HONG KONG – 2005

TOPICS IN ALGEBRA

POLYNOMIAL ALGEBRAS AND THEIR AUTOMORPHISMS

Vesselin Drensky
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
Sofia, Bulgaria
and
Department of Mathematics, University of Hong Kong
Hong Kong

Jie-Tai Yu
Department of Mathematics, University of Hong Kong
Hong Kong

Table of Contents

1. POLYNOMIAL ALGEBRAS AND THEIR IDEALS

Basic Definitions

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 R is a ring with $1 = 1_R$ with respect to the addition and the multiplication, and for any $a, b \in R$ and any constant $\alpha \in K$

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

In other words, the notion of algebra generalizes the both notions 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.

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

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

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 J of R is called an *ideal* if for every $u \in J$ and every $a \in R$ the products ua and au belong to J (we denote this property by $RJ \subseteq J$ and $JR \subseteq J$). The ideal J is generated by the set of its elements $U = \{u_1, u_2, \ldots\}$, the notation is $J = (U)$, if every element $u \in J$ is of the form

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

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

The notion of factor algebra R/J of the algebra R modulo the ideal J 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 R/J are the classes $a + J = \{a + u \mid u \in J\}$ and the operations are defined by

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

The notions of homomorphism and isomorphism are also similar to the corresponding notions for rings. (If $\varphi : R \to S$ is a homomorphism of algebras, we require that $\varphi(1_R) = 1_S$ and $\varphi(\alpha a) = \alpha\varphi(a)$ for all $\alpha \in K$ and $a \in R$.) In particular, the homomorphisms $R \to R$ are called *endomorphisms* and the isomorphisms $R \to R$ are *automorphisms*.

In the most of our further considerations we shall consider commutative algebras only.

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. If $J = (f(x))$ is the principal ideal of $K[x]$ generated by the polynomial

$$f(x) = x^k + \alpha_1 x^{k-1} + \cdots + \alpha_{k-1} x + \alpha_k, \quad \alpha_i \in K,$$

then the factor algebra $K[x]/J$ has a basis consisting of

$$1 + J, x + J, \ldots, x^{k-1} + J.$$

For the algebra of polynomials in more than one variable such results are 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. Also, even for easy examples of ideals it is not obvious which monomials form a basis of the factor algebra. Below we shall present a technique which allows to solve such kind of problems.

Orderings of Monomials and Hilbert Basis Theorem

We fix the finite set of (commuting) variables $X = \{x_1, \ldots, x_n\}$. We denote

$$[X] = \{x_1^{a_1} \cdots x_n^{a_n} \mid a_i \geq 0\}$$

the set of all monomials equipped with the operation of the usual multiplication, i.e.

$$(x_1^{a_1}\cdots x_n^{a_n})\cdot(x_1^{b_1}\cdots x_n^{b_n}) = x_1^{a_1+b_1}\cdots x_n^{a_n+b_n}.$$

The set $[X]$ is called the *free unitary commutative semigroup* and X is the set of *free generators* of $[X]$. For two monomials $u, v \in [X]$, we say that u divides v if there exists $w \in [X]$ such that $v = uw$. The nonempty subset I of $[X]$ is called an *ideal* of $[X]$ if for every $u \in I$ and every $v \in [X]$ we have $uv \in I$. The ideal I is generated by the set $S = \{u_1, u_2, \ldots\}$ if it consists of all elements of $[X]$ divisible by some $u \in S$, and denote this with $I = (S)$.

Theorem 1.4. *Every ideal of* $[X]$ *is finitely generated.*

Proof. We use induction on the number of variables n in the set $X = X_n$. For $n = 1$ the set $[X_1]$ consists of all powers x_1^k of x_1. For an ideal I of $[X_1]$, we choose the element x_1^a of minimal degree in I. Since $x_1^b \cdot x_1^a$ also belongs to I, we derive that $I = \{x_1^c \mid c \geq a\}$ and $I = (x_1^a)$.

Now, by induction, let every ideal of $[X_n]$ be finitely generated. We consider an ideal I of $[X_{n+1}]$. Let, for $k \geq 0$,

$$J_k = \{x_1^{a_1}\cdots x_n^{a_n} \in [X_n] \mid x_1^{a_1}\cdots x_n^{a_n}x_{n+1}^k \in I\}$$

be the set of all monomials in n variables which are "coefficients" of the monomials in I of degree k with respect to x_{n+1}. If $x_1^{a_1}\cdots x_n^{a_n} \in J_k$, then $x_1^{a_1}\cdots x_n^{a_n}x_{n+1}^k \in I$, and

$$(x_1^{b_1}\cdots x_n^{b_n})(x_1^{a_1}\cdots x_n^{a_n}x_{n+1}^k) = x_1^{a_1+b_1}\cdots x_n^{a_n+b_n}x_{n+1}^k \in I.$$

Hence $(x_1^{b_1}\cdots x_n^{b_n})(x_1^{a_1}\cdots x_n^{a_n}) \in J_k$ and J_k is an ideal of $[X_n]$ (of course, if J_k is not empty). Similarly,

$$(x_1^{a_1}\cdots x_n^{a_n}x_{n+1}^k)x_{n+1} = (x_1^{a_1}\cdots x_n^{a_n})x_{n+1}^{k+1} \in I.$$

Hence $x_1^{a_1}\cdots x_n^{a_n} \in J_{k+1}$ and this means that $J_k \subseteq J_{k+1}$. In this way, we obtain an ascending chain of ideals of $[X_n]$,

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots.$$

Since the union of any ascending chain of ideals of $[X_n]$ is an ideal again, we obtain that $J = \cup_{k\geq 0} J_k$ is an ideal of $[X_n]$. By induction, J is generated by a finite set of monomials, say $S = \{u_1, \ldots, u_p\}$. Since $J_k \subseteq J_{k+1}$ for all $k \geq 0$, there exists an m such that all $u_1, \ldots, u_p$ are in J_m. Since the set S is a subset of the ideal J_m and generates the bigger ideal J, we derive that S generates also J_m. Hence $J_m = J_{m+1} = \cdots = J$. Now, for each $k = 0, 1, \ldots, m-1$, we choose a generating set $S_k = \{u_{k1}, \ldots, u_{kp_k}\}$ of J_k.

We claim that the set

$$T = \{u_{ki_k}x_{n+1}^k, u_j x_{n+1}^m \mid i_k = 1, \ldots, p_k,\ k = 0, 1, \ldots, m-1,\ j = 1, \ldots, p\}$$

generates the ideal I. First of all, since u_{ki_k} belongs to I_k, by the definition of J_k, we obtain that $u_{ki_k}x_{n+1}^k$ belongs to I; and similarly $u_j x_{n+1}^m \in I$. Hence $T \subset I$. An arbitrary element of I has the form ux_{n+1}^k, where $u = x_1^{a_1}\cdots x_n^{a_n} \in [X_n]$. Then $u \in J_k$. If $k < m$, then the ideal J_k of X_n is generated by the set S_k and hence $u = u_{ki}v$ for some $u_{ki} \in S_k$ and some $v = x_1^{b_1}\cdots x_n^{b_n} \in [X_n] \subset [X_{n+1}]$. Since $u_{ki}x_{n+1}^k \in T$, we obtain that $(u_{ki}x_{n+1}^k)\cdot v = (u_{ki}v)x_{n+1}^k = ux_{n+1}^k$ belongs to the ideal of $[X_{n+1}]$ generated by T. If $k \geq m$, then $u \in J_m = J$ and $u = u_i v$ for some $u_i \in S$ and some $v \in [X_n]$. Again, $u_i x_{n+1}^m \in T$ and $(u_i x_{n+1}^m)\cdot(vx_{n+1}^{k-m}) = ux_{n+1}^k$ belongs to the ideal generated by T. Hence, any element of I belongs to the ideal of $[X_{n+1}]$ generated by T and T is the generating set of I.

Definition 1.5. We say that the binary relation $\prec$ of the set $[X]$ of monomials in n variables is an *admissible order* on $[X]$, if

(i) If u, v are two different monomials in $[X]$, then either $u \prec v$ or $v \prec u$ (*total order*);
(ii) There exists no infinite sequence of monomials such that $u_1 \succ u_2 \succ \cdots$ (*descending chain condition* or *well-ordering*);
(iii) If $u = x_1^{a_1}\cdots x_n^{a_n}$ is different from 1, then $1 \prec u$;
(iv) If $u, v, w \in [X]$ and $u \prec v$, then $uw \prec vw$.

Examples 1.6. (i) The *lexicographical order* on $[X]$ is defined with $x_1 \succ \cdots \succ x_n$ and then extended to $[X]$ by

$$x_1^{a_1}\cdots x_n^{a_n} \prec x_1^{b_1}\cdots x_n^{b_n}$$

if and only if $a_1 = b_1, \ldots, a_k = b_k$ for some $k < n$ and $a_{k+1} < b_{k+1}$.

(ii) In the *degree lexicographical order* (*Deg-Lex*) we say that

$$u = x_1^{a_1}\cdots x_n^{a_n} \prec x_1^{b_1}\cdots x_n^{b_n} = v$$

if

$$a_1 + \cdots + a_n = \deg(u) < \deg(v) = b_1 + \cdots + b_n,$$

or, if $\deg(u) = \deg(v)$, then $u \prec v$ in the usual lexicographical order.

Exercise 1.7. If $u, v \in [X]$, $u \neq v$, and u divides v, then $u \prec v$ for any admissible order on $[X]$.

Solution. If $v = uw$ for some $w \in [X]$, then $1 \prec w$ and $u \prec uw = v$.

Definition 1.8. Let us fix some admissible order on $[X]$. If $f(X) \in K[X]$ is a nonzero polynomial, it is written in the form

$$f(X) = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_k u_k, \quad 0 \neq \alpha_i \in K, \quad u_i \in [X],$$

where $u_1 \succ u_2 \succ \cdots \succ u_k$. The monomial u_1 is called the *leading monomial* of f. We shall denote it by $\bar{f} = \mathrm{lm}(f)$.

From now on, we shall always assume that $[X]$ is equipped with some fixed admissible order.

Exercise 1.9. If $0 \neq f(X), g(X) \in K[X]$, then $\overline{fg} = \bar{f}\bar{g}$.

Hint. If $\bar{f} = u_1$ and $\bar{g} = v_1$, then $f = \sum_{i=1}^{k} \alpha_i u_i$ and $g = \sum_{j=1}^{l} \beta_j v_j$ for some $0 \neq \alpha_i, \beta_j \in K$, $u_i, v_j \in [X]$, and $u_1 \succ u_i$, $v_1 \succ v_j$ for all $i, j > 1$. Derive from here that $u_1 v_1 \succ u_1 v_j, u_i v_1, u_i v_j$ if $i, j > 1$.

Hilbert Basis Theorem 1.10. *Every ideal of $K[X]$ is finitely generated.*

(Usually the Hilbert Basis Theorem, or the Hilbert Basissatz, is stated in a stronger form, namely: If R is a noetheiran commutative ring (or algebra), then the ring (or algebra) of polynomials $R[x]$ is also noetherian.)

Proof. Let J be an ideal of $K[X]$. If $J = \{0\}$, then it is generated by 0. So, we may assume that J contains also nonzero polynomials. Let $I = \bar{J}$ be the set of all leading monomials of the nonzero elements of J (with respect to some admissible order). If $u \in I$, then there exists an $f \in J$ such that $u = \bar{f}$. Hence $fv \in J$ for any monomial $v \in [X]$ and, since $\overline{fv} = \bar{f}\bar{v} = uv$, this implies that $uv \in I$. Hence I is an ideal of $[X]$. By Theorem 1.4, I is generated by some finite set $u_1, \ldots, u_k$. Let $f_1, \ldots, f_k \in J$ be polynomials with leading monomials $u_1, \ldots, u_k$, respectively. Let $f_i = \alpha_i u_i + \cdots$, where $0 \neq \alpha_i \in K$ and $\cdots$ states for the linear combinations of the monomials in f_i which are lower than u_i. We shall show that J is generated by $f_1, \ldots, f_k$. Let $g = g_1$ be any nonzero polynomial in J, $g_1 = \beta_1 v_1 + \cdots + \beta_p v_p$, where $0 \neq \beta_j \in K$ and $\overline{g_1} = v_1$. Since $v_1 \in I$ and I is generated by $u_1, \ldots, u_k$, there exists an i and $w \in [X]$ such that $v_1 = w u_i$. Since $g_1, f_i \in J$, we obtain that $g_2 = g_1 - (\beta_1/\alpha_i) f_i w$ also belongs to J. Clearly,

$$g_2 = (\beta_1 v_1 + \cdots + \beta_p v_p) - \frac{\beta_1}{\alpha_i} w(\alpha_i u_i + \cdots) = \sum_{j=2}^{l} \beta_j v_j - \frac{\beta_1}{\alpha_i} w(\cdots),$$

and, if $g_2 \neq 0$, then $\overline{g_2} \prec \overline{g_1}$. In this way we obtain a sequence of polynomials $g_1, g_2, \ldots \in J$ such that $\overline{g_1} \succ \overline{g_2} \succ \overline{g_3} \succ \cdots$. The descending chain condition gives that such infinite sequences do not exist. Hence $g_s = 0$ for some s and we obtain that g has the form $g = \gamma_1 w_1 f_{i_1} + \gamma_1 w_2 f_{i_2} + \cdots + \gamma_s w_s f_{i_s}$ for some $\gamma_j \in K$ and some monomials w_j. This means that g belongs to the ideal generated by $f_1, \ldots, f_k$ and J is finitely generated.

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

Proposition 1.11. *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 $\varphi : K[x_1, \ldots, x_n] \to R$ by

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

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 $\mathrm{Im}(\varphi)$

of φ is isomorphic to the factor algebra $K[x_1,\dots,x_n]/\mathrm{Ker}(\varphi)$ of $K[x_1,\dots,x_n]$ modulo the kernel $\mathrm{Ker}(\varphi)$. Hence $R \cong K[x_1,\dots,x_n]/\mathrm{Ker}(\varphi)$.

Definition 1.12. If the algebra R is isomorphic to $K[x_1,\dots,x_n]/J$ for some ideal J generated by the set of polynomials $\{u_i(x_1,\dots,x_n) \mid i = 1,2,\dots\}$, then we say that $\{u_i(x_1,\dots,x_n) = 0 \mid i = 1,2,\dots\}$ is a set of *defining relations* of the algebra R and write this as

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

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

Corollary 1.13. *Every finitely generated commutative algebra is finitely presented.*

The proof follows immediately from Proposition 1.11 and the Hilbert Basis Theorem.

Exercise 1.14. Prove that every finitely generated commutative algebra R is noetherian, i.e. every ideal of R is finitely generated.

Hint. Use Proposition 1.11. If $\varphi : K[X] \to R$ is an epimorphism (i.e. $\varphi(K[X]) = R$), then there is a 1-1 correspondence between the ideals I of R and the ideals of $J = \varphi^{-1}(I)$ of $K[X]$ containing the kernel of φ, and $\varphi(J) = I$. Then J is finitely generated and so is the ideal I.

Gröbner Bases

We still fix some admissible order on $[X]$ and denote by $\bar{f}$ the leading monomial of $f \in K[X]$.

Definition 1.15. Let G be a subset of $K[X]$ and let $\bar{G}$ be the set of leading monomials of the nonzero elements in G. We call a monomial $u \in [X]$ *normal* (with respect to G) if it is not divisible by any monomial from $\bar{G}$. (This means that $[X]$ is a disjoint union of the ideal generated by $\bar{G}$ and the set of normal monomials.)

Lemma 1.16. *If J is an ideal of $K[X]$, then the set of normal monomials with respect to J forms a basis of the factor algebra of $K[X]$ modulo J.*

Proof. Let $\bar{J}$ be the ideal of $[X]$ consisting of the leading monomials of the nonzero elements of J (we already proved that $\bar{J}$ is an ideal of $[X]$). Let N be the set of normal monomials (i.e. $[X] = \bar{J} \cup N$ and $\bar{J} \cap N = \emptyset$). Let

$$h = \alpha_1 u_1 + \dots + \alpha_k u_k \in K[X], \quad \alpha_i \in K, \quad u_i \in [X], \quad u_1 \succ \dots \succ u_k.$$

If $u_i \in \bar{J}$, then there exists an $f_i \in J$ such that $f_i = \beta_i u_i + \cdots$ ($\cdots$ is for the monomials which are lower than u_i). Then $h - (\alpha_i/\beta_i) f_i \equiv h \pmod{J}$ and

$$h - (\alpha_i/\beta_i) f_i = \alpha_1 u_1 + \dots + \alpha_{i-1} u_{i-1} + \cdots,$$

where the right $\cdots$ above is a linear combination of monomials which are lower than u_i. Continuing in this way, we shall express h modulo J as a linear combination of normal monomials. If we assume that the normal monomials are linearly dependent modulo J,

then, for some normal monomials $v_1 \succ \cdots \succ v_m$ and some constants γ_i, the polynomial $h = \gamma_1 v_1 + \cdots + \gamma_m v_m$ belongs to J. Hence $\bar{h} = v_1$ belongs to $\bar{J}$, which is a contradiction. Therefore the normal monomials are linearly independent modulo J and form a basis of the factor algebra $K[X]/J$ modulo J.

Examples 1.17. (i) Let J be the ideal of $K[x]$ generated by the polynomial $f(x)$ of degree k. Then the set $\bar{J}$ consists of all monomials divisible by x^k and the set of normal monomials consists of $1, x, \ldots, x^{k-1}$.

(ii) Let $G = \{x^2, xy^2, y^3\} \subset K[x, y]$. Since G consists of monomials, we have $\bar{G} = G$. Then the ideal $(\bar{G})$ of $[x, y]$ generated by $\bar{G}$ consists of all monomials divisible by some of x^2, xy^2, y^3. Hence the set of normal monomials with respect to G is $N = \{1, x, y, xy, y^2\}$. The ideal (G) of $K[x, y]$ is spanned by $(\bar{G}) \subset [x, y]$ and the factor algebra $K[x, y]/(G)$ has a basis N.

(iii) Let $G = \{g_1, g_2, g_3\} \subset K[x, y]$, with the lexicographical order $(x \succ y)$, where

$$g_1 = x^2 + y^3, \quad g_2 = xy + y^2, \quad g_3 = x^3 + 2y^3.$$

Then $\bar{G} = \{x^2, xy, x^3\}$ and the set of normal monomials with respect to G consists of $1, x, y^i$, $i = 1, 2, \ldots$. On the other hand, if J is the ideal of $K[x, y]$ generated by G, then

$$f_1 = g_3 - xg_1 = -xy^3 + 2y^3 \in J, \overline{f_1} = xy^3, \quad f_2 = f_1 + y^2 g_2 = y^4 + 2y^3 \in J, \overline{f_2} = y^4,$$

and $\bar{J}$ contains the monomial y^4 which is normal with respect to G.

Hence, if we know the generators of the ideal of $K[X]$, we cannot say immediately, which are the normal monomials with repsect to this ideal, and to find a basis of the factor algebra.

Definition 1.18. Let G be a subset of the ideal J of $K[X]$. We say that G is a *Gröbner basis* of J (with respect to the fixed admissible order), if G and J have the same sets of normal monomials, i.e. if $\bar{G}$ generates the ideal $\bar{J}$ of $[X]$. The name *Gröbner* has also another spelling *Groebner*.

Exercise 1.19. If G is a Gröbner basis of the ideal J of $K[X]$, then G generates J.

Hint. Use the arguments of the proof of the Hilbert Basis Theorem and show that if $G \subset J$ and $\bar{G}$ generates $\bar{J}$, then G generates J.

Definition 1.20. The Gröbner basis G of the ideal J of $K[X]$ is *minimal*, if it is minimal with respect to the inclusion, i.e. no proper subset of G is a Gröbner basis of J. The Gröbner basis G of J is *reduced*, if the leading monomials of G are not divisible by each other and every polynomial $g \in G$ has the form $g = \alpha\bar{g} + \sum \beta_i u_i$, where $0 \neq \alpha, \beta_i \in K$ and all u_i are normal monomials with respect to $G \setminus \{g\}$. (It is easy to see that every reduced Gröbner basis is minimal.)

Theorem 1.21. Let us fix and admissible order on $[X]$.

(i) *Minimal Gröbner bases always exist and are finite.*

(ii) *The reduced Gröbner basis always exists and is unique, up to scalar multiples of its elements.*

Proof. (i) Let $\bar{J}$ be the ideal of $[X]$ consisting of the leading monomials of the nonzero ideal J of $K[X]$. Then $\bar{J}$ is finitely generated. Let us choose a minimal set of generators $V = \{v_1, \dots, v_k\}$ of $\bar{J}$. If $G = \{g_1, \dots, g_k\} \subset J$ is such that $\overline{g_i} = v_i$, then, clearly, G is a Gröbner basis of J. It is minimal because we need all elements of V to produce the leading monomials of J.

(ii) Starting with any finite Gröbner basis $G = \{g_1, \dots, g_m\}$ of J, we write the elements $g_i \in G$ in the form

$$g_i = \alpha_i u_i + \sum_{j=1}^{k_i} \beta_{ij} v_{ij}, \quad 0 \neq \alpha_i, \beta_{ij} \in K, \quad u_i \succ v_{i1} \succ \cdots \succ v_{ik_i}.$$

If for some i, j, say $i = 1$, $j = 2$, one of the leading monomials u_2 divides the other one u_1, then $u_1 = wu_2$ for some $w \in [X]$. The polynomial

$$g_1' = g_1 - \frac{\alpha_1}{\alpha_2} w g_2$$

belongs to the ideal J. It is easy to see that G and $G' = \{g_1', g_2, \dots, g_m\}$ are Gröbner bases for the same ideal J. The difference is that the leading monomial of g_1' is lower than this of g_1. (This is if $g_1' \neq 0$. If $g_1' = 0$, we remove it from G'.) Hence G' looks out simpler that G. Similarly, if some monomial v_{1j} in the expression of g_1 is divisible by u_2, then we can repeat the above arguments and to replace v_{1j} with something which is lower. In a finite number of steps, we obtain a Gröbner basis G'' of J with the property that the monomials of the expressions of the $g_i'' \in G''$ are not divisible by the leading monomials of the other polynomials in G''. Hence G'' is a reduced Gröbner basis of J and the reduced Gröbner basis always exists.

We have to show that the reduced Gröbner basis is unique. Let G_1 and G_2 be two reduced Gröbner bases of the ideal J. Hence $\overline{G_1}$ and $\overline{G_2}$ are minimal sets of generators of the ideal $\bar{J}$. It is easy to see that $\overline{G_1}$ and $\overline{G_2}$ conicide: If $\overline{G_1} = \{v_1, \dots, v_k\}$, $\overline{G_2} = \{w_1, \dots, w_l\}$ are different, then, since there are generating sets of $\bar{J}$, w_1 is divisible by some v_i, e.g. by v_1. Therefore, if $v_1 \neq w_1$, then v_1 is divisible by some w_j, and we obtain that w_j divides w_1. This contradicts with the minimality of $\overline{G_2}$. Hence $v_1 = w_1$ and, after a finite number of steps, we obtain that $\overline{G_1} = \overline{G_2}$. This means that the polynomials of G_1 and G_2 can be rearranged in a way, say $G_1 = \{p_1, \dots, p_k\}$, $G_2 = \{q_1, \dots, q_k\}$, such that $\overline{p_i} = \overline{q_i}$. Let $p_1 \neq q_1$. Then, since p_1 and q_1 have the same leading monomials, there exists a constant $\alpha \in K$, such that $p_1 - \alpha q_1 = \sum \gamma_j w_j$, where $\gamma_j \in K$ and the monomials w_j are lower than $\overline{p_1}$. Clearly, $p_1 - \alpha q_1 \in J$. The facts that G_1, G_2 are reduced Gröbner bases, $\overline{G_1} = \overline{G_2}$, and $\overline{p_1} \succ \overline{p_1 - \alpha q_1}$, give that the monomials of $p_1 - \alpha q_1$ are not divisible by any of the monomials from $\overline{G_1}$. If $p_1 - \alpha q_1 \neq 0$, this is impossible. Hence p_1, q_1 are equal, up to a multiplicative constant, and the reduced Gröbner basis of J is unique.

Now we present the algorithm of Buchberger for computing of Gröbner bases of ideals of $K[X]$. Of course, *when we consider algorithms, we assume that the base field K is constructive. This means that we are able to perform calculations in K.*

Algorithm of Buchberger 1.22. Let the ideal J of $K[X]$ be generated by the set $G = \{g_1, \dots, g_k\}$ of nonzero polynomials and let $\bar{G} = \{u_1, \dots, u_k\}$, where $\overline{g_i} = u_i$.

Multiplying by constants, we may assume that $g_i = u_i + \cdots$, i.e. the leading coefficient of g_i is equal to 1.

Step 1. If u_i divides u_j, and $u_j = u_i v$ for some $v \in [X]$, then we replace $g_j := g_j - g_i v$. Then we make the leading coefficient of g_j equal to 1. If the new g_j is equal to 0, then we remove it from G. This operation is called *reduction*. We continue the reductions, until possible.

Step 2. Let $u_i = \overline{g_i}$ and $u_j = \overline{g_j}$ have a nontrivial common divisor, i.e. $u_i = v_i w$, $u_j = v_j w$ for some $w \in [X]$, $w \neq 1$. Since there are no possibilities for reductions between the leading monomials of G, $v_i, v_j \neq 1$. We consider the polynomial $g = g_i v_j - g_j v_i$ which also belongs to J. We have $\overline{g_i v_j} = u_i v_j = v_i w v_j = \overline{g_j v_i}$. This operation is called *composition*. We add g to G and go to Step 1.

If there are no more possible reductions and compositions between the polynomials in G, we stop the process. The obtained set G is a Gröbner basis of J. If we additionally make all possible reductions also between the leading monomials of $g_i \in G$ and all the monomials in the expressions of the other $g_j \in G$, then, as in the proof of Theorem 1.21, we obtain the reduced Gröbner basis of J.

Example 1.23. (This is Example 1.17 (iii).) Let $G = \{g_1, g_2, g_3\} \subset K[x, y]$, with the lexicographical order $(x \succ y)$, where

$$g_1 = x^2 + y^3, \quad g_2 = xy + y^2, \quad g_3 = x^3 + 2y^3.$$

Find the Gröbner basis of the ideal generated by G.

Solution. We apply the Buchberger algorithm. We start with reductions. Since $\overline{g_1} = x^2$ divides $\overline{g_3} = x^3$, we replace

$$g_3 := g_3 - x g_1 = -xy^3 + 2y^3, \quad g_3 := -g_3 = xy^3 - 2y^3.$$

Again, $\overline{g_2} = xy$ divides $\overline{g_3} = xy^3$ and the next reduction is

$$g_3 := g_3 - y^2 g_2 = -y^4 - 2y^3, \quad g_3 := -g_3 = y^4 + 2y^3.$$

Now the set $G = \{g_1, g_2, g_3\}$ becomes

$$g_1 = x^2 + y^3, \quad g_2 = xy + y^2, \quad g_3 = y^4 + 2y^3.$$

No further reductions are possible and we start with the compositions. For example, x divides

$$\overline{g_2} = xy, \quad \overline{g_3} = y^4,$$

and $\overline{g_2} y^3 = \overline{g_3} x$. We construct the polynomial $g_4 := g_2 y^3 - g_3 x$ and continue with the reductions:

$$g_4 = -2xy^3 + y^5, \quad g_4 := g_4 + 2g_2 y^2 = y^5 + 2y^4, \quad g_4 := g_4 - y g_3 = 0.$$

Hence we remove g_4 from the set G. We have one possible composition, because $\overline{g_1}$ and $\overline{g_2}$ are divisible by x. The equality $\overline{g_1} y = \overline{g_2} x$ suggests the composition, with further reductions

$$g_4 := g_1 y - g_2 x = -xy^2 + y^4, \quad g_4 := g_4 + g_2 y = y^4 + y^3,$$

$$g_4 := g_4 - g_3 = -y^3, g_4 := -g_4 = y^3,$$

$$g_3 := g_3 - g_4 y = y_3, \quad g_3 := g_3 - g_4 = 0.$$

Hence we remove g_3 and obtain the set $G = \{g_1, g_2, g_4\}$, where

$$g_1 = x^2 + y^3, \quad g_2 = xy + y^2, \quad g_4 = y^3.$$

We have one more composition, but after the possible reductions we do not obtain anything new:

$$g_5 := g_2 y^2 - g_4 x = y^4, \quad g_5 := g_5 - g_4 y = 0.$$

(We already had the composition between g_1, g_2.) Hence the Buchberger algorithm stops and the Gröbner basis of the ideal generated by G consists of

$$g_1 = x^2 + y^3, \quad g_2 = xy + y^2, \quad g_4 = y^3.$$

If we want to obtain the reduced Gröbner basis, we have to replace g_1 with $g_1 - g_4 = x^2$ and obtain

$$g_1 = x^2, \quad g_2 = xy + y^2, \quad g_4 = y^3.$$

We derive from here, that the set of normal monomials is $\{1, x, y, y^2\}$ and this is the basis of the factor algebra $K[x, y]/(G)$.

Example 1.24. How many solutions has the system

$$x^2 + x = yz$$

$$y^2 + y = xz$$

$$z^2 + z = xy$$

over an algebraically closed field of characteristic 0?

Solution. It is known (a consequence of the Hilbert Nullstellensatz, i.e. the Hilbert Zeros Theorem) that a system $f_i(X) = 0$, $i = 1, \ldots, k$, has a finite number of solutions if and only if the factor algebra $K[X]/(f_1, \ldots, f_k)$ is finite dimensional. This means that the set of normal monomials with respect to the ideal $(f_1, \ldots, f_k)$ is finite. We calculate the Gröbner basis of the ideal generated by

$$g_1 = x^2 - yz + x, \quad g_2 = xy - z^2 - z, \quad g_3 = xz - y^2 - y,$$

with respect to the degree lexicographical order ($x \succ y \succ z$). Hence

$$\overline{g_1} = x^2, \quad \overline{g_2} = xy, \quad \overline{g_3} = xz.$$

The first composition is based either on $\overline{g_1} y = \overline{g_2} x$ (or on $\overline{g_1} z = \overline{g_3} x$), or on $\overline{g_2} z = \overline{g_3} y$. For example, let

$$g_4 := g_1 y - g_2 x = xz^2 - y^2 z + xy + xz.$$

The consecutive reductions give

$$g_4 := g_4 - g_3 z = xy + xz + yz, \quad g_4 := g_4 - g_2 = xz + z^2 + yz + z,$$

$$g_4 := g_4 - g_3 = y^2 + z^2 + y + z.$$

One can show by direct calculations, that the further compositions do not give new elements. Hence the set

$$G = \{g_1, g_2, g_3, g_4 = y^2 + z^2 + y + z\}$$

is a minimal Gröbner basis (to make it reduced we have to replace g_3 with $g_3 + g_4$). In this way, the set of normal monomials consists of $1, x, y, z^k$, $k = 1, 2, \ldots$, and the factor algebra is infinite dimensional. Hence the system has infinitely many solutions. The system is equivalent to the system

$$x^2 + x - yz = y^2 + y - xz = z^2 + z - xy = y^2 + z^2 + y + z = 0.$$

Considering z as a parameter, for each z_0 we can find (one or several) solutions (x_0, y_0).

Practical Hint 1.25. Instead of working with the generators of the ideal of $K[X]$, sometimes it is more convenient to work with the defining relations of the corresponding factor algebra. For instance, in Example 1.24, let the factor algebra have the presentation

$$R = K[x, y, z]/(x^2 = yz - x, xy = z^2 + z, xz = y^2 + y).$$

Then, working in R (and denoting its generators also by x, y, z), we have

$$x^2 = yz - x, \quad xy = z^2 + z, \quad (x^2)y = (yz - x)y = (xy)x = (z^2 + z)x, \quad xz^2 + xz = y^2 z - xy,$$

which is the same as the fact that $xz^2 - y^2 z + xy + xz$ belongs to the ideal.

For general reading on polynomial algebras see the books [AM] and [L]. For theory of Gröbner bases see the books [AL] and [BW], and the big survey article [U] which deals also (and mainly) with noncommutative generalizations.

Many computer systems have packages of for computing of Gröbner bases. For example, the Computer Centre of the HKU has (at least temporary) possibilities for usage of *Maple*. For this purpose, the students can access the system by telnet to "netback1.hku.hk" and use the HKUSUA UID/PIN to login the system; then type "maple" to access *Maple* for Gröbner bases computations.

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. 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 if 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.

3. 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.

4. 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 $x^n - 1$.

5*. 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.)

6. 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 $x, xy, \ldots, xy^n$.)

7. Calculate the Gröbner bases from Example 1.23 with respect to the degree lexicographical order (and $x \succ y$) and with respect to the *inverse lexicographical order* (with $x \prec y$).

8. Caluclate the Gröbner bases with respect to the lexicographical order ($x \succ y$) of the ideals (G_1) and (G_2) of $K[x, y]$ generated, respectively, by

$$G_1 = \{g_1 = x^2 + y^3, \quad g_2 = xy, \quad g_3 = x^3 + 2y^3\},$$
$$G_2 = \{g_1 = x^2 + y^3, \quad g_2 = xy + 2y^2, \quad g_3 = x^3 + 2y^3\}.$$

9. How many solutions has the system

$$x^2 - x = yz, \quad y^2 + y = xz, \quad z^2 + z = xy$$

over an algebraically closed field of characteristic 0? (Comparing with Example 1.24, only the sign of x is changed.)

10. If the ideal J of $K[X]$ is generated by a set G of monomials (such ideals are called *monomial ideals*, and the factor algebras are *monomial algebras*), show that G is a Gröbner basis of J with respect to any admissible order on $[X]$.

2. AUTOMORPHISMS AND DERIVATIONS OF POLYNOMIAL ALGEBRAS

Basic Definitions

We assume that K is a field of characteristic 0, e.g. $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}$. 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 2.1. 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 $f_j = \varphi(x_j)$. 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 $\psi \circ \varphi$ (first applying φ and then ψ). We shall also denote the automorphisms as $\varphi = (\varphi(x_1), \dots, \varphi(x_n))$, but shall use the notation $\psi\varphi = \psi \circ \varphi$ instead of $F(G)$.

Definition 2.2. The automorphisms of the form

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

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

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

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 2.3. (i) Let $\varphi, \psi \in \mathrm{End}K[x, y]$ (where $\mathrm{End}K[X]$ is the set of all endomorphisms of $K[X]$, equipped with the operation "composition") be defined by

$$\varphi(x) = x + y^2, \varphi(y) = y, \quad \text{or} \quad \varphi = (x + y^2, y),$$

$$\psi(x) = x - y^2, \psi(y) = y, \quad \text{or} \quad \psi = (x - y^2, y).$$

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

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

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

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

$$\varphi(x) = x + y^2, \varphi(y) = y, \quad \text{or} \quad \varphi = (x + y^2, y),$$

$$\psi(x) = x, \psi(y) = y + x^3, \quad \text{or} \quad \psi = (x, y + x^3)$$

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

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

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

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

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

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

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

Example 2.4. The endomorphism of $K[x,y,z]$

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

is an automorphism with inverse

$$\nu^{-1} = \rho = (x + 2(y^2 + xz)y - (y^2 + xz)^2 z, y - (y^2 + xz)z, z).$$

It is called the *Nagata automorphism* and was constructed by Nagata [N] in 1970.

The easiest way to check that $\rho \circ \nu = \nu \circ \rho$ is the identity of $K[x,y,z]$ is to see first that $\nu(y^2 + xz) = y^2 + xz$. Hence $w = y^2 + xz$ behaves as a constant under the action of ν and by direct calculation one sees that

$$\nu \circ \rho(x) = \nu(\rho(x)) = \nu(x + 2wy - w^2 z)$$

$$= \nu(x) + 2w\nu(y) - w^2 z = (x - 2wy - w^2 z) + 2w(y + wz) - w^2 z = x,$$

and similarly for $\nu \circ \rho(y) = y$, $\nu \circ \rho(z) = z$.

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

We shall be interested in several natural problems:

Problems 2.5. (i) *How to construct examples of automorphisms?*

(ii) *Do the automorphisms of $K[X]$ have any "canonical" form? Can they be presented as compositions of some simpler automorphisms?*

(iii) *How to recongnize whether an endomorphism of $K[X]$ is an automorphism?*

(iv) *How to calculate the inverse of a given automorphism?*

Definition 2.6. 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 2.7. (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 similiar. 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 2.8. *The Jacobian matrix of any automorphism of $K[X]$ 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 is the following:

Jacobian Conjecture 2.9. (Keller, 1939) *Every endomorphism of $K[X]$ with an invertible Jacobian matrix is an automorphism (of $K[X]$).*

Now we shall show the importance of derivations in the study of automorphisms of polynomial algebras.

Definition 2.10. 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 2.11. (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

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

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 2.12. *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 $r = \sum \alpha_p r_{p_1} \cdots r_{p_m}$, $\alpha_p \in K$, and

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

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 2.11 (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:

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

Lemma 2.13. (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 depending 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 2.14. *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 2.12, $\Delta = w\delta$ 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 2.15. 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.

Exercise 2.16. *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*

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

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 2.17. 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 kernel of δ such that*

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

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

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.

In 1900, Hilbert outlined 23 mathematical problems to the International Congress of Mathematicians in Paris. His famous address influenced, and still today influence, mathematical research all over the world. An important partial case of the 14-th Hilbert Problem is: *If G is a group of automorphisms of $K[X]$, is it true that the subalgebra $K[X]^G$ of all polynomials which are invariant under the action of G is finitely generated?* Especially interesting is the case, when the group G consists of linear automorphisms only, i.e. in the case of invariant theory. The negative answer was given by Nagata in the 1950's in terms of invariant theory. For the exposition of the result of Nagata see [DC]. See also the book by Nowicki [No] and the survey paper by Freudenburg [F] 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 2.18. Let δ be a locally nilpotent derivation of an algebra R. Then the mapping $\phi : R \to R$ defined by

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

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 2.19. (i) If δ is a triangular derivation of $K[X]$, then $\delta(x_i)$ belongs to $K[x_{i+1}, \ldots, x_n]$ 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 2.11 (iii). 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.

Automorphisms and Gröbner Bases

We shall present an algorithm which decides whether an endomorphism of the polynomial algebra $K[X]$ is an automorphism and, if this is the case, finds the inverse. The algorithm works in a very general situation (even for noncommutative algebras). The theoretical result has several proofs, see van den Essen [E1] and Shannon and Sweedler [SS] for

fields, Abhyankar and Li [AbL] for arbitrary commutative rings R and Drensky, Gutierrez and Yu [DGY] in the general noncommutative setup.

Lemma 2.20. *Let $X = \{x_1, \dots, x_n\}$, $Y = \{y_1, \dots, y_n\}$ and let $\theta : K[X] \to K[Y]$ be a homomorphism such that $\theta(x_i) = h_i(Y) = h_i(y_1, \dots, y_n)$, $i = 1, \dots, n$. Extend θ to a homomorphism $\theta_0 : K[X, Y] \to K[Y]$ by $\theta_0(x_i) = \theta(x_i)$, $\theta_0(y_i) = y_i$, $i = 1, \dots, n$. Then the kernel of θ_0 is the ideal U of $K[X, Y]$*

$$\mathrm{Ker}(\theta_0) = U = (x_i - h_i(Y) \mid i = 1, \dots, n)$$

generated by all $x_i - h_i(Y)$ and $\mathrm{Ker}(\theta_0) \cap K[Y] = (0)$.

Proof. (For another proof see [AL], Theorem 2.4.2.) Obviously $\theta_0(x_i - h_i(Y)) = \theta(x_i) - h_i(Y) = h_i(Y) - h_i(Y) = 0$ and $x_i - h_i(Y) \in \mathrm{Ker}(\theta_0)$. Hence the ideal U generated by all $x_i - h_i(Y)$ is contained in $\mathrm{Ker}(\theta_0)$. Consider $t_i = x_i - h_i(Y)$, $i = 1, \dots, n$, 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, $\theta_0(t_i) = \theta_0(x_i - h_i(Y)) = 0$, $\theta_0(y_i) = y_i$ and θ_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 θ_0 is the ideal of $K[T, Y]$ generated by T and

$$\mathrm{Ker}(\theta_0) = (t_i \mid i = 1, \dots, n) = (x_i - h_i(Y) \mid i = 1, \dots, n),$$

and $\mathrm{Ker}(\theta_0) \cap K[Y] = (0)$.

Proposition 2.21. *Let $X = \{x_1, \dots, x_n\}$, $Y = \{y_1, \dots, y_n\}$ and let $\phi : K[Y] \to K[X]$, $\psi : K[X] \to K[Y]$ be homomorphisms such that*

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

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

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

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

$$x_i = \phi(\psi(x_i)) = \phi(g_i(y_1, \dots, y_n)) = g_i(\phi(y_1), \dots, \phi(y_n)) = g_i(f_1(X), \dots, f_n(X)),$$

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

$$x_i = g_i(f_1(X), \dots, f_n(X)) \equiv g_i(y_1, \dots, y_n) \equiv g_i(Y) \pmod{U},$$

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

$$x_i \equiv g_i(y_1, \ldots, y_n) \equiv g_i(f_1(X), \ldots, f_n(X)) \equiv \phi \circ \psi(x_i) \pmod{U}$$

and $\phi \circ \psi$ is the identity mapping on $K[X]$ modulo the ideal U. Similarly, $\psi \circ \phi$ is the identity mapping on $K[Y]$ modulo the ideal V and for every $p(Y) \in K[Y]$ we have $\psi \circ \phi(p(Y)) \equiv p(Y) \pmod{V}$. The polynomial $\psi \circ \phi(y_i)$ belongs to $K[Y]$ and is equal to y_i modulo the ideal V. Hence $\psi \circ \phi(y_i) - y_i \in V \cap K[X]$ and this intersection is equal to 0 by Lemma 2.20. Hence $y_i = \psi \circ \phi(y_i)$, $i = 1, \ldots, n$. Similarly, we obtain that $x_i = \phi \circ \psi(x_i)$, $i = 1, \ldots, n$, and the mappings ϕ and ψ are inverse to each other. Hence ϕ and ψ are isomorphisms and $\psi = \phi^{-1}$.

Theorem 2.22. *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*

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

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 $\phi : K[Y] \to K[X]$ defined by $\phi(y_i) = f_i(X)$, $i = 1, \ldots, n$, is an isomorphism. Then the proof of the theorem follows immediately from Proposition 2.21.

By Theorem 2.22, if θ is an endomorphism of $K[X]$, and $\theta(x_i) = f_i(X)$, 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 $y_i - f_i(X)$, $i = 1, \ldots, n$, has a system of generators of the form $x_i - g_i(Y)$, $i = 1, \ldots, n$. This problem can be solved effectively using Gröbner bases.

Definition 2.23. Let X, Y be two sets of variables with admissible orders $\prec_X$ and $\prec_Y$, respectively. We define the *elimination order* on $[X,Y]$ with the variables X larger than the variables Y, by

$$u_1(X)v_1(Y) \prec u_2(X)v_2(Y),$$

if $u_1(X) \prec_X u_2(X)$ or, if $u_1(X) = u_2(X)$, then $v_1(Y) \prec_Y v_2(Y)$.

The idea of the algorithm which recognizes whether an endomorphism of $K[X]$ is an automorphism is the following. We introduce a new set of variables Y, with the same cardinality as X. Then we define arbitrary admissible orders on $[X]$ and $[Y]$ and extend them to an elimination order with the variables X larger than the variables Y. Then the leading monomials of the polynomials $y_i - f_i(X)$ depend on X. If we calculate the Gröbner basis of U with respect to this elimination order, we shall obtain some new system of generators of U where the monomials containing x's are higher than those containing only y's. The monomial x_i is the smallest monomial which contains x_i. Hence, if θ is an automorphism, we shall obtain that some polynomials $x_i - g_i(Y)$ belong to the new

Gröbner basis. If θ is not an automorphism, then for some i there will be no polynomial of the form $x_i - g_i(Y)$ in U and, of course, there will be no such polynomial in the Gröbner basis.

One can use computer packages for computing with Gröbner bases to decide whether an endomorphism is an automorphism and to find the inverse.

Example 2.24. A typical session of *Maple* (using netback1.hku.hk and working in Unix regime) is ("netback1%" and ">" are beginnings of command lines and the other lines are for the results):

netback1% maple

>with(grobner);

[finduni, finite, gbasis, ...]

>gbasis([x-2*(y^2+x*z)*y-(y^2+x*z)^2*z-u,y+(y^2+x*z)*z-v,z-w], [x,y,z,u,v,w], plex);

$$[x + w^3u^2 + 2w^2uv^2 - 2vwu - u + v^4w - 2v^3, y - v + w^2u + wv^2, z - w]$$

>quit;

netback1% logout

The meaning of the command "gbasis([f,g,h],[x,y,z,u,v,w],plex);" is that we find the Gröbner basis of the ideal of the algebra $\mathbf{Q}[x, y, z, u, v, w]$ generated by the polynomials f, g, h with respect to the lexicographic order defined by $x \succ y \succ z \succ u \succ v \succ w$. For degree lexicographic order one needs "tdeg" instead of "plex".

In the example, we start with the Nagata automorphism

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

and consider the ideal of the algebra of polynomials in six variables generated by the polynomials

$$(x - 2(y^2 + xz)y - (y^2 + xz)^2z) - u, \quad (y + (y^2 + xz)z) - v, \quad z - w.$$

The result is a triple of polynomials

$$(x - p(u, v, w), y - q(u, v, w), z - r(u, v, w)),$$

which means that ν is an automorphism with inverse

$$\nu^{-1} = (p(x, y, z), q(x, y, z), r(x, y, z))$$

$$= (-(z^3x^2 + 2z^2xy^2 - 2yzx - x + y^4z - 2y^3), -(-y + z^2x + zy^2), z)$$

$$= (x + 2(y^2 + xz)y - (y^2 + xz)^2z, y - (y^2 + xz)z, z).$$

For general reading on automorphisms of polynomial algebras (and the Jacobian conjecture) see the books by van den Essen [E2] and Mikhalev, Shpilrain and Yu [MSY]. For derivations of polynomial algebras see [E2] and the book by Nowicki [No] available also online in postscript format.

Exercises

1. Find (calculations by hand only!) 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 following derivations δ_1 and δ_2 are locally nilpotent and the polynomials w_1 and w_2', w_2'' belong to the kernels of δ_1 and δ_2, respectively:

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

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

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

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 the inverse of the automorphisms from Exercise 1, using computers.

11. Using computers, determine whether the following endomorphisms of $K[X]$ are automorphisms and find the inverse of the automorphisms:

(i) $\phi \in \mathrm{End}K[x, y]$, where

$$\phi(x) = (-8x - 11y) + (6x^2 + 12xy + 6y^2) + 11,$$

$$\phi(y) = (179x + 246y) + (-198x^2 - 444xy - 255y^2)$$

$$+(96x^3 + 324x^2y + 360xy^2 + 132y^3) + (-36x^4 - 144x^3y - 216x^2y^2 - 144xy^3 - 36y^4) - 126;$$

(ii) $\phi \in \mathrm{End}K[x, y]$, where

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

Answers. (i) Yes, because the Gröbner basis of the ideal of $K[x, y, u, v]$ generated by $\phi(x) - u$ and $\phi(y) - v$ consists of the polynomials

$$x + 12u + 37v + 39u^2 + 12uv + 18v^2 + 12u^3 + 36u^2v + 18u^4 + 21,$$

$$y - 13u - 40v - 42u^2 - 12uv - 18v^2 - 12u^3 - 36u^2v - 18u^4 - 25,$$

and the inverse of ϕ is

$$\phi^{-1}(x) = -((12x + 37y) + (39x^2 + 12xy + 18y^2) + (12x^3 + 36x^2y) + 18x^4 + 21),$$

$$\phi^{-1}(y) = (13x + 40y) + (42x^2 + 12xy + 18y^2) + (12x^3 + 36x^2y) + 18x^4 + 25.$$

(ii) No, because the Gröbner basis of the ideal of $K[x, y, u, v]$ generated by $x + xy - u$ and $y + x^2 + xy - v$ is

$$\{x + xy - u, xy + y + xy^2 - v - 2uxy + u^2\}.$$

12. Using Gröbner bases, but without computer, 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

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

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

3. TAME AND WILD AUTOMORPHISMS

Polynomials in Two Variables

We assume that K is a field of characteristic 0, e.g. $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}$. 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 $K[X] = K[x_1, \dots, x_n]$. Sometimes we shall denote the automorphisms as $\varphi = (f_1, \dots, f_n)$, where $f_i = \varphi(x_i)$, $i = 1, \dots, n$, but the composition will be as for operators, from right to left, e.g. $\varphi \circ \psi : u \to \varphi(\psi(u))$.

Recall that an automorphism φ of $K[X]$ is called affine if it is of the form

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

where the $n \times n$ matrix (α_{ij}) is invertible. The automorphism φ is triangular, if

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

and the polynomials $f_j(x_{j+1}, \dots, x_n)$ do not depend on $x_1, \dots, x_j$. Sometimes, especially when $X = \{x, y\}$, we shall call the automorphisms φ satisfying

$$\varphi(x) = \alpha x, \quad \varphi(y) = \beta y + f(x), \quad \alpha, \beta \in K^*,$$

also triangular, or *upper triangular* because their Jacobian matrix is an upper triangular matrix of the form

$$J(\varphi) = \begin{pmatrix} \alpha & df(x)/dx \\ 0 & \beta \end{pmatrix}.$$

The automorphisms which belong to the group generated by the affine and the triangular automorphisms are called tame. The automorphisms which are not tame are called wild.

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

For the case of polynomials in two variables the answer is affirmative and this is the famous theorem of Jung–van der Kulk [J, K].

Theorem 3.2. *Every automorphism of the polynomial algebra $K[x, y]$ over an arbitrary field K of any characteristic is tame.*

The theorem was proved by Jung [J] in 1942 for $K = \mathbf{C}$. In 1953 van der Kulk [K] proved it over any field. Now there are many different proofs of this theorem. One of the simplest is due to Makar-Limanov [ML]. It is based on locally nilpotent derivations and can be found in the book [D].

In 1970 Nagata [N] constructed his automorphism of $K[x, y, z]$, conjectured that it is wild, and gave some supporting evidences, see Theorem 3.7 and Conjecture 3.9 below. Only recently, his conjecture has been solved by Shestakov and Umirbaev, see the comments

following Conjecture 3.9. The problem for existing wild automorphisms for $K[X]$ when $n = |X| > 3$ is still open.

We may consider polynomial algebras with coefficients from any commutative K-algebra R. We shall accept the same definition for the tame automorphisms of $R[X]$ (compositions of affine and triangular automorphisms), although we may have some problems with the tameness of the affine automorphisms, see the example of Nagata-Anick which we shall present later. Now we start the study of the case of $R[x, y]$ and $K[x, y]$.

Lemma 3.3. *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

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

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, $\phi = \rho_1 \circ \cdots \circ \rho_n$, 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 $\phi = \sigma_1^{\delta} \circ \tau_1 \circ \sigma_2 \circ \cdots \circ \sigma_k \circ \tau_k \circ \sigma_{k+1}^{\varepsilon}$.

For a nonzero polynomial $g(x, y)$ we denote by $\overline{g(x, y)}$ the homogeneous component of maximal degree of $g(x, y)$. Since we shall not use Gröbner bases, this will not lead to misunderstandings.

Proposition 3.4. *In the notation of the previous lemma, if $\phi = \sigma_1^{\delta} \circ \tau_1 \circ \sigma_2 \circ \cdots \circ \sigma_k \circ \tau_k$, 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*

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

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 $m = d_1 \cdots d_{k-1}$.

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 $i = 2, \ldots, k$. 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

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

$$\overline{\sigma_2 \tau_2 \cdots \sigma_k \tau_k(y)} = \kappa_2(\mu_2 x + \nu_2 y)^n,\ n = d_2 \cdots d_{k-1}, \mu_2 \neq 0,\ \kappa_2 \in R,$$

and obtain

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

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

$$\begin{aligned}\sigma_1\tau_1(\sigma_2 \cdots \tau_k(x)) &= \lambda_2(\kappa_2(\mu_2\sigma_1\tau_1(x) + \nu_2\mu_2\sigma_1\tau_1(y))^n)^{d_k} + \cdots \\ &= \lambda_2(\kappa_2(\mu_2\theta_1)^n(\xi_1 x + \eta_1 y)^{d_1} + \cdots)^n)^{d_k} + \cdots\end{aligned}$$

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

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

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

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

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

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

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 3.5. *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 $\phi = \sigma_1^{\delta} \circ \tau_1 \circ \sigma_2 \circ \cdots \circ \sigma_k \circ \tau_k \circ \sigma_{k+1}^{\varepsilon}$, where $\sigma_i \in A$, $\tau_i \in B$, as in Lemma 3.3. If $\varepsilon = 0$, then ϕ is in the form of Proposition 3.4 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 3.4, for $\psi = \sigma_1^{\delta}\tau_1\sigma_2 \cdots \sigma_k\tau_k$

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

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

Theorem 3.5 and Proposition 3.4 give an algorithm which allows to decompose the tame automorphisms of $R[x, y]$ as products of affine and triangular automorphisms.

Example 3.6. (Compare with Exercise 11, Part 2 of the lecture notes). Decompose the following automorphism of $K[x, y]$ as a product of affine and triangular automorphisms:

$$\phi(x) = f(x, y) = (-8x - 11y) + (6x^2 + 12xy + 6y^2) + 11,$$

$$\phi(y) = g(x,y) = (179x + 246y) + (-198x^2 - 444xy - 255y^2)$$
$$+(96x^3 + 324x^2y + 360xy^2 + 132y^3) + (-36x^4 - 144x^3y - 216x^2y^2 - 144xy^3 - 36y^4) - 126;$$

Solution. The homogeneous components of maximal degree of $f(x,y)$ and $g(x,y)$ are

$$\overline{f(x,y)} = 6x^2 + 12xy + 6y^2 = 6(x+y)^2,$$

$$\overline{g(x,y)} = -36x^4 - 144x^3y - 216x^2y^2 - 144xy^3 - 36y^4 = -36(x+y)^4.$$

Hence $\bar{g} = -(\bar{f})^2$. We define the automorphism

$$\tau_1 = (x, y + x^2)$$

and consider the composition

$$\phi_1 = \phi \circ \tau_1 = (f_1(x,y), g_1(x,y)).$$

Clearly, $f_1(x,y) = f(x,y)$. Direct calculations give that

$$g_1(x,y) = g + f^2 = (3x + 4y) + (-2x^2 - 4xy - 2y^2) - 5 = (3x + 4y) - 2(x+y)^2 - 5.$$

Again, $\overline{f_1} = -3\overline{g_1}$ and we define

$$\tau_2 = (x + 3y, y), \quad \phi_2 = \phi_1 \circ \tau_2 = (f_2(x,y), g_2(x,y)).$$

We have $g_2(x,y) = g_1(x,y)$ and

$$f_2(x,y) = f_1 + 3g_1^2 = (x+y) - 4.$$

Since $\overline{g_2} = -2(\overline{f_2})^2$, the next step is to define

$$\tau_3 = (x, y + 2x^2), \quad \phi_3 = \phi_2 \circ \tau_3 = (f_3(x,y), g_3(x,y)),$$

where

$$f_3(x,y) = f_2(x,y) = (x+y) - 4, \quad g_3(x,y) = g_2(x,y) + 2f_2(x,y) = -(13x + 12y) + 27.$$

Hence we obtain the affine automorphism

$$\rho = ((x+y) - 4, -(13x + 12y) + 27) = \phi_2 \circ \tau_3 = (\phi_1 \circ \tau_2) \circ \tau_3 = \phi \circ \tau_1 \circ \tau_2 \circ \tau_3,$$

$$\phi = \rho \circ \tau_3^{-1} \circ \tau_2^{-1} \circ \tau_1^{-1},$$

where

$$\tau_3^{-1} = (x, y - 2x^2), \quad \tau_2^{-1} = (x - 3y, y), \quad \tau_1^{-1} = (x, y - x^2).$$

Theorem 3.7. (Nagata [N]) *The Nagata automorphism of* $K[x,y,z]$

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

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 3.5, 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 3.8. 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 was one of the most famous conjectures on automorphisms of polynomial algebras.

Conjecture 3.9. (The Nagata Conjecture, [N]) *The Nagata automorphism is wild considered as an automorphism of the polynomial algebra* $K[x,y,z]$.

Nagata made its conjecture in 1970. It was solved, into affirmative, only in 2003 by Shestakov and Umirbaev [SU1, SU2, SU3]. They developed a special technique, based on noncomutative (and even nonassociative) ring theory. The first paper [SU1] contains the explonation of the main ideas and the sketch of the proof and the other two papers contain the complete details. Some idea about the main steps of the proof is given also in the paper by van den Essen [E3]. The proof of Shestakov and Umirbaev gives also an effective algorithm to decide whether an automorphism of $K[x,y,z]$ is tame or not. In particular, they proved the following theorem.

Theorem 3.10. (i) *Let* ϕ *be an automorphism of* $K[x,y,z]$ *which fixes* z. *Then* ϕ *is tame if and only if it is tame as an automorphism of the polynomial algebra* $(K[z])[x,y]$ *in two variables* x, y *with coefficients depending on* z.

(ii) *The Nagata automorphism of* $K[x,y,z]$ *is wild.*

Hence, Theorem 3.5 gives an algorithm recognizing the automorphisms of $(K[z])[x,y]$ which are wild considered also as automorphisms of $K[x,y,z]$. In order to produce more

wild automorphisms of $K[x,y,z]$ we need some methods to construct "Nagata like" automorphisms, which fix z. Such a method was given in [DY2], see also the survey article [DY1].

Example 3.11. Nagata and Anick suggested the following example, see the book by Cohn [C2], p. 343:

$$\phi = (x + (xt - yz)z, y + (xt - yz)t, z, t) \in \mathrm{End}K[x,y,z,t].$$

It is easy to see that ϕ fixes $(xt - yz)$ and is an automorphism of $K[x,y,z,t]$ with inverse

$$\phi = (x - (xt - yz)z, y - (xt - yz)t, z, t).$$

Clearly, ϕ fixes z, t and we may consider it as an automorphism of $(K[z,t])[x,y]$, the polynomial algebra in two variables x, y with coefficients which are polynomials in z, t. Since all monomials of $\phi(x), \phi(y)$ are linear in x, y, this automorphism is linear, and by our definition of tameness, is tame, as a $K[z,t]$-automorphism of $(K[z,t])[x,y]$. On the other hand, it is not clear whether ϕ is a tame automorphism of $K[x,y,z,t]$. This shows that our definition for tameness over a commutative domain R is not very good. Where is the problem? If we consider invertible matrices over the field K or over a principal ideal domain R, every such matrix is a product of elementary matrices of the form

$$\begin{pmatrix} \alpha & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}, \quad E + aE_{ij}, \quad i \neq j,$$

where α is an invertible and a is any element of K (or of R), E is the identity matrix and the E_{ij} are the usual matrix units. This well known fact is not more true for 2×2 matrices over a polynomial algebra in more than one variable. For example, see the paper by Cohn [C1], the matrix

$$\begin{pmatrix} 1 + zt & t^2 \\ -z^2 & 1 - zt \end{pmatrix}$$

is invertible over $K[z,t]$ but cannot be presented as a product of elementary matrices with entries from $K[z,t]$. And it is easy to see that this is the matrix which corresponds to the above defined linear automorphism of $(K[z,t])[x,y]$ (this is its Jacobian matrix).

For the case of matrices of bigger size, the famous theorem of Suslin [Su] states that *for $n \geq 3$ any invertible matrix with entries from $K[X]$ is a product of elementary matrices.* (A constructive proof of the theorem of Suslin is given by Park and Woodburn [PW].)

Hence, to avoid the problems with the definition of tame and wild automorphisms for polynomial algebras over arbitrary rings of coefficients (the problems appear for polynomials in two variables only), the "correct" definition should be that the group of tame automorphisms of $R[X]$ is generated by the *elementary automorphisms* of the form

$$\phi : x_i \to \alpha_i x_i + f(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n), \quad \phi : x_j \to \alpha_j x_j, \quad j \neq i,$$

with all $\alpha_j \in R^*$. In the case of two variables, these are the upper and lower triangular automorphisms, respectively

$$\phi = (\alpha x, \beta y + f(x)), \quad \psi = (\alpha x + f(y), \beta y).$$

Stably Tame Automorphisms

Let $X = \{x_1, \dots, x_n\}$, $Y = \{y_1, \dots, y_m\}$, and let ϕ be an automorphism of $K[X]$. Then we can extend ϕ to (an automorphism!) ψ of $K[X, Y]$ by $\psi(y_j) = y_j$, $j = 1, \dots, m$.

Definition 3.12. If ϕ is an automorphism of $K[X]$ and, for some Y, its extension ψ by $\psi(y_j) = y_j$, $i = 1, \dots, m$, to an automorphism of $K[X, Y]$ is a tame automorphism of $K[X, Y]$, we say that ϕ is a *stably tame automorphism* of $K[X]$. (In other words, we do not know whether ϕ is tame, but it becomes tame in some bigger polynomial algebra.)

Recall that the linear mapping $\delta : R \to R$ of the algebra R is called a derivation if $\delta(uv) = \delta(u)v + u\delta(v)$ for all $u, v \in R$, and $\mathrm{Ker}\delta = R^\delta$ is the kernel of δ (considered as a linear operator of the vector space R). 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 $K[X]$ is triangular if $\delta(x_j) \in K[x_{j+1}, \dots, x_n]$, $j = 1, \dots, n$. For any locally nilpotent derivation δ of the algebra R, the mapping

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

is well defined and is an automorphism of R, which we call an exponential automorphism and denote by $\exp(\delta)$.

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

Theorem 3.13. (Martha Smith [S]) *Let δ be a triangular derivation of $K[X]$ and let $w \in \mathrm{Ker}(\delta)$. Then the automorphism $\exp(w\delta)$ is stably tame and becomes tame extended to $K[X, y]$ by $\exp(w\delta) : y \to y$.*

Proof. Let us extend the action of δ to $K[X, y]$ by $\delta(y) = 0$. Clearly, δ is still triangular considered as a derivation of $K[X, y]$. Since $y \in \mathrm{Ker}(\delta)$, the derivation $\Delta_1 = y\delta$ is locally nilpotent and even triangular ($\Delta_1(x_i) \in yK[x_{i+1}, \dots, x_n]$, $i = 1, \dots, n$, because δ is triangular and $\Delta_1(y) = 0$). Hence $\exp(\Delta_1)$ is a triangular automorphism. Consider the tame automorphism σ of $K[X, y]$ defined by

$$\sigma(x_i) = x_i, \quad i = 1, \dots, n, \quad \sigma(y) = y + w(X)$$

(which is triangular if we consider the inverse ordering of the variables). Clearly σ acts as the identity mapping on $K[X]$. 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

$$\exp(\pm\Delta_1)(y) = y, \quad \exp(\pm\Delta_1)(w) = w$$

because y and w are in the kernel of Δ_1 (equal to the kernel of δ),

$$\phi(y) = \sigma^{-1}(\exp(-\Delta_1)(\sigma(\exp(\Delta_1)(y)))) = \sigma^{-1}(\exp(-\Delta_1)(\sigma(y))) =$$

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

For $u \in K[X]$ we have

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

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

because σ is the identity mapping on $u \in K[X]$,

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

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

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

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 $K[X, y]$ and is stably tame for $K[X]$.

Corollary 3.14. *The Nagata automorphism is stably tame.*

Proof. We consider the presentation of the Nagata automorphism in Example 2.19 (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.

Example 3.15. Consider the derivation δ of $K[x, y, z, t]$ defined by

$$\delta(x) = z, \quad \delta(y) = t, \quad \delta(z) = \delta(t) = 0.$$

It is triangular and $w = xt - yz$ is in the kernel of δ. Since $\delta^2(x) = \delta^2(y) = 0$, we obtain that $\phi = \exp(w\delta)$ acts on x, y, z, t by the rule

$$\phi(x) = x + w\delta(x) = x + wz, \quad \phi(y) = y + w\delta(y) = y + wt, \quad \phi(z) = z, \quad \phi(t) = t.$$

Hence ϕ is the automorphism of Nagata-Anick from Example 3.11. By the theorem of Martha Smith, ϕ is stably tame.

Coordinates in Polynomial Algebras

Very often one considers the n-tuples of variables $(x_1, \ldots, x_n)$ as coordinates of the n-dimensional vector space K^n and the polynomial algebra $K[X]$ as the algebra of polynomial functions on K^n. In such setup, the automorphisms of $K[X]$ correspond to changes of the coordinate systems in K^n.

Definition 3.16. The polynomial $p(X)$ is a *coordinate* if it is an image of x_1 under some automorphism of $K[X]$.

In the second part of these lecture notes we gave an algorithm which decides whether an endomorphism is an automorphism. In the case of arbitrary number of variables, no algorithm is known which decides whether a polynomial is a coordinate. Now we shall discuss this problem for the case of two variables.

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 $v(x, y)$, using in each step the Euclidean algorithm only.

The theorem of Jung–van der Kulk and Theorem 3.5 give 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 shall obtain that the endomorphism is an automorphism and shall find its decomposition, or, we shall be not able to perform some step of the algorithm and this will mean that the endomorphism is not an automorphism. Studying the proof of Theorem 3.5 more precisely, we observe that the algorithm is based on comparing the homogeneous components of highest degree of the images of x and y.

Now we present an algorithm which decides whether a polynomial $p(x, y) \in K[x, y]$ is a coordinate and, if the answer is affirmative, finds another polynomial $q(x, y)$ such that the pair (p, q) defines an automorphism. The proof is based on the idea of the proof of a theorem of Wright on the Jacobian conjecture [W].

Theorem 3.17. (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 in $K[x, y]$;*

(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).*

Instead of presenting the formal algorithm, we shall give an example.

Example 3.18. Consider the polynomial of $K[x,y]$:

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

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

$$p_y = \frac{3}{2}p_x + r, \quad r = -4(1+2(12x+17y)+4(2x+3y)^3),$$

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

$$p_x = 48(2x+3y)^2 s + t, \quad t = 46+96(12x+17y)+192(2x+3y)^3,$$

$$t = 48s+u, \quad u=-2.$$

We have obtained that p_x and p_y are relatively prime by the Euclidean algorithm. Hence $p(x,y)$ is a coordinate.

Now we shall find an automorphism of $K[x,y]$ which sends x to $p(x,y)$. First, we rewrite the above equalities in matrix form:

$$\begin{pmatrix} p_x \\ p_y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3/2 & 1 \end{pmatrix} \begin{pmatrix} p_x \\ r \end{pmatrix}, \quad \begin{pmatrix} p_x \\ r \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -4 \end{pmatrix} \begin{pmatrix} p_x \\ s \end{pmatrix},$$

$$\begin{pmatrix} p_x \\ s \end{pmatrix} = \begin{pmatrix} 1 & 48(2x+3y)^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t \\ s \end{pmatrix}, \quad \begin{pmatrix} t \\ s \end{pmatrix} = \begin{pmatrix} 1 & 48 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u \\ s \end{pmatrix},$$

$$\begin{pmatrix} u \\ s \end{pmatrix} = \begin{pmatrix} -2 \\ 1+2(12x+17y)+4(2x+3y)^3 \end{pmatrix}.$$

In this way we obtain

$$\begin{pmatrix} p_x \\ p_y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3/2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -4 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 48(2x+3y)^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 48 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2 \\ 1+2(12x+17y)+4(2x+3y)^3 \end{pmatrix}.$$

The theorem gives that there exists a polynomial $q = q(x,y)$ such that $\phi = (p,q)$ is an automorphism of $K[x,y]$. We shall use the above matrix equality, to find a similar equality

for the Jacobian matrix of ϕ. Namely, we want to find polynomials $v = v(x, y)$, $w = w(x, y)$ such that

$$J(\phi) = \begin{pmatrix} p_x & q_x \\ p_y & q_y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3/2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -4 \end{pmatrix} \begin{pmatrix} 1 & 48(2x+3y)^2 \\ 0 & 1 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 48 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & v \\ 1 + 2(12x + 17y) + 4(2x + 3y)^3 & w \end{pmatrix}.$$

The chain rule gives that, if $\phi = \rho_1 \circ \psi$, then $J(\phi) = J(\rho_1)\rho_1(J(\psi))$. The matrix

$$\begin{pmatrix} 1 & 0 \\ 3/2 & 1 \end{pmatrix}$$

is the Jacobian matrix of the linear automorphism

$$\rho_1 = \left(x + \frac{3}{2}y, y \right),$$

and we are looking for an automorphism ψ_1 such that

$$\rho_1(J(\psi_1)) = \begin{pmatrix} 1 & 0 \\ 0 & -4 \end{pmatrix} \begin{pmatrix} 1 & 48(2x+3y)^2 \\ 0 & 1 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 48 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & v \\ 1 + 2(12x + 17y) + 4(2x + 3y)^3 & w \end{pmatrix}.$$

Applying the inverse of ρ_1, which is $\rho_1^{-1} = (x - (3/2)y, y)$, to the above matrix equation, we obtain (because $\rho_1^{-1}(2x + 3y) = 2x$ and $\rho_1^{-1}(12x + 17y) = 12x - y$)

$$J(\psi_1) = \begin{pmatrix} 1 & 0 \\ 0 & -4 \end{pmatrix} \begin{pmatrix} 1 & 192x^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 48 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & \rho_1^{-1}(v) \\ 1 + 2(12x - y) + 32x^3 & \rho_1^{-1}(w) \end{pmatrix}.$$

We continue in the same way, assuming that $\psi_1 = \rho_2 \circ \psi_2$, where

$$J(\rho_2) = \begin{pmatrix} 1 & 0 \\ 0 & -4 \end{pmatrix}, \quad \rho_2 = (x, -4y).$$

Applying $\rho_2^{-1} = (x, -y/4)$, we obtain

$$J(\psi_2) = \begin{pmatrix} 1 & 192x^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 48 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & \rho_2^{-1}\rho_1^{-1}(v) \\ 1 + 24x + y/2 + 32x^3 & \rho_2^{-1}\rho_1^{-1}(w) \end{pmatrix}.$$

In the next step we assume that $\psi_2 = \rho_3 \circ \psi_3$ and choose

$$J(\rho_3) = \begin{pmatrix} 1 & 192x^2 \\ 0 & 1 \end{pmatrix}, \quad \rho_3 = (x, y + 64x^3).$$

Then, after applying ρ_3^{-1}, the calculations give that

$$J(\psi_3) = \begin{pmatrix} 1 & 48 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & \rho_3^{-1}\rho_2^{-1}\rho_1^{-1}(v) \\ 1 + 24x + y/2 & \rho_3^{-1}\rho_2^{-1}\rho_1^{-1}(w) \end{pmatrix}.$$

Fixing $\psi_3 = \rho_4 \circ \psi_4$, we obtain

$$J(\rho_4) = \begin{pmatrix} 1 & 48 \\ 0 & 1 \end{pmatrix}, \quad \rho_4 = (x, y + 48x),$$

$$J(\psi_4) = \begin{pmatrix} -2 & \rho_4^{-1}\rho_3^{-1}\rho_2^{-1}\rho_1^{-1}(v) \\ 1 + y/2 & \rho_4^{-1}\rho_3^{-1}\rho_2^{-1}\rho_1^{-1}(w) \end{pmatrix}.$$

Now we are able to find an automorphism ψ_4 with the above Jacobian matrix. It is sufficient to choose in a proper way the second column of the matrix. For example, we may fix

$$J(\psi_4) = \begin{pmatrix} -2 & 0 \\ 1 + y/2 & 1 \end{pmatrix},$$

which gives that

$$\psi_4 = (-2x + y^2, y).$$

Hence $\phi = \rho_1 \circ \rho_2 \circ \rho_3 \circ \rho_4 \circ \psi_4$.

Example 3.19. Applied to a polynomial $p(x, y) \in (K[z])[x, y]$, the above algorithm recognizes the tame coordinates only. For example, let

$$p_1(x, y) = x - 2(y^2 + zx)y - (y^2 + zx)^2 z, \quad p_2(x, y) = y + (y^2 + zx)z.$$

These polynomials are the first and the second coordinate of the Nagata automorphism. First, let $p = p_1$. Then

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

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

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

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

and again we cannot apply the Euclidean algorithm. Hence, there exists no tame automorphism of $(K[z])[x, y]$ which sends x to $p_1(x, y)$ or to $p_2(x, y)$.

Nevertheless, there is an algorithm, which recognizes coordinates in $(K[z])[x, y]$. (See [DY2], for generalizations see the survey article [DY1].)

Theorem 3.20. (Drensky and Yu [DY2]) *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.*

Example 3.21. Let, as in Example 3.19,

$$p(x,y) = p_1(x,y) = x - 2(y^2+zx)y - (y^2+zx)^2 z,$$
$$p_x = 1 - 2zy - 2(y^2+zx)z^2, \quad p_y = -2(y^2+zx) - 4y^2 - 4zy(y^2+zx).$$

If we work over $K(z)$, allowing division by polynomials in z, we obtain that

$$p_y = \frac{2}{z} y p_x + 2\left((y^2+zx) + \frac{y}{z}\right), \quad p_x = -2\left((y^2+zx) + \frac{y}{z}\right) z^2 + 1,$$

and this gives that $p(x,y)$ is a coordinate in $(K(z))[x,y]$. On the other hand, the ideal of $K[x,y,z]$ generated by p_x and p_y contains

$$u = 2yp_x - p_y z = 2(z(y^2+zx)+y), \quad p_x + zu = 1,$$

and coincides with $K[x,y,z]$. This gives that $p_1(x,y)$ is a coordinate of a wild automorphism of $(K[z])[x,y]$. (Pay attention: In practice, we have applied the Buchberger algorithm for computing the Gröbner basis of the ideal generated by p_x and p_y.) The case $p_2(x,y) = y + (y^2+zx)z$ is similar.

Remark 3.22. Let R be any commutative domain and let $p(x,y) \in R[x,y]$ be a coordinate. Let ϕ and ψ be two automorphisms of $R[x,y]$ such that ψ is wild, ϕ is tame, and $\phi(x) = \psi(x) = p(x,y)$. Then $\phi^{-1} \circ \psi$ is also wild and $\phi^{-1} \circ \psi(x) = x$. But this is impossible because the only automorphisms of $R[x,y]$ which fix x are of the form $(x, y+f(x))$ (prove it!) and are tame. Hence, if a coordinate $p(x,y)$ in $R[x,y]$ is the image of x under a wild automorphism, then all automorphisms sending x to $p(x,y)$ are also wild. The situation is different for the case of three variables. For example, z is a coordinate of the wild Nagata automorphism as well as a coordinate of the identical automorphism which is tame. This motivates the following problem suggested by Yu in 2002.

Problem 3.21. *For $|X| = n > 2$, do there exist coordinates $p(X)$ of $K[X]$ such that all automorphisms sending x_1 to $p(X)$ are wild?* We call such coordinates *wild*.

The affirmative answer for $|X| = n = 3$ was obtained by Umirbaev and Yu [UY], using techniques from [SU1–SU3]:

Theorem 3.22. *If $\phi = (p,q,r)$ is a wild automorphism of $K[x,y,z]$, then at least two of the coordinates p,q,r are wild.*

For general reading on the topics of this lecture see the books by van den Essen [E2] and Mikhalev, Shpilrain and Yu [MSY], and the survey article by Drensky and Yu [DY1].

Exercises

1. Decompose the automorphism of $K[x,y]$ from Exercise 11, Part 2 of the lecture notes, as a product of affine and triangular automorphisms.

2. Using theory of locally nilpotent derivations, Theorem 3.5, and the theorem of Shestakov and Umirbaev, show that the following automorphism of $K[x,y,z]$ is wild:

$$\phi = (x - 2f(w,z)y - f^2(w,z)z, y + f(w,z)z, z),$$

where $f(w,z)$ is a polynomial in $w = y^2 + xz$ which essentially depends on w, i.e. $f(w,z)$ cannot be expressed as a polynomial in z only.

REFERENCES

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

[AL] 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.

[C1] P.M. Cohn, On the structure of the GL_2 of a ring, Inst. Hautes Études Sci. Publ. Math. **30** (1966), 5-53.

[C2] P.M. Cohn, Free Rings and Their Relations, Second Edition, London Math. Soc. Monographs **19**, Acad. Press, 1985.

[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.

[E3] A. van den Essen, The solution of the tame generators conjecture according to Shestakov and Umirbaev, Colloq. Math. **100** (2004), No. 2, 181-194.

[F] G. Freudenburg, A survey of counterexamples to Hilbert's fourteenth problem, Serdica Math. J. **27** (2001), 171-192.

[H] D. Hilbert, Mathematical problems, Bull. Am. Math. Soc., New Ser. **37** (2000), No.4, 407-436.

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

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

[LY] C.-M. Lam, J.-T. Yu, Tame and wild coordinates of $\mathbf{Z}[x, y]$, J. Algebra **279** (2004), No. 2, 425-436.

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

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

[MSY] A.A. Mikhalev, V. Shpilrain, J.-T. Yu, Combinatorial Methods. Free Groups, Polynomials, and Free Algebras, CMS Books in Mathematics **19**, Springer, New York, 2004.

[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. http://www-users.mat.uni.torun.pl/˜anow/polder.html

[PW] H. Park, C. Woodburn, An algorithmic proof of Suslin's stability theorem for polynomial rings, J. Algebra **178** (1995), 277-298.

[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.

[SU1] I.P. Shestakov, U.U. Umirbaev, The Nagata automorphism is wild, Proc. Natl. Acad. Sci. USA **100** (2003), No. 22, 12561-12563.

[SU2] I.P. Shestakov, U.U. Umirbaev, Poisson brackets and two-generated subalgebras of rings of polynomials, J. Amer. Math. Soc. **17** (2004), No. 1, 181-196.

[SU3] I.P. Shestakov, U.U. Umirbaev, The tame and the wild automorphisms of polynomial rings in three variables, J. Amer. Math. Soc. **17** (2004), No. 1, 197-227.

[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.

[Su] A.A. Suslin, On the structure of the special linear group over polynomial rings (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **41** (1977), 235-252. Translation: Math. USSR Izv. **11** (1977), 221-239.

[U] V.A. Ufnarovski, Combinatorial and asymptotic methods in algebra, in A.I. Kostrikin, I.R. Shafarevich (Eds.), "Algebra VI", Encyclopedia of Math. Sciences **57**, Springer-Verlag, 1-196, 1995.

[UY] U.U. Umirbaev, J.-T. Yu, The strong Nagata conjecture, Proc. Natl. Acad. Sci. USA **101** (2004), No. 13, 4352-4355.

[W] D. Wright, The amalgamated free product structure of $\mathrm{GL}_2(k[X_1, \ldots, X_n])$ and the weak Jacobian theorem for two variables. J. Pure Appl. Algebra **12** (1978), No. 3, 235-251.

Topics in Algebra

Class Test on April 28, 2005

1. (40 points) Let $X = \{x, y, z\}$. Prove that every ideal of

$$[X] = \{x^a y^b z^c \mid a, b, c \geq 0\}$$

is finitely generated.

2. (30 points) Let K be a field of characteristic zero. Find the Gröbner basis with respect to the degree lexicographical order (assuming that $x \succ y$) of the ideal of $K[x, y]$ generated by

$$g_1 = y^3 + x^2, \quad g_2 = xy + 3y^2, \quad g_3 = 2y^4 + x^3.$$

3.(30 points) Let K be a field of characteristic zero. Decompose the automorphism

$$\rho = (5x - 3y + 7x^2 - 8xy + 4y^2 + 8x^2(x - y) + 4x^4, 2x - y + 3x^2 - 4xy + 2y^2 + 4x^2(x - y) + 2x^4)$$

of $K[x, y]$ into a product of affine and triangular automorphisms.

Answers and Solutions:

1. This is a partial case of the theorem that the ideals of $\{x_1^{a_1} \cdots x_n^{a_n} \mid a_i \geq 0\}$ are finitely generated. This theorem is the main step in one of the standard proofs for Hilbert Basis Theorem, see Lecture Notes.

2. The reduced Gröbner basis consists of

$$g_1 = y^3, \quad g_2 = xy + 3y^2, \quad g_3 = x^2.$$

Possible intermediate calculations:
Reduction:

$$g_3 := g_3 - 2yg_1 = x^3 - 2x^2y.$$

Composition:

$$g_4 := xg_1 - y^2 g_2 = -3y^4 + x^3.$$

Reductions:

$$g_4 := g_4 + 3yg_1 = x^3 + 3x^2y,$$

$$g_4 := g_4 - g_3 = 5x^2y, \quad g_4 := (1/5)g_4 = x^2y,$$

$$g_4 := g_4 - xg_2 = -3xy^2,$$

$$g_4 := g_4 + 3yg_2 = 9y^3,$$

$$g_4 := g_4 - 9g_1 = 9y^3,$$
$$g_4 := g_4 - 9g_1 = -9x^2, \quad g_4 := (1/9)g_4 = x^2,$$
$$g_3 := g_3 - xg_4 = -2x^2y, \quad g_3 := g_3 + 2yg_4 = 0.$$

We obtain the polynomials

$$g_1 = y^3 + x^2, \quad g_2 = xy + 3y^2, \quad g_4 := x^2.$$

No more reductions and compositions between the leading monomials of g_1, g_2, g_4 are possible, so the polynomials g_1, g_2, g_4 consitute a minimal Gröbner basis. After the additional reduction $g_1 := g_1 - g_3$, we obtain the reduced Gröbner basis.

3. One decomposition of ρ is

$$\rho = \tau_5\tau_4^{-1}\tau_3^{-1}\tau_2^{-1}\tau_1^{-1},$$

where

$$\tau_5 = (x - y, x), \quad \tau_4^{-1} = (x + y^2, y), \quad \tau_3^{-1} = (x, y + x),$$
$$\tau_2^{-1} = (x, y + 2x^2), \quad \tau_1^{-1} = (x + 2y, y).$$

Possible intermediate calculations:
Let $\rho = (f(x,y), g(x,y))$. Then $\overline{f(x,y)} = 2\overline{g(x,y)}$ and we define $\tau_1 = (x - 2y, y)$. Then

$$\rho\tau_1 = (f - 2g, g) = (f_1, g_1) = (x - y + x^2, 2x - y + 3x^2 - 4xy + 2y^2 + 4x^2(x - y) + 2x^4),$$

$\overline{g_1} = 2\overline{f_1}^2$, we define $\tau_2 = (x, y - 2x^2)$. Then

$$\rho\tau_1\tau_2 = (f_1, g_1 - 2f_1^2) = (f_2, g_2) = (x - y + x^2, 2x - y + x^2),$$

$\overline{f_2} = \overline{g_2}$, we fix $\tau_3 = (x, y - x)$,

$$\rho\tau_1\tau_2\tau_3 = (f_2, g_2 - f_2) = (f_3, g_3) = (x - y + x^2, x),$$

$\overline{f_3} = \overline{g_3}^2$, $\tau_4 = (x - y^2, y)$,

$$\tau_5 = \rho\tau_1\tau_2\tau_3\tau_4 = (f_3 - g_3^2, g_3) = (f_4, g_4) = (x - y, x),$$

and τ_5 is linear. Hence, we obtain

$$\rho\tau_1\tau_2\tau_3\tau_4 = \tau_5, \quad \rho = \tau_5\tau_4^{-1}\tau_3^{-1}\tau_2^{-1}\tau_1^{-1}.$$

Topics in Algebra

Questions for Final Examination on May 24, 2005

1. Let $X = \{x, y, z\}$. Define $[X] := \{x^a y^b z^c \mid a, b, c \geq 0\}$. A nonempty subset I of $[X]$ is called an ideal of $[X]$ if for every $u \in [X]$ and every $v \in I$, we have $uv \in I$.

(i) (15 points) Prove that every ideal of $[X]$ is finitely generated.

(ii) (10 points) For a fixed admissible order on $[X]$, let $\overline{f}$ be the leading monomial of the nonzero polynomial $f(X) \in K[X]$. Let J be a nonzero ideal of $K[X]$ and suppose that for some $f_1, \ldots, f_k \in J$, the monomials $\overline{f_1}, \ldots, \overline{f_k}$ generate the ideal $\overline{J}$ (which consists of the leading monomials of all polynomials in J) of $[X]$. Prove that the polynomials $f_1, \ldots, f_k$ generate the ideal J.

2. Let K be a field of characteristic zero. Define the automorphisms of $K[x, y, z, t]$

$$\rho = (x - 2ty - t^2 z, y + tz, z, t), \quad \sigma = (x, y, z, t + (y^2 + xz)).$$

(i) (5 points) Calculate $\rho(y^2 + xz)$;

(ii) (8 points) Find ρ^{-1} and σ^{-1};

(iii) (12 points) Find the composition $\tau = \sigma^{-1} \circ \rho^{-1} \circ \sigma \circ \rho$ (first apply ρ, then σ, etc.) in the form $\tau = (\tau(x), \tau(y), \tau(z), \tau(t))$. Besed on this, prove that the Nagata automorphism of $K[x, y, z]$ is stably tame.

Sketch of solutions

1. Basically it is the special case ($n = 3$) of the proof for the Hilbert Basis Theorem.

2. (i) $\rho(y^2 + xz) = y^2 + xz$.

(ii) $\rho^{-1} = (x + 2ty - t^2z, y + tz, z, t)$, $\sigma^{-1} = (x, y, z, t - (y^2 + xz))$.

(iii) Since $\rho(y^2 + xz) = y^2 + xz = \rho^{-1}(y^2 + xz)$, $\rho(z) = z = \rho^{-1}(z)$, $\rho(t) = t = \rho^{-1}(t)$, we obtain

$$\rho(x) = x - 2ty - t^2z, \quad \sigma(\rho(x)) = x - 2(t + (y^2 + xz))y - (t + (y^2 + xz))^2z,$$

$$\begin{aligned}\rho^{-1}(\sigma(\rho(x))) &= \rho^{-1}(x) - 2(t + (y^2 + xz))\rho^{-1}(y) - (t + (y^2 + xz))^2z \\ &= (x + 2ty - t^2z) - 2(t + (y^2 + xz))(y - tz) - (t + (y^2 + xz))^2z.\end{aligned}$$

Using that $t = \sigma^{-1}\sigma(t) = \sigma^{-1}(t + (y^2 + xz))$, we have

$$\begin{aligned}\sigma^{-1}(\rho^{-1}(\sigma(\rho(x)))) &= x + 2(t - (y^2 + xz))y - (t - (y^2 + xz))^2z - 2t(y - (t - (y^2 + xz))z) - t^2z \\ &= x - 2(y^2 + xz)y - (y^2 + xz)^2z = \tau(x).\end{aligned}$$

Similarly, we can obtain $\tau(y) = y + (y^2 + xz)z$; $\tau(z) = z$; $\tau(t) = t$. Therefore $\tau = (x - 2(y^2 + xz)y - (y^2 + xz)^2z, y + (y^2 + xz)z, z, t)$. Note that the first three components of τ is just the Nagata automorphism, hence the Nagata automorphism is stably tame as both ρ and σ are obviously elementary automorphisms.