Radboud Repository

Radboud University Nijmegen

PDF hosted at the Radboud Repository of the Radboud University Nijmegen

The following full text is a preprint version which may differ from the publisher's version.

For additional information about this publication click this link.
http://hdl.handle.net/2066/126106

Please be advised that this information was generated on 2019-10-14 and may be subject to change.

arXiv:1201.1137v2 [math.AC] 8 Oct 2012

Linearized polynomial maps over finite fields

Joost Berson

Abstract

We consider polynomial maps described by so-called *(multivariate) linearized polynomials*. These polynomials are defined using a fixed prime power, say q. Linearized polynomials have no mixed terms. Considering invertible polynomial maps without mixed terms over a characteristic zero field, we will only obtain (up to a linear transformation of the variables) triangular maps, which are the most basic examples of polynomial automorphisms. However, over the finite field $\mathbb{F}_q$ automorphisms defined by linearized polynomials have (in general) an entirely different structure. Namely, we will show that the linearized polynomial maps over $\mathbb{F}_q$ are in one-to-one correspondence with matrices having coefficients in a univariate polynomial ring over $\mathbb{F}_q$. Furthermore, composition of polynomial maps translates to matrix multiplication, implying that invertible linearized polynomial maps correspond to invertible matrices.

This alternate description of the linearized polynomial automorphism subgroup leads to the solution of many famous conjectures (most notably, the Jacobian Conjecture) for this kind of polynomials and polynomial maps.

Keywords: Affine space; polynomials over commutative rings; group of polynomial automorphisms; group of tame automorphisms

1 Introduction

Let $K[X] := K[X_1, \ldots, X_n]$ be a polynomial ring over a field K. A natural problem in commutative algebra and algebraic geometry is to understand the group $\mathrm{GA}_n(K)$ of automorphisms of $K[X]$ preserving K. There are various long-standing open problems and conjectures in affine algebraic geometry concerning polynomial rings and their automorphisms (see [10], [11] and [15] for more details). Below we mention a few of the most famous ones. (Precise definitions will be provided in later sections.)

Polynomial automorphisms are generally studied over a field of characteristic zero, but the prime characteristic case is gaining interest (for example in [2],[6],[8],[19] and [22]). In Section 4 of this paper, for the problems and conjectures mentioned below, we give a complete answer in cases involving *linearized polynomials* (over a finite field $\mathbb{F}_q$), the main objects of interest of this paper. These polynomials, which are by definition (Section 3) $\mathbb{F}_q$-linear combinations of monomials of the form $X_i^{q^m}$, have thus far only been studied in case $n = 1$, first by Ore in [23] and [24] (more on that in the same section). Section 3 is also devoted to a proof of the fact that the linearized polynomial maps over $\mathbb{F}_q$ are in one-to-one correspondence with matrices having coefficients in a univariate polynomial ring over $\mathbb{F}_q$ (where $\mathbb{F}_q$ is the finite field with q elements).

Funded by a Free Competition grant from the Netherlands Organisation for Scientific Research (NWO)

Joost Berson, Radboud University, Faculty of Science, P.O. Box 9010, 6500 GL Nijmegen, The Netherlands, j.berson@science.ru.nl

Finally, in Section 5, we will emphasize the exceptional nature of linearized polynomial maps over finite fields. Namely, these maps form a special example of polynomial maps without mixed terms, which can be studied over a field of any characteristic. But the main result of this last section is that, over a characteristic zero field, every automorphism defined by polynomials without mixed terms is a triangular automorphism (after a linear transformation of the variables). This is certainly not the case for linearized polynomial maps over a finite field. Also, the other problems and conjectures mentioned below are discussed for the case of polynomials without mixed terms.

Tame Generators Problem: Give necessary and sufficient conditions for tameness of automorphisms of $K[X]$.

In two variables, this has already been solved by Jung [13] and Van der Kulk [16], saying that *all* automorphisms in two variables are tame. In more variables there is only one big result: Shestakov and Umirbaev gave a criterion for tameness (over characteristic zero fields) of automorphisms of the form $(f_1(X_1, X_2, X_3), f_2(X_1, X_2, X_3), X_3)$ in their groundbreaking paper [25]. This gave a negative answer to the question of tameness of the famous Nagata automorphism, introduced in [21] (viewed as an automorphism in three variables over a field). We will show that all linearized polynomial automorphisms are tame, in any dimension (Theorem 4.2).

Jacobian Conjecture: If a polynomial map f over a field K with $\mathrm{char}(K) = 0$ has invertible Jacobian matrix, then f itself is invertible.

This famous conjecture was first proposed by Keller [14] in 1939 for $K = \mathbb{C}$. After more than six decades of intensive study by mathematicians, the conjecture is still open, even for the case n = 2. It is listed as one of the 18 important mathematical problems for the 21st century in Smale's list [26]. More background and (references to) partial results on the Jacobian Conjecture can be found in [4] and [10]. In nonzero characteristic the conjecture is easily shown to be false, but we will present an analogue of this conjecture for linearized polynomial maps, and give a proof (Corollary 4.3).

Coordinate Recognition Problem: Given a polynomial $f \in K[X]$, give necessary and sufficient conditions for f to be a coordinate.

In case we have two variables, this problem has already been solved in [7] and in [9]. The Coordinate Recognition Problem is still open for three or more variables. Our Proposition 4.4 describes exactly when a linearized polynomial is a coordinate.

Polynomial Ring Recognition Problem: For a finitely generated K-algebra A, give necessary and sufficient conditions for A to be (isomorphic to) a polynomial ring over K.

A necessary condition for being a polynomial ring over K is that A is a domain. Surprisingly, if A is defined by linearized polynomials this is also sufficient (Corollary 4.10). This doesn't hold in general for an algebra defined over a field of characteristic zero, where the problem has only been solved in case A is at most two-generated over K. Corollary 4.10 also implies the Abhyankar-Sathaye Conjecture below, but then for linearized polynomials over a finite field (Theorem 4.11). In characteristic zero, this conjecture has only been completely solved for $n \leq 2$.

Abhyankar-Sathaye Conjecture: If $\mathrm{char}(K) = 0$ and $f \in K[X_1, \ldots, X_n]$ satisfies $K[X_1, \ldots, X_n]/(f) \cong_K K[Y_1, \ldots, Y_{n-1}]$, then f is a coordinate.

Last but not least, we present the

Linearization Conjecture: If an automorphism over a field K with $\mathrm{char}(K) = 0$ has finite order, then it is conjugate to a linear automorphism.

An automorphism that is conjugate to a linear one is called *linearizable*. For $n = 2$ the (affirmative) answer easily follows from the structure of $\mathrm{GA}_2(K)$, which was already observed in [15]. For $n \geq 3$ this conjecture is still unsolved. However, we will show (Corollary 4.18) that a linearized polynomial automorphism over $\mathbb{F}_q$ of finite order relatively prime to q, is linearizable.

2 Polynomial maps, conventions

Associating a matrix to a polynomial map is a recurring thing in this paper, so first we write down the basic notations used in this paper concerning matrices. Given any commutative ring R, let $\mathrm{M}_{m\times n}(R)$ (or $\mathrm{M}_n(R)$, if $m = n$) be the set of all $m \times n$ matrices with entries in R. For the group of all invertible matrices in $\mathrm{M}_n(R)$ we use the usual notation $\mathrm{GL}_n(R)$. I_n will be the identity matrix in $\mathrm{GL}_n(R)$.

A *polynomial map over* K is a list $f = (f_1, \ldots, f_m)$ of polynomials in $K[X]$. We can view polynomial maps as K-algebra homomorphisms $K[Y] \to K[X]$, $Y_i \mapsto f_i$, where $Y := (Y_1, \ldots, Y_m)$ is another list of variables. But they are often also identified with maps $K^n \to K^m$ given by polynomial substitutions, which is actually only an exact identification if K is infinite.

Now consider another polynomial map $g = (g_1, \ldots, g_n)$, with each $g_i \in K[Z]$ for yet another list of variables $Z = (Z_1, \ldots, Z_l)$. In the usual notation, the composition of f and g is defined as $f \circ g = (f_1(g_1, \ldots, g_n), \ldots, f_m(g_1, \ldots, g_n))$. Restricting to the case $m = n$, the map f is called an *invertible polynomial map* or *automorphism* if there exists another $g = (g_1, \ldots, g_n) \in K[X]^n$ with $f \circ g = g \circ f = X$ (the identity map). Furthermore, we call a polynomial in $K[X]$ a *coordinate* if it equals one of the components f_i of some automorphism f.

The automorphisms form a group, $\mathrm{GA}_n(K)$. $\mathrm{GL}_n(K)$ is usually viewed as a subgroup (the subgroup of *linear automorphisms*), but there are more "usual" subgroups. They will be introduced in this paper where they are needed. As the first and foremost example of associating a matrix to a polynomial map, we write $\mathrm{J}f$ for the Jacobian matrix $(\frac{\partial f_i}{\partial X_j})$ of a polynomial map f. By the chain rule, for any automorphism f we have $\mathrm{J}f \in \mathrm{GL}_n(K[X])$, whence $|\mathrm{J}f| \in K^*$. (Throughout this paper, the operator $|\cdot|$ takes the determinant of a matrix.)

3 Linearized polynomial maps and the q-Jacobian

Here we will describe the main objects of study of this paper, and their basic properties. For now, X denotes just one variable.

Definition 3.1. Let q be a positive power of a prime number. Then $\mathbb{F}_q[X]^{(q)}$ will be the $\mathbb{F}_q$-subspace of $\mathbb{F}_q[X]$ generated by all monomials of the form X^{q^m} (with $m \geq 0$). Furthermore, the *composition* $f \circ g$ of $f, g \in \mathbb{F}_q[X]^{(q)}$ is defined as the substitution of the two polynomials, *i.e.* $(f \circ g)(X) := f(g(X))$.

Remark 3.2. The elements of $\mathbb{F}_q[X]^{(q)}$ are precisely the polynomials in $\mathbb{F}_q[X]$ that induce an $\mathbb{F}_q$-linear map $K \to K$, where K is any infinite extension field of $\mathbb{F}_q$. Indeed, X^q induces the $\mathbb{F}_q$-linear map $x \mapsto x^q$ ($x \in K$), and any map induced by an element of $\mathbb{F}_q[X]^{(q)}$ is an $\mathbb{F}_q$-linear combination of iterates of this particular map. On the other hand, suppose $f \in \mathbb{F}_q[X]$ induces an $\mathbb{F}_q$-linear map $K \to K$, and let X^m be a monomial appearing in f. Since K is an infinite field, the hypothesis implies that $f(X+Y) = f(X) + f(Y)$ and $f(aX) = af(X)$, where Y is a new variable and a generates the multiplicative group of $\mathbb{F}_q$. Comparing terms of equal degree yields $(X+Y)^m = X^m + Y^m$ and $(aX)^m = aX^m$. Let p be the unique prime number such that $q = p^r$, with $r \geq 1$. Suppose m is not a power of p, say $m = dp^e$ with $d > 1$, $p \nmid d$ and $e \geq 0$. Then $(X+Y)^m = ((X+Y)^{p^e})^d = (X^{p^e} + Y^{p^e})^d$ contains the nonzero term $dX^{(d-1)p^e}Y^{p^e}$, which contradicts the fact that $(X+Y)^m = X^m + Y^m$. Hence, m is a power of p. Since a generates $\mathbb{F}_q^*$ and $a \in \mathbb{F}_m$ (as $a^m = a$), we have $\mathbb{F}_q \subseteq \mathbb{F}_m$. So $\mathbb{F}_m$ is a finite dimensional $\mathbb{F}_q$-space, whence m is a power of q.

The above remark implies that $\mathbb{F}_q[X]^{(q)}$ is closed under composition. Moreover, this composition operation has some remarkable properties compared to the composition of any two univariate polynomials over any field (which can be defined in a similar way). For one easily verifies that

- $f(g+h) = f(g) + f(h) \ \ \forall\ f, g, h \in \mathbb{F}_q[X]^{(q)}$
- composition is commutative: $f(g(X)) = g(f(X)) \ \ \forall\ f, g \in \mathbb{F}_q[X]^{(q)}$

(The first property follows directly from Remark 3.2.) Using these facts, it is easy to check that $\mathbb{F}_q[X]^{(q)}$ is a commutative ring (with addition inherited from $\mathbb{F}_q[X]$, and "multiplication" being composition). Also, note that X is the identity element in this ring, and that $\mathbb{F}_q \to \mathbb{F}_q[X]^{(q)},\ a \mapsto aX$ makes $\mathbb{F}_q[X]^{(q)}$ an $\mathbb{F}_q$-algebra. In fact, Theorem 3.3 will show that $\mathbb{F}_q[X]^{(q)}$ is isomorphic as $\mathbb{F}_q$-algebra to the univariate polynomial ring over $\mathbb{F}_q$!

Here we should remark that linearized polynomials (sometimes referred to as "p-polynomials" or "q-polynomials") have already been studied in several papers. Their focus is mostly on the fact that the roots of a linearized polynomial form an $\mathbb{F}_q$-subspace of its splitting field (the kernel of the induced linear map). The result of Theorem 3.3 was first mentioned by Ore ([23],[24]). Later, the property mentioned in Remark 3.2 was noted in [5] and [12]. Both properties also appeared in [3],[17] and [18]. However, in this section we will also define *multivariate* linearized polynomials (the main objects of study of this paper), which have not been studied before in the literature.

Theorem 3.3. *There is a unique isomorphism of $\mathbb{F}_q$-algebras $\delta : \mathbb{F}_q[X]^{(q)} \to \mathbb{F}_q[t]$ such that $\delta\left(X^{q^m}\right) = t^m$ for all $m \geq 0$. Thus, $\delta(f(g)) = \delta(f) \cdot \delta(g) \ \ \forall\ f, g \in \mathbb{F}_q[X]^{(q)}$.*

Proof. By the universal property of $\mathbb{F}_q$-algebras, there is a unique $\mathbb{F}_q$-algebra homomorphism $\mathbb{F}_q[t] \to \mathbb{F}_q[X]^{(q)}$ such that $t \mapsto X^q$. This map clearly gives a one-to-one correspondence between the $\mathbb{F}_q$-bases $\{t^m \mid m \geq 0\}$ and $\{X^{q^m} \mid m \geq 0\}$. Hence, the algebra homomorphism is a vector space isomorphism, and thus even an $\mathbb{F}_q$-algebra isomorphism (with inverse δ). □

Now let $X := (X_1, \ldots, X_n)$ be a list of variables. Then the polynomials in

$$\mathbb{F}_q[X]^{(q)} := \mathbb{F}_q[X_1]^{(q)} \oplus \cdots \oplus \mathbb{F}_q[X_n]^{(q)}$$

are called *(multivariate) linearized polynomials in* $X_1, \ldots, X_n$. And the elements of $(\mathbb{F}_q[X]^{(q)})^m$ (as subset of $\mathbb{F}_q[X]^m$) are the *(multivariate) linearized polynomial maps.*

Remark 3.4. The elements of $\mathbb{F}_q[X]^{(q)}$ are precisely the polynomials in $\mathbb{F}_q[X]$ that induce an $\mathbb{F}_q$-linear map $K^n \to K$, where K is any infinite extension field of $\mathbb{F}_q$. Indeed, any term of a given element of $\mathbb{F}_q[X]^{(q)}$ is in fact an element of $\mathbb{F}_q[X_i]^{(q)}$ for some i (and the induced map $K^n \to K$ factorizes through the projection $K^n \to K$ on the ith factor), so Remark 3.2 implies that elements of $\mathbb{F}_q[X]^{(q)}$ induce $\mathbb{F}_q$-linear maps. On the other hand, suppose $f \in \mathbb{F}_q[X]$ induces an $\mathbb{F}_q$-linear map $K^n \to K$, and let $X_1^{m_1} \cdots X_n^{m_n}$ be a monomial appearing in f. As K is an infinite field, the hypothesis implies that $f(X+Y) = f(X) + f(Y)$, where $Y := (Y_1, \ldots, Y_n)$ is a new list of variables. But then

$$(X_1 + Y_1)^{m_1} \cdots (X_n + Y_n)^{m_n} = X_1^{m_1} \cdots X_n^{m_n} + Y_1^{m_1} \cdots Y_n^{m_n} \tag{1}$$

since the lefthandside exactly contains all terms $X_1^{\alpha_1} Y_1^{\beta_1} \cdots X_n^{\alpha_n} Y_n^{\beta_n}$ in $f(X+Y)$ such that $\alpha_i + \beta_i = m_i$ for all i. Now suppose we have $i \neq j$ such that both $m_i > 0$ and $m_j > 0$. Substituting $X_i = Y_j = 0$ in (1), we get that

$$Y_i^{m_i} X_j^{m_j} \prod_{k \neq i,j} (X_k + Y_k)^{m_k} = 0$$

which is a contradiction. Thus, only one of the m_i is positive, *i.e.* the monomial under consideration is a power of one of the X_i. As a result, $f = f_1 + \cdots + f_n$ with $f_i \in K[X_i]$ for all i. We may even assume that $f_1(0) = \cdots = f_n(0) = 0$, since the hypothesis on f implies that it has no constant term. Then each f_i induces an $\mathbb{F}_q$-linear map $K \to K$ (the composition of f and the embedding $K \to K^n$, $\alpha \mapsto \alpha e_i$). Remark 3.2 now implies that $f \in \mathbb{F}_q[X]^{(q)}$.

The composition of linearized polynomial maps gives another one: if $Z := (Z_1, \ldots, Z_l)$ is another list of variables, then the composition (already defined for polynomial maps in general) of $f = (f_1, \ldots, f_m) \in (\mathbb{F}_q[X]^{(q)})^m$ and $g = (g_1, \ldots, g_n) \in (\mathbb{F}_q[Z]^{(q)})^n$ is the element $f \circ g = (f_1(g_1, \ldots, g_n), \ldots, f_m(g_1, \ldots, g_n))$, which can easily be shown to be an element of $(\mathbb{F}_q[Z]^{(q)})^m$. For the case $m = n$ this implies that $(\mathbb{F}_q[X]^{(q)})^n$ is closed under composition. Also, Theorem 4.2 will show that $\mathrm{GA}_n(\mathbb{F}_q)^{(q)} := \mathrm{GA}_n(\mathbb{F}_q) \cap (\mathbb{F}_q[X]^{(q)})^n$ is a subgroup of $\mathrm{GA}_n(\mathbb{F}_q)$.

Theorem 3.7 will show that we can view polynomial maps in $(\mathbb{F}_q[X]^{(q)})^m$ as matrices having univariate polynomials over $\mathbb{F}_q$ as entries. To make this explicit, we define the q-Jacobian of polynomial maps of this form. The definition is based on certain maps δ_j (one for each variable X_j) that are very similar to the map δ of Theorem 3.3.

Definition 3.5. Let $f = (f_1, \ldots, f_m) \in (\mathbb{F}_q[X]^{(q)})^m$, and t a new variable. For each $j \in \{1, \ldots, n\}$, let $\delta_j : \mathbb{F}_q[X]^{(q)} \to \mathbb{F}_q[t]$ be the $\mathbb{F}_q$-linear map uniquely determined by

$$\delta_j\left(X_i^{q^m}\right) = \begin{cases} t^m & i = j \\ 0 & i \neq j \end{cases} \qquad (m = 0, 1, 2, \ldots)$$

Furthermore, we define $\mathrm{J}_q(f)$ as the matrix $(\delta_j(f_i)) \in \mathrm{M}_{m \times n}(\mathbb{F}_q[t])$, and call it the *q-Jacobian* of f (or "*J-q-bian*").

Remark 3.6. The map

$$\begin{array}{ccc} (\mathbb{F}_q[X]^{(q)})^m & \longrightarrow & \mathrm{M}_{m\times n}(\mathbb{F}_q[t]) \\ (f_1,\ldots,f_m) & \mapsto & \mathrm{J}_q(f) \end{array}$$

is obviously one-to-one and onto. We will need this fact henceforth.

Now let $g=(g_1,\ldots,g_n)\in(\mathbb{F}_q[Z]^{(q)})^n$. We will denote the maps $\mathbb{F}_q[Z]^{(q)}\to\mathbb{F}_q[t]$ (similarly defined as the δ_j) by ε_j. In this situation we have

Theorem 3.7. *If $f=(f_1,\ldots,f_m)\in(\mathbb{F}_q[X]^{(q)})^m$ and $g=(g_1,\ldots,g_n)\in(\mathbb{F}_q[Z]^{(q)})^n$, then $\mathrm{J}_q(f\circ g)=\mathrm{J}_q(f)\,\mathrm{J}_q(g)$.*

In particular, J_q induces an isomorphism of $\mathbb{F}_q$-algebras $(\mathbb{F}_q[X]^{(q)})^n\xrightarrow{\sim}\mathrm{M}_n(\mathbb{F}_q[t])$.

Proof. Write $f_i=\sum_{k=1}^n f_i^{(k)}(X_k)$ and $g_i=\sum_{r=1}^l g_i^{(l)}(Z_r)$ for all i. Then

$$f_i(g)=\sum_{k=1}^n f_i^{(k)}(g_k)=\sum_{k=1}^n f_i^{(k)}(\sum_{r=1}^l g_k^{(r)}(Z_r))=\sum_{r=1}^l\sum_{k=1}^n f_i^{(k)}(g_k^{(r)}(Z_r))$$

and thus the (i,j)-entry of $\mathrm{J}_q(f(g))$ equals

$$\begin{aligned} \varepsilon_j(f_i(g))=\varepsilon_j\,(\sum_{k=1}^n f_i^{(k)}(g_k^{(j)}(Z_j))) &= \sum_{k=1}^n \varepsilon_j\,(f_i^{(k)}(Z_j))\cdot\varepsilon_j\,(g_k^{(j)}(Z_j)) \\ &= \sum_{k=1}^n \delta_k\,(f_i^{(k)}(X_k))\cdot\varepsilon_j\,(g_k) \\ &= \sum_{k=1}^n \delta_k\,(f_i)\cdot\varepsilon_j\,(g_k) \end{aligned}$$

which is exactly equal to the (i,j)-entry of the product $(\delta_j(f_i))\cdot(\varepsilon_j(g_i))$. Thus, $\mathrm{J}_q(f(g))=\mathrm{J}_q(f)\cdot\mathrm{J}_q(g)$. The second statement follows from Remark 3.6. □

4 The famous problems and conjectures for linearized polynomials

This section is devoted to the solutions that we found for the famous problems and conjectures that were stated in the Introduction, for the cases where the involved polynomials are linearized polynomials.

4.1 Tame Generators Problem and Jacobian Conjecture

Before solving the Tame Generators Problem for linearized polynomial maps, we recall the concept of tameness.

Definition 4.1. $\mathrm{EA}_n(K)$ (for any field K) is the subgroup of $\mathrm{GA}_n(K)$ generated by the elementary automorphisms. An *elementary* automorphism is one of the form $(X_1, \ldots, X_{i-1}, X_i + f_i, X_{i+1}, \ldots, X_n)$ for some i, where $f_i \in K[\hat{X}_i]$. Furthermore, $\mathrm{TA}_n(K)$, the group of *tame* automorphisms, is the subgroup generated by $\mathrm{GL}_n(K)$ and $\mathrm{EA}_n(K)$.

As mentioned in the Introduction, the question which automorphisms are tame is still open in general if $n \geq 3$. However, Theorem 4.2 will show that all invertible linearized polynomial maps are tame. To formulate the precise statement, we need to define a few automorphism subgroups consisting of linearized polynomial maps. First, we put

$$\mathrm{EA}_n(\mathbb{F}_q)^{(q)} := \langle\, (X_1, \ldots, X_{i-1}, X_i + f_i, X_{i+1}, \ldots, X_n) \mid 1 \leq i \leq n, f_i \in \mathbb{F}_q[\hat{X}_i]^{(q)} \,\rangle$$

Furthermore, let $\mathrm{TA}_n(\mathbb{F}_q)^{(q)} := \langle\, \mathrm{EA}_n(\mathbb{F}_q)^{(q)}, \mathrm{GL}_n(\mathbb{F}_q) \,\rangle$. Under the isomorphism of Theorem 3.7, the subgroup $\mathrm{EA}_n(\mathbb{F}_q)^{(q)}$ corresponds to $\mathrm{E}_n(\mathbb{F}_q[t])$, the subgroup of $\mathrm{GL}_n(\mathbb{F}_q[t])$ generated by all elementary matrices. Also, this isomorphism is the identity on $\mathrm{GL}_n(\mathbb{F}_q)$.

Theorem 4.2. *Let $f = (f_1, \ldots, f_m) \in (\mathbb{F}_q[X]^{(q)})^m$. Then there exist $h_1 \in \mathrm{TA}_m(\mathbb{F}_q)^{(q)}$ and $h_2 \in \mathrm{TA}_n(\mathbb{F}_q)^{(q)}$ such that $h_1 f h_2$ is a "diagonal map",* i.e. *a map of the form $g = (g_1, \ldots, g_m)$, where $g_i \in \mathbb{F}_q[X_i]^{(q)}$ for all i (and $g_i = 0$ if $m > n$ and $n < i \leq m$).*
Furthermore, $\mathrm{GA}_n(\mathbb{F}_q)^{(q)} = \mathrm{TA}_n(\mathbb{F}_q)^{(q)}$.

Proof. $\mathrm{J}_q(f)$ is a matrix over a Euclidean domain, so there exist $M \in \mathrm{GL}_m(\mathbb{F}_q[t])$ $(= \langle \mathrm{E}_m(\mathbb{F}_q[t]), \mathrm{GL}_m(\mathbb{F}_q) \rangle)$ and $N \in \mathrm{GL}_n(\mathbb{F}_q[t])$ such that $M\,\mathrm{J}_q(f)N$ is a (in general non-square) diagonal matrix. By Remark 3.6, there exist $h_1 \in \mathrm{TA}_m(\mathbb{F}_q)^{(q)}$ and $h_2 \in \mathrm{TA}_n(\mathbb{F}_q)^{(q)}$ such that $h_1 f h_2$ is of the prescribed form. For the next statement, suppose $f \in \mathrm{GA}_n(\mathbb{F}_q)^{(q)}$. The above says that f is tamely equivalent to a map $g = (g_1, \ldots, g_n)$ with $g_i \in \mathbb{F}_q[X_i]^{(q)}$ for all i. Since f is an automorphism, g is too, so let $h = (h_1, \ldots, h_n) \in \mathrm{GA}_n(\mathbb{F}_q)$ be the inverse of g. Since $\mathbb{F}_q[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ is a domain, the equations $g_i(h_i(X)) = X_i$ imply that $h_i \in \mathbb{F}_q[X_i]$ and that both g_i and h_i have degree 1 (for all i). Consequently, $f \in \mathrm{TA}_n(\mathbb{F}_q)^{(q)}$. □

Note that this theorem in particular implies that $f^{-1} \in \mathrm{GA}_n(\mathbb{F}_q)^{(q)}$ if $f \in \mathrm{GA}_n(\mathbb{F}_q)^{(q)}$, *i.e.* $\mathrm{GA}_n(\mathbb{F}_q)^{(q)}$ is a subgroup of $\mathrm{GA}_n(\mathbb{F}_q)$. As a result, we can affirm an analogue of the Jacobian Conjecture for linearized polynomial maps and their q-Jacobians.

Corollary 4.3. *$f \in (\mathbb{F}_q[X]^{(q)})^n$ is an automorphism if and only if $\mathrm{J}_q(f) \in \mathrm{GL}_n(\mathbb{F}_q[t])$.*

Proof. This follows from Theorem 3.7 and Theorem 4.2: if $f \in \mathrm{GA}_n(\mathbb{F}_q)^{(q)}$ then $f^{-1} \in \mathrm{GA}_n(\mathbb{F}_q)^{(q)}$ and $\mathrm{J}_q(f)\,\mathrm{J}_q(f^{-1}) = \mathrm{J}_q(ff^{-1}) = I_n$. If on the other hand $\mathrm{J}_q(f) \in \mathrm{GL}_n(\mathbb{F}_q[t])$, let $g \in (\mathbb{F}_q[X]^{(q)})^n$ such that $\mathrm{J}_q(g) = (\mathrm{J}_q(f))^{-1}$ (which exists by Remark 3.6). Then $\mathrm{J}_q(fg) = \mathrm{J}_q(f)\,\mathrm{J}_q(g) = I_n$ implies that f is an automorphism with inverse g. □

Note that if we take the *usual* Jacobian, the statement doesn't hold; namely, the Jacobian of any linearized polynomial map equals the Jacobian of its linear part.

4.2 Coordinate Recognition Problem

Corollary 4.3 provides us with the following useful tool: a criterion to decide whether a linearized polynomial is a coordinate.

Proposition 4.4. *For $f_1 \in \mathbb{F}_q[X]^{(q)}$, the following are equivalent.*

1. *f_1 is a coordinate of an automorphism in $\mathbb{F}_q[X]^n$*
2. *f_1 is a coordinate of an automorphism in $(\mathbb{F}_q[X]^{(q)})^n$*
3. *$(\delta_1(f_1), \ldots, \delta_n(f_1)) = (1)$ in $\mathbb{F}_q[t]$*

Proof of the equivalence of 2. and 3. f_1 is a coordinate in $(\mathbb{F}_q[X]^{(q)})^n$ if and only if $(\delta_1(f_1), \ldots, \delta_n(f_1))$ is a row that is extendible to a matrix in $\mathrm{GL}_n(\mathbb{F}_q[t])$ if and only if $(\delta_1(f_1), \ldots, \delta_n(f_1)) = (1)$ in $\mathbb{F}_q[t]$. (We use Remark 3.6 again.) □

From this we obtain the remarkable fact (Corollary 4.5) that all prime power polynomials are essentially univariate (*i.e.*, up to a polynomial transformation). This fact in turn will help us complete the proof of Proposition 4.4.

Corollary 4.5. *Every element of $\mathbb{F}_q[X]^{(q)}$ is a linearized polynomial in a coordinate of an automorphism in $(\mathbb{F}_q[X]^{(q)})^n$.*

Proof. Let $f \in \mathbb{F}_q[X]^{(q)}$, and $h := \gcd(\delta_1(f), \ldots, \delta_n(f)) \in \mathbb{F}_q[t]$ (unique if we assume h to be a monic polynomial). Then we have $(\delta_1(f), \ldots, \delta_n(f)) = (h)$ (as ideals in $\mathbb{F}_q[t]$), and we can write $\delta_i(f) = hg_i$ with $g_1, \ldots, g_n \in \mathbb{F}_q[t]$. Now let $\tilde{f}_i \in \mathbb{F}_q[X_i]^{(q)}$ ($i = 1, \ldots, n$) and $\tilde{h} \in \mathbb{F}_q[X_1]^{(q)}$ such that $\delta_i(\tilde{f}_i) = g_i(t)$ and $\mathrm{J}_q(\tilde{h}) = h(t)$ (using Remark 3.6 again). Then $\tilde{f} := \tilde{f}_1 + \cdots + \tilde{f}_n$ gives

$$\mathrm{J}_q(f) = (\delta_1(f) \ \cdots \ \delta_n(f)) = (hg_1 \ \cdots \ hg_n) = h \cdot (g_1 \ \cdots \ g_n) = \mathrm{J}_q(\tilde{h})\,\mathrm{J}_q(\tilde{f}) = \mathrm{J}_q(\tilde{h}(\tilde{f}))$$

Hence, $f = \tilde{h}(\tilde{f})$, and $(\delta_1(\tilde{f}), \ldots, \delta_n(\tilde{f})) = (g_1, \ldots, g_n) = (1)$ in $\mathbb{F}_q[t]$, so $\tilde{f}$ is a coordinate by the equivalence of *2.* and *3.* in Proposition 4.4. □

Proof of the equivalence of 1. and 2.(Proposition 4.4). The only nontrivial implication is *1.* $\Rightarrow$ *2.*, so assume that f_1 is a coordinate of an automorphism in $\mathbb{F}_q[X]^n$. By Corollary 4.5, $f_1 = g_1(h_1)$ with $g_1 \in \mathbb{F}_q[X_1]^{(q)}$ and $h_1 \in \mathbb{F}_q[X]^{(q)}$, and such that h_1 is the first coordinate of an automorphism in $(\mathbb{F}_q[X]^{(q)})^n$. Applying the inverse of this automorphism to f_1, we deduce that $g_1(X_1)$ is a coordinate as well. Just as in the proof of Theorem 4.2, this implies that g_1 has degree 1, say $g_1(X_1) = aX_1 + b$ with $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. But $g_1 \in \mathbb{F}_q[X_1]^{(q)}$, so $b = 0$. Now $f_1 = ah_1$ is the first coordinate of an automorphism in $(\mathbb{F}_q[X]^{(q)})^n$. □

One can write down many coordinates over finite fields of *such* a form, that they can't possibly be coordinates when considered over a field of characteristic zero. This is illustrated in the following example. A polynomial as described there, *i.e.* of the form $\tilde{f} := f(X) + Y^{q^n}$, can only be a coordinate over a characteristic zero field K in the trivial cases $n = 0$ or f has degree 1 (as will follow from Proposition 5.12).

Example 4.6. Any element of $\mathbb{F}_q[X,Y]^{(q)}$ (two variables) of the form $f(X)+Y^{q^n}$, with $n \geq 0$ and linear part of f equal to X, is a coordinate. Namely, let $g(X) := f(X)-X \in \mathbb{F}_q[X]^{(q)}$. Note that $g(X) = h(X)^q$ for some $h \in \mathbb{F}_q[X]^{(q)}$ (for g contains no linear term), whence $\hat{g}(t) := \delta_1(g(X)) = \delta_1(X^q)\delta_1(h(X)) = t\hat{h}(t)$, where $\hat{h}(t) := \delta_1(h(X))$. Thus,

$$\begin{pmatrix} 1+\hat{g}(t) & t^n \\ (-1)^{n+1}\hat{h}(t)^n & \frac{1-(-\hat{g}(t))^n}{1-(-\hat{g}(t))} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q[t])$$

Note that the lower right entry is indeed an element of $\mathbb{F}_q[t]$: it equals the finite geometric series $1-\hat{g}(t)+\hat{g}(t)^2-\cdots+(-1)^{n-1}\hat{g}(t)^{n-1}$. From the above we obtain

$$(f(X)+Y^{q^n}, (-1)^{n+1}h(X)^{(n)} + \sum_{k=0}^{n-1}(-1)^k g(Y)^{(k)}) \in \mathrm{GA}_2(\mathbb{F}_q)$$

where each exponent "(k)" of a polynomial denotes k-fold composition of that polynomial with itself (and $g(Y)^{(0)} := Y$). In particular, $h(X) := X^{q^{m-1}}$ $(m \geq 1)$ gives

$$(X + X^{q^m} + Y^{q^n}, (-1)^{n+1}X^{q^{(m-1)n}} + \sum_{k=0}^{n-1}(-1)^k Y^{q^{km}}) \in \mathrm{GA}_2(\mathbb{F}_q)$$

Assuming $m, n \geq 2$, and writing $n = rm + s$ with $r \in \mathbb{N}$ and $0 \leq s \leq m-1$, we can also complete this automorphism using a polynomial of lower degree. Namely,

$$(X + X^{q^m} + Y^{q^n}, (-1)^r X^{q^{m-s}} + \sum_{k=0}^{r}(-1)^k Y^{q^{km}}) \in \mathrm{GA}_2(\mathbb{F}_q)$$

since

$$\begin{pmatrix} 1+t^m & t^n \\ (-1)^r t^{m-s} & \frac{1-(-t^m)^{r+1}}{1-(-t^m)} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q[t])$$

4.3 Polynomial Ring Recognition Problem and Abhyankar-Sathaye Conjecture

A finitely generated K-algebra A can be represented as $A = K[X]/I$, where I is an ideal of $K[X]$. A necessary condition for being a polynomial ring over K is that A is a domain, whence I must be a prime ideal. If K is a finite field and I is generated by linearized polynomials, we will show that the condition of being a domain is actually also sufficient (Corollary 4.10). This differs significantly from the characteristic zero case, which has only been solved in case X represents at most two variables. We will first summarize the results of this case.

To begin, if I is even a maximal ideal, then $K[X]/I$ is a field, which is of course only a polynomial ring over K if it equals K (the units of both fields must coincide). In other words, the canonical embedding $K \to K[X]/I$ is actually an isomorphism. In this case, choosing $a_1, \ldots, a_n \in K$ such that $X_i - a_i \in I$ for all i (which exist since the embedding is onto), we get that $I = (X_1 - a_1, \ldots, X_n - a_n)$. So in case of a maximal ideal I, A is a polynomial ring if and only if I is of this form.

This also solves the general case $n = 1$, since any nonzero prime ideal of $K[X]$ is then maximal. And in the case of two variables, any non-maximal, nonzero prime ideal of $K[X]$ is generated by one irreducible polynomial (since $K[X]$ is a factorial ring). Hence, the following result, proved by Abhyankar and Moh in [1] and independently by Suzuki in [27], completes the solution of the two-variable Polynomial Ring Recognition Problem over a field of characteristic zero.

Theorem 4.7 (Abhyankar-Moh-Suzuki)**.** *Let K a field with* $\mathrm{char}(K) = 0$*. If a polynomial $f_1 \in K[X, Y]$ satisfies $K[X, Y]/(f_1) \cong_K K[Z]$, then f_1 is a coordinate.*

Contrary to the characteristic zero case, several counterexamples to Theorem 4.7 have been found in characteristic $p > 0$. Here is one which was also mentioned in [20].

Example 4.8. Take any prime number $p > 2$, and let $f_1 := Y^{p^2} - X^{2p} - X$. Then $\mathbb{F}_p[X, Y]/(f_1) \cong \mathbb{F}_p[T]$, where T is a variable; this isomorphism is induced by $\varphi : \mathbb{F}_p[X, Y] \to \mathbb{F}_p[T],\ X \mapsto T^{p^2}, Y \mapsto T^{2p} + T$. But we claim that f_1 is not a coordinate.

First, note that φ is indeed surjective since $f_2 := Y-(Y^p-X^2)^2$ satisfies $\varphi(f_2) = T$. Now we show that $\mathrm{Ker}(\varphi) = (f_1)$. Since the (Krull) dimensions of $\mathbb{F}_p[X, Y]$ and $\mathbb{F}_p[T]$ are equal to 2 resp. 1, $\mathrm{Ker}(\varphi)$ must be a height 1 prime ideal, and thus a principal ideal due to the factoriality of $\mathbb{F}_p[X, Y]$. So it suffices to show that f_1 is irreducible over $\mathbb{F}_p$. So let β be an element of an extension field of $K := \mathbb{F}_p(X)$ such that $\beta^{p^2} = \alpha := X^{2p} + X$. Then $f_1 = Y^{p^2} - \alpha = (Y - \beta)^{p^2}$ over $K(\beta)$. Let $1 \le m \le p^2$ be minimal such that $(Y - \beta)^m \in K[Y]$. Then $(Y - \beta)^m$ is irreducible over K, and in fact the only irreducible factor of f_1 (since two positive powers of $Y - \beta$ cannot be coprime). Hence f_1 is a power of $(Y-\beta)^m$, and $m \mid p^2$. Now suppose $m = 1$ or $m = p$. Then $Y^p - \beta^p = (Y - \beta)^p \in K[Y]$, so $\alpha = (\beta^p)^p \in K^p = \mathbb{F}_p(X^p)$, a contradiction. As a result, $m = p^2$, and the conclusion is that f_1 is irreducible over K.

Now suppose f_1 is a coordinate. Using the fact that $\mathbb{F}_p$ is a field, Corollary 5.1.6 in [10] yields an $f_2' \in \mathbb{F}_p[X, Y]$ with $\deg(f_2') < \deg(f_1)$ and $(f_1, f_2') \in \mathrm{GA}_2(\mathbb{F}_p)$. (Here "deg" denotes the (total) degree of a polynomial.) Since $\mathbb{F}_p[X, Y]/(f_1) = \mathbb{F}_p[f_1, f_2']/(f_1) = \mathbb{F}_p[\overline{f_2'}]$ ($\overline{f_2'}$ being the equivalence class of f_2' modulo (f_1)), we must have $\mathbb{F}_p[\varphi(f_2')] = \mathbb{F}_p[T]$, whence $\varphi(f_2') = aT + b$ with $a \in \mathbb{F}_p^*, b \in \mathbb{F}_p$. But $\varphi(f_2) = T$, which implies that $f_2' - af_2 - b \in \mathrm{Ker}(\varphi) = (f_1)$. From $\deg(f_2' - af_2 - b) < \deg(f_1)$ we now conclude that $f_2' - af_2 - b = 0$. Thus, $(f_1, f_2) \in \mathrm{GA}_2(\mathbb{F}_p)$. But according to Corollary 5.1.6 in [10] either $\deg(f_1) \mid \deg(f_2)$ or $\deg(f_2) \mid \deg(f_1)$, contradicting the fact that $\deg(f_1) = p^2$ and $\deg(f_2) = 2p$.

Theorem 4.9 is the key to the solution of the Polynomial Ring Recognition Problem for $\mathbb{F}_q$-algebras which are defined by linearized polynomials (Corollary 4.10).

Theorem 4.9. *Let $\mathfrak{p}$ be a prime ideal in $\mathbb{F}_q[X]$ generated by linearized polynomials. Then these polynomials can be chosen in such a way that together they are extendible to an automorphism in* $\mathrm{GA}_n(\mathbb{F}_q)^{(q)}$*.*

More generally, let $\mathfrak{a}$ be any ideal in $\mathbb{F}_q[X]$ generated by linearized polynomials. Then there exist $h = (h_1, \ldots, h_n) \in \mathrm{GA}_n(\mathbb{F}_q)^{(q)}$, $r \le n$ and $g_i \in \mathbb{F}_q[X_i]^{(q)} \backslash \{0\}$ for $i = 1, \ldots, r$, such that $\mathfrak{a} = (g_1(h_1), \ldots, g_r(h_r))$.

Proof. We first derive the first statement from the second one. Given $\mathfrak{p}$, let h and $g_1, \ldots, g_r \neq 0$ as in the second statement such that $\mathfrak{p} = (g_1(h_1), \ldots, g_r(h_r))$. Applying h^{-1} to $\mathfrak{p}$, we may even assume that $\mathfrak{p} = (g_1(X_1), \ldots, g_r(X_r))$. For $i \in \{1, \ldots, r\}$ we write $g_i(X_i) = X_i^{e_i}\tilde{g}_i(X_i)$ with $\tilde{g}_i \in \mathbb{F}_q[X_i]$, $\tilde{g}_i(0) \neq 0$ and $e_i > 0$ (note that $g_i \in \mathbb{F}_q[X_i]^{(q)}$, so indeed $g_i \in (X_i)$). Since $g_0(0) = 0$ for all $g_0 \in \mathfrak{p}$, we must have $\tilde{g}_i(X_i) \notin \mathfrak{p}$, whence $X_i \in \mathfrak{p}$ (since $\mathfrak{p}$ is a prime ideal). Substituting $X_j := 0$ for all $j \neq i$, we obtain $X_i \in (X_i^{e_i}\tilde{g}_i(X_i))$. This implies that $e_i = 1$ and $\tilde{g}_i(X_i) \in \mathbb{F}_q^*$. Consequently, $\mathfrak{p} = (X_1, \ldots, X_r)$.

Now we prove the second statement. First note that $\mathfrak{a}$ is generated by *finitely many* linearized polynomials. Namely, $\mathfrak{a}$ is generated by finitely many general polynomials (since $\mathfrak{a}$ is an ideal in a Noetherian ring), and each of these general polynomials can be

written as an $\mathbb{F}_q[X]$-linear combination of finitely many of the linearized polynomials that generate $\mathfrak{a}$. These together form the announced finite generating set.

So let $\mathfrak{a} = (f_1, \ldots, f_m)$ for some $m \in \mathbb{N}$ and $f_1, \ldots, f_m \in \mathbb{F}_q[X]^{(q)}$. By Theorem 4.2, there exist $h \in \mathrm{TA}_n(\mathbb{F}_q)^{(q)}$ and $\tilde{h} \in \mathrm{TA}_m(\mathbb{F}_q)^{(q)}$ such that $g := \tilde{h}fh^{-1}$ has the form $g = (g_1, \ldots, g_m)$, where $g_i \in \mathbb{F}_q[X_i]^{(q)}$ for all i (and $g_i = 0$ if $m > n$ and $n < i \leq m$). Modifying h and $\tilde{h}$ by a suitable permutation of the variables, we may assume that $g_1, \ldots, g_r \neq 0$ and $g_{r+1} = \cdots = g_m = 0$ for some $0 \leq r \leq \min\{m, n\}$. Since

$$\begin{aligned}(\tilde{h}_1(f), \ldots, \tilde{h}_m(f)) &= ((\tilde{h}f)_1, \ldots, (\tilde{h}f)_m) &&= ((gh)_1, \ldots, (gh)_m) \\ &&&= (g_1(h_1), \ldots, g_r(h_r))\end{aligned}$$

we are done as soon as we show that $\mathfrak{a} = (\tilde{h}_1(f), \ldots, \tilde{h}_m(f))$. Well then, we have $\tilde{h}_i(0) = 0$ for all i, whence $(\tilde{h}_1(f), \ldots, \tilde{h}_m(f)) \subseteq (f_1, \ldots, f_m)$. Likewise,

$$\begin{aligned}(f_1, \ldots, f_m) &= \Big(\big(\tilde{h}^{-1}\big)_1\big(\tilde{h}_1(f), \ldots, \tilde{h}_m(f)\big), \ldots, \big(\tilde{h}^{-1}\big)_m\big(\tilde{h}_1(f), \ldots, \tilde{h}_m(f)\big)\Big) \\ &\subseteq (\tilde{h}_1(f), \ldots, \tilde{h}_m(f))\end{aligned}$$

and thus $\mathfrak{a} = (f_1, \ldots, f_m) = (\tilde{h}_1(f), \ldots, \tilde{h}_m(f))$. □

Corollary 4.10. *Let $A = \mathbb{F}_q[X]/I$ be a finitely generated $\mathbb{F}_q$-algebra, where I is an ideal in $\mathbb{F}_q[X]$ generated by linearized polynomials. Then A is (isomorphic to) a polynomial ring over $\mathbb{F}_q$ if and only if A is a domain.*

Theorem 4.7 relates the Polynomial Ring Recognition Problem to the Coordinate Recognition Problem for the case of two variables. But this connection is in fact more general. Namely, it is easily seen, that if $f_1 \in K[X_1, \ldots, X_n]$ is a coordinate, then the K-algebra $K[X_1, \ldots, X_n]/(f_1)$ is a polynomial ring over K in $n-1$ variables. The reverse statement is the Abhyankar-Sathaye Conjecture, which in case $n = 2$ has an affirmative answer by Theorem 4.7. Although the Abhyankar-Sathaye Conjecture is false in nonzero characteristic in general (as shown in Example 4.8), the statement holds for linearized polynomials:

Theorem 4.11. *If $f_1 \in \mathbb{F}_q[X]^{(q)}$ satisfies $\mathbb{F}_q[X]/(f_1) \cong_{\mathbb{F}_q} \mathbb{F}_q[Y_1, \ldots, Y_{n-1}]$, then f_1 is a coordinate.*

Proof. According to Corollary 4.5, $f_1 = g_1(h_1)$, where h_1 is a coordinate in $\mathbb{F}_q[X]^{(q)}$ and $g_1 \in \mathbb{F}_q[X_1]^{(q)}$. Then $g_1(0) = 0$, so h_1 divides f_1. Additionally, (f_1) is a prime ideal (as $\mathbb{F}_q[Y_1, \ldots, Y_{n-1}]$ is a domain), whence $f_1 = ch_1$ for some $c \in \mathbb{F}_q^*$. Thus, f_1 is a coordinate. □

4.4 Linearization Conjecture

The Linearization Conjecture doesn't hold in general in positive characteristic, which is demonstrated in the following example. Throughout this section, X (and also Y) denotes one variable.

Example 4.12. $f := (X + Y^2, Y) \in \mathrm{GA}_2(\mathbb{F}_2)$ has order 2, but is not linearizable. This already follows from two obvious facts about f: its linear part equals the identity, and $f(0) = 0$. Namely, suppose $g \in \mathrm{GA}_2(\mathbb{F}_2)$ such that $gfg^{-1} = l \in \mathrm{GL}_2(\mathbb{F}_2)$, and let $c := g(0)$. Then $\tilde{g} := (X - c_1, Y - c_2) \circ g$ satisfies $\tilde{g}(0) = 0$, and

$$\tilde{g}f\tilde{g}^{-1} = (X - c_1, Y - c_2)l(X + c_1, Y + c_2) \tag{2}$$

Since f and $\tilde{g}$ have zero constant part, we can find the linear part of the lefthandside of (2) by composing the linear parts of the factors of this composition. Hence, the linear part of the lefthandside equals the identity. Looking at the righthandside of (2), we conclude that $l = (X, Y)$. But then also $f = (X, Y)$, a contradiction.

In view of this example, a question arises: is the Linearization Conjecture true in nonzero characteristic if we additionally assume that the characteristic doesn't divide the order of the automorphism? For linearized polynomial maps, this question has an affirmative answer (Corollary 4.18). Because of Theorem 3.7, the proof of this fact involves matrices in $\mathrm{GL}_n(K[t])$ satisfying a polynomial relation over K.

Lemma 4.13. *Let R be a domain containing a field K, such that K is integrally closed in L, the field of fractions of R. Furthermore, let $h(X) \in R[X]$ be the characteristic polynomial of a given $A \in \mathrm{GL}_n(R)$, and $g(X) \in L[X]$ the minimal polynomial of A over L. Suppose $f(A) = 0$ for some $f(X) \in K[X]$. Then also $g(X), h(X) \in K[X]$.*

Proof. $g(X)$ divides $f(X)$ in $L[X]$. Let L' be a splitting field of f over L. Since $f(X) \in K[X]$, the roots of f in L' (and in particular those of g) are integral over K, whence the coefficients of g are too. Moreover, $h(X)$ has the same roots as $g(X)$, so the coefficients of h are integral over K as well. But K is integrally closed in L, so $g(X), h(X) \in K[X]$. □

Proposition 4.14. *Suppose $A \in \mathrm{GL}_n(K[t])$ satisfies $f(A) = 0$ for some $f \in K[X]$, $f \neq 0$. Furthermore, write $f = f_1 \cdots f_r$, with $f_1, \ldots, f_r \in K[X]$ mutually coprime. Then $K[t]^n = \mathrm{Ker}(f_1(A)) \oplus \cdots \oplus \mathrm{Ker}(f_n(A))$, and A is conjugate over $K[t]$ to a block diagonal matrix, with blocks $A_1, \ldots, A_r$ satisfying $f_i(A_i) = 0$ for all i.*

Moreover, if f is the minimal (resp. characteristic) polynomial of A, and each f_i is monic, then f_i is the minimal (resp. characteristic) polynomial of A_i for all i.

Proof. Consider the ideals $\mathfrak{a}_i := (f_i) \subseteq K[X]$. Then $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ for all $i \neq j$. Note that the ideals $\hat{\mathfrak{a}_i} := \mathfrak{a}_1 \cdots \mathfrak{a}_{i-1}\mathfrak{a}_{i+1} \cdots \mathfrak{a}_r$ satisfy

$$(1) = \prod_{i<j} (\mathfrak{a}_i + \mathfrak{a}_j) \subseteq \hat{\mathfrak{a}_1} + \cdots + \hat{\mathfrak{a}_r}$$

whence $\hat{\mathfrak{a}_1} + \cdots + \hat{\mathfrak{a}_r} = (1)$. The above inclusion can be justified as follows: any term $\mathfrak{a}_{k_1} \cdots \mathfrak{a}_{k_m}$ in the product on the left (with $m := \frac{1}{2}r(r-1)$) originates from choices between the two terms in all factors $\mathfrak{a}_i + \mathfrak{a}_j$. Any term $\mathfrak{a}_{k_1} \cdots \mathfrak{a}_{k_m}$ must contain at least $r - 1$ of the $\mathfrak{a}_i$. Namely, given any $\mathfrak{a}_i$ and $\mathfrak{a}_j$ with $i \neq j$, the factor $\mathfrak{a}_i + \mathfrak{a}_j$ appears in the product, so at least one of the two must appear in the mentioned term. Therefore, $\mathfrak{a}_{k_1} \cdots \mathfrak{a}_{k_m} \subseteq \hat{\mathfrak{a}_i}$ for some i.

So let $g_1, \ldots, g_r \in K[X]$ such that $g_1\hat{f}_1 + \cdots + g_r\hat{f}_r = 1$, where for $i = 1, \ldots, r$, $\hat{f}_i := f_1 \cdots f_{i-1}f_{i+1} \cdots f_r$. We now claim that $K[t]^n = V_1 \oplus \cdots \oplus V_r$, where $V_i := \mathrm{Ker}(f_i(A))$ for all i. First, note that the V_i are A-invariant $K[t]$-submodules, and that they are all free modules, being submodules of a finite free module over a principal ideal domain. Second, for any $v \in K[t]^n$ we have

$$v \;=\; Iv \;=\; g_1(A)\hat{f}_1(A)v + \cdots + g_r(A)\hat{f}_r(A)v \;\in\; V_1 + \cdots + V_r$$

since $f_i(A)\hat{f}_i(A)v = f(A)v = 0$ for all i. Finally, to justify the direct sum notation, suppose $v_1 + \cdots + v_r = 0$ for certain $v_1 \in V_1, \ldots, v_r \in V_r$. Then each v_i satisfies

$$v_i = (g_1(A)\hat{f}_1(A) + \cdots + g_r(A)\hat{f}_r(A))v_i = g_i(A)\hat{f}_i(A)v_i = g_i(A)\hat{f}_i(A)(v_1 + \cdots + v_r) = 0$$

Now, for all $i \in \{1, \ldots, n\}$, let m_i be the rank of V_i as a free $K[t]$-module, and $A_i \in \mathrm{GL}_{m_i}(K[t])$ the matrix representation of the restriction of A to V_i, with respect to some basis of V_i. Taking these r bases together to form a new basis of $K[t]^n$, we see that A is conjugate over $K[t]$ to the block diagonal matrix A_0 with $A_1, \ldots, A_r$ on the diagonal. Also, $f_i(A_i) = 0$ since $f_i(A) = 0$ on V_i.

Now assume that each f_i is monic. It is obvious from the shape of A_0 that the characteristic polynomial of A_0 (which is also the characteristic polynomial of A) is equal to the product of the characteristic polynomials of the A_i. Also, the characteristic polynomial of A_i (an element of $K[X]$ by Lemma 4.13) must be a power of the same monic irreducible polynomial that f_i is also a power of. Hence, if f is the characteristic polynomial of A, then f_i is the characteristic polynomial of A_i.

Finally, assume that f is the minimal polynomial of A (which is also the minimal polynomial of A_0). Choose $j \in \{1, \ldots, r\}$. Suppose $h(A_j) = 0$ for some $h(X) \in K[X]$, and define $\hat{f} := f_1 \cdots f_{j-1} h f_{j+1} \cdots f_r$. Then $\hat{f}(A_0) = 0$, since it is the block diagonal matrix consisting of the blocks $\hat{f}(A_i)$. (And $f_i(A_i) = 0$ if $i \neq j$, and $h(A_i) = 0$ if $i = j$.) Whence, $f(X) \mid \hat{f}(X)$, *i.e.* $f_i(X) \mid h(X)$. So f_i must be the minimal polynomial of A_i. □

Theorem 4.15. *Let $A \in \mathrm{GL}_n(K[t])$ such that its minimal polynomial $g(X)$ over $K(t)$ is an irreducible polynomial in $K[X]$ of degree $d \geq 1$.*

1. *If g is separable over K, then A is conjugate (over $K[t]$) to the $n \times n$ block diagonal matrix where each block is the companion matrix of g.*
2. *If $d = n$ then A is conjugate (over $K[t]$) to the companion matrix of g.*

Proof. The characteristic polynomial of A (an element of $K[X]$ by Lemma 4.13) must be a power of g, say g^m with $m \in \mathbb{N}^*$ such that $n = dm$. Write $g(X) = X^d + c_{d-1}X^{d-1} + \cdots + c_1 X + c_0$, where $c_i \in K$ for all i. Moreover, let L denote the splitting field of g over K. Also, we use the following notation: if $K_1 \subseteq K_2$ are fields and $M \in \mathrm{M}_n(K_1[t])$, then $\mathrm{Ker}_{K_2}(M)$ denotes the kernel of the endomorphism of $K_2[t]^n$ induced by M. This kernel is then viewed as a $K_2[t]$-module. Furthermore, $M^\top$ denotes the transpose of any matrix M.

First, assume that g is separable over K. Then g has d distinct roots in L. Furthermore, L/K is a Galois extension, say with Galois group G. Since L is the splitting field of an irreducible polynomial over K, G acts transitively on the roots of g. Therefore, we can find $\sigma_1, \sigma_2, \ldots, \sigma_d \in G$ (with σ_1 the identity map) and $\alpha \in L$ such that $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ are the roots of g in L. Then $\mathrm{Ker}_L(A - \sigma_i(\alpha)I) = \tilde{\sigma}_i(\mathrm{Ker}_L(A - \alpha I))$, where the automorphism $\tilde{\sigma}_i$ is the natural extension of σ_i to $L[t]^n$ (preserving t). As a result, $\mathrm{Ker}_L(A - \sigma_1(\alpha)I), \ldots, \mathrm{Ker}_L(A - \sigma_d(\alpha)I)$ all have the same rank as free $L[t]$-modules. (Note that indeed they are all free modules, being submodules of a finite free module over a principal ideal domain.) Moreover, from Proposition 4.14 (over $L[t]$ instead of $K[t]$) we learn that $L[t]^n = \mathrm{Ker}_L(A - \sigma_1(\alpha)I) \oplus \cdots \oplus \mathrm{Ker}_L(A - \sigma_d(\alpha)I)$. Consequently, the rank of $\mathrm{Ker}_L(A - \sigma_i(\alpha)I)$ equals m for all i.

Again by Proposition 4.14 (and using the fact that g is separable over K), we know that $\mathrm{Ker}_{K(\alpha)}(A - \alpha I)$ is a direct summand of $K(\alpha)[t]^n$. Also, tensoring with a free (and thus flat) module preserves kernels, so we have $L \otimes_{K(\alpha)} \mathrm{Ker}_{K(\alpha)}(A - \alpha I) = \mathrm{Ker}_L(A - \alpha I)$. Hence, since $\mathrm{Ker}_{K(\alpha)}(A - \alpha I)$ is a free $K(\alpha)[t]$-module, its rank over $K(\alpha)[t]$ is equal to the rank of $\mathrm{Ker}_L(A - \alpha I)$ over $L[t]$, which is m.

Let $\{v_1, \ldots, v_m\}$ be a basis of $\mathrm{Ker}_{K(\alpha)}(A - \alpha I)$. Let $B \in \mathrm{M}_{n\times m}(K(\alpha)[t])$ be the matrix with $v_1, \ldots, v_m$ as its columns, which satisfies $AB = \alpha B$. Note that then

$$\mathrm{M}_n(K(\alpha)[t])B = \sum_{i=0}^{d-1} \mathrm{M}_n(K[t])\alpha^i B = \sum_{i=0}^{d-1} \mathrm{M}_n(K[t])A^i B \subseteq \mathrm{M}_n(K[t])B$$

whence $\mathrm{M}_n(K(\alpha)[t])B = \mathrm{M}_n(K[t])B$. Since $v_1, \ldots, v_m$ are the first m elements of a basis of $K(\alpha)[t]^n$, B can be completed to an invertible $n \times n$ matrix over $K(\alpha)[t]$. Taking together the first m rows of its inverse, we obtain a $B' \in \mathrm{M}_{m\times n}(K(\alpha)[t])$ such that $B'B = I_m$. Now define

$$E_\alpha := \begin{pmatrix} e_\alpha & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & e_\alpha \end{pmatrix} \in \mathrm{M}_{n\times m}(K(\alpha))$$

where $e_\alpha := (1\ \alpha \cdots \alpha^{d-1})^\top$ and each "0" is a column consisting of d zeroes. For every $n' \geq 1$ this gives an isomorphism of $K[t]$-modules

$$\begin{array}{ccc} \mathrm{M}_{n'\times n}(K[t]) & \longrightarrow & \mathrm{M}_{n'\times m}(K(\alpha)[t]) \\ N & \mapsto & NE_\alpha \end{array}$$

using the fact that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a $K[t]$-basis of $K(\alpha)[t]$. In particular, there exists a $D \in \mathrm{M}_n(K[t])$ such that $DE_\alpha = B$. But we claim that even $D \in \mathrm{GL}_n(K[t])$. Namely, $E_\alpha = (E_\alpha B')B \in \mathrm{M}_n(K(\alpha)[t])B = \mathrm{M}_n(K[t])B$, say $E_\alpha = D'B$ with $D' \in \mathrm{M}_n(K[t])$. Then $D'DE_\alpha = D'B = E_\alpha$, so $D'D = I_n$. As a result, $D'A(D')^{-1}E_\alpha = D'AB = D'\alpha B = \alpha D'B = \alpha E_\alpha$. It is also readily verified that $C^\top e_\alpha = \alpha e_\alpha$, where

$$C := \begin{pmatrix} 0 & \cdots & \cdots & 0 & -c_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -c_{d-1} \end{pmatrix}$$

is the companion matrix of g. Hence,

$$D'A(D')^{-1} = \begin{pmatrix} C^\top & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & C^\top \end{pmatrix}$$

Note that if in all of the above we replace A by C (so then $m = 1$), we obtain a proof of the fact that C is conjugate to $C^\top$. Combined with the above, this establishes the first statement of this theorem.

Now we turn to the second statement. To explain why we don't need separability in this case, note that in the proof of the first statement we only used the fact that the rank of $\mathrm{Ker}_{K(\alpha)}(A - \alpha I)$ is *at least* m. So if in the second case we can show directly that the rank is at least 1, we are done by copying the remainder of the proof of the first statement (with $m = 1$).

We will now show that $\mathrm{Ker}_{K(\alpha)}(A - \alpha I) \neq \{0\}$ (which proves that the rank is at least 1). Since $g(A) = (A - \alpha I)h(A)$ for some $h(X) \in K(\alpha)[X]$, $\mathrm{Ker}_{K(\alpha)}(A - \alpha I)$ contains the image of $h(A)$. So it suffices to show that $h(A) \neq 0$. To see this, note that $h(X) = \sum_{i=0}^{d-1} h_i(X)\alpha^i$, where $h_0, \ldots, h_{d-1} \in K[X]$ all have degree strictly less than d. So $h_i(A) \neq 0$ for all i, whence $h(A) \neq 0$. □

Remark 4.16. In Theorem 4.15 the assumption that the minimal polynomial is irreducible (instead of the more general case of being a power of an irreducible polynomial), is really necessary. Namely, suppose $A = I_n + tN$, where N is any nonzero nilpotent matrix in $\mathrm{M}_n(K)$. Then $(A - I_n)^n = 0$, so the minimal polynomial of A over $K(t)$ is a nontrivial power of $X - 1$ (and thus separable). However, A is not conjugate to an element of $\mathrm{GL}_n(K)$: for any $B \in \mathrm{GL}_n(K[t])$ we have $B^{-1}AB = I + tB^{-1}NB$, and $tB^{-1}NB \notin \mathrm{M}_n(K)$.

Corollary 4.17. *Let K be a field and $A \in \mathrm{GL}_n(K[t])$ satisfying $A^d = I_n$, where $\mathrm{char}(K) \nmid d$. Then there exists a $B \in \mathrm{GL}_n(K[t])$ such that $B^{-1}AB \in \mathrm{GL}_n(K)$.*

Proof. Note that the minimal polynomial of A over $K(t)$, say $g(X)$, is an element of $K[X]$ by Lemma 4.13, and of course a factor of $X^d - 1$. Since $\mathrm{char}(K) \nmid d$, $X^d - 1$ and its derivative have no common zero in an algebraic closure of K, so neither do g and g'. Hence, g is a product of mutually coprime monic irreducible polynomials, which are also separable. Using Proposition 4.14, we may reduce to the case that g is irreducible and separable. But this case is settled by Theorem 4.15. □

Theorem 3.7 now gives

Corollary 4.18. *If d and q are relatively prime and $f \in \mathrm{GA}_n(\mathbb{F}_q)^{(q)}$ has finite order d, then f is linearizable.*

5 Polynomial maps without mixed terms

In this final section we study all problems and conjectures mentioned in the Introduction for the case of a polynomial (map) *without mixed terms*. K will be a field, mostly of characteristic zero.

Definition 5.1. A polynomial $f_1 \in K[X]$ is said to be *without mixed terms* if we have $f_1 \in K[X_1] + \cdots + K[X_n]$. A polynomial map $(f_1, \ldots, f_n) \in K[X]^n$ (K a field) is *without mixed terms* if each of the f_i is.

Linearized polynomial maps are examples of polynomial maps without mixed terms. But the properties of linearized polynomial maps are very different from those of polynomial maps without mixed terms over a zero characteristic field. Namely, we have the following theorem. First, $\mathrm{BA}_n(K)$ is the subgroup of *triangular* automorphisms, *i.e.* all automorphisms $f = (f_1, \ldots, f_n)$ with $f_i - a_i X_i \in K[X_{i+1}, \ldots, X_n]$ and $a_i \in K^*$ for all i. (The notation comes from the fact that $\mathrm{BA}_n(K) \cap \mathrm{GL}_n(K)$ equals the Borel subgroup of $\mathrm{GL}_n(K)$.) Furthermore, such an f is called *unitriangular* if $a_1 = \cdots = a_n = 1$. $\mathrm{BA}_n^{(1)}(K)$ will be the subgroup of unitriangular automorphisms.

Theorem 5.2. *Let $f \in \mathrm{GA}_n(K)$ without mixed terms, and assume further that its linear part equals the identity. If K has characteristic zero, then there exists a permutation π of the X_i such that $\pi^{-1} f \pi$ is unitriangular.*

Furthermore, if K has characteristic $p > 0$, then there exists a permutation π of the X_i such that $\pi^{-1} f \pi \in \mathrm{BA}_n^{(1)}(K) + \left(K\left[X_1^p\right] + \cdots + K\left[X_n^p\right]\right)^n$.

Proof. The first statement is a direct consequence (using Jacobians) of Theorem 5.4, which considers certain matrices with entries in $K[X]$. In characteristic $p > 0$ we can use the same theorem, but we need to take into account that the ith partial derivative of a power X_i^m vanishes if and only if $p \mid m$. □

Note that, given any automorphism without mixed terms, we can compose it on the left with the inverse of its linear part, to obtain an automorphism satisfying all hypotheses of Theorem 5.2.

Definition 5.3. $A = (a_{ij}) \in \mathrm{M}_n(K[X])$ is a *matrix in separated variables* if $a_{ij} \in K[X_j]$ for all i and j. These matrices form a left $\mathrm{M}_n(K)$-submodule of $\mathrm{M}_n(K[X])$.

In the following, we use some well-known terminology from matrix theory: A *principal submatrix (of order k)* of a square matrix is a submatrix formed by a subset of (k) rows and the corresponding subset of columns. And a *principal (k-)minor* of a square matrix is the determinant of a principal submatrix (of order k).

Theorem 5.4. *Every matrix $A \in \mathrm{GL}_n(K[X])$ in separated variables with $A(0) = I_n$ is (after conjugation by a permutation matrix) unitriangular (upper triangular with only 1's on the diagonal).*

Proof. By Lemma 5.7, we are done if we can prove that all principal minors of A are equal to 1. First, note that $|A| \in K^*$ and $|A(0)| = 1$ together imply that $|A| = 1$. For all $1 \leq j \leq n$, let A_j be the matrix obtained from A by deleting its jth row and column. Note that $A_j \in \mathrm{M}_{n-1}(K[\hat{X}_j])$ is a matrix in seperated variables satisfying $A_j(0) = I_{n-1}$. Moreover, expanding the determinant of A along its jth column and substituting $X_j = 0$, we obtain $1 = |A_{|_{X_j=0}}| = a_{jj}(0) \cdot |A_j| = |A_j|$ ($A(0) = I_n$, so $a_{ij}(0) = 0$ whenever $i \neq j$).

From all this we may conclude that for every $A \in \mathrm{GL}_n(K[X])$ in separated variables satisfying $A(0) = I_n$, we have $|A| = 1$, each A_j is a matrix in $\mathrm{GL}_{n-1}(K[\hat{X}_j])$ in separated variables and $A_j(0) = I_{n-1}$. Induction now proves that for every matrix $A \in \mathrm{GL}_n(K[X])$ in separated variables satisfying $A(0) = I_n$, all principal minors are equal to 1. □

Remark 5.5. The proof of the above theorem in particular implies that all diagonal elements of A (being principal minors) are equal to 1. But this can also be proved directly. Namely, since $A(0) = I_n$, each non-diagonal entry a_{ij} satisfies $X_j \mid a_{ij}$. The fact that $A \in \mathrm{GL}_n(K[X])$ implies that $(a_{i1}(X_1), \ldots, a_{in}(X_n)) = (1)$ in $K[X]$ for all i. Substituting $X_j = 0$ for all $j \neq i$, we obtain $a_{ii} \in K^*$. But $A(0) = I_n$, whence $a_{11} = \cdots = a_{nn} = 1$.

Additionally, Theorem 5.4 partly solves the Jacobian Conjecture:

Corollary 5.6. *The Jacobian Conjecture is satisfied for polynomial maps without mixed terms.*

Proof. If f is a polynomial map without mixed terms satisfying $|\mathrm{J}\, f| \in K^*$, then also $|\mathrm{J}\, f(0)| \in K^*$, *i.e.* f has invertible linear part. Composing f on the left with the inverse of its linear part, we may assume that $\mathrm{J}\, f(0) = I_n$. According to Theorem 5.4, this means that f is unitriangular after a permutation of the variables. □

Lemma 5.7. *Let R be a domain. Suppose $A = (a_{ij}) \in \mathrm{GL}_n(R)$ has the property that all its principal minors are equal to 1. Then A is (after conjugation by a permutation matrix) unitriangular.*

Proof. We may assume that R is a field. Note that if all principal minors of a matrix equal 1, then any principal submatrix also has this property. Further, a column of a square matrix is called an *elementary column* if its diagonal entry equals 1 and all its remaining entries are 0. Note that the property of having an elementary column is invariant under conjugation by a permutation matrix. (Partly due to the fact that conjugation by a permutation matrix permutes the diagonal elements.)

We will prove the theorem by induction on n. It is trivial for $n = 1$. If $n = 2$ then $|A| = 1$ implies $a_{12}a_{21} = 0$, which also settles this case (as R is a field). So we will assume from now on that $n \geq 3$ and that the statement holds in lower dimensions. For all $1 \leq i \leq n$, let A_i be the matrix obtained from A by deleting its ith row and column. Note that we may apply the induction hypothesis to A_i.

We are done if A contains an elementary column: if this is the case, we may (after permutation) assume that the first column is elementary, and then apply the induction hypothesis to A_1 to obtain (after permutation) a unitriangular matrix.

Now we assume that A doesn't have an elementary column, and aim to arrive at a contradiction. Take $i \in \{1, \ldots, n\}$. By the induction hypothesis, A_i contains an elementary column. So there is a $j \neq i$ such that the jth column of A is "almost elementary", *i.e.* $a_{jj} = 1$ and $a_{kj} = 0$ for $k \notin \{i, j\}$. And $a_{ij} \neq 0$, as A has no elementary column. Associating a j to each i in this way, we obtain a map σ from $\{1, \ldots, n\}$ to itself. σ is obviously injective, and thus a permutation. Hence, $a_{ij} = 0$ for all i and j with $j \notin \{i, \sigma(i)\}$ (and $a_{ii} = 1$ for all i).

Using the induction hypothesis on A_n again, we may assume (after conjugation by a permutation matrix) that A_n is unitriangular. Hence, $\sigma(i) > i$ for all $i < n$. But then we must have $\sigma(n) = 1$ and $\sigma(i) = i + 1$ for all $i < n$. Hence, expanding the determinant of A along the nth row we obtain $0 = |A| - 1 = a_{1\sigma(1)} \cdots a_{n\sigma(n)}$, which contradicts the fact that all $a_{i\sigma(i)}$ are nonzero. □

Remark 5.8. For a domain R and any $A' \in \mathrm{M}_n(R)$, Corollary 6.3.9 in [10] gives a result which is very similar to Lemma 5.7. It says that if every principal minor of A' is equal to 0, then A' can be conjugated by a permutation matrix such that the resulting matrix is an upper triangular matrix with zero diagonal. This result and Lemma 5.7 are actually easily shown to be equivalent!

Namely, we can use the well-known fact that the coefficient of X^{n-k} in the characteristic polynomial $P_\cdot(X)$ of an $n \times n$-matrix equals $(-1)^k$ times the sum of all principal k-minors. So suppose $A \in \mathrm{GL}_n(R)$ is such that all its principal minors are equal to 1. Then any principal submatrix A'_0 of $A' := A - I_n$ is of the form $A'_0 = A_0 - I$, where I is the identity matrix of the corresponding size, and A_0 is the principal submatrix of A consisting of the corresponding rows and columns. Let m be the number of rows (or columns) of A_0. Since all principal minors of A_0 are equal to 1, and for each k there are $\binom{m}{k}$ principal k-minors, $P_{A_0}(X) = X^m - mX^{m-1} + \binom{m}{2}X^{m-2} - \cdots + (-1)^m = (X-1)^m$. But then $P_{A'_0}(X) = |XI_m - A'_0| = |(X+1)I_m - A_0| = P_{A_0}(X+1) = X^m$. So A'_0 is nilpotent, and in particular $|A'_0| = 0$. Now that every principal minor of A' is equal to 0, the result in [10] gives a permutation matrix B such that $B^{-1}AB = B^{-1}A'B + I_n$ is upper unitriangular. Similarly, we can obtain the result in [10] from our Lemma 5.7.

Now we consider the remaining problems and conjectures presented in the Introduction. First, the Tame Generators Problem: an immediate consequence of Theorem 5.2. (Triangular automorphisms are obviously tame.)

Corollary 5.9. *Over a characteristic zero field, all invertible polynomial maps without mixed terms are tame.*

Also, we can use Theorem 5.2 to partly solve the Linearization Conjecture (Corollary 5.11). It is unknown to the author whether this conjecture also holds for the most general form of an invertible polynomial map without mixed terms.

Lemma 5.10. *Let $f = (aX_1 + p, g) \in \mathrm{GA}_n(K)$, where $a \in K^*$, $p \in K[X_2, \ldots, X_n]$ and $g \in \mathrm{GA}_{n-1}(K)$ (in the variables $X_2, \ldots, X_n$). Suppose f has finite order. Then $h^{-1}fh = (aX_1, g)$ for some $h \in \mathrm{EA}_n(K)$ with $h(X_i) = X_i$ for $i \geq 2$.*

In particular, the Linearization Conjecture holds for triangular maps.

Proof. The second statement follows by repeatedly applying the first one to a given triangular map. So let $f = (aX_1 + p, g)$ be as described, and suppose it has finite order $d \geq 1$. One readily verifies that for all $k \geq 1$, f^k has the form $(a^k X_1 + p_k, g^k)$, where $p_k \in K[X_2, \ldots, X_n]$ (and $p_d = 0$). From $f^{k+1} = f^k \circ f$ we get that $p_{k+1} = p_k(g) + a^k p$ for all k.

Now let $q := \sum_{k=1}^{d-1} \frac{1}{da^k} p_k$, and $h := (X_1 - q, X_2, \ldots, X_n)$. Then $h^{-1}fh = (aX_1, g)$ if and only if $-aq + p + q(g) = 0$. The latter follows from the fact that $q(g)$ equals

$$\sum_{k=1}^{d-1} \tfrac{1}{da^k} p_k(g) \;=\; \sum_{k=1}^{d-1} \tfrac{1}{da^k}(p_{k+1} - a^k p) \;=\; \sum_{m=2}^{d} \tfrac{1}{da^{m-1}} p_m - \tfrac{d-1}{d} p \;=\; aq - p$$

using $p_1 = p$ and $p_d = 0$. □

Corollary 5.11. *Let f be a polynomial map without mixed terms over a characteristic zero field, and suppose the matrix of its linear part is diagonal. Then the Linearization Conjecture holds for f.*

Proof. By Theorem 5.2, we may assume that f is triangular. □

The next one (the Coordinate Recognition problem) is easy.

Proposition 5.12. *Let $\mathrm{char}(K) = 0$ and $f \in K[X]$ a polynomial without mixed terms, say $f = f_1 + \cdots + f_n$ with $f_i \in K[X_i]$ for all i. Then f is a coordinate iff at least one of the f_i has degree 1.*

Proof. A necessary condition for any polynomial in $K[X]$ to be a coordinate, is that the ideal of its partial derivatives is the unit ideal in $K[X]$ (as these partial derivatives form the first row of an invertible Jacobian matrix). In this case this condition is also sufficient, since it is here equivalent to saying that at least one of these partial derivatives is a nonzero constant (the partial derivatives cannot have a common zero in an algebraic closure of K). □

Unfortunately, the Polynomial Ring Recognition Problem (say for a finitely generated K-algebra $A = K[X]/I$, I an ideal) is still unsolved if $\mathrm{char}(K) = 0$ and A is at least three-generated over K, even if I is generated by polynomials without mixed terms. In particular, we can finish this paper with the following question.

Question 5.13. Do polynomials without mixed terms satisfy the Abhyankar-Sathaye Conjecture?

Acknowledgement

The author is very grateful to Arno van den Essen and Stefan Maubach for useful discussions and comments.

References

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

[2] K. Adjamagbo, On separable algebras over a U.F.D. and the Jacobian Conjecture in any characteristic, in Automorphisms of affine spaces (Curaçao, 1994), 89-103, Kluwer Acad. Publ., Dordrecht, 1995

[3] R. Baker, J. Dover, G. Ebert, K. Wantz, Perfect Baer subplane partitions and three-dimensional flag-transitive planes, Des. Codes Cryptogr. 21 (2000), No. 1-3, 19-39

[4] H. Bass, E. Connell, D. Wright, The Jacobian conjecture, reduction of degree and formal expansion of the inverse, Bull. Amer. Math. Soc. 7 (1982) 287-330

[5] E. Berlekamp, Algebraic coding theory, McGraw-Hill, New York, 1968

[6] A. Borisov and M. Sapir, Polynomial maps over finite fields and residual finiteness of mapping tori of group endomorphisms, Invent. Math. 160 (2005), No. 2, 341-356

[7] J. Chądzyński and T. Krasiński, On the Lojasiewicz exponent at infinity for polynomial mappings of $\mathbb{C}^2$ into $\mathbb{C}^2$ and components of polynomial automorphisms of $\mathbb{C}^2$, Ann. Polon. Math. 57 (3) (1992) 291-302

[8] V. Drensky and J.-T. Yu, Automorphisms of polynomial algebras and Dirichlet series, J. Algebra 321 (2009), no. 1, 292-302

[9] A. van den Essen, Locally nilpotent derivations and their applications III, J. Pure Appl. Algebra 98 (1993), 15-23

[10] A. van den Essen, Polynomial automorphisms and the Jacobian Conjecture, Progr. Math. Vol. 190, Birkhäuser, Basel-Boston-Berlin, 2000

[11] A. van den Essen and P. van Rossum, Triangular derivations related to problems on affine n-space, Proc. Amer. Math. Soc. 130 (5) (2001) 1311-1322

[12] R. Jamison, Covering finite fields with cosets of subspaces, J. Comb. Theory Ser. A 22 (1977), No. 3, 253-266

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

[14] O. Keller, Ganze Gremona-transformation, Monats. Math. Physik 47 (1939), 299-306

[15] H. Kraft, Challenging problems on affine n-space, Séminaire Bourbaki, Vol. 1994/95, Astérisque No. 237 (1996), Exp. No. 802, 5, 295-317

[16] W. van der Kulk, On polynomial rings in two variables, Nieuw Arch. Wiskd. 3 (1) (1953) 33-41

[17] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, revision of the 1986 first edition, Cambridge University Press, Cambridge, 1994

[18] F. MacWilliams and N. Sloane, The theory of error-correcting codes, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., 1977

[19] Maubach, Stefan, Polynomial automorphisms over finite fields, Serdica Math. J. 27 (2001), No. 4, 343-350

[20] M. Nagata, A theorem of Gutwirth, J. Math. Kyoto Univ. 11 (1971), 149-154

[21] M. Nagata, On automorphism group of $k[x, y]$, Department of Mathematics, Kyoto University, Lectures in Mathematics, No. 5, Kinokuniya Book-Store Co., Ltd., Tokyo, 1972

[22] P. Nousiainen, On the Jacobian Problem in positive characteristic, Pennsylvania State Univ., preprint (1981)

[23] O. Ore, On a special class of polynomials, Trans. Amer. Math. Soc. 35 (1933), No. 3, 559-584

[24] O. Ore, Contributions to the theory of finite fields, Trans. Amer. Math. Soc. 36 (1934), No. 2, 243-274

[25] I. Shestakov and U. Umirbaev, The tame and the wild automorphisms of polynomial rings in three variables, J. Amer. Math. Soc. 17 (1) (2004) 197-227

[26] S. Smale, Mathematical problems for the next century, Math. Intelligencer 20 (2) (1998) 7-15

[27] M. Suzuki, Propriétés topologiques des polynômes de deux variables complexes, et automorphismes algébriques de l'espace $\mathbb{C}^2$, J. Math. Soc. Japan 26 (3) (1974) 241-257