

On reconstruction of polynomial automorphisms

by PAWEŁGNIADK (Kraków)

Abstract. We extend results on reconstructing a polynomial automorphism from its restriction to the coordinate hyperplanes to some wider class of algebraic surfaces. We show that the algorithm proposed by M. Kwieciński in [K2] and based on Gröbner bases works also for this class of surfaces.

1. Introduction. In [J1] Jelonek states the following definition.

DEFINITION 1.1. An algebraic subset X of \mathbb{k}^n is said to be an *identity set for polynomial automorphisms of \mathbb{k}^n* (an *identity set*, for short) iff the following implication holds: If $f, g : \mathbb{k}^n \rightarrow \mathbb{k}^n$ are polynomial automorphisms of \mathbb{k}^n which coincide on X , then $f = g$.

The class of identity sets has been well researched. For instance, it is known that in the case of $\mathbb{k} = \mathbb{C}$, a generic algebraic hypersurface of degree $d \geq n \geq 2$ in \mathbb{k}^n is an identity set ([J2]). The above definition implies that a polynomial automorphism is completely determined by its restriction to an identity set. Thus, the problem arises of finding an explicit formula for reconstructing the automorphism. The first paper in this field was the one by McKay and Wang [McK-W], where formulae were given to reconstruct the inverse of an automorphism in \mathbb{k}^2 from the restriction to the coordinate hyperplanes. However, analogous formulae in the case of $n > 2$ are not known. Instead, there are algorithmic methods—developed by A. van den Essen and M. Kwieciński—which work in higher dimensions. In [E-K], [K2] some algorithms were proposed based on the theory of Gröbner bases for reconstructing an automorphism from the restriction to the union of the coordinate hyperplanes for $n \geq 2$.

Our purpose is to extend those results to some greater class of algebraic subsets of \mathbb{k}^n . We will show that the algorithm used in [K2] for the set

1991 *Mathematics Subject Classification*: Primary 14Q20; Secondary 14E09, 13P10.

Key words and phrases: polynomial automorphisms, reconstruction of polynomial automorphisms, Gröbner bases.

This work was supported by the KBN Grant No. 2 P03A 061 08.

$V(X_1 \cdots X_n)$ can be applied to a more general class of algebraic sets—here called the *reconstructing sets*.

More precisely, define a partial ordering \sqsubseteq on \mathbb{N}^n as follows:

$$\alpha \sqsubseteq \beta \quad \text{iff} \quad \forall i = 1, \dots, n, \alpha_i \leq \beta_i.$$

Now, if a polynomial $P = \sum_{\alpha} c_{\alpha} X^{\alpha} \in \mathbb{k}[X_1, \dots, X_n]$ satisfies the following conditions:

- (1) there exists a greatest element $\alpha = (\alpha_1, \dots, \alpha_n)$ in $\text{supp } P = \{\alpha \in \mathbb{N}^n : c_{\alpha} \neq 0\}$ with respect to the ordering \sqsubseteq ,
- (2) $\alpha_i > 0$ for $i = 1, \dots, n$,

and V is an algebraic set of \mathbb{k}^n such that $I(V) = \langle P \rangle$ then the algorithm of Kwieciński also works for V , i.e. V is a reconstructing set.

In addition, we will show that if V is a reconstructing set, then so is any algebraic subset of \mathbb{k}^n containing V , as well as the image of V under any linear automorphism.

2. Preliminaries. In this paper \mathbb{k} denotes an infinite field.

We employ usual notations: $X = (X_1, \dots, X_n)$, $Y = (Y_1, \dots, Y_m)$ and $\mathbb{k}[X]$, $\mathbb{k}[Y]$, $\mathbb{k}[X, Y]$ are the rings of polynomials over \mathbb{k} in n , m , $n + m$ variables respectively. For any $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ we write $X^{\alpha} = X^{\alpha_1} \cdots X^{\alpha_n}$.

All ideals considered are ideals in polynomial rings over \mathbb{k} . For any P_1, \dots, P_r in $\mathbb{k}[X]$ we denote by $\langle P_1, \dots, P_r \rangle$ the ideal in $\mathbb{k}[X]$ generated by P_1, \dots, P_r . If V is an algebraic subset in \mathbb{k}^n then $I(V)$ denotes the ideal in $\mathbb{k}[X]$ consisting of the polynomials vanishing on V . If S is a subset of $\mathbb{k}[X]$, we write $V(S)$ for the set of common zeros in \mathbb{k}^n of the polynomials in S .

Let us start with recalling the basic facts about Gröbner bases which we will need further (an outline of the theory may be found e.g. in [B], [L-J], [P-P] or [W]).

DEFINITION 2.1. A total ordering “ $<$ ” on the set \mathbb{N}^n is called *admissible* if the following conditions are satisfied:

- (1) $\forall \alpha \in \mathbb{N}^n \setminus \{0\}, 0 < \alpha$,
- (2) $\forall \alpha, \beta, \gamma \in \mathbb{N}^n, \alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$.

An admissible ordering on the set \mathbb{N}^n induces an ordering on the set of monomials in $\mathbb{k}[X_1, \dots, X_n]$ via the natural correspondence

$$\mathbb{N}^n \ni \alpha = (\alpha_1, \dots, \alpha_n) \mapsto X^{\alpha} = X^{\alpha_1} \cdots X^{\alpha_n} \in \mathbb{k}[X].$$

We will sometimes write $X^{\alpha} < X^{\beta}$ when $\alpha < \beta$.

For any fixed nonzero polynomial $P = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha \in \mathbb{k}[X]$ we define the *support* of P to be

$$\text{supp } P = \{\alpha \in \mathbb{N}^n : c_\alpha \neq 0\}.$$

Let us fix an admissible ordering on \mathbb{N}^n . Then for $P \neq 0$ we define

$$\text{exp } P = \max \text{supp } P, \quad \text{lt } P = c_{\text{exp } P}, \quad \text{in } P = \text{lt } P X^{\text{exp } P},$$

and for a subset $A \subset \mathbb{k}[X]$ we write

$$\text{exp } A = \{\text{exp } P : P \in A\}, \quad \text{in } A = \{\text{in } P : P \in A\}.$$

DEFINITION 2.2. A finite system of polynomials $\mathcal{B} = \{G_1, \dots, G_r\} \subset \mathbb{k}[X]$ is a *Gröbner basis* of the ideal $I \subset \mathbb{k}[X]$ with respect to the fixed admissible ordering iff the following conditions hold:

- (1) $\mathcal{B} \subset I$,
- (2) $\langle \text{in } I \rangle = \langle \text{in } \mathcal{B} \rangle$.

It is known that for any admissible ordering on \mathbb{N}^n and for any nonzero ideal of $\mathbb{k}[X]$ there exists a Gröbner basis. However, it is not unique. Thus, in applications we often use *reduced* Gröbner bases.

DEFINITION 2.3. Fix an admissible ordering on \mathbb{N}^n . Let P, Q be polynomials in $\mathbb{k}[X]$, and A an arbitrary subset of $\mathbb{k}[X]$.

- (1) We say that the polynomial P is *reduced modulo* Q if $\text{lt } P = 1$ and no term appearing in P with nonzero coefficient is divisible by $\text{in } Q$.
- (2) The polynomial P is *reduced modulo* A if P is reduced modulo every polynomial Q in A .
- (3) We say that a Gröbner basis $\mathcal{B} = \{G_1, \dots, G_r\}$ is *reduced* if every polynomial G_i is reduced modulo G_j for every $j \neq i$.

The reduced Gröbner basis is uniquely determined for any nonzero ideal in $\mathbb{k}[X]$ (assuming that we have fixed an admissible ordering). We emphasize that there exists an algorithm for calculating the reduced Gröbner basis of an ideal from a finite set of its generators. The algorithm consists of a finite number of rational operations on coefficients of the generators.

Remark 2.4. From the definition of the reduced Gröbner basis it follows immediately that, if \mathcal{B} is a Gröbner basis of I , then P is reduced modulo I iff P is reduced modulo every element of \mathcal{B} .

We also need a special type of admissible ordering.

DEFINITION 2.5. We say that an admissible ordering on \mathbb{N}^{n+m} *n-separates the variables* X, Y if $X^\alpha > Y^\beta$ for all $\alpha \in \mathbb{N}^n \setminus \{0\}$, $\beta \in \mathbb{N}^n$.

A simple example of a separating ordering is the lexicographic ordering in \mathbb{N}^{n+m} .

We recall a theorem proved by M. Kwieciński (a particular version was proved earlier by van den Essen [E]) which plays a fundamental role in our proofs.

THEOREM 2.6 [K1]. *Let $F = (F_1, \dots, F_n) : \mathbb{k}^n \rightarrow \mathbb{k}^m$ be a polynomial mapping, V a nonempty algebraic subset of \mathbb{k}^n and $P_1(X), \dots, P_s(X)$ a system of generators of the ideal $I(V)$. Let \mathcal{B} be the reduced Gröbner basis of the ideal $J = \langle Y_1 - F_1(X), \dots, Y_n - F_n(X), P_1(X), \dots, P_s(X) \rangle$ with respect to some admissible ordering in \mathbb{N}^{n+m} which n -separates the variables X, Y . Then $F|_V : V \rightarrow \overline{F(V)}$ is an isomorphism iff $\mathcal{B} = \mathcal{B}_{\text{inv}} \cup \mathcal{B}_{\text{im}}$, where $\mathcal{B}_{\text{inv}} = \{X_1 - G_1(Y), \dots, X_n - G_n(Y)\}$ for some $G_i \in \mathbb{k}[Y]$ and $\mathcal{B}_{\text{im}} = \emptyset$ or $\mathcal{B}_{\text{im}} = \{Q_1(Y), \dots, Q_r(Y)\}$ for some $Q_i \in \mathbb{k}[Y]$. In that case \mathcal{B}_{im} is the reduced Gröbner basis of $I(\overline{F(V)})$ and G_i are the coordinates of the inverse.*

Note that the theorem gives an effective way of determining whether a given polynomial mapping is invertible and then computing its inverse.

3. Reconstructing sets. Assume that V is an algebraic subset of \mathbb{k}^n , $P_1(X), \dots, P_s(X)$ are generators of the ideal $I(V)$ and $F = (F_1, \dots, F_n) : \mathbb{k}^n \rightarrow \mathbb{k}^n$ is a polynomial automorphism. Suppose also $\tilde{F} = (\tilde{F}_1, \dots, \tilde{F}_n) : \mathbb{k}^n \rightarrow \mathbb{k}^n$ is a polynomial mapping (not necessarily an automorphism) which coincides with F on V . Now, let $I_{\tilde{F}|_V}$ be the ideal of the graph of \tilde{F} restricted to V , i.e.

$$I_{\tilde{F}|_V} = \langle Y_1 - \tilde{F}_1(X), \dots, Y_n - \tilde{F}_n(X), P_1(X), \dots, P_s(X) \rangle,$$

and fix an admissible ordering in \mathbb{N}^{2n} n -separating the variables X, Y . Since $\tilde{F}(V)$ is an algebraic set and $\tilde{F}|_V : V \rightarrow \tilde{F}(V)$ is an isomorphism, by Theorem 2.6 the reduced Gröbner basis of the ideal $I_{\tilde{F}|_V}$ is of the form

$$\mathcal{B} = \{X_1 - \tilde{G}_1(Y), \dots, X_n - \tilde{G}_n(Y), Q_1(Y), \dots, Q_r(Y)\},$$

where $\{Q_1(Y), \dots, Q_r(Y)\}$ is the reduced Gröbner basis of $I(\tilde{F}(V))$ and the mapping $\tilde{G} = (\tilde{G}_1, \dots, \tilde{G}_n)$ restricted to $\tilde{F}(V)$ is the inverse of $\tilde{F}|_V$. However, \tilde{G} is not necessarily equal to the inverse of F . Therefore we introduce the following

DEFINITION 3.1. An algebraic subset V of \mathbb{k}^n is said to be a *reconstructing set* if for any admissible ordering on \mathbb{N}^{2n} which n -separates the variables X, Y , for any polynomial automorphism F and for any polynomial mapping \tilde{F} such that $\tilde{F}|_V = F|_V$, the mapping \tilde{G} is the inverse of F .

Remark 3.2. For any reconstructing set we can compute the inverse of the automorphism F , knowing only the mapping \tilde{F} . In order to do this we use the following algorithm (see [K2]).

(1) Compute the reduced Gröbner basis \mathcal{B} of the ideal $I|_{\tilde{F}|V}$ with respect to any admissible ordering on \mathbb{N}^{2n} which n -separates the variables X, Y . The basis has the form

$$\mathcal{B} = \{X_1 - \tilde{G}_1(Y), \dots, X_n - \tilde{G}_n(Y), Q_1(Y), \dots, Q_r(Y)\},$$

where, by Definition 3.1, $\tilde{G} = (\tilde{G}_1, \dots, \tilde{G}_n)$ is the inverse of F .

(2) Compute the reduced Gröbner basis \mathcal{B}' of the ideal

$$I_{\tilde{G}} = \{X_1 - \tilde{G}_1(Y), \dots, X_n - \tilde{G}_n(Y)\}$$

with respect to any admissible ordering n -separating the variables Y, X . Since $\tilde{G} = F^{-1}$, by Theorem 2.6 we have

$$\mathcal{B}' = \{Y_1 - F_1(X), \dots, Y_n - F_n(X)\}.$$

The algorithm calculates F using two Gröbner bases computations.

Let us notice that the mapping \tilde{F} appearing in Definition 3.1 is superfluous. Since the reduced Gröbner basis of an ideal does not depend on the choice of generators and since $I_{F|V} = I_{\tilde{F}|V}$, we can reformulate the definition in the following way.

DEFINITION 3.1. An algebraic subset V of \mathbb{k}^n is said to be a *reconstructing set* if for any ordering on \mathbb{N}^{2n} which n -separates the variables X, Y and for any polynomial automorphism F , the mapping \tilde{G} determined from the reduced Gröbner basis of the ideal $I_{F|V}$ is the inverse of F .

Remark 3.3. Every reconstructing set is an identity set.

To show this, take two polynomial automorphisms f_1, f_2 which coincide on a reconstructing set V . Notice that according to the definition of a reconstructing set, the automorphism \tilde{g}_1 calculated from the Gröbner basis of the ideal $I_{f_1|V}$ is the inverse of f_1 . The same argument applies to f_2 and we get its inverse \tilde{g}_2 . On the other hand, the ideals $I_{f_1|V}$ and $I_{f_2|V}$ are equal, thus $\tilde{g}_1 = \tilde{g}_2$ and consequently $f_1 = f_2$.

Kwieciński proved in [K2] that the set $V(X_1 \cdots X_n)$ is a reconstructing set. Now, we find other examples of reconstructing sets.

LEMMA 3.4. Fix an admissible ordering in \mathbb{N}^n and let $P, G_1, \dots, G_n \in \mathbb{k}[X]$ be such that

- (1) $\exp G_i > 0$ for $i = 1, \dots, n$,
- (2) there exists a greatest element in $\text{supp } P$ with respect to the ordering \sqsubseteq ,
- (3) $(1, \dots, 1) \sqsubseteq \exp P$.

Then G_i is reduced modulo $Q := P(G_1, \dots, G_n)$ for $i = 1, \dots, n$.

Proof. Let α be the greatest element of $\text{supp } P$. Of course, $\alpha = \exp P$. Then

$$P(X) = c_\alpha X^\alpha + \sum_{\beta < \alpha} c_\beta X^\beta$$

and

$$Q = P(G_1, \dots, G_n) = c_\alpha G_1^{\alpha_1} \dots G_n^{\alpha_n} + \sum_{\beta < \alpha} c_\beta G^\beta.$$

Since $\exp G_i > 0$,

$$\exp(c_\beta G^\beta) = \sum_{i=1}^n \beta_i \exp G_i < \sum_{i=1}^n \alpha_i \exp G_i = \exp(c_\alpha G^\alpha) \quad \text{for } \beta \sqsubset \alpha.$$

Therefore,

$$\exp Q = \exp(c_\alpha G_1^{\alpha_1} \dots G_n^{\alpha_n}) = \sum_{i=1}^n \alpha_i \exp G_i.$$

Using the fact that $\alpha_i \geq 1$ and $\exp G_i > 0$, we get $\exp Q > \exp G_i$, which implies that G_i is reduced modulo Q . ■

THEOREM 3.5. *Let V be an algebraic subset of \mathbb{k}^n such that $I(V) = \langle P \rangle$, where $P \in \mathbb{k}[X]$ satisfies the following conditions:*

- (1) *there exists a greatest element in $\text{supp } P$ with respect to the ordering \sqsubseteq ,*
- (2) *$(1, \dots, 1) \sqsubseteq \exp P$.*

Then V is a reconstructing set.

Proof. Fix an admissible ordering on \mathbb{N}^{2n} which n -separates X, Y , and a polynomial automorphism $F : \mathbb{k}^n \rightarrow \mathbb{k}^n$. We shall denote by $G = (G_1, \dots, G_n)$ the inverse of F . From Theorem 2.6 we know that the reduced Gröbner basis of the ideal $I_{F|V}$ has the form

$$\mathcal{B} = \{X_1 - \tilde{G}_1(Y), \dots, X_n - \tilde{G}_n(Y), Q(Y)\}, \quad \tilde{G}_i, Q \in \mathbb{k}[Y].$$

(Here we have used the fact that the Gröbner basis of a principal ideal has only one element, so \mathcal{B}_{im} in Theorem 2.6 consists of exactly one polynomial.)

Moreover, $\tilde{G}|_{F(V)} = (\tilde{G}_1, \dots, \tilde{G}_n)|_{F(V)}$ is the inverse of $F|_V$. Thus G has to coincide on $F(V)$ with \tilde{G} , and so

$$(*) \quad G_i(Y) - \tilde{G}_i(Y) \in I(F(V)), \quad i = 1, \dots, n.$$

Since $I(F(V)) = \langle Q(Y) \rangle$ and \mathcal{B} is the reduced basis, all $\tilde{G}_i(Y)$ must be reduced modulo $Q(Y)$. Observe that the ideal $I(F(V))$ is generated by $P(G_1(Y), \dots, G_n(Y))$. Thus, there exists $c \in \mathbb{k} - \{0\}$ such that $Q(Y) = c \cdot P(G_1(X), \dots, G_n(X))$ and Lemma 3.4 implies that $G_i(Y)$ is also reduced

modulo $Q(Y)$ for $i = 1, \dots, n$. So $G_i(Y) - \tilde{G}_i(Y)$ is reduced modulo $Q(Y)$ and from (*) we have $G_i(Y) = \tilde{G}_i(Y)$. ■

The following two propositions show some properties of the family of all reconstructing sets.

PROPOSITION 3.6. *Let V and W be algebraic subsets of \mathbb{k}^n such that $V \subset W$. If V is a reconstructing set, then so is W .*

PROOF. Choose an admissible ordering on \mathbb{N}^{2n} which n -separates the variables X, Y , and a polynomial automorphism $F : \mathbb{k}^n \rightarrow \mathbb{k}^n$. Denote by \mathcal{B}_V and \mathcal{B}_W the reduced Gröbner bases of $I_{F|V}$ and $I_{F|W}$ respectively. From Theorem 2.6 and the definition of a reconstructing set we have

$$\begin{aligned}\mathcal{B}_V &= \{X_1 - G_1(Y), \dots, X_n - G_n(Y), Q_1(Y), \dots, Q_s(Y)\}, \\ \mathcal{B}_W &= \{X_1 - \tilde{G}_1(Y), \dots, X_n - \tilde{G}_n(Y), R_1(Y), \dots, R_t(Y)\},\end{aligned}$$

where $G = (G_1, \dots, G_n)$ is the inverse of F . Since $(\tilde{G}_1, \dots, \tilde{G}_n)|_{F(W)}$ is the inverse of $F|_W$, we have

$$\tilde{G}_i(Y) - G_i(Y) \in I(F(W)) = \langle R_1(Y), \dots, R_t(Y) \rangle \quad \text{for } i = 1, \dots, n.$$

By definition of the reduced basis, $\tilde{G}_i(Y)$ is reduced modulo $R_j(Y)$ ($j = 1, \dots, t$). Therefore, it is reduced modulo the ideal $I(F(W))$. Similarly, $G_i(Y)$ is reduced modulo $I(F(V))$. But $I(F(V)) \supset I(F(W))$, so G_i is reduced modulo $I(F(W))$. Thus, $G_i(Y) = \tilde{G}_i(Y)$ for $i = 1, \dots, n$, which completes the proof. ■

PROPOSITION 3.7. *Let V be a reconstructing subset of \mathbb{k}^n and let $\varphi : \mathbb{k}^n \rightarrow \mathbb{k}^n$ be a linear automorphism. Then $\varphi(V)$ is a reconstructing set.*

PROOF. Take an admissible ordering on \mathbb{N}^{2n} which n -separates the variables X, Y , and a polynomial automorphism $F : \mathbb{k}^n \rightarrow \mathbb{k}^n$, and let \mathcal{B} be the reduced Gröbner basis of the ideal $I_{F|\varphi(V)}$. As before we have

$$\mathcal{B} = \{X_1 - \tilde{G}_1(Y), \dots, X_n - \tilde{G}_n(Y), Q_1(Y), \dots, Q_s(Y)\}.$$

Denoting by $G = (G_1, \dots, G_n)$ the inverse of F , we have to show that $G_i(Y)$ is reduced modulo $I(F(\varphi(V)))$ for $i = 1, \dots, n$.

In order to prove that, consider the set V and the automorphism $F \circ \varphi$. Since V is a reconstructing set, we have

$$\mathcal{B}' = \{X_1 - (\psi_1 \circ G)(Y), \dots, X_n - (\psi_n \circ G)(Y), Q_1(Y), \dots, Q_s(Y)\},$$

where \mathcal{B}' denotes the reduced Gröbner basis of $I_{F \circ \varphi|V}$ and $\psi = \varphi^{-1}$.

Because $X_i - G_i(Y)$ is a linear combination of the polynomials $X_j - (\psi_j \circ G)(Y)$, we deduce that $X_i - G_i(Y)$ is also reduced modulo the ideal $\langle Q_1(Y), \dots, Q_s(Y) \rangle$. Using the same argument as before we see that $\tilde{G}_i = G_i$. ■

EXAMPLE 3.8 ⁽¹⁾. We construct an identity set which is not a reconstructing set. We also show that the image of a reconstructing set under an algebraic automorphism is not always a reconstructing set.

Let $P(X, Y) = (Y - X^2)(X + X^2 - Y)$. To show that $V = V(P)$ is not a reconstructing set, take $F(X, Y) = (X^2 + X - Y, Y - X^2)$. The inverse of F is of the form $G(Z, T) = (Z + T, (Z + T)^2 + T)$. Denoting by W the F -image of V , one can easily see that $I(W) = \langle Z \cdot T \rangle$. Let \mathcal{B} be the reduced Gröbner basis in an admissible ordering on \mathbb{N}^4 2-separating the variables XY and ZT . Then

$$\mathcal{B} = \{X - \tilde{G}_1(Z, T), Y - \tilde{G}_2(Z, T), Z \cdot T\}$$

and $\tilde{G}_2(Z, T)$ is reduced modulo $Z \cdot T$. But $G_2(Z, T) = Z^2 + 2ZT + T^2 + T$ is not reduced modulo $Z \cdot T$, thus $\tilde{G}_2 \neq G_2$. This implies that V is not a reconstructing set. However, V is an identity set because it is the image of $V(Z \cdot T)$ under a polynomial automorphism.

One can also notice that V is an image of a reconstructing set $V(Z \cdot T)$. Thus, the image of a reconstructing set under an algebraic automorphism is not necessarily a reconstructing set.

Acknowledgements. The author is extremely grateful to Professor T. Winiarski for suggesting the problem and many helpful discussions.

References

- [A-E] K. Adjamagbo and A. van den Essen, *A resultant criterion and formula for the inversion of a polynomial map in two variables*, J. Pure Appl. Algebra 64 (1990), 1–6.
- [E] A. van den Essen, *A criterion to decide if a polynomial map is invertible and to compute the inverse*, Comm. Algebra 18 (1990), 3183–3186.
- [E-K] A. van den Essen and M. Kwieciński, *On the reconstruction of polynomial automorphisms from their face polynomials*, J. Pure Appl. Algebra 80 (1992), 327–336.
- [B] B. Buchberger, *Gröbner bases: An algorithmic method in polynomial ideal theory*, in: Multidimensional Systems Theory, N. Bose (ed.), Reidel, Dordrecht, 1985, 164–232.
- [J1] Z. Jelonek, *Identity sets for polynomial automorphisms*, J. Pure Appl. Algebra 76 (1991), 333–337.
- [J2] —, *Irreducible identity sets for polynomial automorphisms*, Math. Z. 212 (1993), 601–617.
- [K1] M. Kwieciński, *A Gröbner basis criterion for isomorphisms of algebraic varieties*, J. Pure Appl. Algebra 74 (1991), 275–279.
- [K2] —, *Automorphisms from face polynomials via two Gröbner bases*, ibid. 82 (1992), 65–70.

⁽¹⁾ The example is due to M. Kwieciński.

- [L-J] M. Lejeune-Jalabert, *Effectivité de Calculs Polynomiaux*, Cours de D.E.A., Univ. de Grenoble, 1986.
- [McK-W] J. McKay and S. Wang, *An inversion formula for two polynomials in two variables*, J. Pure Appl. Algebra 52 (1988), 103–119.
- [P-P] F. Pauer and M. Pheifhofer, *The theory of Gröbner bases*, Enseign. Math. 34 (1988), 215–232.
- [W] T. Winiarski, *Application of Gröbner bases in the theory of polynomial mappings*, XIV Instructional Conf. in the Theory of Extremal Problems, Łódź Univ., 1993 (in Polish).

Institute of Mathematics
Jagiellonian University
Reymonta 4
30-059 Kraków, Poland
E-mail: gniadek@im.uj.edu.pl

Reçu par la Rédaction le 27.2.1995
Révisé le 5.6.1995