Polynomial Composition Rigidity and Plane Polynomial Automorphisms

Jean-Philippe FURTER, Dpt. of Math., Univ. of La Rochelle, av. M. Crépeau, 17 000 La Rochelle, France email: jpfurter@univ-lr.fr

October 10, 2013

Abstract

In the first part of this paper, we briefly present a conjecture dealing with polynomial composition and we prove it in some particular cases. In the second and longest part, we prove our main result, which consists of an application of the conjecture to plane polynomial automorphisms. More precisely, we describe the closure of the set of plane polynomial automorphisms having a prescribed multidegree of length two.

Keywords

Affine algebraic geometry, polynomial automorphisms, affine space, commutative algebra

0 INTRODUCTION

The theory of polynomials in one indeterminate and the theory of plane polynomial automorphisms are intimately connected. The most striking illustration of this phenomenon is probably the easy way to deduce the theorem of Jung from the theorem of Abhyankar, Moh, Suzuki (for this deduction, see e.g. [Ess00, Proof of Cor. 5.3.6, p. 100]). Let us recall these famous statements (see [AM75, Suz74] and [Jun42]).

Theorem (Abhyankar, Moh, Suzuki). Let K be a field of characteristic 0. If $a, b \in K[X]$ are two polynomials which generate the whole algebra K[X], i.e. such that K[a,b] = K[X], then deg a divides deg b or deg b divides deg a.

Theorem (Jung). Let K be a field of characteristic 0. Any polynomial automorphism of the affine plane \mathbb{A}_{K}^{2} is a composition of affine and triangular automorphisms, where by definition an affine automorphism is of the form

 $(x,y) \mapsto (\alpha x + \beta y + \gamma, \delta x + \varepsilon y + \zeta), \quad with \ \alpha, \dots, \zeta \in K \text{ and } \alpha \varepsilon - \beta \delta \neq 0$

and a triangular automorphism is of the form

 $(x,y) \mapsto (\alpha x + p(y), \beta y + \gamma)$ with $\alpha, \beta, \gamma \in K, \ p \in K[y]$ and $\alpha \beta \neq 0$.

In the same vein, the main result of this paper consists in proving that the following rigidity conjecture R(m, n) dealing with polynomials in one indeterminate has some applications to the theory of plane polynomial automorphisms (see Th. B below). Using Gröbner basis, we have checked R(m, n) when $m \leq 8$ and $n \leq 5$.

Conjecture R(m, n). Let $a = X(1+a_1X+\dots+a_mX^m)$, $b = X(1+b_1X+\dots+b_nX^n) \in \mathbb{C}[X]$, where the $a_i, b_j \in \mathbb{C}$. Let us write $a \circ b = X(1+c_1X+\dots+c_NX^N)$, where N = (m+1)(n+1) - 1 and the $c_k \in \mathbb{C}$. If $c_1 = \dots = c_{m+n} = 0$, then a = b = X.

Remark. This conjecture being obvious for m or n = 0, we generally assume that m and n are ≥ 1 .

Let us begin to explain why this conjecture may be interpreted as a rigidity statement. Considering a_i, b_i as indeterminates of degree *i* allows us to see each c_i as a homogeneous polynomial of degree *i* in $\mathbb{C}[a_1, \ldots, a_m, b_1, \ldots, b_n]$. The conjecture $\mathbb{R}(m, n)$ means that c_1, \ldots, c_{m+n} is a hop (homogeneous system of parameters) of $\mathbb{C}[a_1, \ldots, a_m, b_1, \ldots, b_n]$. For the definition of a hop and several characterizations, we refer to subsection 2.2 below and in particular to Lemma 11. This terminology (hop) is for example used in [Sta96, Chap. I, Def. 5.1, p. 33]. By Lemma 11, the conjecture $\mathbb{R}(m, n)$ is still equivalent to asserting that the polynomial endomorphism of the complex affine space \mathbb{A}^{m+n} sending $(a_1, \ldots, a_m, b_1, \ldots, b_n)$ to (c_1, \ldots, c_{m+n}) is quasi-finite, i.e. admits finite fibers. In some sense, this means that polynomial composition is rigid.

In this connection, let us recall the famous result of Ritt on polynomial composition (see [Rit22]). A polynomial $a \in \mathbb{C}[X]$ of degree ≥ 2 is prime if the relation $a = b \circ c$ implies that b or c has degree 1. If deg $f \geq 2$, it is clear that f admits a decomposition $f = f_1 \circ \cdots \circ f_r$ into prime polynomials. Let us note that $a \circ b = c \circ d$ in the three following cases:

- *i*) a, b are any polynomials and $c = a \circ l$, $d = l^{-1} \circ b$, where l has degree 1 and l^{-1} is its inverse for the composition;
- *ii)* $a = d = t_m$ and $b = c = t_n$, where $t_m(X) = \cos(m \arccos X)$ is the *m*-th Chebyshev polynomial;
- *iii)* $a = d = X^m$, $b = X^n p(X^m)$ and $c = X^n p(X)^m$, where p is any polynomial, and the converse situation, i.e. $b = c = X^m$, $d = X^n p(X^m)$ and $a = X^n p(X)^m$.

If $f = f_1 \circ \cdots \circ f_r$ is a prime decomposition, then, by replacing an adjacent pair $(f_i, f_{i+1}) = (a, b)$ by (c, d) where a, b, c, d are as in i) - iii) above, we obtain a new prime decomposition. This process is called an elementary transformation.

Theorem (Ritt). The prime decomposition is unique modulo elementary transformations, i.e. if we have two prime decompositions of some polynomial, we can pass from one to the other by applying a finite number of elementary transformations.

Many problems related to polynomial composition (and iteration!) are intricate. For example, the famous Mandelbrot set is defined as the set of complex c-values for which the orbit of 0 under iteration of $p(X) = X^2 + c$ remains bounded. In fact, the conjecture R(m, n) is related to the following one which perhaps looks more attractive. **Conjecture R(m).** Let $a = X(1 + a_1X + \dots + a_mX^m) \in \mathbb{C}[X]$ and let $a^{-1} \in \mathbb{C}[[X]]$ be its formal inverse for the composition. If m consecutive coefficients of a^{-1} vanish, then a = X.

If $a^{-1} = X\left(1 + \sum_{k \ge 1} \tilde{a}_k X^k\right)$, the vanishing conditions means that there exists an

integer $n \ge 0$ such that $\tilde{a}_{n+k} = 0$ for $1 \le k \le m$. With words, the conjecture $\mathbb{R}(m)$ means that the inverse for the composition of a non trivial polynomial is badly approximated by polynomials. Let us remark the analogy with Heisenberg's uncertainty principle in quantum mechanics asserting that one cannot reduce arbitrarily the uncertainty as to the position and the momentum of a free particle. Here is a mathematical statement:

Let f be a nonzero element of $L^2(\mathbb{R})$ describing a particle: the probability density that this particle is located at t is $\frac{1}{\|f\|^2} |f^2(t)|$. Let $\hat{f} \in L^2(\mathbb{R})$ be the Fourier transform of f. The probability density that the momentum of this particle is equal to ω is $\frac{1}{2\pi \|f\|^2} |\hat{f}^2(\omega)|$. If σ_t (resp. σ_{ω}) denotes the variance of the location (resp. momentum), then Heisenberg uncertainty is expressed by the following inequality:

$$\sigma_t \, \sigma_\omega \geq \frac{1}{2}.$$

For more details, we refer to [Wey31, p. 77], [Mal99, Th. 2.5] or [KL98, Th. 1, p. 311].

Many mathematical results contain a close idea. For example, rationals are badly approximated by rationals: if α is any real number, Hurwitz has proved that α is irrational if and only if there are infinitely many rationals $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5q^2}}$ (see [Hur1891]). Algebraic numbers are also badly approximated by rationals. Roth has proved that for any algebraic number α and any real $\varepsilon > 0$, there exist only finitely many rationals $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$ (see [Rot55]). On the converse, this idea was first used by Liouville to construct transcendental numbers (see [Lio1844a, Lio1844b]). We show below (see Lemma 2) that the conjecture R(m, n) holds if and only if the conjecture R(m, n), our first result is the following:

Theorem A. If m or $n \leq 2$, then the conjecture R(m, n) holds.

Before giving an application to plane polynomial automorphisms, we need some notations. A polynomial endomorphism of \mathbb{A}_{K}^{2} will be identified with its sequence $f = (f_{1}, f_{2})$ of coordinate functions $f_{j} \in K[X, Y]$. We define its degree by deg $f = \max_{j} \deg f_{j}$.

The space $\mathcal{E} := \mathbb{C}[X, Y]^2$ of polynomial endomorphisms of the complex affine plane \mathbb{A}^2 is naturally an infinite dimensional algebraic variety (see [Sha66, Sha82] for the definition). This roughly means that $\mathcal{E}_{\leq m} := \{f \in \mathcal{E}, \deg f \leq m\}$ is a (finite dimensional) algebraic variety for any $m \geq 1$, which comes out from the fact that it is an affine space. If $Z \subseteq \mathcal{E}$, we set $Z_{\leq m} := Z \cap \mathcal{E}_{\leq m}$. The space \mathcal{E} is endowed with the topology of the inductive limit, in which Z is closed (resp. open) if and only if $Z_{\leq m}$ is closed (resp. open) in $\mathcal{E}_{\leq m}$ for any m.

Let \mathcal{G} be the group of polynomial automorphisms of \mathbb{A}^2 . Since \mathcal{G} is locally closed in \mathcal{E} (see [FM10] and also [BCW82, Sha66, Sha82]), it is naturally an infinite dimensional algebraic variety. Let

$$\mathcal{A} := \{ (aX + bY + c, dX + eY + f), a, b, c, d, e, f \in \mathbb{C}, ae - bd \neq 0 \}$$

be the subgroup of affine automorphisms and

$$\mathcal{B} := \{ (aX + p(Y), bY + c), a, b, c \in \mathbb{C}, p \in \mathbb{C}[Y], ab \neq 0 \}$$

be the subgroup of (upper) triangular automorphisms (\mathcal{B} may be viewed as a Borel subgroup of \mathcal{G}). By [Jun42, Kul53, Nag72], any element f of \mathcal{G} admits an expression:

$$f = \alpha_1 \circ \beta_1 \circ \cdots \circ \alpha_k \circ \beta_k \circ \alpha_{k+1},$$

where the α_j 's (resp. β_j 's) belong to \mathcal{A} (resp. \mathcal{B}). By contracting such an expression, one might as well suppose that it is reduced, i.e. $\forall j, \beta_j \notin \mathcal{A}$ and $\forall j, 2 \leq j \leq k, \alpha_j \notin \mathcal{B}$. It follows from the amalgamated structure of \mathcal{G} that if

$$f = \alpha'_1 \circ \beta'_1 \circ \dots \circ \alpha'_l \circ \beta'_l \circ \alpha'_{l+1}$$

is another reduced expression of f, then k = l and there exist $(\gamma_j)_{1 \le j \le k}$, $(\delta_j)_{1 \le j \le k}$ in $\mathcal{A} \cap \mathcal{B}$ such that $\alpha'_1 = \alpha_1 \circ \gamma_1^{-1}$, $\alpha'_j = \delta_{j-1} \circ \alpha_j \circ \gamma_j^{-1}$ (for $2 \le j \le k$), $\alpha'_{k+1} = \delta_k \circ \alpha_{k+1}$ and $\beta'_j = \gamma_j \circ \beta_j \circ \delta_j^{-1}$ (for $1 \le j \le k$). Following [FM89] and [Fur02], we define the multidegree and the length of f by:

$$\operatorname{mdeg}(f) = (\operatorname{deg} \beta_1, \dots, \operatorname{deg} \beta_k) \text{ and } l(f) = k.$$

These notions of multidegree and length could be defined in the same way for a polynomial automorphism of \mathbb{A}^2_K , where K is any field. We recall (see [Wri79, FM89]) that degree and multidegree are related by

$$\deg f = \deg \beta_1 \times \cdots \times \deg \beta_k.$$

Let \mathcal{D} be the set of multidegrees, i.e. of finite sequences of integers ≥ 2 (including the empty sequence). If $d = (d_1, \ldots, d_k) \in \mathcal{D}$, \mathcal{G}_d will denote the set of automorphisms whose multidegree is equal to d. By [FM89, Fur09], \mathcal{G}_d is an irreducible smooth, locally closed subset of \mathcal{G} of dimension $d_1 + \cdots + d_k + 6$. Let us note that $\mathcal{G}_d \subseteq \mathcal{G}_{\leq n}$ as soon as $n \geq d_1 \ldots d_k$ and that we have a partition of \mathcal{G} as a disjoint union $\mathcal{G} = \prod_{d \in \mathcal{D}} \mathcal{G}_d$. What

can be said on the closure of \mathcal{G}_d ?

By [Fur02], the length of an automorphism is lower semicontinuous. Therefore, any element of $\overline{\mathcal{G}}_d$ has length $\leq k$. The simplest non trivial related example is induced by the Nagata automorphism (see [Nag72]):

$$N := (X - 2YW - ZW^2, Y + ZW, Z), \text{ where } W = XZ + Y^2.$$

This automorphism of the complex affine space \mathbb{A}^3 can be seen as an automorphism of $\mathbb{A}^2_{\mathbb{C}[Z]}$ inducing as well a morphism from the complex affine line \mathbb{A}^1 to \mathcal{G} sending z to

$$N_z = (X - 2Y(Xz + Y^2) - z(Xz + Y^2)^2, Y + z(Xz + Y^2)) \in \mathcal{G}.$$

If $z \neq 0$, the factorization

$$N_z = (X - z^{-1}Y^2, Y) \circ (X, Y + z^2X) \circ (X + z^{-1}Y^2, Y)$$

shows us that N_z has multidegree (2, 2). If z = 0, we have $N_0 = (X - 2Y^3, Y)$ so that N_0 has multidegree (3). This yields us $\mathcal{G}_{(3)} \cap \overline{\mathcal{G}}_{(2,2)} \neq \emptyset$. Inspired by the analysis of similar examples, we hoped (erroneously) that the equality $\overline{\mathcal{G}}_d = \bigcup_{e \leq d} \mathcal{G}_e$ might always be true,

where \leq is defined in the following way:

Definition. The partial order \leq on \mathcal{D} is induced by the following relations:

- i) $\emptyset \leq d$ (for any d);
- ii) $(d_1, \ldots, d_k) \preceq (e_1, \ldots, e_k)$ when $d_j \leq e_j$ for any j;
- iii) $(d_1, \ldots, d_{j-1}, d_j + d_{j+1} 1, d_{j+2}, \ldots, d_k) \preceq (d_1, \ldots, d_k)$ when $1 \le j \le k 1$.

However, by [EF04], there cannot exist any partial order \sqsubseteq such that $\overline{\mathcal{G}}_d = \bigcup_{e \vdash d} \mathcal{G}_e$

when d = (11, 3, 3)! Actually, it is proved there that $\mathcal{G}_{(19)} \cap \overline{\mathcal{G}}_{(11,3,3)} \neq \emptyset$ and for grounds of dimension we cannot have $\mathcal{G}_{(19)} \subseteq \overline{\mathcal{G}}_{(11,3,3)}$. As a matter of fact reality is often complex. We now think that the equality $\overline{\mathcal{G}}_d = \bigcup_{e \prec d} \mathcal{G}_e$ is actually true in length 0, 1

and 2. In length 0 it is obvious. In length 1, it is proved in [Fur97]. This paper settles the length 2 case modulo the conjecture R(m, n). Indeed, here is the main result of our paper:

Theorem B. If the conjecture R(m, n) holds and if we set d = (m + 1, n + 1), then we have:

$$\overline{\mathcal{G}}_d = \bigcup_{e \leq d} \mathcal{G}_e.$$

Remark. If the equality $\overline{\mathcal{G}}_d = \bigcup_{e \leq d} \mathcal{G}_e$ holds when d is of length 2, then, a straightforward induction on the length on d would establish that for any d the following inclusion holds:

$$\bigcup_{e \leq d} \mathcal{G}_e \subseteq \overline{\mathcal{G}}_d$$

Theorems A and B directly imply:

Theorem C. If $d = (d_1, d_2)$ is a multidegree with d_1 or $d_2 \leq 3$, then $\overline{\mathcal{G}}_d = \bigcup_{e \leq d} \mathcal{G}_e$.

Remark. We would like to stress that even if the conjecture R(m,n) is obvious when m or n = 1 (cf. the proof of conjecture R(1) in subsection 1.4), its consequence for polynomial automorphisms (given via Theorem B) is not obvious at all. Indeed, it asserts that if $d = (d_1, d_2)$ is a multidegree such that d_1 or $d_2 \leq 2$, then $\overline{\mathcal{G}}_d = \bigcup_{e \prec d} \mathcal{G}_e$. The

simplest case where $d_1 = d_2 = 2$ means that

$$\overline{\mathcal{G}}_{(2,2)} = \mathcal{G}_{\emptyset} \ \cup \ \mathcal{G}_{(2)} \ \cup \ \mathcal{G}_{(3)} \ \cup \ \mathcal{G}_{(2,2)}$$

In particular, this equality implies the two following points:

• $\mathcal{G}_{(3)} \cap \overline{\mathcal{G}}_{(2,2)} \neq \emptyset$. As explained above, this point can be established using the family of plane automorphisms induced by the Nagata automorphism;

• $\overline{\mathcal{G}}_{(2,2)} \cap \mathcal{G}_{(4)} = \emptyset$. This equality follows from [Fur09, Th. A] asserting that for any multidegree $d = (d_1, \ldots, d_l)$, the set \mathcal{G}_d is closed in the set of all automorphisms of degree $d_1 \ldots d_l$. The weaker fact that $\mathcal{G}_{(4)}$ is not included into $\overline{\mathcal{G}}_{(2,2)}$ was a consequence of [Fur97, Th. 2] and was also the object of [Fur97, Prop. 12].

As a funny consequence of Th. C, we will show:

Theorem D. Any closed subgroup of \mathcal{G} containing the affine group and an automorphism of length 1 is equal to \mathcal{G} .

Remark. 1. Let us note that any subgroup of \mathcal{G} strictly containing the affine group is dense in \mathcal{G} for the Krull topology (see [Fur07, Th. A]). This means that any element of \mathcal{G} can be approximated at the origin and at any order by an element of this subgroup.

2. We recall that any closed subgroup of \mathcal{G} which is a finite dimensional algebraic variety is conjugate to either a subgroup of \mathcal{A} or \mathcal{B} (see [Sha66, Th. 8], [Kam79, Th. 4.3] or [GD75, Th. 7]).

We finish this introduction by the following natural question.

Question. Does there exist a non trivial closed subgroup of \mathcal{G} containing the affine group?

This paper is divided into two parts. The first part is the shortest one and is only composed of section 1, where we study the rigidity conjecture R(m, n) and prove Th. A. The second part is composed of the three sections 2, 3, 4. In section 2, we give some preliminary results. In sections 3 and 4, we respectively prove Th. B and Th. D.

1 THE RIGIDITY CONJECTURE

In subsection 1.1 we prove that the conjectures R(m, n) and R(n, m) are equivalent. In subsection 1.2, we relate the conjectures R(m, n) and R(m). In subsection 1.3, we give some generalities on the conjecture R(m). In subsection 1.4, we prove the conjectures R(1) and R(2). In subsection 1.5, we give some information on the conjecture R(3). We explain why we were not able to solve it and hope that the given information might help or motivate some reader for further investigations.

1.1 The conjecture R(m, n) and R(n, m) are equivalent

Lemma 1. The conjectures R(m, n) and R(n, m) are equivalent.

Proof. Let val: $\mathbb{C}((X)) \to \mathbb{Z} \cup \{+\infty\}$ be the valuation associated to the discrete valuation ring $\mathbb{C}[[X]]$. The conjecture $\mathbb{R}(m,n)$ means that if $a = X(1 + a_1X + \dots + a_mX^m)$ and $b = X(1 + b_1X + \dots + b_nX^n)$ are such that $\operatorname{val}(a \circ b - X) \ge m + n + 2$, then a = b = X. Therefore, it is enough to check that $\operatorname{val}(a \circ b - X) = \operatorname{val}(b \circ a - X)$. Indeed, if $k = \operatorname{val}(a \circ b - X)$, we have $a \circ b(X) \equiv X \mod X^k$. Let $a^{-1}(X) \in \mathbb{C}[[X]]$ be the formal inverse of a for the composition. We get $a^{-1} \circ (a \circ b) \circ a(X) \equiv a^{-1} \circ a(X) \mod X^k$, i.e. $b \circ a(X) \equiv X \mod X^k$, so that $\operatorname{val}(b \circ a - X) \ge \operatorname{val}(a \circ b - X)$. We would show the other inequality in the same way, so that finally $\operatorname{val}(a \circ b - X) = \operatorname{val}(b \circ a - X)$. \Box

1.2 Relations between the conjectures R(m, n) and R(m)

Lemma 2. If $m \ge 1$, the two following assertions are equivalent:

- i) The conjecture R(m, n) holds for any $n \ge 0$;
- ii) The conjecture R(m) holds.

Proof. If $a = X(1 + a_1X + \dots + a_mX^m) \in \mathbb{C}[X]$, let us set

$$a^{-1} = X\left(1 + \sum_{k \ge 1} \tilde{a}_k X^k\right) \in \mathbb{C}[[X]].$$

By definition, the conjecture R(m) holds if and only if for any integer $n \ge 0$ the following assertion $\tilde{R}(m, n)$ holds:

Assertion
$$\tilde{\mathbf{R}}(m,n)$$
. $(\tilde{a}_{n+1} = \dots = \tilde{a}_{n+m} = 0) \implies a(X) = X.$

However, if $b = X(1 + b_1X + \dots + b_nX^n) \in \mathbb{C}[X]$, we have:

$$a \circ b(X) \equiv X \mod X^{m+n+2} \iff a^{-1}(X) \equiv b(X) \mod X^{m+n+2}.$$

Using this equivalence, let us show that the assertions $\mathbf{R}(m, n)$ and $\mathbf{R}(m, n)$ are equivalent. This will be enough for showing the lemma.

Assume that the conjecture R(m, n) holds and that we have $\tilde{a}_{n+1} = \cdots = \tilde{a}_{n+m} = 0$.

Set
$$b(X) = X\left(1 + \sum_{1 \le k \le n} \tilde{a}_k X^k\right) = X\left(1 + \sum_{1 \le k \le m+n} \tilde{a}_k X^k\right).$$

We get $a^{-1}(X) \equiv b(X) \mod X^{m+n+2}$, so that $a \circ b(X) \equiv X \mod X^{m+n+2}$ and finally a(X) = X.

Assume that the assertion $\tilde{\mathbb{R}}(m, n)$ holds and that we have $a \circ b(X) \equiv X \mod X^{m+n+2}$. Then, we have $a^{-1}(X) \equiv b(X) \mod X^{m+n+2}$, so that $\tilde{a}_{n+1} = \cdots = \tilde{a}_{n+m} = 0$ and we get a(X) = X. The equality b(X) = X follows at once.

1.3 Generalities on the conjecture R(m)

Let $m \ge 1$ be a fixed integer. Set $a(X) = X(1 - \lambda_1 X) \dots (1 - \lambda_m X) \in \mathbb{C}[X]$, where the λ_k are complex numbers, and express the formal inverse for the composition of a as

$$a^{-1}(X) = X\left(1 + \sum_{n \ge 1} \frac{u_n}{n+1} X^n\right) \in \mathbb{C}[[X]],$$

where the $u_n, n \ge 1$, are complex numbers.

Lemma 3. If \oint denotes integration over a little circle around the origin, we have

$$u_n = \frac{1}{2\pi i} \oint \frac{dX}{a^{n+1}(X)} = \sum_{j_1 + \dots + j_m = n} \binom{n+j_1}{n} \dots \binom{n+j_m}{n} \lambda_1^{j_1} \dots \lambda_m^{j_m}.$$

Proof. By Lagrange formula, we have:

$$u_n = \frac{n+1}{2\pi i} \oint \frac{a^{-1}(X)}{X^{n+2}} dX = \frac{n+1}{2\pi i} \oint \frac{Y}{a^{n+2}(Y)} a'(Y) dY \quad \text{by setting } X = a(Y);$$

 $=\frac{1}{2\pi i}\oint \frac{dY}{a^{n+1}(Y)}$ by integrating by parts.

Therefore, u_n is the X^n -coefficient of the formal series $\prod_{1 \le k \le m} \frac{1}{(1 - \lambda_k X)^{n+1}} \in \mathbb{C}[[X]].$ We conclude thanks to the Taylor expansion $\frac{1}{(1 - X)^{n+1}} = \sum_{j \ge 0} \binom{n+j}{n} X^j.$

Note that u_n is a homogeneous polynomial of degree n in the $\lambda_1, \ldots, \lambda_m$ (where each λ_k has weight 1). The conjecture $\mathbf{R}(m)$ means that if m consecutive u_n vanish, then the λ_i also. In other words, m consecutive polynomials u_n always constitute a hop of $\mathbb{C}[\lambda_1, \ldots, \lambda_m]$.

Remark 4. In order to prove R(m), it is sufficient to prove that if m consecutive u_n vanish, then $u_k = 0$ when k is large enough. Indeed, in this case a^{-1} is a polynomial and the relation $X = a \circ a^{-1}$ shows that a = X (by taking the degree).

The proof of the following lemma is due to Laurent Manivel.

Lemma 5. The sequence $n \mapsto u_n$ satisfies a linear recurrence relation with polynomial coefficients of length m. More precisely, there exist polynomials $\mu_0(n), \ldots, \mu_m(n)$ in $\mathbb{C}[\lambda_1, \ldots, \lambda_m][n]$, not all zero, such that

$$\forall n \ge 1, \quad \sum_{0 \le k \le m} \mu_k(n) \, u_{n+k} = 0.$$

Proof. By Lemma 3, it is enough to show an analogous linear recurrence relation for the sequence

$$n \mapsto v_n := \oint \frac{dX}{a^n(X)}.$$

Set $v_{n,k} = \oint \frac{X^k}{a^n} dX$ and $V_n = \begin{pmatrix} v_{n,0} \\ \vdots \\ v_{n,m-1} \end{pmatrix}.$

<u>Claim.</u> There exists a square matrix M_n whose entries belong to the field $\mathbb{C}(\lambda_1, \ldots, \lambda_m)(n)$ such that

$$V_n = M_n V_{n+1}.$$

Set
$$\gamma(X) = X^{-1}a(X) = (1 - \lambda_1 X) \dots (1 - \lambda_m X)$$
. We have $v_{n,k} = \oint \frac{X^{k-n}}{\gamma^n} dX$. If $k \neq n-1$, we get $v_{n,k} = \frac{n}{k-n+1} \oint \frac{X^{k-n+1}\gamma'}{\gamma^{n+1}} dX$, i.e.
$$\frac{k-n+1}{n} v_{n,k} = \oint \frac{X^{k-n+1}\gamma'}{\gamma^{n+1}} dX.$$

Note that this last equality still holds for k = n - 1. By Euclidean division, there exist polynomials A_k, B_k such that

$$X^{k+1}\gamma' = A_k\gamma - B_k$$

and we have $\deg A_k = k$ and $\deg B_k < \deg \gamma = m$. We have:

$$\frac{k-n+1}{n} v_{n,k} = \oint \frac{X^{-n} (A_k \gamma - B_k)}{\gamma^{n+1}} \, dX = \oint \frac{A_k}{a^n} \, dX - \oint \frac{X B_k}{a^{n+1}} \, dX$$

This gives us a relation of the following form:

$$\frac{n-k-1}{n} v_{n,k} + \sum_{j=0}^{k} a_{k,j} v_{n,j} = \sum_{j=1}^{m} b_{k,j} v_{n+1,j} \quad (*).$$

But we have $\oint \frac{a'}{a^{n+1}} dX = 0$ and $a(X) = X \sum_{k=0}^{m} (-1)^k \sigma_k X^k$, where
 $\sigma_k = \sum_{i_1 < \dots < i_k} \lambda_{i_1} \dots \lambda_{i_k}$

denotes the k-th elementary symmetric polynomial in the variables $\lambda_1, \ldots, \lambda_m$ (with the usual convention $\sigma_0 = 1$), so that:

$$\sum_{k=0}^{m} (-1)^k (k+1) \sigma_k v_{n+1,k} = 0 \quad (**).$$

This relation allows us to express $v_{n+1,m}$ in terms of the $v_{n+1,j}$'s, $0 \le j \le m-1$. By making such a substitution in the right hand side of (*), we obtain a relation of the form

$$\frac{n-k-1}{n} v_{n,k} + \sum_{j=0}^{k} a_{k,j} v_{n,j} = \sum_{j=0}^{m-1} c_{k,j} v_{n+1,j} \quad (***).$$

However, the relations (***) for $0 \le k \le m-1$ can be expressed with matrices as

$$K_n V_n = C V_{n+1},$$

where the matrix C does not depend on n, i.e. has entries in $\mathbb{C}(\lambda_1, \ldots, \lambda_m)$, and the matrix K_n is lower triangular with diagonal entries the numbers

$$\frac{n-k-1}{n} + a_{k,k} = \frac{n-k-1}{n} + m, \quad 0 \le k \le m-1$$

In particular, the matrix K_n is invertible. By setting $M_n := K_n^{-1}C$, we have proved the claim.

By using several times the claim, we get:

$$V_{n+m} = V_{n+m}$$

$$V_{n+m-1} = M_{n+m-1}V_{n+m}$$

$$\vdots$$

$$V_n = (M_n M_{n+1} \dots M_{n+m-1})V_{n+m}$$

Therefore, the m + 1 elements v_n, \ldots, v_{n+m} can be expressed as linear combination, with coefficients in $\mathbb{C}(\lambda_1, \ldots, \lambda_m)(n)$, of the *m* elements $v_{n+m,0}, \ldots, v_{n+m,m-1}$. As a consequence, the elements v_n, \ldots, v_{n+m} are linearly dependent over the field $\mathbb{C}(\lambda_1, \ldots, \lambda_m)(n)$ and hence also over the ring $\mathbb{C}[\lambda_1, \ldots, \lambda_m][n]$.

1.4 Proof of theorem A

According to Lemmas 1 and 2, it is sufficient to prove the conjectures R(1) and R(2).

a) Proof of R(1)

We use the notations of subsection 1.3 with m = 1. Note that $u_n = \binom{2n}{n} \lambda_1^n$. If $u_n = 0$, we want to prove that $\lambda_1 = 0$. This is obvious.

b) Proof of R(2)

We use the notations of subsection 1.3 with m = 2. Note that:

$$u_n = \sum_{i+j=n} \binom{n+i}{n} \binom{n+j}{n} \lambda_1^i \lambda_2^j.$$

We rely on the following linear recurrence relation.

Lemma 6. For any $n \ge 3$, we have:

$$n(n-1)(\lambda_1 - \lambda_2)^2 u_n + (n-1)(2n-1)(\lambda_1 + \lambda_2)(\lambda_1 - 2\lambda_2)(\lambda_2 - 2\lambda_1)u_{n-1} - 3(3n-4)(3n-2)\lambda_1^2\lambda_2^2 u_{n-2} = 0.$$

Proof. We follow the beginning of the proof of Lemma 5 in the case where m = 2 and we compute the relations (*), (**) and (***). We get

$$A_0 = 2$$
, $B_0 = 2 - \sigma_1 X$, $A_1 = \frac{\sigma_1}{\sigma_2} + 2X$ and $B_1 = \frac{\sigma_1}{\sigma_2} + \frac{2\sigma_2 - \sigma_1^2}{\sigma_2}X$,

so that the relations (*) for k = 0, 1 are the following:

$$\begin{cases} \frac{3n-1}{n} v_{n,0} &= 2 v_{n+1,1} - \sigma_1 v_{n+1,2} \\ \sigma_1 v_{n,0} &+ \frac{3n-2}{n} \sigma_2 v_{n,1} &= \sigma_1 v_{n+1,1} + (2\sigma_2 - \sigma_1^2) v_{n+1,2}. \end{cases} (*).$$

We get at once:

$$v_{n+1,0} - 2\,\sigma_1\,v_{n+1,1} + 3\,\sigma_2\,v_{n+1,2} = 0 \quad (**),$$

so that the relations (***) for k = 0, 1 are the following:

$$\begin{cases} 3\frac{3n-1}{n}\sigma_2 v_{n,0} = \sigma_1 v_{n+1,0} + (6\sigma_2 - 2\sigma_1^2) v_{n+1,1} \\ 3\sigma_1\sigma_2 v_{n,0} + 3\frac{3n-2}{n}\sigma_2^2 v_{n,1} = (\sigma_1^2 - 2\sigma_2) v_{n+1,0} + (7\sigma_1\sigma_2 - 2\sigma_1^3) v_{n+1,1}, \end{cases}$$

i.e.

$$(6\sigma_2 - 2\sigma_1^2) v_{n+1,1} = 3 \frac{3n-1}{n} \sigma_2 v_n - \sigma_1 v_{n+1} \quad (A),$$

and

$$3\,\sigma_1\sigma_2\,v_n + 3\,\frac{3n-2}{n}\,\sigma_2^2\,v_{n,1} = (\sigma_1^2 - 2\sigma_2)\,v_{n+1} + (7\sigma_1\sigma_2 - 2\sigma_1^3)\,v_{n+1,1} \quad (B).$$

The relation (A) expresses $v_{n+1,1}$ in terms of v_n, v_{n+1} . Replacing n by n-1 allows to express $v_{n,1}$ in terms of v_{n-1}, v_n :

$$(6\sigma_2 - 2\sigma_1^2) v_{n,1} = 3 \frac{3n-4}{n-1} \sigma_2 v_{n-1} - \sigma_1 v_n \quad (A)'.$$

By substituting (A) and (A)' in (B), we get the following relation between v_{n-1}, v_n, v_{n+1} :

$$\begin{aligned} 3\,\sigma_1\sigma_2(6\sigma_2 - 2\sigma_1^2)\,v_n + \,3\,\frac{3n-2}{n}\,\sigma_2^2 \left[3\,\frac{3n-4}{n-1}\,\sigma_2\,v_{n-1} - \sigma_1\,v_n\right] \\ = \,(\sigma_1^2 - 2\sigma_2)(6\sigma_2 - 2\sigma_1^2)\,v_{n+1} \,+ (7\sigma_1\sigma_2 - 2\sigma_1^3)\,\left[3\,\frac{3n-1}{n}\,\sigma_2\,v_n - \sigma_1\,v_{n+1}\right], \\ &\text{i.e.} \quad \mu_2\,v_{n+1} + \mu_1\,v_n + \mu_0\,v_n = 0, \quad \text{where} \end{aligned}$$

$$\begin{split} \mu_2 &= (\sigma_1^2 - 2\sigma_2)(2\sigma_1^2 - 6\sigma_2) + \sigma_1(7\sigma_1\sigma_2 - 2\sigma_1^3) \\ &= -3\,\sigma_2(\lambda_1 - \lambda_2)^2 \\ \mu_1 &= 3\,\sigma_1\sigma_2(6\sigma_2 - 2\sigma_1^2) - 3\,\frac{3n-2}{n}\,\sigma_1\sigma_2^2 - 3\,\frac{3n-1}{n}(7\sigma_1\sigma_2 - 2\sigma_1^3)\sigma_2 \\ &= 3\,\sigma_1\sigma_2(9\sigma_2 - 2\sigma_1^2)\,\frac{2n-1}{n} \\ &= 3\,\sigma_1\sigma_2(\lambda_1 - 2\lambda_2)(\lambda_2 - 2\lambda_1)\,\frac{2n-1}{n} \\ \mu_0 &= 3^2\sigma_2^3\,\frac{3n-2}{n}\,\frac{3n-4}{n-1}. \end{split}$$

Since $v_{k+1} = 2\pi i u_k$ for any k, the result follows.

Remark 7. Another way to prove Lemma 6 is more elementary, but tedious. The left hand side being homogeneous of degree n + 2 in λ_1, λ_2 , it is enough to check that for $0 \le i \le n + 2$, the coefficient of $\lambda_1^i \lambda_2^{n+2-i}$ vanish.

Let us prove R(2). If $u_k = u_{k+1} = 0$, we want to prove that $\lambda_1 = \lambda_2 = 0$. We begin by showing by contradiction that $\lambda_1 = \lambda_2$. Otherwise, Lemma 6 shows us that the following implication holds:

$$\forall n \ge 3, \quad (u_{n-2} = u_{n-1} = 0) \implies u_n = 0.$$

Therefore, $u_n = 0$ for $n \ge k$ and by Remark 4, this implies the equality $\lambda_1 = \lambda_2 = 0$. A contradiction. Therefore $\lambda_1 = \lambda_2$. Set $\lambda := \lambda_1 = \lambda_2$. Lemma 6 gives us for any $n \ge 3$:

 $2(n-1)(2n-1)\lambda^3 u_{n-1} - 3(3n-4)(3n-2)\lambda^4 u_{n-2} = 0.$

Let us show by contradiction that $\lambda = 0$. Otherwise, the following implication would hold:

$$\forall n \ge 3, \quad u_{n-2} = 0 \implies u_{n-1} = 0.$$

We still get $u_n = 0$ for $n \ge k$, so that $\lambda = 0$. A contradiction. We have indeed $\lambda = 0$, so that $\lambda_1 = \lambda_2 = 0$.

1.5 The conjecture R(3).

The first aim of this subsection is to explain why we were not able to solve conjecture R(3) in the previous way. The second aim is to give some information (and motivation) for the reader who might be interested to undertake some investigations on this subject.

We use the notations of subsection 1.3 with m = 3, so that:

$$u_n = \sum_{i+j+k=n} \binom{n+i}{n} \binom{n+j}{n} \binom{n+k}{n} \lambda_1^i \lambda_2^j \lambda_3^k \in \mathbb{Z}[\lambda_1, \lambda_2, \lambda_3].$$

Before giving the linear recurrence relation satisfied by the u_n , we need some notations. If $\mu = (\mu_1, \mu_2, \mu_3)$ where μ_i are integers satisfying $\mu_1 \ge \mu_2 \ge \mu_3 \ge 0$, we define $m_\mu \in \mathbb{Z}[\lambda_1, \lambda_2, \lambda_3]$ by $m_\mu := \sum \lambda_1^{\nu_1} \lambda_2^{\nu_2} \lambda_3^{\nu_3}$ where (ν_1, ν_2, ν_3) describes all distinct permutations

of the triple
$$(\mu_1, \mu_2, \mu_3)$$
. We identify (μ_1, μ_2) and $(\mu_1, \mu_2, 0)$ as well as (μ_1) and $(\mu_1, 0, 0)$.
Hence $m_{(1)} = \lambda_1 + \lambda_2 + \lambda_3$, $m_{(1,1)} = \lambda_1 \lambda_2 + \lambda_1 \lambda_3 + \lambda_2 \lambda_3$, $m_{(1,1,1)} = \lambda_1 \lambda_2 \lambda_3$ and $m_{(3,2,1)} = \lambda_1^3 \lambda_2^2 \lambda_3 + \lambda_1^2 \lambda_2^3 \lambda_3 + \lambda_1 \lambda_2^3 \lambda_3^2 + \lambda_1^2 \lambda_2 \lambda_3^2 + \lambda_1 \lambda_2^2 \lambda_3^2$.
We set $\Delta = (\lambda_1 - \lambda_2)^2 (\lambda_1 - \lambda_3)^2 (\lambda_2 - \lambda_3)^2$ and define the M_i , N_i for $1 \le i \le 5$ by:
 $M_1 = 9m_{(4,2)} - 14m_{(4,1,1)} - 9m_{(3,3)} + 3m_{(3,2,1)} - 3m_{(2,2,2)}$;
 $M_2 = 5m_{(4,2)} - 8m_{(4,1,1)} - 5m_{(3,3)} + 2m_{(3,2,1)} - 3m_{(2,2,2)}$;
 $M_3 = 39m_{(4,2)} - 62m_{(4,1,1)} - 39m_{(3,3)} + 15m_{(3,2,1)} - 21m_{(2,2,2)}$;
 $M_4 = 33m_{(4,2)} - 52m_{(4,1,1)} - 3m_{(3,3)} + 12m_{(3,2,1)} - 15m_{(2,2,2)}$;
 $M_5 = 6m_{(4,2)} - 10m_{(4,1,1)} - 6m_{(3,3)} + 3m_{(3,2,1)} - 6m_{(2,2,2)}$;
 $N_1 = -2m_{(5,2)} + 4m_{(5,1,1)} + 3m_{(4,3)} - 3m_{(4,2,1)} - 8m_{(3,3,1)} + 8m_{(3,2,2)} + 10m_{(7,6)} + 30m_{(5,1)} - 146m_{(7,4,2)} + 216m_{(7,3,3)} - 60m_{(6,6,1)} + 70m_{(6,5,2)} - 32m_{(6,4,3)} - 60m_{(5,5,3)} + 40m_{(5,4,4)}$;
 $N_3 = -27m_{(4,4)} + 36m_{(4,3,1)} - 2m_{(4,2,2)} - 52m_{(3,3,2)}$;
 $N_4 = -342m_{(8,6)} + 1006m_{(8,5,1)} - 1110m_{(8,4,2)} + 972m_{(8,3,3)} + 342m_{(7,7)} - 141m_{(7,6,1)} - 1301m_{(7,5,2)} + 900m_{(7,4,3)} + 1178m_{(6,6,2)} - 15m_{(6,5,3)} - 724m_{(6,4,4)} + 238m_{(5,5,4)}$;
 $N_5 = 10m_{(8,6)} - 30m_{(8,5,1)} + 34m_{(8,4,2)} - 30m_{(8,3,3)} - 10m_{(7,7)} + 5m_{(7,6,1)} + 37m_{(7,5,2)} - 27m_{(7,4,3)} - 38m_{(6,6,2)} + 5m_{(6,5,3)} + 20m_{(6,4,4)} - 10m_{(5,5,4)}$.
Set:
 $A_n = n(n-1)(n-2)[(M_1n - 3M_2)\Delta$;
 $B_n = (n-1)(n-2)[(2M_1n^2 - M_3n)N_1 - 3N_2]$;
 $C_n = (n-2)[(M_1n^3 - M_nn^2)N_3 + 3nN_4 + 36N_5]$;

1 (

()

11

 $\langle \rangle$

1 (

(0, 0)

 $C_n = (n-2)[(M_1n^3 - M_4n^2)N_3 + 3nN_4 + 36N_5];$ $D_n = 8(2n-3)(4n-7)(4n-9)(M_1n - M_5)m_{(1,1,1)}^3.$

One could show the next result (using a computer!):

Lemma 8. For any $n \ge 4$, we have:

C 1 1 1 1 /

$$A_n u_n + B_n u_{n-1} + C_n u_{n-2} + D_n u_{n-3} = 0.$$

The difference with the recurrence relations obtained in Lemma 6 is that the factor $M_1n - 3M_2$ of A_n may suddenly vanish for a large value of n. Therefore, if we assume that $u_k = u_{k+1} = u_{k+2} = 0$, we do not succeed to show that $u_{k+3} = 0$. However, a closer analysis of the recurrence formula might probably be sufficient for proving R(3).

2 PRELIMINARY RESULTS

In subsection 2.1, we recall a valuative criterion characterizing the elements of $\overline{f(V)}$ where $f: V \to W$ is a morphism of complex algebraic varieties. The only valuation ring we need is the ring of complex formal power series. In subsection 2.2, after recalling equivalent definitions of a hsop, we give two results related with formal power series. In subsection 2.3, we make some technical definitions which will allow us (in the next section) to prove Th. B. Finally, in subsection 2.4, we prove an easy lemma on the multidegree.

2.1 Valuative criterion

The valuative criterion given in Lemma 9 below is familiar (e.g. [MFK94, chap. 2, §1, pp 52-54] or [Gro61a, §7]). We proved it in [Fur09].

Let $\mathbb{C}[[T]]$ be the algebra of complex formal power series and let $\mathbb{C}((T))$ be its quotient field. If V is a complex algebraic variety and A a complex algebra, V(A) will denote the points of V with values in A, i.e. the set of morphisms Spec $A \to V$. If v is a closed point of V and $\varphi \in V(\mathbb{C}((T)))$, we will write $v = \lim_{T \to 0} \varphi(T)$ when:

- i) the point φ : Spec $\mathbb{C}((T)) \to V$ is a composition Spec $\mathbb{C}((T)) \to \text{Spec }\mathbb{C}[[T]] \to V$;
- *ii)* v is the point $\operatorname{Spec} \mathbb{C} \to \operatorname{Spec} \mathbb{C}[[T]] \to V$.

For example, if $V = \mathbb{A}^1$ and $\varphi \in V(\mathbb{C}((T))) = \mathbb{C}((T))$, we will write $v = \lim_{T \to 0} \varphi(T)$ when $\varphi \in \mathbb{C}[[T]]$ and $v = \varphi(0)$.

Lemma 9. Let $f : V \to W$ be a morphism of complex algebraic varieties and let w be a closed point of W. The two following assertions are equivalent:

i) $w \in \overline{f(V)};$ ii) $w = \lim_{T \to 0} f(\varphi(T))$ for some $\varphi \in V(\mathbb{C}((T))).$

Remark. Note the analogy with the metric case where $w \in \overline{f(V)}$ if and only if there exists a sequence $(v_n)_{n\geq 1}$ of V such that $w = \lim_{n \to +\infty} f(v_n)$.

The following result is an easy consequence of Lemma 9 (see [Fur09, Cor. 1.1]).

Corollary 10. If $d = (d_1, \ldots, d_k)$ is a multidegree and $f \in \mathcal{G}$, the following assertions are equivalent:

- i) $f \in \overline{\mathcal{G}}_d$;
- ii) $f = \lim_{T \to 0} g_T$ for some $g \in \mathcal{G}_d(\mathbb{C}((T)))$.

Proof. For any integer $m \geq 2$, let \mathcal{B}_m be the set of triangular automorphisms whose degree is exactly equal to m. Let $\mathcal{A}' = \mathcal{A} \setminus \mathcal{B}$ be the set of affine non triangular automorphisms. It is enough to note that \mathcal{G}_d is the image of the following morphism of algebraic varieties:

$$\mathcal{A}^2 \times (\mathcal{A}')^{k-1} \times \prod_{1 \le i \le k} \mathcal{B}_{d_i} \longrightarrow \mathcal{G}$$

sending $((a_1, a_2), (a'_i)_i, (b_i)_i)$ to $a_1 \circ b_1 \circ a'_1 \circ b_2 \circ a'_2 \circ \cdots \circ a'_{k-1} \circ b_k \circ a_2$. The details are left to the reader.

Remark. Since \mathcal{G}_d is locally closed in \mathcal{G} (see [Fur09]), there is a natural identification between $\mathcal{G}_d(K)$ and the set of automorphisms of \mathbb{A}^2_K whose multidegree are equal to d, for any field K containing \mathbb{C} .

2.2 Homogeneous system of parameters and formal power series

Let K be an algebraically closed field and let \mathbb{A}_K^r be the affine r-space over K. Let us grade the polynomial algebra $R = K[z_1, \ldots, z_r]$ by assigning each z_k to be homogeneous of some strictly positive degree (depending on k). For each $m \geq 0$, the set of mhomogeneous polynomials is denoted by R_m . If $p = (p_1, \ldots, p_r) \in \mathbb{R}^r$, let $\phi_p \colon \mathbb{A}_K^r \to \mathbb{A}_K^r$ be the morphism of algebraic varieties defined by $\phi_p(w) = (p_1(w), \ldots, p_r(w))$ for $w \in \mathbb{A}_K^r$. Let also I_p be the ideal of R generated by p_1, \ldots, p_r . Following a usual terminology (e.g. [Sta96, Chap. I, Def. 5.1, p. 33]), if each p_k is homogeneous of some strictly positive degree (depending on k) and if $K[z_1, \ldots, z_r]$ is a finitely generated module over $K[p_1, \ldots, p_r]$, the sequence p is said to be a **hsop** (homogeneous system of parameters). For the sake of completeness, we give the proof of the following classical lemma characterizing hsop.

Lemma 11. Let $p = (p_1, \ldots, p_r)$ be a sequence of homogeneous polynomials of $R = K[z_1, \ldots, z_r]$, each z_k being homogeneous of some strictly positive degree (depending on k). The r-uple p is a hop of R if and only if the following equivalent assertions are satisfied:

- i) ϕ_p is a finite morphism;
- ii) ϕ_p is a quasi-finite morphism;
- iii) $(\phi_p)^{-1}(0)$ is a finite set;
- iv) $dim_K R/I_p < +\infty;$
- v) $(\phi_p)^{-1}(0) = \{0\};$
- vi) ϕ_p is a proper morphism;
- vii) R is a finitely generated and free module over $K[p_1, \ldots, p_r]$;
- viii) ϕ_p is a flat morphism;
- ix) For any $d > \max_k \deg p_k$, we have $R_{dl} \subseteq I_p^l$ when l is large enough;
- x) For some $d > \max_k \deg p_k$, we have $R_{dl} \subseteq I_p^l$ when l is large enough.

Proof. Note that assertion i) is a reformulation of the definition.

- i) \implies ii) and ii) \implies iii) are obvious.
- iii) \iff iv) follows from the Hilbert's Nullstellensatz.

iv) \implies i). Let h_1, \ldots, h_s be homogeneous elements of R which form a K-basis of R/I_p . Set $S := K[p_1, \ldots, p_r]$. It is enough to show that $R = \sum_i h_i S$. Set $N = \sum_i h_i S$ and let $S_+ = p_1 S + \cdots + p_r S$ be the ideal of S generated by the p_i . Note that S is a subgraded ring of R and that R and N are both graded module over S. Finally, since $R = N + S_+ R$, by the graded version of Nakayama's lemma, we get R = N.

iii) \implies v). Let us show by contradiction that $(\phi_p)^{-1}(0) = \{0\}$. Otherwise $(\phi_p)^{-1}(0)$ would contain a nonzero element $w = (w_1, \ldots, w_r)$. If $d_i := \deg z_i$ and $e_i := \deg p_i$, we have:

$$\forall \lambda \in K, \ p_i(\lambda^{a_1} z_1, \dots, \lambda^{a_r} z_r) = \lambda^{e_i} p_i(z_1, \dots, z_r).$$

This proves that $(\lambda^{d_1} w_1, \ldots, \lambda^{d_r} w_r)$ belongs to $(\phi_p)^{-1}(0)$ for any λ , contradicting (iii).

 $v) \Longrightarrow iii)$ is obvious.

i) \iff vi) follows from a theorem of Chevalley (see [Gro61b, EGA, III, 4.4.2, p. 136]) asserting that a morphism of algebraic varieties is finite if and only if it is proper and affine (see also [Mur67, Lemma (3.5.1), p. 52] or [BCW82, p. 296]). Alternatively, it is well known that a morphism is finite if and only if it is proper and quasi-finite (see the previous reference of Grothendieck!). Furthermore, it is clear that an affine proper morphism is quasi-finite. Indeed, each of its fibers being affine and complete, it has to be finite.

i) \iff vii) follows from [Sta96, Chapter I, Th. 5.9, p. 35]. Note that the implication vii) \implies i) is obvious. The implication i) \implies vii) also follows from [Bou07, §4, n° 4, Cor. of Prop. 5, p. 58]. This reference claims that R is a projective module over $K[p_1, \ldots, p_r]$. In this graded situation, any projective module is free.

vii) \implies viii). Any free module is flat.

viii) \implies ii) is clear, since a flat morphism is equidimensional (e.g. [Har77, (III, Cor. 9.6), p. 257]).

vii) \implies ix). Set $S = K[p_1, \ldots, p_r]$ and let h_1, \ldots, h_s be homogeneous elements of R such that $R = \sum_i h_i S$. Set $M = \max_i \deg h_i$, $m = \max_k \deg p_k$ and let d > m be any integer. Let us check that for any $l \geq \frac{M}{d-m}$, we have $R_{dl} \subseteq (I_p)^l$. Let f be any element of R_{dl} . There exists homogeneous elements u_i of S such that $f = \sum_i h_i u_i$. Furthermore, each u_i admits an expression $u_i = \sum_{\alpha} u_{i,\alpha} p^{\alpha}$, where the sum is over $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, $p^{\alpha} := p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ and $u_{i,\alpha}$ belongs to K. Set $|\alpha| = \alpha_1 + \cdots + \alpha_r$. We have $f = \sum_{i,\alpha} u_{i,\alpha} h_i p^{\alpha}$. If $u_{i,\alpha} \neq 0$, we may assume that $\deg f = \deg(h_i p^{\alpha})$. We get

$$m |\alpha| \geq \deg p^{\alpha} = \deg f - \deg h_i \geq dl - M \geq ml$$

from which follows $|\alpha| \geq l$ and finally $f \in (I_p)^l$.

ix) \implies x) is obvious.

 $x) \Longrightarrow v$ is easy and left to the reader.

Corollary 12. If $p = (p_1, \ldots, p_r)$ is a hoop of $K[z_1, \ldots, z_r]$, the map $\phi_p \colon \mathbb{A}_K^r \to \mathbb{A}_K^r$ is surjective.

Proof. Since ϕ_p is proper, it is a closed morphism and in particular its image is closed. Since ϕ_p is flat, it is an open morphism (see [Gro65, EGA, IV₂, 2.4.6, p. 20]) and in particular its image is open.

Remark 13. Let $p = (p_1, \ldots, p_r)$ be a sequence of homogeneous polynomials of $R = K[z_1, \ldots, z_r]$. The surjectivity of the morphism $\phi_p : \mathbb{A}_K^r \to \mathbb{A}_K^r$ is not sufficient to ensure that p is a hsop. Consider the algebra $\mathbb{C}[x, y]$ with the usual grading. The morphism $\mathbb{A}^2 \to \mathbb{A}^2$, $(x, y) \mapsto (xy^2, x(x+y)^2)$ is surjective, but not finite.

Let val: $\mathbb{C}((T)) \to \mathbb{Z} \cup \{+\infty\}$ be the valuation associated to the discrete valuation ring $\mathbb{C}[[T]]$.

Lemma 14. If (p_1, \ldots, p_r) is a hop of $R := \mathbb{C}[z_1, \ldots, z_r]$ and $q \in R$ is homogeneous with deg $q > \max_k \deg p_k$, then for any $b \in \mathbb{A}^r_{\mathbb{C}[T]}$ satisfying b(0) = 0, we have:

$$\operatorname{val} q(b) \ge \min_{k} \operatorname{val} p_k(b) + 1.$$

Proof. By point ix) of Lemma 11, there exists $l \ge 1$ such that $q^l \in (p_1, \ldots, p_r)^l$. For any $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, set $p^{\alpha} = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ and $|\alpha| = \alpha_1 + \cdots + \alpha_r$. If $A := \{\alpha \in \mathbb{N}^r, |\alpha| = l\}$, we can write $q^l = \sum_{\alpha \in A} s_\alpha p^\alpha \ (s_\alpha \in R)$. Furthermore, we may assume that $s_\alpha \in R_{d_\alpha}$, where $d_\alpha := \deg q^l - \deg p^\alpha \ge l(\deg q - \max_k \deg p_k) \ge l \ge 1$. Evaluating at band taking the valuation, we get: $l \operatorname{val} q(b) \ge \min_{\alpha \in A} \operatorname{val} s_\alpha(b) p^\alpha(b)$. But $\operatorname{val} s_\alpha(b) \ge 1$ and $\operatorname{val} p^\alpha(b) \ge l \min_k \operatorname{val} p_k(b)$, so that $l \operatorname{val} q(b) \ge l \min_k \operatorname{val} p_k(b) + 1$. \Box

The following lemma is a nice application of Cor. 12.

Lemma 15. If $p = (p_1, \ldots, p_r)$ is a hsop of $\mathbb{C}[z_1, \ldots, z_r]$ and $\gamma \in \mathbb{A}^r_{\mathbb{C}}$, there exist $q \ge 1$ and $b \in \mathbb{A}^r_{\mathbb{C}[[T]]}$ such that b(0) = 0 and $p(b) = T^q \gamma$.

Proof. Let $K := \bigcup_{q \ge 1} \mathbb{C}((T^{\frac{1}{q}}))$ be the quotient field of the ring $\bigcup_{q \ge 1} \mathbb{C}[[T^{\frac{1}{q}}]]$ of all formal Puiseux series. By Newton-Puiseux theorem (see e.g. [Rui93, Prop. 4.4]), K is an algebraic closure of $\mathbb{C}((T))$. Let us note that p is a hoop of $R := K[z_1, \ldots, z_r]$. By Cor. 12, there exists an element a in the affine space \mathbb{A}_K^r such that $p(a) = T\gamma$. Let $q \ge 1$ be such that $b := a(T^q) \in \mathbb{A}_{\mathbb{C}((T))}^r$. Replacing T by T^q , we get $p(b) = T^q\gamma$. Using the valuative criterion of properness (see e.g. [Har77, (II, 4.7), p. 101]) to the proper morphism $\phi_p \colon \mathbb{A}^r \to \mathbb{A}^r$ (see Lemma 11), it is clear that $b \in \mathbb{A}_{\mathbb{C}[[T]]}^r$. Since p(b(0)) = 0, by point v) of Lemma 11, we get b(0) = 0.

2.3 Technical definitions

Let $m, n \geq 1$ be fixed integers and set N := (m+1)(n+1)-1. Let $A_0, \ldots, A_m, B_1, \ldots, B_n$ be indeterminates and let $\mathbb{C}[B]$, resp. $\mathbb{C}[A, B]$, be the polynomial algebra generated by the B_j , resp. by the A_i, B_j . We grade these polynomial algebras by assigning A_i, B_i to be homogeneous of degree i.

We now successively define homogeneous polynomials:

- $C_i \in \mathbb{C}[A, B]$ of degree *i* for $1 \leq i \leq N$;
- $U_{i,j} \in \mathbb{C}[B]$ of degree i j for $1 \le i \le N, 0 \le j \le m$;
- $W_{i,j} \in \mathbb{C}[B]$ of degree i j for $1 \le i, j \le m$;
- $D_i \in \mathbb{C}[B], E_i \in \mathbb{C}[A, B]$ of degree i for $1 \le i \le m$;
- $F_i \in \mathbb{C}[B], \ G_i \in \mathbb{C}[A, B] \text{ of degree } i \text{ for } 1 \le i \le N;$

satisfying the following points:

$$(0) \sum_{1 \le i \le N} C_i X^{i+1} = A \circ B(X) - A_0 X$$

where $A(X) := \sum_{0 \le i \le m} A_i X^{i+1}$ and $B(X) := X + \sum_{1 \le i \le n} B_i X^{i+1}$;
(1) $A_i = A_0 D_i + E_i$ for $1 \le i \le m$;
(2) $C_i = A_0 F_i + G_i$ for $1 \le i \le N$;
(3) $E_i = \sum_{1 \le j \le m} W_{i,j} C_j$ for $1 \le i \le m$;
(4) $G_i := \sum_{1 \le j \le m} U_{i,j} E_j$ for $1 \le i \le N$;

(5) the matrices $(U_{i,j})_{1 \le i,j \le m}$ and $(W_{i,j})_{1 \le i,j \le m}$ are inverses of one another.

Later on, we will only use the above points (0)-(5) so that the reader in a hurry can skip the following trivial, but technical, construction.

Construction.

- The $C_i \in \mathbb{C}[A, B]$ are uniquely defined by (0).
- The $U_{i,j} \in \mathbb{C}[B]$ are uniquely defined by $C_i = \sum_{0 \le j \le m} U_{i,j}A_j \ (1 \le i \le N).$

Matricially, this may be written C = U.A, where A (resp. C) is the column vector $A = (A_i)_{0 \le i \le m}$ (resp. $C = (C_i)_{1 \le i \le N}$) and U is the matrix $U = (U_{i,j})_{\substack{1 \le i \le N \\ 0 \le j \le m}}$.

We have $\mathsf{U} = \begin{pmatrix} \mathsf{V} \\ \mathsf{B} \\ * \end{pmatrix}$ where B is the column vector $\mathsf{B} = {}^t(B_1, \dots, B_n, 0, \dots, 0)$

and $V := (U_{i,j})_{1 \le i,j \le m}$ is a lower triangular square matrix with 1's on the diagonal.

• The matrix $W = (W_{i,j})_{1 \le i,j \le m}$ is defined as the inverse of V.

• The column vectors $D = (D_i)_{1 \le i \le m}$ and $E = (E_i)_{1 \le i \le m}$ are defined by $D := -W.\widetilde{B}$ and $E := W.\widetilde{C}$, where \widetilde{B} (resp. \widetilde{C}) denotes the column vector obtained from B (resp. C) by keeping the first *m* rows. Since the column vector $\widetilde{A} := {}^t(A_1, \ldots, A_m)$ satisfies $\widetilde{C} = A_0 \widetilde{B} + V.\widetilde{A}$, we get $\widetilde{A} = -A_0 W.\widetilde{B} + W.\widetilde{C}$, i.e. $\widetilde{A} = A_0 D + E$, which is (1).

• F_i, G_i are defined by $F_i := U_{i,0} + \sum_{1 \le j \le m} U_{i,j} D_j$ and $G_i := \sum_{1 \le j \le m} U_{i,j} E_j$ $(1 \le i \le N)$.

Since $C_i = \sum_{\substack{0 \le j \le m \\ 1 \le j \le m}} U_{i,j}A_j$ for $1 \le i \le N$ and $A_j = A_0D_j + E_j$ for $1 \le j \le m$, we get $C_i = U_{i,0}A_0 + \sum_{\substack{1 \le j \le m \\ 1 \le j \le m}} U_{i,j}(A_0D_j + E_j)$ and (2) follows. The assertions (3), (4) and (5) are obvious.

Remark 16. We have $G_i = \sum_{1 \leq j, k \leq m} U_{i,j} W_{j,k} C_k$, so that if $i \leq m$, we get $G_i = C_i$ and $F_i = 0$.

We will always use the conjecture R(m, n) through the next statement.

Lemma 17. If the conjecture $\mathbb{R}(m, n)$ holds, the family $(F_{m+i})_{1 \le i \le n}$ is a hop of $\mathbb{C}[B]$.

Proof. If $\overline{b} = (\overline{b}_1, \dots, \overline{b}_n) \in \mathbb{C}^n$ satisfies $F_{m+i}(\overline{b}) = 0$ for $1 \leq i \leq n$, we want to show that $\overline{b} = 0$. Let us set $\overline{a}_0 = 1$, $\overline{a}_i = D_i(\overline{b})$ for $1 \le i \le m$ and $\overline{a} = (\overline{a}_0, \ldots, \overline{a}_m)$. By (1) evaluated at $(\overline{a}, \overline{b})$, we get $E_i(\overline{a}, \overline{b}) = 0$ for $1 \leq i \leq m$. By (3) and (5), we get $C_i(\overline{a}, \overline{b}) = 0$ for $1 \leq i \leq m$. Moreover, for any $m+1 \leq i \leq m+n$, we get $G_i(\overline{a}, \overline{b}) = 0$ by (4), so that $C_i(\overline{a}, \overline{b}) = 0$ by (2) and by Remark 16. For the moment, we have proved that $C_i(\overline{a}, \overline{b}) = 0$ for $1 \leq i \leq m+n$.

Let us set $a := X(1 + \overline{a}_1 X + \dots + \overline{a}_m X^m)$, $b := X(1 + \overline{b}_1 X + \dots + \overline{b}_n X^n)$ and $c := a \circ b = X(1 + \overline{c}_1 X + \cdots + \overline{c}_N X^N) \in \mathbb{C}[X]$, where the $\overline{c}_i \in \mathbb{C}$. Using the relation (0), we get $\overline{c}_i = C_i(\overline{a}, \overline{b}) = 0$ for $1 \le i \le m + n$. By R(m, n), we get a = b = X.

We finish this subsection by a technical result to be used in Lemma 20 below. Even if the proof relies on the above technical definitions, the statement itself is self-contained.

Lemma 18. Set $a(X) = \sum_{0 \le i \le m} a_i X^{i+1}$ and $b(X) = X + \sum_{1 \le i \le n} b_i X^{i+1}$, where a_i, b_i are elements of $\mathbb{C}((T))$. Set $c(X) = a \circ b(X) - a_0 X$. Note that a(X), b(X) and c(X) are elements of $\mathbb{C}((T))[X]$. Assume that $\lim_{T \to 0} b = X$ and $\lim_{T \to 0} c = p \in \mathbb{C}[X]$. Then, if the conjecture R(m, n) holds, we get deg $p \leq m + n + 1$.

Proof. If $\mathbf{a} := (a_0, \dots, a_m)$ and $\mathbf{b} := (b_1, \dots, b_n)$, we have $c(X) = \sum_{\substack{1 \le i \le N \\ T \to 0}} C_i(\mathbf{a}, \mathbf{b}) X^{i+1}$ by the relation (0). Since $\lim_{\substack{T \to 0 \\ T \to 0}} b = X$ all the b_i belong to $T\mathbb{C}[[T]]$ and since $\lim_{\substack{T \to 0 \\ T \to 0}} c$ exists all

the $C_i(\mathsf{a}, \mathsf{b})$ belong to $\mathbb{C}[[T]]$

<u>Claim.</u> If $m + 1 \le i \le N$, then $G_i(\mathsf{a}, \mathsf{b}) \in T\mathbb{C}[[T]]$.

If $1 \leq j, k \leq m$, we have:

• $U_{i,j}(\mathbf{b}) \in T\mathbb{C}[[T]]$ since $U_{i,j} \in \mathbb{C}[B]$ is homogeneous of degree $i - j \ge m + 1 - m = 1$;

- $W_{j,k}(\mathbf{b}) \in \mathbb{C}[[T]]$ since $W_{j,k}$ is a polynomial;
- $C_k(\mathsf{a},\mathsf{b}) \in \mathbb{C}[[T]].$

By (5) or Remark 16, we have $G_i = \sum_{1 \le i, k \le m} U_{i,j} W_{j,k} C_k$ and the claim follows.

By (2), we have $C_i(\mathsf{a}, \mathsf{b}) = a_0 F_i(\mathsf{b}) + G_i(\mathsf{a}, \mathsf{b})$.

If $i \ge m+1$, we have val $C_i(\mathbf{a}, \mathbf{b}) \ge 0$ and val $G_i(\mathbf{a}, \mathbf{b}) \ge 1$, so that val $a_0 F_i(\mathbf{b}) \ge 0$. We want to show that val $C_i(\mathbf{a}, \mathbf{b}) \geq 1$, when i > m + n. For this, it is sufficient to show that val $a_0 F_i(\mathbf{b}) \geq 1$. By Lemmas 14 and 17, if i > m + n, we have:

$$\operatorname{val} F_i(\mathsf{b}) \ge \min_{1 \le j \le n} \operatorname{val} F_{m+j}(\mathsf{b}) + 1,$$

so that $\operatorname{val} a_0 F_i(\mathsf{b}) \ge \min_{1 \le j \le n} \operatorname{val} a_0 F_{m+j}(\mathsf{b}) + 1 \ge 1.$

2.4 An easy lemma on the multidegree

Lemma 19. Let K be any field containing \mathbb{C} and let $f = (f_1, f_2)$ be an automorphism of \mathbb{A}^2_K of multidegree (d_1, \ldots, d_k) with $k \ge 1$, then deg $f_1 = d_1 \ldots d_k$ or $d_2 \ldots d_k$ (and the same holds for f_2). Furthermore, if deg $f_1 = d_1 \ldots d_k$, then there exists a unique scalar $\lambda \in K$ such that deg $(f_2 - \lambda f_1) < d_1 \ldots d_k$, or equivalently such that deg $(f_2 - \lambda f_1) =$ $d_2 \ldots d_k$

Proof. By definition of the multidegree, f admits a reduced expression

$$f = \alpha_1 \circ \beta_1 \circ \cdots \circ \alpha_k \circ \beta_k \circ \alpha_{k+1},$$

where each α_i is affine and each β_i is triangular of degree d_i . Set

$$g := \alpha_1^{-1} \circ f = \beta_1 \circ \alpha_2 \circ \cdots \circ \alpha_k \circ \beta_k \circ \alpha_{k+1}.$$

An easy induction would establish that $\deg g_1 = d_1 \dots d_k$ and $\deg g_2 = d_2 \dots d_k$ (for details, see [Fur97, Proof of Prop. 1, p. 606]). The result follows.

3 PROOF OF THEOREM B

In this section, $m, n \ge 1$ are fixed integers and we assume that the conjecture R(m, n) holds. We set $d = (d_1, d_2) = (m + 1, n + 1)$ and we want to show that $\overline{\mathcal{G}}_d = \bigcup \mathcal{G}_e$.

Subsection 3.1 is devoted to the proof of the first inclusion $\overline{\mathcal{G}}_d \subseteq \bigcup_{\substack{e \leq d \\ e \leq d}} \mathcal{G}_e$. It only relies on the self-contained Lemma 18. Subsection 3.2 is devoted to the proof of the second inclusion $\bigcup_{\substack{e \leq d \\ e \leq d}} \mathcal{G}_e \subseteq \overline{\mathcal{G}}_d$. It is a little more involved, since it uses the polynomials C_i, D_i, E_i, F_i, G_i defined in subsection 2.3.

3.1 The first inclusion

If $f \in \overline{\mathcal{G}}_d$, let us show that $f \in \bigcup_{e \leq d} \mathcal{G}_e$. By [Fur02], the length is a lower semicontinuous

function on \mathcal{G} so that the length of f satisfies $l \leq 2$. We will consider 3 cases:

- l = 0. There is nothing to show;
- l = 1. We conclude by Lemma 20 below;
- l = 2. We conclude by Lemma 21 below.

Lemma 20. If $e \geq 2$ and $\mathcal{G}_{(e)} \cap \overline{\mathcal{G}}_{(d_1,d_2)} \neq \emptyset$, then $e < d_1 + d_2$.

Proof. If $f \in \mathcal{G}_{(e)} \cap \overline{\mathcal{G}}_d$, let us prove that $e < d_1 + d_2$. Since $\mathcal{A} \circ f \circ \mathcal{A} \subseteq \overline{\mathcal{G}}_d$, we may assume that f = (X + p(Y), Y) with deg p = e. If $e \leq d_2$, there is nothing to prove. So, let us assume that $e > d_2$. By Cor. 10, there exists $g = (g_1, g_2) \in \mathcal{G}_d\left(\mathbb{C}((T))\right)$ such that $f = \lim_{T \to 0} g_T$. By Lemma 19, we must have deg $g_1 = d_1 d_2$.

<u>First claim</u>. We may assume that deg $g_2 = d_2$.

Indeed, since g is of multidegree (d_1, d_2) , by Lemma 19, there exists a unique $\lambda \in$ $\mathbb{C}((T))$ such that $\deg(g_2 - \lambda g_1) = d_2$. It is enough to show that $\operatorname{val}(\lambda) > 0$, because we can then replace g by $(u_1, u_2) := (g_1, g_2 - \lambda g_1)$. Let μ (resp. $\nu) \in \mathbb{C}((T))$ be the Y^{e} -coefficient of g_{2} (resp. u_{1}). Applying the equality $g_{2} = u_{2} + \lambda u_{1}$ to the Y^{e} -coefficient, we get $\mu = \lambda \nu$ (since we have assumed that $e > d_2$). However, we have val $(\nu) = 0$ (since $\lim_{T\to 0} u_1(T) = X + p(Y)$ and $\deg p = e$, so that $\operatorname{val}(\lambda) = \operatorname{val}(\mu) > 0$ and the claim is proved.

Since deg $g_1 > deg g_2$, it is well-known (see e.g. [Fur97, Th. 1.i]) that we can write (in a unique way)

$$g = \tau \circ t_1 \circ \sigma \circ t_2 \circ l,$$

where $\tau = (X + a, Y + b)$ is a translation,

 $t_1 = \left(X + \sum_{0 \le i \le m} a_i Y^{i+1}, Y\right), t_2 = \left(X + \sum_{1 \le i \le n} b_i Y^{i+1}, Y\right) \text{ are triangular automorphisms,}$ $\sigma = (Y, X)$ and $l = (l_1, l_2) = (\alpha X + \beta Y, \gamma X + \delta Y)$ are linear automorphisms, with the

 a_i 's, b_i 's, $a, b, \alpha, \beta, \gamma, \delta$ belonging to $\mathbb{C}((T))$. By making the composition, we get:

$$g = \left(l_2 + \sum_{0 \le i \le m} a_i \left[l_1 + \sum_{1 \le j \le n} b_j l_2^{j+1}\right]^{i+1} + a, \quad l_1 + \sum_{1 \le j \le n} b_j l_2^{j+1} + b\right).$$

Since $f = \lim_{T \to 0} g_T$, by looking at the constant terms, we get $a, b \in \mathbb{C}[[T]]$ and there is no restriction to assume that a = b = 0.

<u>Second claim.</u> We may assume that $l = (l_1, l_2) = (Y, X + \rho Y)$ for some $\rho \in \mathbb{C}((T))$. Note that $\lim_{T \to 0} \alpha = 0$, $\lim_{T \to 0} \beta = 1$ and $\lim_{T \to 0} \alpha \delta - \beta \gamma = -1$. The last relation comes from the Jacobian equality $\operatorname{Jac} g = \operatorname{Jac} \sigma \times \operatorname{Jac} l = -(\alpha \delta - \beta \gamma)$. Set $\rho := \frac{\delta - \alpha}{\beta}$. Since $(l_1, l_2) = (Y, X + \rho Y) \circ h_T$, where $h_T := (-\rho l_1 + l_2, l_1)$, it is enough to show that $\lim_{T\to 0} h_T = (X, Y)$. For the second component, it is clear. For the first, we have $-\rho l_1 + l_2 = (\gamma - \rho \alpha) X + (\delta - \rho \beta) Y. \text{ But } \gamma - \rho \alpha = \frac{\alpha^2}{\beta} - \frac{\alpha \delta - \beta \gamma}{\beta}, \text{ so that } \lim_{T \to 0} \gamma - \rho \alpha = 1$ and $\delta - \rho\beta = \alpha$, so that $\lim_{T \to 0} \delta - \rho\beta = 0$ and the claim is proved.

So, we can now assume that:

$$g = \left(X + \rho Y + \sum_{0 \le i \le m} a_i \left[Y + \sum_{1 \le j \le n} b_j (X + \rho Y)^{j+1}\right]^{i+1}, \quad Y + \sum_{1 \le j \le n} b_j (X + \rho Y)^{j+1}\right).$$

Inspecting the Y-powers, the relation $\lim_{T\to 0} g_T = (X + p(Y), Y)$ gives us:

$$\lim_{T \to 0} \rho Y + \sum_{0 \le i \le m} a_i \left[Y + \sum_{1 \le j \le n} b_j \rho^{j+1} Y^{j+1} \right]^{i+1} = p(Y) \quad \text{and} \lim_{T \to 0} \sum_{1 \le j \le n} b_j \rho^{j+1} Y^{j+1} = 0.$$

Setting $\tilde{b}_j := b_j \rho^{j+1}$, we get:

$$\lim_{T \to 0} \rho Y + \sum_{0 \le i \le m} a_i \left[Y + \sum_{1 \le j \le n} \widetilde{b}_j Y^{j+1} \right]^{i+1} = p(Y) \quad \text{and} \quad \lim_{T \to 0} \sum_{1 \le j \le n} \widetilde{b}_j Y^{j+1} = 0.$$

Looking at the Y-coefficient, the first relation shows us that $\lim_{T\to 0} \rho + a_0 = p_1$, where p_1 is the Y-coefficient of p(Y).

Therefore
$$\lim_{T \to 0} \sum_{0 \le i \le m} a_i \left[Y + \sum_{1 \le j \le n} \widetilde{b}_j Y^{j+1} \right]^{i+1} - a_0 Y = p(Y) - p_1 Y \text{ and Lemma 18}$$

tells us that $\deg \left(p(Y) - p_1 Y \right) \le m + n + 1 = d_1 + d_2 - 1.$

Lemma 21. If $\mathcal{G}_{(e_1, e_2)} \cap \overline{\mathcal{G}}_{(d_1, d_2)} \neq \emptyset$, then $e_1 \leq d_1$ and $e_2 \leq d_2$.

This lemma is a consequence of the following result, which is [Fur09, Th. C]:

Theorem 22. If $u = (u_1, \ldots, u_l)$, $v = (v_1, \ldots, v_l)$ are two multidegrees with the same length, then the following assertions are equivalent:

i) $\mathcal{G}_u \subseteq \overline{\mathcal{G}}_v$;

ii)
$$\mathcal{G}_u \cap \overline{\mathcal{G}}_v \neq \emptyset;$$

iii) $u_i \leq v_i$ for each i (i.e. $u \leq v$).

However, here is a simple proof of Lemma 21:

Proof of Lemma 21. Let V be the polynomial algebra $\mathbb{C}[X, Y]$. Any element v of V admits a unique expression $v = \sum_{i \ge 0} v_i$, where v_i is homogeneous of degree i. Let $\Pi_{>k} \colon V \to V$ be the projection sending v to $\sum_{i>k} v_i$. Two polynomials $u, v \in V$ are linearly dependent if and only if $u \wedge v = 0$ in $\bigwedge^2 V$. The key point is the fact that for each $f = (f_1, f_2) \in \mathcal{G}_{(d_1, d_2)}$, we have

$$d_2 = \min\{k, \ \Pi_{>k}(f_1) \land \Pi_{>k}(f_2) = 0\}.$$

In particular, we have $\Pi_{>d_2}(f_1) \wedge \Pi_{>d_2}(f_2) = 0$ and this condition still holds if we only assume that f belongs to $\overline{\mathcal{G}}_{(d_1,d_2)}$. Therefore, if $f \in \mathcal{G}_{(e_1,e_2)} \cap \overline{\mathcal{G}}_{(d_1,d_2)}$, we get $e_2 \leq d_2$. The map $g \mapsto g^{-1}$ being an automorphism of (the infinite dimensional algebraic variety) \mathcal{G} sending an automorphism of multidegree (u_1,\ldots,u_l) to an automorphism of multidegree (u_l,\ldots,u_1) , we also have $f^{-1} \in \mathcal{G}_{(e_2,e_1)} \cap \overline{\mathcal{G}}_{(d_2,d_1)}$ so that $e_1 \leq d_1$. \Box

3.2The second inclusion

Let us show that $\mathcal{G}_e \subseteq \overline{\mathcal{G}}_d$ for any $e \preceq d$.

If e is of length 0 or 2, it is easy. For the sake of completeness, let us prove it by using [Fur97, section 4] (see also [Fur09, subsection 7.2]). Indeed, we define the partial order \leq on the set of multidegrees in the following way. If $u = (u_1, \ldots, u_k)$ and $v = (v_1, \ldots, v_l)$ are multidegrees, we say that $u \leq v$ if $k \leq l$ and if there exists a finite sequence $1 \leq i_1 < i_2 < \cdots < i_k \leq l$ such that $u_j \leq v_{i_j}$ for $1 \leq j \leq k$. By [Fur97, section 4] the inequality $u \leq v$ implies the inclusion $\mathcal{G}_u \subseteq \overline{\mathcal{G}}_v$. If e is of length 2, the inclusion $\mathcal{G}_e \subseteq \overline{\mathcal{G}}_d$ is also a consequence of Th. 22 above. Therefore, for showing the second inclusion, it is enough to prove the next result:

Lemma 23. If $2 \leq e < d_1 + d_2$, then the following inclusion holds: $\mathcal{G}_{(e)} \subseteq \overline{\mathcal{G}}_{(d_1,d_2)}$.

Proof. It is sufficient to show that
$$\left(X + \sum_{1 \leq i \leq m+n} \gamma_i Y^{i+1}, Y\right) \in \overline{\mathcal{G}}_d$$
 for any $\gamma_i \in \mathbb{C}$.

We take back the notations of subsection 2.3. By Lemmas 15 and 17, there exist $q \ge 1$ and $b := (b_1, \ldots, b_n) \in \mathbb{A}^n_{\mathbb{C}[[T]]}$ such that b(0) = 0 and

$$T^{-q}F_{m+i}(\widetilde{b}) = \gamma_{m+i}, \quad 1 \le i \le n.$$

Set $a_0 := T^{-q}$, $a_i := a_0 D_i(\widetilde{b})$ for $1 \le i \le m$, $\rho := -T^{-q}$ and $b_j := \widetilde{b}_j \rho^{-j-1}$ for $1 \le j \le n$. Set $g := t_1 \circ \sigma \circ t_2 \circ l$, where

$$t_1 = \left(X + \sum_{0 \le i \le m} a_i Y^{i+1}, Y \right), \quad t_2 = \left(X + \sum_{1 \le i \le n} b_i Y^{i+1}, Y \right)$$

are triangular automorphisms, $\sigma = (Y, X)$ and $l = (Y, X + \rho Y)$. We have:

$$g = \left(X + \rho Y + \sum_{0 \le i \le m} a_i \left[Y + \sum_{1 \le j \le n} b_j (X + \rho Y)^{j+1}\right]^{i+1}, \quad Y + \sum_{1 \le j \le n} b_j (X + \rho Y)^{j+1}\right).$$

Claim.
$$\lim_{T \to 0} g_T = \left(X + \sum_{m+1 \le i \le m+n} \gamma_i Y^{i+1}, \quad Y\right).$$

Let us begin to show that $\lim_{T\to 0} g_2 = Y$. For $1 \le j \le n$, we have $b_j (X + \rho Y)^{j+1} = \tilde{b}_j (\rho^{-1}X + Y)^{j+1}$, where $\lim_{T\to 0} \tilde{b}_j = \lim_{T\to 0} \rho^{-1} = 0$, so that $\lim_{T\to 0} b_j (X + \rho Y)^{j+1} = 0$ and the result is clear.

Let us now deal with the first component $g_1 = X + \rho Y + \sum_{0 \le i \le m} a_i g_2^{i+1}$.

First step. Let us show that in this last expression of g_1 , the limit of g_1 is unchanged if we replace g_2 by

$$p := Y + \sum_{1 \le j \le n} \widetilde{b}_j Y^{j+1}.$$

It is sufficient to check that $\lim_{T \to 0} a_i (g_2^{i+1} - p^{i+1}) = 0.$

As $\lim_{T \to 0} g_2 = \lim_{T \to 0} p = Y$ and $g_2^{i+1} - p^{i+1} = (g_2 - p)(g_2^i + \dots + p^i)$, we will only check that $\lim_{T \to 0} a_i (g_2 - p) = 0$.

Since $g_2 - p = \sum_{1 \le i \le n} b_j \left[(X + \rho Y)^{j+1} - (\rho Y)^{j+1} \right]$, it is enough to show that: $\lim_{T \to 0} a_i b_j \left[(X + \rho Y)^{j+1} - (\rho Y)^{j+1} \right] = 0.$

As $\lim_{T \to 0} \frac{(X + \rho Y)^{j+1} - (\rho Y)^{j+1}}{(j+1)XY^j \rho^j} = 1$, we will only show that $\lim_{T \to 0} a_i b_j \rho^j = 0$.

It is clear, because $a_i b_j \rho^j = -\frac{a_i}{a_0} \tilde{b}_j$ where $\lim_{T \to 0} \tilde{b}_j = 0$ and $\lim_{T \to 0} \frac{a_i}{a_0} = 1$ (resp. 0) if i = 0 (resp. $i \ge 1$).

<u>Second step.</u> Let us show that $\lim_{T \to 0} c = \sum_{m+1 \le i \le m+n} \gamma_i Y^{i+1}$, where

$$c := \rho Y + \sum_{0 \le i \le m} a_i \, p^{i+1} = -a_0 Y + \sum_{0 \le i \le m} a_i \, p^{i+1}.$$

If $\mathbf{a} := (a_0, \dots, a_m)$, by the relation (0) we have $c = \sum_{1 \le i \le N} C_i(\mathbf{a}, \widetilde{b}) Y^{i+1}$.

We get $E_j(\mathbf{a}, \widetilde{b}) = 0$ for $1 \leq j \leq m$ by (1), so that $G_i(\mathbf{a}, \widetilde{b}) = 0$ for $1 \leq i \leq N$ by (4) and $C_i(\mathbf{a}, \widetilde{b}) = a_0 F_i(\widetilde{b}) = T^{-q} F_i(\widetilde{b})$ for $1 \leq i \leq N$ by (2). Therefore:

- $C_i(\mathbf{a}, \widetilde{b}) = 0$ for $1 \le i \le m$ (see Remark 16); $\lim_{T \to 0} C_{m+i}(\mathbf{a}, \widetilde{b}) = \lim_{T \to 0} T^{-q} F_{m+i}(\widetilde{b}) = \gamma_{m+i}$ for $1 \le i \le n$;

• $\lim_{T \to 0} C_i(\mathbf{a}, \widetilde{b}) = 0$ for i > m + n, since val $F_i(\widetilde{b}) \ge \min_{1 \le j \le n} \operatorname{val} F_{m+j}(\widetilde{b}) + 1 \ge q + 1$ (by Lemma 14).

This proves the second step and the claim follows.

If we now set
$$f := t \circ g$$
, where $t := \left(X + \sum_{1 \leq i \leq m} \gamma_i Y^{i+1}, Y\right)$ is a triangular automorphism, then $f \in \mathcal{G}_d\left(\mathbb{C}((T))\right)$ and $\lim_{T \to 0} f_T = \left(X + \sum_{1 \leq i \leq m+n} \gamma_i Y^{i+1}, Y\right)$. We conclude by Cor. 10.

4 PROOF OF THEOREM D

We begin with the following lemma:

Lemma 24. Let $d \ge 2$ be an integer. Then the subset $\mathcal{G}_{(d)}$ of the group \mathcal{G} is a double coset modulo the affine subgroup \mathcal{A} if and only if d = 2 or 3.

Proof. Let us define the equivalence relation \sim on \mathcal{G} by: $\forall f, g \in \mathcal{G}, f \sim g \iff f$ and g have the same double coset modulo \mathcal{A} , i.e. $\mathcal{A} \circ f \circ \mathcal{A} = \mathcal{A} \circ g \circ \mathcal{A}$.

Let us note that any automorphism in the double coset $\mathcal{A} \circ f \circ \mathcal{A}$ has the same degree as f. Let $p(Y), q(Y) \in \mathbb{C}[Y]$ be any polynomials.

<u>Claim</u>. The following assertions are equivalent:

i) $(X + p(Y), Y) \sim (X + q(Y), Y);$

ii) There exists $\alpha, \beta, \gamma \in \mathbb{C}$ with $\alpha \beta \neq 0$ such that $q''(Y) = \alpha p''(\beta Y + \gamma)$.

<u>Proof of the claim</u>. There is no restriction to assume that deg $p = \deg q \ge 2$.

i) \implies ii). If $(X + p(Y), Y) \sim (X + q(Y), Y)$, there exists affine automorphisms u and v such that $(X + q(Y), Y) = u \circ (X + p(Y), Y) \circ v$. If u = (aX + bY + c, dX + eY + f) and $v = (\tilde{a}X + \tilde{b}Y + \tilde{c}, \tilde{d}X + \tilde{e}Y + \tilde{f})$, we get:

$$X + q(Y) = a p(\tilde{d}X + \tilde{e}Y + \tilde{f}) + a (\tilde{a}X + \tilde{b}Y + \tilde{c}) + b (\tilde{d}X + \tilde{e}Y + \tilde{f}) + c.$$

Setting X = 0 and derivating two times with respect to Y, we get: $q''(Y) = \alpha p''(\beta Y + \gamma)$, where we have set: $\alpha := a(\tilde{e})^2$, $\beta := \tilde{e}$ and $\gamma := \tilde{f}$. Since $q'' \neq 0$, it is clear that $\alpha \neq 0$. If deg $p = \deg q \ge 3$, we have $\beta \neq 0$ for reason of degrees. If deg $p = \deg q = 2$, we can assume that $\beta \neq 0$.

ii) \implies i). If $q''(Y) = \alpha p''(\beta Y + \gamma)$, then, by integrating two times, we get: aq(Y) + bY + c = p(dY + e), where $a, b, c, d, e \in \mathbb{C}$ and $ad \neq 0$. It follows that:

$$(X + p(Y), Y) \circ (aX, dY + e) = (aX + bY + c, dY + e) \circ (X + q(Y), Y)$$

and finally $(X + p(Y), Y) \sim (X + q(Y), Y)$. The claim is proved.

If d = 2 or 3 and $\deg p = \deg q = d$, the claim implies that $(X + p(Y), Y) \sim (X + q(Y), Y)$. Therefore, in this case, $\mathcal{G}_{(d)}$ is a double coset modulo \mathcal{A} .

If $d \geq 4$, let us set $p(Y) = Y^d$ and $q(Y) = Y^d + Y^{d-1}$. There does not exist any $\alpha, \beta, \gamma \in \mathbb{C}$ such that $q''(Y) = \alpha p''(\beta Y + \gamma)$, because the polynomial $p''(\beta Y + \gamma)$ has a unique root and this is not the case of the polynomial q''(Y). By the claim, it follows that the automorphisms (X + p(Y), Y) and (X + q(Y), Y) have distinct double coset modulo \mathcal{A} . In particular, $\mathcal{G}_{(d)}$ is not a double coset modulo \mathcal{A} . \Box

Let us now prove Th. D.

If \mathcal{H} is a subgroup of \mathcal{G} as in Th. D, let us show that $\mathcal{H} = \mathcal{G}$. By the hypothesis, \mathcal{H} contains a triangular automorphism f = (X + p(Y), Y) with deg $p \ge 2$. If we set $g_{\alpha} := (X, Y + \alpha) \in \mathcal{H} \ (\alpha \in \mathbb{C})$, then the commutator $[f, g_{\alpha}] := f \circ g_{\alpha} \circ f^{-1} \circ g_{\alpha}^{-1} \in \mathcal{H}$ is equal to (X + q(Y), Y), where $q(Y) := p(Y) - p(Y - \alpha)$. If α is well chosen, one may assume that deg $q = \deg p - 1$. Therefore, by a decreasing induction, we see that \mathcal{H} contains a triangular automorphism of degree 2.

Since $\mathcal{G}_{(2)}$ is a double coset modulo \mathcal{A} by Lemma 24, we get $\mathcal{G}_{(2)} \subseteq \mathcal{H}$. By induction, we get $\mathcal{G}_{(d)} \subseteq \mathcal{H}$ for any $d \geq 2$. Indeed, if $\mathcal{G}_{(d)} \subseteq \mathcal{H}$, we get $\mathcal{G}_{(d,2)} \subseteq \mathcal{H}$, so that $\overline{\mathcal{G}}_{(d,2)} \subseteq \overline{\mathcal{H}} = \mathcal{H}$ and $\mathcal{G}_{(d+1)} \subseteq \overline{\mathcal{G}}_{(d,2)}$ by Th. C. Since \mathcal{H} contains all $\mathcal{G}_{(d)}$, $d \geq 2$, it is now clear that $\mathcal{H} = \mathcal{G}$.

Acknowledgements. I would like to thank Michel Brion and Laurent Manivel for their generous help.

References

- [AM75] S.S. Abhyankar, T.T. Moh, Embeddings of the line in the plane, J. Reine Angew. Math., 276 (1975), 148-166.
- [BCW82] H. Bass, E. Connell, D. Wright, The Jacobian conjecture: reduction of degree and formal expansion of the inverse, Bull. of the A.M.S., 7 (1982), 287-330.
- [Bou07] N. Bourbaki, Éléments de mathématique. Algèbre commutative. Chapitre 10. (French) [Elements of mathematics. Commutative algebra. Chapter 10] Reprint of the 1998 original. Springer-Verlag, Berlin, 187 pp, ISBN: 978-3-540-34394-3, 2007.
- [EF04] E. Edo, J.-P. Furter, Some families of polynomial automorphisms, J. of Pure and Applied Algebra 194 (2004), 263-271.
- [Ess00] A. van den Essen, Polynomial automorphisms and the Jacobian conjecture, Progress in Mathematics 190, Birkhäuser Verlag, Basel, 329 pp., ISBN: 3-7643-6350-9, 2000.
- [FM89] S. Friedland, J. Milnor, Dynamical properties of plane polynomial automorphisms, Ergod. Th & Dyn. Syst. 9 (1989), 67-99.
- [Fur97] J.-P. Furter, On the variety of automorphisms of the affine plane, J. Algebra 195 (1997), 604-623.
- [Fur02] J.-P. Furter, On the length of automorphisms of the affine plane, Math. Ann. 322 (2002), 401-411.
- [Fur07] J.-P. Furter, Jet groups, J. Algebra 315 (2007), no. 2, 720-737.
- [Fur09] J.-P. Furter, Plane polynomial automorphisms of fixed multidegree, Math. Ann. 343 (2009), 901-920.
- [FM10] J.-P. Furter, S. Maubach, A characterization of semisimple plane polynomial automorphisms, J. of Pure and Appl. Algebra 214 (2010), no 5, 574-583.
- [GD75] M. H. Gizatullin, V. I. Danilov, Automorphisms of affine surfaces I (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 39 (1975), no. 3, 523-565, 703.
- [Gro61a] A. Grothendieck, Éléments de géométrie algébrique II, Étude globale élémentaire de quelques classes de morphismes, Inst. Hautes Études Sci. Publ. Math. No. 8, 222 pp, 1961.
- [Gro61b] A. Grothendieck, Éléments de géométrie algébrique III, Étude cohomologique des faisceaux cohérents I, Inst. Hautes Études Sci. Publ. Math. No. 11, 167 pp, 1961.
- [Gro65] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II. (French) Inst. Hautes Études Sci. Publ. Math. No. 24, 231 pp, 1965.

- [Har77] R. Hartshorne, Algebraic geometry, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977.
- [Hur1891] A. Hurwitz, Über die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche, Math. Ann. 46 (1891), 279-284.
- [Jun42] H. W. E. Jung, Über ganze birationale Transformationen der Ebene, J. Reine Angew. Math. 184 (1942), 161-174.
- [KL98] J.-P. Kahane, P.-G. Lemarié-Rieusset, Séries de Fourier et ondelettes, Cassini, ISBN: 2-84225-001-X, 1998
- [Kam79] T. Kambayashi, Automorphism group of a polynomial ring and algebraic group action on an affine space, J. Algebra 60 (1979), no. 2, 439-451.
- [Kul53] W. van der Kulk, On polynomial rings in two variables, Nieuw. Arch. Wisk. (3) 1 (1953), 33-41.
- [Lio1844a] J. Liouville, Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques, C.R. Acad. Sci. Paris, 18 (1844), 883-885.
- [Lio1844b] J. Liouville, Nouvelle démonstration d'un théorème sur les irrationnelles algébriques inséré dans le compte rendu de la dernière séance, C.R. Acad. Sci. Paris, 18 (1844), 910-911.
- [Mal99] S. Mallat, A wavelet tour of signal processing, 2nd edition. Academic Press, Inc., San Diego, CA, 1999.
- [MFK94] D. Mumford, J. Fogarty, F. Kirwan, Geometric invariant theory. Third edition. Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], 34. Springer-Verlag, Berlin, 1994.
- [Mur67] J. P. Murre, Lectures on an introduction to Grothendieck's theory of the fundamental group, Notes by S. Anantharaman, Tata Institute of Fundamental Research Lectures on Mathematics No 40, Tata Institute of Fundamental Research, Bombay, 176 pp, 1967.
- [Nag72] M. Nagata, On automorphism group of k[x,y], Lecture Notes in Math., Kyoto Univ., 5, (1972).
- [Rit22] J. F. Ritt, Prime and composite polynomials. Trans. Amer. Math. Soc. 23 (1922), no. 1, 51-66.
- [Rot55] K. F. Roth, Rational approximations to algebraic numbers, Mathematika 2 (1955), 1-20; corrigendum, 168.
- [Rui93] J. M. Ruiz, The basic theory of power series. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1993.
- [Sha66] I. R. Shafarevich, On some infinite-dimensional groups, Rend. Mat. e Appl. (5) 25 (1966), no. 1-2, 208-212.
- [Sha82] I. R. Shafarevich, On some infinite-dimensional groups II, Math. USSR Izv., 18 (1982), 214-226.
- [Sta96] R. P. Stanley, Combinatorics and commutative algebra, Second edition, Progress in Mathematics 41, Birkäuser Boston, Inc., Boston, MA, 164 pp, ISBN 0-8176-3836-9, 1996.
- [Suz74] M. Suzuki, Propriétés topologiques des polynômes de deux variables complexes et automorphismes algébriques de l'espace C², J. Math. Soc. Japan. 26 (1974), 241-257.
- [Wey31] H. Weyl, The theory of groups and quantum mechanics. Dutton, New York, 1931.
- [Wri79] D. Wright, Abelian subgroups of $\operatorname{Aut}_k(k[X,Y])$ and applications to actions on the affine plane, Illinois J. Math., 23.4 (1979), 579-634.