BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 56, No. 1, 2008

FIELD THEORY AND POLYNOMIALS

Polynomial Imaginary Decompositions for Finite Separable Extensions

by

Adam GRYGIEL

Presented by Andrzej SCHINZEL

Summary. Let K be a field and let $L = K[\xi]$ be a finite field extension of K of degree $m > 1$. If $f \in L[Z]$ is a polynomial, then there exist unique polynomials $u_0, \dots, u_{m-1} \in K[X_0, \dots, X_{m-1}]$ such that $f(\sum_{j=0}^{m-1} \xi^j X_j) = \sum_{j=0}^{m-1} \xi^j u_j$. A. Nowicki and S. Spodzieja proved that, if K is a field of characteristic zero and $f \neq 0$, then $u_0, \dots, u_{m-1}$ have no common divisor in $K[X_0, \dots, X_{m-1}]$ of positive degree. We extend this result to the case when L is a separable extension of a field K of arbitrary characteristic. We also show that the same is true for a formal power series in several variables.

1. Introduction. Throughout the paper, K is a field and $L = K[\xi]$ is a finite field extension of K of degree $m > 1$. For $j = 1, \dots, n$ let $\mathbf{X}_j = (X_{j,0}, \dots, X_{j,m-1})$ denote a system of variables and set

$$[\mathbf{X}_j] = X_{j,0} + \xi X_{j,1} + \dots + \xi^{m-1} X_{j,m-1}.$$

If $n = 1$, then we write briefly $\mathbf{X} = (X_0, \dots, X_{m-1})$ instead of $\mathbf{X}_1 = (X_{1,0}, \dots, X_{1,m-1})$. If $f \in L[Z_1, \dots, Z_n]$ is a polynomial, then there exist unique polynomials $u_0, \dots, u_{m-1} \in K[\mathbf{X}_1, \dots, \mathbf{X}_n]$ such that

$$f([\mathbf{X}_1], \dots, [\mathbf{X}_n]) = u_0 + \xi u_1 + \dots + \xi^{m-1} u_{m-1}.$$

This representation is called the *imaginary decomposition* of f relative to ξ, and the polynomials $u_0, \dots, u_{m-1}$ are the *imaginary parts* of f (see [1]).

Assume that

$$\phi(t) = t^m - a_{m-1} t^{m-1} - \dots - a_1 t - a_0, \quad \text{where } a_0, \dots, a_{m-1} \in K,$$

is the minimal polynomial of ξ over K and let $u = (u_0, \dots, u_{m-1})$ be a sequence of polynomials belonging to $K[\mathbf{X}]$. Denote by $\overline{u} = (\overline{u}_0, \dots, \overline{u}_{m-1})$

2000 *Mathematics Subject Classification*: Primary 12E05, 12F10.
Key words and phrases: polynomial, decomposition, separable extension.

the sequence of polynomials defined by

$$\overline{u}_0 = a_0 u_{m-1}, \quad \overline{u}_1 = a_1 u_{m-1} + u_0, \ \ldots, \ \overline{u}_{m-1} = a_{m-1} u_{m-1} + u_{m-2}.$$

We say that u is a ξ-*sequence* if u satisfies the following generalized Cauchy–Riemann equations introduced in [1]:

$$\frac{\partial u}{\partial X_i} = \frac{\partial \overline{u}}{\partial X_{i-1}}, \qquad i = 1, \ldots, m-1.$$

In 2003, A. Nowicki and S. Spodzieja proved the following theorem.

THEOREM 1 ([1, Theorem 3.8]). *Let K be a field of characteristic zero and let $L = K[\xi]$ be a finite field extension of K of degree $m > 1$. The following two conditions are equivalent*:

(i) *u is a ξ-sequence.*
(ii) *There exists $f \in L[Z]$ such that $u_0, \ldots, u_{m-1}$ are the imaginary parts of f.*

As a consequence of Theorem 1, A. Nowicki and S. Spodzieja also proved the following curious theorem.

THEOREM 2 ([1, Theorem 5.3]). *If under the assumptions of Theorem* 1, *$u_0, \ldots, u_{m-1}$ are the imaginary parts of $f \in L[Z_1, \ldots, Z_n] \setminus \{0\}$, then* $\gcd(u_0, \ldots, u_{m-1}) = 1$.

The assumption that $\operatorname{char} K = 0$ played an essential role in the proof of Theorem 2. The aim of this paper is to extend this theorem to the case when L is a separable extension of a field K of arbitrary characteristic. More precisely, our main result is the following.

THEOREM 3. *Let K be a field and let $L = K[\xi]$ be a finite separable extension of K of degree $m > 1$. If $u_0, \ldots, u_{m-1}$ are the imaginary parts of $f \in L[Z_1, \ldots, Z_n] \setminus \{0\}$, then* $\gcd(u_0, \ldots, u_{m-1}) = 1$.

Additionally, in Section 4 we generalize Theorems 1–3 to formal power series (Propositions 4–6, respectively).

2. Some auxiliary results. To prove Theorem 3 we need several known simple facts (see [1]).

PROPOSITION 1. *If $u_0, \ldots, u_{m-1}$ are the imaginary parts of a homogeneous polynomial $f \in L[Z_1, \ldots, Z_n]$ of degree s, then u_i is zero or a homogeneous polynomial of degree s for $i = 0, \ldots, m-1$.*

PROPOSITION 2. *If the polynomials $u_0, \ldots, u_{m-1} \in K[\mathbf{X}_1, \ldots, \mathbf{X}_n]$ are not relatively prime, then their homogeneous components of the highest degree are also not relatively prime.*

Let $d, n \in \mathbb{Z}$, $d, n \geq 2$. Consider the *Kronecker substitution* (cf. [2, 1.6, Definition 5]), i.e. the L-automorphism κ_d of $L[Z_1, \ldots, Z_n]$ defined by

$$\kappa_d(Z_j) = \begin{cases} Z_1 & \text{if } j = 1, \\ Z_j + Z_1^{d^{j-1}} & \text{if } j = 2, \ldots, n. \end{cases}$$

Proposition 3 ([1, Proposition 5.1]). *Let $f \in L[Z_1, \ldots, Z_n]$, and let $d > \max_{j=1,\ldots,n} \deg_{Z_j} f > 0$. Then*

$$\kappa_d(f) = aZ_1^N + \textit{terms of degrees lower than } N, \qquad N \geq 1,\ a \in L \setminus \{0\}.$$

Let $P_j = \kappa_d(Z_j) \in L[Z_1, \ldots, Z_n]$ for $j = 1, \ldots, n$ and

$$P_j([\mathbf{X}_1], \ldots, [\mathbf{X}_n]) = v_{j,0} + \xi v_{j,1} + \cdots + \xi^{m-1} v_{j,m-1}, \quad v_{j,i} \in K[\mathbf{X}_1, \ldots, \mathbf{X}_n].$$

Let $\gamma : K[\mathbf{X}_1, \ldots, \mathbf{X}_n] \to K[\mathbf{X}_1, \ldots, \mathbf{X}_n]$ be the homomorphism such that $\gamma(X_{j,i}) = v_{j,i}$.

Lemma 1 ([1, Lemma 5.2]). *γ is a K-automorphism of $K[\mathbf{X}_1, \ldots, \mathbf{X}_n]$.*

3. Proof of Theorem 3. A crucial role in the proof is played by the following lemma.

Lemma 2. *If under the assumptions of Theorem 3, $u_0, \ldots, u_{m-1}$ are the imaginary parts of $f(Z) = a_0 Z^s$, $a_0 \in L \setminus \{0\}$, then $\gcd(u_0, \ldots, u_{m-1}) = 1$.*

Proof. Let ϕ be the minimal polynomial of ξ over K and let M be a decomposition field of ϕ. Then $K[\xi] = K(\xi) \subset M$ and $\deg \phi = m > 1$. Consequently, since ξ is a simple root of ϕ, there exists $b \in M$, $b \neq \xi$, such that $\phi(b) = 0$. There is a K-isomorphism $\varphi : K(\xi) \to K(b)$ such that $\varphi(\xi) = b$.

Suppose that there is a polynomial $v \in K[\mathbf{X}]$ of positive degree which is a common divisor of $u_0, \ldots, u_{m-1}$ in $K[\mathbf{X}]$, and so also in $L[\mathbf{X}]$. Since $L[\mathbf{X}]$ is a UFD and $X_0 + \xi X_1 + \cdots + \xi^{m-1} X_{m-1}$ is irreducible in $L[\mathbf{X}]$, there exist $l \in \mathbb{Z}$, $l \geq 1$, and $a \in L \setminus \{0\}$ such that

$$v(X_0, \ldots, X_{m-1}) = a(X_0 + \xi X_1 + \cdots + \xi^{m-1} X_{m-1})^l.$$

Then $v(-\xi, 1, 0, \ldots, 0) = 0$, and so, since $v \in K[\mathbf{X}]$, we get

$$a(-b + \xi)^l = v(-b, 1, 0, \ldots, 0) = \varphi(v(-\xi, 1, 0, \ldots, 0)) = 0,$$

a contradiction. ∎

Using the facts in Section 2 we will extend Lemma 2 so as to obtain Theorem 3.

Proof of Theorem 3. Suppose that $u_0, \ldots, u_{m-1}$ have a common divisor in $K[\mathbf{X}_1, \ldots, \mathbf{X}_n]$ of positive degree. Denote by $f^{(s)}$ the homogeneous part of the highest degree of f and let $u_0^{(s)}, \ldots, u_{m-1}^{(s)}$ be the homogeneous parts of the highest degree of $u_0, \ldots, u_{m-1}$, respectively. By Proposition 3 and Lemma 1 one can assume that $f^{(s)}(Z_1, \ldots, Z_n) = a_0 Z_1^s$, $a_0 \in L \setminus \{0\}$, and so $f^{(s)} \in L[Z_1]$. By Propositions 1 and 2, $u_0^{(s)}, \ldots, u_{m-1}^{(s)}$ are the imaginary parts of $f^{(s)}$ and they are not relatively prime. This contradicts Lemma 2 and ends the proof. ∎

The following example, due to the referee, shows that the assumption of Theorem 3 concerning separability of the extension L of K is necessary.

EXAMPLE 1. Let $K = \mathbb{F}_2(t^2)$, $L = \mathbb{F}_2(t)$ and let $\xi = t$. Consider the polynomial $f(Z) = Z^2$. Then

$$f(X_0 + \xi X_1) = X_0^2 + t^2 X_1^2 \in K[X_0, X_1].$$

Hence $u_0 = X_0^2 + t^2 X_1^2$ and $u_1 = 0$ are the imaginary parts of f and they are not relatively prime.

4. Generalizations to formal power series. In this section we generalize Theorems 1–3 to formal power series.

Let $f \in L[[Z_1, \ldots, Z_n]]$ be a formal power series of the form $f = \sum_{r=d}^{\infty} f^{(r)}$, where $f^{(r)}$ is zero or a homogeneous polynomial of degree r for $r \geq d$, and let $u_0, \ldots, u_{m-1} \in K[[\mathbf{X}_1, \ldots, \mathbf{X}_n]]$ be formal power series of the form $u_j = \sum_{r=d}^{\infty} u_j^{(r)}$, where $u_j^{(r)}$ is zero or a homogeneous polynomial of degree r for $r \geq d$, $j = 0, \ldots, m-1$. By Proposition 1 we get immediately

COROLLARY 1. *$u_0^{(r)}, \ldots, u_{m-1}^{(r)}$ are the imaginary parts of $f^{(r)}$ for $r \geq d$ if and only if*

$$f([\mathbf{X}_1], \ldots, [\mathbf{X}_n]) = u_0 + \xi u_1 + \cdots + \xi^{m-1} u_{m-1}.$$

We call this representation the *imaginary decomposition* of f relative to ξ, and the power series $u_0, \ldots, u_{m-1}$ the *imaginary parts* of f.

Similarly to Lemma 3.5 in [1] we obtain a version of that lemma for power series.

LEMMA 3. *$(u_0, \ldots, u_{m-1})$ is a ξ-sequence if and only if $(u_0^{(r)}, \ldots, u_{m-1}^{(r)})$ is a ξ-sequence for $r \geq d$.*

Now we show the following generalizations of Theorems 1 and 2.

PROPOSITION 4. *Under the assumptions of Theorem 1 on K and L, if $u_0, \ldots, u_{m-1} \in K[[\mathbf{X}]]$ are power series, then the following two conditions are equivalent:*

(i) *$(u_0, \ldots, u_{m-1})$ is a ξ-sequence.*
(ii) *There exists $f \in L[[Z]]$ such that $u_0, \ldots, u_{m-1}$ are the imaginary parts of f.*

Proof. By Lemma 3 and Theorem 1, $(u_0, \ldots, u_{m-1})$ is a ξ-sequence if and only if there exist $f^{(d)}, f^{(d+1)}, \ldots \in L[Z]$ such that $u_0^{(r)}, \ldots, u_{m-1}^{(r)}$ are the imaginary parts of $f^{(r)}$ for $r \geq d$. By Corollary 1 this is equivalent to the fact that $u_0, \dots, u_{m-1}$ are the imaginary parts of $f := \sum_{r=d}^{\infty} f^{(r)}$. Thus, the proof is finished. ■

PROPOSITION 5. *Under the assumptions of Theorem* 1 *on* K *and* L, *if the power series* $u_0, \dots, u_{m-1}$ *are the imaginary parts of* $f \in L[[Z_1, \dots, Z_n]] \setminus \{0\}$, *then* $\gcd(u_0, \dots, u_{m-1}) = 1$.

Proof. If $u_0, \dots, u_{m-1}$ have a common divisor in $K[[\mathbf{X}_1, \dots, \mathbf{X}_n]]$ of positive order, then by Corollary 1, $u_0^{(d)}, \dots, u_{m-1}^{(d)}$ are the imaginary parts of $f^{(d)}$ and they have a common divisor in $K[\mathbf{X}_1, \dots, \mathbf{X}_n]$ of positive degree. This contradicts Theorem 2 and ends the proof. ■

Analogously we obtain the following generalization of Theorem 3.

PROPOSITION 6. *Under the assumptions of Theorem* 3 *on* K *and* L, *if the power series* $u_0, \dots, u_{m-1}$ *are the imaginary parts of* $f \in L[[Z_1, \dots, Z_n]] \setminus \{0\}$, *then* $\gcd(u_0, \dots, u_{m-1}) = 1$.

Acknowledgments. I would like to thank the anonymous referee for his remarks improving the paper, and Professors Andrzej Schinzel and Stanisław Spodzieja for their valuable comments and advice. I am also grateful to my colleague Krzysztof Kamiński for pointing out a few mistakes in the paper.

References

[1] A. Nowicki and S. Spodzieja, *Polynomial imaginary decompositions for finite extensions of fields of characteristic zero*, Bull. Polish Acad. Sci. Math. 51 (2003), 157–168.

[2] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Cambridge Univ. Press, Cambridge, 2000.

Adam Grygiel
Faculty of Mathematics and Computer Science
University of Łódź
Banacha 22
90-238 Łódź, Poland
E-mail: adamgry@op.pl

Received March 15, 2008;
received in final form March 21, 2008 (7652)