Equivalence of polynomials under automorphisms of $K[x, y]$

Leonid Makar-Limanov[*] **Vladimir Shpilrain**[†]
Jie-Tai Yu[°]

Abstract. Let $K[x, y]$ be the algebra of polynomials in two variables over an arbitrary field K. We show that if the maximum of the x- and y-degrees of a given polynomial $p(x, y)$ cannot be decreased by a single triangular or linear automorphism of $K[x, y]$, then it cannot be decreased by *any* automorphism of $K[x, y]$. If K is an algebraically closed constructible field, this result yields an algorithm for deciding whether or not two polynomials $p, q \in K[x, y]$ are equivalent under an automorphism of $K[x, y]$.

We also show that if there is an automorphism of $K[x, y]$ taking p to q, then it is "almost" unique. More precisely: if an automorphism α of $K[x, y]$ is not conjugate to a triangular or linear automorphism, then any polynomial invariant (or even semiinvariant) under α is a constant.

1 Introduction

Let $K[x, y]$ be the algebra of polynomials in two variables over an arbitrary field K. For a polynomial $p = p(x, y) \in K[x, y]$ denote by $\deg_x(p)$ the x-degree of p, i.e., the highest exponent on x that occurs in monomials of p. The y-degree $\deg_y(p)$ is defined similarly. One more piece of terminology: when $\deg_x(p) = \deg_y(p)$, we say that $\max(\deg_x(p), \deg_y(p)) = \deg_x(p)$ if the highest degree monomial of p with respect to the lexdeg ordering with $x > y$ is $x^n y^m$, the highest degree monomial of p with respect to the lexdeg ordering with $y > x$ is $x^s y^n$, and $m > s$. Similarly, by somewhat abusing notation, we write $\max(\deg_x(p), \deg_y(p)) > \max(\deg_x(q), \deg_y(q))$ in the case where, say, $\max(\deg_x(p), \deg_y(p)) = \deg_x(p) = \deg_x(q) = \max(\deg_x(q), \deg_y(q))$, but $\deg_y(p) > \deg_y(q)$.

It is a well-known result of Jung and van der Kulk that every automorphism of $K[x, y]$ is a product of triangular and linear automorphisms. To be more specific, we call an automorphism of $K[x, y]$ triangular if it is of one of the following two types:

(T1) $(x, y) \longrightarrow (ax + f(y),\ by),\ a, b \in K^*$.

(T2) $(x, y) \longrightarrow (ax,\ by + f(x))$.

2000 Mathematics Subject Classification: Primary 14A05, 13B25; Secondary .

∗) Partially supported by an NSA grant.

†) Partially supported by the NSF grant DMS-0405105.

°) Partially supported by a RGC-CERG grant.

Our main result is as follows.

Theorem 1. Let $p = p(x, y) \in K[x, y]$. If the maximum of $\deg_x(p)$ and $\deg_y(p)$ cannot be decreased by a single triangular or linear automorphism of $K[x, y]$, then it cannot be decreased by *any* automorphism of $K[x, y]$.

Note that $\max(\deg_x(p), \deg_y(p)) \leq \deg(p) \leq 2\max(\deg_x(p), \deg_y(p))$. The example of $p(x, y) = x^3 + y^3 + x^2y^2$ shows that the inequalities can be strict. Here $\deg_x(p) = \deg_y(p) = 3$, and $\deg(p) = 2 + 2 = 4$.

Our proof of Theorem 1 is based on a simple but powerful idea of "peak reduction" [12] which goes back to Whitehead (see [7]). In the context of the present paper this means the following. If at some point of applying a sequence of triangular or linear automorphisms to p, $\max(\deg_x(p), \deg_y(p))$ goes up (or remains unchanged) before eventually going down, then there must be a pair of *subsequent* automorphisms in this sequence (a "peak") such that one of them increases $\max(\deg_x(p), \deg_y(p))$ of the current polynomial (or leaves it unchanged), and then the other one decreases it. We show that such a peak can always be reduced, i.e., can be replaced by a single triangular or linear automorphism that decreases $\max(\deg_x(p), \deg_y(p))$ of the current polynomial.

We note that, upon replacing $\max(\deg_x(p), \deg_y(p))$ by $\deg(p)$, the result of Theorem 1 was obtained by Wightwick [15] in the case where $K = \mathbb{C}$. She also used "peak reduction" motivated by our earlier paper [11] where we addressed the same problem for a special class of polynomials, namely those whose Newton polygon is a triangle. Wightwick's proof is rather complicated, and it uses a subtle analysis of Newton polygons. She notes that the complexity of the corresponding algorithm for solving the automorphic conjugacy problem (see below) can be reduced if one uses another ingredient, called splice diagrams, see [5]. It appears however that using $\max(\deg_x(p), \deg_y(p))$ instead of $\deg(p)$ as the parameter of "peak reduction" does make a difference, and the proof becomes easier.

Theorem 1 leads to a solution of the automorphic conjugacy problem for $K[x, y]$, i.e., to an algorithm that, given two polynomials $p, q \in K[x, y]$, decides whether or not $\varphi(p) = q$ for some automorphism φ of $K[x, y]$. This algorithm is in two parts. In the first part of the algorithm, one reduces $p(x, y)$ to $p'(x, y)$ by applying a sequence of triangular or linear automorphisms reducing $\max(\deg_x, \deg_y)$ at every step, such that $\max(\deg_x(p'), \deg_y(p'))$ cannot be reduced any further. Similarly, one reduces $q(x, y)$ to $q'(x, y)$ with minimum possible $\max(\deg_x, \deg_y)$.

Corollary 1. Let $p = p(x, y)$ and $r = r(x, y)$ be two polynomials equivalent under an automorphism of $K[x, y]$, and assume that $\max(\deg_x(r), \deg_y(r))$ cannot be reduced by any automorphism of $K[x, y]$. Then there exists a series of triangular automorphisms $\phi_1, \ldots, \phi_n$ such that, for $p' = (\phi_1 \circ \ldots \circ \phi_n)(p)$, one has

$$\max(\deg_x(p'), \deg_y(p')) = \max(\deg_x(r), \deg_y(r))$$

and

$$\max(\deg_x, \deg_y)((\phi_1 \circ \ldots \circ \phi_i)(p)) > \max(\deg_x, \deg_y)((\phi_1 \circ \ldots \circ \phi_{i+1})(p))$$

for all $i = 1, \ldots, n-1$.

If $\max(\deg_x(p'), \deg_y(p')) \neq \max(\deg_x(q'), \deg_y(q'))$, then p and q are inequivalent. If $\max(\deg_x(p'), \deg_y(p')) = \max(\deg_x(q'), \deg_y(q'))$, then one applies the second part of the algorithm to the polynomials $p'(x, y)$ and $q'(x, y)$ of the same minimum $\max(\deg_x, \deg_y)$. This second part is rather straightforward theoretically but usually has a higher computational complexity than the first part of the algorithm. We note that for either part of the algorithm to work, the ground field K has to be algebraically closed because one should be able to determine whether or not a given system of polynomial equations over K is consistent (cf. [15, p. 360] or our Section 4). Of course, the ground field K also has to be constructible, i.e., given two elements of K, one should be able to tell whether or not they are equal. Thus, we have:

Corollary 2. Let K be an algebraically closed constructible field, and let $p, q \in K[x, y]$. Then there is an algorithm that decides whether or not $\varphi(p) = q$ for some automorphism φ of $K[x, y]$.

We also note that if $\max(\deg_x(p'), \deg_y(p')) = 1$ (i.e., if p' is just a linear combination of variables), then the second part of the algorithm is not needed and, in particular, the ground field K does not have to be algebraically closed. If a polynomial p is equivalent to a variable, it is called *coordinate*. Thus, our Corollary 1 provides, in fact, yet another algorithm for recognizing coordinate polynomials in $K[x, y]$ for an arbitrary field K. See [9] for a survey of previously known algorithms for recognizing coordinates in $K[x, y]$.

Finally, we show that if there is an automorphism of $K[x, y]$ taking p to q, then it is "almost" unique. To make a precise statement, we recall that a polynomial $p \in K[x, y]$ is called *invariant* under if $\alpha(p) = p$ and *semiinvariant* if $\alpha(p) = \lambda p$ for some $\lambda \in K^*$.

Theorem 2. Let K be any field, and let α be an automorphism of $K[x, y]$ which is not conjugate to a triangular or linear automorphism. Then any polynomial $p \in K[x, y]$ semiinvariant under α is a constant.

We note that in the case where K has characteristic 0, this statement was proved, with some additional conditions on α, by M. Smith [13]. She also remarks that W. Dicks had pointed out to her that a proof of this fact, without additional conditions on α, was given in Lane's thesis [6], but was never published. Finally, we note that there is a similar result for automorphisms of the free associative algebra $K\langle x, y\rangle$ which appears as Theorem 6.9.7 in Cohn's monograph [3]. Note however that the statement of Theorem 2 does not hold verbatim for $K\langle x, y\rangle$ because the commutator $xy - yx$ is semiinvariant under any automorphism of $K\langle x, y\rangle$ (see [3, 4, 8]).

2 Proof of Theorem 1

As we have mentioned in the Introduction, we are going to use the idea of "peak reduction" [12]. More specifically, we assume that $\max(\deg_x(p), \deg_y(p))$ can be decreased by an automorphism φ of $K[x, y]$, which is not a single triangular or linear automorphism. Then φ can be factored as a product of triangular and linear automorphisms, and there must be a pair of *subsequent* automorphisms in this factorization (a "peak") such that, for example, one of them increases, say, $\deg_x$ of the current polynomial (or leaves it unchanged), and then the other one decreases it. We show that such a peak can always be reduced, i.e., can be replaced by a single triangular or linear automorphism that decreases $\max(\deg_x, \deg_y)$ of the current polynomial.

Before we consider different possibilities for a "peak", we are going to break up linear automorphisms into "simple" and "flip" automorphism. Simple linear automorphisms are similar to triangular ones; they are either of the form $(x, y) \longrightarrow (a_1x + a_2y,\ by)$ (type I) or $(x, y) \longrightarrow (ax,\ b_1y + b_2x)$ (type II). Flip automorphisms are of the form $(x, y) \longrightarrow (b \cdot y,\ a \cdot x)$.

Now flip automorphisms can be "moved forward", so that no triangular automorphism is applied after a flip automorphism. The relevant procedure is straightforward; e.g. a flip automorphism followed by a triangular of type I is equal to a triangular automorphism of type II followed by a flip.

After we move all flip automorphisms forward, we need to do one more thing with linear automorphisms, based on the following simple observation:

Lemma 1. Let $\alpha : (x, y) \longrightarrow (a_{11}x+a_{12}y,\ a_{21}x+a_{22}y)$ be a linear automorphism such that $a_{11} \neq 0, a_{22} \neq 0$. Then α can be factored as a product $\tau_1\tau_2$ as well as a product $\tau_2'\tau_1'$, where τ_1, τ_1' are simple linear automorphisms of type I, and τ_2, τ_2' are simple linear automorphisms of type II.

The proof is a straightforward computation; we omit the details. Now we do the following. Suppose in our factorization of a given automorphism, there is a subproduct of the form $\rho_1\alpha\rho_2$, where ρ_1 is a triangular non-linear automorphism of type I, say, α is a linear automorphism as in Lemma 1, and ρ_2 is a triangular non-linear automorphism of type II, say. Then we factor α as a product $\tau_1\tau_2$ (by Lemma 1), and get

$$\rho_1\alpha\rho_2 = \rho_1\tau_1\tau_2\rho_2 = \rho_1'\rho_2',$$

where ρ_1', ρ_2' are triangular non-linear automorphisms. If ρ_2 was triangular of type I, then we get

$$\rho_1\alpha\rho_2 = \rho_1\tau_1\tau_2\rho_2 = \rho_1'\tau_2\rho_2.$$

Other combinations are treated similarly. Thus, we end up with a product of simple linear and triangular non-linear automorphisms, where no simple linear automorphism is immediately followed by another simple linear.

This leaves us with just two principal cases to consider: where a triangular non-linear automorphism is followed by another triangular (of different type), and where a simple linear automorphism is followed by a triangular non-linear automorphism of different type.

(1) The main case is where a triangular automorphism of degree ≥ 2 is followed by another triangular (of different type). Assume, without loss of generality, that a triangular automorphism of type I is applied first. Suppose there is a polynomial $u = u(x, y)$, a triangular automorphism $\alpha : (x, y) \longrightarrow (ax + f(y),\ by)$ of type I, and a triangular automorphism $\beta : (x, y) \longrightarrow (ax,\ by + h(x))$ of type II such that

$$\max(\deg_x, \deg_y)(\beta(\alpha(u))) < \max(\deg_x, \deg_y)(\alpha(u)).$$

For $\max(\deg_x, \deg_y)$ to drop after applying β, either $\deg_x$ or $\deg_y$ has to drop. However, $\deg_y$ cannot change after a triangular automorphism of type II is applied. Therefore, we are going to focus on $\deg_x$. Since a triangular automorphism of type I cannot change $\deg_x$, that means $\deg_x(u) = \max(\deg_x(u), \deg_y(u))$. Thus, the proof in this case will be complete if we establish the following

Lemma 2. Let $u = u(x, y)$ be such that $\max(\deg_x(u), \deg_y(u)) = \deg_x(u) > 1$. Let $\alpha : (x, y) \longrightarrow (ax + f(y),\ by)$ be a triangular automorphism with $\deg(f) \geq 2$. Then $\deg_y(\alpha(u)) > \deg_x(\alpha(u))$.

Proof. For notational convenience, we shall assume that $a = b = 1$; obviously, the values of a and b do not change degree considerations.

Let $f(y) = \sum_{i=0}^{k} c_i \cdot y^i,\ k \geq 2$. Applying α is equivalent to applying a sequence of $\alpha_i : (x, y) \longrightarrow (x + c_i \cdot y^i,\ y)$. We start with α_k, followed by automorphisms of smaller degree. Denote $c_k \neq 0$ by c, to simplify the notation. Thus, $\alpha_k : (x, y) \longrightarrow (x + c \cdot y^k,\ y)$.

Let $x^n y^m, n \geq 1$, be the highest degree monomial of u with respect to the lexdeg ordering with $x > y$. Let $F(x, y)$ be the $(k, 1)$-homogeneous form of $u(x, y)$ containing the monomial $x^n y^m$ (i.e., the weight of x is assumed to be k and the weight of y is assumed to be 1). Thus, the weight of a monomial $x^i y^j$ is $ki + j$, so that, for example, the polynomial $x + y^k$ is homogeneous with respect to this weight. Furthermore, under the automorphism α_k the weight of any $(k, 1)$-homogeneous form does not change and different $(k, 1)$-homogeneous forms stay different. Therefore, to prove that $\deg_y(\alpha_k(u)) > \deg_x(\alpha_k(u))$, it is sufficient to show that $\deg_y(F(x + c \cdot y^k, y)) > \deg_x(F(x, y))$.

Over the algebraic closure of the ground field K, one can factor $F(x, y)$ as follows:

$$F(x, y) = x^a y^b (x - c \cdot y^k)^s \prod_{i=1}^{N} (x - \lambda_i y^k), \tag{1}$$

where $\lambda_i \neq c,\ \lambda_i \neq 0$. Then $F(x + c \cdot y^k, y) = (x + c \cdot y^k)^a y^b x^s \prod_{i=1}^{N} (x - (\lambda_i - c) y^k)$.

Since we assumed that $n = \deg_x(u) \geq \deg_y(u)$, we have

$$n = a + s + N \geq b + (s + N)k.$$

If $\deg_x(F(x,y)) \geq \deg_y(F(x + c \cdot y^k, y))$ then $a + s + N \geq (a + N)k + b$, therefore $2(a + s + N) \geq (a + s + N)k + 2b + Nk$. Since $k > 1$, this implies $b = N = 0$ and, if $k > 2$, then also $s = N = a = 0$. In the latter case, $n = a + s + N = 0$, contrary to the assumption $n > 1$. If $k = 2$, then $a + s \geq 2s$ (from the displayed inequality) and $a + s \geq 2a$ (from the inequality $a + s + N \geq (a + N)k + b$). Therefore, $s = a$ and $F(x,y) = (x^2 - cxy^2)^a$, where $a > 0$. This contradicts the assumption $\deg_x(F(x,y)) > \deg_y(F(x,y))$.

Thus, $\deg_x(F(x,y)) < \deg_y(F(x + c \cdot y^k, y))$, as was to be shown.

Now we have to study the effect of applying an $\alpha_i,\ i < k$, to $\alpha_k(u)$. Consider two cases:

(i) $F(x,y)$ is the leading $(k,1)$-homogeneous form (i.e., the $(k,1)$-homogeneous form of maximum $(k,1)$-weight) of $u(x,y)$. Then applying $\alpha_i,\ i < k$, will not affect the leading monomial $x^s y^{b+k(a+N)}$ of $F(x + c \cdot y^k, y)$ in the sense that this monomial will be the monomial with the smallest y-degree (and the largest x-degree) in any $(i,1)$-homogeneous form with $i < k$.

(ii) $F(x,y)$ is not the leading $(k,1)$-homogeneous form of $u(x,y)$. Let $G(x,y)$ be the leading $(k,1)$-homogeneous form of $u(x,y)$; then $w(G) > w(F)$, where w denotes the $(k,1)$-weight of the corresponding form. Over the algebraic closure of the ground field K, factor $G(x,y)$ as follows:

$$G(x,y) = x^d y^e (x - c \cdot y^k)^f \prod_{i=1}^{M} (x - \mu_i y^k), \tag{2}$$

where $\mu_i \neq c,\ \mu_i \neq 0$. By our assumptions, $n \geq \deg_y(G(x,y))$, so $n \geq e + k(f + M)$. If we also assume that $\deg_y(G(x + c \cdot y^k, y)) \leq n$, then $n \geq e + k(d + M)$. Hence

$$2n \geq 2e + k(d + f + 2M) = w(G) + e + kM > w(F) = kn + b.$$

Since $k > 1$, this is a contradiction, so that our last assumption was incorrect, whence $\deg_y(G(x + c \cdot y^k, y)) > n$. As above, applying any further automorphism α_i with $i < k$ will not change the leading monomial of $G(x + c \cdot y^k, y)$. This completes the proof of the lemma. □

(2) Suppose a simple linear automorphism is followed by a triangular non-linear automorphism of different type. Assume, without loss of generality, that a simple linear automorphism ρ of type I is applied first, followed by a triangular non-linear automorphism β of type II. Then $\deg_x(\rho(u)) = \deg_x(u)$. If $\deg_y(\rho(u)) > \deg_x(\rho(u))$, then, since applying an automorphism of type II cannot change $\deg_y$, we would have

$\max(\deg_x(\beta(\rho(u))), \deg_y(\beta(\rho(u))) > \max(\deg_x(\rho(u)), \deg_y(\rho(u)))$, contrary to the definition of the peak.

Thus, we may assume that $\deg_y(\rho(u)) \leq \deg_x(\rho(u))$. If $\deg_y(\rho(u)) = \deg_x(\rho(u))$, then β would increase $\max(\deg_x(\rho(u)), \deg_y(\rho(u)))$ by Lemma 2, so again there would be no peak.

Thus, we assume that $\deg_y(\rho(u)) < \deg_x(\rho(u))$. If this is the case, that means the argument from the proof of Lemma 2 in the previous Case (1) fails for $k = 1$ for our polynomial $u(x, y)$. Let ρ be the automorphism $(x, y) \longrightarrow (x + cy,\ y), c \in K^*$. Let $x^n y^m, n \geq 1$, be the highest degree monomial of u with respect to the lexdeg ordering with $x > y$. Let $F(x, y)$ be the $(1, 1)$-homogeneous form of $u(x, y)$ containing the monomial $x^n y^m$. Recall the factorization (1) from Case (1) upon taking $k = 1$:

$$F(x, y) = x^a y^b (x - c \cdot y)^s \prod_{i=1}^{N} (x - \lambda_i y), \tag{3}$$

where $\lambda_i \neq c,\ \lambda_i \neq 0$. Retracing the computations given after the factorization (1), we see that the only situation where the argument can fail for $k = 1$ is where $s > b$. However, if this is the case, we claim that the following (simple linear) automorphism would reduce $\max(\deg_x(u), \deg_y(u))$ in the first place: $\tau : (x, y) \longrightarrow (x,\ y + \frac{1}{c}x)$. Indeed, this automorphism would obviously reduce $\deg_x(F(x, y))$. Assume that, like in the case (ii) in the proof of Lemma 2, $F(x, y)$ was not the leading $(1, 1)$-homogeneous form of $u(x, y)$. Let $G(x, y)$ be another $(1, 1)$-homogeneous form:

$$G(x, y) = x^d y^e (x - c \cdot y)^f \prod_{i=1}^{M} (x - \mu_i y), \tag{4}$$

where $\mu_i \neq c,\ \mu_i \neq 0$. Then a direct computation shows that

$$\deg_x(\tau(G(x, y))) = \deg_y(\rho(G(x, y))) = d + e + M.$$

At the same time, we have

$$\deg_y(\tau(G(x, y))) = \deg_y(G(x, y))$$

because applying τ does not change the y-degree. Since $\deg_y(\rho(u)) < \deg_x(\rho(u)) = \deg_x(u)$ (see above), the last two displayed equalities imply $\deg_x(\tau(u)) < \deg_x(u)$. If $\deg_y(u) < \deg_x(u)$, this implies $\max(\deg_x(\tau(u)), \deg_y(\tau(u))) < \max(\deg_x(u), \deg_y(u))$, as was to be shown. If $\deg_y(u) = \deg_x(u)$, then $\deg_y(\tau(u)) = \deg_y(u) = \deg_x(u)$ and since $\deg_x(\tau(u)) < \deg_x(u)$, we again have

$$\max(\deg_x(\tau(u)), \deg_y(\tau(u))) < \max(\deg_x(u), \deg_y(u))$$

by our notational agreement (see the Introduction).

This completes the proof of Theorem 1. □

3 Proof of Theorem 2

First of all, we observe that if α_i is not conjugate to a triangular or linear automorphism, then α has infinite order. This follows from the fact that the group $Aut(K[x,y])$ is a free product with amalgamation; see e.g. [16] for details.

Let $p = p(x,y) \in K[x,y]$ be (semi)invariant under α. If $p = p_1^{d_1} \dots p_k^{d_k}$ is a factorization of p into a product of irreducible polynomials, then a power of α fixes all $p_i^{d_i}$, up to a constant factor. Therefore, without loss of generality, we may assume that $\alpha(p_i) = \lambda_i p_i$. From now on, we assume that p is irreducible and $\alpha(p) = \lambda p$.

Clearly, α induces an automorphism β of the algebra $B = K[x,y]/\langle p\rangle$, where $\langle p\rangle$ is the ideal of $K[x,y]$ generated by p. Our first goal is to show that β has infinite order.

If β has finite order, then, upon replacing α by its appropriate power, we have $\alpha(x) - x \equiv 0 \pmod{\langle\rangle p\rangle}$ and $\alpha(y) - y \equiv 0 \pmod{\langle\rangle p\rangle}$. Then also $\overline{\alpha(x) - x} \equiv 0 \pmod{\overline{P}}$ and $\overline{\alpha(y) - y} \equiv 0 \pmod{\overline{P}}$, where $\overline{u}$ here means the leading homogeneous form of a polynomial u with respect to any choice of weights for x and y. Now choose positive weights for x and y so that either $\alpha(x)$ or $\alpha(y)$ is not a monomial; this is always possible except for some trivial cases.

Consider now two cases:

(1) Either $\overline{\alpha(x) - x} = \overline{\alpha(x)}$ or $\overline{\alpha(y) - y} = \overline{\alpha(y)}$. Suppose, say, $\overline{\alpha(x) - x} = \overline{\alpha(x)}$. Then, since $\overline{p}$ divides $\overline{\alpha(x) - x}$ (see above), we get that $\overline{p}$ divides $\overline{\alpha(x)}$. Then, for an appropriate choice of weights, $\overline{p} = (ax + by^k)^n$ or $\overline{p} = (ax^k + by)^n$; in either case the degree of p can be reduced by an automorphism, call it φ. Then the polynomial $q = \varphi(p)$ satisfies $\varphi\alpha\varphi^{-1}(q) = q$, i.e., the polynomial q and the automorphism $\varphi\alpha\varphi^{-1}$ satisfy the conditions of Theorem 2, but q has lower degree than p does. Thus, the proof in this case can be completed by induction, with $p = x$ as the base of induction (in which case an automorphism fixing p must be triangular).

(2) $\overline{\alpha(x) - x} \neq \overline{\alpha(x)}$ and $\overline{\alpha(y) - y} \neq \overline{\alpha(y)}$. Then one should have $\overline{\alpha(x)} = ax + by^k$, $\overline{\alpha(y)} = cy + dx^l$ for some k, l. Again, consider two cases:

(i) $\overline{\alpha(x)} = ax + by^k$, $ab \neq 0$, $k > 1$. If $a \neq 1$, then $\overline{p} = (a-1)x + by^k$, so that the degree of p can be reduced by an automorphism. Therefore, we can ignore this case (see above).

If $a = 1$, then $\overline{p} = cy^i$. Then, since $\overline{p}$ divides $\overline{\alpha(y) - y}$, we must have $\overline{\alpha(y) - y} = y^i \cdot h(x,y)$ for some polynomial $h(x,y)$. Since we are under the assumption $\overline{\alpha(y) - y} \neq \overline{\alpha(y)}$, this implies $i = 1$, in which case p is of the form $by + h(x)$. Then p can be taken to x by an automorphism of $K[x,y]$, which implies (as above) that α is conjugate to a triangular automorphism, a contradiction with our assumption.

(ii) $\overline{\alpha(x)} = ax + by$, $ab \neq 0$. As in the previous case (i), we can focus on $a = 1$. Then $\alpha(x) - x = by$, hence $\overline{p} = cy$, so that p can be taken to x by an automorphism of $K[x,y]$, which implies that α is conjugate to a triangular automorphism. This contradiction completes the proof in this case.

Thus, we have shown so far that α induces an automorphism β of infinite order of the algebra $K[x,y]/\langle p\rangle$. Now we use a result of [10] saying that the only algebraic plane curves with infinite group of automorphisms are affine line and affine line with one puncture. We consider two cases accordingly:

(1) Let $K[x,y]/\langle p\rangle \cong K[t]$ and let π be the corresponding projection. Denote $X(t) = \pi(x)$, $Y(t) = \pi(y)$. Let, say, $\deg(X) > \deg(Y)$. We may assume that $\deg(Y)$ does not divide $\deg(X)$ since otherwise, a relevant automorphism of $K[x,y]$ would reduce the degree of p. (We note that for a ground field of characteristic 0, $\deg(Y)$ would divide $\deg(X)$ in this case by the Abhyankar-Moh-Suzuki theorem [1, 14], but in positive characteristic we do not have this facility.)

Thus, let $\deg(X) = nk$, $\deg(Y) = mk$, where $\min(n,m) > 1$ and $(n,m) = 1$.

Since p is irreducible and parametrizable by one-variable polynomials, the leading form of p is $(ax^m + by^n)^k$ (see [17]). Now recall (see e.g. [3]) that, for an appropriate choice of weights, the leading form of $\alpha(x)$ is $c\cdot h(x,y)^r$ and the leading form of $\alpha(y)$ is $d\cdot h(x,y)^s$, where $h(x,y)$ is either $(a_1x + b_1y^l)$ or $(a_1y + b_1x^l)$, and either r divides s or s divides r. In either case, the leading form of $\alpha(p)$ is either $h(x,y)^{rmk}$ or $h(x,y)^{snk}$. Therefore, since we have assumed that $\alpha(p) = \lambda p$, this implies that the leading form of p is either $h(x,y)^{rmk}$ or $h(x,y)^{snk}$, in which case an appropriate automorphism of $K[x,y]$ would reduce the degree of p. This completes the proof in this case.

(2) Let $K[x,y]/\langle p\rangle \cong K[t,t^{-1}]$ and let π be the corresponding projection. Again, denote $X(t) = \pi(x)$, $Y(t) = \pi(y)$, and let $\deg(X) = nk$, $\deg(Y) = mk$, where $\min(n,m) > 1$ and $(n,m) = 1$. Assume that either $\deg(X)$ and $\deg(Y)$ have different signs or they are both positive. (Both $\deg(X)$ and $\deg(Y)$ cannot be negative because $t \in K[X,Y]$.) Also, as in the previous case, recall that, for an appropriate choice of weights, $\overline{\alpha(x)}$ is $c\cdot h(x,y)^r$ and $\overline{\alpha(y)}$ is $d\cdot h(x,y)^s$, where $h(x,y)$ is either $(a_1x + b_1y^l)$ or $(a_1y + b_1x^l)$, and either r divides s or s divides r.

The automorphism α induces an automorphism β on $F[t,t^{-1}]$ such that $\beta(t) = \lambda t$, where λ is not a root of 1 since we have shown before that β has infinite order. (We cannot have $\beta(t) = \lambda t^{-1}$ since such an automorphism has order 2.) Note that we have

$$\pi(\alpha(x)) = \beta(X(t)). \tag{5}$$

We are now going to show that (5) yields a contradiction. Obviously, $\deg(\beta(X)) = \deg(X)$. Now let $h(x,y)$ denote either $(ax + by^l)$ or $(ay + bx^l)$. Since $\overline{\alpha(x)} = h(x,y)^r$, we have $\deg(\pi(\alpha(x))) = \deg(\pi(h(x,y)^r))$. If $h(x,y) = ax + by^l$, then $\deg(X) = nk = r\cdot\max(nk, lmk) = \deg(\pi(\alpha(x)))$. Therefore, $r = 1$ and $nk > lmk$. Similarly, we get $\deg(Y) = mk = s\cdot\max(nk, lmk) = \deg(\pi(\alpha(y)))$, and either $m = sn$ contrary to our assumption $(n,m) = 1$, or $s = 1$ and $lmk > nk$. The latter contradicts the inequality $nk > lmk$ established before.

In a similar way, one can bring to a contradiction the case where $h(x,y) = (ay + bx^l)$. Thus, we conclude that there is no choice of weights for x and y such that $\overline{\alpha(x)} =$

$c \cdot h(x,y)^r$ and $\overline{\alpha(y)} = d \cdot h(x,y)^s$, where $h(x,y)$ is either $(a_1x + b_1y^l)$ or $(a_1y + b_1x^l)$. That means α is either triangular or linear automorphism. This contradiction completes the proof of Theorem 2. □

4 Proofs of Corollaries

Corollary 1 follows immediately from Theorem 1; we singled it out into a separate statement just to better explain how our algorithm for solving the automorphic conjugacy problem in $K[x,y]$ works.

Proof of Corollary 2. Based on Corollary 1, we can reduce given polynomials $p, q \in K[x,y]$ to polynomials p', q', respectively, such that neither $\max(\deg_x(p'), \deg_y(p'))$ nor $\max(\deg_x(q'), \deg_y(q'))$ can be reduced by any automorphism of $K[x,y]$. In the course of this reduction we apply, alternatingly, triangular automorphisms of types I and II. More specifically, a triangular automorphism of type I, say, is applied to a polynomial $u(x,y)$ in the course of this procedure if and only if

$$\max(\deg_x(u(x,y)), \deg_y(u(x,y))) > \max(\deg_x(u(ax+f(y),by)), \deg_y(u(ax+f(y),by))) \tag{6}$$

for some $a, b \in K^*$, $f(y) \in K[y]$. To find out whether such a, b, and $f(y)$ exist for a given $u = u(x,y)$, one has to observe first that the degree of $f(y)$ can be bounded as follows. Let $x^n y^m, n \geq 1$, be the highest degree monomial of u with respect to the lexdeg ordering with $x > y$, and let $d = \deg_y(u)$. Then, if $k = \deg(f(y)) > d$, the monomial y^{kn+m} arising from the expansion of $(ax + f(y))^n y^m$ cannot cancel out with any other monomial in $u(ax+f(y), by)$, whence $\deg_y(u(ax+f(y), by)) > \deg_y(u(x,y))$. Since $\deg_x(u(ax + f(y), by)) = \deg_x(u(x,y))$, this contradicts the condition (6) above.

Thus, $\deg(f(y))$ is bounded by $d = \deg_y(u)$, and therefore, one can look for $f(y)$ in the form $f(y) = \sum_{i=0}^{d} c_i \cdot y^i$ with indeterminate coefficients c_i. Then the condition (6) translates into a system of polynomial equations in the indeterminates c_i. If the ground field K is constructible and algebraically closed, one can find out whether or not this system is consistent (see e.g. [2]). If it is not, then the first part of the algorithm is complete. If it is consistent, then, in general, one cannot find an "explicit" solution, but this is not a problem for our algorithm. We just keep all c_i as indeterminates and proceed to the next step of the procedure. At the next step, we are going to have some extra indeterminates, call them c'_i, and again we have to find out whether or not a relevant system of polynomial equations is consistent, only this time we are going to have more indeterminates, namely, c'_i as well as c_i. Continuing this way, we shall eventually end up either with a one-variable polynomial or with an inconsistent system of equations. In either case, the first part of the algorithm is complete; the output of this part is a pair p', q' of polynomials such that neither $\max(\deg_x(p'), \deg_y(p'))$ nor $\max(\deg_x(q'), \deg_y(q'))$ can be reduced by any automorphism of $K[x,y]$.

The second part of the algorithm applies to the polynomials p' and q'. If $\max(\deg_x(p'), \deg_y(p')) \neq \max(\deg_x(q'), \deg_y(q'))$, then the given p and q were inequivalent. If $\max(\deg_x(p'), \deg_y(p')) = \max(\deg_x(q'), \deg_y(q'))$, then one has to find out whether or not there is a single linear or a single triangular automorphism of $K[x, y]$ taking p' to q'. If it is a single triangular automorphism, then its degree is bounded, as above. Thus, the problem amounts again to deciding whether or not a relevant system of polynomial equations is consistent. □

Acknowledgements

The first and the second authors are grateful to the Department of Mathematics of the University of Hong Kong for its warm hospitality during their visit when part of this work was done. We are also grateful to Warren Dicks for bringing Smith's paper [13] and Lane's thesis [6] to our attention.

References

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

[2] W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, v.3, American Mathematical Society, 1994.

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

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

[5] D. Eisenbud and W. D. Neumann, *Three-dimensional link theory and invariants of plane curve singularities.* Ann. Math. Stud. **110**, Princeton. Princeton Univ. Press (1985).

[6] D. Lane, *Free algebras of rank two and their automorphisms*, Thesis, London University, 1976.

[7] R. Lyndon and P. Schupp, *Combinatorial Group Theory*. Reprint of the 1977 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2001.

[8] L. G. Makar-Limanov, *On automorphisms of free algebra with two generators*, Funk. Analiz i ego Prilozh. **4** (1970), No.3, 107-108 (Russian).

[9] A. A. Mikhalev, V. Shpilrain, and J.-T. Yu, *Combinatorial Methods: Free Groups, Polynomials, and Free Algebras*, Springer-Verlag, New York, 2003.

[10] M. Rosenlicht, *Automorphisms of function fields*, Trans. Amer. Math. Soc. **79** (1955), 1–11.

[11] V. Shpilrain and J.-T. Yu, *Embeddings of curves in the plane*, J. Algebra **217** (1999), 668–678.

[12] V. Shpilrain and J.-T. Yu, *Peak reduction technique in commutative algebra: a survey*, in: Combinatorial and computational algebra (Hong Kong, 1999), 237–247, Contemp. Math. **264**, Amer. Math. Soc., Providence, RI, 2000.

[13] M. Smith, *Eigenvectors of automorphisms of polynomial rings in two variables*, Houston J. Math. **10** (1984), 559–573.

[14] M.Suzuki, *Propriétés topologiques des polynomes de deux variables complexes, et automorphismes algébriques de l'espace* $\mathbf{C}^2$, J. Math. Soc. Japan **26** (1974), 241–257.

[15] P. Wightwick, *Equivalence of polynomials under automorphisms of* $\mathbb{C}^2$, J. Pure Appl. Algebra **157** (2001), 341–367.

[16] D. Wright, *The amalgamated free product structure of* $GL_2(k[X_1, ..., X_n])$ *and the weak Jacobian theorem for two variables*, J. Pure Appl. Algebra **12** (1978), 235–251.

[17] J.-T. Yu, *Face polynomials and inversion formula*, J. Pure Appl. Algebra **78** (1992), 213–219.

Department of Mathematics, Wayne State University, Detroit, MI 48202
e-mail address: lml@math.wayne.edu

Department of Mathematics, The City College of New York, New York, NY 10031
e-mail address: shpil@groups.sci.ccny.cuny.edu
http://www.sci.ccny.cuny.edu/˜shpil/

Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong
e-mail address: yujt@hkucc.hku.hk
http://hkumath.hku.hk/˜jtyu