

On the degree of the inverse of an automorphism of the affine space

Jean-Philippe FURTER

Abstract : We study the degree of the inverse of an automorphism f of the affine n -space over a \mathbb{C} -algebra k , in terms of the degree d of f and of other data. For $n = 1$, we obtain a sharp upper bound for $\deg(f^{-1})$ in terms of d and of the nilpotency index of the ideal generated by the coefficients of f'' . For $n = 2$ and arbitrary $d \geq 3$, we construct a (triangular) automorphism f of Jacobian one such that $\deg(f^{-1}) > d$. This answers a question of A. van den Essen (see [3]) and enables us to deduce that some schemes introduced by authors to study the Jacobian Conjecture are not reduced. Still for $n = 2$, we give an upper bound for $\deg(f^{-1})$ when f is triangular. Finally, in the case $d = 2$ and any n , we complete a result of G. Meisters and C. Olech and use it to give the sharp bound for the degree of the inverse of a quadratic automorphism, with Jacobian one, of the affine 3-space.

1. Introduction

In this paper, unless explicitly mentioned, k will denote a \mathbb{C} -algebra.

If n is a positive integer, we have the polynomial algebra $k^{[n]} = k[X_1, \dots, X_n]$ and the affine space $\mathbb{A}_k^n = \text{Spec}(k^{[n]})$. When $n = 1$, we will use X instead of X_1 and when $n = 2$, we will use X, Y instead of X_1, X_2 . A k -endomorphism f of \mathbb{A}_k^n will be identified with its sequence $f = (f_1, \dots, f_n)$ of coordinate functions $f_i \in k^{[n]}$ ($i = 1, \dots, n$). Its Jacobian matrix is $J(f) = (\frac{\partial f_i}{\partial X_j})_{1 \leq i, j \leq n}$, its Jacobian determinant is $\text{Jac}(f) = \det J(f)$ and its degree is $\deg(f) = \max_{1 \leq i \leq n} \deg(f_i)$. The chain rule $J(f \circ g) = J(f)(g) \cdot J(g)$, where g is a k -endomorphism of \mathbb{A}_k^n , shows us that if f is invertible, then, $J(f)$ is invertible, i.e. $\text{Jac}(f) \in (k^{[n]})^*$. The Jacobian Conjecture asserts the converse when $k = \mathbb{C}$. If d is a positive integer, specializing this conjecture to endomorphisms of degree less than or equal to d , we get :

JC(n,d) : If f is a \mathbb{C} -endomorphism of $\mathbb{A}_{\mathbb{C}}^n$ with $\deg(f) \leq d$, then

$$f \text{ is invertible} \iff J(f) \text{ is invertible (i.e., } \text{Jac}(f) \in \mathbb{C}^* \text{)}.$$

Following the notations introduced by different authors investigating the Jacobian Conjecture, $\text{End}_k(\mathbb{A}_k^n)$ is the space of all k -endomorphisms of \mathbb{A}_k^n and we set (where I_n is the identity matrix of rank n) :

$$\begin{aligned} E_n(k) &= \{f \in \text{End}_k(\mathbb{A}_k^n) \text{ such that } f(0) = 0 \text{ and } J(f)(0) = I_n\} \\ J_n(k) &= \{f \in E_n(k) \text{ such that } \text{Jac}(f) = 1\} \\ G_n(k) &= \{f \in J_n(k) \text{ such that } f \text{ is invertible}\} \\ E_{n,d}(k) &= \{f \in E_n(k) \text{ such that } \deg(f) \leq d\} \\ J_{n,d}(k) &= J_n(k) \cap E_{n,d}(k) \\ G_{n,d}(k) &= G_n(k) \cap E_{n,d}(k) \\ c(k, n, d) &= \sup\{\deg(f^{-1}), f \in G_{n,d}(k)\} \end{aligned}$$

We have $c(k, n, d) \in \mathbb{N} \cup \{\infty\}$ and we define $c(n, d) \in \mathbb{N} \cup \{\infty\}$ as the supremum of the $c(k, n, d)$ when k varies through all \mathbb{C} -algebras.

If r is a positive integer, we also set

$$G_{n,d,r}(k) = \{f \in G_{n,d}(k) \text{ such that } \deg(f^{-1}) \leq r\}$$

When $n = 2$, the subgroup $T_2(k)$ of $G_2(k)$ of triangular automorphisms will play an important role in this paper :

$$T_2(k) = \{f = (f_1, f_2) \in G_2(k) \text{ such that } \frac{\partial f_1}{\partial Y} = 0\}.$$

The following theorem of H. Bass ([1]) is enough to motivate the problem of estimating the degree of the inverse of an automorphism of the affine space.

Theorem ([1]). *The following four assertions are equivalent :*

- i) $JC(n, d)$ is true ;
- ii) for all \mathbb{C} -algebras k , $J_{n,d}(k) = G_{n,d}(k)$;
- iii) for all \mathbb{C} -algebras k and all k -endomorphism f of \mathbb{A}_k^n satisfying $\deg(f) \leq d$, f is invertible if and only if $J(f)$ is invertible ;
- iv) $c(n, d) < \infty$.

If k is a reduced \mathbb{C} -algebra, it is well known that $c(k, n, d) = d^{n-1}$ (cf [1]), the main point is a formula of Gabber asserting that for any automorphism

f of \mathbb{A}_k^n , we have $\deg(f^{-1}) \leq (\deg(f))^{n-1}$. But what about the degree of the inverse of an automorphism of affine n -space in the general case ?

In section 2 (resp. 3), we study the case $n = 1$ (resp. $n = 2$).

The main goal of section 2 is an application to section 3, but the following sharp estimation (see Theorem 1) may have interest for its own :

Theorem. *If $f = (P(X))$ is an automorphism of \mathbb{A}_k^1 and if the ideal I in k generated by the coefficients of the polynomial P'' satisfies $I^{e+1} = 0$ where $e \geq 0$ is an integer, then $\deg(f^{-1}) \leq (\deg(f) - 1).e + 1$.*

The main result of section 3 is (see Proposition 2 and the commentary preceding Lemma 5) :

Proposition. *There exists a \mathbb{C} -algebra k and an element f of $T_2(k)$ such that $\deg(f^{-1}) > \deg(f)$.*

and we prove moreover (see Proposition 3) that :

Proposition. *If f is an element of $T_2(k)$, then $\deg(f^{-1}) \leq 4(\deg(f))^4$.*

Section 4 is devoted to the quadratic case. We complete there a result of G. Meisters and C. Olech (see Proposition 4) and prove that $c(3, 2) = 6$.

2. Automorphisms of the affine line

Let us recall that k is any \mathbb{C} -algebra. In particular, it is not necessarily reduced. We will use the following definition :

Definition. *If $m \geq 0$ is an integer and $P(X) = \sum_{i=0}^{\infty} a_i X^i$ is an element of $k[X]$, we define $I(m, P)$ as the ideal of k generated by a_m, a_{m+1}, \dots .*

Let us note that for any integer $l \geq 0$, we have $I(m, P^{(l)}) = I(m+l, P)$ where $P^{(l)}$ is the l -th derivative of P . It is well known that the polynomial $P(X)$ is invertible in $k[X]$ if and only if $P(0)$ is invertible in k and $I(1, P)$ is a nilpotent ideal. We also know that an endomorphism $f = (P(X))$ of

\mathbb{A}_k^1 is invertible if and only if the polynomial $P'(X)$ is invertible in $k[X]$. We could deduce it from the last quoted theorem of H. Bass because the Jacobian Conjecture is true in dimension one. However, we can prove it easily, using the following version of Hensel's lemma :

Hensel's lemma. *Let A be a \mathbb{C} -algebra, I a nilpotent ideal of A , $g \in A[Z]$ (where Z is an indeterminate) and $\alpha_0 \in A$. If $g'(\alpha_0) \in A^*$ and $g(\alpha_0) \in I$, then the sequence*

$$\alpha_{i+1} = \alpha_i - \frac{g(\alpha_i)}{g'(\alpha_i)}$$

is well defined and it satisfies the relation $g(\alpha_i) = 0$ when i is big enough.

Proof. It is sufficient to show by induction on i that $g'(\alpha_i) \in A^*$ and $g(\alpha_i) \in I^{2^i}$. For $i = 0$, it follows from the hypothesis. If $i \geq 0$, using Taylor's expansion, we get the existence of $\beta, \gamma \in A$ such that

$$g'(\alpha_{i+1}) = g'(\alpha_i) + \beta \cdot (\alpha_{i+1} - \alpha_i) \text{ and}$$

$$g(\alpha_{i+1}) = g(\alpha_i) + g'(\alpha_i) \cdot (\alpha_{i+1} - \alpha_i) + \gamma \cdot (\alpha_{i+1} - \alpha_i)^2$$

and if we suppose that $g'(\alpha_i) \in A^*$ and $g(\alpha_i) \in I^{2^i}$, the equality $g'(\alpha_{i+1}) - g'(\alpha_i) = -\beta \cdot \frac{g(\alpha_i)}{g'(\alpha_i)}$ shows us that $g'(\alpha_{i+1}) - g'(\alpha_i) \in I$ whence $g'(\alpha_{i+1}) \in A^*$ while the equality $g(\alpha_{i+1}) = \gamma \frac{g(\alpha_i)^2}{g'(\alpha_i)^2}$ shows us that $g(\alpha_{i+1}) \in I^{2^{i+1}}$. \square

If $f = (P(X))$ is invertible, we have already mentioned that P' has to be an invertible polynomial. Conversely, if P' is an invertible polynomial, we can suppose that $P(0) = 0$ and $P'(0) = 1$ which means that we can write $P = X + a_2X^2 + \dots + a_dX^d$ where d is a positive integer and a_2, \dots, a_d belong to k . Then, by taking $A = k[X]$, $I = I(2, P) \cdot A$, $g(Z) = P(Z) - X$, $\alpha_0 = X$, we check that $g'(\alpha_0) = 1 + 2a_2X + \dots + da_dX^{d-1} \in k[X]^*$ and that $g(\alpha_0) = a_2X^2 + \dots + a_dX^d \in I(2, P) \cdot A$. We can thus apply Hensel's lemma and deduce the existence of an element $Q(X) \in k[X]$ such that $P(Q(X)) = X$ which is enough to prove that f is invertible with inverse $g = (Q(X))$.

The following amusing lemma shows us the importance of knowing more than the degree of f to estimate the degree of its inverse (of course, the automorphisms of Lemma 1 do not have their Jacobian equal to one) :

Lemma 1. *If $d \geq 2, d' \geq 2$ are two integers, then there exist a \mathbb{C} -algebra k and an automorphism f of \mathbb{A}_k^1 such that $\deg(f) = d$ and $\deg(f^{-1}) = d'$.*

Proof. By, if necessary, exchanging f and f^{-1} , we can suppose that $d \leq d'$. Let us consider the following algebraic equation :

$$(1 + \varepsilon X)^d = 1 + \varepsilon X'.$$

By solving this equation for X' , we get

$$\begin{aligned} X' &= \frac{(1 + \varepsilon X)^d - 1}{\varepsilon} \\ &= \sum_{i=1}^d \binom{d}{i} \varepsilon^{i-1} X^i \end{aligned}$$

and by solving it for X , we get :

$$\begin{aligned} X &= \frac{(1 + \varepsilon X')^{\frac{1}{d}} - 1}{\varepsilon} \\ &= \sum_{i=1}^{\infty} \binom{\frac{1}{d}}{i} \varepsilon^{i-1} X'^i \end{aligned}$$

We just have to note that for all $i > 0$, $\binom{\frac{1}{d}}{i} \neq 0$ and then, it is clear that we can take $k = \mathbb{C}[\varepsilon]/(\varepsilon)^{d'}$ and $f = (\sum_{i=1}^d \binom{d}{i} \varepsilon^{i-1} X^i)$. \square

If P is invertible with $\deg(P) = d$ and $I(1, P)^{e+1} = 0$, it is easy to check that

$$\deg(P^{-1}) \leq de.$$

(we can suppose that $P(0) = 1$ and then, if we write $P = 1 + Q$, the formula $P^{-1} = \sum_{i=0}^{\infty} (-1)^i Q^i$ gives us the result). The next proposition establishes the converse of this inequality :

Proposition 1. *If P is an invertible polynomial of $k[X]$ with $\deg(P) = d$ and $\deg(P^{-1}) = d'$, then*

$$I(1, P)^{\min(d, d') \cdot (d+d'-1)+1} = 0.$$

Remark. Before giving the proof, it may be interesting to see how we can first deduce the existence of an integer e depending only on d and d' such that $I(1, P)^{e+1} = 0$ for each P satisfying the hypothesis of the proposition. Of course, we can always suppose that such a P satisfies $P(0) = 1$ and then, by writing again $P = 1 + Q$ and expressing P^{-1} as $\sum_{i=0}^{\infty} (-1)^i Q^i$, it suffices to prove the following lemma :

Lemma 2. *If d, d' are nonzero integers, $A = \{A_1, \dots, A_d\}$ is a set of indeterminates, $(P_i)_{i \geq 1}$ is the sequence of elements of $\mathbb{C}[A]$ defined by*

$$(1 + \sum_{i=1}^d A_i X^i)^{-1} = 1 + \sum_{i=1}^{\infty} P_i(A_1, \dots, A_d) X^i$$

(where the inverse is meant for the multiplicative law of $\mathbb{C}[A][[X]]$)

and if I (resp. J) is the ideal of $\mathbb{C}[A]$ generated by the $(P_i)_{i > d'}$ (resp. by A_1, A_2, \dots, A_d), then there exists an integer e such that : $J^{e+1} \subset I$.

Proof of Lemma 2. If $(a_1, \dots, a_d) \in \mathbb{C}^d$, we have

$$(\forall i > d', P_i(a_1, \dots, a_d) = 0) \Rightarrow (a_1, \dots, a_d) = 0$$

because the relation $(\forall i > d', P_i(a_1, \dots, a_d) = 0)$ implies that $1 + \sum_{i=1}^d a_i X^i$ is an invertible element of $\mathbb{C}[X]$. So, the zero locus of I is the zero locus of J and we conclude by applying the Hilbert Nullstellensatz. \square

Proof of Proposition 1. If we take P as in the proposition, we can suppose that $P(0) = 1$. Let us set $R(Y) = Y^d P(1/Y)$. $R(Y)$ is a monic element of $k[Y]$ so that there exists a \mathbb{C} -algebra k' containing k and elements $\varepsilon_1, \dots, \varepsilon_d$ in k' such that $R(Y) = \prod_{i=1}^d (Y + \varepsilon_i)$. Finally, observing that $P(X) = X^d R(1/X)$, we obtain

$$P(X) = \prod_{i=1}^d (1 + \varepsilon_i X).$$

Then, for all $1 \leq i \leq d$, we have $\varepsilon_i^{d+d'} = 0$ because of the relation

$$\deg(1 + \varepsilon_i X)^{-1} \leq d + d' - 1.$$

Let \mathcal{E} be the ideal of k' generated by the ε_i . The relations $\varepsilon_i^{d+d'} = 0$ (for $1 \leq i \leq d$) show us that $\mathcal{E}^{d(d+d'-1)+1} = 0$. Furthermore, we have $I(1, P) \subset \mathcal{E}$ so that $I(1, P)^{d(d+d'-1)+1} = 0$.

In the same way, we get $I(1, P^{-1})^{d'(d+d'-1)+1} = 0$ and so, we conclude by noting that $I(1, P) = I(1, P^{-1})$. Indeed, by writing $P = 1 + Q$ and expressing P^{-1} as $\sum_{i=0}^{\infty} (-1)^i Q^i$, we get $I(1, P^{-1}) \subset I(1, P)$ and in the same manner we get $I(1, P) \subset I(1, P^{-1})$. \square

The next theorem gives us an accurate bound for the degree of the inverse of an automorphism $f = (P(X))$ of the affine line in terms of the degree of the automorphism and of the nilpotency index of the ideal $I(2, P)$:

Theorem 1. *If $d \geq 1$, $e \geq 0$ are integers and $f = (P(X))$ is an automorphism of \mathbb{A}_k^1 satisfying $\deg(f) \leq d$ and $I(2, P)^{e+1} = 0$, then*

$$\deg(f^{-1}) \leq (d-1)e + 1.$$

Remark. If $f^{-1} = (Q(X))$, then the previous formula may also be written

$$\deg(Q') \leq e \cdot \deg(P')$$

but we did not find any way to prove it directly.

Proof. We can suppose $d \geq 2$, otherwise the proof is obvious. The result is then a consequence of the following lemma :

Lemma 3. *If $d \geq 2$ is an integer, $A = \{A_2, \dots, A_d\}$ is a set of indeterminates, $(B_i)_{i \geq 2}$ is the sequence of elements of $\mathbb{C}[A]$ defined by*

$$(X + \sum_{i=2}^d A_i X^i)^{-1} = X + \sum_{i=2}^{\infty} B_i(A_2, \dots, A_d) X^i$$

(where the inverse is meant for the composition law of $\mathbb{C}[A][[X]]$)

and if J is the ideal of $\mathbb{C}[A]$ generated by A_2, \dots, A_d , then we have :

$$\forall i \geq 2, B_i \in J^{\lceil \frac{i-1}{d-1} \rceil},$$

(where $\lceil x \rceil$ is the least integer n such that $x \leq n$ if x is any real number).

Indeed, we can suppose that P is of the shape $P = X + \sum_{i=2}^d a_i X^i$ and, by lemma 3, the coefficient of X^i in f^{-1} will vanish as soon as $\frac{i-1}{d-1} > e$, i.e., $i > (d-1)e + 1$. \square

Proof of Lemma 3. We prove the result by induction on i . If $2 \leq i \leq d$, we have $\lceil \frac{i-1}{d-1} \rceil = 1$ and it is clear that $B_i \in J$.

Suppose $i > d$. For each $j \in \mathbb{N}$, let us define $C(j)$ in $\mathbb{C}[A]$ as the coefficient of X^i in the X -polynomial $(X + A_2 X^2 + \dots + A_d X^d)^j$. When $j < \frac{i}{d}$ or $j > i$, we have $C(j) = 0$ and also $C(i) = 1$, so, the equality

$$X + \sum_{k=2}^d A_k X^k + \sum_{j=2}^{\infty} B_j (X + A_2 X^2 + \dots + A_d X^d)^j = X$$

implies that

$$B_i = - \sum_{\frac{i}{d} \leq j \leq i-1} B_j \cdot C(j) \quad (1)$$

When $\frac{i}{d} \leq j \leq i-1$, we claim that $C(j) \in J^{\lceil \frac{i-j-1}{d-1} \rceil + 1}$.

Indeed, let us consider the expansion of $(X + A_2 X^2 + \dots + A_d X^d)^j$. To obtain terms of degree i in X , we have to take at least $\lceil \frac{i-j-1}{d-1} \rceil + 1$ terms of the shape $A_k X^k$ ($2 \leq k \leq d$). Otherwise, if we only took p of these terms, with $p < \lceil \frac{i-j-1}{d-1} \rceil + 1$ then we would get a term of degree at most $(j-p) \cdot 1 + p \cdot d < i$ because $p < \frac{i-j}{d-1}$.

So, using our induction hypothesis and (1), it suffices to show that when $\frac{i}{d} \leq j \leq i-1$, we have :

$$\lceil \frac{j-1}{d-1} \rceil + \lceil \frac{i-j-1}{d-1} \rceil + 1 \geq \lceil \frac{i-1}{d-1} \rceil.$$

This can be proved by distinguishing three cases :

a) If $\frac{j-1}{d-1}$ and $\frac{i-2}{d-1}$ are both integers, then $\frac{i-j-1}{d-1}$ is also an integer and the inequality can be written $i + d - 3 \geq i - 1$ which is true because $d \geq 2$.

b) If $\frac{j-1}{d-1}$ is not an integer, then, $\lceil \frac{j-1}{d-1} \rceil = \lceil \frac{j}{d-1} \rceil$ and the inequality follows from the inequality :

$$\forall (x, y) \in \mathbb{R}^2, \lceil x \rceil + \lceil y \rceil + 1 \geq \lceil x + y \rceil.$$

c) If $\frac{i-2}{d-1}$ is not an integer, then, $\lceil \frac{i-1}{d-1} \rceil = \lceil \frac{i-2}{d-1} \rceil$ and the inequality follows from the same inequality as in b). \square

We now prove that the inequality in Theorem 1 is optimal. We can suppose that $d \geq 2$. The following lemma shows us that if we take $k = \mathbb{C}[\varepsilon]/(\varepsilon^{e+1})$, then, the automorphism $f = (X - \varepsilon X^d)$ of \mathbb{A}_k^1 satisfies $\deg(f^{-1}) = (d-1)e + 1$.

Lemma 4. *If $d \geq 2$ is an integer, then the inverse (for the composition law of formal power series) of $f(X) = X - \varepsilon X^d \in \mathbb{C}[\varepsilon][[X]]$ is of the shape*

$$g(X) = \sum_{i=0}^{\infty} \alpha_i \varepsilon^i X^{1+i(d-1)},$$

where $(\alpha_i)_{i \in \mathbb{N}}$ is a sequence of nonzero positive integers.

Proof. Let us set $f_1(X) = X - X^d \in \mathbb{C}[[X]]$ and let $g_1(X)$ be its inverse (for the composition law of formal power series). If ω is a primitive $(d-1)$ -root of unity, then we have the relation $f_1(\omega X) = \omega f_1(X)$ from which we get $g_1(\omega f_1(X)) = \omega X$. By making the substitution $X := g_1(X)$, we obtain $g_1(\omega X) = \omega g_1(X)$ so that

$$g_1(X) = \sum_{i=0}^{\infty} \alpha_i X^{1+i(d-1)},$$

where $(\alpha_i)_{i \in \mathbb{N}}$ is a sequence of real numbers. However, by writing $f_1(g_1(X)) = X$, we get $\alpha_0 = 1$ and

$$\alpha_{k+1} = \sum_{i_1+i_2+\dots+i_d=k} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_d}$$

from which we get easily by induction on i that $\forall i \in \mathbb{N}, \alpha_i \in \mathbb{N}^*$. The same computation for f as for f_1 (inserting some ε in the right places) ends up the proof of Lemma 4. \square

3. Automorphisms of the affine plane

The following theorem, which was already known when $k = \mathbb{C}$ (see [5]), implies (taking $d = 2$) that $c(2, 2) = 2$.

Theorem 2. *If $d \geq 2$ is an integer, h is an endomorphism of \mathbb{A}_k^2 which is homogeneous of degree d and if $f = Id + h$ is an endomorphism of \mathbb{A}_k^2 satisfying $Jac(f) = 1$, then f is invertible and $f^{-1} = Id - h$.*

Proof. If $h = (h_1, h_2)$, the equality $Jac(f) = 1$ implies :

$$\frac{\partial h_1}{\partial X} + \frac{\partial h_2}{\partial Y} + \frac{\partial h_1}{\partial X} \cdot \frac{\partial h_2}{\partial Y} - \frac{\partial h_1}{\partial Y} \cdot \frac{\partial h_2}{\partial X} = 0$$

and by considering the homogeneous components of degree $d - 1$ and $2d - 2$, we get :

$$\frac{\partial h_1}{\partial X} + \frac{\partial h_2}{\partial Y} = 0 \text{ and } \frac{\partial h_1}{\partial X} \cdot \frac{\partial h_2}{\partial Y} - \frac{\partial h_1}{\partial Y} \cdot \frac{\partial h_2}{\partial X} = 0$$

The first of these equations shows us that there exists a unique homogeneous polynomial P of degree $d + 1$ in $k[X, Y]$ such that $(h_1, h_2) = (-\frac{\partial P}{\partial Y}, \frac{\partial P}{\partial X})$ and the remaining equation writes now :

$$\frac{\partial^2 P}{\partial X^2} \cdot \frac{\partial^2 P}{\partial Y^2} - \left(\frac{\partial^2 P}{\partial X \partial Y}\right)^2 = 0.$$

We set $D = h_1 \frac{\partial}{\partial X} + h_2 \frac{\partial}{\partial Y} = -\frac{\partial P}{\partial Y} \frac{\partial}{\partial X} + \frac{\partial P}{\partial X} \frac{\partial}{\partial Y}$ which is a derivation of $k[X, Y]$ and we check that

$$\begin{aligned} D^2 X &= \frac{\partial P}{\partial Y} \cdot \frac{\partial^2 P}{\partial X \partial Y} - \frac{\partial P}{\partial X} \cdot \frac{\partial^2 P}{\partial Y^2} \\ &= \frac{1}{d} (X \cdot \frac{\partial^2 P}{\partial X \partial Y} + Y \cdot \frac{\partial^2 P}{\partial Y^2}) \cdot \frac{\partial^2 P}{\partial X \partial Y} - \frac{1}{d} (X \cdot \frac{\partial^2 P}{\partial X^2} + Y \cdot \frac{\partial^2 P}{\partial X \partial Y}) \cdot \frac{\partial^2 P}{\partial Y^2} \\ &= -\frac{1}{d} X \cdot \left(\frac{\partial^2 P}{\partial X^2} \cdot \frac{\partial^2 P}{\partial Y^2} - \left(\frac{\partial^2 P}{\partial X \partial Y}\right)^2\right) \\ &= 0 \end{aligned}$$

and, in a similar manner, $D^2 Y = 0$.

Therefore, by Leibnitz's formula, D is a locally nilpotent derivation of $k[X, Y]$ ($\forall a \in k[X, Y], \exists i \in \mathbb{N}$ such that $D^i a = 0$) and so we can associate to D the following mapping which defines an action of $(k, +)$ over $k[X, Y]$:

$$\begin{aligned} k \times k[X, Y] &\rightarrow k[X, Y] \\ (t, a) &\mapsto \exp(tD).a = \sum_{i=0}^{\infty} \frac{(tD)^i}{i!} \cdot a \end{aligned}$$

Hence, the mappings $\exp(D)$ and $\exp(-D)$ are k -automorphisms of $k[X, Y]$, one being the inverse of the other. These automorphisms are defined by their action on X and Y . The automorphism $\exp(D)$ sends (X, Y) to $(X + h_1, Y + h_2)$ whereas the automorphism $\exp(-D)$ sends (X, Y) to $(X - h_1, Y - h_2)$. \square

If $d \geq 3$, the next proposition shows that $c(2, d) > d$. This is a very interesting phenomenon. Indeed, let n be a positive integer. On the first hand, if one believes that the Jacobian Conjecture in dimension n and degree d (JC(n,d)) is true, then we know that $c(n, d) < \infty$ and on the second hand, if k is a reduced \mathbb{C} -algebra, we know that $c(k, n, d) = d^{n-1}$. That is why we may be tempted to make the following Generalized Jacobian Conjecture (for $n = 2$, this corresponds to Question 2.19 of A. van den Essen, in the paper [3]) :

GJC(n,d). $c(n, d) = d^{n-1}$.

Proposition 2 shows us that this Generalized Jacobian Conjecture is wrong. It means that we no longer have any candidate for $c(n, d)$. In particular, when $d \leq 100$, we know that $c(2, d) < \infty$ because $JC(2, d)$ has been proved in this case by T.T. Moh ([7]), but we do not know how to estimate $c(2, d)$.

The first counter-example to this Generalized Jacobian Conjecture was found for $n = 2, d = 3$, using a computer. It turned out that the automorphism we obtained was triangular and that the counter-example could be easily generalized to $n = 2, d \geq 3$. We will give here these generalized counter-examples. We use the following lemma, whose proof is left to the reader :

Lemma 5. $T_2(k)$ is the subgroup of $G_2(k)$ consisting of the elements of the shape

$$f = (P(X), P'(X)^{-1}Y + Q(X))$$

where $g = (P(X))$ is any automorphism of \mathbb{A}_k^1 belonging to $E_1(k)$ and Q is any element of $k[X]$ such that $Q(0) = Q'(0) = 0$. Moreover, if $g^{-1} = (R(X))$, then

$$f^{-1} = (R(X), R'(X)^{-1}Y - R'(X)^{-1}Q(R(X))).$$

□

Proposition 2. *If $d \geq 3$ is an integer, then*

$$f = (X + \varepsilon X^d, (1 - d\varepsilon X^{d-1})Y + X^2) \in T_2(\mathbb{C}[\varepsilon]/(\varepsilon^2)),$$

$$\deg(f) = d \text{ and } \deg(f^{-1}) = d + 1.$$

Proof. We can just apply Lemma 5 with $k = \mathbb{C}[\varepsilon]/(\varepsilon^2)$, $P = X + \varepsilon X^d$, $Q = X^2$ so that $R = X - \varepsilon X^d$, $R^{-1} = 1 + d\varepsilon X^{d-1}$, $f \in T_2(\mathbb{C}[\varepsilon]/(\varepsilon^2))$ and

$$f^{-1} = (X - \varepsilon X^d, (1 + d\varepsilon X^{d-1})Y - X^2 - (d - 2)\varepsilon X^{d+1}).$$

□

We now introduce the schemes $J_{n,d}$ and $G_{n,d,r}$. Proposition 2 allows us to deduce that these schemes are not always reduced (see Remark (3.3) in [1]).

It is easy to see that $(k \mapsto J_{n,d}(k))$ can be identified with the functor of points of an affine scheme defined over \mathbb{C} , which we shall of course call $J_{n,d}$.

Indeed, we have $J_{n,d} = \text{Spec}(A_{n,d})$, where the \mathbb{C} -algebra $A_{n,d}$ (called the Jacobian algebra of dimension n and degree d) is described as follows :

We set $E_{n,d} = \{\alpha = (\alpha_1, \dots, \alpha_n), \forall i \alpha_i \in \mathbb{N}, 2 \leq \alpha_1 + \dots + \alpha_n \leq d\}$ and let $Y = \{Y_{i,\alpha}, 1 \leq i \leq n, \alpha \in E_{n,d}\}$ be a set of indeterminates. We define the endomorphism $g_{n,d}$ of $\mathbb{A}_{\mathbb{C}[Y]}^n$ by the formula :

$$g_{n,d} = (X_i + \sum_{\alpha \in E_{n,d}} Y_{i,\alpha} X_1^{\alpha_1} \dots X_n^{\alpha_n})_{1 \leq i \leq n}$$

Let us write : $\text{Jac}_X(g_{n,d}) - 1 = \sum_{(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n} P_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$, where the P_α are in $\mathbb{C}[Y]$. If I is the ideal generated by the $P_\alpha (\alpha \in \mathbb{N}^n)$, we have $A_{n,d} = \mathbb{C}[Y]/I$.

Furthermore, if r is a positive integer, it is proved in [1] that $(k \mapsto G_{n,d,r}(k))$ can be identified with the functor of points of an affine scheme defined over \mathbb{C} , which we call $G_{n,d,r}$.

Let $f_{n,d}$ be the endomorphism of $\mathbb{A}_{A_{n,d}}^n$ which is obtained by replacing each coefficient of the monomials appearing in the expression of $g_{n,d}$ by its reduction modulo I . The endomorphism $f_{n,d}$ is of Jacobian one by construction and so, if $\text{CJ}(n,d)$ is true, $f_{n,d}$ is invertible and it is now easy to see that $c(n,d) = \deg(f_{n,d}^{-1})$. Always assuming that $\text{CJ}(n,d)$ is true, we also deduce the existence of a positive integer r such that $G_{n,d,r} = J_{n,d}$.

Because $\text{JC}(2,d)$ is true when $3 \leq d \leq 100$ ([7]) and $c(k,2,d) = d$ if k is a reduced \mathbb{C} -algebra, we get :

Corollary of Proposition 2. *For each $3 \leq d \leq 100$, the scheme $J_{2,d}$ is not reduced and there exists a positive integer r such that the scheme $G_{2,d,r}$ is not reduced.* \square

However, we get a bound for the degree of the inverse of an element of $T_2(k)$:

Proposition 3. *If f is an element of $T_2(k)$, then we have $\deg(f^{-1}) \leq 4(\deg(f))^4$.*

Proof. We set $d = \deg(f)$ and let $P, Q \in k[X]$ be such that

$$f = (P(X), P'(X)^{-1}Y + Q(X)).$$

We know that $g = (P(X))$ is an automorphism of \mathbb{A}_k^1 and let $R \in k[X]$ be such that $g^{-1} = (R(X))$.

Then, $f^{-1} = (R(X), R'(X)^{-1}Y - R'(X)^{-1}Q(R(X)))$.

We get successively :

$$\begin{aligned} \deg(P) &\leq d ; \\ \deg(P') &\leq d - 1 ; \\ \deg(P'^{-1}) &\leq d - 1 ; \\ I(2, P)^{(d-1)(2d-3)+1} &= 0 \text{ (by Prop. 1 and because } I(2, P) = I(1, P') \text{)} ; \\ \deg(R) &\leq (d-1)^2(2d-3) + 1 \text{ (by Theorem 1)} ; \\ \deg(R'^{-1}) &\leq (d-1)[(d-1)^2(2d-3) + 1] \text{ (because } R'^{-1} = P'(R) \text{)} ; \\ \deg(f^{-1}) &\leq (2d-1)[(d-1)^2(2d-3) + 1] \leq 4d^4 \text{ (by the formula for } f^{-1} \text{)}. \quad \square \end{aligned}$$

Remarks. The majorations made in the proof of Proposition 3 are of course not optimal at several places. Concerning the problem of estimating $c(2,d)$

($d \geq 3$), with Michel Fournie and Didier Pinchon, we have checked that $c(2, 3) = 9$, using a computer.

4. Quadratic automorphisms of the affine space

In this section, n will denote a positive integer. Contrary to the foregoing, X will denote the set of indeterminates X_1, X_2, \dots, X_n and Y will denote the set of indeterminates Y_1, Y_2, \dots, Y_n . $q = q(X)$ will denote an endomorphism of \mathbb{A}_k^n which is homogeneous of degree two and f will denote the endomorphism of \mathbb{A}_k^n defined by the formula $f = \text{Id} + q$.

Let us begin by recalling that $\text{JC}(n, 2)$ has been proven by S. Wang ([9]) so that $c(n, 2) < \infty$ and $G_{n,2}(k) = J_{n,2}(k)$. It is easy to deduce from this that the three following assertions are equivalent :

- i) J_q is a nilpotent matrix ;
- ii) $I_n + J_q$ is an invertible matrix (in $M_n(k[X])$) ;
- iii) f is an automorphism.

The following result of G. Meisters and C. Olech gives us, in some particular cases, explicit formula for f^{-1} which allow us to bound $\deg(f^{-1})$. Their proof is for $k = \mathbb{C}$ but it may remain unchanged in the case where k is any \mathbb{C} -algebra :

Theorem ([6]). *i) If $(J_q)^2 = 0$, then we have $f^{-1}(X) = X - q(X)$;*
ii) If $(J_q)^3 = 0$, then we have $f^{-1}(X) = X - q(X) + J_q(X).q(X) - q(q(X)) + \frac{1}{2}J_q(q(X))^2.X - \frac{1}{2}J_q(q(X))^2.q(X)$.

The next proposition answers the question made in [6] asking whether the terms $\frac{1}{2}J_q(q(X))^2.X$ and $\frac{1}{2}J_q(q(X))^2.q(X)$ could effectively be nonzero in case ii) when $k = \mathbb{C}$:

Proposition 4. *Let q be the endomorphism of $\mathbb{A}_{\mathbb{C}}^6$ defined by*

$$q = (2X_2X_6 - 2X_3^2 - X_4X_5, 2X_3X_5 - X_4X_6, X_5X_6, X_5^2, X_6^2, 0),$$

then we have $(J_q)^3 = 0$, hence, $f = \text{Id} + q$ is an automorphism of $\mathbb{A}_{\mathbb{C}}^6$. Moreover, $\deg(f^{-1}) = 6$.

Proof. By a calculation, one checks that $(J_q)^3 = 0$ and that the inverse $g = (g_1, g_2, g_3, g_4, g_5, g_6)$ of f is given by :

$$\begin{cases} g_1 = X_1 - 2X_2X_6 + 2X_3^2 + X_4X_5 - 3X_4X_6^2 - X_5^3 + 3X_5^2X_6^2 - 3X_5X_6^4 + X_6^6 \\ g_2 = X_2 - 2X_3X_5 + X_4X_6 + 2X_3X_6^2 + X_5^2X_6 - 2X_5X_6^3 + X_6^5 \\ g_3 = X_3 - X_5X_6 + X_6^3 \\ g_4 = X_4 - X_5^2 + 2X_5X_6^2 - X_6^4 \\ g_5 = X_5 - X_6^2 \\ g_6 = X_6 \end{cases}$$

□

Remark : For $d = 3$, A. van den Essen already gave a counter-example in [4] to a Conjecture of K. Rusek (see [8]) asserting that for any automorphism $g = \text{Id} + h$ of $\mathbb{A}_{\mathbb{C}}^n$, where h is a homogeneous endomorphism of $\mathbb{A}_{\mathbb{C}}^n$ of degree $d \geq 2$, we have $\deg(f^{-1}) \leq d^{i_N(J_h)-1}$ where $i_N(J_h)$ is the nilpotency index of J_h . The automorphism given in Proposition 4 gives us a counterexample in the case $d = 2$. However, in the quadratic case, we can correct the previous formula (see Proposition 5), using the next definition which is taken from [6] :

Definition. J_q , which can be seen as a (linear) mapping from \mathbb{C}^n to $M_n(\mathbb{C})$, is said to be strongly nilpotent of order l (l is an integer) if

$$\forall (x^1, \dots, x^l) \in (\mathbb{C}^n)^l, J_q(x^1).J_q(x^2).\dots.J_q(x^l) = 0.$$

We define $i_{SN}(J_q)$ as the smallest integer l satisfying the above relation.

Proposition 5. If $k = \mathbb{C}$ and f is an automorphism, then $\deg(f^{-1}) \leq 2^{i_{SN}(J_q)-1}$.

Proof. We may have $i_{SN}(J_q) = \infty$ (cf [6]), but, in this case, there is nothing to prove. So, let us suppose that $i_{SN}(J_q) = l \in \mathbb{N}$. For $1 \leq i \leq l$, we denote by V_{l-i} the vector space spanned by

$$\bigcup_{(x^1, \dots, x^i) \in (\mathbb{C}^n)^i} \text{Im}(J_q(x^1).J_q(x^2).\dots.J_q(x^i))$$

and we set $V_l = \mathbb{C}^n$.

$(V_i)_{0 \leq i \leq l}$ is an increasing sequence of subspaces of \mathbb{C}^n satisfying

$$\forall 0 < i \leq l, \forall x \in \mathbb{C}^n, J_q(x)(V_i) \subset V_{i-1}$$

and $V_l = \mathbb{C}^n$. By the hypothesis of strong nilpotency of order l , we have $V_0 = \{0\}$. So, there exist $l + 1$ integers $n_0 = 0 \leq n_1 \leq n_2 \leq \dots \leq n_{l-1} \leq n_l = n$ and a basis e_1, \dots, e_n of \mathbb{C}^n such that $\forall 0 \leq i \leq l, e_1, \dots, e_{n_i}$ is a basis of V_i . This implies the existence of an element $G \in \text{GL}_n(\mathbb{C})$ such that $G^{-1}.J_q.G = (A_{i,j})_{1 \leq i, j \leq l}$ where the $A_{i,j}$ are $(n_i - n_{i-1}, n_j - n_{j-1})$ matrices such that $A_{i,j} = 0$ when $i \leq j$. The formula $J_{G^{-1} \circ q \circ G}(x) = G^{-1}.J_q(G.x).G$ shows us that $J_{G^{-1} \circ q \circ G}(x)$ is of the same shape and so, by conjugating f by the mapping $(x \rightarrow G.x)$, we can suppose that J_q is of the same shape. Now, writing $q = (q_1, \dots, q_n)$, this implies that for $n_i < j \leq n_{i+1}$ (where $0 \leq i < l$) q_j depends only on the variables $X_{n_{i+1}+1}, X_{n_{i+1}+2}, \dots, X_n$ and so the system $X + q(X) = Y$ (in the unknown X with parameter Y) is triangular. We can see, by induction on i (beginning with $i = l - 1$ and finishing with $i = 0$) that when $n_i < j \leq n_{i+1}$ we have $\deg_Y(X_j(Y)) \leq 2^{l-1-i}$ and the proof is finished. \square

In the proof of the next proposition and in the remark following it, we will see some close connections between the case where $n = 3$, k is any \mathbb{C} -algebra and the case where there is no condition on n , $k = \mathbb{C}$, $(J_q)^3 = 0$.

A. van den Essen pointed out to us that the following well known lemma when $k = \mathbb{C}$ (see for example [2]) remains true when k is any \mathbb{C} -algebra :

Lemma 6. *If $d \geq 2$ is an integer and h is an endomorphism of \mathbb{A}_k^n which is homogeneous of degree d , then $\det(I_n + J_h) = 1 \Rightarrow (J_h)^n = 0$.*

Proof. If $\det(I_n + J_h) = 1$, then the degrees of the polynomials appearing as coefficients of the matrix $(I_n + J_h)^{-1}$ do not exceed $(n - 1).(d - 1)$ (by the formula of the inverse of a matrix). However, for all $i \geq 0$, the coefficients of the matrix $(J_h)^i$ are homogeneous of degree $(d - 1).i$, so, the formula $(I_n + J_h)^{-1} = \sum_{i=0}^{\infty} (-1)^i (J_h)^i$ gives us the result. \square

Proposition 6. $c(3, 2) = 6$.

Proof. If $n = 3$ and f is an element of $G_{3,2}(k)$, then it follows from Lemma

6 that $(J_q)^3 = 0$ and by the Theorem quoted earlier from [6], we have $\deg(f^{-1}) \leq 6$.

We now claim that if we take

$$k = \mathbb{C}[\varepsilon_1, \varepsilon_2, \varepsilon_3]/(\varepsilon_1 + \varepsilon_2 + \varepsilon_3, \varepsilon_1^2 + \varepsilon_2^2 + \varepsilon_3^2, \varepsilon_1^3 + \varepsilon_2^3 + \varepsilon_3^3)$$

$$\text{and } q = (2\varepsilon_1 X_1 X_3 - X_2^2, 2\varepsilon_2 X_2 X_3 - X_3^2, \varepsilon_3 X_3^2),$$

then $f = \text{Id} + q$ belongs to $G_{3,2}(k)$ and its inverse is of degree (at least) 6. To check it, we begin by remarking that

$$k = \mathbb{C}[\varepsilon_1, \varepsilon_2, \varepsilon_3]/(\varepsilon_1 + \varepsilon_2 + \varepsilon_3, \varepsilon_1 \varepsilon_2 + \varepsilon_1 \varepsilon_3 + \varepsilon_2 \varepsilon_3, \varepsilon_1 \varepsilon_2 \varepsilon_3)$$

which implies that if Z is any indeterminate

$$\prod_{i=1}^3 (1 + \varepsilon_i Z) = 1 \quad (\text{in } k[Z]).$$

By this remark, we see firstly that $\text{Jac}(f) = 1$ (so $f \in J_{3,2}(k) = G_{3,2}(k)$) and also $\deg(1 + \varepsilon_i Z)^{-1} \leq 2$, so, $\varepsilon_i^3 = 0$. To compute the inverse of f , we have to solve the following system in the unknown (X_1, X_2, X_3) with the parameters (Y_1, Y_2, Y_3) :

$$\begin{cases} Y_1 &= X_1 + 2\varepsilon_1 X_1 X_3 - X_2^2 \\ Y_2 &= X_2 + 2\varepsilon_2 X_2 X_3 - X_3^2 \\ Y_3 &= X_3 + \varepsilon_3 X_3^2 \end{cases}$$

If $f^{-1} = (g_1, g_2, g_3)$ where the g_i are elements of $k[Y_1, Y_2, Y_3]$, we see that

$$g_1(0, 0, Y_3) = (1 + 2\varepsilon_1 X_3)^{-1} (1 + 2\varepsilon_2 X_3)^{-2} X_3^4,$$

where $X_3 = Y_3 - \varepsilon_3 Y_3^2 + 2\varepsilon_3^2 Y_3^3$. The relations between the ε_i imply that

$$g_1(0, 0, Y_3) = (1 + 2\varepsilon_1 X_3)(1 + 2\varepsilon_3 X_3)^2 X_3^4,$$

whence :

$$g_1(0, 0, Y_3) = X_3^4 + (2\varepsilon_1 + 4\varepsilon_3)X_3^5 + (8\varepsilon_1 \varepsilon_3 + 4\varepsilon_3^2)X_3^6 + 8\varepsilon_1 \varepsilon_3^2 X_3^7.$$

We calculate that the coefficients of Y_3^6 in the Y_3 -polynomials X_3^i ($i = 4, 5, 6, 7$) are respectively : $14\varepsilon_3^2, -5\varepsilon_3, 1, 0$ and we finally get that the coefficient of Y_3^6 in $g_1(0, 0, Y_3)$ is

$$14\varepsilon_3^2 - 5\varepsilon_3(2\varepsilon_1 + 4\varepsilon_3) + (8\varepsilon_1 \varepsilon_3 + 4\varepsilon_3^2) = -2(\varepsilon_1 + \varepsilon_3)\varepsilon_3 = 2\varepsilon_2 \varepsilon_3 \neq 0.$$

□

Remark : The automorphism exhibited in the proof of Proposition 6 gives us quite naturally an endomorphism \tilde{q} of $\mathbb{A}_{\mathbb{C}}^{18}$ which is homogeneous of degree 2, such that $(J_{\tilde{q}})^3 = 0$ and that $\deg(\tilde{f}^{-1}) = 6$ where $\tilde{f} = \text{Id} + \tilde{q}$. Indeed, let us take $k = \mathbb{C}[\varepsilon_1, \varepsilon_2, \varepsilon_3]/(\varepsilon_1 + \varepsilon_2 + \varepsilon_3, \varepsilon_1^2 + \varepsilon_2^2 + \varepsilon_3^2, \varepsilon_1^3 + \varepsilon_2^3 + \varepsilon_3^3)$ and $q = (2\varepsilon_1 X_1 X_3 - X_2^2, 2\varepsilon_2 X_2 X_3 - X_3^2, \varepsilon_3 X_3^2)$. The mapping

$$\begin{aligned} i : \quad \mathbb{C}^6 & \rightarrow k \\ (a, b, c, d, e, f) & \mapsto a + b\varepsilon_1 + c\varepsilon_2 + d\varepsilon_1^2 + e\varepsilon_2^2 + f\varepsilon_1^2\varepsilon_2 \end{aligned}$$

is an isomorphism of \mathbb{C} -vector spaces and so the following mapping is an isomorphism too :

$$\begin{aligned} j : \quad \mathbb{C}^{18} = \mathbb{C}^6 \times \mathbb{C}^6 \times \mathbb{C}^6 & \rightarrow \mathbb{A}_k^3 \\ (u, v, w) & \mapsto (i(u), i(v), i(w)) \end{aligned}$$

We just now have to set $\tilde{q} = j^{-1} \circ q \circ j$.

Questions.

1. Can one find explicit upper bounds for $c(n, 2)$?
2. If l is a positive integer, does there exist a constant c_l (independent of n) such that $(J_q)^l = 0$ implies that $\deg(f^{-1}) \leq c_l$?
3. Can we take $c_l = c(l, 2)$?

Acknowledgments. I would like to thank Pascal K. Adjmagbo and Arno van den Essen for their help, kindness, enthusiasm and encouragement.

References :

- [1] H. BASS, The Jacobian Conjecture and Inverse Degrees, Arithmetic and Geometry, vol. II, 65-75, Prog. Math., 36, Birkhäuser, Boston, Mass., 1983
- [2] H. BASS, E.H. CONNELL and D. WRIGHT, The Jacobian Conjecture : Reduction of degree and formal expansion of the inverse, Bull. Amer. Math. Soc. (1982)
- [3] A. van den ESSEN, Polynomial maps and the Jacobian Conjecture, Computational Aspects of Lie Group Representations and Related Topics, Proceedings of the 1990 Computational Algebra Seminar, 29-44, in CWI Tract

84, 1991

- [4] A. van den ESSEN, A counterexample to a conjecture of Druzkowski and Rusek, *Annales Polonici Mathematici* LXII.2 (1995), 173-176
- [5] A. van den ESSEN and H. TUTAJ, A remark on the two dimensional Jacobian Conjecture, *J. Pure and Applied Algebra* 96 (1994) 19-22
- [6] G. MEISTERS and C. OLECH, Strong nilpotence holds in dimensions up to five only, *Linear and Multilinear Algebra*, vol. 30, 231-255, 1991
- [7] T.T. MOH, On the global Jacobian Conjecture and the configuration of roots, *J. Reine Angew. Math.* 340 (1983), 140-212
- [8] K. RUSEK, Polynomial automorphisms, Institute of Mathematics, Polish academy of Sciences, Preprint 456, May 1989
- [9] S. WANG, A Jacobian criterion for separability, *J. Algebra* 65, 453-494, 1980

Jean-Philippe FURTER
U.M.P.A.,E.N.S.L.
46 Allée d'Italie
69 007 LYON
FRANCE

email : jfurter@umpa.ens-lyon.fr