Locally Finite Polynomial Endomorphisms

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

Stefan MAUBACH.
Dpt. of Math., Radboud University Nijmegen (RUN),
postbus 9010, 6500 GL Nijmegen, THE NETHERLANDS
email: s.maubach@science.ru.nl

Abstract.

We study polynomial endomorphisms F of $\mathbb{C}^N$ which are locally finite in the following sense: the vector space generated by $r \circ F^n$ $(n \geq 0)$ is finite dimensional for each $r \in \mathbb{C}[x_1, \ldots, x_N]$. We show that such endomorphisms exhibit features similar to linear endomorphisms: they satisfy the Jacobian Conjecture, have vanishing polynomials, admit suitably defined minimal and characteristic polynomials, and the invertible ones admit a Dunford decomposition into "semisimple" and "unipotent" constituents. We also explain a relationship with linear recurrent sequences and derivations. Finally, we give particular attention to the special cases where F is nilpotent and where $N = 2$.

Keywords.

Polynomial automorphisms, affine algebraic geometry, derivations.

INTRODUCTION.

This paper is devoted to the study of polynomial endomorphisms F of $\mathbb{C}^N$ satisfying the following equivalent conditions (see Theorem 1.1 for details):

(i) $\dim \underset{n\geq 0}{Span}\ F^n < +\infty$;

(ii) $\sup_{n\geq 0} \deg F^n < +\infty$;

(iii) $\dim \underset{n\geq 0}{Span}\ r\circ F^n < +\infty$ for each $r\in\mathbb{C}[x_1,\ldots,x_N]$.

Such a polynomial endomorphism is called *locally finite* (LF for short) since condition (ii) exactly means that the *linear* endomorphism $r\mapsto r\circ F$ is locally finite in a more familiar sense (see [10] and Definition 1.2 below). The most intuitive way of understanding a LF polynomial endomorphism is probably via condition (i) which says that such an endomorphism is characterized by the requirement that it satisfy a relation of the kind $p(F)=0$ where $p\in\mathbb{C}[T]$ is non-zero. Our motivation for studying these endomorphisms stems from the Jacobian Conjecture. This conjecture generalizes the classical result saying that a finite-dimensional linear endomorphism is invertible if and only if its determinant is non-zero. For linear endomorphisms, the determinant amounts to the last coefficient of the characteristic polynomial. Furthermore, by the Cayley-Hamilton theorem, the characteristic polynomial of a linear endomorphism, when evaluated at the endomorphism itself, vanishes. These observations raise the question whether and how this kind of relationship extends to polynomial endomorphisms.

It should be pointed out immediately that many (heuristically "almost all") polynomial endomorphisms are *not* LF, though. Indeed, it is worth noting that a LF endomorphism is necessarily dynamically trivial in the sense that its dynamical degree $dd(F):=\lim_{n\to\infty}(\deg F^n)^{\frac{1}{n}}$ is equal to one; for an automorphism, this is equivalent to requiring that the topological entropy be zero, see [11] and [30]. Nevertheless, surprisingly many polynomial endomorphisms are LF:

1. Affine endomorphisms are LF.

2. Triangular and elementary maps are LF. We recall that an elementary map is one of the kind $(x_1,\ldots,x_{L-1},x_L+p,x_{L+1},\ldots,x_N)$, where $p\in\mathbb{C}[x_1,\ldots,\widehat{x_L},\ldots,x_N]$.

3. The Nagata automorphism $F:=(x-2yw-zw^2,y+zw,z)\in Aut(\mathbb{C}^3)$ where $w=xz+y^2$ is LF. Indeed, this automorphism is a root of the polynomial $p(T)=(T-1)^3$. This observation means that $F^3-3F^2+3F-I=0$, which is not the same as requiring that $(F-I)^3=0$ (since F is not linear!).

4. In [4], de Bondt has recently used so-called quasi-translations as the main tool to obtain strong new results. Such a quasi-translation is defined to be a map of the kind $I+H$ whose inverse is $I-H$. It is not very difficult to check that F is a quasi-translation if and only if F is a root of the polynomial $(T-1)^2$.

5. Every automorphism of finite order (i.e. a map satisfying $F^k=I$ for some $k\geq 1$) is LF. However, it is still unknown whether or not such maps are linear up to conjugation.

6. When D is a locally finite derivation (including the locally nilpotent case), then $\exp D$ is a LF automorphism (see II.2). Thus the question arises whether the converse is true, that is, whether any LF automorphism is the exponential of a LF derivation.

7. Nilpotent endomorphisms are LF.

So, even though "very few" endomorphisms are LF, they constitute an important subclass, and the purpose of the present paper is to begin exploring LF endomorphisms systematically. Up to now, little work seems to have been undertaken in this direction. For example, only recently has it been proved that the Nagata automorphism is not tame (see [27] and [28]). This result shows that LF and dynamically trivial endomorphisms are not trivial. At the present stage, the search for generators of the automorphism group is wide open. In [10], van den Essen asked whether the automorphism group is generated by exponentials of locally nilpotent derivations. Less ambitiously, we may ask whether this group is generated by LF automorphisms.

The paper is divided into four sections. In section I, we define the minimal polynomial (Definition 1.1), prove an extension of the Cayley-Hamilton theorem (Theorem 1.2) and relate the theory of LF polynomial endomorphisms to the theory of linear recurrent sequences (Proposition 1.3). In section II, we study the case of automorphisms. We give a Dunford decomposition (Theorem 2.1) and explain some (possible) connections with LF derivations. In section III, we show that when F is a nilpotent polynomial endomorphism of $\mathbb{C}^N$, then $F^N = 0$ (Theorem 3.1). In section IV, we explore the special case where the dimension is two. In this case, the amalgamated structure of the automorphism group provides considerable simplification. Given a LF polynomial endomorphism F of $\mathbb{C}^2$ satisfying $F(0) = 0$, we define an explicit vanishing polynomial of degree $\dfrac{d(d+3)}{2}$ where $d = \deg F$, and we show that the minimal polynomial of F has degree at most $d + 1$.

I. GENERALITIES.

1. LF ENDOMORPHISMS.

We denote by $\mathbb{A}^N = \mathbb{C}^N$ the complex affine space of dimension N and by $End = End(\mathbb{A}^N)$ the set of polynomial endomorphisms of $\mathbb{A}^N$. As usual, we identify an element F of End with the N-uple of its coordinate functions $F = (F_1, \ldots, F_N)$ where each F_L belongs to the ring $\mathbb{C}[X] := \mathbb{C}[x_1, \ldots, x_N]$ of regular functions on $\mathbb{A}^N$. We set $\deg F = \max_{1 \le L \le N} \deg F_L$. We denote by $F^{\#} : \mathbb{C}[X] \to \mathbb{C}[X]$, $r \mapsto r \circ F$, the $\mathbb{C}$-algebra morphism associated with F. To simplify the notation, we use the indeterminates x, y, z instead of the x_L when $N \le 3$.

We recall that a (complex) near-algebra A is a linear space on which a composition is defined such that (i) A forms a semigroup under composition; (ii) composition is right distributive with respect to addition (i.e. $(a+b) \circ c = a \circ c + b \circ c$ for all $a, b, c \in A$); (iii) $\lambda(a \circ b) = (\lambda a) \circ b$ for all $a, b \in A$ and $\lambda \in \mathbb{C}$. If $a \in A$, we set $\mathcal{I}_a := \{p \in \mathbb{C}[T],\ p(a) = 0\}$. Since $\mathcal{I}_a$ is a vector subspace of $\mathbb{C}[T]$ which is closed under multiplication by T, it is clear that $\mathcal{I}_a$ is an ideal of $\mathbb{C}[T]$.

Example 1.1. When l belongs to the algebra $\mathcal{L}(V)$ of linear endomorphisms of a vector space V, it is well known that $\mathcal{I}_l$ is an ideal of $\mathbb{C}[T]$. When W is a subspace which is closed under l and if $l_{||W} \in \mathcal{L}(W)$ denotes the induced endomorphism, let us note that $\mathcal{I}_l \subset \mathcal{I}_{l_{||W}}$.

Example 1.2. When F belongs to the near-algebra $End(\mathbb{A}^N)$, $\mathcal{I}_F$ is an ideal of $\mathbb{C}[T]$, but since $F^\# \in \mathcal{L}(\mathbb{C}[X])$, $\mathcal{I}_{F^\#}$ is also an ideal of $\mathbb{C}[T]$. In general we do not have $\mathcal{I}_F = \mathcal{I}_{F^\#}$ (see Theorem 2.2), but only $\mathcal{I}_{F^\#} \subset \mathcal{I}_{(F^\#)_{||W}} = \mathcal{I}_F$, where

$$W = \text{Span}\left((F^\#)^n(x_L)\right)_{n\in\mathbb{N},\ 1\le L\le N.}$$

Indeed, $p(F) = 0 \iff \forall\, L,\ x_L \circ p(F) = 0$, i.e. $p(F^\#)\,(x_L) = 0 \iff W \subset \text{Ker }p(F^\#)$.

Definition 1.1. When a belongs to a near-algebra A and if $\mathcal{I}_a \neq 0$, we define the minimal polynomial μ_a of a as the (unique) monic polynomial generating the ideal $\mathcal{I}_a$.

We now recall a few things on LF linear endomorphisms. When l is a linear endomorphism of a vector space V, let us denote by $\mathcal{F}(l)$ the set of finite dimensional subspaces W of V such that $l(W) \subset W$.

Definition 1.2. A linear endomorphism l is LF if it satisfies the following equivalent assertions (see [10]): (i) $\dim \underset{n\ge 0}{Span}\ l^n(v) < +\infty$ for each $v \in V$; (ii) $V = \bigcup_{W\in\mathcal{F}(l)} W$; (iii) any finite dimensional subspace of V is included into some $W \in \mathcal{F}(l)$.

In other words: l is LF if it is an (inductive) limit of finite dimensional linear endomorphisms. Indeed, it is uniquely determined by $l_{||W}$, $W \in \mathcal{F}(l)$. Therefore, most definitions made in the finite dimensional case extend to the LF case (see [10]):

Definition 1.3. A LF endomorphism l is *semisimple* when $l_{||W}$ is semisimple for each $W \in \mathcal{F}(l)$; it is *unipotent* when $l_{||W}$ unipotent for each $W \in \mathcal{F}(l)$; and it is *locally nilpotent* when $l_{||W}$ is nilpotent for each $W \in \mathcal{F}(l)$.

By applying the additive Jordan decomposition to each $l_{||W}$, we obtain the additive Jordan decomposition for l: there exist unique LF endomorphisms l_s, l_n such that:
(i) $l = l_s + l_n$ with $l_s \circ l_n = l_n \circ l_s$; (ii) l_s is semisimple ; (iii) l_n is locally nilpotent.
In the same way, we obtain the multiplicative Jordan decomposition (or Dunford decomposition) in the invertible case: there exist unique LF endomorphisms l_s, l_u such that: (i) $l = l_s \circ l_u = l_u \circ l_s$; (ii) l_s is semisimple ; (iii) l_u is unipotent.

Theorem 1.1. Let $F \in End$. The three following assertions are equivalent:
(i) $\mathcal{I}_F \neq \{0\}$; (ii) $\sup_{n\ge 0} \deg F^n < +\infty$; (iii) $F^\#$ is LF.

Proof. (i) $\Longrightarrow$ (ii). If $F^d = a_{d-1}F^{d-1} + \ldots + a_0F^0$, an easy induction would show that $F^n \in \text{Span}(F^0, \ldots, F^{d-1})$ (for each $n \ge 0$), so that $\deg F^n \le C := \max_{0\le k\le d-1} \deg F^k$.
(ii) $\Longrightarrow$ (iii). If $r \in \mathbb{C}[X]$ and $\deg F^n \le C$ for any n, then $\deg r \circ F^n \le \deg r \times C$, so that $\dim \underset{n\ge 0}{Span}\ r \circ F^n < +\infty$.
(iii) $\Longrightarrow$ (i). If W is as in Example 1.2, then $\dim W < +\infty$, so that $\mathcal{I}_{(F^\#)_{||W}} \neq \{0\}$. $\square$

Definition 1.4. A polynomial endomorphism F satisfying (i)-(iii) of Theorem 1.1. is said to be LF.

As in the linear case, the following result holds.

Proposition 1.1. When $F \in End$ is LF, the five following assertions are equivalent:
(i) F is an automorphism; (ii) F is injective; (iii) F is surjective;
(iv) $\mu_F(0) \neq 0$; (v) Jac $F \neq 0$ (where Jac F is the Jacobian determinant of F).

Proof. (i) and (ii) are equivalent even if F is not LF (see Proposition 17.9.6 p. 80 in [15] for the original idea, but the precise result is proved in [2], [5], [3], [8] and [24]). (i) $\Longrightarrow$ (iii) and (i) $\Longrightarrow$ (v) are obvious. Let us prove (iii) $\Longrightarrow$ (iv) $\Longrightarrow$ (ii) and (v) $\Longrightarrow$ (i).
(iii) $\Longrightarrow$ (iv). If we had $\mu_F(0) = 0$, then $p(T) := \mu_F(T)\,T^{-1} \in \mathbb{C}[T]$ and $p(F) \circ F = 0$. Since F is onto, this would imply $p(F) = 0$ contradicting the definition of μ_F.
(iv) $\Longrightarrow$ (ii). If $\mu_F(0) \neq 0$, there exists $p \in \mathbb{C}[T]$ such that $p(T)T \equiv 1 \bmod \mu_F(T)$, so that $p(F) \circ F = I$ and F is injective.
(v) $\Longrightarrow$ (i). If F is not an automorphism, we have $\mu_F(0) = 0$ and we have seen that $p(F) \circ F = 0$ where $p(T) := \mu_F(T)\,T^{-1} \in \mathbb{C}[T]$. Since $p(F) \neq 0$ (by definition of μ_F), there exists some non-zero component $r \in \mathbb{C}[X]$ of the endomorphism $p(F)$. We have $r(F_1, \ldots, F_N) = 0$, which shows that $F_1, \ldots, F_N$ are algebraically dependant over $\mathbb{C}$. This last condition is equivalent to Jac $F = 0$ (see [23] and [14]). □

Corollary 1.1. When F is LF, then Jac F is a constant.

Corollary 1.2. When F is LF, then the Jacobian conjecture holds for F, i.e. F is an automorphism if and only if Jac F is a non-zero constant.

2. THE CHARACTERISTIC POLYNOMIAL.

When F is a finite dimensional linear endomorphism, the Cayley-Hamilton theorem shows us that $\chi_F(F) = 0$ where χ_F is the (classical) characteristic polynomial of F. We note that this characteristic polynomial χ_F is given by a closed formula. When F is a LF polynomial endomorphism, we would like to find a closed formula giving a polynomial χ_F such that $\chi_F(F) = 0$. The next result gives us a partial answer since it allows us to find a vanishing polynomial of F depending only on the linear part $\mathcal{L}(F)$ of F and on $\sup_{n\in\mathbb{N}} \deg F^n$. However, there remains the problem of computing $\sup_{n\in\mathbb{N}} \deg F^n$.

Theorem 1.2. Let $F \in End(\mathbb{A}^N)$ be such that $F(0) = 0$ and $d := \sup_{n\in\mathbb{N}} \deg F^n < +\infty$, let $(\lambda_L)_{1\leq L\leq N}$ denote the eigenvalues of $\mathcal{L}(F)$ and, for $\alpha = (\alpha_L)_L \in \mathbb{N}^N$, let $\lambda^\alpha := \prod_L \lambda_L^{\alpha_L}$ and $|\alpha| := \sum_L \alpha_L$. Then $\prod_{\substack{\alpha\in\mathbb{N}^N \\ 0<|\alpha|\leq d}} (T - \lambda^\alpha)$ is a vanishing polynomial of F.

Our proof will use the next two lemmata. We recall a few facts about symmetric powers (for more details, see chap. 3, § 6 in [6], app. 2 in [9] or any book dealing with multilinear algebra). When E is a vector space with basis $e_1, \ldots, e_N$, the k-th symmetric power of E, denoted by $\mathrm{Sym}^k E$, is naturally isomorphic to the vector space whose elements are the k-homogeneous polynomials in the indeterminates $e_1, \ldots, e_N$. Since any element of E can be thought of as a 1-homogeneous polynomial in the indeterminates $e_1, \ldots, e_N$, we have $E \simeq \mathrm{Sym}^1 E$. In the same way, $a_1 \ldots a_k$ can be seen as an element of $\mathrm{Sym}^k E$ where all a_L belong to E. Finally, when $u : E \to F$ is a linear map, $\mathrm{Sym}^k u : \mathrm{Sym}^k E \to \mathrm{Sym}^k F$ is the unique linear map sending $a_1 \ldots a_k \in \mathrm{Sym}^k E$ to $u(a_1) \ldots u(a_k) \in \mathrm{Sym}^k F$.

Lemma 1.1. Let E be a finite dimensional complex vector space and let $u \in \mathcal{L}(E)$. Given the characteristic polynomial $\chi(u, E) = \prod_{1 \le L \le N} (T - \lambda_L)$ of u, the characteristic polynomial of the k-th symmetric power $\mathrm{Sym}^k u \in \mathcal{L}(\mathrm{Sym}^k E)$ is the polynomial

$$\chi(\mathrm{Sym}^k u, \mathrm{Sym}^k E) = \prod_{\substack{\alpha \in \mathbb{N}^N \\ |\alpha| = k}} (T - \lambda^\alpha).$$

Proof. It is a classical result. Let us prove it anyway for the sake of completeness. Let $(e_1, \ldots, e_N)$ be a basis of E such that the matrix of u in this basis is an upper triangular matrix $\begin{bmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_N \end{bmatrix}$, i.e. $\forall\, L,\ u(e_L) - \lambda_L e_L \in \mathrm{Span}(e_M)_{M<L}$.

For $\alpha = (\alpha_1, \ldots, \alpha_N) \in \mathbb{N}^N$, let us set $e^\alpha := e_1^{\alpha_1} \ldots e_N^{\alpha_N} \in \mathrm{Sym}^{|\alpha|} E$. Let $M := \{e^\alpha,\ \alpha \in \mathbb{N}^N\}$ be the set of all monomials in $e_1, \ldots, e_N$ and let us endow M with any monomial order $\prec$ such that $e_1 \prec e_2 \prec \ldots \prec e_N$ (we say that $\prec$ is a monomial order if $m_1 \prec m_2$ implies $m_1 \prec m m_1 \prec m m_2$ for any $m, m_1, m_2 \in M$ with $m \neq 1$, see [9]). We can for example take the orders $\prec_1$ or $\prec_2$ defined by

$e^\alpha \prec_1 e^\beta \Longleftrightarrow \alpha_L < \beta_L$ for the last integer L such that $\alpha_L \neq \beta_L$ and

$e^\alpha \prec_2 e^\beta \Longleftrightarrow \alpha_L > \beta_L$ for the first integer L such that $\alpha_L \neq \beta_L$

where $\alpha = (\alpha_1, \ldots, \alpha_N),\ \beta = (\beta_1, \ldots, \beta_N) \in \mathbb{N}^N$.

It is well known that $M_k := \{e^\alpha, |\alpha| = k\}$ is a basis of $\mathrm{Sym}^k E$. Furthermore, since $\prec$ is a monomial order: $\forall\, e^\alpha \in M_k,\ \mathrm{Sym}^k u(e^\alpha) - \lambda^\alpha e^\alpha \in \mathrm{Span}(e^\beta)_{e^\beta \in M_k}$ and $e^\beta \prec e^\alpha$.

The matrix of $\mathrm{Sym}^k u$ in the basis e^α where the e^α are taken with the order $\prec$ is upper triangular with the λ^α on the diagonal. □

We will omit the proof of the following familiar result.

Lemma 1.2. Let E be a finite dimensional complex vector space and let $u \in \mathcal{L}(E)$ be a linear endomorphism of E. We assume that $E = E_1 \supset E_2 \supset \ldots \supset E_d \supset E_{d+1} = \{0\}$ is a filtration of E by subspaces which are closed under u (i.e. $u(E_k) \subset E_k$). When $\chi(u, E)$ denotes the characteristic polynomial of u and if $\chi(u, E_k/E_{k+1})$ denotes the characteristic polynomial of the endomorphism induced by u on E_k/E_{k+1}, then

$$\chi(u, E) = \prod_{1 \le k \le d} \chi(u, E_k/E_{k+1}).$$

Proof of Theorem 1.2. If W is defined as in Example 1.2, then $W \in \mathcal{F}(F^{\#})$ and $\chi(F^{\#}, W)$ is a vanishing polynomial of F. Let $\mathcal{M}$ be the maximal ideal of $\mathbb{C}[X]$ generated by $x_1, \ldots, x_N$. Since $F(0) = 0$, we have $F^{\#}(\mathcal{M}) \subset \mathcal{M}$, so that $F^{\#}(\mathcal{M}^k) \subset \mathcal{M}^k$ (for $k \geq 0$). If we set $W_k := W \cap \mathcal{M}^k$ (for $1 \leq k \leq d+1$), then W_k is closed under $F^{\#}$ and we have the filtration: $W = W_1 \supset W_2 \supset \ldots \supset W_d \supset W_{d+1} = \{0\}$. By Lemma 1.2, we have $\chi(F^{\#}, W) = \prod_{1 \leq k \leq d} \chi(F^{\#}, W_k/W_{k+1})$. But, there is a natural embedding of $W_k/W_{k+1} = W \cap \mathcal{M}^k \ / \ W \cap \mathcal{M}^{k+1}$ in $\mathcal{M}^k/\mathcal{M}^{k+1}$, so that $\chi(F^{\#}, W_k/W_{k+1})$ divides $\chi(F^{\#}, \mathcal{M}^k/\mathcal{M}^{k+1})$. We denote by $u_k \in \mathcal{L}(\mathcal{M}^k/\mathcal{M}^{k+1})$ the linear endomorphism induced by $F^{\#}$ on $\mathcal{M}^k/\mathcal{M}^{k+1}$. If $k = 1$, $\mathcal{M}/\mathcal{M}^2$ is classically called the cotangent space at the origin of the affine space $\mathbb{A}^N$. The dual map of u_1 is naturally identified to the differential at the origin of the map $F : \mathbb{A}^N \to \mathbb{A}^N$, which is itself identified to the linear part $\mathcal{L}(F)$ of F, so that $\chi(F^{\#}, \mathcal{M}/\mathcal{M}^2) = \prod_{1 \leq L \leq N} (T - \lambda_L)$. If $k \geq 1$ is any integer, $\mathcal{M}^k/\mathcal{M}^{k+1}$ is naturally isomorphic to $\mathrm{Sym}^k\left(\mathcal{M}/\mathcal{M}^2\right)$ and u_k is naturally identified to $\mathrm{Sym}^k u_1$. Therefore, by Lemma 1.1, we have $\chi(F^{\#}, \mathcal{M}^k/\mathcal{M}^{k+1}) = \prod_{\substack{\alpha \in \mathbb{N}^N \\ |\alpha| = k}} (T - \lambda^\alpha)$. □

3. LINEAR RECURRENT SEQUENCES.

We now introduce the language of linear recurrent sequences (LRS for short), because they are a nice tool for some proofs (see section IV). Let V be any complex vector space. The set of sequences $u : \mathbb{N} \to V$ will be denoted by $V^{\mathbb{N}}$. For $p = p(T) = \sum_k p_k \, T^k \in \mathbb{C}[T]$, we define $p(u) \in V^{\mathbb{N}}$ by the formula

$$\forall \ n \in \mathbb{N}, \ \big(p(u)\big)\,(n) = \sum_k p_k \ u(n+k).$$

The theory of LRS relies on the next result (see [7]).

Proposition 1.2. Let $u = u(n)_{n \in \mathbb{N}} \in V^{\mathbb{N}}$ and let p be a non-zero polynomial of $\mathbb{C}[T]$. When $p(T) = \alpha \prod_{1 \leq k \leq c} (T - \omega_k)^{r_k}$ is the decomposition into irreducible factors of p, then the two following assertions are equivalent: (i) $p(u) = 0$; (ii) there exist $q_1, \ldots, q_c \in V[T]$ with deg $q_k \leq r_k - 1$ such that $\forall \ n, \ u(n) = \sum_{1 \leq k \leq c} \omega_k^n q_k(n)$ (*).

Remarks. 1. The vector space $V[T]$ is the set of polynomials in T with coefficients in V alias the set of "polynomial" maps from $\mathbb{C}$ to V.

2. The expression (*) is called an exponential-polynomial. We say that u is polynomial when $c = 1$ and $\omega_1 = 1$. We say that u of exponential type when all the q_k's are constant.

3. In the case where u is of exponential-type, we will sometimes be more precise and say that u is of Ω-exponential type, where $\Omega := \{\omega_1, \ldots, \omega_c\}$. When u is a complex se-

quence of Ω-exponential type, then $u+v$ is obviously of $\Omega\cup\Omega'$-exponential type; likewise, when u' is a complex sequence of Ω'-exponential type, then uv is of $\Omega.\Omega'$-exponential type. In particular, when $u_1, \dots, u_e$ are of Ω exponential type, then $u_1 u_2 \dots u_e$ is of Ω^e-exponential type, where $\Omega^e = \underbrace{\Omega.\Omega.\dots.\Omega}_{e}$. Therefore, when u_1, u_2 are of Ω-exponential type and when $q(x,y) \in \mathbb{C}[x,y]$ is such that $q(0,0)=0$ and $\deg q \ \le e$, then the sequence $q(u_1,u_2)$ is of $\bigcup_{1\le k\le e} \Omega^k$-exponential type.

Using Proposition 1.2, it is clear that if $u \in V^{\mathbb{N}}$, then $\mathcal{I}_u := \{p \in \mathbb{C}[T],\ p(u)=0\}$ is an ideal of $\mathbb{C}[T]$.

Definition 1.5. We say that $u \in V^{\mathbb{N}}$ is a LRS if $\mathcal{I}_u \neq \{0\}$. In this case, we define the minimal polynomial of u as the (unique) monic polynomial μ_u generating the ideal $\mathcal{I}_u$.

Remarks. 1. The LRS are classically complex sequences, but we found it convenient to extend their definition to the case of vector spaces.

2. A LRS is polynomial if and only if its minimal polynomial is of the kind $(T-1)^m$; it is of exponential type if and only if its minimal polynomial has only single roots.

3. Let E be a finite dimensional vector space and let $F \in \mathcal{L}(E)$ be a linear endomorphism of E. It is a classical fact that F is unipotent if and only if the sequence $(F^n)_{n\in\mathbb{N}}$ is polynomial and, likewise, F is semisimple if and only if the sequence $(F^n)_{n\in\mathbb{N}}$ is of exponential type. We will later on generalize this definition to the case of LF polynomial endomorphisms.

Proposition 1.3. For $F \in End$ and $u := (F^n)_{n\in\mathbb{N}} \in End^{\mathbb{N}}$, we have $\mathcal{I}_F = \mathcal{I}_u$. In particular, F is LF if and only if u is a LRS. If this is the case, we have $\mu_F = \mu_u$.

Proof. If $p = \sum_k p_k T^k \in \mathbb{C}[T]$, $\quad \sum_k p_k\ F^k = 0 \iff \forall\ n \in \mathbb{N},\ \sum_k p_k\ F^{k+n} = 0.$ □

Remark. When $F \in End$ is LF, then $(F^n(a))_{n\in\mathbb{N}}$ is a LRS for any $a \in \mathbb{A}^N$, but the converse is false: take $F = (xy, y) \in End(\mathbb{A}^2)$. When $\mathbb{C}(X) := \mathbb{C}(x_1, \dots, x_N)$ and $K := \{r \in \mathbb{C}(X),\ r \circ F = r\}$, it is shown in [13] that the following assertions are equivalent :

(i) $(F^n(a))_{n\in\mathbb{N}}$ is a LRS for any a; (ii) $p(F)=0$ for some non-zero $p \in K[T]$.

II. LF AUTOMORPHISMS.

1. DUNFORD DECOMPOSITION.

Proposition 2.1. When $F \in End$ is LF, the following assertions are equivalent:

(i) $F^{\#}$ is unipotent; (ii) $\mu_F = (T-1)^m$ for some $m \ge 0$;

(iii) the sequence $(F^n)_{n\in\mathbb{N}}$ is polynomial.

For $F(0)=0$, these assertions are still equivalent to the following one:

(iv) the linear map $\mathcal{L}(F)$ is unipotent.

Proof. (i) $\Longrightarrow$ (ii). Let W be as in Example 1.2. Since $F^{\#}_{||W}$ is unipotent, its characteristic polynomial is equal to $\chi(F^{\#}, W) = (T-1)^{\dim W}$ and it is a vanishing polynomial of F.

(ii) $\Longleftrightarrow$ (iii) is obvious from the theory of LRS.

(iii) $\Longrightarrow$ (i) Let $W \in \mathcal{F}(F^{\#})$. We want to show that $F^{\#}_{||W}$ is unipotent. But for all $w \in W$, the sequence $n \mapsto \left(F^{\#}\right)^n(w)$ is polynomial since $\left(F^{\#}\right)^n(w) = w \circ F^n$. This implies that the sequence $n \mapsto \left(F^{\#}_{||W}\right)^n$ is polynomial and this means that $F^{\#}_{||W}$ is unipotent (see rem. 3 following Definition 1.5).

We now assume that $F(0) = 0$.

(iii) $\Longrightarrow$ (iv). Since $F(0) = 0$, we have $\mathcal{L}(F^n) = \mathcal{L}(F)^n$ and since the sequence $(F^n)_{n\in\mathbb{N}}$ is polynomial, the sequence$(\mathcal{L}(F)^n)_{n\in\mathbb{N}}$ also, so that $\mathcal{L}(F)$ is unipotent.

(iv) $\Longrightarrow$ (ii). We know that the characteristic polynomial of $\mathcal{L}(F)$ is equal to $(T-1)^N$. Therefore, by Theorem 1.2, F admits a vanishing polynomial of the kind $(T-1)^p$. $\square$

Definition 2.1. When F satisfies (i)-(iii) of Proposition 2.1, we say that F is unipotent.

Example. When the Nagata automorphism is LF, it has to be unipotent by Proposition 2.1. It is indeed the case because one checks easily that its minimal polynomial is $(T-1)^3$.

When $F(0) \neq 0$, let us show by two examples that (i)-(iii) and (iv) are independant. We take $N = 2$. If $F = (F_1, F_2) \in End(\mathbb{A}^2)$ and $a \in \mathbb{A}^2$, $F'(a)$ will denote the Jacobian matrix of F at the point a. We will identify $\mathcal{L}(F)$ and $F'(0)$. We set $a := (1,1) \in \mathbb{A}^2$ and let us consider the group H of all automorphisms φ of $\mathbb{A}^2$ such that $\varphi(0) = 0$, $\varphi'(0) = I$ and $\varphi(a) = a$. If $\varphi \in H$, it is clear that $\varphi'(a) \in SL_2$ since $\det \varphi'(a) = \det \varphi'(0) = 1$. We show that the group-morphism $m : H \to SL_2$, $\varphi \mapsto \varphi'(a)$ is onto. If we set $\alpha_u := (x + uy^2(y-1), y)$ and $\beta_u := (x, y + ux^2(x-1)) \in H$ for each $u \in \mathbb{C}$, then $m(\alpha_u) = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$ and $m(\beta_u) = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$. Since SL_2 is generated by these matrices, we actually obtain $m(H) = SL_2$. If G is any automorphism of $\mathbb{A}^2$ such that $G(0) = a$ and if φ is any element of H, then $F := F_{(G,\varphi)} := \varphi^{-1} \circ G \circ \varphi$ satisfies $F'(0) = \varphi'(a)^{-1} G'(0) \varphi'(0) = \varphi'(a)^{-1} G'(0)$ and the equality $F^n = \varphi^{-1} \circ G^n \circ \varphi$ shows that F is unipotent if and only if G is unipotent.

First example. If $G := (x+1, y+1)$ and $\varphi \in H$, then $F := F_{(G,\varphi)}$ is unipotent and $F'(0) = \varphi'(a)^{-1}$. Therefore, if we choose φ such that $m(\varphi) = \varphi'(a)$ is not unipotent, then $\mathcal{L}(F) = F'(0)$ will not be unipotent. We can just take $\varphi := \alpha_1 \circ \beta_1$, because

$$\varphi'(a) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \text{ is not unipotent.}$$

Second example. If $G := (1-x, 1-y)$ and $\varphi \in H$, then $F := F_{(G,\varphi)}$ is not unipotent and $F'(0) = -\varphi'(a)^{-1}$. Therefore, if we choose φ such that $-m(\varphi) = -\varphi'(a)$ is unipotent, then $\mathcal{L}(F) = F'(0)$ will be unipotent. We can just take $\varphi := (\alpha_2 \circ \beta_{-1})^2$, because

$$\varphi'(a) = \left(\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \right)^2 = -I.$$

The next result is established in the same way as Proposition 2.1:

Proposition and definition 2.2. When F satisfies the following equivalent assertions, we say that F is semisimple: (i) $F^{\#}$ is semisimple; (ii) μ_F has single roots; (iii) the sequence $(F^n)_{n\in\mathbb{N}}$ is of exponential type.

Remark. When F is semisimple and $F(0) = 0$, one can show that $\mathcal{L}(F)$ is semisimple. The converse is false even if $F(0) = 0$ (take the Nagata automorphism).

We can now state the Dunford decomposition for LF polynomial automorphisms.

Theorem 2.1. Let F be a LF polynomial automorphism of $\mathbb{A}^N$, then there exist unique LF polynomial automorphisms F_s and F_u such that
(i) $F = F_s \circ F_u = F_u \circ F_s$; (ii) F_s is semisimple ; (iii) F_u is unipotent.

The proof is a direct consequence of the following result applied to $F^{\#}$:

Lemma 2.1. When l is a LF automorphism of a $\mathbb{C}$-algebra A, then its semisimple and unipotent parts (l_s and l_u) are algebra-morphisms.

Proof. Let $a, b \in A$. We want to show that $l_s(ab) = l_s(a)l_s(b)$ and $l_u(ab) = l_u(a)l_u(b)$. Let $W \in \mathcal{F}(l)$ be such that a, b and $ab \in W$. Let $H \subset GL(W)$ be the closed subgroup defined by $H := \{h \in GL(W),\ h(ab) = h(a)h(b)\}$. Since $l_{||W} \in H$, by the classical Dunford decomposition for linear algebraic groups (see [16]), we know that the semisimple and unipotent parts of $l_{||W}$ still belong to H. □

Lemma 2.2. When a unipotent automorphism F of $\mathbb{A}^N$ satisfies $\mathcal{I}_{F^{\#}} \neq \{0\}$, then $F = I$.

Proof. Let $r \in \mathbb{C}[X]$. Since the sequence $n \mapsto (F^{\#})^n(r)$ is polynomial, its minimal polynomial is of the kind $\mu_r = (T-1)^{m_r}$, where $m_r \geq 0$ is an integer.

However, since $I_{F^{\#}} \neq \{0\}$, the sequence $n \mapsto (F^{\#})^n$ is a LRS with minimal polynomial μ. The polynomial μ is the least common multiple of the μ_r ($r \in \mathbb{C}[X]$). This shows that $\mu = (T-1)^m$, where $m = \max\limits_r m_r$. We show by contradiction that $m = 1$. Otherwise, let $r \in \mathbb{C}[X]$ be such that $m_r = m \geq 2$. This means that the sequence $n \mapsto (F^{\#})^n(r)$ is polynomial of degree $m-1$. Therefore, the sequence $n \mapsto (F^{\#})^n(r^2)$ is polynomial of degree $2(m-1)$, showing that $m_{r^2} = 2m-1 > m$. This is impossible. □

Theorem 2.2. The only automorphisms F of $\mathbb{A}^N$ such that $\mathcal{I}_{F^{\#}} \neq \{0\}$ are the automorphisms of finite order.

Proof. When $F^k = I$, we clearly have $(F^{\#})^k = I$ and $T^k - 1 \in \mathcal{I}_{F^{\#}}$.

We now assume that F is an automorphism of $\mathbb{A}^N$ such that $\mathcal{I}_{F^{\#}} \neq \{0\}$. Let F_s be its semisimple and F_u its unipotent constituent. When l is a linear endomorphism, let $\mathcal{E}(l)$ be the set of its eigenvalues. Since $\mathcal{E}(F^{\#})$ is a finite subset of $\mathbb{C}^*$ (because $\mathcal{I}_{F^{\#}} \neq \{0\}$) which is closed under multiplication (because $F^{\#}$ is an algebra-morphism), it is a finite subgroup of $\mathbb{C}^*$, so that it is equal to some $U_k := \{z \in \mathbb{C},\ z^k = 1\}$. However,

$\mathcal{E}(F_s^{\#}) = \mathcal{E}(F^{\#})$, so that $(F_s)^k = I$. The automorphism $G := F^k = (F_u)^k$ is unipotent and satisfies $\mathcal{I}_{G\#} \neq \{0\}$. By Lemma 2.2, we have $G = I$. □

2. DERIVATIONS.

We begin by noting that the exponential of a LF linear endomorphism $l : V \to V$ is well defined by $(\exp\, l)_{||W} := \exp\; l_{||W}$, $W \in \mathcal{F}(l)$. We observe that $\exp l$ is LF.

Lemma 2.3 (i) the exponential defines a surjective map from the LF linear endomorphisms of V to the LF linear automorphisms of V;

(ii) the exponential defines a bijective map from the locally nilpotent linear endomorphisms to the LF unipotent automorphisms.

Proof. When V is finite-dimensional, the statement is well known. When V is not necessarily finite-dimensional, (ii) is a direct consequence of the finite dimensional case. The assertion (i) is more complicated. It is easy to show that the exponential of a LF endomorphism is an automorphism. We now prove that if l is a LF automorphism, then there exists a LF endomorphism m such that $\exp m \;=\; l$. Let $l = l_s \circ l_u$ be the Dunford decomposition of l.

For $\lambda \in \mathbb{C}$, the characteristic space N_λ of l is defined by $N_\lambda := \bigcup_{k \in \mathbb{N}} \mathrm{Ker}(l - \lambda\, I)^k$. Since l is a LF automorphism, it is easy to prove that $V \;=\; \bigoplus_{\lambda \in \mathbb{C}^*} N_\lambda$. Furthermore, it is well known that $l_{s||N_\lambda} = \lambda\; I_{N_\lambda}$. For each $\lambda \in \mathbb{C}^*$, let us choose $\ln\lambda \in \mathbb{C}$ such that $\exp(\ln\lambda) \;=\; \lambda$ (of course, the map $\ln : \mathbb{C}^* \to \mathbb{C}$ is not continuous !).

There exists a unique endomorphism $m_s \in \mathcal{L}(V)$ such that $m_{s||N_\lambda} \;=\; (\ln\lambda)\; I_{N_\lambda}$, $\lambda \in \mathbb{C}^*$. It is clear that m_s is a LF (semisimple) endomorphism such that $\exp m_s \;=\; l_s$. Also, since l_u is unipotent, by (ii), there exists a unique locally nilpotent endomorphism m_u such that $\exp m_u \;=\; l_u$.

Since $l = l_s \circ l_u = \exp m_s \circ \exp m_u$, in order to see that $l = \exp(m_s + m_u)$ it remains to show that m_s and m_u commute (in particular, if m_s and m_u commute, $m_s + m_u$ will still be LF !). But this is clear, because for each $\lambda \in \mathbb{C}^*$ we have $m_s(N_\lambda) \;\subset\; N_\lambda$, $m_u(N_\lambda) \;\subset\; N_\lambda$ and $m_{s||N_\lambda} = (\ln\lambda)\; I_{N_\lambda}$ so that $m_{s||N_\lambda}$ commutes with any endomorphism of N_λ ! □

We recall that a derivation of $\mathbb{C}[X]$ is an operator of the kind $D = \sum_{1 \le L \le N} a_L \dfrac{\partial}{\partial x_L}$ where the a_L belong to $\mathbb{C}[X]$ (see [10]). It turns out that if D is a LF derivation of $\mathbb{C}[X]$, then $\exp D$ is a LF algebra-automorphism of $\mathbb{C}[X]$. Therefore, there exists a LF polynomial automorphism F of $\mathbb{A}^N$ such that $F^{\#} = \exp D$. One often writes (improperly) $F = \exp D$ and we have of course $F = ((\exp D)(x_1), \ldots, (\exp D)(x_N))$.

If we assume furthermore that D is locally nilpotent, then we know that $F^{\#}$ is a LF unipotent linear automorphism, which means that F is unipotent. Conversely, if F (and therefore $F^{\#}$) is unipotent, we know that there exists a unique locally nilpotent linear endomorphism D of $\mathbb{C}[X]$ such that $\exp D = F^{\#}$. Moreover, D must be a derivation. Indeed, for any locally nilpotent linear endomorphism l of a $\mathbb{C}$-algebra A, the two following assertions are equivalent (see Exercise 6, p. 50 of [10]):

(i) $\exp l$ is an algebra-morphism ;   (ii) l is a derivation.

Hence, we have shown the following result.

Theorem 2.3. The exponential defines a bijective map from the locally nilpotent derivations of $\mathbb{C}[X]$ to the unipotent polynomial automorphisms of $\mathbb{A}^N$.

Example. Since the Nagata automorphism is unipotent (see the remark following Definition 2.1), it is the exponential of a locally nilpotent derivation (see [29]).

When F is any LF polynomial automorphism of $\mathbb{A}^N$, there still exists a LF linear endomorphism D such that $F^{\#} = \exp D$ (by Lemma 2.3), but D does not need to be a derivation ! However, there exist infinitely many D such that $F^{\#} = \exp D$ and one can ask our main question.

Question 2.1. Is any LF polynomial automorphism of $\mathbb{A}^N$ the exponential of a LF derivation of $\mathbb{C}[X]$?

We are not even able to answer the following.

Question 2.2. Is any semisimple polynomial automorphism of $\mathbb{A}^N$ the exponential of a semisimple derivation of $\mathbb{C}[X]$?

Remark. Of course, if l is a LF linear endomorphism, then l is semisimple if and only if $\exp l$ is semisimple (this is just the generalization of the corresponding fact in the finite dimensional case).

At this point, let us recall that a famous linearization conjecture asserts that if F is a finite order automorphism of $\mathbb{A}^N$ (i.e. $F^k = I$ for some non negative integer k), then F should be conjugate to some linear automorphism (i.e. there should exist an automorphism φ such that $\varphi \circ F \circ \varphi^{-1}$ is linear). This conjecture is still open for $N \geq 3$. Since the polynomial $T^k - 1$ has single roots, F is necessarily semisimple. One can generalize the linearization conjecture in the following manner.

Question 2.3. Is any semisimple polynomial automorphism of $\mathbb{A}^N$ linearizable ?

It had also been conjectured by Kambayashi in 1979 (see [18] or section 9.4 in [10]) that any (algebraic) action of a reductive algebraic group G on $\mathbb{A}^N$ is linearizable. However, Schwarz gave a counterexample in 1989 (see [25]) for $G = SL_2$ (and some other groups) and Knop gave counterexamples in 1991 (see [19]) when G is any non commutative connected reductive (algebraic) group. What happens if G is a commutative connected reductive group, i.e. $G = (\mathbb{C}^*)^p$ is a torus ? The next question (which seems very difficult) is still open.

Question 2.4. Is any action of a torus $(\mathbb{C}^*)^p$ on the affine space $\mathbb{A}^N$ linearizable ?

It has been pointed to us by Mathieu that a positive answer to question 2.3 would imply a positive answer to question 2.4. Indeed, if we are given an action of $G = (\mathbb{C}^*)^p$ on $\mathbb{A}^N$ and if we choose an element $g \in G$ such that the subgroup generated by g in G is Zariski dense, then the automorphism of $\mathbb{A}^N$ induced by g is semisimple. Therefore, it should be linearizable and the G-action also.

Finally, we can ask a question similar to question 2.3 at the level of derivations.

Question 2.5. Is any semisimple derivation of $\mathbb{C}[X]$ "linearizable" ?

In other words, is it conjugate to some $D = \sum_{1 \leq L \leq N} \lambda_L x_L \frac{\partial}{\partial x_L}$, $\lambda_L \in \mathbb{C}$?

We can express question 2.5 in the following way: does there exist an automorphism $F = (F_1, \ldots, F_N)$ of $\mathbb{A}^N$ such that $F_1, \ldots, F_N$ are eigenvectors of D ? A positive answer to questions 2.2 and 2.5 would imply a positive answer to question 2.3.

III. NILPOTENT ENDOMORPHISMS.

In the linear case, it is well known that if F is a nilpotent linear endomorphism of $\mathbb{C}^N$, then $F^N = 0$. It turns out that this result is still true for polynomial endomorphisms.

Theorem 3.1. Let $F \in End(\mathbb{A}^N)$ be nilpotent, then $F^N = 0$.

Proof. Let F be any polynomial endomorphism of $\mathbb{A}^N$ and let us endow $\mathbb{A}^N$ with the Zariski topology. If k is a non negative integer, we set $V_k := \overline{F^k(\mathbb{A}^N)}$. This is an irreducible closed variety of $\mathbb{A}^N$. Indeed, $F^k(\mathbb{A}^N)$ is irreducible since it is the image of the irreducible variety $\mathbb{A}^N$ and we know that the closure of an irreducible subset remains irreducible. We have $V_{k+1} = \overline{F^k\left(F(\mathbb{A}^N)\right)} \subset \overline{F^k(\mathbb{A}^N)} = V_k$, so that $\mathbb{A}^N = V_0 \supset V_1 \supset \ldots \supset V_k \supset V_{k+1} \supset \ldots$. We show that $V_{k+1} = \overline{F(V_k)}$. We have $F(V_k) = F\left(\overline{F^k(\mathbb{A}^N)}\right) \subset \overline{F\left(F^k(\mathbb{A}^N)\right)} = V_{k+1}$, whence $\overline{F(V_k)} \subset V_{k+1}$. We have used the fact that if F is a continuous map, then for any set A, we have $F(\overline{A}) \subset \overline{F(A)}$. Indeed, A is a subset of the closed set $F^{-1}\left(\overline{F(A)}\right)$, so that $\overline{A} \subset F^{-1}\left(\overline{F(A)}\right)$, which proves that $F(\overline{A}) \subset \overline{F(A)}$. On the converse $F(V_k) = F\left(\overline{F^k(\mathbb{A}^N)}\right) \supset F\left(F^k(\mathbb{A}^N)\right)$ so that $\overline{F(V_k)} \supset \overline{F^{k+1}(\mathbb{A}^N)} = V_{k+1}$. If we assume that $\dim V_k = \dim V_{k+1}$ for some k, since V_{k+1} is a closed subvariety of the irreducible variety V_k, this implies that $V_{k+1} = V_k$. Hence, we also have $\overline{F(V_{k+1})} = \overline{F(V_k)}$, i.e. $V_{k+2} = V_{k+1}$. Finally, we will have $V_k = V_{k+1} = \ldots = V_n$ for each $n \geq k$. We now assume that F is nilpotent and let m be the smallest integer such that $F^m = \{0\}$. If $k < m$, we cannot have $\dim V_k = \dim V_{k+1}$, because otherwise we would have $V_k = V_{k+1} = \ldots = V_m = \{0\}$. Therefore, $N = \dim V_0 > \dim V_1 > \ldots > \dim V_m = 0$ and $m \leq N$. □

Remark. When F is a nilpotent linear endomorphism, it is well known that the sequence $u_n := \dim \operatorname{Im} F^n - \dim \operatorname{Im} F^{n+1}$ is decreasing. In the polynomial case, it is no longer true. When we take the endomorphism $F := (xz, yz, 0)$ of $\mathbb{A}^3$, we have $\dim \operatorname{Im} F^0 = 3$, $\dim \operatorname{Im} F^1 = 2$ and $\dim \operatorname{Im} F^2 = 0$.

IV. DIMENSION TWO.

From now on, we set $N = 2$. In Subsection 1 we analyze LF polynomial endomorphisms of $\mathbb{A}^2$ which are invertible and in Subsection 2 we analyze those which are not invertible. In Subsection 3 we apply these results to characteristic polynomials and in Subsection 4 to minimal ones.

1. THE INVERTIBLE CASE.

One of the direct consequences of the amalgamated structure of the group of polynomial automorphisms of $\mathbb{A}^2$ (see [17], [20], [26], [11]) is the well known fact that an automorphism of $\mathbb{A}^2$ is dynamically trivial if and only if it is conjugate to a triangular automorphism. One can show easily that for an automorphism F the following assertions are equivalent (see [12]):

(i) F is dynamically trivial ; (ii) F is triangularizable ; (iii) F is LF ;
(iv) $\deg F^2 \le \deg F$; (v) $\forall\, n \in \mathbb{N},\ \deg F^n \le \deg F$.

In fact, any triangularizable automorphism F can be triangularized in a "good" way with respect to the degree:

Lemma 4.1. When F is a triangularizable automorphism of $\mathbb{A}^2$, then there exist a triangular automorphism G and an automorphism φ such that

$$F = \varphi \circ G \circ \varphi^{-1} \text{ and } \deg F = \deg G\, (\deg \varphi)^2.$$

Proof. Let Aut be the group of polynomial automorphisms of $\mathbb{A}^2$, let $\mathcal{A}$ be the subgroup of affine automorphisms, and let $\mathcal{T}$ be the subgroup of upper triangular ones. We have $\mathcal{A} = \{K \in Aut,\ \deg K = 1\}$ and $\mathcal{T} = \{K = (K_1, K_2) \in Aut,\ \dfrac{\partial K_2}{\partial x_1} = 0\}$.

Let $F = A^{[1]} \circ T^{[1]} \circ A^{[2]} \circ T^{[2]} \circ \ldots \circ A^{[l]} \circ T^{[l]} \circ A^{[l+1]}$ be a reduced expression of F where the $A^{[k]}$'s belong to $\mathcal{A}$ and the $T^{[k]}$'s to $\mathcal{T}$: this means that $\forall\, k,\ T^{[k]} \notin \mathcal{A}$ and that $\forall\, k \in \{2, \ldots, l\},\ A^{[k]} \notin \mathcal{T}$ (see [26]).

Let B be the composition (in the same order) of the first l terms and E that of the last l terms of the sequence $A^{[1]},\ T^{[1]},\ A^{[2]},\ \ldots,\ A^{[l]},\ T^{[l]},\ A^{[l+1]}$ and let M be the middle term (i.e. $M = A^{[k+1]}$ if $l = 2k$ and $M = T^{[k+1]}$ if $l = 2k+1$), so that we have $F = B \circ M \circ E$.

The triangularizability of F is equivalent to saying that $E \circ B \in \mathcal{A} \cap \mathcal{T}$ (see Proposition 4 of [12]). Thus we have $F = B \circ H \circ B^{-1}$ where $H := M \circ E \circ B \in \mathcal{A} \cup \mathcal{T}$. The first expression of F being reduced, we get $\deg F = \prod_k \deg T^{[k]} = \deg B \deg M \deg E$.

But $\deg E = \deg B^{-1} = \deg B$ and $\deg M = \deg M \circ E \circ B = \deg H$, so that $\deg F = \deg H (\deg B)^2$. For $H \in \mathcal{T}$, we can just set $\varphi := B$ and $G := H$.

For $H \in \mathcal{A}$, let $A \in \mathcal{A}$ be such that $G := A^{-1} \circ H \circ A \in \mathcal{A} \cap \mathcal{T}$. We can now just set $\varphi := B \circ A$ and we are done since $\deg G = \deg H\ (= 1)$ and $\deg \varphi = \deg B$. □

Remark. When $F(0) = 0$, we can assume that $\varphi(0) = 0$ and $G(0) = 0$ by using the groups $Aut_0 := \{F \in Aut,\ F(0) = 0\}$, $\mathcal{A}_0 := \mathcal{A} \cap Aut_0$ and $\mathcal{T}_0 := \mathcal{T} \cap Aut_0$.

Before computing a vanishing polynomial for triangularizable automorphisms (see Lemma 4.3 below), we deal with the triangular case:

Lemma 4.2. Let $G = (ax + r(y), by)$ be a triangular endomorphism of degree d with $a, b \in \mathbb{C}$ and $r(y) \in \mathbb{C}[y]$ satisfying $r(0) = 0$. Then $p(T) := (T-a)(T-b)(T-b^2)\dots(T-b^d)$ is a vanishing polynomial of G.

Proof. We may assume that $r = \sum_{l=1}^{d} r_l y^l$ is a fixed polynomial.

First case. We assume that $\forall\ l \in \{1, \dots, d\},\ a \neq b^l$. By induction, we get (for any $n \geq 0$)

$$G^n = \left(a^n x + \sum_{k=0}^{n-1} a^k r(b^{n-1-k} y), b^n y \right).$$ But we have

$$\begin{aligned} \sum_{k=0}^{n-1} a^k\ r(b^{n-1-k} y) &= \sum_{k=0}^{n-1} a^k \sum_{l=1}^{d} r_l y^l\ (b^{n-1-k})^l = \sum_{l=1}^{d} r_l y^l \sum_{k=0}^{n-1} a^k (b^l)^{n-1-k} \\ &= \sum_{l=1}^{d} r_l y^l\ \frac{a^n - (b^l)^n}{a - b^l}. \end{aligned}$$

Therefore there exist endomorphisms $K_0, \dots, K_l$ such that

$$\forall\ n \in \mathbb{N},\ G^n = a^n K_0 + b^n K_1 + (b^2)^n K_2 + \ldots + (b^d)^n K_d.$$

If we set $\Omega := \{a, b, \dots, b^d\}$, this means that the sequence $(G^n)_{n\in\mathbb{N}}$ is of Ω-exponential type (see rem. 3 following Proposition 1.2) and this proves our result in this case.

Second case. The general case.
If we set $G_{a,b} := (ax + r(y), by)$ and $p_{a,b} := (T-a)(T-b)(T-b^2)\dots(T-b^d)$, we have shown above that $p_{a,b}(G_{a,b}) = 0$ for all $(a, b) \in \mathbb{C}^2$ outside the curve $(a-b)(a-b^2)\dots(a-b^l) = 0$. Therefore, by density, this equality remains true for any $(a, b) \in \mathbb{C}^2$. □

Lemma 4.3. Let $F = \varphi \circ G \circ \varphi^{-1}$ be an endomorphism of $\mathbb{A}^2$ where φ is an automorphism of degree e with $\varphi(0) = 0$ and where $G = (ax + r(y), by)$ is a triangular endomorphism of degree d with $a, b \in \mathbb{C}$ and $r(y) \in \mathbb{C}[y]$ satisfying $r(0) = 0$. Then F is a zero of

$$p(T) := \prod_{\substack{(k,l)\in\mathbb{N}^2 \\ 0\ <\ dk+l\ \leq\ de}} (T - a^k b^l).$$

Proof. *First case.* We assume that $\forall\ l \in \{1, \dots, d\},\ a \neq b^l$.

We have seen in the proof of Lemma 4.2 that in this case the sequence $(G^n)_{n\in\mathbb{N}}$ is of Ω-exponential type where $\Omega := \{a, b, b^2, \dots, b^d\}$.

The sequence $(G^n \circ \varphi^{-1})_{n\in\mathbb{N}}$ will still be of Ω-exponential type.

If we write $G^n \circ \varphi^{-1} = (u_1(n), u_2(n))$ and $\varphi = (\varphi_1, \varphi_2)$, we have $F^n = \varphi \circ G^n \circ \varphi^{-1} = (\varphi_1(u_1(n), u_2(n)), \varphi_2(u_1(n), u_2(n)))$. Since the sequences u_1 and u_2 are of Ω-exponential type, the sequences $\varphi_1(u_1, u_2)$ and $\varphi_2(u_1, u_2)$ are of Ω'-exponential type with $\Omega' = \bigcup_{k=1}^{e} \Omega^k$

(see rem. 3 following Proposition 1.2).

But $\Omega' = \{a^{j_0}b^{j_1+2j_2+\ldots+dj_d},\ j=(j_0,\ldots,j_d)\in\mathbb{N}^{d+1},\ 0<|j|\le e\}$ is included into $\Omega''=\{a^kb^l,\ (k,l)\in\mathbb{N}^2,\ 0<dk+l\le de\}$ because the inequality $j_0+\ldots j_d\le e$ implies the inequality $dj_0+(j_1+2j_2+\ldots+dj_d)\ \le\ de$.

So, the sequence $(F^n)_{n\in\mathbb{N}}$ is of Ω''-exponential type and this implies that $p(F)=0$.

Second case. The general case. As in Lemma 4.2, we conclude by a density argument. □

2. THE NON-INVERTIBLE CASE.

Below, we will identify a polynomial map $u\ :\ \mathbb{A}^2\to\mathbb{A}^1$ with a polynomial $u(x,y)\in\mathbb{C}[x,y]$, and we will identify a polynomial map $v\ :\ \mathbb{A}^1\to\mathbb{A}^2$ with a pair $v=(v_1,v_2)$ where $v_1,v_2\in\mathbb{C}[x]$.

Lemma 4.4. Let F be a LF endomorphism of $\mathbb{A}^2$ which is not invertible and such that $F(0)=0$. Then, there exist polynomial maps $u\ :\ \mathbb{A}^2\to\mathbb{A}^1$ and $v\ :\ \mathbb{A}^1\to\mathbb{A}^2$ such that

(i) $F=v\circ u$; (ii) $u(0,0)=0$ and $v(0)=(0,0)$;

(iii) the map $L:=u\circ v\ :\ \mathbb{A}^1\to\mathbb{A}^1$ is linear, i.e. $L(x)=ax$ for some $a\in\mathbb{C}$.

Proof. We may assume that $F\neq 0$. We have already seen that $\mathrm{Jac}(F_1,F_2)=0$. This condition is equivalent to saying that F_1 and F_2 are algebraically dependant over $\mathbb{C}$ or to saying that there exist $u(x,y)\in\mathbb{C}[x,y]$ and $v_1(x),v_2(x)\in\mathbb{C}[x]$ such that $F_1=v_1(u)$ and $F_2=v_2(u)$ (see [14], [23] and [22]). We may assume that $u(0,0)=0$ and since $F(0)=0$, we obtain $v_1(0)=v_2(0)=0$.

If we set $L(x):=u\circ v(x)\in\mathbb{C}[x]$, we have $\forall\ k\in\mathbb{N}$, $(F^{\#})^k(u)\ =\ u\circ F^k\ =\ L^k\circ u$. Since the degree of $(F^{\#})^k(u)$ must be upper bounded and since $\deg(L^k\circ u)\ =\ (\deg\ L)^k\deg\ u$, this implies $\deg\ L\ \le\ 1$ (since $\deg\ u\neq 0$). □

Lemma 4.5. Let F be a LF endomorphism of $\mathbb{A}^2$ which is not invertible and such that $F(0)=0$. We write $F=v\circ u$ as in Lemma 4.4 and let a be such that $u\circ v(x)=ax$. If $d:=\deg\ F$, then $p=T(T-a)(T-a^2)\ldots(T-a^d)$ is a vanishing polynomial of F.

Proof. If $u=0$, we obtain at once $F=0$, $p=T$ and $p(F)=0$. If $u\neq 0$ let us note that $\deg\ v_1$ and $\deg\ v_2\ \le\ d$ and that $\forall\ n\in\mathbb{N}$, $F^{n+1}=(v_1(a^nu),v_2(a^nu))$. We set $\Omega:=\{a,a^2,\ldots,a^d\}$. The sequences $n\mapsto p_1(a^nu)$ and $n\mapsto p_2(a^nu)$ are of Ω-exponential type, so that the sequence $n\mapsto F^{n+1}$ is also of Ω-exponential type. This means that $q\ :=\ (T-a)(T-a^2)\ldots(T-a^d)$ is a vanishing polynomial of this sequence. This is equivalent to saying that $p(T)=Tq(T)$ is a vanishing polynomial of the sequence $n\mapsto F^n$. By Proposition 1.3, this is still equivalent to $p(F)=0$. □

Remark. If $\mathrm{supp}\,r\ :=\ \{k,\ r_k\neq 0\}$ for $r=\sum_k r_kx^k$ and if $\Omega'\ :=\ \{a^k,\ k\in\mathrm{supp}\ v_1\cup\mathrm{supp}\ v_2\}$, we can show that $\mu_F=T\prod_{\omega\in\Omega'}(T-\omega)$ when $u\neq 0$.

We will now explain how to build any LF polynomial endomorphism F of $\mathbb{A}^2$ which is not invertible and such that $F(0) = 0$. We will distinguish two cases:

First case. F is nilpotent.

1. Choose any non-zero polynomial map $v : \mathbb{A}^1 \to \mathbb{A}^2$ such that $v(0) = (0,0)$;
2. Since v is proper, its image is a closed curve of $\mathbb{A}^2$. Therefore, $\mathcal{I}_v := \{r \in \mathbb{C}[x,y],\ r \circ v = 0\}$ is a non-zero principal ideal of $\mathbb{C}[x,y]$, i.e. $\mathcal{I}_v = (r)$ for some (non-zero) element $r \in \mathbb{C}[x,y]$;
3. When $q \in \mathbb{C}[x,y]$, then $u := qr \in \mathcal{I}_v$ defines a map $u : \mathbb{A}^2 \to \mathbb{A}^1$ such that $u \circ v = 0$;
4. If we set $F := v \circ u$, then F is a nilpotent endomorphism of $\mathbb{A}^2$ such that $F(0) = 0$.

Second case. F is not nilpotent.

We will now show that F is conjugate to a polynomial endomorphism of the kind $G = (\lambda x + yq(x,y), 0)$ where $\lambda \in \mathbb{C}^*$ and $q(x,y) \in \mathbb{C}[x,y]$. This will imply that Im F is a closed curve of $\mathbb{A}^2$ isomorphic to $\mathbb{A}^1$ and that Im F^n = Im F (for $n \geq 1$), since $G^n = (\lambda^n x + \lambda^{n-1} yq(x,y), 0)$ (for $n \geq 1$).

We write $F = v \circ u$ as in Lemma 4.4. We have $u \circ v(x) = ax$ with $a \neq 0$. By the Abhyankar-Moh theorem (see [1]), there exists an automorphism φ of $\mathbb{A}^2$ such that $\varphi \circ v(x) = (x, 0)$. Therefore, if we set $G := \varphi \circ F \circ \varphi^{-1}$, then the second coordinate of G is zero. We write the first coordinate in the form $G_1 = r(x) + yq(x,y)$. Since the sequence $n \mapsto G^n$ is of bounded degree, the sequence $n \mapsto G^n \circ (x,0)$ also. But $G^n \circ (x,0) = (r^n(x), 0)$, where r^n stands for the composition $\underbrace{r \circ r \circ \ldots \circ r}_{n}$. We must have deg $r \leq 1$ and finally we obtain $r(x) = \lambda x$ for some non-zero complex number λ.

3. THE CHARACTERISTIC POLYNOMIAL.

Theorem 4.1. Let $F \in End(\mathbb{A}^2)$ be LF and such that $F(0) = 0$. If $d :=$ deg F and if λ_1, λ_2 are the eigenvalues of $\mathcal{L}(F)$, then $\prod_{\substack{\alpha \in \mathbb{N}^2 \\ 0 < |\alpha| \leq d}} (T - \lambda^\alpha)$ is a vanishing polynomial of F.

Proof. This comes from Theorem 1.2. since deg $F^n \leq d$ for $n \geq 0$ (if F is invertible, it has already been said and if F is not, it is a consequence of Lemma 4.4). $\square$

Remark. This characteristic polynomial is of degree $\dfrac{d(d+3)}{2}$. If $d = 1$, we find the classical characteristic polynomial of a linear endomorphism (in dimension two).

4. THE MINIMAL POLYNOMIAL.

Theorem 4.2. Let F be a LF endomorphism of $\mathbb{A}^2$ such that $F(0) = 0$ and let μ_F be the minimal polynomial of F, then deg $\mu_F \leq$ deg $F + 1$.

Proof. When F is not invertible, this comes from Lemma 4.5. When F is invertible, we can write $F = \varphi \circ G \circ \varphi^{-1}$ with $\varphi(0) = G(0) = 0$ and deg $F = de^2$, where $d =$ deg G and $e =$ deg φ (see Lemma 4.1 and the remark following it). By Lemma 4.3, deg μ_F is less than or equal to the cardinal of the set $A := \{(k,l) \in \mathbb{N}^2,\ 0 < dk + l \leq de\}$. But

$$|A|+1 \;=\; |\{(k,l)\in\mathbb{N}^2,\ 0\le dk+l\le de\}| \;=\; \sum_{k=0}^{e}(de-dk+1) \;=\; e+1+d\sum_{k=0}^{e}(e-k)$$
$$\;=\; e+1+d\,\frac{e(e+1)}{2} \;=\; (e+1)\left(\frac{de}{2}+1\right) \text{ so that } |A| = e\left(\frac{de}{2}+\frac{d}{2}+1\right) \text{ and}$$

we want to prove that $|A| \;\le\; de^2+1$. If $\dfrac{de}{2}+\dfrac{d}{2}+1 \;\le\; de$, i.e. $2 \;\le\; d(e-1)$, we are done. Otherwise, we get $e=1$ or $(e,d)=(2,1)$ so that $|A| = de^2+1$. □

Acknowledgements. We are indebted to the referees and to the editor for a number of comments which helped improve the exposition. The second author is grateful to the University of La Rochelle for financial support for two pleasant stays at this place.

References

[1] S.S. Abhyankar, T.T. Moh, Embeddings of the line in the plane, J. Reine Angew. Math., 276 (1975), 148-166.

[2] J. Ax, The elementary theory of finite fields, Ann. of Math. (2) 88 (1968), 239-271.

[3] J. Ax, Injective endomorphisms of varieties and schemes, Pac. J. Math. 31 (1969), 1-7.

[4] M. de Bondt, Quasi-translations and counterexamples to the homogeneous dependence problem, to appear in the Proc. of the A.M.S.

[5] A. Borel, Injective endomorphisms of algebraic varieties, Arch. Math. (Basel) 20 (1969), 531-537.

[6] N. Bourbaki, Éléments de Mathématiques, Algèbre, chap. 1-3, Hermann, Paris, 1970.

[7] L. Cerlienco, M. Mignotte, F. Piras, Suites récurrentes linéaires, propriétés algébriques et arithmétiques, L'Enseignement Mathématique 33 (1987), 67-108.

[8] S. Cynk, R. Rusek, Injective endomorphisms of algebraic and analytic sets, Ann. Pol. Math. 56, n°1 (1991), 29-35.

[9] D. Eisenbud, Commutative algebra. With a view toward algebraic geometry. Graduate Texts in Mathematics, 150, Springer-Verlag, New York, 1995.

[10] A. van den Essen, Polynomial Automorphisms and the Jacobian Conjecture, Progress in Math, vol 190, Birkhäuser Verlag, Basel, Boston, Berlin, 2000.

[11] S. Friedland, J. Milnor, Dynamical properties of plane polynomial automorphisms, Ergod. Th. & Dynam. Syst 9 (1989), 67-99.

[12] J.-P. Furter, On the degree of iterates of automorphisms of the affine plane, Manuscripta Mathematica, 98 (1999), 183-193.

[13] J.-P. Furter, Quasi-locally finite polynomial endomorphisms, in preparation.

[14] P. Gordan, Über biquadratische Gleichungen, Math. Annalen 29 (1987), 318-326.

[15] A. Grothendieck, EGA 4, Inst. Hautes Études Sci. Publ. Math. n°32, 1967.

[16] J.E. Humphreys, Linear Algebraic Groups, Springer-Verlag, New York, 1975, 1981.

[17] H.W.E. Jung, Über ganze birationale Transformationen der Ebene, J. Reine Angew. Math., 184 (1942), 161-174.

[18] T. Kambayashi, Automorphism group of a polynomial ring and algebraic group actions on affine space, J. Algebra 60, n°2 (1979), 439-451.

[19] F. Knop, Nichtlinearisierbare Operationen halbeinfacher Gruppen aud affinen Raümen, Invent. Math. 105, n°1 (1991), 217-220.

[20] W. van der Kulk, On polynomial rings in two variables, Nieuw Archief voor Wiskunde, 3, n° 1 (1953), 33-41.

[21] M. Nagata, On the automorphism group of k[X,Y], Kyoto Univ. Lectures in Math. 5, Kyoto University, Kinokuniya-Tokio, 1972.

[22] A. Nowicki, On the jacobian equation J(f,g)=0 for polynomials in k[x,y], Nagoya Math. J., 109 (1988), 151-157.

[23] O. Perron, Algebra I, Die Grundlagen, Walter de Gruyter & Co., Berlin, 1951.

[24] W. Rudin, Injective polynomial maps are automorphisms, Amer. Math. Monthly 102, n°6 (1995), 540-543.

[25] G. Schwarz, Exotic algebraic group actions, C.R. Acad. Sci. Paris Sér. I Math., 309, n°2 (1989), 89-94.

[26] J.-P. Serre, Trees, Springer Verlag, Berlin, Heidelberg, New York, 1980.

[27] I.P. Shestakov, U.U. Umirbaev, Poisson brackets and two-generated subalgebras of rings of polynomials, J. Amer. Math. Soc 17 (2004), 181-196.

[28] I.P. Shestakov, U.U. Umirbaev, The tame and the wild automorphisms of polynomial rings in three variables, J. Amer. Math. Soc 17 (2004), 197-227.

[29] M.K. Smith, Stably Tame Automorphisms, J. of Pure and Applied Algebra, 58 (1989), 209-212.

[30] B.L. van der Waerden, Die Alternative bei nichtlinearen Gleichungen. Nachr. Gesellsch. Wiss. Göttingen, Math. Phys. Klasse (1928), 77-87.