Some combinatorial questions about polynomial mappings

Arno van den Essen*and Vladimir Shpilrain †

Abstract

The purpose of this note is to show how recent progress in non-commutative combinatorial algebra gives a new input to Jacobian-related problems in a commutative situtation.

1991 Mathematics Subject Classification: primary 13B25, 13B10, secondary 14A05

1 Introduction

Let K be a commutative field of characteristic 0, and $P_n = K[x_1, \ldots, x_n]$ the polynomial algebra over K. If $p_1, \ldots, p_n \in P$ are polynomials, we can form the Jacobian matrix $J = (d_j(p_i))_{1 \le i,j \le n}$. Then we have:

The Jacobian conjecture (JC). If the Jacobian matrix $J = (d_j(p_i))_{1 \le i,j \le n}$ is invertible, then the polynomials $p_1, \ldots, p_n$ generate the whole algebra P_n.

We deliberately avoid mentioning determinant here in order to make the conjecture suitable for non-commutative algebraic systems as well (upon defining partial derivatives appropriately.)

The Jacobian conjecture has been introduced by O. Keller in 1939 [11], and it still remains unsettled for $n \ge 2$ (the case $n = 1$ being trivial). A good survey on the progress made during 1939-1981, and some partial results can be found in [1]. More recent survey papers are [7], [8], [9] and [15].

Due to its obvious attractivity, this problem was being considered by people working in different areas; in particular, several non-commutative analogs of JC appeared to be easier to settle. The first result in this direction was that of Birman [3]: she has proved JC for free groups (on replacing commutative Leibnitz derivatives with non-commutative Fox derivatives [10]). More sophisticated non-commutative derivatives have to be used to

*Department of Mathematics, University of Nijmegen, Nijmegen, The Netherlands; e-mail: essen@sci.kun.nl

†Department of Mathematics, University of California, Santa Barbara, CA 93106; e-mail: shpil@math.ucsb.edu

obtain an analog of JC for free associative algebras [6].

After some period of "stagnation", more results on non-commutative JC have appeared recently. In the case of free Lie algebras, JC has been proved independently in [14], [16] and [18]. Then, back to free groups, Umirbaev [19] has proved (in particular) the following: an element g of the free group F_n is a part of some free generating system if and only if its "gradient" $(d_1(g), \ldots, d_n(g))$ is right invertible over the group ring $\mathbf{Z}F_n$ (derivatives here are non-commutative Fox derivatives). A similar result in case of a free Lie algebra has been obtained in [12].

In this paper, we consider polynomials which can be included in a generating set of cardinality n of the algebra P_n. We shall call those polynomials *coordinate* to simplify the language (in a non-commutative setting one uses the notion of "primitive element" instead of coordinate).

Unfortunately, the above cited result does not hold in the case of the commutative algebra P_n; for example, the polynomial $p = x_1 + x_1^2 x_2$ has invertible gradient, but is not a coordinate polynomial since it has a non-trivial factorization.

In the positive direction, we have the following result (here the main field K may have an arbitrary characteristic):

Theorem 1.1 *If an endomorphism of the algebra P_2 takes every coordinate polynomial to a coordinate one, then it is actually an automorphism.*

We also note that our proof of this theorem works in the case of *free associative algebra* of rank 2 as well. Furthermore we show in Remark 2.3 that the proof of Theorem 1.1 can also be extended to the case when K is an arbitrary commutative ring.

Every endomorphism φ of the algebra P_n is defined by n polynomials $\varphi(x_1), \ldots, \varphi(x_n)$; it is an automorphism if and only if these n polynomials generate the whole algebra P_n (see e.g. [4]). Therefore the Jacobian conjecture can be re-formulated as follows: every endomorphism of P_n with invertible Jacobian matrix is actually an automorphism.

It is clear that every automorphism takes any coordinate polynomial of P_n to a coordinate one, so that the set of all coordinate polynomials in P_n forms an *orbit* under the action of the group Aut (P_n). Now our theorem says that (in case of P_2) if an endomorphism acts "like an automorphism" *on one particular orbit*, then it acts like an automorphism everywhere.

This set-up has been introduced in [17] in case of free groups. The question of whether or not every primitivity-preserving endomorphism of a free group is actually an automorphism, appears to be quite difficult; it has been settled only when a free group has rank 2 (S. Ivanov, verbal communication). On the other hand, in [13], this question has been settled (in the affirmative) for free Lie algebras of arbitrary finite rank.

Now we can go on and assume that automorphisms can be distinguished from non-automorphisms by means of their value on just a *single element*; we call it a *test element*.

More formally: a polynomial $p \in P_n$ is called a test polynomial if $\varphi(p) = \alpha(p)$ for some endomorphism φ and automorphism α implies that φ is actually an automorphism itself. The condition $\varphi(p) = \alpha(p)$ can be obviously replaced here with just $\varphi(p) = p$.

For a survey on test elements in a free group, we refer to [17]. We also mention a well-known "commutator test" in a free associative algebra of rank 2 due to Dicks [5]. It is not difficult to come up with test elements also in polynomial algebras P_n - see Example 3.1 in Section 3. We give a necessary condition for a polynomial to be a test polynomial in P_n (Proposition 3.2). This condition however is not sufficient (Example 3.3).

Summing up, we have the following "Jacobian-related" problems that are also of independent interest:

Problem 1. Is it true that every endomorphism of P_n taking any coordinate polynomial to a coordinate one, is actually an automorphism?

The answer to this problem is probably "yes". In fact we show below that if JC is true then the answer is indeed affirmative. Moreover, there is a "dimension shift":

Theorem 1.2. If the Jacobian conjecture is true for the algebra P_{n-1} ($n \geq 2$), then Problem 1 has an affirmative answer for the algebra P_n in case the main field is algebraically closed and has characteristic zero.

A more general question arises if we consider arbitrary orbits under the action of $\mathrm{Aut}(P_n)$:

Problem 2. Let p be a polynomial; deg $p \geq 1$. Let φ be an endomorphism of P_n with the following property: for any automorphism α of P_n, there is another automorphism β such that $\varphi(\alpha(p)) = \beta(p)$ (in other words, φ preserves the orbit of p under the action of $\mathrm{Aut}(P_n)$). Is it true that φ is actually an automorphism?

As far as test polynomials are concerned, it seems to be difficult to somehow characterize all of them; perhaps some algorithm for detecting them might be easier to find.

One might go even further on and assume that it is possible to completely determine an endomorphism by means of its value on a single element. In other words, one might look for a polynomial $p \in P_n$ with the following property: whenever $\varphi(p) = \psi(p)$ for endomorphisms φ and ψ of the algebra P_n, it follows that $\varphi = \psi$.

If φ and ψ are automorphisms, polynomials p with this property do exist - see discussion in Section 3. In contrast, we will prove in Section 3

Proposition 1.3 Let K be a real or algebraically closed field. For any set of $n-1$ polynomials $\{p_1, \ldots, p_{n-1}\} \subseteq P_n$, there exist two *different* endomorphisms φ, ψ of the algebra P_n, such that $\varphi(p_i) = \psi(p_i)$, for all $1 \leq i \leq n-1$.

2 Problem 1: the case $n = 2$ and a relation to the Jacobian Conjecture

Proof of Theorem 1.1. i) Let φ be an endomorphism of P_2 which takes every coordinate polynomial to a coordinate one. Let $\varphi(x_1) = p$ and $\varphi(x_2) = q$. Then p is a coordinate polynomial. Hence there is an automorphism ψ such that $\psi(x_1) = p$. Therefore, on replacing φ by $\psi^{-1} \cdot \varphi$ we may assume that $p = x_1$.
ii) Write $q = \widetilde{q} \cdot x_2 + q_0(x_1)$, $\widetilde{q} \in P_2$, $q_0(x_1) \in K[x_1]$. Since $x_2 - q_0(x_1)$ is a coordinate polynomial, so is its image under the endomorphism φ, i.e., the polynomial $q - q_0(x_1)$. It follows that $\widetilde{q} \cdot x_2$ is a coordinate polynomial and therefore irreducible in P_2. Consequently, $\widetilde{q} \in K^*$, whence $\varphi = (x_1, \widetilde{q}x_2 + q_0(x_1)$ is an automorphism. □

Remark 2.1 As we have mentioned in the Introduction, the same proof gives the same result for the free associative algebra of rank 2.

Remark 2.2 A similar proof can be carried out to get the following generalization of Theorem 1.1: if an endomorphism of the algebra P_n, $n \geq 2$, takes every coordinate $(n-1)$-tuple of polynomials to another coordinate $(n-1)$-tuple, then it is actually an automorphism.

Remark 2.3 The proof of Theorem 1.1 can also be extended to the case when K is any commutative ring. This can be seen as follows:

i). First observe that if K is a reduced ring (i.e., a ring without non-zero nilpotent elements) then $K[x_1, x_2]^* = K^*$. Therefore the proof of Theorem 1.1 applies.

ii). Now let K be an arbitrary commutative ring. Put $\overline{K} = K/\eta$, where η is the nilradical of K, so that $\overline{K}$ is a reduced ring. Put $\overline{\varphi} = (x_1, \overline{\tilde{q}} \cdot x_2 + \overline{q_0}(x_1))$ (obtained from φ by reducing the coefficients mod η). Since $\tilde{q}$ is a unit in $K[x_1, x_2]$, hence so is $\overline{\tilde{q}}$ in $\overline{K}[x_1, x_2]$. Hence by i), $\overline{\varphi}$ is an automorphism of $\overline{K}[x_1, x_2]$. Then by Remark 1.1 (6) of [1] it follows that φ is an automorphism of $K[x_1, x_2]$. □

Proof of Theorem 1.2. The proof of this theorem is based on the following lemma which is due to Harm Derksen.
Lemma 2.4. Let K be an algebraically closed field. Let $p_1, \dots, p_n$ be in P_n. If $\lambda_1 p_1 + \cdots + \lambda_n p_n$ is a coordinate polynomial for every non-trivial K-linear combination, then $\det J \in K^*$, where $J = d_j(p_i)_{1 \leq i,j \leq n}$.
Proof. If $\det J \notin K^*$, then for some $z \in K^n$, $\det J(z) = 0$. Hence the rows of $J(z)$ are K-linearly dependent, say

$$\lambda_1(d_1(p_1)(z), \dots, d_n(p_1)(z)) + \cdots + \lambda_n(d_1(p_n)(z), \dots, d_n(p_n)(z)) = (0, \dots, 0)$$

for some $\lambda_i \in K$, not all of them zero. Thus if we put $p = \lambda_1 p_1 + \cdots + \lambda_n p_n$, then $d_1 p(z) = \ldots = d_n p(z) = 0$. However p is a coordinate polynomial, so its partial derivatives have no common zeros, a contradiction. □

Proof of Theorem 1.2. Let $\varphi = (p_1, \ldots, p_n)$ be an endomorphism taking coordinates to coordinates. Then, arguing as in the proof of Theorem 1.1, we may assume that $p_1 = x_1$. Since each non-trivial K-linear combination of the x_i is a coordinate polynomial in P_n, we have the conditions of Lemma 2.4 satisfied. Therefore, det $(d_j(p_i)_{1\le i,j\le n}) \in K^*$. Since $P_1 = x_1$, we deduce that det $(d_j(p_i)_{2\le i,j\le n}) \in K^*$. Now applying the $(n-1)$-dimensional JC, we see that $K(x_1)[p_2, \ldots, p_n] = K(x_1)[x_2, \ldots, x_n]$. In particular, $K(x_1, p_2, \ldots, p_n) = K(x_1, x_2, \ldots, x_n)$, which by Keller's theorem ([11]) implies $K[x_1, p_2, \ldots, p_n] = P_n$. Thus φ is an automorphism. □

3 Test polynomials

Example 3.1 The following polynomial p is a test polynomial for distinguishing automorphisms from non-automorphisms of the algebra P_n over **R**, the field of reals, or any of its subfields:

$$p = x_1^2 + \cdots + x_n^2.$$

Indeed, suppose $\varphi(p) = p$ for some endomorphism φ of P_n. Then φ is clearly a linear map since monomials of highest degree in $(\varphi(x_1))^2$ cannot cancel. Using the "chain rule", we get:

$$(x_1, \ldots, x_n) = (\varphi(x_1), \ldots, \varphi(x_n))J_\varphi. \tag{1}$$

If φ is a degenerate linear transformation, then the elements of the row-matrix on the right-hand side of (1) are R-linearly dependent, whereas the elements on the left-hand side are not. Therefore φ must be a non-degenerate linear transformation, hence an automorphism.

Nowe we introduce an important notion of *outer rank* of a polynomial:

Definition. Let $p \in P_n$ be an arbitrary polynomial. The *outer rank* of p (*orank* p) is the minimal number of generators x_1 on which the image of p under an automorphism of P_n can depend.

In other words, a polynomial p has outer rank $k \le n$ if there is a decomposition $P_n = \widetilde{P}_k \oplus \widetilde{P}_{n-k}$, where $\widetilde{P}_k$ and $\widetilde{P}_{n-k}$ are algebras of polynomials in k and $n-k$ variables respectively; $p \in \widetilde{P}_k$, and k is the minimal integer with these properties.

Polynomials of maximal outer rank (i.e., of outer rank n) appear to be of relevance to recognizing automorphisms:

Proposition 3.2 If p is a test polynomial, then *orank* $p = n$.

Proof. Suppose *orank* $p = m < n$. Then there is an automorphism α of the algebra P_n such that $\alpha(p) = q = q(x_1, \ldots, x_m)$. Define now an endomorphism ψ as follows: $\psi(x_i) = x_i$, $1 \leq i \leq m$; $\psi(x_i) = 1$, $m < i \leq n$. Then the endomorphism $\varphi = \alpha^{-1}\psi\alpha$ fixes p, but φ is clearly not an automorphism of P_n. □

On the other hand, we have:

Example 3.3 The polynomial $p = x_1 + x_1x_2$ has outer rank 2, but it is not a test polynomial of P_2.

Indeed, p is fixed by a non-automorphism φ which takes x_1 to $x_1 + x_1x_2$, and x_2 to 0. If the outer rank of p were equal to 1, then for some $\varphi \in \mathrm{Aut}(P_2)$, we would have $\varphi(q) = \varphi(x_1)(\varphi(x_2) + 1) \in k[x_1]$. This means that both $\varphi(x_1)$ and $\varphi(x_2)$ depend on x_1 only. A mapping like that cannot be an autormophism, hence a contradiction.

It seems plausible however that polynomials of maximal outer rank can be used as test polynomials for distinguishing automorphisms among arbitrary *monomorphisms*, i.e., injective homomorphisms.

We are now going to prove Proposition 1.3 from the Introduction. The proof is based on the following lemma.

Lemma 3.4 Let K be a real or algebraically closed field, and let $p_1, \ldots, p_{n-1}$ belong to P_n. Then the map $p : K^n \to K^{n-1}$ defined by $p(a) = (p_1(a), \ldots, p_{n-1}(a))$ for all $a \in K^n$, is not injective.

Proof. Let $i : K^{n-1} \to K^n$ be the natural inclusion map. If p is injective, then the map $i \circ p : K^n \to K^n$ is injective, too. Hence it is surjective by [2]. This means i is surjective, a contradiction. □

Proof of Proposition 1.3. Let $p = (p_1, \ldots, p_{n-1})$ as in Lemma 3.1. Then there exist λ in K^n and α, β in K^n with $\alpha \neq \beta$ such that $p(\alpha) = \lambda = p(\beta)$. Then φ defined by $\varphi(x_i) = \alpha_i$ and ψ defined by $\psi(x_i) = \beta_i$ for all i, are as desired. □

In case when φ and ψ are automorphisms, not just arbitrary endomorphisms, polynomials with the required property do exist - a proof of this fact has been submitted to us by D. Markushevich. However this proof appeals to several facts from algebraic geometry, and cannot be reproduced here without large amount of background material.

Acknowledgement

We are grateful to V. Lin, D. Markushevich and D. Panyushev for useful discussions. The second author also thanks Department of Mathematics of the University of Nijmegen for warm hospitality during his visit when this work has been initiated.

References

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

[2] A. Bialynicki-Birula, M. Rosenlicht, *Injective morphisms of real algebraic varieties*, Proc. Amer. Math. Soc. 13 (1962), 200-203.

[3] J.S. Birman, *An inverse function theorem for free groups*, Proc. Amer. Math. Soc. 41 (1973), 634-638.

[4] P.M. Cohn, *Free rings and their relations*, Second edition, Academic Press, London, 1985.

[5] W. Dicks, *A commutator test for two elements to generate the free algebra of rank two*, Bull. London Math. Soc. 14 (1982), 48-51.

[6] W. Dicks and J. Lewin, *A Jacobian conjecture for free associative algebras*, Comm. Algebra 10 (1982), 1285-1306.

[7] L.M. Drużkowski, *The Jacobian Conjecture*, preprint 492, Institute of Mathematics, Polish Academy of Sciences, IMPAN, Warsaw, 1991.

[8] A. van den Essen, *Polynomial maps and the Jacobian Conjecture*, in Computational aspects of Lie group representations and related topics, Proc. of the 1990 Computational Algebra Seminar, 29-44. CWI Amsterdam, 1991.

[9] A. van den Essen, *Seven lectures on polynomial automorphisms*, in Automorphisms of Affine Spaces (ed. A. van den Essen), Proc. of the conference 'Invertible Polynomial maps', July 1994, Curaçao, 3-39. Kluwer Academic Publishers, 1995.

[10] R.H. Fox, *Free differential calculus. I. Derivation in the free group ring*, Ann. of Math. 57 (1953), 547-560.

[11] O. Keller, *Ganze Cremona-Transformationen*, Monatsh. Math. Phys. 47 (1939), 299-306

[12] A.A. Mikhalev and A.A. Zolotykh, *Rank and primitivity of elements of free color Lie* (p)*-superalgebras*, Internat. J. Algebra Comput. 4 (1994), 517-555.

[13] A.A. Mikhalev and A.A. Zolotykh, *Automorphisms and primitive elements of free Lie algebras*, Comm. Algebra 22 (1994), 5889-5901.

[14] C. Reutenauer, *Applications of a noncommutative Jacobian matrix*, J. Pure Appl. Algebra 77 (1992), 169-181.

[15] K. Rusek, *Polynomial Automorphisms*, preprint 456, Institute of Mathematics, Polish Academy of Sciences, Warsaw, 1989.

[16] V. Shpilrain, *On generators of L/R^2 Lie algebras*, Proc. Amer. Math. Soc. 119 (1993), 1039-1043.

[17] V. Shpilrain, *Recognizing automorphisms of the free groups*, Arch. Math. 62 (1994), 385-392.

[18] U.U. Umirbaev, *Partial derivatives and endomorphisms of some relatively free Lie algebras*, Sib. Math. J. 34 (1993), 1161-1170.

[19] U.U. Umirbaev, *Primitive elements of free groups*, Russian Math. Surveys 49(2) (1994), 184-185.