<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>A Product Formula for Minimal Polynomials and Degree Bounds for Inverses of Polynomial Automorphisms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Yu, JT</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>American Mathematical Society Proceedings, 1995, v. 123 n. 2, p. 343-349</td>
</tr>
<tr>
<td><strong>Issued Date</strong></td>
<td>1995</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10722/44912">http://hdl.handle.net/10722/44912</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>First published in American Mathematical Society Proceedings, 1995, v. 123 n. 2, p. 343-349, published by the American Mathematical Society.; This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.</td>
</tr>
</tbody>
</table>
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 $\{f_0, f_1, \ldots, f_n\} \subset K[x_1, \ldots, x_n]$ 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 $\{f_0, \ldots, f_n\} \subset K[x_1, \ldots, x_n]$ contain $n$ algebraically independent polynomials over $K$. Then there is a unique irreducible polynomial (up to a constant factor in $K^*$) $G(y_0, \ldots, y_n) \in K[y_1, \ldots, y_n]$ such that $G(f_0, \ldots, f_n) = 0$. We call this $G$ the minimal polynomial of $f_0, \ldots, f_n$ 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 $\alpha$ be algebraic over a field $K$ and $m_\alpha(x)$ be the minimal polynomial of $\alpha$ over $K$. Then

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

where $\alpha^{(1)}, \ldots, \alpha^{(d)}$ 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 $m_\alpha(x)$. \(\square\)
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 $G$,

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

Moreover, if for some $k$, $\deg(f_k) = \min \{\deg(f_i)\}$, 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 $f_i^+$ is the highest homogeneous form of $f_i$, 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 $K(x_1, \ldots, x_n)/K(f_1, \ldots, f_n)$ 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

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

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

$$
\begin{align*}
&f_1^+(x_1, \ldots, x_n) = 0 \\
&\vdots \\
&f_n^+(x_1, \ldots, x_n) = 0
\end{align*}
$$

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 $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$ be algebraically independent over $K$. Let $(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})$, $i = 1, \ldots, d$, be all solutions of the system of equations

$$
\begin{align*}
&f_1(x_1, \ldots, x_n) = y_1 \\
&\vdots \\
&f_n(x_1, \ldots, x_n) = y_n
\end{align*}
$$

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

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

Then $\overline{E}_{K(y_1, \ldots, y_n)}$ is a Galois extension and the Galois group

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

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

**Proof.** First observe that

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

Hence

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

Define

$$\sigma_i: K(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)}) \rightarrow K(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})$$

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

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

there are precise $d K(y_1, \ldots, y_n)$-isomorphisms in a fixed algebraic closure of $K(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})$. 

Hence \( \sigma_i, \ i = 1, \ldots, d, \) are all such \( dK(y_1, \ldots, y_n) \)-isomorphisms. Now let \( \theta_1 \) be a primitive element of \( K(\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}) \) over \( K(y_1, \ldots, y_n) \); then
\[
K(\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}) = K(\theta_1).
\]
Therefore,
\[
\alpha_k^{(1)} = g_k(\theta_1), \quad k = 1, \ldots, n; \ g_k(x) \in K(y_1, \ldots, y_n)(x).
\]
Let \( \theta_i := \sigma_i(\theta_1) \). Then
\[
\alpha_k^{(i)} = \sigma_i(\alpha_k^{(1)}) = \sigma_i(g_k(\theta_1)) = g_k(\sigma_i(\theta_1)) = g_k(\theta_i),
\]
\[
k = 1, \ldots, n; \ i = 1, \ldots, d.
\]
Hence \( \theta_i \) is a primitive element of \( K(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)}) \) over \( K(y_1, \ldots, y_n) \). Let \( m(x) \) be the minimal polynomial of \( \theta_i \) over \( K(y_1, \ldots, y_n) \). Then \( m(\theta_i) = m(\sigma_i(\theta_1)) = \sigma_i(m(\theta_1)) = 0 \). In other words, \( \theta_i, \ i = 1, \ldots, d, \) are all conjugates of \( \theta_1 \) over \( K(y_1, \ldots, y_n) \). Thus \( m(x) = \prod_{i=1}^d (x - \theta_i) \). Hence \( E = K(\theta_1, \ldots, \theta_d) \) is the splitting field of \( m(x) \) over \( K(y_1, \ldots, y_n) \). By Galois theory, \( K(\alpha_1, \ldots, \alpha_n) \) is a Galois extension and the Galois group \( G \) acts transitively on \( \{\theta_1, \ldots, \theta_d\} \), hence acts transitively on \( \{\alpha_1^{(i)}, \ldots, \alpha_n^{(i)} | i = 1, \ldots, d\} \).

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

(i) \( \forall \sigma \in G, \)
\[
\sigma \left( \prod_{i=1}^d (y_0 - f_0(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})) \right) = \prod_{i=1}^d (y_0 - f_0(\sigma(\alpha_1^{(i)}), \ldots, \sigma(\alpha_n^{(i)})))
\]
\[
= \prod_{i=1}^d (y_0 - f_0(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})),
\]
by the transitivity of \( G \). Hence
\[
\prod_{i=1}^d (y_0 - f_0(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})) \in K[y_0](y_1, \ldots, y_n).
\]
Denote by \( D \) its minimal denominator in \( K[y_1, \ldots, y_n] \). Let
\[
h(y_0, \ldots, y_n) \in K(\alpha_1, \ldots, \alpha_n)[y_0]
\]
be the unique minimal polynomial of \( f_0(\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}) \) over \( K(y_1, \ldots, y_n) \) such that \( h \) is an irreducible polynomial in \( K[y_0, \ldots, y_n] \) (up to a constant factor in \( K^* \)). Then
\[
h(f_0(\sigma(\alpha_1^{(1)}), \ldots, \sigma(\alpha_n^{(1)}))) = h(\sigma(f_0(\alpha_1^{(1)}, \ldots, \alpha_n^{(1)})))
\]
\[
= \sigma(h(f_0(\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}))) = 0, \quad \forall \sigma \in G.
\]
Hence
\[
h(f_0(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})) = 0, \quad i = 1, \ldots, d.
\]
This means that \( f_0(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)}), \ i = 1, \ldots, d, \) have the same minimal polynomial over \( K(y_1, \ldots, y_n) \) which is an irreducible polynomial in \( K[y_0, \ldots, y_n] \), namely, \( h(y_0, \ldots, y_n) \). Now let \( G(y_0, \ldots, y_n) \) be an irreducible factor of
A PRODUCT FORMULA FOR MINIMAL POLYNOMIALS

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

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

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

$$[K(x_1, \ldots, x_n) : K(f_0, \ldots, f_n)][K(f_0, \ldots, f_n) : K(f_1, \ldots, f_n)] = [K(x_1, \ldots, x_n) : K(f_1, \ldots, f_n)] = d.$$ 

On the other hand, since the system of equations

$$f_0(t_1, \ldots, t_n) = f_0(x_1, \ldots, x_n)$$
$$f_1(t_1, \ldots, t_n) = f_1(x_1, \ldots, x_n)$$
$$\vdots$$
$$f_n(t_1, \ldots, t_n) = f_n(x_1, \ldots, x_n)$$

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

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

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

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

(ii) If $d_i > 0$, then

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

by Lemma 2.1. By (i), $\deg_{y_1}(G) = \frac{d_i}{q}$.

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

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

where we choose suitable $a_1, \ldots, a_n \in K$ so that one of the monomials of the highest total degree in $H$ is $ay_1^{\deg(H)}$, $a \in K^*$. Then $H$ is the minimal polynomial of

$$f_0, f_1 + a_1 f_0, \ldots, f_n + a_n f_0.$$
We obtain
\[ \deg(G) = \deg(H) = \deg_{yo}(H) \]
\[ = \frac{[k(x_1, \ldots, x_n) : k(f_1 + a_1 f_0, \ldots, f_n + a_n f_0)]}{q} \]
by (ii)
\[ \leq \frac{1}{q} \prod_{i=1}^{n} \deg(f_i) \]
by Lemma 2.1. Moreover, if the system of equations \( f_i^+ = 0, \ i = 1, \ldots, n, \)
has only the trivial solution, then
\[ \deg(G) \leq \deg_{yo}(G) = \frac{1}{q} \prod_{i=1}^{n} (\deg(f_i)) \]
by (ii) and Lemma 2.1. Hence the equality holds. \( \Box \)

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 \( f = (f_1, \ldots, f_n) : K^n \to K^n \) be a polynomial automorphism. Then
\[ \deg(f^{-1}) \leq (\deg(f))^{n-1}, \]
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 \( f = (f_1, \ldots, f_n) \in (K[x_1, \ldots, x_n]^n) \) and \( f^{-1} = g = (g_1, \ldots, g_n). \) By Yu [11], \( g_i \) is the minimal polynomial of the \( i \)th face polynomials \( f_1(x_i = 0), \ldots, f_n(x_i = 0) \) and obviously
\[ K[x_1, \ldots, x_n] = K[f_1(x_i = 0), \ldots, f_n(x_i = 0)]. \]

By Theorem 2.2(iii),
\[ \deg(g_i) \leq \left( \max_k \{ \deg(f_k(x_i = 0)) \} \right)^{n-1} \leq (\deg(f))^{n-1}, \ \forall i. \]
Hence \( \deg(g) = \max_i \{ \deg(g_i) \} \leq (\deg(f))^{n-1}. \) \( \Box \)

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 \( \Res_{x_i}(y_0 - f_0(x_i), y_1 - f_1(x_i)). \) 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 \( n, \)
\[ D \prod_{i=1}^{d} (y_0 - f_0(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})) \]
A PRODUCT FORMULA FOR MINIMAL POLYNOMIALS

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


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: yuj@hku-xa.hku.hk