PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 2, February 1995

A PRODUCT FORMULA FOR MINIMAL POLYNOMIALS AND DEGREE BOUNDS FOR INVERSES OF POLYNOMIAL AUTOMORPHISMS

JIE-TAI YU

(Communicated by Wolmer V. Vasconcelos)

ABSTRACT. By means of Galois theory, we give a product formula for the minimal polynomial G of $\{f_0, f_1, \dots, f_n\} \subset K[x_1, \dots, x_n]$ which contains n algebraically independent elements, where K is a field of characteristic zero. As an application of the product formula, we give a simple proof of Gabber's degree bound inequality for the inverse of a polynomial automorphism.

0. INTRODUCTION

Let K be a field, and let $\{f_0, \dots, f_n\} \subset K[x_1, \dots, x_n]$ contain n algebraically independent polynomials over K. Then there is a unique irreducible polynomial (up to a constant factor in K^*) $G(y_0, \dots, y_n) \in K[y_1, \dots, y_n]$ such that $G(f_0, \dots, f_n) = 0$. We call this G the minimal polynomial of $f_0, \dots, f_n$ over K. It can be viewed as a natural generalization of the minimal polynomial of an algebraic element over a field K. Minimal polynomials are very useful for studying polynomial automorphisms, as well as birational maps. See, for instance, Yu [11, 12] and Li and Yu [3, 4]. In [3] and [12], two different effective algorithms for computing minimal polynomials are given, by means of Gröbner bases and Generalized Characteristic Polynomials (GCP), respectively.

The following theorem is well known.

Theorem 0.1. *Let α be algebraic over a field K and $m_\alpha(x)$ be the minimal polynomial of α over K. Then*

$$m_\alpha(x) = \prod_{i=1}^{d}(x - \alpha^{(i)}),$$

where $\alpha^{(1)}, \dots, \alpha^{(d)}$ are all roots of the polynomial $m_\alpha(x)$ in the algebraic closure of $K(\alpha)$ and $\deg(m_\alpha(x)) = d$, the number of roots of $m_\alpha(x)$. $\square$

Received by the editors December 22, 1992 and, in revised form, May 5, 1993; presented at AMS Special Session Geometry of Affine Space, Springfield, MO, March 20–21, 1992.

1991 *Mathematics Subject Classification.* Primary 12E05, 12F05, 12Y05, 13B05.

Key words and phrases. Minimal polynomials, Galois theory, product formula, polynomial automorphisms.

One can ask a natural question: Can Theorem 0.1 be generalized to higher-dimension cases?

The answer is affirmative. In this paper, by means of Galois theory, we give a product formula for the above minimal polynomial G of $f_0, \ldots, f_n$.

1. Statement of the main theorem

Theorem 1.1. *Let K be a field of characteristic zero, and let*

$$\{f_0, f_1, \ldots, f_n\} \subset K[x_1, \ldots, x_n]$$

with $f_1, \ldots, f_n$ algebraically independent over K. Let

$$q := [K(x_1, \ldots, x_n) : K(f_0, \ldots, f_n)]$$

and $G(y_0, \ldots, y_n)$ be the minimal polynomial of $f_0, \ldots, f_n$. Then

(i)

$$c[G(y_0, \ldots, y_n)]^q = D \prod_{i=1}^{d} (y_0 - f_0(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})),$$

where $c \in K^*$, $(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})$, $i = 1, \ldots, d$, are all solutions of the system of equations $f_i(x_1, \ldots, x_n) = y_i$, $i = 1, \ldots, n$, in the algebraic closure of the field $K(y_1, \ldots, y_n)$; $y_1, \ldots, y_n$ are algebraically independent transcendentals over K; and $D \in K[y_1, \ldots, y_n]$ is the unique minimal denominator (up to a constant factor in K^*) of the product $\prod_{i=1}^{d}(y_0 - f_0(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})) \in K(y_1, \ldots, y_n)[y_0]$.

(ii) *The partial degrees of G, $\deg_{y_i}(G) = d_i/q$, where d_i is the number of solutions of the system of equations $f_j(x_1, \ldots, x_n) - y_j$, $j = 0, \ldots, i-1, i+1, \ldots, n$, in the algebraic closure of $K(y_1, \ldots, y_n)$. If $d_i > 0$, then*

$$d_i = [K(x_1, \ldots, x_n) : K(f_0, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)].$$

(iii) *The total degree of G,*

$$\deg(G) \le \frac{1}{q} \max \left\{ \prod_{i \ne j} \deg(f_i) \right\}.$$

Moreover, if for some k, $\deg(f_k) = \min_i\{\deg(f_i)\}$, and $f_0, \ldots, f_{k-1}, f_{k+1}, \ldots, f_n$ are algebraically independent over K and the system of equations $f_i^+ = 0$, $i = 0, \ldots, k-1, k+1, \ldots, n$, has only the trivial solution, where f^+ is the highest homogeneous form of f, then the equality holds.

2. Proof of the main theorem

To prove Theorem 1.1, we need some lemmas.

Lemma 2.1 (Mumford [6]). *Let K be a field of characteristic zero and let $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$ be algebraically independent over K. Then $\frac{K(x_1, \ldots, x_n)}{K(f_1, \ldots, f_n)}$ is a finite algebraic field extension. Let $d := [K(x_1, \ldots, x_n) : K(f_1, \ldots, f_n)]$. Then the system of equations*

$$\begin{cases} f_1(x_1, \ldots, x_n) = y_1 \\ \qquad\vdots \\ f_n(x_1, \ldots, x_n) = y_n \end{cases}$$

has precisely d *distinct solutions in the algebraic closure of the field* $K(y_1, \dots, y_n)$, *where* $y_1, \dots, y_n$ *are algebraically independent transcendentals over* K. *Moreover, if the system of equations*

$$\begin{cases} f_1^+(x_1, \dots, x_n) = 0 \\ \qquad\qquad\vdots \\ f_n^+(x_1, \dots, x_n) = 0 \end{cases}$$

has only trivial solutions in the algebraic closure of K, *then* $d = \prod_{i=1}^n \deg(f_i)$. □

The next lemma is the key lemma in this paper. It has its own interests.

Lemma 2.2. *Let* K *be a field of characteristic zero and let* $f_1, \dots, f_n \in K[x_1, \dots, x_n]$ *be algebraically independent over* K. *Let* $(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})$, $i = 1, \dots, d$, *be all solutions of the system of equations*

$$\begin{cases} f_1(x_1, \dots, x_n) = y_1 \\ \qquad\qquad\vdots \\ f_n(x_1, \dots, x_n) = y_n \end{cases}$$

in the algebraic closure of $K(y_1, \dots, y_n)$, *and let*

$$E := K(\alpha_1^{(1)}, \dots, \alpha_n^{(1)}, \dots, \alpha_1^{(d)}, \dots, \alpha_n^{(d)}).$$

Then $\frac{E}{K(y_1, \dots, y_n)}$ *is a Galois extension and the Galois group*

$$G := \mathrm{Gal}\left(\frac{E}{K(y_1, \dots, y_n)}\right)$$

acts transitively on the set $\{(\alpha_1^{(i)}, \dots, \alpha_n^{(i)}) \mid i = 1, \dots, d\}$.

Proof. First observe that

$$\frac{K(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})}{K(y_1, \dots, y_n)} \cong \frac{K(x_1, \dots, x_n)}{K(f_1, \dots, f_n)}, \qquad i = 1, \dots, d.$$

Hence

$$\frac{K(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})}{K(y_1, \dots, y_n)} \cong \frac{K(\alpha_1^{(1)}, \dots, \alpha_n^{(1)})}{K(y_1, \dots, y_n)}, \qquad i = 1, \dots, d.$$

Define

$$\sigma_i\colon K(\alpha_1^{(1)}, \dots, \alpha_n^{(1)}) \to K(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})$$

as follows: $\sigma_i(\alpha_k^{(1)}) = \alpha_k^{(i)}$, $k = 1, \dots, d$, and $\sigma_i|_K$ is the identity map of K. Then linearly extend σ to $K(\alpha_1^{(1)}, \dots, \alpha_n^{(1)})$. Obviously $\sigma_i(y_k) = y_i$, $k = 1, \dots, n$. Hence σ_i is a $K(y_1, \dots, y_n)$-isomorphism. Since

$$[K(\alpha_1^{(1)}, \dots, \alpha_n^{(1)}) : K(y_1, \dots, y_n)] = [K(x_1, \dots, x_n) : K(f_1, \dots, f_n)] = d,$$

there are precise $dK(y_1, \dots, y_n)$-isomorphisms in a fixed algebraic closure of

$$K(\alpha_1^{(1)}, \dots, \alpha_n^{(1)}).$$

Hence σ_i, $i=1, \dots, d$, are all such $dK(y_1, \dots, y_n)$-isomorphisms. Now let θ_1 be a primitive element of $K(\alpha_1^{(1)}, \dots, \alpha_n^{(1)})$ over $K(y_1, \dots, y_n)$; then

$$K(\alpha_1^{(1)}, \dots, \alpha_n^{(1)}) = K(y_1, \dots, y_n)(\theta_1).$$

Therefore,

$$\alpha_k^{(1)} = g_k(\theta_1), \qquad k=1, \dots, n;\ g_k(x) \in K(y_1, \dots, y_n)(x).$$

Let $\theta_i := \sigma_i(\theta_1)$. Then

$$\alpha_k^{(i)} = \sigma_i(\alpha_k^{(1)}) = \sigma_i(g_k(\theta_1)) = g_k(\sigma_i(\theta_1)) = g_k(\theta_i),$$
$$k=1, \dots, n;\ i=1, \dots, d.$$

Hence θ_i is a primitive element of $K(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})$ over $K(y_1, \dots, y_n)$. Let $m(x)$ be the minimal polynomial of θ_1 over $K(y_1, \dots, y_n)$. Then $m(\theta_i) = m(\sigma_i(\theta_1)) = \sigma_i(m(\theta_1)) = 0$. In other words, θ_i, $i=1, \dots, d$, are all conjugates of θ_1 over $K(y_1, \dots, y_n)$. Thus $m(x) = \prod_{i=1}^d (x-\theta_i)$. Hence $E = K(\theta_1, \dots, \theta_d)$ is the splitting field of $m(x)$ over $K(y_1, \dots, y_n)$. By Galois theory, $\frac{E}{K(y_1, \dots, y_n)}$ is a Galois extension and the Galois group G acts transitively on $\{\theta_1, \dots, \theta_d\}$, hence acts transitively on $\{\alpha_1^{(i)}, \dots, \alpha_n^{(i)} \mid i=1, \dots, d\}$. $\square$

Proof of Theorem 1.1. We use the same notation as in Lemma 2.2 and its proof.

(i) $\forall \sigma \in G$,

$$\sigma\left(\prod_{i=1}^d (y_0 - f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)}))\right) = \prod_{i=1}^d (y_0 - f_0(\sigma(\alpha_1^{(i)}), \dots, \sigma(\alpha_n^{(i)})))$$
$$= \prod_{i=1}^d (y_0 - f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})),$$

by the transitivity of G. Hence

$$\prod_{i=1}^d (y_0 - f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})) \in K[y_0](y_1, \dots, y_n).$$

Denote by D its minimal denominator in $K[y_1, \dots, y_n]$. Let

$$h(y_0, \dots, y_n) \in K(y_1, \dots, y_n)[y_0]$$

be the unique minimal polynomial of $f_0(\alpha_1^{(1)}, \dots, \alpha_n^{(1)})$ over $K(y_1, \dots, y_n)$ such that h is an irreducible polynomial in $K[y_0, \dots, y_n]$ (up to a constant factor in K^*). Then

$$h(f_0(\sigma(\alpha_1^{(1)}), \dots, \sigma(\alpha_n^{(1)}))) = h(\sigma(f_0(\alpha_1^{(1)}, \dots, \alpha_n^{(1)})))$$
$$= \sigma(h(f_0(\alpha_1^{(1)}, \dots, \alpha_n^{(1)}))) = 0, \quad \forall \sigma \in G.$$

Hence

$$h(f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})) = 0, \qquad i=1, \dots, d.$$

This means that $f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})$, $i=1, \dots, d$, have the same minimal polynomial over $K(y_1, \dots, y_n)$ which is an irreducible polynomial in $K[y_0, \dots, y_n]$, namely, $h(y_0, \dots, y_n)$. Now let $G(y_0, \dots, y_n)$ be an irreducible factor of

$D\prod_{i=1}^{d}(y_0 - f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)}))$ in $K[y_0, \dots, y_n]$. Then G is also irreducible in $K(y_1, \dots, y_n)[y_0]$ by Gauss Lemma. Hence essentially G and h are the same (up to a constant factor in K^*). Thus

$$c[G(y_0, \dots, y_n)]^q = D\prod_{i=1}^{d}(y_0 - f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})), \qquad c \in K^*.$$

To show $q = [K(x_1, \dots, x_n) : K(f_0, \dots, f_n)]$, note that

$$\begin{aligned}[K(x_1, \dots, x_n) &: K(f_0, \dots, f_n)][K(f_0, \dots, f_n) : K(f_1, \dots, f_n)] \\ &= [K(x_1, \dots, x_n) : K(f_1, \dots, f_n)] = d.\end{aligned}$$

On the other hand, since the system of equations

$$\begin{aligned} f_0(t_1, \dots, t_n) &= f_0(x_1, \dots, x_n) \\ f_1(t_1, \dots, t_n) &= f_1(x_1, \dots, x_n) \\ &\vdots \\ f_n(t_1, \dots, t_n) &= f_n(x_1, \dots, x_n) \end{aligned}$$

has a solution $t_i = x_i$, $i = 1, \dots, n$, it follows that

$$G(f_0(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)) = 0.$$

Therefore, $G(y_0, \dots, y_n)$ is the minimal polynomial of $f_0, \dots, f_n$. Moreover, $G(y_0, f_1, \dots, f_n)$ is the irreducible polynomial in $K(f_1, \dots, f_n)[y_0]$, since f_i, $i = 1, \dots, n$, are transcendentals over K. Hence $G(y_0, f_1, \dots, f_n)$ is the minimal polynomial of f_0 over $K(f_1, \dots, f_n)$. Hence

$$\begin{aligned} q &= \frac{\deg_{y_0}(D\prod_{i=1}^{d}(y_0 - f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)})))}{\deg_{y_0}(G(y_0, \dots, y_n))} \\ &= \frac{[K(x_1, \dots, x_n) : K(f_1, \dots, f_n)]}{[K(f_0, f_1, \dots, f_n) : K(f_1, \dots, f_n)]} \\ &= [K(x_1, \dots, x_n) : K(f_0, f_1, \dots, f_n)]. \end{aligned}$$

(ii) If $d_i > 0$, then

$$d_i = [K(x_1, \dots, x_n) : K(f_0, \dots, f_{i-1}, f_{i+1}, \dots, f_n)]$$

by Lemma 2.1. By (i), $\deg_{y_i}(G) = \frac{d_i}{q}$.

If $d_i = 0$, then $f_0, \dots, f_{n-1}, f_{n+1}, \dots, f_n$ are algebraically dependent over K by Lemma 2.2. Hence y_i does not appear in the minimal polynomial G of $f_0, \dots, f_n$. Hence $\deg_{y_i}(G) = 0 = \frac{d_i}{q}$.

(iii) Without loss of generality, we can assume that $\deg(f_0) = \min_i\{\deg(f_i)\}$. Let

$$H(y_0, \dots, y_n) = G(y_0, y_0 - a_1 y_0, \dots, y_n - a_n y_0)$$

where we choose suitable $a_1, \dots, a_n \in K$ so that one of the monomials of the highest total degree in H is $a y_1^{\deg(H)}$, $a \in K^*$. Then H is the minimal polynomial of

$$f_0, f_1 + a_1 f_0, \dots, f_n + a_n f_0.$$

We obtain

$$\begin{aligned}\deg(G) &= \deg(H) = \deg_{y_0}(H)\\ &= \frac{[k(x_1, \dots, x_n) : k(f_1 + a_1 f_0, \dots, f_n + a_n f_0)]}{q} \quad \text{by (ii)}\\ &\le \frac{1}{q}\prod_{i=1}^{n} \deg(f_i)\end{aligned}$$

by Lemma 2.1. Moreover, if the system of equations $f_i^+ = 0$, $i = 1, \dots, n$, has only the trivial solution, then

$$\deg(G) \le \deg_{y_0}(G) = \frac{1}{q}\prod_{i=1}^{n}(\deg(f_i))$$

by (ii) and Lemma 2.1. Hence the equality holds. □

Remark 1. Our main theorem can be generalized to minimal polynomials of rational functions over K.

3. An application

As an application of the main theorem, we give a very simple proof of the following known result.

Theorem 3.1 (Gabber, see [2]). *Let K be a field and $f = (f_1, \dots, f_n) : K^n \to K^n$ be a polynomial automorphism. Then*

$$\deg(f^{-1}) \le (\deg(f))^{n-1},$$

where $\deg(f) := \max_i\{\deg(f_i)\}$.

Remark 2. Wang [10] first conjectured the above theorem holds. It is proved by Gabber (see [2]), who uses deep algebraic geometry. But here it is just an immediate consequence of Theorem 1.1(iii).

Proof. Write $f = (f_1, \dots, f_n) \in (K[x_1, \dots, x_n])^n$ and $f^{-1} = g = (g_1, \dots, g_n)$. By Yu [11], g_i is the minimal polynomial of the ith face polynomials $f_1(x_i = 0), \dots, f_n(x_i = 0)$ and obviously

$$K[x_1, \dots, x_n] = K[f_1(x_i = 0), \dots, f_n(x_i = 0)].$$

By Theorem 2.2(iii),

$$\deg(g_i) \le \left(\max_k\{\deg(f_k(x_i = 0))\}\right)^{n-1} \le (\deg(f))^{n-1}, \quad \forall i.$$

Hence $\deg(g) = \max_i\{\deg(g_i)\} \le (\deg(f))^{n-1}$. □

Remark 3. For the special case $n = 1$ in Theorem 1.1, Abhyankar [1] and McKay and Wang [5] have proved $D\prod_{i=1}^{d}(y_0 - f_0(\alpha_1^{(i)}))$ is essentially the sylvester resultant $\mathrm{Res}_{x_1}(y_0 - f_0(x_1), y_1 - f_1(x_1))$. In a forthcoming paper [9], by means of the sparse elimination theory in Sturmfels [8] and Pederson and Sturmfels [7], we prove that for any n,

$$D\prod_{i=1}^{d}(y_0 - f_0(\alpha_1^{(i)}, \dots, \alpha_n^{(i)}))$$

is essentially the 'sparse resultant' of $y_0 - f_0, \ldots, y_n - f_n$ with respect to $y_1, \ldots, y_n$. Hence we can explicitly express the minimal polynomial of $f_0, \ldots, f_n$ in terms of all coefficients of $f_0, \ldots, f_n$.

REFERENCES

1. S. S. Abhyankar, *Algebraic geometry for scientists and engineers*, Amer. Math. Soc., Providence, RI, 1990.
2. H. Bass, E. Connell, and D. Wright, *The Jacobian conjecture: reduction on degree and formal expansion of the inverse*, Bull. Amer. Math. Soc. (N.S.) **7** (1982), 287–330.
3. W. Li and J.-T. Yu, *Computing minimal polynomials and the degree of unfaithfulness*, Comm. Algebra **21** (1993), 3557–3569.
4. ——, *Reconstructing birational maps from their face functions*, Manuscripta Math. **76** (1992), 353–366.
5. J. MaKay and S. S.-S. Wang, *An inversion formula for two polynomials in two variables*, J. Pure Appl. Algebra **40** (1986), 245–257.
6. D. Mumford, *Algebraic geometry* I. *Complex projective varieties*, Springer-Verlag, New York, 1976.
7. P. Pederson and B. Sturmfels, *Product formulas for sparse resultants*, J. Algebra (to appear) (1993).
8. B. Sturmfels, *Sparse elimination theory*, Proceedings of Computational Algebraic Geometry and Commutative Algebra, Cortona, Italy, 1992.
9. B. Sturmfels and J.-T. Yu, *Minimal polynomials and sparse resultants*, Proceedings of the Zero Dimensional Conference (Ravello, Italy, June 8–13, 1992), Cortona, Italy, 1993.
10. S. S.-S. Wang, *A Jacobian criterion for separability*, J. Algebra **65** (1980), 453–494.
11. J.-T. Yu, *Face polynomials and inversion formula*, J. Pure Appl. Algebra **78** (1992), 213–219.
12. ——, *Computing minimal polynomials and the inverse via GCP*, Comm. Algebra **21** (1993), 2279–2294.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF NOTRE DAME, NOTRE DAME, INDIANA 46556
Current address: Department of Mathematics, University of Hong Kong, Hong Kong
E-mail address: yujt@hku-xa.hku.hk