AUTOMORPHIC EQUIVALENCE PROBLEM FOR FREE ASSOCIATIVE ALGEBRAS OF RANK TWO

VESSELIN DRENSKY AND JIE-TAI YU

Abstract. Let $K\langle x,y\rangle$ be the free associative algebra of rank 2 over an algebraically closed constructive field of any characteristic. We present an algorithm which decides whether or not two elements in $K\langle x,y\rangle$ are equivalent under an automorphism of $K\langle x,y\rangle$. A modification of our algorithm solves the problem whether or not an element in $K\langle x,y\rangle$ is a semiinvariant of a nontrivial automorphism. In particular, it determines whether or not the element has a nontrivial stabilizer in $\mathrm{Aut}K\langle x,y\rangle$.

An algorithm for equivalence of polynomials under automorphisms of $\mathbb{C}[x,y]$ was presented by Wightwick. Another, much simpler algorithm for automorphic equivalence of two polynomials in $K[x,y]$ for any algebraically closed constructive field K was given by Makar-Limanov, Shpilrain, and Yu. In our approach we combine an idea of the latter three authors with an idea from the unpubished thesis of Lane used to describe automorphisms which stabilize elements of $K\langle x,y\rangle$. This also allows us to give a simple proof of the corresponding result for $K[x,y]$ obtained by Makar-Limanov, Shpilrain, and Yu.

1. Introduction

Let K be an arbitrary field of any characteristic and let $K[x,y]$ and $K\langle x,y\rangle$ be, respectively, the polynomial algebra in two variables and the free unitary associative algebra of rank 2 (or the algebra of polynomials in the noncommuting variables x and y). Two polynomials $u(x,y)$ and $v(x,y)$ from $K[x,y]$ or $K\langle x,y\rangle$ are automorphically equivalent, if there exists an automorphism of the corresponding algebra which brings u to v. Wightwick [14] has presented an algorithm which

2000 *Mathematics Subject Classification.* Primary 16S10. Secondary 16W20; 16Z05; 13B25; 13P10; 14R10.

Key words and phrases. Automorphisms of free and polynomial algebras, automorphic equivalence in free algebras.

The research of Vesselin Drensky was partially supported by Grant MI-1503/2005 of the Bulgarian National Science Fund.

The research of Jie-Tai Yu was partially supported by a Hong Kong RGC-CERG Grant.

decides whether or not two polynomials in $\mathbb{C}[x, y]$ are automorphically equivalent. Makar-Limanov, Shpilrain, and Yu [10] have given a much simpler algorithm which works for $K[x, y]$ for any algebraically closed constructive K. Their method is based on *peak reduction*. See the survey article of Shpilrain and Yu [12] for other applications of the peak reduction method to problems for commutative algebra. Shpilrain and Yu [11] have settled a special case of the automorphic equivalence problem for $K\langle x, y\rangle$, namely, the case where one of the elements is primitive.

It is a classical result of Jung [6] and van der Kulk [7] that every automorphism of $K[x, y]$ is tame and is a product of two kind of automorphisms – affine and triangular. Even more, $\mathrm{Aut}K[x, y]$ is isomorphic to $A *_C B$, the free product of the subgroup A of affine automorphisms and the subgroup B of triangular automorphisms amalgamating their intersection C, the subgroup of affine triangular automorphisms. This implies that every $\varphi \in \mathrm{Aut}K[x, y]$ has a canonical form $\varphi = \psi_n \cdots \psi_1$, where each ψ_i is an affine or triangular automorphism, and the length n is invariant of ψ.

Let $\varphi = \psi_1 \cdots \psi_n \in \mathrm{Aut}K[x, y]$ bring $u(x, y)$ to $v(x, y)$. Makar-Limanov, Shpilrain, and Yu [10] have studied the behaviour of the sequence

$$d_i = \max(\deg_x(\psi_i \cdots \psi_1 u), \deg_y(\psi_i \cdots \psi_1 u)), \quad i = 0, 1, \ldots, n,$$

where $\deg_x$ and $\deg_y$ denote the degree with respect to x and y, respectively. If, at some step $d_i \leq d_{i+i} > d_{i+2}$ (a peak), then they replace ψ_{i+1} with another affine or triangular automorphism ψ'_{i+1} such that the new maximum d'_{i+1} of the degrees in x and y of $\psi'_{i+1}\psi_i \cdots \psi_1 u$ is smaller than d_{i+1}. In this way they move the peak to the right. This procedure gives that $u(x, y)$ and $v(x, y)$ are automorphically equivalent if and only if there exist two sequences of affine or triangular automorphisms, $\rho_1, \ldots, \rho_r$ and $\sigma_1, \ldots, \sigma_s$, with the following property. The sequences of degrees $p_i = \max(\deg_x(\rho_i \cdots \rho_1 u), \deg_y(\rho_i \cdots \rho_1 u))$, $i = 1, \ldots, r$, and $q_j = \max(\deg_x(\sigma_j \cdots \sigma_1 v), \deg_y(\sigma_j \cdots \sigma_1 v))$, $j = 1, \ldots, s$, strictly decrease, $p_r = q_s$, and there is an affine automorphism which sends $\rho_r \cdots \rho_1 u$ to $\sigma_s \cdots \sigma_1 v$. The procedure which decides whether or not such sequences of automorphisms exist reduces the problem to the decision whether or not a system of algebraic equations in several variables is consistent. Over an algebraically closed constructive K this problem can be solved using Gröbner bases techniques.

The $K\langle x,y\rangle$-analogue of the theorem of Jung-van der Kulk has been established by Czerniakiewicz [4] and Makar-Limanov [9]. Again, every automorphism is tame and $\mathrm{Aut}K\langle x,y\rangle$ is the free product with amalgamation of the subgroups of triangular and affine automorphisms. Clearly, the automorphisms of $K\langle x,y\rangle$ fix, up to a nonzero multiplicative constant, the commutator $[x,y]=xy-yx$.

A theorem of Lane from his unpublished thesis [8] in 1976 states that an automorphism φ of $K\langle x,y\rangle$ has a nontrivial semiinvariant (i.e., $\varphi u=\lambda u$ for some $u(x,y)\in K\langle x,y\rangle\backslash\mathrm{span}([x,y]^k\mid k\geq 0)$ and a nonzero constant $\lambda\in K$) if and only if φ is conjugate in $\mathrm{Aut}K\langle x,y\rangle$ to a linear or triangular automorphism. See Section 9 of Chapter 6 from the book by Cohn [3] for the improved exposition of the results of Lane. The idea of the proof is the following. Every $\varphi=\psi_n\cdots\psi_1\in\mathrm{Aut}K\langle x,y\rangle$ is written in a canonical form and the considerations are modulo the subspace spanned by the powers of the commutator $[x,y]$. The first step is to show that the consecutive action of nonaffine triangular automorphisms ψ_i first strictly decrease the total degree of the element $u(x,y)$. Then, maybe after one action, when the degree is the same, it starts to increase strictly. This allows to bound from above the length n in the canonical form of the automorphisms with $u(x,y)$ as a semiinvariant. Then the proof is completed by arguments from the theory of free products of groups with amalgamation.

Lane [8] (see Exercise 6.9.3, p. 362 of [3]) has proved also that the only automorphisms of $\mathbb{C}[x,y]$ with semiinvariants $u(x,y)\in\mathbb{C}[x,y]\backslash\mathbb{C}$ are conjugate to linear and triangular automorphisms. Smith [13] has determined the eigenvalues and the eigenvectors of triangular automorphisms. (Clearly, after a linear transformation of x and y, the linear automorphisms also become triangular.) Recently, the theorem of Lane has been generalized to any field K by Makar-Limanov, Shpilrain, and Yu [10], involving algebraic geometry.

In the present paper, by combining the algorithmic approach of Makar-Limanov, Shpilrain, and Yu [10] to the automorphic equivalence in $K[x,y]$ with the idea of Lane (as stated in [3]) in the description of automorphisms of $K\langle x,y\rangle$ possessing nontrivial semiinvariants, we obtain an algorithm deciding whether or not two elements in $K\langle x,y\rangle$ are equivalent under an automorphism of $K\langle x,y\rangle$. A modification of our algorithm solves the problem whether or not an element in $K\langle x,y\rangle$ is a semiinvariant of a nontrivial automorphism. In particular, it determines whether or not the element has a nontrivial stabilizer in $\text{Aut}K\langle x, y\rangle$.

Our approach works also in the commutative case. We slightly improve the automorphic equivalence algorithm of Makar-Limanov, Shpilrain, and Yu [10], replacing the study of the behaviour of the degree with respect to x and y with that of the total degree. We simplify also the proof (over an arbitrary field K) of the result for the stabilizer of $u(x, y) \in K[x, y]\backslash K$, avoiding usage of algebraic geometry, and provide an algorithm for the existence of a nontrivial stabilizer for a given $u(x, y)$.

2. Preliminaries

Since automorphisms of $K[x, y]$ and $K\langle x, y\rangle$ are determined by the images of x and y, we shall denote them as $\varphi = (a, b)$, where $\varphi x = a(x, y)$, $\varphi y = b(x, y)$. If $\psi = (c, d)$ is another automorphism, we denote their composition as

$$\psi\varphi = (c, d)(a, b) = (a(c, d), b(c, d)).$$

The automorphism ψ is affine, if it is of the form

$$\psi = (\alpha x + \gamma y + \xi, \beta x + \delta y + \eta), \quad \alpha, \beta, \gamma, \delta, \xi, \eta \in K.$$

It is triangular, if

$$\psi = (\alpha x + p(y), \beta y + \eta), \quad \alpha, \beta \in K^* = K\backslash 0, \quad \eta \in K,$$

and the polynomial $p(y)$ does not depend on x. We denote by A and B, respectively, the groups of affine and triangular automorphisms, and with $C = A \cap B$ their intersection. The results of Jung [6], van der Kulk [7], Czerniakiewicz [4], and Makar-Limanov [9] give that

$$\text{Aut}K[x, y] \cong \text{Aut}K\langle x, y\rangle \cong A *_C B.$$

Hence $\varphi \in \text{Aut}K[x, y]$ (and similarly for $\varphi \in \text{Aut}K\langle x, y\rangle$) has the form

$$\varphi = \psi_n \cdots \psi_1, \tag{1}$$

where each ψ_i is affine or triangular. If two consequent ψ_i, ψ_{i+1} belong to the same A or B, we can replace them with their product. We may always assume that if $n > 1$ in (1), then either $\psi_i \in A\backslash B$ and $\psi_{i+1} \in B\backslash A$, or vise versa. We call this decomposition a canonical form of φ. The group theoretic properties of $A *_C B$ imply that if $n > 1$, then $\varphi \neq 1$. From now on we fix the automorphism

$$\tau = (y, x). \tag{2}$$

Then the form (1) of the automorphism φ can be replaced by

$$\varphi = \rho_n\tau\cdots\tau\rho_1\tau\rho_0, \tag{3}$$

where $\rho_0, \rho_1, \ldots, \rho_n \in B$ and only ρ_0 and ρ_n are allowed to belong to A, see for example p. 350 in [3]. Using the equalities for compositions of automorphisms

$$(\alpha x+p(y), \beta y+\gamma) = (x+\alpha^{-1}(p(x)-p(0)), y)(\alpha x+p(0), \beta y+\gamma), \quad \gamma \in K,$$

$$(\alpha x + \xi, \beta y + \eta)\tau = (\beta y + \eta, \alpha x + \xi), \quad \xi, \eta \in K,$$

we can do further simplifications in (3), assuming that $\rho_i = (x+p_i(x), y)$ with $p_i(0) = 0$ for all $i = 1, \ldots, n$.

In the next considerations we work in the free algebra $K\langle x, y\rangle$. We denote by $|u(x, y)|$ the homogeneous component of maximum total degree of the nonzero element $u(x, y) \in K\langle x, y\rangle$. Following Cohn [3], p. 357, we call $u(x, y)$ biased if $\deg_x|u| \geq \deg_y|u|$.

Let $V = \mathrm{span}([x, y]^k \mid k \geq 0)$ be the subspace of $K\langle x, y\rangle$ spanned by all powers of the commutator $[x, y]$. Since $\mathrm{Aut}K\langle x, y\rangle(V) = V$, the group $\mathrm{Aut}K\langle x, y\rangle$ acts on the factor vector space $\overline{K\langle x, y\rangle} = K\langle x, y\rangle/V$. Since V is also graded, $\overline{K\langle x, y\rangle}$ inherits the grading of $K\langle x, y\rangle$. Hence for the nonzero element $\overline{u(x, y)} \in \overline{K\langle x, y\rangle}$ we may define $\deg \overline{u}$, $\deg_x\overline{u}$, $\deg_y\overline{u}$, and $|\overline{u}|$. Again, $\overline{u(x, y)}$ is biased if $\deg_x|\overline{u}| \geq \deg_y|\overline{u}|$.

The following result is a corollary of a lemma of Lane.

Proposition 1. (Corollary 9.6, pp. 361-362 in [3]) *Let $\overline{0} \neq \overline{u(x, y)} \in \overline{K\langle x, y\rangle}$ and let $\rho = (\alpha x + p(y), \beta y + \gamma)$ be a nonaffine triangular automorphism of $K\langle x, y\rangle$. Then each of the following statements implies the next:*

(i) *$\overline{u(x, y)}$ is biased;*

(ii) *$\deg \overline{u} < \deg(\overline{\tau\rho u})$;*

(iii) *$\deg \overline{u} \leq \deg(\overline{\tau\rho u})$;*

(iv) *$\overline{\tau\rho u} = \overline{u(\alpha y + p(x), \beta x + \gamma)}$ is biased.*

The following consequence of the proposition is the main step of the proof of Theorem 6.9.7, p. 361 in [3]. We include the proof for convenience.

Corollary 2. *Let $\varphi = \rho_n\tau\cdots\tau\rho_1\tau\rho_0 \in \mathrm{Aut}K\langle x, y\rangle$ be written in the form (3). Let $u(x, y) \in K\langle x, y\rangle\backslash V$ and let*

$$d_{-1} = \deg \overline{u}, \quad d_n = \deg(\overline{\varphi u}),$$

$$d_j = \deg(\overline{\tau\rho_j\tau\cdots\tau\rho_1\tau\rho_0 u}), \quad j = 0, 1, \ldots, n-1.$$

If $\rho_i, \dots, \rho_k$ are all nonaffine automorphisms in the decomposition (3), $i \leq 1$, $k \geq n-1$, then there exists an integer m between i and k such that

$$d_{-1} = d_{i-1} > d_i > \cdots > d_m \leq d_{m+1} < \cdots < d_k = d_n.$$

Proof. Clearly, affine automorphisms preserve the degree in $\overline{K\langle x, y\rangle}$. If ρ_0 is affine, then $i = 1$ and $d_{-1} = \deg \overline{u} = \deg(\overline{\rho_0 u}) = \deg(\overline{\tau\rho_0 u})$. Similarly we conclude that $d_k = d_n$. Let $m \geq i$ be the largest integer such that $d_i > d_{i+1} > \cdots > d_m$. Hence either $m = k$ or $m < k$ and $d_m \leq d_{m+1}$. Applying consecutively parts (iii) $\Longrightarrow$ (iv) and (i) $\Longrightarrow$ (ii) of Proposition 1 we obtain that $\overline{\tau\rho_{m+1}\tau\cdots\tau\rho_1\tau\rho_0 u}$ is biased and $d_{m+1} < d_{m+2}$. We complete the proof by obvious induction. $\square$

We shall also need the following well known lemma, see for example Lemma 5.1 in [5].

Lemma 3. *As a vector space $K\langle x, y\rangle$ has a basis consisting of the elements*

$$u_{ab} = x^{a_1}y^{b_1}[x,y]x^{a_2}y^{b_2}\cdots x^{a_r}y^{b_r}[x,y]x^{a_{r+1}}y^{b_{r+1}}, \tag{4}$$

where $a_i, b_i, r \geq 0$.

Note, that the coefficients of $u(x, y) \in K\langle x, y\rangle$ with resepct to the basis (4) can be found explicitly using the equation $yx = xy - [x, y]$, see e.g. the proof of the lemma in [5] for details.

Corollary 4. *Let the element $u(x, y)$ in $K\langle x, y\rangle\backslash V$ be written as a linear combination*

$$u(x,y) = \sum \gamma_{ab}u_{ab}, \quad \gamma_{ab} \in K,$$

of the basis (4) and let $\rho = (\alpha x + p(y), \beta y + \gamma)$ be a nonaffine triangular automorphism of $K\langle x, y\rangle$. If $a_1 = \cdots = a_{q+1} = 0$ for all summands u_{ab} with nonzero coefficients γ_{ab}, then $\deg u = \deg(\rho u)$. If some a_i is not equal to 0 and $\deg p(y) = k > \deg u$, then $\deg(\overline{\rho u}) \geq k$.

Proof. We use the idea of the proof of Theorem 5.2 in [5]. If all a_i are equal to 0, then x participates in $u(x, y)$ in commutators $[x, y]$ only. Since $[\alpha x + p(y), \beta y] = \alpha\beta[x, y]$, we obtain

$$\rho u = \sum \gamma_{ab}\alpha^r\beta^r(\beta y + \gamma)^{b_1}[x,y](\beta y + \gamma)^{b_2}[x,y]\cdots[x,y](\beta y + \gamma)^{b_{r+1}}.$$

Hence $\deg u = \deg(\rho u)$. Now, let some a_i be not equal to 0. Let $p(y) = \delta_0 y^k + \cdots + \delta_{k-1}y + \delta_k$, $\delta_i \in K$, $\delta_0 \neq 0$, and $\deg p = k > \deg u$.

We order the elements u_{ab} from the basis (4) lexicographically assuming that $y > x$. The leading monomial of $\rho u_{ab} = u_{ab}(\alpha x + p(y), \beta y + \gamma)$ is

$$(-1)^r \alpha^r \beta^{B+r} \gamma^{kA} y^{ka_1+b_1+1} x y^{ka_2+b_2+1} x \cdots y^{a_r+b_r+1} x y^{a_{r+1}+b_{r+1}+1},$$

$A = \sum a_i$, $B = \sum b_i$. Since $k > \deg u \geq A+B+2r$, we obtain that the different ρu_{ab} have linearly independent leading monomials. If $a_i > 0$ for some i, then the leading monomial of ρu_{ab} has different degrees with respect to x and y. Hence, the corresponding bihomogeneous (homogeneous in x and in y) component does not belong to V. Since $\deg(\rho u_{ab}) \geq kA + B + 2r$ and there exists a nonzero a_i, we conclude that $\deg(\overline{\rho u}) \geq k$. □

Finally, we need some facts from the theory of Gröbner bases.

Proposition 5. *Let K be an algebraically closed constructive field and let $f_j(t_1, \ldots, t_N)$, $j = 0, 1, \ldots, M$, be a finite set of polynomials in $K[t_1, \ldots, t_N]$. There is an algorithm which decides whether or not the system*

$$f_j(t_1, \ldots, t_N) = 0, \quad j = 1, \ldots, M,$$

has a solution $(\xi_1, \ldots, \xi_N) \in K^N$ such that $f_0(\xi_1, \ldots, \xi_N) \neq 0$.

Proof. The Hilbert Nullstellensatz gives that the system

$$f_j(t_1, \ldots, t_N) = 0, \quad j = 1, \ldots, M,$$

has a solution if and only if the ideal I of $K[t_1, \ldots, t_N]$ generated by $f_j(t_1, \ldots, t_N)$, $j = 1, \ldots, M$, does not coincide with the whole $K[t_1, \ldots, t_N]$. We can decide whether or not $I = K[t_1, \ldots, t_N]$ calculating its Gröbner basis. If for every solution $(\xi_1, \ldots, \xi_N)$ of the system we have $f_0(\xi_1, \ldots, \xi_N) = 0$, then the Hilbert Nullstellensatz again implies that some power of $f_0(t_1, \ldots, t_N)$ belongs to I and f_0 belongs to the radical $\mathrm{Rad}(I)$ of I. There is an algorithm which uses Gröbner bases and decides whether or not $f_0(t_1, \ldots, t_N) \in \mathrm{Rad}(I)$, see for example [1] or the algorithm RADICALMEMTEST, p. 268 in [2]. □

3. The main results

The following two theorems are the main results of this paper.

Theorem 6. *Let K be an algebraically closed constructive field and let $u(x, y), v(x, y) \in K\langle x, y\rangle$. Then there is an algorithm which decides whether or not $v = \varphi u$ for some $\varphi = (f(x, y), g(x, y)) \in \mathrm{Aut}K\langle x, y\rangle$. The elements $f(x, y)$ and $g(x, y)$ which determine φ can be expressed in terms of the solutions of systems of algebraic equations.*

Proof. We want to find $\varphi = (f, g) \in \mathrm{Aut} K\langle x, y\rangle$ such that $v = \varphi u$. We can decide efficiently, presenting u and v as linear combinations of the basis (4) in Lemma 3, whether or not $u(x, y), v(x, y) \in V$.

Case 1. If

$$u(x, y) = \sum_{k=0}^{m} \lambda_k [x, y]^k \in V, \quad \lambda_k \in K,$$

then $v = \varphi u$ is impossible if $v \notin V$. Let

$$v(x, y) = \sum_{k=0}^{m} \mu_k [x, y]^k \in V, \quad \mu_k \in K.$$

Since $\varphi[x, y] = \omega[x, y]$, $\omega \in K^*$, the action of φ on u is determined by the linear components $f_1 = \xi_1 x + \xi_2 y$ and $g_1 = \eta_1 x + \eta_2 y$ of f and g, respectively. Hence

$$\varphi u = \sum_{k=0}^{m} \lambda_k \vartheta^k [x, y]^k, \quad \vartheta = \xi_1\eta_2 - \xi_2\eta_1.$$

Therefore, we have to decide whether or not the equations

$$t_k(\omega) = \lambda_k \omega^k - \mu_k = 0, \quad k = 0, 1, \ldots, m,$$

have a common solution. This can be handled efficiently, determining with the Euclidean algorithm the greatest common divisor of the polynomials $t_k(\omega)$. It is easy to see that automorphisms φ which send u to v can be characterized in their normal form (3) as follows. For any common solution ω_0 of the equations $t_k(\omega) = 0$ and any $n \geq 0$ we define in an arbitrary way $\rho_i = (x + p_i(y), y)$, $p_i(0) = 0$, $i = 1, \ldots, n$. Then we choose $\alpha \in K^*$, $p(y) \in K[y]$, $\gamma \in K$, and define $\rho_0 = (\alpha x + p(y), \alpha^{-1}\omega_0 y + \gamma)$.

Case 2. Now we assume that $u, v \notin V$. We repeat the main idea of the proof of Makar-Limanov, Shpilrain, and Yu [10] of the result in the commutative case. We search for φ in the form $\varphi = \rho_n \tau \cdots \tau \rho_1 \tau \rho_0$. We can efficiently present $u(x, y)$ and $v(x, y)$ in the form $u = u' + u_V$, $v = v' + v_V$, where $u_V, v_V \in V$ are the sums of the bihomogeneous components of u and v which are equal, up to multiplicative constants, to powers of the commutator $[x, y]$. In the notation of Corollary 2, we define

$$d_{-1} = \deg \overline{u}, \quad d_n = \deg(\overline{v}),$$

$$d_j = \deg(\overline{\tau \rho_i \tau \cdots \tau \rho_1 \tau \rho_0 u}), \quad j = 0, 1, \ldots, n - 1.$$

We assume that both ρ_0 and ρ_n are affine. The other cases are similar and also have to be considered. Hence $i = 1$, $k = n - 1$. Since d_{-1} and d_n are equal to the degrees of $\overline{u}$ and $\overline{v}$, they are fixed. Hence there is a finite number of choices for the sequence of positive integers d_j, $j = 0, 1, \dots, n$, with the property that

$$d_{-1} = d_0 > d_1 > \cdots > d_m \leq d_{m+1} < \cdots < d_{n-1} = d_n.$$

This also bounds n from above by $n \leq \deg \overline{u} + \deg \overline{v}$. We have to consider all possible sequences $\{d_j\}$. We fix one of them. We consider the first and the last automorphisms $\rho_0 = (\xi_0 x + \xi_0' y + \xi_0'', \eta_0 y + \eta_0')$ and $\rho_n = (\xi_n x + \xi_n' y + \xi_n'', \eta_n y + \eta_n')$ with unknown coefficients ξ_j, η_j, and all other automorphisms $\rho_j = (\xi_j x + p_j(y), \eta_j y + \eta_j')$ with unknown ξ_j, η_j and unknown polynomials p_j.

Part 1, *Step 1.* If, writing $u(x, y)$ as linear combination $u = \sum \gamma_{ab} u_{ab}$ of the basis (4), we have $a_r = 0$ for all $\gamma_{ab} \neq 0$, then $\rho_0 u$ shares the same property. Hence $\overline{\tau\rho_0 u}$ is biased and by Proposition 1, $d_0 < d_1$. Hence $m = 0$ and we go to the next part of the procedure. We assume that there exists a nonzero a_i. It is easy to see, that the same holds for some basis element in the expression of $\rho_0 u$. Then Corollary 4 gives that the degree of $p_1(y)$ is bounded by the degree of $u(x, y)$. Let $p_1(y) = \omega_{d_0} y^{d_0} + \cdots + \omega_1 y + \omega_0$, where $\omega_0, \omega_1, \dots, \omega_{d_0}$ are unknown coefficients. This bounds the degree of $\rho_1\tau\rho_0 u$ from above in terms of d_0, e.g. $\deg(\rho_1\tau\rho_0 u) \leq d_0^2$. We write $\rho_1\tau\rho_0 u$ in the form

$$\rho_1\tau\rho_0 u = \sum \delta_i z_{i_1} z_{i_2} \cdots z_{i_s}, \quad z_{i_j} = x, y,$$

where the coefficients $\delta_i = \delta(\xi, \eta, \omega)$ are polynomials in ξ_j, η_j, ω_j. Now we use the equalities $\deg(\overline{\rho_1\tau\rho_0 u}) = d_1$ and $\deg(\rho_1\tau\rho_0 u) \leq d_0^2$. The monomials $z_{i_1} z_{i_2} \cdots z_{i_s} \in K\langle x, y\rangle$ of degree $s > d_0^2$ do not participate in $\rho_1\tau\rho_0 u$. If $d_1 < s \leq d_0^2$ and $\deg_x(z_{i_1} z_{i_2} \cdots z_{i_s})$ is different from $\deg_y(z_{i_1} z_{i_2} \cdots z_{i_s})$, then $\delta_i = 0$. If $\deg_x(z_{i_1} z_{i_2} \cdots z_{i_s}) = \deg_x(z_{i_1} z_{i_2} \cdots z_{i_s})$ for $d_1 < s \leq d_0^2$, then we write the corresponding bihomogeneous component in the form $\sum \delta_{i'} z_{i_1} z_{i_2} \cdots z_{i_s} = \vartheta[x, y]^{s/2}$ with unknown coefficient ϑ and again obtain equations of the form $\delta_i = 0$ or $\delta_i - \pm\vartheta$. In this way we obtain a finite system of algebraic equations

$$\Delta_q(\xi, \eta, \omega, \vartheta) = 0, \quad q = 1, \dots, Q. \tag{5}$$

We want to decide whether or not the system has a solution with the property that $\deg(\overline{\rho_1\tau\rho_0 u}) = d_1$, the coefficients $\xi_0, \eta_0, \xi_1, \eta_1$ are nonzero, and the polynomial $p_1(y)$ is of degree ≥ 2. This can be done effectively using Proposition 5.

Step 2. We repeat Step 1 with the element $\tau\rho_1\tau\rho_0 u$ instead of with u. If the element $\overline{\tau\rho_1\tau\rho_0 u}$ is biased, we have $m = 1$ and go to the next part of the procedure. If $\overline{\tau\rho_1\tau\rho_0 u}$ is not biased, then we bound from above the degree of the polynomial $p_2(y)$ in the definition of ρ_2 and, continuing as above, add new equations to the system of algebraic equations (5).

We continue till the $m-1$'st step, and obtain the polynomial

$$w_1 = \rho_{m-1}\tau\cdots\rho_1\tau\rho_0 u.$$

when $d_m \leq d_{m+1}$. We finish this part of the procedure.

Part 2. We start a similar procedure with $v(x,y)$, applying to it $\rho_j^{-1}\tau\cdots\tau\rho_{n-1}^{-1}\tau\rho_n^{-1}$ for $j = n, n-1, \ldots, m$ if $d_m < d_{m+1}$ and for $j = n, n-1, \ldots, m+1$ if $d_m = d_{m+1}$.

Part 3. If $d_m < d_{m+1}$, we obtain the element

$$w_2 = \rho_m^{-1}\tau\cdots\tau\rho_{n-1}^{-1}\tau\rho_n^{-1}v,$$

and a system of algebraic equations depending on the unknown coefficients of ρ_i. Since $w_1 = \tau w_2$, we obtain one more relation between the coefficients of $\rho_0, \rho_1, \ldots, \rho_n$. If $d_m = d_{m+1}$, then we consider

$$w_2 = \rho_{m+1}^{-1}\tau\cdots\tau\rho_{n-1}^{-1}\tau\rho_n^{-1}v.$$

Then $w_2 = \tau\rho_m\tau w_1$ and we have two possibilities. If, writing τw_1 as a linear combination $\tau w_1 = \sum\gamma'_{ab}u_{ab}$ of the basis (4), we have $a_j = 0$ for all $\gamma'_{ab} \neq 0$, then

$$\tau w_1 = \sum\gamma'_{ab}y^{b_1}[x,y]\cdots[x,y]y^{b_{r+1}},$$

$$\rho_m\tau w_1 = \sum\gamma'_{ab}\xi_m^r\eta_m^r(\eta_m y + \eta'_m)^{b_1}[x,y]\cdots[x,y](\eta_m y + \eta'_m)^{b_{r+1}}.$$

Hence the result does not depend on the polynomial $p_m(y)$, we can choose it to be arbitrary. The corresponding algebraic system does not depend on its coefficients. If some a_i is positive, then we bound the degree of $p_m(y)$ and determine whether or not the obtained system has a solution with nonzero ξ_j, η_j and nonlinear $p_j(y)$. $\square$

Theorem 7. *Let K be an algebraically closed constructive field and let $u(x,y) \in K\langle x,y\rangle$. Then there is an algorithm which decides whether or not u is a semiinvariant of some $\varphi \in \mathrm{Aut}K\langle x,y\rangle$, and φ can be expressed in terms of the solutions of algebraic systems.*

Proof. Let $0 \neq u(x,y) \in K\langle x,y\rangle$. We want to find $\varphi \in \mathrm{Aut}K\langle x,y\rangle$ and a constant λ such that $\varphi u = \lambda u$. If $u(x,y) \in V$, then the action of $\varphi = (f,g)$ is determined by $\vartheta = \xi_1\eta_2 - \xi_2\eta_1$, where $f_1 = \xi_1 x + \xi_2 y$

and $g_1 = \eta_1 x + \eta_2 y$ are the linear components of f and g, respectively. In particular, u is stabilized by any φ with $\vartheta = 1$. We can find all possible values of ϑ as in the first part of the proof of Theorem 6. If $\varphi u = \sum_{k=0}^{m} \lambda_k \vartheta^k [x,y]^k$, then $\varphi u = \lambda u$ if and only if $\lambda = \vartheta^k$ for all k such that $\lambda_k \neq 0$. If $u(x,y) \notin V$, then the theorem of Lane implies that $\varphi = \psi^{-1}\rho\psi$ for some triangular or affine ρ and some $\psi \in \mathrm{Aut}K\langle x,y\rangle$. We write ψ in the form (3), $\psi = \rho_n\tau\cdots\tau\rho_1\tau\rho_0$. If ρ is triangular, we have

$$\begin{aligned}\varphi &= (\rho_n\tau\cdots\tau\rho_1\tau\rho_0)^{-1}\rho(\rho_n\tau\cdots\tau\rho_1\tau\rho_0)\\ &= \rho_0^{-1}\tau\rho_1^{-1}\tau\cdots\tau(\rho_n^{-1}\rho\rho_n)\tau\cdots\rho_1\tau\rho_0.\end{aligned}$$

If ρ is nontriangular affine, then it has the form $\rho = \rho''\tau\rho'$ some some affine triangular ρ', ρ'' and we proceed in a similar way. Then we complete the proof as in the second case of the proof of Theorem 6. □

Remark 8. The unitarity of $K\langle x,y\rangle$ is not essential. The same proofs work in the free nonunitary associative algebra in two variables.

4. Applications to commutative case

From now on we work in the polynomial algebra $K[x,y]$ over an arbitrary field K, keeping some notation from the case $K\langle x,y\rangle$. If $0 \neq u(x,y) \in K[x,y]$, we denote by $|u|$ the homogeneous component of maximum total degree and say that u is biased if $\deg_x|u| \geq \deg_y|u|$.

One of the main steps in the approach of Makar-Limanov, Shpilrain, and Yu [10] is Lemma 2 in [10]. A minor modification in its proof allows us to simplify the proof of the theorem for the existence of a nontrivial stabilizer of $u \in K[x,y]$.

Proposition 9. *Let $u(x,y) \in K[x,y]\backslash K$ be biased and let $\rho = (\alpha x + p(y), \beta y + \gamma)$ be a nonaffine triangular automorphism. Then* $\deg(\rho u) > \deg u$.

Proof. For simplicity of the exposition we assume that $\alpha = \beta = 1$ and $p(x) = x^k + \pi_{k-1}x^{k-1} + \cdots + \pi_1 x + \pi_0$ is monic, with $k \geq 2$. Let the homogeneous component of maximum degree of $u(x,y)$ be

$$|u| = \gamma_a x^a y^b + \gamma_{a-1}x^{a-1}y^{b+1} + \cdots + \gamma_1 x y^{a+b-1} + \gamma_{a+b}y^{a+b}, \quad \gamma_a \neq 0.$$

Since $u(x,y)$ is biased, we have $a \geq b$. Define a $(k,1)$-grading on $K[x,y]$ assuming that $\deg_{(k,1)}x = k$, $\deg_{(k,1)}y = 1$. Let $u_m(x,y)$ be the homogeneous component of u of $(k,1)$-degree m, and let

$$u_{ka+b}(x,y) = \beta_d x^d y^j + \beta_{d-1}x^{d-1}y^{j+k} + \cdots + \beta_e x^e y^{j+k(d-e)}, \quad \beta_d, \beta_e \neq 0.$$

Then, over the algebraic closure $\overline{K}$ of K, the $(k,1)$-homogenity of u_{ka+b} implies the decompostion

$$u_{ka+b}(x,y) = \xi x^q y^r (x-y^k)^s \prod_{i=1}^{t} (x-\lambda_i y^k), \quad 1 \neq \lambda_i \in \overline{K}.$$

Clearly,

$$\begin{aligned} \deg\, u_{ka+b} &= q+r+k(s+t) = e+(j+k(d-e)) \\ &> e+1+(j+k(d-e-1)) > \cdots > d+j. \end{aligned}$$

Since $k \geq 2$, the only summand of maximum total degree contained in u_{ka+b} is $\gamma_a x^a y^b$. We conclude that $\gamma_a x^a y^b = \beta_e x^e y^{j+k(d-e)}$ and this implies that

$$\begin{gathered} (a,b) = (e, j+k(d-e)) = (q, r+k(s+t)), \\ a+b = \deg\, u = \deg\, u_{ka+b} = q+r+k(s+t). \end{gathered}$$

As in the proof of Lemma 2 [10], the first step is to show that $\deg\, u_{ka+b}(x+y^k,y) > \deg\, u_{ka+b}(x,y)$. Let us assume that the oposite inequality $\deg\, u_{ka+b}(x+y^k,y) \leq \deg\, u_{ka+b}(x,y)$ holds. Since

$$u_{ka+b}(x+y^k,y) = \xi (x+y^k)^q y^r x^s \prod_{i=1}^{t} (x-(\lambda_i-1)y^k),$$

and $k \geq 2$, we derive that

$$\begin{gathered} \deg\, u_{ka+b}(x+y^k,y) = kq+r+s+kt \leq q+r+k(s+t) = \deg\, u_{ka+b}(x,y), \\ (k-1)q \leq (k-1)s, \quad q \leq s. \end{gathered}$$

Since $u(x,y)$ is biased and

$$q = a \geq b = r+k(s+t), \quad q > 0, r, s, t \geq 0,$$

we obtain that $q \geq 2s$. This is a contradiction because we already have $s \geq q > 0$. In this way $\deg\, u_{ka+b}(x+y^k,y) > \deg\, u(x,y)$. Since the leading $(k,1)$-components of $x+p(y)$ and $y+\gamma$ are $x+y^k$ and y, respectively, we derive that

$$\begin{gathered} u_m(x+p(y), y+\gamma) = u_m(x+y^k, y) \\ +(k,1)\text{-homogeneous components of lower } (k,1)\text{-degree}. \end{gathered}$$

Hence the monomials of $u_{ka+b}(x+y^k,y)$ can vanish in $u(x+p(y),y+\gamma)$ only if they cancel with some monomials from $u_m(x+p(y),y+\gamma)$ for $m > ka+b$. Let m_0 be the $(k,1)$-degree of $u(x,y)$. If $m_0 = ka+b$, then the monomials of $u_{ka+b}(x+y^k,y)$ do not cancel with anything. Hence $\deg(\rho u) \geq \deg\, u_{ka+b}(x+y^k,y) > \deg\, u(x,y)$. So, we may assume that

$m_0 > ka+b$. Again, the leading $(k,1)$-component of $u_{m_0}(x+p(y),y+\gamma)$ is $u_{m_0}(x+y^k,y)$. If

$$u_{m_0}(x,y) = \xi_0 x^{q_0} y^{r_0}(x-y^k)^{s_0}\prod_{i=1}^{t_0}(x-\lambda_i' y^k), \quad \lambda_i' \neq 1,$$

then the leading $(k,1)$-component of $u_{m_0}(x+p(y),y+\gamma)$ is

$$u_{m_0}(x+y^k,y) = \xi_0 (x+y^k)^{q_0} y^{r_0} x^{s_0}\prod_{i=1}^{t_0}(x-(\lambda_i'-1)y^k)$$

and does not cancel with other elements of $u(x+p(y),y+\gamma)$. In particular, $\deg u(x+p(y),y+\gamma) \geq \deg u_{m_0}(x+y^k,y)$. We have the inequalities

$$a+b = \deg u(x,y) \geq \deg u_{m_0}(x,y) = q_0+r_0+k(s_0+t_0), \tag{6}$$

$$kq_0+r_0+k(s_0+t_0) = m_0 > ka+b. \tag{7}$$

The sum of (6) and (7) gives

$$a+b+kq_0+r_0+k(s_0+t_0) > ka+b+q_0+r_0+k(s_0+t_0),$$

$$(k-1)q_0 > (k-1)a, \quad q_0 > a,$$

If we assume that

$$a+b = \deg u(x,y) \geq \deg u_{m_0}(x+y^k,y) = kq_0+r_0+s_0+kt_0, \tag{8}$$

then the sum of (7) and (8) implies

$$a+b+kq_0+r_0+k(s_0+t_0) > ka+b+kq_0+r_0+s_0+kt_0,$$

$$(k-1)s_0 > (k-1)a, \quad s_0 > a,$$

and (6) gives

$$2a \geq a+b \geq q_0+r_0+k(s_0+t_0) \geq q_0+s_0 > 2a,$$

which is impossible. Hence

$$\deg u(x+p(y),y+\gamma) \geq \deg u_{m_0}(x+y^k,y) > \deg u(x,y).$$

□

Proposition 9 implies immediately commutative analogues of Proposition 1 and Corollary 2. We shall state the first of them.

Corollary 10. *Let $u(x,y)\in K[x,y]\backslash K$ and let $\rho=(\alpha x+p(y),\beta y+\gamma)$ be a nonaffine triangular automorphism of $K[x,y]$. Then each of the following statements implies the next:*
(i) $u(x,y)$ *is biased;*
(ii) $\deg u<\deg(\tau\rho u)$*;*
(iii) $\deg u\leq\deg(\tau\rho u)$*;*
(iv) $\tau\rho u=u(\alpha y+p(x),\beta x+\gamma)$ *is biased.*

Proof. The only part of the proof left is the implication (iii) $\Longrightarrow$ (iv). If some $v(x,y)\in K[x,y]$ is not biased, then $v(y,x)=\tau v$ is. Hence, if $\tau\rho u$ is not biased, then ρu is and Proposition 9 gives that $\deg u=\deg(\rho^{-1}(\rho u))>\deg(\rho u)=\deg(\tau\rho u)$ which is a contradiction. □

Now we can prove easily the theorem of Lane [8] and Makar-Limanov, Shpirain, and Yu [10].

Theorem 11. *If K is any field and the automorphism φ of $K[x,y]$ is not conjugate to a linear or triangular automorphism, then any semiinvariant $u(x,y)\in K[x,y]$ of φ is a constant.*

Proof. Let $u(x,y)\in K[x,y]\backslash K$ and let G be the subgroup of $\mathrm{Aut}K[x,y]$ which stabilizes the vector space spanned by $u(x,y)$. Writing $\varphi\in G$ in the form (3), $\varphi=\rho_n\tau\cdots\tau\rho_1\tau\rho_0$ and applying the commutative analogue of Corollary 2, we obtain that the length n in the expression of φ is bounded by $2\cdot\deg u$. Now the proof is completed by the well known theorem in group theory (see e.g. Theorem 6.8.7, p. 351 [3]), which states that if G is a subgroup of $A*_C B$ and its elements are of the form

$$g=a_mb_m\cdots a_1b_1,\quad a_i\in A,\quad b_i\in B,$$

where the integers $m=m(g)$ are bounded by the same n for all $g\in G$, then G is conjugate to a subgroup of A or B. In order to replace the affine automorphisms with linear ones, we need to use the fact that $\mathrm{Aut}K[x,y]$ is also a free product of the linear group $GL_2(K)$ and the triangular group B with amalgamation over their intersection. □

Clearly, we have analogues for $K[x,y]$ of the algorithms described in Theorems 6 and 7 (compare the first algorithm with this of Makar-Limanov, Shpilrain, and Yu [10]). In particular, when K is an algebraically closed constructive field, we can decide whether or not $u\in K[x,y]$ is a semiinvariant of some $\varphi\in\mathrm{Aut}K[x,y]$ and to express φ in terms of solutions of algebraic systems.

Remark 12. Clearly, over an algebraically closed field K any linear automorphism can be triangularized. Smith [13] has determined the eigenvalues and the eigenvectors of any triangular automorphism ρ of $K[x,y]$ when $\text{char}K = 0$. Up to conjugation, the possibilities are:

(i) $\rho = (\alpha x, \beta y)$, $u(x,y)$ is a linear combination of monomials $x^n y^m$ with the same value of $\alpha^n \beta^m$;

(ii) $\rho = (\alpha x, \beta y + \gamma)$, $\gamma \neq 0$, $u(x,y)$ does not depend on y and is a linear combination of powers x^n with the same value of α^n;

(iii) $\rho = (\alpha x + p(y), \beta y)$, $p(y) \neq 0$, $u(x,y)$ does not depend on x and is a linear combination of powers y^m with the same value of β^m.

If $u = w(f)$ for some coordinate $f(x,y)$ and some polynomial $w(z)$, we have

$$u_x = \frac{\partial u}{\partial x} = w'(f) f_x, \quad u_y = \frac{\partial u}{\partial y} = w'(f) f_y,$$

and the ideal of $K[x,y]$ generated by f_x and f_y conicides with the whole $K[x,y]$. Hence the greatest common divisor of u_x and u_y is $w'(f)$ and this can be used to determine whether or not u is a semiinvariant of a nontrivial automorphism in the cases (ii) and (iii). We cannot see how to handle directly the case (i), i.e., to determine whether or not $u = w(f,g)$ with some specific properties of the polynomial $w(z,t)$.

Acknowledgements

The authors would like to thank L. Makar-Limanov and V. Shpilrain for helpful comments and an anonymous referee for the numerous suggestions for improving the exposition.

References

[1] W.W. Adams, P. Loustaunau, An Introduction to Gröbner bases, Graduate Studies in Mathematics **3**, American Mathematical Society, Providence, RI, 1994.

[2] T. Becker, V. Weispfenning, Gröbner Bases: A Computational Approach to Commutative Algebra, In cooperation with H. Kredel, Graduate Texts in Mathematics **141**, Springer-Verlag, New York, 1993.

[3] P.M. Cohn, Free Rings and Their Relations, Second Edition, Acad. Press, London, 1985.

[4] A.J. Czerniakiewicz, Automorphisms of a free associative algebra of rank 2. I, II, Trans. Amer. Math. Soc. **160** (1971), 393-401; **171** (1972), 309-315.

[5] V. Drensky, J.-T. Yu, Test polynomials for automorphisms of polynomial and free associative algebras, J. Algebra **207** (1998), No. 2, 491-510.

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

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

[8] D.R. Lane, Free Algebras of Rank Two and Their Automorphisms, Thesis, London Univiversity, 1976.

[9] L.G. Makar-Limanov, On automorphisms of free algebra with two generators (Russian), Funk. Analiz i ego Prilozh. **4** (1970), No. 3, 107-108. Translation: Functional Anal. Appl. **4** (1970), 262-263.

[10] L. Makar-Limanov, V. Shpilrain, J.-T. Yu, Equivalence of polynomials under automorphisms of $K[x,y]$, J. Pure Appl. Algebra (to appear).

[11] V. Shpilrain, J.-T. Yu, On generators of polynomial algebras in two commuting or non-commuting variables, J. Pure Appl. Algebra **132** (1998), No. 3, 309-315.

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

[13] M. Smith, Eigenvectors of automorphisms of polynomial rings in two variables, Houston J. Math. **10** (1984), No. 4, 559-573.

[14] P.G. Wightwick, Equivalence of polynomials under automorphisms of $\mathbb{C}^2$, J. Pure Appl. Algebra **157** (2001), No. 2-3, 341-367.

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria

E-mail address: `drensky@math.bas.bg`

Department of Mathematics, The University of Hong Kong, Hong Kong SAR, China

E-mail address: `yujt@hkucc.hku.hk`