HONG KONG – 2001

TOPICS IN ALGEBRA

INVARIANTS AND AUTOMORPHISMS OF POLYNOMIAL ALGEBRAS

Vesselin Drensky
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Block 8, 1113 Sofia, Bulgaria

Table of Contents

1. POLYNOMIAL ALGEBRAS

We fix the following notation:
K is any field, e.g. the field $\mathbf{Q}$ of rational numbers, the field $\mathbf{R}$ of real numbers, the field $\mathbf{C}$ of complex numbers or the finite field $\mathbf{F}_q$ with q elements, where $q = p^m$ for some prime p and a positive integer m, etc. We shall call the elements of K scalars or constants. All vector spaces are over a fixed field K.

Definition 1.1. A vector space R is called an *associative algebra* with 1 (or a unitary associative algebra), if R is equipped with a binary operation $\cdot$ (i.e. a mapping $(R, R) \to R$) called *multiplication*, such that for any $a, b, c \in R$ and any constant $\alpha \in K$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),\ (a + b) \cdot c = a \cdot c + b \cdot c,\ a \cdot (b + c) = a \cdot b + a \cdot c,$$

$$\alpha(a \cdot b) = (\alpha a) \cdot b = a \cdot (\alpha b).$$

In other words, the notion of algebra generalize both the notion of vector space and of ring. If we want to emphasize that R is an algebra over K, we shall say that R is a K-algebra. The algebra is called *commutative* if it additionally satisfies the property

$$a \cdot b = b \cdot a$$

for all $a, b \in R$. Usually we shall omit the $\cdot$ in the multiplication and shall denote $a \cdot b$ by ab.

Examples 1.2. (i) The field K itself is a commutative algebra with respect to the usual operations. Every field extension L of the field K is also a commutative K-algebra.

(ii) The ring of polynomials $K[x]$ in one variable x is an algebra. Another example is the field $K(x)$ of rational functions. By definition, $K(x)$ consists of all fractions $f(x)/g(x)$ of two polynomials $f(x)$ and $g(x)$, where $g(x) \neq 0$. Recall, that in Algebra usually we do not consider polynomials as functions and $g(x) \neq 0$ means that at least one of the coefficients of $g(x)$ is not equal to zero.

(iii) The ring of polynomials $K[x_1, \ldots, x_n]$ in n (a fixed number) variables $x_1, \ldots, x_n$ is also an algebra. When we consider polynomials in small number of variables, we shall usually denote the variables by x, y, z, etc.

(iv) The ring $M_n(K)$ of all $n \times n$ matrices with entries from K is an example of a non-commutative algebra.

In the all part of the course we shall consider commutative algebras only.

Definition 1.3. The vector subspace S of the algebra R is called a *subalgebra* if it contains 1 and is closed with respect to the multiplication. (Clearly, our definition of algebra implies that any algebra contains the base field K as a subalgebra.) The subalgebra S is generated by the set of its elements $\{s_1, s_2, \ldots\}$ (called *generators of* S) if every element $s \in S$ can be presented as a finite sum of the form

$$s = \sum \alpha_i s_{i_1} \ldots s_{i_k},\ \alpha_i \in K.$$

Sometimes we shall denote this by $S = K[s_1, s_2, \ldots]$. Usually from the context will be clear whether $s_1, s_2, \ldots$ are variables (i.e. S is a polynomial algebra in many (maybe infinitely

many) variables, or $s_1, s_2, \ldots$ are simply the generators of S. The subalgebra S is *finitely generated*, respectively, *n-generated* if it can be generated by a finite set, respectively, by a set with n elements. The vector subspace U of R is called an *ideal* if for every $u \in U$ and every $a \in R$ the products ua and au belong to U (we denote this property by $RU \subseteq U$ and $UR \subset U$). The ideal U is generated by the set of its elements $\{u_1, u_2, \ldots\}$ if every element $u \in U$ is of the form

$$u = \sum a_i u_i b_i,\ a_i, b_i \in R.$$

The notions of finite generation and n-generation of ideals are similar to those for subalgebras. In the case of commutative algebras, the ideal U is *principal* if it is generated by one element, i.e. there exists an element $u_0 \in U$ such that $U = \{au_0 \mid a \in R\}$.

The notion of factor algebra R/U of the algebra R modulo the ideal U is similar to the corresponding notion for rings. The basic theorems for ideals and factor rings are true also in the case of algebras. In particular, the elements of $\bar{R} = R/U$ are the classes $\bar{a} = a + U = \{a + u \mid u \in U\}$ and the operations are defined by

$$(a+U) + (b+U) = (a+b) + U,\ \alpha(a+U) = (\alpha a) + U,\ (a+U)(b+U) = ab + U.$$

The notions of homomorphism and isomorphism are also similar to the corresponding notions for rings. In particular, the homomorphisms $R \to R$ are called *endomorphisms* and the isomorphisms $R \to R$ are *automorphisms*.

Remark 1.4. It is a basic result of the undergraduate Algebra course, that every ideal of the polynomial algebra in one variable is principal and its generator can be found by the Euclidean algorithm. For the algebra of polynomials in more than one variable this is not more true. For example, the set of all polynomials without constant terms (i.e. $f(0,0) = 0$) in $K[x, y]$ is an ideal which is not principal.

The following easy proposition gives one of the universal properties of polynomial algebras in the class of all commutative algebras.

Proposition 1.5. *Every finitely generated commutative algebra is a homomorphic image of some polynomial algebra.*

Proof. Let the commutative algebra R be generated by the finite set $\{r_1, \ldots, r_n\}$. We define a mapping $\phi : K[x_1, \ldots, x_n] \to R$ by

$$\phi\left(\sum \alpha_k x_1^{k_1} \ldots x_n^{k_n}\right) = \sum \alpha_k r_1^{k_1} \ldots r_n^{k_n},\ \alpha_i \in K.$$

Clearly ϕ is a homomorphism of algebras. (Why? Use that the commutativity of R implies that ϕ is well defined.) Since the generators $r_1, \ldots, r_n$ of R are the images of $x_1, \ldots, x_n$, we obtain that the mapping ϕ is onto R. By the isomorphism theorem the image $\mathrm{Im}(\phi)$ of ϕ is isomorphic to the factor algebra $K[x_1, \ldots, x_n]/\mathrm{Ker}(\phi)$ of $K[x_1, \ldots, x_n]$ modulo the kernel $\mathrm{Ker}(\phi)$.

Definition 1.6. If the algebra R is isomorphic to $K[x_1, \ldots, x_n]/U$ for some ideal U generated by the set of polynomials $\{u_i(x_1, \ldots, x_n) \mid i = 1, 2, \ldots\}$, then we say that $\{u_i(x_1, \ldots, x_n) = 0 \mid i = 1, 2, \ldots\}$ is a set of *defining relations* of the algebra R and write this as

$$R = K[x_1, \ldots, x_n \mid u_i(x_1, \ldots, x_n) = 0,\ i = 1, 2, \ldots].$$

The algebra is *finitely presented* if it is finitely generated and has a finite number of defining relations.

Definition 1.7. The (commutative) algebra R is called *noetherian* if every ideal of R is finitely generated.

Hilbert Basis Theorem 1.8. *If R is a noetheiran algebra, then the algebra of polynomials $R[x]$ is also noetherian.*

Proof. Let R be noetherian and let U be any ideal of $R[x]$. If $U = (0)$, then it is finitely generated and without loss of generality we may assume that $U \neq 0$. For each $n \geq 0$ we define the set V_n of R consisting of all $b \in R$ such that there exists a polynomial $f(x) = bx^n + b_1x^{n-1} + \ldots + b_{n-1}x + b_n$ in U of degree n and with leading coefficient b (or $b = 0$). It is easy to see that V_n is an ideal of R. (*Proof.* If $b, c \in V_n$, then there exist polynomials $f(x), g(x) \in U$ of degree n and with leading coefficients b, c, respectively. Then $f(x) \pm g(x) \in U$ and its leading coefficient is equal to $b \pm c$ and, since the elements of R are polynomials of zero degree, for each $a \in R$ the polynomial $af(x)$ with leading coefficient ab is also in U.) If $b \in V_n$ and $f(x) \in U$ is a polynomial with leading coefficient b, then b is also the leading coefficient of $xf(x) \in U$ and we obtain that $V_n \subseteq V_{n+1}$. In this way we obtain an ascending chain of ideals $V_0 \subseteq V_1 \subseteq V_2 \subseteq \ldots$. The union $V = \cup_{n\geq 0} V_n$ of the elements of the chain is also an ideal of R (prove it!). Since R is noetherian, we derive that the ideal V is generated by some finite set of elements $\{c_1, \ldots, c_s\}$. Let k be a positive integer with the property that all $c_1, \ldots, c_s$ belong to V_k. Then $V = V_k = V_{k+1} = \ldots$. For each $m \leq k$ we consider a finite set of generators $\{b_{m1}, \ldots, b_{mq_m}\}$ of the ideal V_m and choose in U polynomials $f_{m1}(x), \ldots, f_{mq_m}(x)$ of degree m and with leading coefficients $b_{m1}, \ldots, b_{mq_m}$. We shall show by induction on the degree d of $f(x) \in U$ that the finite set

$$\{f_{m1}(x), \ldots, f_{mq_m}(x) \mid m = 0, 1, \ldots, k\}$$

generates the ideal U. Let W be the ideal of $R[x]$ generated by this set. The base of the induction is $d = 0$. Then $f(x) = b$ is a constant and, by the definition of V_0, we obtain that $b \in V_0$. Hence, there exist $a_1, \ldots, a_{q_0} \in R$ such that $b = a_0b_{01} + \ldots + a_{q_0}b_{0q_0}$. Again, since $f_{0i}(x) \in U$ are polynomials of degree 0, we have that $f_{0i}(x) = b_{0i}$ and $b = f(x) = a_0f_{01}(x) + \ldots + a_{m_0}f_{0q_0}(x)$ is in W. Now, let $d \leq k$. If $b \in V_d$, then $b = a_0b_{d1} + \ldots + a_{q_d}b_{dq_d}$ for some $a_1, \ldots, a_{q_d} \in R$. Then the leading coefficient of $g(x) = a_0f_{d1}(x) + \ldots + a_{q_d}f_{dq_d}(x)$ is also equal to b. Since $g(x) \in W$ and $W \subset U$, we obtain that the degree of $h(x) = f(x) - g(x)$ is less than d and, by induction, $h(x) \in W$. Hence $f(x) = g(x) + h(x)$ also belongs to W. The considerations for $d > n$ are similar: If $f(x) = bx^d + b_1x^{d-1} + \ldots + b_d \in U$, since $V_d = V_k$, we have that $b = a_0b_{k1} + \ldots + a_{q_k}b_{kq_k}$ for some $a_1, \ldots, a_{q_d} \in R$. Hence $g(x) = (a_0x^{d-k})f_{k1}(x) + \ldots + (a_{q_k}x^{d-k})f_{kq_k}(x)$ belongs to W. By inductive arguments, $h(x) = f(x) - g(x) \in W$ and $f(x) \in W$.

Corollary 1.9. *The algebra of polynomials $K[x_1, \ldots, x_n]$ in n variables over any field K is noetherian.*

Proof. The only ideals of the field K are (0) and K (because every nonzero element of K is invertible and generates K as an ideal). Hence K is a noetherian algebra. Then we proceed by induction on the number of variables. If $R_{n-1} = K[x_1, \ldots, x_{n-1}]$ is already noetheiran (where $R_0 = K$), then by Hilbert Basis Theorem,

$$R_{n-1}[x_n] = (K[x_1, \ldots, x_{n-1}])[x_n] = K[x_1, \ldots, x_n]$$

is also noetherian.

The following corollary follows immediately from Hilbert Basis Theorem and Proposition 1.5.

Corollary 1.10. *Every finitely generated commutative algebra is finitely presented.*

Corollary 1.11. *Every finitely generated commutative algebra is noetherian.*

Proof. Let $R \cong K[x_1, \ldots, x_n]/U$ for some ideal U and let V be any ideal of R. We take any ideal W in $K[x_1, \ldots, x_n]$ which maps onto V modulo U. By Hilbert Basis Theorem, the ideal W is finitely generated. Hence its homomorphic image V is also finitely generated in the homomorphic image R of $K[x_1, \ldots, x_n]$ modulo U.

Definition 1.12. (i) The vector space V is called *graded* if it is presented as a direct sum of its subspaces V_d, $d = 0, 1, 2, \ldots$, i.e.

$$V = V_0 \oplus V_1 \oplus V_2 \oplus \ldots = \sum_{d \geq 0}^{\oplus} V_d.$$

The subspace V_d is called the homogeneous component of degree d of V. The subspace W of V is a *graded* (or *homogeneous*) *subspace* if $W = \sum_{d \geq 0}(W \cap V_d)$. In this case, the factor space $V/W = \sum_{d \geq 0} V_d/(W \cap V_d)$ can also be naturally graded (and we say that V/W *inherits the grading* of V).

(ii) If all homogeneous components V_d of the graded vector space V are finite dimensional, then the formal power series

$$H(V, t) = \mathrm{Hilb}(V, t) = \sum_{d \geq 0} (\dim V_d) t^d$$

is called the *Hilbert* (or *Poincaré*) *series of* V. For a function $f(t)$, we shall write $H(V, t) = f(t)$ if $H(V, t)$ converges in some neighbourhood of 0 and the functions $H(V, t)$ and $f(t)$ are equal there.

Definition 1.13. The algebra R is *graded*, if it is graded as a vector space and its homogeneous components R_d satisfy $R_d R_e \subseteq R_{d+e}$ for all $d, e \geq 0$.

Example 1.14. The polynomial algebra $R = K[x_1, \ldots, n_n]$ in n variables is naturally graded with homogeneous component R_d of degree d consisting of all homogeneous polynomials of degree d. Since a basis of R_d consists of all monomials $x_1^{d_1} \ldots x_n^{d_n}$ of total degree d (i.e. $d_1 + \ldots + d_n = d$), we obtain for the Hilbert series of R:

$$H(K[x_1, \ldots, x_n], t) = \sum_{d_i \geq 0} t^{d_1} \ldots t^{d_n} = \frac{1}{(1-t)^d}$$

because $\sum_{d \geq 0} t^d = 1/(1-t)$.

Remark 1.15. The Hilbert-Serre theorem states that the Hilbert series of any finitely generated graded commutative algebra is rational (i.e. is equal to a rational function).

Exercises

1. (i) Show that the subalgebra $K[x^2, x^3]$ of $K[x]$ generated by x^2 and x^3 consists of all polynomials with coefficient of x^1 equal to 0.

(ii) Show that $K[x^2, x^3]$ is isomorphic to the factor algebra of $K[y, z]$ modulo the principal ideal generated by $y^3 - z^2$.

2. (i) Show that the algebra of *Laurent polynomials* in one variable generated as a subalgebra of $K(x)$ by x and x^{-1}, consists of all rational functions of the form $\sum_{i=-p}^{q} a_i x^i$, $a_i \in K$. Very often this algebra is denoted by $K[x, x^{-1}]$.

(ii) Show that every ideal of the algebra of Laurent polynomials is principal. (*Hint.* Use that if U is an ideal of $K[x, x^{-1}]$ and $0 \neq f(x) \in U$, then we may write $f(x)$ as $f(x) = x^{-m} g(x)$, $g(x) \in U \cap K[x]$. Take a nonzero element $h(x)$ of minimal degree in $U \cap K[x]$ and show that U is generated by $h(x)$.)

(iii) Show that $K[x, x^{-1}]$ is isomorphic to the factor algebra $K[x, y]/(xy-1)$ of $K[x, y]$ modulo the ideal generated by $xy - 1$.

3. Let V be a vector space with basis $\{v_i \mid i = 1, 2, \ldots\}$. Let us define a multiplication between the basis elements by $v_i \cdot v_j = \sum_k \alpha_{ij}^k v_k$, where for fixed i, j only a finite number of constants α_{ij}^k are different from 0. Show that the operation

$$\left(\sum_{i=1}^{m} \beta_i v_i\right) \cdot \left(\sum_{j=1}^{n} \gamma_j v_j\right) = \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k} \beta_i \gamma_j \alpha_{ij}^k v_k$$

gives to the vector space the structure of algebra if and only if $(v_i \cdot v_j) \cdot v_l = v_i \cdot (v_j \cdot v_l)$ for all basis elements v_i, v_j, v_l and there exists an element $e \in V$ such that $e \cdot v_i = v_i \cdot e = v_i$ for all basis elements v_i. This algebra is commutative if and only if $v_i \cdot v_j = v_j \cdot v_i$ for all i, j.

4. If G is a group, then the *group algebra* KG is defined as a vector space with basis consisting of the elements of G and multiplication between the basis elements given by $g \cdot h = gh$, where gh is the product in G of $g, h \in G$. (We say that the multiplication in KG is defined by the group operation in G.) Show that the group algebra is an algebra which is commutative if and only if the group G is abelian.

5. (i) Let $G = \langle g \mid g^n = 1 \rangle$ be the cyclic group of order n. Show that the group algebra KG is isomorphic to the factor algebra $K[x]/(x^n - 1)$ of the polynomial algebra in one variable modulo the ideal generated by $x^n - 1$.

(ii) If G is an infinite cyclic group, show that its group algebra is isomorphic to the algebra of Laurent polynomials in one variable.

6. Calculate the Hilbert series of:

(i) $R = K[x, y]/(x^2 - y^2)$;

(ii) $R = K[x, y]/(x^2 - y^2, x^3 - y^3)$. (*Hint.* Use that in the factor algebra $x(x^2 - y^2) = x^3 - y^3 = 0$ and $xy^2 - y^3 = 0$. Hence every element of R has the form $f(y) + x(a + by)$, $f(y) \in K[y]$, $a, b \in K$. Using that the ideal $(x^2 - y^2, x^3 - y^3)$ in $K[x, y]$ is homogeneous, show that the elements $1, y, y^2, y^3, \ldots, x, xy$ are linearly independent in R.)

7. Calculate the Hilbert series of the algebra of symmetric polynomials in n variables.

8. Calculate the Hilbert series of the subalgebra R of $K[x,y,z]$ generated by

$$e_1(x,y,z) = x+y+z,\ e_2(x,y,z) = xy+xz+yz,\ e_3(x,y,z) = xyz,$$

$$f(x,y,z) = x^2y + y^2z + z^2y$$

and find a presentation of this algebra as a homomorphic image of $K[u_1,u_2,u_3,u_4]$. (*Hint.* Show that $g(x,y,z) = f(x,y,z) + f(y,x,z)$ and $f(x,y,z)(g(x,y,z) - f(x,y,z))$ are symmetric polynomials and derive that as a vector space $R{=}S \oplus f(x,y,z)S$, where S is the algebra of symmetric polynomials in three variables. Show that R is a homomorphic image of $K[u_1,u_2,u_3,u_4]$ (with $u_i \to e_i$, $i=1,2,3$, $u_4 \to f$) modulo a principal ideal generated by a polynomial of second degree with respect to u_4.)

9*. Show that every subalgebra of $K[x]$ is finitely generated. (*Hint.* Let R be a nonzero subalgebra of $K[x]$ and let D be the set of $d \in \mathbf{N} \cup \{0\}$ such that there exists a polynomial of degree d in R. Show that D is an additivelly written semigroup which is finitely generated. For each generator d_i of D take a polynomial f_i of degree d_i in R and show that the set of all f_i generates R.)

10. Show that the subalgebra R of $K[x,y]$ generated by all xy^k, $k=0,1,2,\ldots$, is not finitely generated. (*Hint.* If R is finitely generated, then it can be generated by a finite number of polynomials $x, xy, xy^2, \ldots, xy^n$. Show that xy^{n+1} cannot be expressed as a polynomial in $x, xy, \ldots, xy^n$.)

2. INVARIANT THEORY OF FINITE GROUPS

In this section we assume that K is a fixed algebraically closed field of characteristic 0, e.g. $K = \mathbf{C}$. The assumption that K is algebraically closed is not essential for the results (but simplifies the proofs). The requirement for the characteristic is essential. We fix an n-dimensional vector space V with basis $\{x_1, \ldots, x_n\}$ and assume that V is contained in the polynomial algebra $K[x_1, \ldots, x_n]$. In this way, we consider the elements of V as linear (and homogeneous) polynomials in n variables.

The group $GL_n(K) = GL(V)$ of all invertible linear operators on V can be identified (fixing some basis of V, e.g. $\{x_1, \ldots, x_n\}$) with the group of all invertible $n \times n$ matrices with entries from K. It acts on V and this action can be extended to an action on $K[x_1, \ldots, x_n]$ by

$$(g(f))(x_1, \ldots, x_n)) = f(g(x_1), \ldots, g(x_n)),$$

$$g \in GL_n(K), f = f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n].$$

Since every mapping $x_i \to K[x_1, \ldots, x_n]$, $i = 1, \ldots, n$, induces an endomorphism of $K[x_1, \ldots, x_n]$, and the elements of $GL_n(K)$ act invertible on V, we obtain that $GL_n(K)$ acts as a group of automorphisms of $K[x_1, \ldots, x_n]$. Pay attention, that this action is homogeneous. Since $g(x_i)$, $g \in GL_n(K)$, is a linear combination of $x_1, \ldots, x_n$, if f is a homogeneous polynomial of degree d, then $g(f)$ is also homogeneous of the same degree d.

Definition 2.1. Let G be a subgroup of $GL_n(K)$. The polynomials $f = f(x_1, \ldots, x_n)$ in $K[x_1, \ldots, x_n]$ with the property that $g(f) = f$ for all $g \in G$ are called *invariants of* G (or G*-invariants*). The set of all G-invariants is called the *algebra of invariants of* G. We shall denote it by $K[x_1, \ldots, x_n]^G$.

Exercise 2.2. Show that the algebra of invariants $K[x_1, \ldots, x_n]^G$ is a graded subalgebra of the polynomial algebra $K[x_1, \ldots, x_n]$ for any subgroup G of $GL_n(K)$. (*Hint.* In order to prove that $K[x_1, \ldots, x_n]^G$ is graded, write the invariant polynomials in the form $f = f_0 + f_1 + \ldots + f_m$, where f_d is homogeneous of degree d. Then $f = g(f) = g(f_0) + g(f_1) + \ldots + g(f_m)$ for $g \in G$ and $g(f_d)$ is homogeneous of degree d. Comparing the homogeneous components of f and $g(f)$ we obtain that $g(f_d) = f_d$.)

Till the end of the section we fix: $R = K[x_1, \ldots, x_n]$. For every graded subspace W of R we denote by W_d its homogeneous component of degree d. $V = R_1$ is the subspace of R with basis $\{x_1, \ldots, x_n\}$ $G = \{g_1, \ldots, g_k\}$ is a finite subgroup of $GL_n(K)$ with k elements and $S = R^G$ is the algebra of G-invariants.

Examples 2.3. (i) The symmetric group S_n may be considered as a subgroup of $GL_n(K)$ acting on R by $\sigma(f) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. The theory of symmetric polynomials gives that the algebra of invariants $S = R^{S_n}$ consists of the symmetric polynomials in n variables. This algebra is generated by the elementary symmetric polynomials

$$e_1 = x_1 + x_2 + \ldots + x_n,\ e_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \ldots, e_n = x_1x_2 \ldots x_n$$

and the elementary symmetric polynomials are algebraically independent, i.e. S is isomorphic to the polynomial algebra $K[e_1, e_2, \ldots, e_n]$.

(ii) Let $R = K[x, y, z]$ and let G be the cyclic group of order 3 generated by the linear operator g defined by

$$g(x) = y,\ g(y) = z,\ g(z) = x,$$

i.e. G is the subgroup of S_3 generated by

$$g = \begin{pmatrix} x & y & z \\ y & z & x \end{pmatrix}.$$

Then all symmetric functions are invariants of G but G has also other invariants, e.g. $f(x,y,z) = x^2y + y^2z + z^2y$. One can show (see the exercises in the end of the section) that R^G is generated by the elementary symmetric polynomials e_1, e_2, e_3 and f.

(iii) The dihedral group D_8 of order 8 of all symmetries of the square with vertices $A_1 = (1,0)$, $A_2 = (0,1)$, $A_3 = (-1,0)$, $A_4(0,-1)$ is isomorphic to the subgroup of the symmetric group S_4 generated by $\sigma_1 = (1234)$ and $\tau_1 = (24)$ (where S_4 acts on the vertices A_1, A_2, A_3, A_4). The corresponding matrices in $GL_2(K)$ are

$$\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The polynomial $f(x,y) = x^2 + y^2$ is a D_8-invariant.

Lemma 2.4. *Let ϕ be any linear operator of a vector space W of any (maybe infinite) dimension and such that $\phi^2 = \phi$. Then W is a direct sum of the image* $\mathrm{Im}(\phi)$ *and the kernel* $\mathrm{Ker}(\phi)$ *and ϕ acts as the identity map on* $\mathrm{Im}(\phi)$.

Proof. Every element $w \in W$ can be written as $w = \phi(w) + (w - \phi(w))$. Obviously $\phi(w)$ is in $\mathrm{Im}(\phi)$ and, since $\phi^2 = \phi$, we obtain that $\phi((w - \phi(w)) = \phi(w) - \phi^2(w) = 0$ and $w - \phi(w) \in \mathrm{Ker}(\phi)$. Hence $W = \mathrm{Im}(\phi) + \mathrm{Ker}(\phi)$ and we have to show that $\mathrm{Im}(\phi) \cap \mathrm{Ker}(\phi) = 0$. If $w_1 = \phi(w) \in \mathrm{Im}(\phi)$, then $\phi(w_1) = \phi^2(w) = \phi(w) = w_1$ and ϕ acts identically on $\mathrm{Im}(\phi)$. Hence, if $w_1 \in \mathrm{Ker}(\phi)$, then $0 = \phi(w_1) = w_1$. In this way, W is a direct sum of its subspaces $\mathrm{Im}(\phi)$ and $\mathrm{Ker}(\phi)$ and ϕ acts as the identity map on $\mathrm{Im}(\phi)$.

Now we define the *Reynolds operator* on R by

$$\rho(f) = \frac{1}{|G|} \sum_{g \in G} g(f),\ f \in R.$$

Proposition 2.5. *The Reynolds operator ρ satisfies:*
(i) $h(\rho(f)) = \rho(f)$ *for any $h \in G$ and $f \in R$.*
(ii) $\rho^2 = \rho$.
(iii) *The polynomial $f \in R$ is a G-invariant if and only if $\rho(f) = f$. As a vector space, the algebra of invariants is spanned by all polynomials of the form $\rho\left(x_1^{d_1} \dots x_n^{d_n}\right)$.*
(iv) $\rho(fh) = f\rho(h)$ *for every G-invariant f and every polynomial $h \in R$.*

Proof. (i) For any $h \in G$ and $f \in R$,

$$h(\rho(f)) = h\left(\frac{1}{|G|} \sum_{g \in G} g(f)\right) = \frac{1}{|G|} \sum_{g \in G} (hg)(f).$$

Since the sets $hG = \{hg \mid g \in G\}$ and G coincide, we obtain that

$$h(\rho(f)) = \frac{1}{|G|} \sum_{g \in G} g(f) = \rho(f).$$

(ii) By (i)

$$\rho^2(f) = \frac{1}{|G|}\sum_{g\in G} g(\rho(f)) = \frac{1}{|G|}\sum_{g\in G}\rho(f) = \rho(f).$$

(iii) If f is a G-invariant, then $g(f) = f$ for every $g \in G$ and

$$\rho(f) = \frac{1}{|G|}\sum_{g\in G} g(f) = \frac{1}{|G|}\sum_{g\in G} f = f.$$

If $\rho(f) = f$, then $g(\rho(f)) = \rho(f) = f$ for every $g \in G$ and f is G-invariant. Since $S = R^G = \mathrm{Im}(\rho) = \rho(R)$ and R is spanned by all polynomials $\rho\left(x_1^{d_1}\dots x_n^{d_n}\right)$, we obtain the statement for the generating set of S.

(iv) Since G acts as a group of automorphisms of R and $g(fh) = g(f)g(h)$ for every $g \in G$ and $f, h \in R$, if $f \in S = R^G$, then $g(f) = f$ and

$$\rho(fg) = \frac{1}{|G|}\sum_{g\in G} g(fh) = \frac{1}{|G|}\sum_{g\in G} g(f)g(h) = \frac{1}{|G|}\sum_{g\in G} fg(h) = f\left(\frac{1}{|G|}\sum_{g\in G} g(h)\right) = f\rho(h).$$

Now we shall prove the following theorem of Emmy Noether, which is one of the most important theorems of invariant theory of finite groups.

Theorem 2.6. *The algebra of invariants of any finite group is finitely generated.*

Proof. Let G be a finite subgroup of $GL_n(K)$, $R = K[x_1, \dots, x_n]$ and let $S = R^G$ be the algebra of invariants of G. The homogeneous components of the polynomials in S are also invariants and we consider the ideal U of R generated by the homogeneous invariants of positive degree. Clearly, U is a graded subspace of R. By Hilbert Basis Theorem the ideal U is finitely generated and we may choose a finite set $\{f_1, \dots, f_m\}$ of homogeneous invariants which generate U. Let S_0 be the subalgebra of S generated by the invariants $f_1, \dots, f_m$. We shall show that $S_0 = S$. Let us assume that $S \neq S_0$ and let $f \in S$ be a homogeneous invariant of minimal degree which is not in S_0. Then, since $f \in U$, there exist some polynomials $h_1, \dots, h_m \in R$ such that $f = f_1h_1 + f_2h_2 + \dots + f_mh_m$. Since we work with homogeneous polynomials $f, f_1, \dots, f_m$, we may choose $h_1, \dots, h_m$ also homogeneous. All invariants $f_1, \dots, f_m$ are of positive degree and hence the degrees of $h_1, \dots, h_m$ are lower than the degree of f. By Proposition 2.5,

$$f = \rho(f) = \rho(f_1h_1 + \dots + f_mh_m) = f_1\rho(h_1) + \dots + f_m\rho(h_m)$$

and f is expressed by the generators $f_1, \dots, f_m$ of S_0 and the invariants $\rho(h_1), \dots, \rho(h_m)$. Since $\deg(\rho(h_i)) = \deg(h_i) < \deg(f)$, by the minimality of the degree of f, all $\rho(h_i)$ belong to S_0. Hence f also belongs to S_0 and we reach a contradiction with the assumption that $f \notin S_0$.

The following statement is a consequence of the proof of Theorem 2.6.

Corollary 2.7. *For any finite group G, let U be the ideal of $R = K[x_1, \dots, x_n]$ generated by the homogeneous G-invariants of positive degree. Then any set of generators of U which is in $S = R^G$ generates S as a subalgebra of R.*

Remark 2.8. (i) The original proof of Theorem 2.8 given by Emmy Noether (see [St]) contains also an upper bound for the degree of the generators of $S = R^G$: *The algebra S is generated by elements of degree $\leq |G|$.* Of course, these generators can be chosen as in Proposition 2.5 (iii).

(ii) One of the most famous problems in Invariant Theory is the 14-th Hilbert Problem from 1900, a partial case of which asks *whether the algebra of invariants $K[x_1, \ldots, x_n]^G$ is finitely generated for any subgroup G of $GL_n(K)$.* The negative answer was given by Nagata in the 1950's (for the exposition of the result of Nagata see [DC]).

Proposition 2.9. *For $|G| < \infty$ the algebra of invariants R^G has the same transcendence degree as $R = K[x_1, \ldots, x_n]$ and every element of R is a linear combination with coefficients in S of the polynomials $x_1^{d_1} \ldots x_n^{d_n}$, where $d_i < |G|$.*

Proof. Let $G = \{g_1, \ldots, g_k\}$, let $f \in R$ and let

$$h_f(z) = \prod_{g \in G} (z - g(f)) = z^k - e_1 z^{k-1} + e_2 z^{k-2} - \ldots + (-1)^{k-1} e_{k-1} z + (-1)^k e_k,$$

where $e_i = e_i(g_1(f), \ldots, g_k(f))$ are the elementary symmetric polynomials in $g_1(f), \ldots, g_k(f)$. Since $gG = G$ for any $g \in G$, we obtain that

$$g(e_i) = e_i((gg_1)(f), \ldots, (gg_k)(f)) = e_i(g_1(f), \ldots, g_k(f))$$

and e_i is G-invariant. Since some of the elements g_j in G is equal to the identity element of G, we obtain for it that $g_j(f) = f$ and $h_f(f) = 0$. Hence every element of R is algebraic on S and this implies that R and S have the same transcendence degree. Applying the above considerations for the variables x_i, we obtain that x_i^k is a linear combination with coefficients in S of $1, x_i, \ldots, x_i^{k-1}$. From here one easily derives that all degrees of x_i have the same property and this completes the proof.

Remark 2.10. Since the algebra of invariants of a finite group G is finitely generated, it is an image of a polynomial algebra in a finite number of variables. Usually a theorem which gives a set of generators of R^G is called *The First Fundamental Theorem of Invariant Theory of G* and a theorem giving the defining relations between these generators is called *The Second Fundamental Theorem of Invariant Theory of G.*

Example 2.11. (See Example 2.3 (i)) The First Fundamental Theorem of Invariant Theory of S_n states that the elementary symmetric polynomials generate the algebra of invariants. The Second Fundamental Theorem gives that these generators are algebraically independent, i.e. do not satisfy any nontrivial relation. Other examples will be considered in the exercises.

Lemma 2.12. *If $g \in GL_n(K)$ satisfies $g^r = 1$ for some $r > 0$, then g is diagonalizable, i.e. the linear operator corresponding to the matrix g has a diagonal matrix with respect to a properly chosen basis.*

Proof. Since the field K is algebraically closed, every matrix is similar to it Jordan normal form and we shall fix a Jordan basis for the operator of g. In other words, changing the basis of the vector space, we may think that the matrix g consists of blocks

$$g = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & J_s \end{pmatrix},$$

where each matrix J_i is of the form

$$J_i = \begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots\vdots & \\ 0 & 0 & 0 & \cdots & \lambda_i & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{pmatrix}$$

and λ_i is an eigenvalue of g. Since the field is of characteristic 0, if some J_i is a $p \times p$ matrix with $p > 1$, then $J_i^m \neq 1$ for any $m > 0$. Hence $g^m \neq 1$ which is a contradiction. In this way, all blocks J_i are 1×1 matrices, i.e. the normal Jordan form of g is diagonal.

In the exercises we shall give a direct proof of the lemma, without using the Jordan normal form.

Lemma 2.13. *If ϕ is a linear operator acting on a finite dimensional vector space W and $\phi^2 = \phi$, then $\dim(\mathrm{Im}(\phi)) = \mathrm{tr}(\phi)$, where $\mathrm{tr}(\phi)$ is the trace of ϕ.*

Proof. By Lemma 2.4, the vector space W is a direct sum of the image and the kernel of ϕ and ϕ acts on the image as the identity map. We choose a basis of W which is a union of bases of the image and the kernel of ϕ. Hence the dimension of the image of ϕ is equal to the number of 1's on the diagonal of ϕ with respect to the chosen basis, i.e. to the trace of ϕ.

Molien Formula 2.14. *If G is a finite subgroup of $GL_n(K)$, then the Hilbert series of the algebra of invariants $S = R^G = K[x_1, \ldots, x_n]^G$ has the form*

$$H(R^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - gt)},$$

where $\det(1 - gt)$ is the determinant of the matrix $1 - gt$.

Proof. Let R_d be the vector space of the homogeneous polynomials of degree d. Then R^G is a direct sum of the homogeneous components $S_d = (R_d)^G$ and the Hilbert series of S is equal to $\sum_{d \geq 0} (\dim S_d) t^d$. Let ρ_d be the restriction of the Reynolds operator on R_d. By Proposition 2.5, $\rho_d^2 = \rho_d$ and $S_d = \rho(R_d)$. By Lemma 2.13 we obtain that $\dim S = \mathrm{tr}(\rho_d)$. Clearly,

$$\mathrm{tr}(\rho_d) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}(g_d),$$

where g_d is the restriction of $g \in G$ on R_d. Since the group G is finite, its elements are of finite order. Let g be an element of G. The change of the basis of the vector space V with basis $\{x_1, \ldots, x_n\}$ corresponds to a linear change of the variables. It does not change the algebra of invariants and the trace of the matrix g_d acting on R_d. By Lemma 2.12 we may choose new variables $\{y_1, \ldots, y_n\}$ such that $g(y_i) = \lambda_i y_i$ for some roots of unity $\lambda_i = \lambda_i(g)$, $i = 1, \ldots, n$. Hence g_d acts on the basis elements $y_1^{d_1} \ldots y_n^{d_n}$ of R_d, $d_1 + \ldots + d_n = d$, by

$$g_d(y_1^{d_1} \ldots y_n^{d_n}) = \lambda_1^{d_1} \ldots \lambda_n^{d_n} y_1^{d_1} \ldots y_n^{d_n}$$

and the trace of g_d is equal to the sum of all $\lambda_1^{d_1} \dots \lambda_n^{d_n}$ with $d_1 + \dots + d_n = d$. In this way,

$$H(R^d, t) = \sum_{d \geq 0} (\dim S_d) t^d = \sum_{d \geq 0} \operatorname{tr}(\rho_d) t^d$$

$$= \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}(g_d) t^d = \frac{1}{|G|} \sum_{g \in G} \sum_{d_i \geq 0} \lambda_1^{d_1} \dots \lambda_n^{d_n} t^{d_1 + \dots + d_n} =$$

$$= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{d_1 \geq 0} (\lambda_1 t)^{d_1} \right) \dots \left(\sum_{d_n \geq 0} (\lambda_n t)^{d_n} \right) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{(1 - \lambda_1 t) \dots (1 - \lambda_n t)}$$

and in order to complete the proof it is sufficient to observe that

$$(1 - \lambda_1 t) \dots (1 - \lambda_n t) = \det(1 - tg).$$

Remark 2.15. Since the algebra of invariants $S = R^G$ of a finite group G has the same transcendence degree as $R = K[x_1, \dots, x_n]$, the Noether Normalization Theorem in Commutative Algebra gives that *there exist homogeneous invariants $f_1, \dots, f_n$ which are algebraically independent and a finite number of homogeneous invariants $h_1, \dots, h_m$ such that every invariant f has the form $f = p_1 h_1 + \dots + p_m h_m$, where each coefficient $p_1, \dots, p_n$ is a polynomial of $f_1, \dots, f_n$.* Then the Hilbert-Serre theorem has a more precise form which gives that the Hilbert series of S is

$$H(S, t) = \frac{q(t)}{(1 - t^{d_1}) \dots (1 - t^{d_n})},$$

where $q(t) \in \mathbf{Q}[t]$ and d_i is the degree of f_i. In the special case, when

$$H(S, t) = \frac{1}{(1 - t^{d_1}) \dots (1 - t^{d_n})}$$

this means that $S = R^G$ is generated by the algebraically independent invariants $f_1, \dots, f_n$ and S is isomorphic to a polynomial algebra. The theorem of Chevalley-Shephard-Todd gives that *the algebra of invariants is isomorphic to a polynomial algebra if and only if the finite group G is generated by pseudo-reflections.* Recall that a *pseudo-reflection* is a matrix of finite order which has only one eigenvalue (counting the multiplicity) different from 1. In other words, the pseudo-reflections are similar to matrices in the form

$$g = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Exercises

1. Show directly, without using the Jordan normal form: If ϕ is a linear operator acting on a finite dimensional vector space W and such that the minimal polynomial of ϕ has no multiple zeros, then the matrix of ϕ is diagonalizable.

Solution. Let the minimal polynomial of ϕ be $f(z) = (z-\lambda_1)\dots(z-\lambda_k)$, where all λ_i are pairwise different. Consider the operator $\psi = \phi - \lambda_1$. Clearly, the kernel of ψ consists of all eigenvectors of ϕ corresponding to the eigenvalue λ_1, i.e.

$$\mathrm{Ker}(\psi) = \{w \in W \mid \phi(w) = \lambda_1 w\}.$$

On the other hand, if $0 \neq w \in \mathrm{Im}(\psi) \cap \mathrm{Ker}(\psi)$, then there exists some $v \in W$ such that $w = \psi(v)$ and $\phi^2(v) = \psi(w) = 0$. Hence $(\phi-\lambda_1)^2(v) = 0$ and $(\phi-\lambda_1)(v) \neq 0$. Since $(z-\lambda_1)^2$ is relatively prime with $(z-\lambda_2)\dots(z-\lambda_k)$, there exist polynomials $u_1(z), u_2(z) \in K[z]$ such that

$$u_1(z)(z-\lambda_1)^2 + u_2(z)(z-\lambda_2)\dots(z-\lambda_k) = 1.$$

Applying this to v we obtain that

$$u_1(\phi)(\phi-\lambda_1)^2(v) + u_2(\phi)(\phi-\lambda_2)\dots(\phi-\lambda_k)(v) = v,$$

$$u_2(\phi)(\phi-\lambda_2)\dots(\phi-\lambda_k)(v) = v,$$

$$(\phi-\lambda_1)(u_2(\phi)(\phi-\lambda_2)\dots(\phi-\lambda_k))(v) = \psi(v) = w \neq 0.$$

Hence $w = u_2(\phi)((\phi-\lambda_1)(\phi-\lambda_2)\dots(\phi-\lambda_k)(v) = u_2(\phi)f(\phi)(v)$ which is equal to 0, because $f(z)$ is the minimal polynomial of ϕ. This contradiction shows that $\mathrm{Im}(\psi) \cap \mathrm{Ker}(\psi) = 0$. Using the equality $\dim(\mathrm{Im}(\psi)) + \dim(\mathrm{Ker}(\psi)) = \dim(W)$ which holds for any linear operator, we obtain that W is a direct sum of $\mathrm{Im}(\psi)$ and $\mathrm{Ker}(\psi)$. Both subspaces $\mathrm{Im}(\psi)$ and $\mathrm{Ker}(\psi)$ are ϕ-invariant, $\dim \mathrm{Im}(\psi) > 0$ (there is a nonzero eigenvector of ϕ corresponding to λ_1) and the matrix of ϕ considered as an operator on $\mathrm{Im}(\psi)$ is diagonal. We may apply inductive arguments and conclude: $\mathrm{Ker}(\psi)$ has a basis such that the restriction of ϕ on $\mathrm{Ker}(\psi)$ has a diagonal matrix.

2. Show directly, without using the Jordan normal form and Execise 1: If ϕ is a linear operator acting on any vector space W and such that $\phi^k = 1$ for some $k > 0$, then W is a direct sum of subspaces each consisting of eigenvectors of ϕ. In particular, if $\dim(W) < \infty$, then the matrix of ϕ is diagonalizable.

Solution. (Proposed to the lecturer by M.-K. Siu.) Let ω be a fixed primitive root of 1. For any $p = 0, 1, \dots, k-1$, we define a linear operator ψ_p by

$$\psi_p(x) = x + \frac{\phi(x)}{\omega^p} + \frac{\phi^2(x)}{\omega^{2p}} + \dots + \frac{\phi^{k-1}(x)}{\omega^{(k-1)p}},\ x \in W.$$

Using that $\omega^k = 1$ and $\phi^k = 1$, direct verification shows that $\phi(\psi_p(x)) = \omega^p \psi_p(x)$, i.e. $\psi_p(x)$ is an eigenvector of ϕ corresponding to ω^p. Note that $x = \frac{1}{k}(\psi_0(x) + \psi_1(x) + \dots + \psi_{k-1}(x))$. Let $W_p = \{\psi_p(x) \mid x \in W\}$. Then $W = W_0 + W_1 + \dots + W_{k-1}$. On the other

hand, let $u_0, u_1, \ldots, u_{p-1}$ be some elements such that $u_p \in W_p$ and $u_0+u_1+\ldots+u_{k-1} = 0$. Applying ϕ^s, $s = 0, 1, \ldots, k-1$, to this sum, we obtain that

$$\phi^s(u_0 + u_1 + \ldots + u_{k-1}) = (\omega^0)^s u_0 + (\omega^1)^s u_1 + \ldots + (\omega^{k-1})^s u_{k-1} = 0.$$

Considering these equations as a homogeneous linear system with unknowns u_p and determinant equal to the Vandermonde determinant (which is nonzero), we conclude that the only solution of the system is $u_p = 0$, $p = 0, 1, \ldots, k-1$. This means that W is a direct sum of the subspaces $W_0, W_1, \ldots, W_{k-1}$. Since all elements of W_p are eigenvectors of ϕ, we complete the solution.

3. Find the image of $f(x_1, \ldots, x_n)$ under the action of $g \in GL_n(K)$ where:

(i) $n = 2$, $f(x, y) = 2x + 5y + 3x^2 + 5xy^2 + y^3$ and $g(x) = x + 2y$, $g(y) = -2x + 3y$ or in matrix form,

$$g = \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix};$$

(ii) $n = 3$, $f(x, y, z) = xz - y^2$,

$$g = 1 + \frac{\Delta}{1!} + \frac{\Delta}{2!} + \ldots,$$

where the linear operator Δ is defined by $\Delta(x) = -2y$, $\Delta(y) = z$, $\Delta(z) = 0$.

4. Find the generators of the algebra of invariants $K[x, y]^G$ of the group G generated by g and h, where

$$g(x) = -x,\ g(y) = y,\ h(x) = x,\ h(y) = -y.$$

Answer. $K[x, y]^G = K[x^2, y^2]$.

5. Find the invariants of degree ≤ 3 of the cyclic group G of order 3 acting on $K[x, y, z]$ and generated by

$$g = \begin{pmatrix} x & y & z \\ y & z & x \end{pmatrix}.$$

Find the generators of $K[x, y, z]^G$.

Hint. First method: Apply the Reynolds operator to the monomials of degree ≤ 3. Second method: Change the variables in such a way that with respect to the new variables x_1, y_1, z_1 the operator g acts by

$$g(x_1) = x_1,\ g(y_1) = \omega y_1,\ g(z_1) = \omega^2 z_1,$$

where $\omega^3 = 1$, $\omega \neq 1$. Then the invariants are linear combinations of x_1, $y_1 z_1$ and y_1^3, z_1^3. Derive from here (with or without using the bound of Emmy Noether) that the algebra of invariants is generated by homogeneous polynomials of degree $\leq |G| = 3$. *Answer.* $K[x, y, z]^G$ is generated by $x + y + z$, $xy + yz + zx$, xyz and $x^2y + y^2z + z^2x$. (Compare with Exercise 8 from Section 1.)

6. Find generators of the algebra of invariants $K[x, y]^G$, where G is the cyclic group generated by g defined by $g(x) = y$, $g(y) = -x$.

Hint. Use the Reynolds operator or change the basis in such a way that $g(x_1) = ix_1$, $g(y_1) = -iy_1$. The invariants are generated by $x_1^a y_1^b$, $a-b \equiv 0 \pmod 4$. Then the generators of the algebra of invariants with respect to the new basis are x_1y_1, x_1^4, y_1^4. *Answer.* $K[x,y]^G$ is generated by $f_1 = x^2 + y^2$, $f_2 = x^2y^2$ and $f_3 = xy(x^2 - y^2)$.

7. Calculate the Hilbert series of the algebra of invariants in Exercises 4, 5 and 6 and find defining relations between the generators.

Hint. For Exercise 4 use that $K[x,y]^G = K[x^2, y^2]$ is the polynomial algebra in two variables of degree 2. Hence

$$H(K[x,y]^G, t) = \frac{1}{(1-t^2)^2}.$$

For the other exercisess apply the Molien formula. For Example 5 use that with respect to a specially chosen basis g and g^2 are diagonal matrices with entries $1, \omega, \omega^2$ and

$$\det(1 - tg) = \det(1 - tg^2) = (1-t)(1-\omega t)(1-\omega^2 t) = 1 - t^3.$$

Together with $\det(1-t) = (1-t)^3$ we obtain

$$H(K[x,y,z]^G, t) = \frac{1}{3}\left(\frac{1}{(1-t)^3} + \frac{2}{1-t^3}\right) = \frac{1-t+t^2}{(1-t)^2(1-t^3)} = \frac{1+t^3}{(1-t)(1-t^2)(1-t^3)}.$$

Hence $K[x,y,z]^G$ has the form $(K + K(x^2y + y^2z + z^2x))K[e_1, e_2, e_3]$, where e_j are the elementary symmetric polynomials. Compare with Exercise 8 of Section 1. The considerations for Exercise 6 are similar.

8. Calculate the Hilbert series and find generating sets and defining relations of the algebra of invariants of the following groups:

(i) The dihedral group D_8 of order 8 generated by

$$g = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \; h = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

(ii) The quaternion group $\mathbf{Q}_8$ of order 8 generated by

$$g = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \; h = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

Hint. Calculate the determinants of $1 - bt$, $b \in G$. The answer is

$$H(K[x,y]^{D_8}, t) = \frac{1}{(1-t^2)(1-t^4)}$$

which confirms the fact that D_8 is generated by pseudo-reflections and its algebra of invariants has algebraically independent generators. The generators are $x^2 + y^2$ and x^2y^2. For the quaternion group

$$H(K[x,y]^{\mathbf{Q}_8}, t) = \frac{1-t^2+t^4}{(1-t^2)(1-t^4)} = \frac{1+t^6}{(1-t^4)^2}.$$

Derive from here that the algebra of invariants has two generators of degree 4 and one of degree 6. The generators are $x^2y^2, x^4+y^4, xy(x^4-y^4)$. The defining relation between them is $(xy(x^4-y^4))^2 = (x^2y^2)((x^4+y^4)^2 - 4(x^2y^2)$.

9. Let the symmetric group act on the vector subspace W of $V = \mathrm{span}\{x_1, \ldots, x_n\}$ with basis $\{y_i = x_i - x_{i+1} \mid i = 1, \ldots, n-1\}$. Calculate the Hilbert series of the algebra of invariants $K[y_1, \ldots, y_{n-1}]^{S_n}$.

Hint. Use that V is a direct sum of W and the one-dimensional vector space spanned by $x_1 + x_2 + \ldots + x_n$, where S_n acts identically. For every $\sigma \in S_n$, the determinant of $1 - \sigma t$ on V is a product of $1 - t$ and the determinant of $1 - \sigma t$ on W. Hence in the Molien formula

$$H(K[x_1, \ldots, x_n]^{S_n}, t) = \frac{1}{1-t} H(K[y_1, \ldots, y_{n-1}]^{S_n}, t) = \prod_{k=1}^{n} \frac{1}{1-t^k}.$$

3. AUTOMORPHISMS AND DERIVATIONS OF POLYNOMIAL ALGEBRAS

In this section we assume that K is a fixed algebraically closed field of characterisric 0, e.g. $K = \mathbf{C}$. The assumption that K is algebraically closed is not essential for the results (but simplifies the proofs). The requirement for the characteristic sometimes is essential. We fix a finite set of variables $X = \{x_1, \dots, x_n\}$ and consider the polynomial algebra $K[X] = K[x_1, \dots, x_n]$.

Definition 3.1. The isomorphisms $K[X] \to K[X]$ are called *automorphisms* of $K[X]$. All automorphisms ϕ of $K[X]$ form a group which we denote by $\mathrm{Aut}K[X]$. Since every mapping $X \to K[X]$ can be extended to an endomorphism of $K[X]$, it is sufficient to define the automorphisms of $K[X]$ only on X. In commutative algebra and algebraic geometry one often denotes the automorphisms as $F = (f_1, \dots, f_n)$, where $f_j = \phi(x_j)$. Then, if $G = (g_1, \dots, g_n)$ is another automorphism, where $g_j = \psi(x_j)$, one has $F \circ G = F(G) = (f_1(G), \dots, f_n(G))$, $f_j(G) = f_j(g_1, \dots, g_n)$ which corresponds to the composition $\psi \circ \phi$ (first applying ϕ and then ψ). We shall use the notation $\psi\phi = \psi \circ \phi$ instead of $F(G)$.

Definition 3.2. The automorphisms of the form

$$\phi(x_j) = \sum_{i=1}^{n} \alpha_{ij} x_i + \beta_j,\ \alpha_{ij}, \beta_j \in K,\ i, j = 1, \dots, n,$$

(where the $n \times n$ matrix (α_{ij}) is invertible) are called *affine*. The automorphisms of the form

$$\phi(x_j) = \alpha_j x_j + f_j(x_{j+1}, \dots, x_n),\ \alpha_j \in K^*,\ j = 1, \dots, n,$$

where the polynomials $f_j(x_{j+1}, \dots, x_n)$ do not depend on $x_1, \dots, x_j$, are called *triangular*. The automorphisms which belong to the group generated by the affine and the triangular automorphisms are called *tame automorphisms*. The automorphisms which are not tame are called *wild*.

Example 3.3. (i) Let $\phi, \psi \in \mathrm{End}K[x, y]$ be defined by

$$\phi(x) = x + y^2, \phi(y) = y,$$

$$\psi(x) = x - y^2, \psi(y) = y.$$

Then $\phi \circ \psi(y) = \phi(\psi(y)) = \phi(y) = y$,

$$\phi \circ \psi(x) = \phi(\psi(x)) = \phi(x - y^2) = \phi(x) - \phi(y)^2 = (x + y^2) - y^2 = x.$$

Hence $\phi \circ \psi$ is the identity automorphism. Similarly $\psi \circ \phi$ is the identity. Hence ϕ, ψ are automorphisms and $\psi = \phi^{-1}$. Clearly, ϕ, ψ are triangular automorphisms.

(ii) Let $\phi, \psi \in \mathrm{Aut}K[x, y]$ be defined by

$$\phi(x) = x + y^2, \phi(y) = y,$$

$$\psi(x) = x, \psi(y) = y + x^3,$$

(ψ may be considered as a triangular automorphism with respect to the ordering of the variables $x_1 = y, x_2 = x$). Then

$$\phi^{-1}(x) = x - y^2,\ \phi^{-1}(y) = y,$$

$$\psi^{-1}(x) = x,\ \psi^{-1}(y) = y - x^3,$$

$$\phi \circ \psi(x) = \phi(\psi(x)) = \phi(x) = x + y^2,\ \phi \circ \psi(y) = \phi(\psi(y)) = \phi(y + x^3) = y + (x + y^2)^3,$$

$$\psi \circ \phi(x) = \psi(x + y^2) = x + (y + x^3)^2,\ \psi \circ \phi(y) = \psi(y) = y + x^3,$$

$$(\phi \circ \psi)^{-1}(x) = \psi^{-1}(\phi^{-1}(x)) = \psi^{-1}(x - y^2) = x - (y - x^3)^2,$$

$$(\phi \circ \psi)^{-1}(y) = \psi^{-1}(\phi^{-1}(y)) = \psi^{-1}(y) = y - x^3.$$

One of the main open problems in the theory of automorphisms of the polynomial algebras, which will be also in the centre of our course, is the following:

Problem 3.4. *Is every automorphism of $K[X]$ tame?*

Lemma 3.5. *For any commutative domain R let $\mathrm{Aut}R[x, y]$ be the group of R-automorphisms of $R[x, y]$ (i.e. automorphisms fixing the elements of R) and let*

$$A = \{\sigma \in \mathrm{Aut}R[x, y] \mid \sigma(x) = \alpha x + \beta y + \gamma,\ \sigma(y) = \xi x + \eta y + \zeta,\ \alpha, \beta, \gamma, \xi, \eta, \zeta \in R\}$$

be the affine group of automorphisms, let

$$B = \{\tau \in \mathrm{Aut}R[x, y] \mid \tau(x) = \pi x + f(y),\ \tau(y) = \rho y + \omega,\ \pi, \rho \in R^*, \omega \in R, f(y) \in R[y]\}$$

be the triangular group and let $C = A \cap B$. Then every tame automorphism ϕ of $R[x, y]$ can be presented in the form

$$\phi = \sigma_1^{\delta} \circ \tau_1 \circ \sigma_2 \circ \ldots \circ \sigma_k \circ \tau_k \circ \sigma_{k+1}^{\varepsilon},$$

where $\delta, \varepsilon = 0, 1$ (i.e. the expression of ϕ may start with τ_1 or finish with τ_k), $\sigma_i \in A$, $\tau_i \in B$, $\sigma_2, \ldots, \sigma_k$ (and σ_1 and σ_{k+1} if they participate in the expression) do not belong to B, $\tau_1, \ldots, \tau_k$ do not belong to A.

Proof. Clearly, every tame automorphism is a product of affine and triangular automorphisms, $\phi = \rho_1 \circ \ldots \circ \rho_n$, where $\rho_i \in A \cup B$, $i = 1, \ldots, n$. If two consecutive ρ_i, ρ_{i+1} belong to the same group A or B, then we may replace them with their product. Hence, we may assume that if $\rho_i \in A$, then $\rho_{i+1} \in B$ and ρ_{i+1} does not belong to A; similarly if $\rho_i \in B$. So, ϕ has the presentation $\phi = \sigma_1^{\delta} \circ \tau_1 \circ \sigma_2 \circ \ldots \circ \sigma_k \circ \tau_k \circ \sigma_{k+1}^{\varepsilon}$.

For a nonzero polynomial $g(x, y)$ we denote by $\overline{g(x, y)}$ the homogeneous component of maximal degree of $g(x, y)$.

Proposition 3.6. *In the notation of the previous lemma, if $\phi = \sigma_1^{\delta} \circ \tau_1 \circ \sigma_2 \circ \ldots \circ \sigma_k \circ \tau_k$, where $\varepsilon = 0, 1$, $\sigma_i \in A$, (and σ_i does not belong to B for $i = 2, \ldots, k$), $\tau_i \in B$, $\tau_i(x) = \pi_i x + f_i(y)$, $\tau_i(y) = \rho_i y + \omega_i$, and the degree $\deg f(y)$ of $f_i(y)$ is equal to $d_i > 1$, then*

$$\deg(\phi(x)) = d_1 d_2 \ldots d_k,\ \deg(\phi(y)) = d_1 \ldots d_{k-1},$$

and the homogeneous components $\overline{\phi(x)}$ *and* $\overline{\phi(y)}$ *of maximal degree respectively of* $\phi(x)$ *and* $\phi(y)$ *are of the form*

$$\overline{\phi(x)} = \lambda(\kappa(\mu x + \nu y)^m)^{d_k},\ \overline{\phi(y)} = \kappa(\mu x + \nu y)^m,$$

for some $\kappa, \lambda, \mu, \nu \in R$ *and for* $m = d_1 \dots d_{k-1}$.

Proof. Let $\sigma_i(x) = \alpha_i x + \beta_i y + \gamma_i$, $\sigma_i(y) = \xi_i x + \eta_i y + \zeta_i$. Since $\sigma_i \notin B$, we obtain that $\xi_i \neq 0$ for $i = 2, \dots, k$. Let $\overline{f_i(y)} = \theta_i y^{d_i}$, $0 \neq \theta_i \in R$. Direct calculations give that

$$\sigma_k \circ \tau_k(y) = \sigma_k(\rho_k y + \omega_k) = \rho_k(\xi_k x + \eta_k y + \zeta_k) + \omega_k,$$

$$\overline{\sigma_k \circ \tau_k(y)} = \rho_k(\xi_k x + \eta_k y),\ \rho_k \in R^*, \rho_k \xi_k \neq 0,$$

$$\sigma_k \circ \tau_k(x) = \pi_k(\alpha_k x + \beta_k y + \gamma_k) + f_k(\xi_k x + \eta_k y + \zeta_k),$$

$$\overline{\sigma_k \circ \tau_k(x)} = \theta_k(\xi_k x + \eta_k y)^{d_k} = \left(\theta_k \rho_k^{-d_k}\right)(\rho_k(\xi_k x + \eta_k y))^{d_k}.$$

By induction, we assume that

$$\overline{\sigma_2 \tau_2 \dots \sigma_k \tau_k(x)} = \lambda_2(\kappa_2(\mu_2 x + \nu_2 y)^n)^{d_k},\ \overline{\sigma_2 \tau_2 \dots \sigma_k \tau_k(y)} = \kappa_2(\mu_2 x + \nu_2 y)^n,$$

$$n = d_2 \dots d_{k-1}, \mu_2 \neq 0,\ \kappa_2 \in R,$$

and obtain

$$\sigma_1\tau_1(x) = \pi_1(\alpha_1 x + \beta_1 y + \gamma_1) + f_1(\xi_1 x + \eta_1 y + \zeta_1),\ \sigma_1\tau_1(y) = \rho_1(\xi_1 x + \eta_1 y + \zeta_1) + \omega_1,$$

$$\overline{\sigma_1\tau_1(x)} = \overline{f_1(\xi_1 x + \eta_1 y)} = \theta_1(\xi_1 x + \eta_1 y)^{d_1},\ \overline{\sigma_1\tau_1(y)} = \rho_1(\xi_1 x + \eta_1 y),\ \rho_1 \in R^*,$$

$$\sigma_1\tau_1(\sigma_2 \dots \tau_k(x)) = \lambda_2(\kappa_2(\mu_2\sigma_1\tau_1(x) + \nu_2\mu_2\sigma_1\tau_1(y))^n)^{d_k} + \dots$$

$$= \lambda_2(\kappa_2(\mu_2\theta_1)^n(\xi_1 x + \eta_1 y)^{d_1} + \dots)^n)^{d_k} + \dots$$

where we have denoted with $\dots$ summands of lower degree. Hence

$$\overline{\sigma_1 \dots \tau_k(x)} = \lambda_2\left(\kappa_2\mu_2^n\theta_1^n(\xi_1 x + \eta_1 y)^{d_1 n}\right)^{d_k},$$

$$\sigma_1\tau_1(\sigma_2 \dots \tau_k(y)) = \kappa_2(\mu_2\sigma_1\tau_1(x) + \nu_2\sigma_1\tau_1(y))^n + \dots,$$

$$\overline{\sigma_1 \dots \tau_k(y)} = \kappa_2(\mu_2\theta_1)^n(\xi_1 x + \eta_1 y)^{d_1 n}.$$

Denoting $\kappa_1 = \kappa_2(\mu_2\theta_1)^n$, $m = d_1 n$, we obtain that

$$\overline{\sigma_1 \dots \tau_k(x)} = \lambda_2(\kappa_1(\xi_1 x + \eta_1 y)^m)^{d_k},\ \overline{\sigma_1 \dots \tau_k(y)} = \kappa_1(\xi_1 x + \eta_1 y)^m.$$

If $\sigma_1 \notin B$, then $\xi_1 \neq 0$ and we may continue the inductive steps and prove the statement for larger k.

Theorem 3.7. *Let R be a commutative domain and let $\phi \in \mathrm{Aut}R[x,y]$ be a tame automorphism. Let the homogeneous components of maximal degree of $\phi(x)$ and $\phi(y)$ be, respectively $f(x,y)$ and $g(x,y)$, $\deg(f) = m$, $\deg(g) = n$. Then either n divides m and*

$$f(x,y) = \lambda(\kappa(\mu x + \nu y)^n)^d,\ g(x,y) = \kappa(\mu x + \nu y)^n,\ \lambda, \kappa, \mu, \nu \in R,\ m = dn,$$

or m divides n and

$$f(x,y) = \kappa(\mu x + \nu y)^m,\ g(x,y) = \lambda(\kappa(\mu x + \nu y)^m)^d,\ \lambda, \kappa, \mu, \nu \in R,\ n = dm,$$

or $m = n$ and there exists an affine automorphism σ of $R[x,y]$ such that

$$\deg(\phi \circ \sigma^{-1}(x)) = m > \deg(\phi \circ \sigma^{-1}(y)).$$

Proof. Let $\phi = \sigma_1^{\delta} \circ \tau_1 \circ \sigma_2 \circ \ldots \circ \sigma_k \circ \tau_k \circ \sigma_{k+1}^{\varepsilon}$, where $\sigma_i \in A$, $\tau_i \in B$, as in Lemma 3.5. If $\varepsilon = 0$, then ϕ is in the form of Proposition 3.6 and we obtain that $\overline{\phi(x)} = \kappa(\overline{\phi(y)})^d$, where d is the degree of $f_k(y)$ in the definition of τ_k. Now, let $\varepsilon = 1$ and let

$$\sigma_{k+1} = \alpha x + \beta y + \gamma,\ \sigma(y) = \xi x + \eta y + \zeta,\ \alpha, \beta, \gamma, \xi, \eta, \zeta \in R,$$

and, by Proposition 3.6, for $\psi = \sigma_1^{\delta}\tau_1\sigma_2 \ldots \sigma_k\tau_k$

$$\overline{\psi(x)} = \lambda_1(\kappa_1(\mu_1 x + \nu_1 y)^n)^d,\ \overline{\psi(y)} = \kappa_1(\mu_1 x + \nu_1 y)^n.$$

Direct calculations give that

$$\overline{\phi(x)} = \overline{\psi \circ \sigma_{k+1}(x)} = \overline{\alpha\overline{\psi(x)} + \beta\overline{\psi(y)}},$$

$$\overline{\phi(y)} = \overline{\psi \circ \sigma_{k+1}(y)} = \overline{\xi\overline{\psi(x)} + \eta\overline{\psi(y)}}.$$

(i) If $\alpha \neq 0$, $\xi = 0$, then $\eta \in R^*$ and

$$\overline{\phi(x)} = \alpha\overline{\psi(x)} = \alpha\lambda_1(\kappa_1(\mu_1 x + \nu_1 y)^n)^d = (\alpha\lambda_1\eta^{-d})(\eta\kappa_1(\mu_1 x + \nu_1 y)^n)^d,$$

$$\overline{\phi(y)} = \eta\overline{\psi(y)} = \eta\kappa_1(\mu_1 x + \nu_1 y)^n.$$

(ii) If $\alpha = 0$, then $\xi \neq 0$, $\beta \in R^*$ and

$$\overline{\phi(x)} = \beta\overline{\psi(y)} = \beta\kappa_1(\mu_1 x + \nu_1 y)^n$$

$$\overline{\phi(y)} = \xi\overline{\psi(x)} = \xi\lambda_1(\kappa_1(\mu_1 x + \nu_1 y)^n)^d = (\alpha\lambda_1\eta^{-d})(\eta\kappa_1(\mu_1 x + \nu_1 y)^n)^d.$$

(iii) If $\alpha \neq 0$, $\xi \neq 0$, then

$$\overline{\phi(x)} = \alpha\overline{\psi(x)},\ \overline{\phi(y)} = \xi\overline{\psi(x)},$$

$\deg\phi(x) = \deg\phi(y) = nd$ and for $\sigma = \sigma_{k+1}$ we obtain

$$\phi \circ \sigma^{-1}(x) = \psi(x),\ \phi \circ \sigma^{-1}(y) = \psi(y)$$

with $\deg\psi(x) = \deg\phi(x) = nd$, $\deg\psi(y) = n < \deg\phi(y)$.

Definition 3.8. The endomorphism ν of $K[x, y, z]$ defined by

$$\nu(x) = x - 2(y^2 + zx)y - (y^2 + zx)^2 z,\ \nu(y) = y + (y^2 + zx)z,\ \nu(z) = z$$

is called the *Nagata automorphism* (and its properties are described in [N]).

Exercise 3.9. Show that the Nagata automorphism is an automorphism.

Hint. Show that $\nu(y^2 + zx) = y^2 + zx$ which would help in the verification that the endomorphism ρ defined by

$$\rho(x) = x + 2(y^2 + zx)y - (y^2 + zx)^2 z,\ \rho(y) = y - (y^2 + zx)z,\ \rho(z) = z$$

is the inverse of ν. Later we shall see that the Nagata automorphism is an example of a general class of naturally arising automorphisms.

Theorem 3.10. (Nagata [N]) *The Nagata automorphism ν is wild considered as an automorphism of the $K[z]$-algebra $(K[z])[x, y]$.*

Proof. Since ν fixes z, we may consider it as a $K[z]$-automorphism of $(K[z])[x, y]$. Let ν be tame. Clearly, the homogeneous components of maximal degree of $\nu(x)$ and $\nu(y)$ are (remember that z is considered to be a "constant")

$$\overline{\nu(x)} = -zy^4,\ \overline{\nu(y)} = zy^2.$$

By Theorem 3.7, there exists a "constant" λ in $R = K[z]$ (i.e. $\lambda = \lambda(z)$ is a polynomial of z) and d such that

$$\overline{\nu(x)} = \lambda(z)(\overline{\nu(y)})^d.$$

Hence $-zy^4 = \lambda(z)(zy^2)^d$, i.e. $d = 2$ and $\lambda(z) = -1/z$ which is not a polynomial. Therefore, ν is not a tame automorphism.

Remark 3.11. The Nagata automorphism is tame considered as an automorphism of $(K(z))[x, y]$, the algebra of polynomials in two variables x, y over the field of rational functions $K(z)$. One can decompose it as $\nu = \tau \circ \sigma \circ \tau^{-1}$, where $\sigma, \tau \in \mathrm{Aut}(K(z))[x, y]$ are defined by

$$\sigma(x) = x,\ \sigma(y) = y + z^2 x,\ \tau(x) = x + \frac{y^2}{z},\ \tau(y) = y.$$

The following conjecture is one of the most famous conjectures on automorphisms of polynomial algebras. For further discussions see e.g. the survey article [DY1].

Conjecture 3.12. (The Nagata Conjecture, [N]) *The Nagata automorphism is wild considered as an automorphism of the polynomial algebra $K[x, y, z]$.*

Definition 3.13. Let ϕ be any endomorphism of $K[x_1, \ldots, x_n]$. The $n \times n$ matrix

$$J(\phi) = \begin{pmatrix} \frac{\partial \phi(x_1)}{\partial x_1} & \frac{\partial \phi(x_2)}{\partial x_1} & \cdots & \frac{\partial \phi(x_n)}{\partial x_1} \\ \frac{\partial \phi(x_1)}{\partial x_2} & \frac{\partial \phi(x_2)}{\partial x_2} & \cdots & \frac{\partial \phi(x_n)}{\partial x_2} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{\partial \phi(x_1)}{\partial x_n} & \frac{\partial \phi(x_2)}{\partial x_n} & \cdots & \frac{\partial \phi(x_n)}{\partial x_n} \end{pmatrix}$$

is called the *Jacobian matrix* of ϕ. (Very often in commutative algebra and algebraic geometry one defines the Jacobian matrix as the transpose of the matrix in our definition.)

Proposition 3.14. (The Chain Rule) *If ϕ and ψ are endomorphisms of $K[x_1, \ldots, x_n]$, then*

$$J(\phi \circ \psi) = J(\phi)\phi(J(\psi)),$$

where $\phi(J(\psi))$ means that we apply ϕ to the entries of the matrix $J(\psi)$.

Proof. We shall prove the chain rule for the case of two variables only. The proof in the general case is similar. Let h_x and h_y denote the partial derivatives of $h = h(x, y)$ with respect to x and y. If

$$\phi(x) = f(x, y),\ \phi(y) = g(x, y),\ \psi(x) = u(x, y),\ \psi(y) = v(x, y),$$

then $\phi \circ \psi(x) = \phi(u(x, y)) = u(\phi(x), \phi(y)) = u(f, g)$, similarly $\phi \circ \psi(y) = v(f, g)$ and

$$(\phi \circ \psi(x))_x = (u(f, g))_x = u_x(f, g)f_x + u_y(f, g)g_x,$$

$$(\phi \circ \psi(y))_x = (v(f, g))_x = v_x(f, g)f_x + v_y(f, g)g_x,$$

$$(\phi \circ \psi(x))_y = (u(f, g))_y = u_x(f, g)f_y + u_y(f, g)g_y,$$

$$(\phi \circ \psi(y))_y = (v(f, g))_y = v_x(f, g)f_y + v_y(f, g)g_y.$$

These equations can be rewritten in a matrix form as

$$\begin{pmatrix} f_x & g_x \\ f_y & g_y \end{pmatrix} \begin{pmatrix} u_x(f, g) & v_x(f, g) \\ u_y(f, g) & v_y(f, g) \end{pmatrix} = J(\phi)\phi(J(\psi)).$$

Corollary 3.15. *The Jacobian matrix of any automorphism of $K[X] = K[x_1, \ldots, x_n]$ is invertible over $K[X]$ (and the determinant of the Jacobian matrix is a nonzero constant).*

Proof. Of course, if ϕ is an automorphism, then the Jacobian matrix of $\phi \circ \phi^{-1}$ is equal to the Jacobian matrix of the identity automorphism which is the unit $n \times n$ matrix. By the chain rule $J(\phi)$ is invertible and its determinant is an invertible element in $(K[X])^*$, hence in K^*.

The inverse function theorem in calculus states that if the Jacobian matrix of a mapping $\mathbf{R}^n \to \mathbf{R}^n$ is invertible, then the mapping is *locally* invertible. The analogue for polynomial algebras is that *any endomorphism of $K[X]$ with an invertible Jacobian matrix and which preserves the augmentation ideal (i.e. sends the variables to polynomials without*

constant terms) induces an automorphism of the algebra $K[[X]]$ of formal power series. The famous Jacobian conjecture (Keller, 1939) is the following:

Jacobian Conjecture 3.16. *Every endomorphism of $K[X] = K[x_1, \ldots, x_n]$ with an invertible Jacobian matrix is an automorphism (of $K[X]$).*

Till the end of the section we shall show the importance of derivations in the study of automorphisms of polynomial algebras.

Definition 3.17. Let R be any (not necessarily commutative) algebra. The linear mapping $\delta : R \to R$ is called a *derivation* of R if

$$\delta(uv) = \delta(u)v + u\delta(v)$$

for all $u, v \in R$. We denote by $\mathrm{Ker}\delta = R^\delta$ the kernel of δ (considered as a linear operator of the vector space R), it is a subalgebra of R, see the exercises. The derivation δ of R is called *locally nilpotent*, if for every $u \in R$ there exists a d such that $\delta^d(u) = 0$.

The derivation δ of the polynomial algebra $K[x_1, \ldots, x_n]$ is called *triangular* if $\delta(x_j) \in K[x_{j+1}, \ldots, x_n]$, $j = 1, \ldots, n$.

Pay attention that for any derivation δ of the algebra R

$$\delta(1) = \delta(1^2) = \delta(1)1 + 1\delta(1) = 2\delta(1)$$

and hence $\delta(1) = 0$. By the linearity of δ we have that $\delta(\alpha) = \alpha\delta(1) = 0$ for any $\alpha \in K \subset R$.

Examples 3.18. (i) Let $R = K[X]$ and $\delta = \partial/\partial x_i$, the partial derivative with respect to x_i. Clearly, δ is a derivation. It is locally nilpotent because for a polynomial $u(X)$ of degree k with respect to x_i one has $\partial^{k+1}u/\partial x_i^{k+1} = 0$.

(ii) Let $f_i(X) \in K[X]$, $i = 1, \ldots, n$. Then the mapping δ defined by

$$\delta(u) = f_1\frac{\partial u}{\partial x_1} + f_2\frac{\partial u}{\partial x_2} + \ldots + f_n\frac{\partial u}{\partial x_n},\ u \in K[X],$$

is a derivation of $K[X]$. Indeed, δ is a linear operator and

$$\delta(uv) = \sum_{i=1}^n f_i\frac{\partial(uv)}{\partial x_i} = \sum_{i=1}^n f_i\left(\frac{\partial u}{\partial x_i}v + u\frac{\partial v}{\partial x_i}\right)$$

$$= \left(\sum_{i=1}^n f_i\frac{\partial u}{\partial x_i}\right)v + u\left(\sum_{i=1}^n f_i\frac{\partial v}{\partial x_i}\right) = \delta(u)v + u\delta(v).$$

(iii) The derivation $\delta = -2y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y}$ is a triangular derivation of $K[x, y, z]$ because sends x to $-2y$, y to z and z to 0.

Lemma 3.19. *Every mapping $X \to K[X]$ can be extended in a unique way to a derivation of $K[X]$. Every derivation of $K[X]$ is of the form $\delta = \sum_{i=1}^n f_i\frac{\partial}{\partial x_i}$ for suitable $f_i \in K[X]$, $i = 1, \ldots, n$.*

Proof. If δ is a derivation of some algebra R, and R is generated by the elements $r_1, r_2, \ldots$, then δ is completely defined by its values on $r_1, r_2, \ldots$ because the elements $r \in R$ have the form $r = \sum \alpha_p r_{p_1} \ldots r_{p_m}$, $\alpha_p \in K$ and

$$\delta(r) = \sum \alpha_p \left(\sum_{i=1}^{m} r_{p_1} \ldots \delta(r_{p_i}) \ldots r_{p_m} \right)$$

is expressed by $\delta(r_1), \delta(r_2), \ldots$ In the case of the polynomial algebra, let $f_1, \ldots, f_n$ be some polynomials in $K[X]$. Then it is direct to see that the derivation $\delta = \sum_{i=1}^{n} f_i \frac{\partial}{\partial x_i}$ from Example 3.18 (ii) satisfies $\delta(x_i) = f_i$, $i = 1, \ldots, n$. Since, if the derivation of $K[X]$ which extends the mapping $x_i \to f_i$ exists, then it is unique, we obtain the proof of the lemma.

The following equality for derivations of any algebra R is the *Leibniz formula*:

$$\delta^m(uv) = \sum_{k=0}^{m} \binom{m}{k} \delta^k(u) \delta^{m-k}(v),\ u, v \in R.$$

It has also the more general form:

$$\delta^m(u_1 \ldots u_p) = \sum_{k_1 + \ldots + k_p = m} \frac{m!}{k_1! \ldots k_p!} \delta^{k_1}(u_1) \ldots \delta^{k_p}(u_p),\ u_1, \ldots, u_p \in R.$$

Lemma 3.20. (i) *A derivation δ of the algebra R is locally nilpotent if and only if it acts nilpotently on the generators of R (i.e. if R is generated by $r_1, r_2, \ldots$, then $\delta^{m_i}(r_i) = 0$ for some m_i dependning on the generator r_i).*

(ii) *The triangular derivations of $K[X]$ are locally nilpotent.*

Proof. (i) It is sufficient to show that any given product of generators is annihilated by some high power of δ. This follows from the Leibniz formula. The proof of (ii) can be obtained by induction on the number of variables: If δ is a triangular derivation, then $\delta(x_n) \in K$ and $\delta^2(x_n) = 0$. If δ acts locally nilpotently on $K[x_{i+1}, \ldots, x_n]$, since $\delta(x_i) \in K[x_{i+1}, \ldots, x_n]$, we obtain that $\delta^m(\delta(x_i)) = 0$ for some m and $\delta^{m+1}(x_i) = 0$, continuing the inductive process.

Lemma 3.21. *If δ is a locally nilpotent derivation of the polynomial algebra $K[X]$ and $w \in \mathrm{Ker}(\delta)$, then $\Delta = w\delta$ is also a locally nilpotent derivation.*

Proof. By Lemma 3.19, $\Delta = w\delta$ is a derivation. If $u \in K[X]$, then $\delta(wu) = \delta(w)u + w\delta(u) = w\delta(u)$ (because $\delta(w) = 0$) and we obtain that $\Delta^m(u) = w^m \delta^m(u)$. Since δ is locally nilpotent and $\delta^m(u) = 0$ for some m, we obtain that Δ is also locally nilpotent.

Example 3.22. The derivation $\delta = -2y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y}$ is triangular, and hence a locally nilpotent derivation of $K[x, y, z]$. It sends x to $-2y$, y to z and z to 0. Hence $\delta^3(x) = 0$, $\delta^2(y) = 0$, $\delta(z) = 0$. The polynomials z and $w = y^2 + zx$ are in the kernel of δ (check it!). Hence $\Delta = h(z, y^2 + zx)\delta$ is a locally nilpotent derivation of $K[x, y, z]$ for any polynomial h in two variables.

Lemma 3.23. *Let $f_1, \ldots, f_{n-1} \in K[X]$ and let the linear operator δ acting on $K[X]$ be defined as the determinant*

$$\delta(u) = \begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \ldots & \frac{\partial f_{n-1}}{\partial x_1} & \frac{\partial u}{\partial x_1} \\ \vdots & \ldots & \vdots & \vdots \\ \frac{\partial f_1}{\partial x_n} & \ldots & \frac{\partial f_{n-1}}{\partial x_n} & \frac{\partial u}{\partial x_n} \end{vmatrix},\ u \in K[X].$$

Then δ is a derivation. If $f_i = \phi(x_i)$, $i = 1, \ldots, n-1$, for some automorphism ϕ of $K[X]$, then δ is locally nilpotent.

Proof. Since the first $n-1$ columns of the determinant are fixed, it is a linear function on its last column, i.e. δ is a linear operator on $K[X]$. The condition $\delta(uv) = \delta(u)v + u\delta(v)$, $u, v \in K[X]$, also follows from the properties of determinants and the fact that the entries of the last column of the determinant for $\delta(uv)$ are $\frac{\partial(uv)}{\partial x_i} = \frac{\partial u}{\partial x_i}v + u\frac{\partial v}{\partial x_i}$, $i = 1, \ldots, n$. If $\phi \in \mathrm{Aut}K[X]$ and $f_i = \phi(x_i)$, $i = 1, \ldots, n$, then $f_1, \ldots, f_n$ generate $K[X]$ and $\delta(f_i) = 0$ for $i = 1, \ldots, n-1$, because two columns of the determinant are equal. Finally, $\delta(f_n)$ is equal to the determinant of the Jacobian matrix of ϕ and is a constant because ϕ is an automorphism. Hence $\delta^2(f_n) = 0$. In this way δ acts nilpotently on a set of generators of $K[X]$ and is locally nilpotent.

Remark 3.24. By a theorem of Rentschler [R] every locally nilpotent derivation of the algebra of polynomials in two variables is of the above form: *If δ is a locally nilpotent derivation of $K[x, y]$, then there exists an automorphism ϕ of $K[x, y]$ and a polynomial w from the kerenl of δ such that*

$$\delta(u) = w(\phi(x)) \begin{vmatrix} \frac{\partial \phi(x)}{\partial x} & \frac{\partial u}{\partial x} \\ \frac{\partial \phi(x)}{\partial y} & \frac{\partial u}{\partial y} \end{vmatrix} = w(\phi(x)) \left(\frac{\partial \phi(x)}{\partial x}\frac{\partial u}{\partial y} - \frac{\partial \phi(x)}{\partial y}\frac{\partial u}{\partial x} \right).$$

If $\delta \neq 0$, then the kernel of δ consists of all polynomials $h(\phi(x))$.

For the algebra of polynomials in three variables a theorem of Miyanishi [M] states: *If Δ is a locally nilpotent derivation of $K[x, y, z]$, then there exist polynomials*

$$f(x, y, z), g(x, y, z), w(x, y, z)$$

such that $\Delta = w\delta$, where w belongs to the kernel of δ and δ is a locally nilpotent derivation defined by

$$\delta(u) = \begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial g}{\partial x} & \frac{\partial u}{\partial x} \\ \frac{\partial f}{\partial y} & \frac{\partial g}{\partial y} & \frac{\partial u}{\partial y} \\ \frac{\partial f}{\partial z} & \frac{\partial g}{\partial z} & \frac{\partial u}{\partial z} \end{vmatrix}.$$

The kernel of Δ consists of all elements of $K[f, g]$.

For polynomial algebras in more than three variables this is not more true. There are examples of locally nilpotent derivations of $K[x, y, z, t]$ with any number of generators of the kernel of the derivation. For polynomial algebras with more than four generators there are locally nilpotent derivations with kernels which are not finitely generated. The most recent example is given by Daigle and Freudenburg [DF] for the algebra with five variables. In this way they have given a counterexample in minimal known number of variables to the 14-th Hilbert Problem. (Originally the problem was solved by Nagata in terms of invariant theory, see Section 2. See also the book by Nowicki [No] amd the paper [DF] for more comments on the 14-th Hilbert Problem and the contributions of other mathematicians to the problem.)

On the other hand, a theorem of Weizenböck from 1932 (see [No]) gives that *if δ is a linear nilpotent operator acting on the vector space with basis X, and we denote by the*

same symbol δ the induced derivation of $K[X]$, then the kernel of the derivation δ is a finitely generated algebra.

Definition 3.25. Let δ be a locally nilpotent derivation of an algebra R. Then the mapping $\phi : R \to R$ defined by

$$\phi(u) = u + \frac{\delta(u)}{1!} + \frac{\delta^2(u)}{2!} + \frac{\delta^3(u)}{3!} + \ldots, \; u \in R,$$

is well defined because δ is locally nilpotent and for any $u \in R$ there exists an m with $\delta^m(u) = 0$ and the sum is finite. It turns out that ϕ is an automorphism of R (see the exercises), which we call an *exponential automorphism* and denote by $\exp(\delta)$.

Example 3.26. (i) If δ is a triangular derivation of $K[X]$, then

$$\delta(x_i) \in K[x_{i+1}, \ldots, x_n]$$

and $\delta^k(x_i)$ also belongs to $K[x_{i+1}, \ldots, x_n]$ for all $k \geq 1$. Moreover δ is locally nilpotent and the corresponding automorphism $\exp(\delta)$ is a triangular automorphism.

(ii) Let $\Delta = (y^2 + zx)\delta$, where $\delta = -2y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y}$, be the derivation in Example 3.22. Since $\delta^3(x) = 0$, $\delta^2(y) = 0$, $\delta(z) = 0$, we obtain that

$$\exp(\Delta) : x \to x + (y^2 + zx)\frac{\delta(x)}{1!} + (y^2 + zx)^2\frac{\delta^2(x)}{2!} = x - 2(y^2 + zx)y + (y^2 + zx)^2 z,$$

$$\exp(\Delta) : y \to y + (y^2 + zx)\frac{\delta(y)}{1!} = y + (y^2 + zx)z,$$

$$\exp(\Delta) : z \to z,$$

and we obtain that $\exp(\Delta)$ is the Nagata automorphism.

Let ϕ be an automorphism of $K[x_1, \ldots, x_n]$. Then for every positive integer m we may extend ϕ to (an automorphism!) $\bar{\phi}$ of $K[x_1, \ldots, x_{n+m}]$ by $\bar{\phi}(x_{n+i}) = x_{n+i}$, $i = 1, \ldots, m$.

Definition 3.27. If ϕ is an automorphism of $K[x_1, \ldots, x_n]$ and its extension $\bar{\phi}$ by $\bar{\phi}(x_{n+i}) = x_{n+i}$, $i = 1, \ldots, m$, to an automorphism of $K[x_1, \ldots, x_{n+m}]$ for some m is a tame automorphism of $K[x_1, \ldots, x_{n+m}]$, we say that ϕ is a *stably tame automorphism* of $K[x_1, \ldots, x_n]$. (In other words, we do not know whether ϕ is tame, but it becomes tame in some bigger polynomial algebra.)

The following theorem of Martha Smith shows that a class of exponential automorphisms, including the Nagata automorphism, are stably tame.

Theorem 3.28. (Martha Smith [S]) *Let δ be a triangular derivation of $K[x_1, \ldots, x_n]$ and let $w \in \mathrm{Ker}(\delta)$. Then the automorphism $\exp(w\delta)$ is stably tame and becomes tame extended to $K[x_1, \ldots, x_{n+1}]$ by $\exp(w\delta) : x_{n+1} \to x_{n+1}$.*

Proof. Let us extend the action of δ to $K[x_1, \ldots, x_{n+1}]$ by $\delta(x_{n+1}) = 0$. Clearly, δ is still triangular considered as a derivation of $K[x_1, \ldots, x_{n+1}]$. Since $x_{n+1} \in \mathrm{Ker}(\delta)$, the derivation $\Delta_1 = x_{n+1}\delta$ is locally nilpotent and even triangular (because δ is triangular, $\Delta_1(x_i) \in x_{n+1}K[x_{i+1}, \ldots, x_n]$, $i = 1, \ldots, n$, and $\Delta_1(x_{n+1}) = 0$.) Consider the tame automorphism σ of $K[x_1, \ldots, x_{n+1}]$ defined by $\sigma(x_i) = x_i$, $i = 1, \ldots, n$, $\sigma(x_{n+1}) = x_{n+1} + w(x_1, \ldots, x_n)$ (which is triangular if we consider the inverse ordering of the variables).

Clearly σ acts as the identity mapping on $K[x_1, \ldots, x_n]$. Let $\phi = \sigma^{-1} \circ \exp(-\Delta_1) \circ \sigma \circ \exp(\Delta_1)$. (Obviously $\exp(-\Delta_1) = (\exp(\Delta_1))^{-1}$.) Direct calculations show that

$$\exp(\pm\Delta_1)(x_{n+1}) = x_{n+1},\ \exp(\pm\Delta_1)(w) = w$$

because x_{n+1} and w are in the kernel of Δ_1 (equal to the kernel of δ),

$$\phi(x_{n+1}) = \sigma^{-1}(\exp(-\Delta_1)(\sigma(\exp(\Delta_1)(x_{n+1})))) = \sigma^{-1}(\exp(-\Delta_1)(\sigma(x_{n+1}))) =$$

$$= \sigma^{-1}(\exp(-\Delta_1)(x_{n+1} + w)) = \sigma^{-1}(x_{n+1} + w) = x_{n+1}.$$

For $u \in K[x_1, \ldots, x_n]$ we have

$$\phi(u) = \sigma^{-1}(\exp(-\Delta_1)(\sigma(\exp(\Delta_1)(u)))) = \sigma^{-1}(\exp(-\Delta_1)(\sigma(\exp(x_{n+1}\delta)(u)))) =$$

$$= \sigma^{-1}(\exp(-\Delta_1)(\exp(\sigma(x_{n+1})\delta)(u))) = \sigma^{-1}(\exp((-x_{n+1}\delta)(\exp(x_{n+1} + w)\delta)(u)))$$

because σ is the identity mapping on $u \in K[x_1, \ldots, x_n]$,

$$\phi(u) = \sigma^{-1}(\exp(-x_{n+1} + (x_{n+1} + w))\delta)(u))$$

because $\exp((w_1 + w_2)\delta) = \exp(w_1\delta) \circ \exp(w_2\delta)$ if $w_1, w_2 \in \mathrm{Ker}(\delta)$ (see the exercises).

$$\phi(u) = \sigma^{-1}(\exp(w\delta)(u)) = \exp(w\delta)(u).$$

In this way $\exp(w\delta) = \phi$ is a composition of the tame automorphisms σ and $\exp(\Delta_1)$ and their inverses. Hence $\exp(w\delta)$ is a tame automorphism of $K[x_1, \ldots, x_{n+1}]$ and is stably tame for $K[x_1, \ldots, x_n]$.

Corollary 3.29. *The Nagata automorphism is stably tame.*

Proof. We consider the presentation of the Nagata automorphism in Example 3.26 (ii) as $\exp(\Delta)$, where $\Delta = (y^2 + zx)\delta$, and $\delta = -2y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y}$ is a triangular derivation. Then the proof follows directly from the theorem.

Exercises

1. Find the inverse of the automorphism ϕ_i (of the corresponding polynomial algebra) defined by:

$$\phi_1(x) = x + (y^2 + 2y + 3),\ \phi_1(y) = y;$$

$$\phi_2(x) = 2x + (y^2 + 2y + 3),\ \phi_2(y) = -y + 2;$$

$$\phi_3(x) = x + (y^2 + 2y + 3z),\ \phi_3(y) = -y + (2z - 3),\ \phi_3(z) = z + 1;$$

$$\phi_4(x) = 2x + 3y,\ \phi_4(y) = x + y;$$

$$\phi_5(x) = 2x + 3y + 1,\ \phi_5(y) = x + y - 3.$$

$$\phi_6(x) = 3x + 5y + 1,\ \phi_6(y) = 2x + 3y + 5.$$

$$\phi_7(x) = 2x + (3y^2 + yz + z^3),\ \phi_7(y) = 3y + (2z + 3),\ \phi_7(z) = -z + 5.$$

Solution. For the triangular automorphisms calculate step by step the action of ϕ_i^{-1} on the variables in inverse order, e.g. first on z, then on y and finally on x:

Obviously, $\phi_1^{-1}(y) = y$. If $\phi_1^{-1}(x) = \alpha x + g(y)$, then

$$x = \phi_1^{-1}(\phi_1(x)) = \phi_1^{-1}(x + y^2 + 2y + 3) = (\alpha x + g(y)) + y^2 + 2y + 3,$$

and $g(y) = -(y^2 + 2y + 3)$. Hence $\phi_1^{-1}(x) = x - (y^2 + 2y + 3)$.

Let $\phi_2^{-1}(y) = \alpha y + \beta$. Then

$$y = \phi_2^{-1}(\phi_2(y)) = \phi_2^{-1}(-y + 2) = -(\alpha y + \beta) + 2,$$

$\alpha = -1$, $-\beta + 2 = 0$, i.e. $\beta = 2$ and $\phi_2^{-1}(y) = -y + 2$. If $\phi_2^{-1}(x) = \gamma x + g(y)$, then

$$x = \phi_2^{-1}(\phi_2(x)) = \phi_2^{-1}(2x + (y^2 + 2y + 3)) = 2(\gamma x + g(y)) + (y^2 + 2y + 3),$$

$2\gamma = 1$, $2g(y) + (y^2 + 2y + 3) = 0$ and $\phi_2^{-1}(x) = x/2 - (y^2 + 2y + 3)/2$.

Similarly, $\phi_3(z) = z - 1$, $\phi_3^{-1}(y) = -y + 2z - 5$, $\phi_3^{-1}(x) = x + f(y, z)$,

$$x = \phi_3^{-1}(\phi_3(x)) = \phi_3^{-1}(x + (y^2 + 2y + 3z))$$

$$= x + f(y, z) + (-y + 2z - 5)^2 + 2(-y + 2z - 5) + 3(z - 1),$$

$\phi_3^{-1}(x) = x - ((-y + 2z - 5)^2 + 2(-y + 2z - 5) + 3(z - 1))$.

For the linear automorphism ϕ_4 with matrix $g = \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix}$ the inverse automorphism has a matrix

$$g^{-1} = \begin{pmatrix} -1 & 1 \\ 3 & -2 \end{pmatrix},\ \text{and } \phi_4^{-1}(x) = -x + 3y,\ \phi_4^{-1}(y) = x - 2y.$$

The inverse of the affine automorphism ϕ_5 has a linear component which is inverse to the linear component of ϕ_5 and

$$\phi_5^{-1}(x) = -x + 3y + \alpha,\ \phi_5^{-1}(y) = x - 2y + \beta.$$

Then

$$x = \phi_5(\phi_5^{-1}(x)) = \phi(-x + 3y + \alpha) = -(2x + 3y + 1) + 3(x + y - 3) + \alpha,\ \alpha = 10,$$

$$y = \phi_5(\phi_5^{-1}(y)) = \phi(x - 2y + \beta) = (2x + 3y + 1) - 2(x + y - 3) + \beta,\ \beta = -7.$$

2. Find the product $\phi^{-1} \circ \psi^{-1} \circ \tau \circ \sigma$, where

$$\sigma(x) = 2x + y + 1,\ \sigma(y) = x + y - 1,$$

$$\tau(x) = x + 2y^2,\ \tau(y) = y,$$

$$\psi(x) = x + 2y + 1,\ \psi(y) = x + 3y + 2,$$

$$\phi(x) = x + 1,\ \phi(y) = y + x^2.$$

3. Prove that the triangular automorphisms ϕ_f of $K[x, y]$ of the form $\phi_f(x) = x + f(y)$, $\phi_f(y) = y$ form an abelian group isomorphic to the additive group of $K[y]$.

Hint. Show that $\phi_f \circ \phi_g = \phi_{f+g}$ for any $f, g \in K[y]$.

4. Show that the the following derivations are locally nilpotent and the polynomials w belong to the kernels of the derivations of $K[X]$:

$$\delta_1 = y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y},\ w_1 = y^2 - 2xz,\ X = \{x, y, z\};$$

$$\delta_2 = 2u(vy - uz)\frac{\partial}{\partial x} - 2v(vy - uz)\frac{\partial}{\partial y} + (v^2x - u^2y)\frac{\partial}{\partial z},$$

$$w_2' = xy - z^2,\ w_2'' = v^2x + u^2y - 2uvz,\ X = \{u, v, x, y, z\}.$$

Hint. Use that $\delta_1(x) = y$, $\delta_1(y) = z$, $\delta_1(z) = 0$ and check that $\delta_1^3(x) = 0$, $\delta_1^2(y) = 0$, $\delta_1(w_1) = 0$. The calculations for δ_2 are similar but more complicated. Then $\delta_2(u) = \delta_2(v) = 0$, $\delta_2(x) = 2u(vy - uz)$, $\delta_2(y) = 2v(vy - uz)$, $\delta_2(z) = (v^2x - u^2y)$, $\delta_2^3(x) = \delta_2^3(y) = \delta_2^3(z) = 0$.

5. Let R be a (not necessarily commutative) algebra and let $\mathcal{D}(R)$ be the set of all derivations of R. Show that $\mathcal{D}(R)$ is a vector space (with respect to the usual operations on sets of linear operators: addition and multiplication with constants). Define $[\delta_1, \delta_2] = \delta_1 \circ \delta_2 - \delta_2 \circ \delta_1$ and show that $\mathcal{D}(R)$ satisfies the relations:

$$[\delta, \delta] = 0\,(\textit{anticommutative low}),$$

$$[[\delta_1, \delta_2], \delta_3] + [[\delta_2, \delta_3], \delta_1] + [[\delta_3, \delta_1], \delta_2] = 0\,(\textit{Jacobi identity}),$$

for all $\delta, \delta_1, \delta_2, \delta_3 \in \mathcal{D}(R)$. (This means that $\mathcal{D}(R)$ is a *Lie algebra*.)

6. Prove the Leibniz formula for $\delta^n(uv)$, where δ is a derivation of the algebra R and $u, v \in R$.

7. Let R be any algebra and let δ be a derivation of R. Show that $\mathrm{Ker}(\delta)$ is a subalgebra of R.

Hint. Use that $\mathrm{Ker}(\delta)$ is a subspace of R for any linear operator δ on R. Then show that if $\delta(u) = \delta(v) = 0$, then $\delta(uv) = 0$.

8. Show that the exponent $\exp(\delta)$ of a locally nilpotent derivation δ of the algebra R is an automorphism.

Hint. Show that $\exp(\delta)$ is a linear operator on R and, using the Leibniz formula, that $(\exp(\delta))(uv) = (\exp(\delta))(u)(\exp(\delta))(v)$, $u, v \in R$.

9. If δ_1, δ_2 are locally nilpotent derivations and $\delta_1 \circ \delta_2 = \delta_2 \circ \delta_1$, show that $\delta_1 + \delta_2$ is also locally nilpotent and $\exp(\delta_1 + \delta_2) = \exp(\delta_1) \circ \exp(\delta_2)$.

Hint. Use, that if the linear operators δ_1, δ_2 commute and are locally nilpotent, then $\delta_1 + \delta_2$ is also locally nilpotent and $\exp(a + b) = \exp(a)\exp(b)$, provided that $ab = ba$ and $a^n = b^m = 0$.

10. Find a system of generators of the kernel of the derivation δ_i of the polynomial algebra $K[X]$, where:

$$\delta_1 = y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y},\ \delta_2 = -2y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y},\ X = \{x, y, z\};$$

$$\delta_3 = y\frac{\partial}{\partial x} + t\frac{\partial}{\partial z},\ \delta_4 = y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y} + t\frac{\partial}{\partial z},\ X = \{x, y, z, t\}.$$

Solution. **Method 1.** We shall consider δ_2 because is related with the Nagata automorphism. The considerations for δ_1 are similar. For δ_3 and δ_4 it is better to use the second method. It is easy to see that $y^2 + zx$ and z are in the kernel of δ_2. Hence $K[y^2 + zx, z] \subseteq \mathrm{Ker}(\delta_2)$. Let $f(x, y, z) \in \mathrm{Ker}(\delta_2)$. We present it in the form

$$f(x,y,z) = f_0(x,y^2,z) + yf_1(x,y^2,z) = f_0(x,(y^2+zx)-zx,z) + yf_1(x,(y^2+zx)-zx,z) =$$

$$= g_0(x, y^2 + zx, z) + yg_1(x, y^2 + zx, z) =$$

$$\sum_{k=0}^{m} a_k(y^2 + zx, z)x^k + y\sum_{k=0}^{m} b_k(y^2 + zx, z)x^k,\ a_k, b_k \in K[y^2 + zx, z].$$

Using that $a_k, b_k \in \mathrm{Ker}(\delta_2)$, we obtain

$$0 = \delta_2(f) = -2y\sum_{k=0}^{m} ka_k(y^2 + zx, z)x^{k-1}$$

$$-2y^2\sum_{k=0}^{m} kb_k(y^2 + zx, z)x^{k-1} + z\sum_{k=0}^{m} b_k(y^2 + zx, z)x^k.$$

First we consider the summands with odd powers of y and obtain that $a_k(y^2+zx, z) = 0$ for $k = 1, \ldots, m$. Then we consider the sum as a polynomial in the new variables $x, y^2 + zx, z$ and compare the powers of x starting from the highest. We obtain consecutively that $b_k(y^2 + zx) = 0$, $k = m, m-1, \ldots, 1$. Hence $f = a_0(y^2 + zx, z) + yb_0(y^2 + zx, z)$ and, since $\delta_2(f) = zb_0(y^2+zx, z) = 0$, we have that $f = a_0(y^2+zx, z)$. Hence $\mathrm{Ker}(\delta_2) = K[y^2+zx, z]$. The result for δ_1 is $\mathrm{Ker}(\delta_1) = K[y^2 - 2zx, z]$.

Method 2. Since $\delta_2(z) = 0$, we may think that z is a constant and (for a moment only) to consider δ_2 as a derivation of $(K(z))[x, y]$. Changing the variables as follows, we obtain a better form of δ_2. Let

$$u = x + \frac{y^2}{z},\ v = \frac{y}{z}.$$

Then $(K(z))[x, y] = (K(z))[u, v]$ and $\delta_2(u) = 0$, $\delta_2(v) = 1$. Hence $\delta_2 = \frac{\partial}{\partial v}$ and $\mathrm{Ker}(\delta_2) = K(z)[u]$. In other words, the kernel of δ_2 in $(K(z))[x, y]$ consists of all polynomials in $u = x + y^2/z$ with coefficients which are rational functions of z. Hence the kernel of δ_2 in $K[x, y, z]$ consists of all polynomials in x, y, z in the form

$$f(x, y, z) = \sum_{k=0}^{m} \frac{a_k(z)}{b_k(z)} \left(x + \frac{y^2}{z}\right)^k = \frac{1}{b(z)} \sum_{k=0}^{m} c_k(z)(y^2 + zx)^k,$$

where a_i, b_i, c_i, b are polynomials in z. From here one can easily deduce that $b(z) = 1$ and to derive that $f(x, y, z)$ is a polynomial of $y^2 + zx$ and z.

The considerations for δ_3 are in the same spirit. Since $\delta_3(y) = \delta_3(t) = 0$, we consider y and t as constants and assume that δ_3 as a derivation of $(K(y, t))[x, z]$. Then $\delta_3(x/y) = \delta_3(z/t) = 1$ and the new variables

$$u = \frac{x}{y} - \frac{z}{t},\ v = \frac{z}{t}$$

of $K(y, t)[x, z]$ satisfy $\delta_3(u) = 0$, $\delta_3(v) = 1$. Hence $\mathrm{Ker}(\delta_3) = (K(y, t))[u]$ and $f(x, y, z, t) \in \mathrm{Ker}(\delta_3)$ is a polynomial of the form

$$f(x, y, z, t) = \sum_{k=0}^{m} \frac{a_k(y, t)}{b_k(y, t)} \left(\frac{x}{y} - \frac{z}{t}\right)^k.$$

From here we can easily derive that $f(x, y, z, t) \in \mathrm{Ker}(\delta_3) \cap K[x, y, z, t]$ is a polynomial of $y, t, xt - zy$.

For $\mathrm{Ker}(\delta_4)$ and the kernels of other linear locally nilpotent derivations see the book by Nowicki [No]. The idea is to use the results for δ_1 and the second method. The answer is that the kerenl of δ_4 is generated by

$$t, z^2 - 2yt, z^3 - 3tyz + 3t^2x, y^2z^2 - 2z^3x + 6txyz - \frac{8}{3}ty^3 - 3t^2x^3.$$

4. TAME AUTOMORPHISMS OF POLYNOMIAL ALGEBRAS IN TWO VARIABLES

In this section we assume that K is a fixed algebraically closed field of characteristic 0, e.g. $K = \mathbf{C}$. The assumption that K is algebraically closed is not essential for the results (but simplifies the proofs). We shall prove the theorem that every automorphism of $K[x, y]$ is tame. The first proof for $K = \mathbf{C}$ was given by Jung [J] in 1942. The general case was established by van der Kulk [V] in 1953. Since this is one of the main results in the theory of automorphisms of polynomial algebras with numerous applications also to algebraic geometry, there are several different proofs of the theorem, see the book by van den Essen [E2]. We shall present the proof of Makar-Limanov [ML] given in a preprint form (and included also in [D]).

Definition 4.1. Let δ be a locally nilpotent derivation of $K[x, y]$. We define a *degree function* $\deg = \deg_\delta$ by

$$\deg_\delta(u) + \min(n \mid \delta^{n+1}(u) = 0),\ 0 \neq u \in K[x, y].$$

If $u = 0$, then we define $\deg_\delta(0) = -\infty$.

In the special case of $\delta = \frac{\partial}{\partial x}$ the degree with respect to δ coincides with the usual degree with respect to x. (One needs to apply 3 times $\frac{\partial}{\partial x}$ to annihilate a polynomial $a(y)x^2 + b(y)x + c(y)$.)

Lemma 4.2. *If δ is a locally nilpotent derivation of $K[x, y]$, then for every $u, v \in K[x, y]$*

(i) $\deg_\delta(u + v) \leq \max(\deg_\delta(u), \deg_\delta(v))$,

(ii) $\deg_\delta(u + v) = \deg_\delta(u) + \deg_\delta(v)$.

(iii) *If* $\deg_\delta(uv) = 0$, *then* $\deg_\delta(u) = \deg_\delta(v) = 0$.

Proof. If $\deg_\delta(u) = n$, $\deg_\delta(v) = m$, then $\delta^{n+1}(u) = \delta^{m+1}(v) = 0$, $\delta^n(u), \delta^m(v) \neq 0$.

(i) If $n \geq m$, then $\delta^{n+1}(u + v) = \delta^{n+1}(u) + \delta^{n+1}(v) = 0$ and $\deg_\delta(uv) \leq n$.

(ii) By the Leibniz formula

$$\delta^p(uv) = \sum_{k=0}^{p} \binom{p}{k} \delta^{p-k}(u)\delta^k(v).$$

If $p = n + m + 1$, then either $p - k \geq n + 1$ or $k \geq m + 1$ and $\delta^{n+m+1}(uv) = 0$. If $p = n + m$, then the only summand with $p - k \leq n$, $k \leq m$ is for $k = m$ and $\delta^{n+m}(uv) = \binom{n+m}{m}\delta^n(u)\delta^m(v) \neq 0$. Hence $\deg_\delta(uv) = n + m$.

(iii) If $\deg_\delta(uv) = 0$, then $u, v \neq 0$, and $\deg_\delta(u), \deg_\delta(v) \geq 0$. By (ii), $0 = \deg_\delta(uv) = \deg_\delta(u) + \deg_\delta(v)$, i.e. $\deg_\delta(u) = \deg_\delta(v) = 0$.

Let $f(x, y) \in K[x, y]$ be a fixed polynomial. We define the derivation δ of $K[x, y]$ by

$$\delta(u) = \begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial u}{\partial x} \\ \frac{\partial f}{\partial y} & \frac{\partial u}{\partial y} \end{vmatrix} = f_x u_y - f_y u_x,\ u \in K[x, y],$$

i.e.

$$\delta = f_x \frac{\partial}{\partial y} - f_y \frac{\partial}{\partial x},$$

(see Section 3 for the properties of δ).

If ϕ and ψ are automorphisms of $K[x, y]$ such that $\phi(x) = \psi(x)$, then $\phi^{-1} \circ \psi(x) = x$. If $\phi^{-1} \circ \psi(y) = g(x, y)$, then, calculating the determinant of the Jacobian matrix of $\phi^{-1} \circ \psi$ (which is a nonzero constant because $\phi^{-1} \circ \psi$ is an automorphism), we obtain that

$$\det J(\phi^{-1} \circ \psi) = \begin{vmatrix} (\phi^{-1} \circ \psi(x))_x & (\phi^{-1} \circ \psi(y))_x \\ (\phi^{-1} \circ \psi(x))_y & (\phi^{-1} \circ \psi(y))_y \end{vmatrix} = \begin{vmatrix} x_x & g_x \\ x_y & g_y \end{vmatrix} = \begin{vmatrix} 1 & g_x \\ 0 & g_y \end{vmatrix} = g_y = \alpha \in K^*.$$

Hence $g(x, y) = \alpha y + h(x)$ and $\phi^{-1} \circ \psi$ is a triangular automorphism. In this way, every automorphism is "almost" determined by the image of x. It is difficult to describe the polynomials $\phi(x)$, where $\phi \in \mathrm{Aut}K[x, y]$ but we are able to describe their highest homogeneous components. (Compare with the description of the tame automorphisms of $R[x, y]$ in Section 3.)

Let us fix two positive relatively prime integers p and q and let us assume that the degree of x is equal to p and the degree of y is equal to q. (We have seen such kind of grading in invariant theory. For example, the algebra of symmetric polynomials in n variables is generated by the elementary symmetric polynomials $e_1, \ldots, e_n$ and we assume that $\deg(e_i) = i$.) For example, if $p = 2$, $q = 5$, then

$$\deg(x^6y^3) = 6.2 + 3.5 = \deg(xy^5) = 1.2 + 5.5 = \deg(x^{11}y) = 11.2 + 1.5 = 27,$$

$$\deg(x^4y^2) = 4.2 + 2.5 = 18, \deg(x^{10}y) = 10.2 + 1.5 = 25,$$

and the homogeneous component of maximal degree (equal to 27) of

$$u(x, y) = 5x^6y^3 - xy^5 + 2x^{11}y + 6x^4y^2 - 3x^{10}y$$

is $\overline{u(x, y)} = 5x^6y^3 - xy^5 + 2x^{11}y$. As in Section 3, we use $\overline{u(x, y)}$ to denote the homogeneous component of maximal degree of $u(x, y)$ with respect to our (p, q)-grading.

Lemma 4.3. (i) *Let p, q be positive relatively prime integers and let $u, v \in K[x, y]$. If $(\overline{u})_x(\overline{v})_y - (\overline{u})_y(\overline{v})_x \neq 0$, then*

$$\overline{u_x v_y - u_y v_x} = (\overline{u})_x(\overline{v})_y - (\overline{u})_y(\overline{v})_x.$$

(ii) *If $f(x, y) \in K[x, y]$ is a fixed polynomial and the derivation δ defined by $\delta(u) = f_x u_y - f_y u_x$, $u \in K[x, y]$, is locally nilpotent, then the derivation δ_1 defined by*

$$\delta_1(u) = (\overline{f})_x u_y - (\overline{f})_y u_x,\ u \in K[x, y],$$

is also locally nilpotent.

Proof. (i) For two monomials $x^a y^b$ and $x^c y^d$, the determinant of the Jacobian matrix is

$$\mathrm{Jac}(x^a y^b, x^c y^d) = \begin{vmatrix} (x^a y^b)_x & (x^c y^d)_x \\ (x^a y^b)_y & (x^c y^d)_y \end{vmatrix} = (ad - bc) x^{a+c-1} y^{b+d-1}.$$

Since $u_xv_y - u_yv_x$ is a linear combination of Jacobian determinants of the monomials which participate in the expressions of u and v, and

$$\deg_{(p,q)}(\mathrm{Jac}(x^ay^b, x^cy^d)) = \deg_{(p,q)}(x^{a+c-1}y^{b+d-1}) = \deg_{(p,q)}(x^ay^b)+\deg_{(p,q)}(x^cy^d)-p-q,$$

we obtain that the (p,q)-degree of $u_xv_y - u_yv_x$ is equal to $\deg_{(p,q)}(u)+\deg_{(p,q)}(v)-p-q$ (if $(\overline{u})_x(\overline{v})_y - (\overline{u})_y(\overline{v})_x \neq 0$), or less otherwise, and the homogeneous component $\overline{u_xv_y - u_yv_x}$ of maximal degree of $u_xv_y - u_yv_x$ is $(\overline{u})_x(\overline{v})_y - (\overline{u})_y(\overline{v})_x$ if this expression is not equal to 0.

(ii) If δ is locally nilpotent, then $\delta^n(u) = 0$ for some n. It is sufficient to prove that $\delta_1^n(x) = \delta_1^m(y) = 0$ for some n, m. If u, v are (p,q)-homogeneous polynomials, then $u_xv_y - u_yv_x$ is also (p,q)-homogeneous (of degree with $p+q$ smaller than the degree of uv). Hence $\delta_1^k(x)$ is homogeneous for all k and $\delta_1^k(x) = \delta^k(x)$ if $\delta_1^k \neq 0$. In this way, $\delta_1^n(x) = 0$ (because $\delta^n(x) = 0$). Similarly $\delta_1^m(y) = 0$ and δ_1 is locally nilpotent.

Lemma 4.4. *Let p, q be positive relatively prime integers and let the nonzero polynomial $f(x,y) \in K[x,y]$ be (p,q)-homogeneous. Then f has a decomposition of the form*

$$f(x,y) = \alpha x^a y^b \prod_{i=1}^{k}(x^q - \beta_i y^p),\ \alpha \in K^*, \beta_i \in K,\ a, b, k \geq 0.$$

Proof. We write $f(x,y)$ in the form

$$f(x,y) = \alpha x^a y^b (x^{c_0} + \gamma_1 x^{c_1}y^{d_1} + \ldots + \gamma_p x^{c_s}y^{d_s} + \gamma_{s+1}y^{d_{s+1}}),\ \gamma_i \in K.$$

Since f is (p,q)-homogeneous, we have for all monomials

$$pc_0 = pc_1 + qd_1 = \ldots = pc_s + qd_s = qd_{s+1}.$$

Since p and q are relatively prime, we obtain that p divides $d_1, \ldots, d_s, d_{s+1}$ and q divides $c_0, c_1, \ldots, c_s$. If $c_i = qn_i$, $i = 0, 1, \ldots, s$, and $d_i = pm_i$, $i = 1, \ldots, s, s+1$, then the degree of the summands are respectively $pqn_0 = pq(n_1 + m_1) = \ldots = pq(n_s + m_s) = pqm_{s+1}$. In other words, $n_i + m_i = n_0 = m_{s+1}$, $i = 1, \ldots, s$, and f is a product of $\alpha x^a y^b$ and an expression of the form $(x^q)^n + \rho_1(x^q)^{n-1}(y^p) + \ldots + \rho_{k-1}(x^q)(y^p)^{k-1} + \rho_k(y^p)^k$, $\rho_i \in K$. Now, it is sufficient to use that the base field K is algebraically closed and to decompose the polynomial $t^n + \rho_1 t^{n-1} + \ldots + \rho_{k-1}t + \rho_k$ as a product of linear factors.

Studying the tame automorphisms of $R[x,y]$ in Section 3, we proved that for every tame automorphism ϕ and up to the action of an affine automorphism, one of the homogeneous components of maximal degree $\overline{\phi(x)}$ and $\overline{\phi(y)}$ is a power of the other. In most of the proofs of the theorem that all automorphisms of $K[x,y]$ are tame, we have to prove something similar for any automorphism of $K[x,y]$.

Lemma 4.5. *Let p, q be positive relatively prime integers and let ϕ be an automorphism of $K[x,y]$. Then the (p,q)-homogeneous component of maximal degree $\overline{\phi(x)}$ of $\phi(x)$ is of the form αx^a, αy^b or $\alpha(x^q - \beta y^p)^k$.*

Proof. Let $f(x,y) = \phi(x)$. Then the derivation δ defined by $\delta(u) = f_x u_y - f_y u_x$, $u \in K[x,y]$, is locally nilpotent (because ϕ is an automorphism, see Section 3). Hence, the

derivation δ_1 defined by $\delta_1(u) = (\overline{f})_x u_y - (\overline{f})_y u_x$, $u \in K[x,y]$, is also locally nilpotent, be Lemma 4.3. Additionally, $\delta_1(\overline{f}) = 0$. Let us decompose $\overline{f}$ as in Lemma 4.4. If

$$\overline{f(x,y)} = \alpha x^a y^b \prod_{i=1}^{k} (x^q - \beta_i y^p),\ \alpha \in K^*, \beta_i \in K,\ a,b,k \geq 0,$$

then, $\overline{f}$ is in the kernel of δ_1 and $\deg_{\delta_1}(\overline{f}) = 0$. By Lemma 4.2, all factors also belong to the kernel of δ_1. If $\overline{f}$ has two different factors, then we obtain that both of them belong to the kernel. Let, for example, $\delta_1(x^q - \beta_1 y^p) = \delta_1(x^q - \beta_2 y^p) = 0$ for $\beta_1 \neq \beta_2$. Then $\delta_1(x^q) = 0$, $\delta_1(y^p) = 0$ and again by Lemma 4.2, $\delta_1(x) = \delta_1(y) = 0$. Hence $\delta_1 = 0$, which is impossible (because $f = \phi(x)$ is not a constant). In this way, $\overline{f(x,y)}$ has only one (maybe multiple) factor.

Lemma 4.6. *Let p, q be positive relatively prime integers and let ϕ be an automorphism of $K[x,y]$. If the (p,q)-homogeneous component of maximal degree $\overline{\phi(x)}$ of $\phi(x)$ is of the form $\alpha(x^q - \beta y^p)^k$ with $\beta \neq 0$, then $p = 1$ or $q = 1$.*

Proof. Let $\overline{f(x,y)} = \overline{\phi(x)} = (x^q - \beta y^p)^k$. (The assumption $\alpha = 1$ is not essential for the considerations.) By Lemma 4.3, the derivation δ_1 defined by $\delta_1(u) = ((x^q - \beta y^p)^k)_x u_y - ((x^q - \beta y^p)^k)_y u_x$, $u \in K[x,y]$, is locally nilpotent. Let us define the derivation δ_2 by $\delta_2(u) = (x^q - \beta y^p)_x u_y - (x^q - \beta y^p)_y u_x$, $u \in K[x,y]$. Then $x^q - \beta y^p$ belongs to the kernel of δ_2 and $\delta_1 = k(x^q - \beta y^p)^{k-1}\delta_2$. Then, as in Section 3, we see that $\delta_1^n = (k(x^q - \beta y^p)^{k-1})^n \delta_2^n$. Since δ_1 is locally nilpotent, δ_2 is also locally nilpotent. We check directly, than $\delta_2(x) = \beta p y^{p-1}$, $\delta_2(y) = q x^{p-1}$. Let $\deg = \deg_{\delta_2}$ be the degree function related (as in Definition 4.1) to the locally nilpotent derivation δ_2. Let $d = \deg(x)$, $e = \deg(y)$. Hence $\delta_2^{d+1}(x) = 0$ and $\delta_2^d(x) \neq 0$. Hence $\delta_2^d(\delta_2(x)) = 0$, $\delta_2^{d-1}(\delta_2(x)) \neq 0$ and $\deg(\delta_2(x)) = d - 1$. Similarly $\deg(\delta_2(e)) = e - 1$. On the other hand, the degree of a product is equal to the sum of the degrees of the factors. Hence the equalities $\delta_2(x) = \beta p y^{p-1}$ and $\delta_2(y) = q x^{p-1}$ imply that

$$d-1 = \deg(\delta_2(x)) = (p-1)\deg(y) = (p-1)e,\ e-1 = \deg(\delta_2(y)) = (q-1)\deg(x) = (q-1)d.$$

Hence $-2 = (q-2)d + (p-2)e$. Since p, q are positive integers, this is possible only if $p = 1$ or $q = 1$.

Theorem 4.7. (Jung [J], van der Kulk [V]) *Every automorphism of $K[x,y]$ is tame.*

Proof. Let ϕ be an automorphism of $K[x,y]$. We apply induction on the product $\deg_x(\phi(x)) \cdot \deg_y(\phi(x))$, the degrees of $\phi(x)$ with respect to x and y. If this product is equal to 0, then $\phi(x)$ depends only on x or only on y. In the first case $\phi(x) = \alpha x + \beta$, the determinant of the Jacobian is an invertible element of K and is equal to

$$\begin{vmatrix} (\phi(x))_x & \phi(y))_x \\ (\phi(x))_y & \phi(y))_y \end{vmatrix} = \begin{vmatrix} \alpha & \phi(y))_x \\ 0 & \phi(y))_y \end{vmatrix} = \alpha(\phi(y))_y.$$

Hence $(\phi(y))_y = \gamma \in K^*$ and $\phi(y) = \gamma y + h(x)$. In this way, ϕ is a triangular automorphism. The case when $\phi(x)$ depends on y only is similar and ϕ is of the form $\phi(x) = \alpha y + \beta$, $\phi(y) = \gamma x + h(y)$. Then $\phi = \theta \circ \psi$, where the triangular automorphism ψ and the linear

automorphism θ are defined by $\psi(x) = \alpha x + \beta$, $\psi(y) = \gamma y + h(x)$ and $\theta(x) = y$, $\theta(y) = x$. In both the cases ϕ is tame. Now we assume that $\phi(x)$ essentially depends on both x and y. Let $\deg_x(\phi(x)) = a$, $\deg_y(\phi(x)) = b$. We choose positive relatively prime integers p and q such that $pa = bq$ and introduce the (p, q)-grading of $K[x, y]$. Let the (p, q)-degree of $\phi(x)$ be equal to c. Clearly, $c \geq pa$ because $\phi(x)$ contains a monomial $\alpha x^a y^m$ for some $m \geq 0$. If $c = pa$, then the (p, q)-homogeneous component $\overline{\phi(x)}$ of $\phi(x)$ contains a summand αx^a. Similarly it contains $\alpha_1 y^b$ and $\overline{\phi(x)}$ essentially depends on both x and y. If $c > pa = qb$, then any monomial $\rho x^n y^n$ of maximal degree satisfies $pn + qm = c > pa = qb$ which (because $n \leq a$, $m \leq b$) is possible only for $n, m \geq 1$. Again, $\overline{\phi(x)}$ depends on both x and y. By Lemma 4.5, $\overline{\phi(x)}$ is of the form $\overline{\phi(x)} = \alpha(x^q - \beta y^p)^k$ (and hence $c = pa = qb = kpq$). By Lemma 4.6 we obtain that $p = 1$ or $q = 1$ and $\overline{\phi(x)} = \alpha(x - \beta y^p)^k$ or $\overline{\phi(x)} = \alpha_1(y - \beta_1 x^q)^k$, for some $\alpha, \beta, \alpha_1, \beta_1 \in K^*$. First, let $\overline{\phi(x)} = \alpha_1(y - \beta_1 x^q)^k$. Let us compose ϕ with the tame automorphism ψ defined by $\psi(x) = x$, $\psi(y) = y + \beta_1 x^q$. Pay attention that the element $\psi(y) = y + \beta_1 x^q$ is (p, q)-homogeneous of degree q (because the degree of x is equal to $p = 1$ and the degree of y is equal to q) and this degree is equal to the degree of y. Hence ψ sends a (p, q)-homogeneous polynomials to homogeneous polynomials of the same degree. In this way, the homogeneous component of maximal degree of $\psi \circ \phi(x) = \psi(\phi(x))$ is equal to the image under ψ of the homogeneous component $\overline{\phi(x)}$. Hence $\overline{\psi \circ \phi(x)} = \psi\left(\overline{\phi(x)}\right) = \psi(\alpha_1(y - \beta_1 x^q)^k) = \alpha_1 y^k$. The (p, q)-degree of $\phi(x)$ is $kq = a = qb$ ($p = 1$) and $\deg_x(\phi(x)) = a = kq$, $\deg_y(\phi(x)) = b = k$. Since the (p, q)-degree of $\psi \circ \phi(x)$ is equal to the same $a = kq$, and the leading homogeneous component is $\alpha_1 y^k$, we obtain that $\deg_x(\psi \circ \phi(x)) < a$, $\deg_y(\psi \circ \phi(x)) = b$, and their product is smaller than the corresponding product for $\phi(x)$. By inductive arguments, the automorphism $\psi \circ \phi$ is tame and, since ψ is also tame, we conclude that ϕ is tame.

Remark 4.8. The proof of Theorem 4.7 gives an algorithm how to decompose any automorphism of $K[x, y]$ as a product of triangular and affine automorphisms (see the exercises for an example).

Exercises

1. Given the automorphisms ϕ_i of $K[x,y]$, where

$$\phi_1(x) = 2x + 3y,\ \phi_1(y) = x + 2y,$$

$$\phi_2(x) = x + 2y^2,\ \phi_2(y) = y,$$

$$\phi_3(x) = x + 2y,\ \phi_3(y) = 2x + 5y,$$

$$\phi_4(x) = x + y^3,\ \phi_4(y) = y,$$

$$\phi_5(x) = x + y,\ \phi_5(y) = 2x + 3y,$$

find the composition $\phi = \phi_5 \circ \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1$ and then decompose ϕ as a product of triangular and affine automorphisms following the proof of the theorem of Jung-van der Kulk.

Solution. By direct calculations one sees that

$$\phi(x) = (46x+65y)+4(12x+17y)^2+8(2x+3y)^3+16(12x+17y)(2x+3y)^3+16(2x+3y)^6,$$

$$\phi(y) = (29x+41y)+2(12x+17y)^2+5(2x+3y)^3+8(12x+17y)(2x+3y)^3+8(2x+3y)^6.$$

For the decomposition, we see that the homogeneous components of maximal degree of $\phi(x)$ and $\phi(y)$ satisfy $\overline{\phi(x)} = 2\overline{\phi(y)}$ and we consider $\rho_1 = \phi \circ \psi_1$, where

$$\psi_1(x) = x - 2y,\ \psi_1(y) = y,$$

and obtain

$$\rho_1(x) = (-12x - 17y) - 2(2x + 3y)^3,$$

$$\rho_1(y) = (29x+41y)+2(12x+17y)^2+5(2x+3y)^3+8(12x+17y)(2x+3y)^3+8(2x+3y)^6.$$

Again, $\overline{\rho_1(y)} = 2(\overline{\rho_1(x)})^2$ and for

$$\psi_2(x) = x,\ \psi_2(y) = y - 2x^2,$$

the composition $\rho_2 = \rho_1 \circ \psi_2$ satisfies

$$\rho_2(x) = (-12x - 17y) - 2(2x + 3y)^3,$$

$$\rho_2(y) = (29x + 41y) + 5(2x + 3y)^3.$$

Since $\overline{\rho_2(y)} = (-5/2)\overline{\rho_2(x)}$, the next step is to calculate $\rho_3 = \rho_2 \circ \psi_3$, where $\psi_3(x) = x$, $\psi_3(y) = y + 5x/2$. In order to work with integers only, we shall consider instead the above ψ_3

$$\psi_3(x) = x,\ \psi_3(y) = 2y + 5x,$$

and $\rho_3 = \rho_2 \circ \psi_3$, and obtain after calculations

$$\rho_3(x) = (-12x - 17y) - 2(2x + 3y)^3,\ \rho_3(y) = -(2x + 3y).$$

Finally, for $\psi_4(x) = x + 2y^3$, $\psi_4(y) = y$ and $\rho_4 = \rho_3 \circ \psi_4$ we obtain

$$\rho_4(x) = -(12x + 17y),\ \rho_4(y) = -(2x + 3y)$$

which is affine. Hence $\phi \circ \psi_1 \circ \psi_2 \circ \psi_3 \circ \psi_4 = \rho_4$ and

$$\phi = \rho_4 \circ \psi_4^{-1} \circ \psi_3^{-1} \circ \psi_2^{-1} \circ \psi_1^{-1}.$$

2. The same problem as in Exercise 1 for the product $\phi^{-1} \circ \psi^{-1} \circ \tau \circ \sigma$, where

$$\sigma(x) = 2x + y + 1,\ \sigma(y) = x + y - 1,$$

$$\tau(x) = x + 2y^2,\ \tau(y) = y,$$

$$\psi(x) = x + 2y + 1,\ \psi(y) = x + 3y + 2,$$

$$\phi(x) = x + 1,\ \phi(y) = y + x^2.$$

5. ALGORITHMS FOR AUTOMORPHISMS OF POLYNOMIAL ALGEBRAS

In this section we assume that K is a fixed field of characteristic 0 and we are able to perform calculations in K. For example, we may assume that $K = \mathbf{Q}$. The proof of the theorem of Jung-van der Kulk presented in Section 4 gives an effective algorithm which decomposes any automorphism of $K[x, y]$ as a product of triangular and affine automorphisms. It is also clear that if we apply the algorithm to any endomorphism of $K[x, y]$, we either will obtain that the endomorphism is an automorphism and will obtain its decomposition, or, we will be not able to perform some step of the algorithm and this will mean that the endomorphism is not an automorphism.

We shall give two more algorithms. The first one works in a very general situation (even for noncommutative algebras). It decides whether an endomorphism of the polynomial algebra $K[X]$ is an automorphism and, if this is the case, finds the inverse.

The second algorithm decides whether a polynomial $p(x, y)$ in $K[x, y]$ is an image of x under some automorphism of $K[x, y]$. The careful study of the proof allows also to deduce an algorithm which finds a concrete $\phi \in \mathrm{Aut}K[x, y]$ such that $p(x, y) = \phi(x)$.

The theoretical result involved in the first algorithm has several proofs, see van den Essen [E1] and Shannon and Sweedler [SS] for fields, Abhyankar and Li [AL] for arbitrary commutative rings R and Drensky, Gutierrez and Yu [DGY] in the general noncommutative setup.

Lemma 5.1. *Let $X = \{x_1, \dots, x_n\}$, $Y = \{y_1, \dots, y_n\}$ and let $\phi : K[X] \to K[Y]$ be a homomorphism such that $\phi(x_i) = f_i(Y) = f_i(y_1, \dots, y_n)$, $i = 1, \dots, n$. Extend ϕ to a homomorphism $\phi_0 : K[X, Y] \to K[Y]$ by $\phi_0(x_i) = \phi(x_i)$, $\phi_0(y_i) = y_i$, $i = 1, \dots, n$. Then the kernel of ϕ_0 is the ideal U of $K[X, Y]$*

$$\mathrm{Ker}(\phi_0) = U = (x_i - f_i(Y) \mid i = 1, \dots, n)$$

generated by all $x_i - f_i(Y)$ and $\mathrm{Ker}(\phi_0) \cap K[Y] = (0)$.

Proof. Obviously $\phi_0(x_i - f_i(Y)) = \phi(x_i) - f_i(Y) = f_i(Y) - f_i(Y) = 0$ and $x_i - f_i(Y) \in \mathrm{Ker}(\phi_0)$. Hence the ideal U generated by all $x_i - f_i(Y)$ is contained in $\mathrm{Ker}(\phi_0)$. Consider $t_i = x_i - f_i(Y)$, $i = 1, \dots, n$, and define an endomorphism $\rho : K[X, Y] \to K[X, Y]$ by $\rho(x_i) = t_i$, $\rho(y_i) = y_i$, $i = 1, \dots, n$. Obviously, ρ is a triangular automorphism of $K[X, Y]$, hence we may replace the algebra $K[X, Y]$ with $K[T, Y]$, where $T = \{t_1, \dots, t_n\}$. Clearly, $\phi_0(t_i) = \phi_0(x_i - f_i(Y)) = 0$, $\phi_0(y_i) = y_i$ and ϕ_0 is the homomorphism $K[T, Y] \to K[Y]$ which sends T to 0 and acts as the identity mapping on $K[Y]$. Hence the kernel of ϕ_0 is the ideal of $K[T, Y]$ generated by T and

$$\mathrm{Ker}(\phi_0) = (t_i \mid i = 1, \dots, n) = (x_i - f_i(Y) \mid i = 1, \dots, n)$$

and $\mathrm{Ker}(\phi_0) \cap K[Y] = (0)$.

Proposition 5.2. *Let $X = \{x_1, \dots, x_n\}$, $Y = \{y_1, \dots, y_n\}$ and let $\phi : K[X] \to K[Y]$, $\psi : K[Y] \to K[X]$ be homomorphisms such that*

$$\phi(x_i) = f_i(Y) = f_i(y_1, \dots, y_n),\ \psi(y_i) = g_i(X) = g_i(x_1, \dots, x_n),$$

$i = 1, \ldots, n$. *Extend* ϕ, ψ *to homomorphisms* $\phi_0 : K[X,Y] \to K[Y]$, $\psi_0 : K[X,Y] \to K[X]$ *by* $\phi_0(x_i) = \phi(x_i) = f_i(Y)$, $\phi_0(y_i) = y_i$, $\psi_0(x_i) = x_i$, $\psi_0(y_i) = \psi(y_i) = g_i(X)$, $i = 1, \ldots, n$. *Let the ideals* U *and* V *of* $K[X,Y]$ *be defined as*

$$U = (x_i - f_i(Y) \mid i = 1, \ldots, n),\ V = (y_i - g_i(X) \mid i = 1, \ldots, n).$$

Then ϕ *and* ψ *are isomorphisms and* $\psi = \phi^{-1}$ *if and only if the ideals* U *and* V *coincide.*

Proof. (i) Let ϕ, ψ be isomorphisms and $\psi = \phi^{-1}$. Hence

$$y_i = \phi(\psi(y_i)) = \phi(g_i(x_1, \ldots, x_n)) = g_i(\phi(x_1), \ldots, \phi(x_n)) = g_i(f_1(Y), \ldots, f_n(Y)),$$

$i = 1, \ldots, n$. Working modulo the ideal U of $K[X,Y]$, we have $x_i \equiv f_i(Y)$. Therefore

$$y_i = g_i(f_1(Y), \ldots, f_n(Y)) \equiv g_i(x_1, \ldots, x_n) \equiv g_i(X) \pmod{U},$$

and $y_i - g_i(X) \in U$ for all $i = 1, \ldots, n$. Since the polynomials $y_i - g_i(X)$ generate the ideal V, we obtain that $V \subseteq U$. Similarly, using that $x_i = \psi(\phi(x_i))$, we derive that $U \subseteq V$ and $U = V$.

(ii) Let $U = V$. Then the factor algebras $K[X,Y]/U$ and $K[X,Y]/V$ coincide and $x_i \equiv f_i(Y)$, $y_i \equiv g_i(X)$ modulo the ideal $U = V$. Hence

$$y_i \equiv g_i(x_1, \ldots, x_n) \equiv g_i(f_1(Y), \ldots, f_n(Y)) \equiv \phi \circ \psi(y_i) \pmod{U}$$

and $\phi \circ \psi$ is the identity mapping on $K[Y]$ modulo the ideal U. Similarly, $\psi \circ \phi$ is the identity mapping on $K[X]$ modulo the ideal V and for every $p(X) \in K[X]$ we have $\psi \circ \phi(p(X)) \equiv p(X) \pmod{V}$. The polynomial $\psi \circ \phi(x_i)$ belongs to $K[X]$ and is equal to x_i modulo the ideal V. Hence $\psi \circ \phi(x_i) - x_i \in V \cap K[X]$ and this intersection is equal to 0 by Lemma 5.1. Hence $x_i = \psi \circ \phi(x_i)$, $i = 1, \ldots, n$. Similarly, we obtain that $y_i = \phi \circ \psi(y_i)$, $i = 1, \ldots, n$, and the mappings ϕ and ψ are inverse to each other. Hence ϕ and ψ are isomorphisms and $\psi = \phi^{-1}$.

Theorem 5.3. *Let* $X = \{x_1, \ldots, x_n\}$ *and let* $\theta : K[X] \to K[X]$ *be an endomorphism of* $K[X]$ *defined by* $\theta(x_i) = f_i(X)$, $i = 1, \ldots, n$. *Then* θ *is an automorphism if and only if there exist polynomials* $g_i(X)$, $i = 1, \ldots, n$, *such that the ideals*

$$U = (x_i - f_i(Y) \mid i = 1, \ldots, n),\ V = (y_i - g_i(X) \mid i = 1, \ldots, n)$$

of $K[X,Y]$ *coincide. Then the inverse automorphism* $\rho = \theta^{-1}$ *is defined by* $\rho(x_i) = g_i(X)$, $i = 1, \ldots, n$.

Proof. The condition that θ is an automorphism is equivalent to the fact that the homomorphism $\phi : K[X] \to K[Y]$ defined by $\phi(x_i) = f_i(Y)$, $i = 1, \ldots, n$, is an isomorphism. Then the proof of the theorem follows immediately from Proposition 5.2.

Remark 5.4. By Theorem 5.3, if θ is an endomorphism of $K[X]$, and $\phi(x_i) = f_i(X)$, the problem to decide whether θ is an automorphism and, if "yes", to find its inverse, is reduced to the problem to decide whether the ideal U of $K[X,Y]$ generated by $x_i - f_i(Y)$, $i = 1, \ldots, n$, has a system of generators of the form $y_i - g_i(X)$, $i = 1, \ldots, n$. In the case of

polynomial algebras this problem can be solved effectively using Gröbner bases. For details we refer to some book on Gröbner bases, e.g. by Adams and Loustaunau [ALo] or Becker and Weispfenning [BW]. The idea is the following. First, let us consider the variables X larger than Y in the lexicographic ordering of $X \cup Y$. Then the leading monomial of the polynomial $x_i - f_i(Y)$ is equal to x_i and the generators $x_i - f_i(Y)$ of the ideal U form a Gröbner basis of U. Now, let us assume that the variables Y are higher than X in the lexicographic ordering of $X \cup Y$. Hence x_i is not more the leading monomial of $x_i - f_i(Y)$. If we calculate the Gröbner basis of U with respect to this new ordering, we shall obtain some new system of generators of U where the monomials containing y's are higher than those containing only x's. The monomial y_i is the smallest monomial (in the lexicographic ordering) which contains y_i. Hence, if θ is an automorphism, we shall obtain that some polynomials $y_i - g_i(X)$ belong to the new Gröbner basis. If θ is not an automorphism, then for some i there will be no polynomial of the form $y_i - g_i(X)$ in U and, of course, there will be no such polynomial in the Gröbner basis.

The second algorithm in our course is due to Shpilrain and Yu [SY] for polynomial algebras $K[x, y]$. It has a version which works for tame automorphisms of $(K[z])[x, y]$, see Drensky and Yu [DY2]. We follow the exposition of [DY2].

Lemma 5.5. *Let $d : K[x, y] \to \mathbf{Z}^2$ be the degree function on $K[x, y]$ induced by the lexicographic ordering $x > y$, i.e. $d(f(x, y)) = (a, b)$ if the leading term of $f \neq 0$ is $\alpha x^a y^b$, $\alpha \in K^*$. Let $a_1, \ldots, a_k$ be matrices in $GL_2(K)$ which do not belong to the lower triangular group and let*

$$c_i = (e_{11} + e_{22}) + f_i e_{21} = \begin{pmatrix} 1 & 0 \\ f_i & 1 \end{pmatrix}, \; i = 1, \ldots, k,$$

where $f_1, \ldots, f_k$ are polynomials of positive degree. Then the column-matrices

$$\begin{pmatrix} u_0 \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \; \begin{pmatrix} u_i \\ v_i \end{pmatrix} = c_i a_i \begin{pmatrix} u_{i-1} \\ v_{i-1} \end{pmatrix}, i = 1, \ldots, k,$$

satisfy the equation

$$d(v_i) = d(u_i) + d(f_i).$$

Proof. We apply induction on k. Let

$$a_i = \begin{pmatrix} \alpha_{1i} & \beta_{1i} \\ \alpha_{2i} & \beta_{2i} \end{pmatrix}, \; \beta_{1i} \neq 0, \; c_i = \begin{pmatrix} 1 & 0 \\ f_i & 1 \end{pmatrix}.$$

Concrete calculation shows that

$$\begin{pmatrix} u_1 \\ v_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ f_i & 1 \end{pmatrix} \begin{pmatrix} \alpha_{11} & \beta_{11} \\ \alpha_{21} & \beta_{21} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \beta_{11} \\ \beta_{11} f_1 + \beta_{21} \end{pmatrix}.$$

Since $\beta_{11} \neq 0$, we obtain that $d(u_1) = d(\beta_1) = (0, 0)$, $d(v_1) = d(f_1)$, and $d(v_1) = d(u_1) + d(f_1)$. We calculate

$$\begin{pmatrix} u_k \\ v_k \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ f_k & 1 \end{pmatrix} \begin{pmatrix} \alpha_{1k} & \beta_{1k} \\ \alpha_{2k} & \beta_{2k} \end{pmatrix} \begin{pmatrix} u_{k-1} \\ v_{k-1} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_{1k}u_{k-1} + \beta_{1k}v_{k-1} \\ f_k(\alpha_{1k}u_{k-1} + \beta_{1k}v_{k-1}) + (\alpha_{2k}u_{k-1} + \beta_{2k}v_{k-1}) \end{pmatrix}.$$

By induction, $d(v_{k-1}) = d(u_{k-1}) + d(f_{k-1}) > d(u_{k-1})$ and, since $\beta_{1k} \neq 0$,

$$d(u_k) = d(\alpha_{1k}u_{k-1} + \beta_{1k}v_{k-1}) = d(v_{k-1}),$$

$$d(v_k) = d(v_{k-1}) + d(f_k) = d(u_k) + d(f_k),$$

completing the inductive arguments.

Recall that the Euclidean algorithm for two polynomials $u(t)$ and $v(t)$ calculates the greatest common divisor of $u(t)$ and $v(t)$ and works as follows: Let, for example $\deg(u) \leq \deg(v)$. We divide $v(t) = u(t)q(t) + r(t)$, where either $\deg(r) < \deg(u)$ or $r(t) = 0$. If $r(t) = 0$, then the greatest common divisor of $u(t)$ and $v(t)$ is equal to $u(t)$. If $r(t) \neq 0$, then we replace $v(t)$ with $r(t)$ and perform the same calculations with $u(t)$ and $r(t)$. We can write this in a matrix form as

$$\begin{pmatrix} u(t) \\ r(t) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -q(t) & 1 \end{pmatrix} \begin{pmatrix} u(t) \\ v(t) \end{pmatrix}.$$

The case $\deg(u) > \deg(v)$ is similar. If $u(t) = v(t)q(t) + r(t)$, we write this in matrix form as

$$\begin{pmatrix} r(t) \\ v(t) \end{pmatrix} = \begin{pmatrix} 1 & -q(t) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u(t) \\ v(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -q(t) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u(t) \\ v(t) \end{pmatrix}.$$

In the case of polynomials in one variable over a field the Euclidean algorithm always gives the greatest common divisor. In the case of more variables it does not always work. We say that the greatest common divisor of two polynomials $u(x, y)$ and $v(x, y)$ can be obtained by the Euclidean algorithm if the leading monomial of one of the polynomials is divisible by the leading monomial of the other, we can perform the first step of the Euclidean algorithm and we can perform the further calculations until we obtain the greatest common divisor of $u(x, y)$ and $v(x, y)$.

Theorem 5.6. (Shpilrain and Yu [SY]) *Let $p(x, y) \in K[x, y]$. The following statements for $p(x, y)$ are equivalent:*

(i) *The polynomial $p(x, y)$ is a coordinate (i.e. an image of x under some automorphism of $K[x, y]$);*

(ii) *Applying the Euclidean algorithm to the partial derivatives p_x and p_y, the result is equal to* 1 *(or to a nonzero constant in K).*

Proof. We shall prove only the part which states that if the Euclidean algorithm applied to the partial derivatives p_x and p_y, gives a nonzero constant, then $p(x, y)$ is a coordinate. The proof of the other part uses: (i) the chain rule for the Jacobian matrices of a product of automorphisms; (ii) the theorem that every automorphism of $K[x, y]$ is tame and there is an algorithm which in each step composes the automorphism with an affine or with a triangular automorphism of the form $\tau(x) = x + h(y)$, $\tau(y) = y$ and the degrees of the images of x and y decrease; (iii) the fact that the Jacobian matrix of an affine automorphism is in $GL_2(K)$ and of a triangular automorphism of the form $\tau(x) = x+h(y)$,

$\tau(y) = y$ is a triangular matrix of the form $c = (e_{11} + e_{22}) + h'(y)e_{21}$. Now, let us assume that the application of the Euclidean algorithm to p_x and p_y gives a nonzero constant. In a matrix form this means that

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = b_1^{\delta} d_1 b_2 d_2 \dots b_k d_k b_{k+1}^{\varepsilon} \begin{pmatrix} p_x \\ p_y \end{pmatrix},$$

where the matrices b_i are linear, $d_i = d_i(x, y) = (e_{11} + e_{22}) + f_i(x, y)e_{21}$, $\delta, \varepsilon = 0, 1$. As in the description of the tame automorphisms in Section 3, we may assume that b_i does not belong to the lower triangular group and $\deg f_i > 1$ for $i = 1, \dots, k$. (The case when the column of the matrix is $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is similar.) We denote $g(x, y) = b_1^{\delta} d_1 b_2 d_2 \dots b_k d_k$, and assume that $\varepsilon = 1$, i.e.

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = g(x, y) \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} \begin{pmatrix} p_x \\ p_y \end{pmatrix},$$

In this equation we replace $x := \alpha_1 x + \alpha_2 y$, $y := \beta_1 x + \beta_2 y$ and obtain

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = g(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y) \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} \begin{pmatrix} p_x(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y) \\ p_y(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y) \end{pmatrix},$$

where $g_1(x, y) = g(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y)$ is a product of $b_i d_i(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y)$, i.e. of the same form as $g(x, y)$. Let $q(x, y) = p(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y)$. Then

$$q_x = \alpha_1 p_x(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y) + \alpha_2 p_y(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y),$$

$$q_y = \beta_1 p_x(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y) + \beta_2 p_y(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y),$$

and in a matrix form

$$\begin{pmatrix} q_x \\ q_y \end{pmatrix} = \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} \begin{pmatrix} p_x(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y) \\ p_y(\alpha_1 x + \alpha_2 y, \beta_1 x + \beta_2 y) \end{pmatrix}.$$

Hence

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = g_1(x, y) \begin{pmatrix} q_x \\ q_y \end{pmatrix}$$

and we may assume that $g(x, y) = b_1^{\delta} d_1(x, y) b_2 d_2(x, y) \dots b_k d_k(x, y)$ and

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = g(x, y) \begin{pmatrix} p_x \\ p_y \end{pmatrix},$$

where the last factor of $g(x, y)$ is $d_k(x, y)$ (and not b_{k+1}). In this way,

$$\begin{pmatrix} p_x \\ p_y \end{pmatrix} = g^{-1}(x, y) \begin{pmatrix} 0 \\ 1 \end{pmatrix} =$$

$$= (b_1^{\delta} d_1(x, y) b_2 d_2(x, y) \dots b_k d_k(x, y))^{-1} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = c_k a_k \dots c_1 a_1^{\delta} \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

where $a_i = b_i^{-1}$, $c_i = d_i^{-1}$. By Lemma 5.5, we obtain that the degrees of p_x, p_y and $f_k(x,y)$ satisfy $d(p_y) = d(p_x) + d(f_k)$. First, let $f_k(x,y)$ depend on x. Hence $d(f_k) = (a,b)$ and $a \geq 1$. Let $d(p_x) = (c,d)$. Then $d(p_y) = (a+c, b+d)$ and p_y contains as a leading monomial $\alpha x^{a+c}y^{b+d}$. Hence the leading monomial of $p_{yx} = (p_y)_x$ is $\alpha(a+c)x^{a+c-1}y^{b+d}$ (here we use that $a \geq 1$) and $d(p_{yx}) = (a+c-1, b+d)$. On the other hand, let the leading monomial of p_x be $\beta x^c y^d$. If it depends on y, then the leading monomial of $p_{xy} = (p_x)_y$ is $\beta d x^c y^{d-1}$ and $d(p_{xy}) = (c, d-1)$. Since $p_{xy} = p_{yx}$, we obtain that $(a+c-1, b+d) = (c, d-1)$ and for the second coordinate this is impossible, because all a, b, c, d are nonnegative integers. If the leading monomial of p_x does not depend on y, then the monomials of p_x containing y are below than βx^c in the lexicographic ordering, i.e. the leading monomial of $(p_x)_y$ is $\gamma x^e y^r$ for some $e \leq c-1$ and $d(p_{xy}) \leq (c-1, r)$. We obtain that $(a+c-1, b+d) \leq (c-1, r)$ and for the first coordinate this is impossible, because $a \geq 1$. The conclusion is that the polynomial f_k does not depend on x and $f_k = f_k(y)$. We have obtained that

$$d_k(x,y) = \begin{pmatrix} 1 & 0 \\ f_k(y) & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = b_1^{\delta} d_1 b_2 d_2 \dots b_k \begin{pmatrix} 1 & 0 \\ f_k(y) & 1 \end{pmatrix} \begin{pmatrix} p_x \\ p_y \end{pmatrix}.$$

In this equation we replace x by $x + g(y)$ where $g'(y) = f_k(y)$ (i.e. $g(y)$ is an integral of $f_k(y)$). It is easy to see, that

$$\begin{pmatrix} 1 & 0 \\ f_k(y) & 1 \end{pmatrix} \begin{pmatrix} p_x(x+g(y), y) \\ p_y(x+g(y), y) \end{pmatrix} = \begin{pmatrix} (p(x+g(y), y))_x \\ (p(x+g(y), y))_y \end{pmatrix} = \begin{pmatrix} q_x \\ q_y \end{pmatrix},$$

where $q(x,y) = p(x+g(y), y)$ and we obtain some shorter expression. The first change of the coordinates

$$x := \alpha_1 x + \alpha_2 y,\ y := \beta_1 x + \beta_2 y$$

corresponds to a linear automorphism. The second one

$$x := x + g(y),\ y := y$$

to a triangular automorphisms. Hence we have replaced the generators x, y of $K[x,y]$ with another system of generators. The shorter expression above means a smaller number of steps of application of the Euclidean algorithm. By inductive arguments, we obtain that q_x and q_y are the derivatives of the image $q(x,y)$ of x under the action of some automorphism of $K[x,y]$.

Remark 5.7. The above theorem gives an algorithm to recognize the coordinate polynomials in $K[x,y]$. The same algorithm allows to find whether $p(x,y)$ is an image of x under a tame automorphism of $R[x,y]$ for some commutative algebras R (see [DY2] for the case $R = K[z]$). In this form the algorithm does not allow to decide whether $f(x,y) \in R[x,y]$ is an image of x under the action of a nontame automorphism. Nevertheless, if the algebra R is good enough (see again [DY2] for $R = K[z]$) one can solve this problem in the following way. *The polynomial $p(x,y) \in (K[z])[x,y]$ is an image of x under some automorphism of $(K[z])[x,y]$ if it is a coordinate polynomial for $(K(z))[x,y]$ and the partial derivatives p_x, p_y generate $K[x,y,z]$ as an ideal.*

Exercises

1. Using the method of Theorem 5.3, find the inverse (i) of the Nagata automorphism of $K[x, y, z]$ and (ii) of the automorphism θ of $K[x, y]$ defined by

$$\theta(x) = (46x + 65y) + 4(12x + 17y)^2 + 8(2x + 3y)^3 + 16(12x + 17y)(2x + 3y)^3 + 16(2x + 3y)^6,$$

$$\theta(y) = (29x + 41y) + 2(12x + 17y)^2 + 5(2x + 3y)^3 + 8(12x + 17y)(2x + 3y)^3 + 8(2x + 3y)^6.$$

Solution. (i) We assume that $x_1 = x$, $x_2 = y$, $x_3 = z$, $y_1 = t$, $y_2 = u$, $y_3 = v$ and form the ideal U of $K[x, y, z, t, u, v]$ generated by

$$p_1 = x - (t - 2(u^2 + tv)u - (u^2 + tv)^2 v),\ p_2 = y - (u + (u^2 + tv)v),\ p_3 = z - v.$$

We assume that the variables are ordered $t > u > v > x > y > z$ and try to minimize the leading monomials of p_1, p_2, p_3, replacing one system of generators of U with another and maybe adding new generators. We mimique the algorithm for calculating of the Gröbner basis of an ideal.

Step 0. We replace $p_3 := -p_3$ and obtain $p_3 = v - z$.

Step 1. In p_1 and p_2 we replace v with $v + p_3 = z - (v - z) = z$. In this way, the new p_1, p_2, p_3 still generate U:

$$p_1 := x - t + 2(u^2 + tz)u + (u^2 + tz)^2 z,\ p_2 = y - u - (u^2 + tz)z,\ p_3 = v - z.$$

Step 2. We replace $p_1 := p_1 + (u_2 + tz)p_2$ in order to annihilate the summand $(u^2 + tz)^2 z$:

$$p_1 := x - t + (u^2 + tz)y + (u^2 + tz)u,\ p_2 = y - u - (u^2 + tz)z,\ p_3 = v - z.$$

Step 3. We add a new relation $p_4 := p_1 z + p_2 u$ because (following the theory of Gröbner bases) the leading summands tuz of p_1 and $-tz^2$ of p_2 have a common factor tz:

$$p_1 := x - t + (u^2 + tz)y + (u^2 + tz)u,\ p_2 = y - u - (u^2 + tz)z,\ p_3 = v - z,$$

$$p_4 := p_1 z + p_2 u = xz + yu - (u^2 + tz) + (u^2 + tz)yz.$$

Step 4. We replace $p_4 := p_4 + p_2 y$ in order to minimize the leading monomial of p_4:

$$p_4 := (xz + y^2) - (u^2 + tz).$$

Step 5. We minimize the leading monomials of p_1, p_2:

$$p_1 := p_1 + p_4 u = x - t + (u^2 + tz)y + (y^2 + xz)u,$$

$$p_1 := p_1 + p_4 y = x - t + (y^2 + xz)y + (y^2 + xz)u,$$

$$p_2 := p_2 - p_4 z = y - u - (y^2 + xz)z.$$

The result is

$$p_1 = x - t + 2(y^2 + xz)y + (y^2 + xz)u,\ p_2 = y - u - (y^2 + xz)z,$$

$$p_3 = v - z,\ p_4 = (xz + y^2) - (u^2 + tz).$$

Pay attention that $-p_2$ and p_3 are already in the desired form $y_i - g_i(X)$, as prescribed by Theorem 5.3.

Step 6. $p_1 := p_1 + p_2(y^2 + xz) = x + 2(y^2 + xz)y - (y^2 + xz)^2 z - t$ and $-p_1$ is also of the form we need.

Step 7. $p_1 := -p_1$, $p_2 := -p_2$:

$$p_1 = t - (x + 2(y^2 + xz)y - (y^2 + xz)u),\ p_2 = u - (y - (y^2 + xz)z),$$

$$p_3 = v - z,\ p_4 = (xz + y^2) - (u^2 + tz).$$

Step 8. We try to annihilate p_4 and replace it by $p_4 := p_4 + p_2^2 + p_1 z$. After some calculations we obtain that

$$p_4 = 2(y - (y^2 + xz)z)(-u + (y - (y^2 + xz)z)) = -2(y - (y^2 + xz)z)p_2.$$

Since p_4 is a multiple of p_2, we may remove it from the system. The ideal U is generated by

$$p_1 = t - (x + 2(y^2 + xz)y - (y^2 + xz)u),\ p_2 = u - (y - (y^2 + xz)z),\ p_3 = v - z,$$

which means that the inverse of the Nagata automorphism is defined by

$$x \to x + 2(y^2 + xz)y - (y^2 + xz)u,\ y \to y - (y^2 + xz)z,\ z \to z.$$

2. Prove that the following polynomial of $K[x, y]$ is an image of x under some automorphism:

$$p(x, y) = (46x+65y)+4(12x+17y)^2+8(2x+3y)^3+16(12x+17y)(2x+3y)^3+16(2x+3y)^6.$$

Solution. We calculate p_x and p_y and obtain

$$p_x = 46 + 96(12x + 17y) + 48(2x + 3y)^2 + 192(2x + 3y)^3$$

$$+96(12x + 17y)(2x + 3y)^2 + 192(2x + 3y)^5,$$

$$p_y = 65 + 136(12x + 17y) + 72(2x + 3y)^2 + 272(2x + 3y)^3$$

$$+144(12x + 17y)(2x + 3y)^2 + 288(2x + 3y)^5.$$

Applying the Euclidean algorithm, we obtain (the factor 2 is for convenience)

$$r = 2(3p_x/2 - p_y) = 8(1 + 2(12x + 17y) + 4(2x + 3y)^3),$$

and, replacing r with $r/8$, we obtain $r = 1 + 2(12x + 17y) + 4(2x + 3y)^3$. The next steps are

$$s = p_x - 48(2x + 3y)^2 r = 46 + 96(12x + 17y) + 192(2x + 3y)^3,$$

$$t = s - 48r = -2.$$

Hence we obtained that p_x and p_y are relatively prime by the Euclidean algorithm. Hence $p(x, y)$ is the image of x under some automorphism of $K[x, y]$.

3. Show that $p_1(x, y) = x - 2(y^2 + zx)y - (y^2 + zx)^2 z$ and $p_2(x, y) = y + (y^2 + zx)z$ are not images of x under a tame automorphism of $(K[z])[x, y]$.

Solution. Let $p = p_1$. Then

$$p_x = 1 - 2zy - 2(y^2 + zx)z,\ p_y = -2(y^2 + zx) - 4y^2 - 4zy(y^2 + zx),$$

$$p_x = -2z^2y^2 + \ldots,\ p_y = -4zy^3 + \ldots$$

and we cannot apply the Euclidean algorithm considering these polynomials as polynomials in x and y with coefficients which are polynomials in z. For the second polynomial $p = p_2$, we have

$$p_x = z^2,\ p_y = 1 + 2yz$$

and again we cannot apply the Euclidean algorithm.

On the other hand, the ideal of $(K[z])[x, y]$ generated by $p_x = z^2$ and $p_y = 1 + 2yz$ contains $p_y z - 2y p_x = z$, $p_y - 2yz = 1$ and coincides with $(K[z])[x, y]$. Working over $K(z)$, we obtain that $p_x = z^2$ is invertible in $K(z)$ and generates the whole $(K(z))[x, y]$ as an ideal. By the theorem mentioned in Remark 5.7, we obtain that p is an image of some (wild) automorphism of $(K[z])[x, y]$. This gives one more proof of the theorem of Nagata, that his automorphism is wild for $(K[z])[x, y]$.

References

[AL] S.S. Abhyankar, W. Li, On the Jacobian conjecture: A new approach via Gröbner Bases, J. Pure and Appl. Algebra **61** (1989), 211-222.

[ALo] W.W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Math. **3**, AMS, Providence, R.I., 1994.

[AM] M.F. Atiyah, I.G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass. 1969.

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

[DF] D. Daigle, G. Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension 5, J. Algebra **221** (1999), 528-535.

[DC] J.A. Diedonné, J.B. Carrell, Invariant Theory, Old and New, Academic Press, New York-London, 1971.

[D] V. Drensky, Free Algebras and PI-Algebras, Springer-Verlag, Singapore, 1999.

[DGY] V. Drensky, J. Gutierrez, J.-T. Yu, Gröbner bases and the Nagata automorphism, J. Pure Appl. Algebra **135** (1999), 135-153.

[DY1] V. Drensky, J.-T. Yu, Automorphisms and coordinates of polynomial algebras, in "Combinatorial and computational algebra (Hong Kong, 1999)", Contemp. Math., **264**, 179-206, Amer. Math. Soc., Providence, RI, 2000.

[DY2] V. Drensky, J.-T. Yu, Tame and wild coordinates of $K[z][x, y]$, Trans. Amer. Math. Soc. **353** (2001), 519-537.

[E1] A. van den Essen, A criterion to decide if a polynomial map is invertible and to compute the inverse, Commun. Algebra **18** (1990), 3183-3186.

[E2] A. van den Essen, Polynomial Automorphisms and the Jacobian Conjecture, Progress in Mathematics **190**, Birkhäuser, Base-Boston-Berlin, 2000.

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

[L] S. Leng, Algebra, Third Edition, Addison-Wesley, Reading, Mass. 1993.

[ML] L. Makar-Limanov, Automorphisms of polynomial rings – a shortcut, preprint.

[M] M. Miyanishi, Normal affine subalgebras of a polynomial ring, in "Algebraic and topological theories (Kinosaki, 1984), Papers from the symposium dedicated to the memory of Dr. Takehiko Miyata", 37-51, Kinokuniya, Tokyo, 1986.

[N] M. Nagata, On the Automorphism Group of $k[x, y]$, Lect. in Math., Kyoto Univ., Kinokuniya, Tokyo, 1972.

[No] A.Nowicki, Polynomial derivations and their rings of constants, Uniwersytet Mikolaja Kopernika, Toruń, 1994.

[R] R. Rentschler, Opérations du groupe additif sur le plan, C.R. Acad. Sci. Paris **267** (1968), 384-387.

[SS] D. Shannon, M. Sweedler, Using Groebner bases to determine Algebra menbership split surjective algebra homomorphisms determine birational equivalence, J. Symbolic Comput. **6** (1988), 267-273.

[SY] V. Shpilrain, J.-T. Yu, Polynomial automorphisms and Groebner reductions, J. Algebra **197** (1997), 546-558.

[S] M. K. Smith, Stably tame automorphisms, J. Pure Appl. Algebra **58** (1989), 209-212.
[Sp] T.A. Springer, Invariant Theory, Lect. Notes in Math. **585**, Springer-Verlag, Berlin-Hedelberg-New York, 1977.
[St] B. Sturmfels, Algorithms in Invariant Theory, Text and Monographs in Symb. Comput., Springer-Verlag, Vienna, 1993.
[V] W. van der Kulk, On polynomial rings in two variables, Nieuw Archief voor Wiskunde (3) **1** (1953), 33-41.

TOPICS IN ALGEBRA

FINAL EXAMINATION

(K is a field of characteristic 0):

I. Theoretical Question: Choose one of the following:

(i) **1. Prove the Hilbert Basis Theorem:** *If R is a noetheiran (commutative) algebra, then the algebra of polynomials $R[x]$ is also noetherian.*

(ii) **1. Prove the Molien Formula:** *If G is a finite subgroup of $GL_n(K)$, then the Hilbert series of the algebra of invariants $S = R^G = K[x_1, \ldots, x_n]^G$ has the form*

$$H(R^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - gt)},$$

where $\det(1 - gt)$ *is the determinant of the matrix* $1 - gt$.

(iii) **1. Prove the Theorem of Martha Smith:** *Let δ be a triangular derivation of $K[x_1, \ldots, x_n]$ and let $w \in \mathrm{Ker}(\delta)$. Then the automorphism* $\exp(w\delta)$ *is stably tame and becomes tame extended to $K[x_1, \ldots, x_{n+1}]$ by* $\exp(w\delta) : x_{n+1} \to x_{n+1}$.

II. Problems: Choose one or two of the following:

1. Calculate the Hilbert series of $R = K[x, y]/(x^2 - y^2)$;

2. Find the generators of the algebra of invariants $K[x, y]^G$ of the group G generated by g and h, where

$$g(x) = -x,\ g(y) = y,\ h(x) = x,\ h(y) = -y.$$

3. Find the generators of the algebra of invariants $K[x, y, z]^G$ of the cyclic group G of order 3 acting on $K[x, y, z]$ and generated by

$$g = \begin{pmatrix} x & y & z \\ y & z & x \end{pmatrix}.$$

4. Show that the the following derivation of $K[u, v, x, y, z]$ is locally nilpotent and the polynomials w_1, w_2 belong to its kernel:

$$\delta = 2u(vy - uz)\frac{\partial}{\partial x} - 2v(vy - uz)\frac{\partial}{\partial y} + (v^2x - u^2y)\frac{\partial}{\partial z},\ w_1 = xy - z^2,\ w_2 = v^2x + u^2y - 2uvz.$$

5. Find the product $\phi^{-1} \circ \psi^{-1} \circ \tau \circ \sigma$, where $\phi, \psi, \sigma, \tau \in \mathrm{Aut}K[x, y]$ are defined by

$$\sigma(x) = 2x + y + 1,\ \sigma(y) = x + y - 1,$$

$$\tau(x) = x + 2y^2,\ \tau(y) = y,$$

$$\psi(x) = x + 2y + 1,\ \psi(y) = x + 3y + 2,$$

$$\phi(x) = x + 1,\ \phi(y) = y + x^2,$$

and, by definition, $\alpha \circ \beta(u) = \alpha(\beta(u))$, for any mappings α, β.

Suggested combinations: I (i) and II 2, 4; I (ii) and II 1, 5; I (iiii) and II 3.