thus there exists a constant $a > 0$ such that

$$\Psi(d^p) < \Phi(ad^q) \quad \forall d >> 0.$$

This means that the canonical $\Bbbk$-linear map

$$\frac{\Bbbk[x]_{ad^q}}{J_{ad^q}} \longrightarrow \frac{M}{(x)^{d^p}}$$

is not injective for d large enough. For any d large enough let p_d be a non-zero element of the kernel of this map. By assumption there exists a constant C such that

$$\mathrm{ord}_M(p_d) \leq C \cdot \deg(p_d) \leq Cad^q.$$

Since p_d is in the kernel of the previous $\Bbbk$-linear map, we have $\mathrm{ord}_M(p_d) \geq d^p$, thus

$$Cad^q \geq d^p.$$

But such an inequality is satisfied (for some constant $a > 0$) if and only if $q \geq p$, i.e. if $\dim(M) \geq \dim\left(\frac{\Bbbk[x]}{J}\right)$. This last inequality is equivalent to $\mathrm{ht}(I) \leq \mathrm{ht}(J)$. This proves (ii)$\Longrightarrow$(i) in Theorem 1.1.

8. Grauert-Hironaka-Galligo Division of power series

Let L be a linear form of $\mathbb{R}^n$ with positive coefficients. Let us consider the following order on $\mathbb{N}^n$: for all α, $\beta \in \mathbb{N}^n$, we say that $\alpha \leq \beta$ if

$$(L(\alpha), \alpha_1, ..., \alpha_n) \leq_{lex} (L(\beta), \beta_1, ..., \beta_n)$$

where $\leq_{lex}$ is the lexicographic order. This order induces an order on the set of monomials $x_1^{\alpha_1}...x_n^{\alpha_n}$: we set $x^\alpha \leq x^\beta$ if $\alpha \leq \beta$. This order is called the *monomial order induced by* L. If

$$f := \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha \in \Bbbk[\![x]\!],$$

the *initial exponent* of f with respect to the previous order is

$$\exp(f) := \min\{\alpha \in \mathbb{N}^n \ / \ f_\alpha \neq 0\} = \inf \mathrm{Supp}(f)$$

where the *support* of f is $\mathrm{Supp}(f) := \{\alpha \in \mathbb{N}^n \ / \ f_\alpha \neq 0\}$. The *initial term* of f is $f_{\exp(f)}x^{\exp(f)}$. This is the smallest non-zero monomial in the Taylor expansion of f with respect to the previous order.
Let g_1,..., g_s be elements of $\Bbbk[\![x]\!]$. Set

$$\Delta_1 := \exp(g_1) + \mathbb{N}^n \text{ and } \Delta_i = (\exp(g_i) + \mathbb{N}^n) \setminus \bigcup_{1 \leq j < i} \Delta_j, \text{ for } 2 \leq i \leq s.$$

Finally, set

$$\Delta_0 := \mathbb{N}^n \setminus \bigcup_{i=1}^{s} \Delta_i.$$

We have the following theorem:

Theorem 8.1. [Gr72][Hi77][Ga79] *Set $f \in \Bbbk[\![x]\!]$. Then there exist unique power series q_1,..., q_s, $r \in \Bbbk[\![x]\!]$ such that*

$$f = g_1 q_1 + \cdots + g_s q_s + r$$

$$\exp(g_i) + Supp(q_i) \subset \Delta_i \text{ and } Supp(r) \subset \Delta_0.$$

The power series r is called the remainder *of the division of f by g_1,..., g_s with respect to the given monomial order.*
Moreover if $\Bbbk$ is a valued field and f, g_1,..., g_s are convergent power series, then the q_i and r are convergent power series.

The uniqueness of the division comes from the fact the Δ_i's are disjoint subsets of $\mathbb{N}^n$. The existence of such decomposition in the formal case is proven through the division algorithm:

Set $\alpha := \exp(g)$. Then there exists an integer i_1 such that $\alpha \in \Delta_{i_1}$.
• If $i_1 = 0$, then set $r^{(1)} := \mathrm{in}(g)$ and $q_i^{(1)} := 0$ for any i.
• If $i_1 \geq 1$, then set $r^{(1)} := 0$, $q_i^{(1)} := 0$ for $i \neq i_1$ and $q_{i_1}^{(1)} := \frac{\mathrm{in}(g)}{\exp(g_{i_1})}$.
Finally set $g^{(1)} := g - \sum_{i=1}^{s} g_i q_i^{(1)} - r^{(1)}$. Thus we have $\exp(g^{(1)}) > \exp(g)$. Then we replace g by $g^{(1)}$ and we repeat the preceding process.
In this way we construct a sequence $(g^{(k)})_k$ of power series such that, for any $k \in \mathbb{N}$, $\exp(g^{(k+1)}) > \exp(g^{(k)})$ and $g^{(k)} = g - \sum_{i=1}^{s} g_i q_i^{(k)} - r^{(k)}$ with

$$\exp(g_i) + \mathrm{Supp}(q_i^{(k)}) \subset \Delta_i \text{ and } \mathrm{Supp}(r^{(k)}) \subset \Delta_0.$$

At the limit $k \longrightarrow \infty$ we obtain the desired decomposition.

But in general if f and the g_i are algebraic power series (or even polynomials) then r and the q_i are not algebraic power series as shown by the following example:

Example 8.2 (Kashiwara-Gabber's Example)**.** ([Hi77] p. 75) Let us perform the division of xy by

$$g := (x - y^a)(y - x^a) = xy - x^{a+1} - y^{a+1} + x^a y^a$$

as formal power series in $\Bbbk[\![x, y]\!]$ with $a > 1$ (here we choose a monomial order induced by the linear form $L(\alpha_1, \alpha_2) = \alpha_1 + \alpha_2$). By symmetry the remainder of this division can be written $r(x, y) := s(x) + s(y)$ where $s(x)$ is a formal power series. By substituting y by x^a we get

$$s(x^a) + s(x) - x^{a+1} = 0.$$

This relation yields the expansion

$$s(x) = \sum_{i=0}^{\infty} (-1)^i x^{(a+1)a^i}.$$

Thus the remainder of the division has Hadamard gaps and thus is not algebraic if $\mathrm{char}\,(\Bbbk) = 0$.

Example 8.3. Let $\Bbbk$ be a field of any characteristic. Set

$$f_n := xy - \sum_{i=0}^{n} (-1)^i x^{(a+1)a^i}.$$

Then by the previous example

$$f_n \equiv \sum_{i>n} (-1)^i x^{(a+1)a^i} \text{ mod. } (g).$$

Thus

$$\mathrm{ord}_{\Bbbk[\![x]\!]/(g)}(f_n) \geq (a+1)a^{n+1}.$$

Since f_n is polynomial of degree $(a+1)a^n$, this shows that ii) of Theorem 1.1 is optimal.

9. Generic Kashiwara-Gabber Example

Definition 9.1. Let $\Bbbk$ be a characteristic zero field. A *D-finite power series* f is a formal power series in $\Bbbk[\![x]\!]$ satisfying a linear diffrential equation with polynomial coefficients, i.e. there exist $D \in \mathbb{N}$ and $a_\alpha(x) \in \Bbbk[x]$ (not all equal to 0) for $\alpha \in \mathbb{N}^n$ and $|\alpha| \leq D$ such that

$$\sum_{\alpha \in \mathbb{N}^n, |\alpha| \leq D} a_\alpha(x) \frac{\partial^\alpha f}{\partial x_1^{\alpha_1} \cdots x_n^{\alpha_n}} = 0.$$

Let us mention that by [Li89] any algebraic power series is D-finite.
In Example 8.2, if $\mathrm{char}\,(\Bbbk) = 0$, the remainder is not D-finite neither since D-finite power series have no Hadamard gaps (see [LR86] for instance). We will show that the situation of Example 8.2 is generic in some sense.

Set

$$g_{\underline{a}}(x,y) = xy - \sum_{(i,j)\in E} a_{i,j} x^i y^j$$

where E is a finite subset of $\mathbb{N}^n$, $(1,1) \notin E$ and $\{(2,0),(0,2)\} \not\subset E$, and $\underline{a}$ denotes the vector of entries $a_{i,j} \in \mathbb{C}$. Let us choose a monomial order induced by a linear form such that xy is the initial term of $g_{\underline{a}}(x,y)$. We perform the division of xy by $g_{\underline{a}}(x,y)$:

$$xy = g_{\underline{a}}(x,y) Q_{\underline{a}}(x,y) + R_{\underline{a}}(x) + S_{\underline{a}}(y).$$

For any $k \in \mathbb{N}\backslash\{0,1\}$ we set

$$E_k = \{(0,k+1),(k+1,0),(k,k)\}.$$

We have the following result:

Proposition 9.2. *Let E be a finite set as before such that $E_k \subset E$. Let $(\alpha_{i,j}) \in \mathbb{C}^{Card(E)}$ whose coordinates are algebraically independent over $\mathbb{Q}$. Then $R_{\underline{\alpha}}(x)$ is not a D-finite power series.*

Proof. Let $N = Card(E)$. The proof is made by induction on N.
If $N = 3$, then $E = E_k$. If $\alpha_{0,k+1}, \alpha_{k+1,0}, \alpha_{k,k} \in \mathbb{C}$ are algebraically independent over $\mathbb{Q}$ and $R(x) := R_{\underline{\alpha}}(x)$ is a D-finite power series, then $R(x)$ satisfies a differential equation:

$$P_d(x)R^{(d)}(x) + \cdots + P_1(x)R(x) + P_0(x) = 0 \tag{7}$$

where $P_1(x)$,..., $P_d(x) \in \mathbb{C}[x]$. If we expand this relation in terms of a $\mathbb{Q}(\underline{\alpha})$-basis of the $\mathbb{Q}(\underline{\alpha})$-vector space $\mathbb{C}$, we obtain at least one non-trivial relation of the same type where the $P_i(x)$ are in $\mathbb{Q}(\underline{\alpha})[x]$. So we assume that $P_i(x) \in \mathbb{Q}(\underline{\alpha})[x]$ for all i and even $P_i(x) \in \mathbb{Q}[\underline{\alpha}][x]$ for all i by multiplying this relation by a well chosen polynomial of $\mathbb{Q}[\underline{\alpha}]$. Since $\alpha_{k+1,0}$, $\alpha_{0,k+1}$ and $\alpha_{k,k}$ are algebraically independent over $\mathbb{Q}$, we are reduced to assume that $R_{a,b,c}(x)$ is D-finite over $\mathbb{Q}[a,b,c]$ where a, b and c are new indeterminates and

$$R_{a,b,c}(x) := xy - ax^{k+1} - by^{k+1} - cx^k y^k.$$

We may assume that the polynomials $P_i = P(a,b,c,x)$, coefficients of the Relation (7), are globally coprime, otherwise we factor out their common divisor. For $0 \leq i \leq d$, let V_i be the subvariety of $\mathbb{C}^3$ which is the zero locus of the coefficients of $P_i(a,b,c,x)$ (seen as a polynomial in x). Let V be the intersection of V_0,..., V_d. Then if $(\underline{\alpha}) \notin V$, one of the $P_i(\underline{\alpha}, x)$ is non-zero and $R_{\underline{\alpha}}(x)$ is D-finite over $\mathbb{C}[x]$. Since we have assumed that the $P_i(a,b,c,x)$ are globally coprime, V is a finite union of algebraic curves and points, except if all but one P_i are equal to 0. In this latter case, we have $P_d(a,b,c,x)R^{(d)}_{a,b,c}(x) = 0$ which means that $R^{(d)}_{a,b,c}(x) = 0$, thus we may replace P_d by 1 and in this case $V = \emptyset$.

From now on we replace c by $-ab$ and we have the relation:

$$xy = (x - by^k)(y - ax^k)Q_{a,b,-ab}(x,y) + R_{a,b,-ab}(x) + S_{a,b,-ab}(y). \tag{8}$$

By symmetry we have $R_{b,a,-ab} = S_{a,b,-ab}$. If replace (x,y) by (bx, ay) in Relation (8) we get

$$abxy = ab(x - ay^k)(y - bx^k)Q_{a,b,-ab}(bx,ay) + R_{a,b,-ab}(bx) + S_{a,b,-ab}(ay),$$

thus

$$\frac{1}{ab}R_{a,b,-ab}(bx) = R_{b,a,-ab}(x) = S_{a,b,-ab}(x).$$

By replacing y by ax^k in (8) we obtain:

$$ax^{k+1} = R_{a,b,-ab}(x) + \frac{1}{ab}R_{a,b,-ab}(abx^k).$$

Thus we obtain

$$R_{a,b,-ab}(x) = \sum_{l=0}^{\infty}(-1)^l a^{(k+1)(k^l-1)-l+1} b^{(k+1)(k^l-1)-k} x^{(k+1)k^l}.$$

Exactly as in the example of Kashiwara-Gabber, this shows that $R_{\alpha,\beta,-\alpha\beta}(x)$ is not D-finite if $\alpha\beta \neq 0$.
Let S be the surface of equation $ab + c = 0$. In particular S is not included in V. Then we see that for any $(\alpha,\beta,\gamma) \in S\backslash\{ab = 0\}$, $R_{\alpha,\beta,\gamma}(x)$ is not D-finite. This contradicts the assumption that $R_{a,b,c}(x)$ is D-finite since we have shown that this would imply that $R_{\alpha,\beta,\gamma}(x)$ is D-finite for any $(\alpha,\beta,\gamma) \notin V$. Thus $R_{a,b,c}(x)$ is not

D-finite.

Let us assume that $N > 3$ and that the proposition is proven for any set of cardinal $N-1$ containing E_k. Let us assume that $R_{\underline{a}}(x)$ is D-finite, i.e. there exist polynomials $P_i \in \mathbb{C}(\underline{a})[x]$, for $1 \leq i \leq d$, such that

$$P_d(\underline{a}, x)R_{\underline{a}}^{(d)}(x) + \cdots + P_1(\underline{a}, x)R_{\underline{a}}(x) + P_0(\underline{a}, x) = 0.$$

As we did before, we may assume that $P_i \in \mathbb{Q}[\underline{a}, x]$ for all i. By dividing the previous relation by a common divisor of the P_i, we may assume that the P_i are globally coprime. For $0 \leq i \leq d$ let V_i denote the subvariety of $\mathbb{C}^N$ which is the zero locus of the coefficients of $P_i(x)$ (seen as a polynomial with coefficients in $\mathbb{Q}[\underline{a}]$). Let V be the intersection of V_0,..., V_d. As in the previous case, since the P_i are globally coprime, then $\mathrm{codim}_{\mathbb{C}^N}(V) \geq 2$.
Let $(i_0, j_0) \in E \backslash E_k$ and set $E' = E \backslash \{(i_0, j_0)\}$. Set $W = \{a_{i_0,j_0} = 0\}$; we have $\mathrm{codim}_{\mathbb{C}^N}(W) = 1$. By the inductive assumption, $R_{\underline{\alpha}}(x)$ is not D-finite for any $\underline{\alpha} \in W$ such that $\mathrm{tr.deg}_{\mathbb{Q}}\mathbb{Q}(\underline{\alpha}) = N-1$. But if $\underline{\alpha} \in W \backslash V$ and $\mathrm{tr.deg}_{\mathbb{Q}}\mathbb{Q}(\underline{\alpha}) = N-1$ (we may find such an $\underline{\alpha}$ since $\mathrm{codim}_{\mathbb{C}^N}(V)$ is strictly larger than $\mathrm{codim}_{\mathbb{C}^N}(W)$), we see that $R_{\underline{\alpha}}(x)$ is not D-finite which is a contradiction since $\underline{\alpha} \notin V$. Thus $R_{\underline{a}}(x)$ is not D-finite and the proposition is proven for sets E of cardinal N.

□

Example 9.3. If E does not contain any of the sets E_k then Proposition 9.2 is no valid in general. For instance let us consider $E \subset \{(i, i+j),\ (i,j) \in \mathbb{N}^2\}$. Let us set $F = \{(i,j),\ (i, i+j) \in E\}$. Let us consider the division

$$z = \left[z - \sum_{(i,j) \in F} a_{i,i+j} x^i z^j \right] Q(x,z) + R(x)$$

where Q and R are algebraic power series by Lafon Division Theorem. Then by replacing z by xy we obtain the division of xy by $g_{\underline{a}}(x,y)$:

$$xy = \left[xy - \sum_{(i,j) \in E} a_{i,j} x^i y^j \right] Q(x, xy) + R(x).$$

Thus $R_{\underline{a}}(x) = R(x)$ is an algebraic power series.

Example 9.4. Let $h(x,y)$ and $d(x,y)$ be two algebraic power series over $\mathbb{C}$ and let us assume that the initial term of $d(x,y)$ is xy. The division of h by d yields the relation:

$$h(x,y) = d(x,y)Q(x,y) + R(x) + S(y).$$

By Newton-Puiseux Theorem there exist $n \in \mathbb{N}$ and $x(y) \in \mathbb{C}\langle y \rangle$, $y(x) \in \mathbb{C}\langle x \rangle$ such that

$$d(x(y), y^n) = d(x^n, y(x)) = 0.$$

Thus we obtain

$$h(x(y^{\frac{1}{n}}), y) = R(x(y^{\frac{1}{n}})) + S(y)$$
$$h(x^n, y(x)) = R(x^n) + S(y(x)).$$

This yields the relation:

$$R(x^n) - R(x(y(x)^{\frac{1}{n}}) = h(x(y(x)^{\frac{1}{n}}) - h(x^n, y(x)).$$

By replacing x by x^n we see that there exist two algebraic power series $f(x)$ and $g(x)$ such that

$$R(x^{n^2}) - R(g(x)) = f(x).$$

But this is impossible if $R(x) = e^x$ by Schanuel's conjecture [Ax71]. This shows that in general D-finite power series (here e^x) which are not algebraic are not remainders of division.

10. Gap Theorem for remainders of division of algebraic power series

By a Theorem of Schmidt (see Hilfssatze 5 [Sc33]) an algebraic power series has no large gaps in their Taylor expansion. More precisely his result asserts that if an algebraic power series f is written as $f = \sum_k f_{n(k)}$ where $f_{n(k)}$ is a non-zero homogeneous polynomial of degree $n(k)$ and $(n(k))_k$ is strictly increasing, then

$$\limsup_{k \longrightarrow \infty} \frac{n(k+1)}{n(k)} < \infty.$$

We prove here the same result for remainders of the Grauert-Hironaka-Galligo Division, i.e. it does not have more than Hadamard gaps.

Lemma 10.1. *Let I be the ideal of $\mathbb{k}[\![x]\!]$ generated by g_1,..., g_s and let us fix a monomial order induced by a linear form as in Section 8. Then there exists a constant $K > 0$ such that the following holds:*
Let $f \in \mathbb{k}[\![x]\!]$ and r be the remainder of the division of f by g_1,..., g_s. Then we have

$$ord_{\mathbb{k}[\![x]\!]/I}(f) \geq K\, ord_{\mathbb{k}[\![x]\!]}(r).$$

Proof. Let us assume that the linear form L inducing the monomial order is defined by

$$L(\alpha) = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n$$

for some positive numbers λ_i. We have $f - r \in I$, thus

$$\operatorname{ord}_{\mathbb{k}[\![x]\!]/I}(f) = \operatorname{ord}_{\mathbb{k}[\![x]\!]/I}(r) \geq \operatorname{ord}_{\mathbb{k}[\![x]\!]}(r) \geq K_1\, \nu_\lambda(r) \geq K_1K_2 \operatorname{ord}_{\mathbb{k}[\![x]\!]}(r)$$

where

$$K_1 := \min\left\{\frac{1}{\lambda_i}\right\} \text{ and } K_2 := \min_i\{\lambda_i\}.$$

□

Theorem 10.2. *Let g_1,..., $g_s \in \mathbb{k}\langle x\rangle$ and let us fix a monomial order induced by a linear form as in Section 8. Then there exists a function $C : \mathbb{N} \longrightarrow \mathbb{R}_{>0}$ such that the following holds:*
Let $f \in \mathbb{k}\langle x\rangle$ be an algebraic power series and let r be the remainder of the division of f by g_1,..., g_s with respect to the given monomial order. Let us write $r = \sum_{k=1}^{\infty} r_{n(k)}$ where r_h is a homogeneous polynomial of degree h, $n(k)$ is an increasing sequence of integers and $r_{n(k)} \neq 0$ for any $k \in \mathbb{N}$. Then

$$n(k+1) \leq C(Deg(f)) \cdot n(k) \qquad \forall k \gg 0.$$

In particular

$$\limsup_{k \longrightarrow \infty} \frac{n(k+1)}{n(k)} < \infty.$$

Proof. Let I denote the ideal generated by $g_1,..., g_s$.
Let us set $f_k := f - \sum_{i=1}^{k} r_{n(i)}$ for any $k \in \mathbb{N}$. The remainder of the division of f by $g_1,..., g_s$ is $\sum_{i=k+1}^{\infty} r_{n(i)}$, thus

$$\mathrm{ord}_{\Bbbk[\![x]\!]/I}(f_k) \geq K\, n(k+1)$$

for some constant $K > 0$ independent of f by Lemma 10.1. Moreover

$$\mathrm{H}(f_k) \leq \mathrm{Deg}(f) \max\{n(k), \mathrm{H}(f)\}$$

thus $\mathrm{H}(f_k) \leq \mathrm{Deg}(f) \cdot n(k)$ for k large enough. Hence, by Theorem 1.1 and since $\mathrm{Deg}(f_k) = \mathrm{Deg}(f)$, there exists $C' > 0$ depending on $\mathrm{Deg}(f)$ such that

$$\mathrm{ord}_{\Bbbk[\![x]\!]/I}(f_k) \leq C' \cdot \mathrm{Deg}(f) \cdot n(k)$$

for k large enough. So the theorem is proved with $C = \frac{C'}{K}\mathrm{Deg}(f)$.

□

Remark 10.3. Example 8.2 shows that this result is sharp.

References

[AB13] B. Adamczewski, J. Bell, Diagonalization and rationalization of algebraic Laurent series, *Ann. Sci. Éc. Norm. Supér.*, **46** (2013), 963-1004.

[AMR91] M. E. Alonso, T. Mora, M. Raimondo, On the complexity of algebraic power series, Applied Algebra, Algebraic algorithms and error-correcting codes, Tokyo 1990, *Lecture Notes in Compt. Sci.*, **508**, (1991), 197-207.

[Ar66] M. Artin, Etale coverings of schemes over Hensel rings, *Amer. J. Math.*, **88**, (1966), 915-934.

[Ax71] J. Ax, On Schanuel's conjectures, *Ann. of Math. (2)*, **93**, (1971), 252-268.

[BB85] D. Bertrand, F. Beukers, Équations différentielles linéaires et majorations de multiplicités, *ann. Scient. ÉC. Norm. Sup*, **18**, (1985), 181-192.

[Ga79] A. Galligo, Théorème de division et stabilité en géométrie analytique locale, *Ann. Inst. Fourier*, **29**, (1979), no. 2, vii, 107-184.

[Gr72] H. Grauert, Über die Deformation isolierter Singularitäten analytischer Mengen, *Invent. Math.*, **15**, (1972), 171-198.

[HK08] H. Hauser, C. Koutschan, Multivariate linear recurrences and power series division, *Discrete Math.*, **312**, (2012), no. 24, 3553-3560.

[He26] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.*, **95**, (1926), no. 1, 736-788.

[Hi64] H. Hironaka, Resolution of singularities of an algebraic variety over a field of characteristic zero I, II, *Ann. of Math.*, (2) **79**, (1964), 109-203; ibid. (2) **79**, (1964) 205-326.

[Hi77] H. Hironaka, Idealistic exponents of singularity, Algebraic Geometry, The John Hopkins Centennial Lectures, John Hopkins University Press, 1977.

[Iz92a] S. Izumi, Increase, convergence and vanishing of functions along a Moishezon space, *J. Math. Kyoto Univ.*, **32**, (1992), 245-258.

[Iz92b] S. Izumi, A criterion for algebraicity of analytic set germs, *Proc. Japan Acad.*, **68**, Ser. A, (1992), 307-309.

[Iz98] S. Izumi, Transcendence measures for subsets of local algebras, Real analytic and algebraic singularities (Nagoya/Sapporo/Hachioji, 1996), 189-206, Pitman Res. Notes Math. Ser., **381**, Longman, Harlow, 1998.

[KK12] I. Kurkova, K. Raschel, On the functions counting walks with small steps in the quarter plane, *Publ. Math. Inst. Hautes Études Sci.*, **116**, (2012), 69-114.

[La65] J.-P. Lafon, Séries formelles algébriques, *C. R. Acad. Sci. Paris Sér. A-B*, **260**, (1965), 3238-3241.

[Li89] L. Lipshitz, *D*-finite power series, *J. of Algebra*, **122**, (1989), 353-373.

[LR86] L. Lipshitz, L. Rubel, A gap theorem for power series solutions of algebraic differential equations, *Amer. J. Math.*, **108**, (1986), no. 5, 1193-1213.

[MM82] E. Mayr, A. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals, *Adv. in Math.*, **46**, (1982), no. 3, 305-329.

[Ne87] Yu. V. Nesterenko, Measures of algebraic independence of numbers and functions, *Journées arithmétiques de Besançon* (Besançon, 1985), *Astérisque*, **147-148**, (1987), 141-149.
[Ni90] K. Nishioka, On an estimate for the orders of zeros of Mahler type functions, *Acta Arith.*, (1990), 249-256.
[Mo82] T. Mora, An algorithm to compute the equations of tangent cones, *Computer algebra (Marseille, 1982)*, pp. 158165, *Lecture Notes in Comput. Sci.*, **144**, Springer, Berlin-New York, 1982.
[Na62] M. Nagata, Local Rings, Interscience, New York, (1962).
[Ra89] R. Ramanakoraisina, Complexité des fonctions de Nash, *Comm. Algebra*, **17**, (1989).
[Sa56] P. Samuel, Algébricité de certains points singuliers algébroïdes, *J. Math. Pures Appl.*, **35**, (1956), 1-6.
[Sc33] F. K. Schmidt, Mehrfach perfkte Körper, *Math. Ann*, **108**, (1933), 1-25.
[Se74] A. Seidenberg, Constructions in algebra, *Trans. Amer. Math. Soc.*, **197**, (1974), 273-313.
[Sh59] A. Shidlovskii, On a criterion for the algebraic independence of the values of a class of entire functions., *Izv. Akad. Nauk. S.S.S.R.*, **23**, (1959), 35-66.
[ZS58] O. Zariski, P. Samuel, Commutative Algebra I, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958.

E-mail address: guillaume.rond@univ-amu.fr

Aix-Marseille Université, CNRS, Centrale Marseille, I2M, UMR 7373, 13453 Marseille, France