COLLOQUIUM MATHEMATICUM

VOL. 80 1999 NO. 1

SALOMON'S THEOREM FOR POLYNOMIALS WITH SEVERAL PARAMETERS

BY

MARIA FRONTCZAK, PRZEMYSŁAW SKIBIŃSKI AND STANISŁAW SPODZIEJA (ŁÓDŹ)

1. Introduction. Let $\mathbb{K}$ be an algebraically closed field, and $\Lambda = (\Lambda_1, \ldots, \Lambda_m)$ and $X = (X_1, \ldots, X_n)$ systems of variables.

Let $\overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$ be the separable closure of $\mathbb{K}(\Lambda)$. We say that polynomials $F_1, F_2 \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[X]$ are *conjugate* over $\mathbb{K}(\Lambda)$ if there exists a $\mathbb{K}(\Lambda, X)$-automorphism φ of $\overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}(X)$ such that $\varphi(F_1) = F_2$.

We say that a polynomial $F \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[X]$ is *monic* if the last coefficient of F in the lexicographic order is equal to 1.

In the theory of polynomials the following Salomon's Theorem is well-known ([Sa], [Sc, Theorem 17]).

SALOMON'S THEOREM. *If $F \in \mathbb{K}[\Lambda_1, X]$ is irreducible over $\mathbb{K}(\Lambda_1)$ then all monic factors of F irreducible over $\overline{\mathbb{K}(\Lambda_1)}^{\mathrm{sep}}$ are conjugate over $\mathbb{K}(\Lambda_1)$ and the number of linearly independent coefficients over $\mathbb{K}$ of any such factor does not exceed* $\deg_{\Lambda_1} F + 1$.

Using the idea of Krull [Kr] (see also [Sc, Theorem 17]) we give a generalization of this theorem to the case of several parameters Λ (Theorem 2). The upper bound $\deg_{\Lambda_1} F + 1$ is replaced by the number $\gamma_\Lambda(F)$ of integer points of the Newton polyhedron of F which we now define. Let $F \in \mathbb{K}[\Lambda, X]$ be of the form $F = \sum_J F_J \Lambda^J$, where $J = (j_1, \ldots, j_m)$ is a multiindex, $\Lambda^J = \Lambda_1^{j_1} \ldots \Lambda_m^{j_m}$, and $F_J \in \mathbb{K}[X]$. Let $\mathrm{supp}_\Lambda(F) = \{J \in \mathbb{Z}^m : F_J \neq 0\}$. Then we define the *Newton polyhedron* $\Delta_\Lambda(F)$ of F and the number $\gamma_\Lambda(F)$ by

$$\Delta_\Lambda(F) = \mathrm{conv}(\mathrm{supp}_\Lambda(F)), \qquad \gamma_\Lambda(F) = \#(\Delta_\Lambda(F) \cap \mathbb{Z}^m),$$

where $\mathrm{conv}\, A$ denotes the convex envelope of a set $A \subset \mathbb{R}^m$. The main difficulty in this generalization is the estimation of the number of linearly

1991 *Mathematics Subject Classification*: Primary 12E05.

Key words and phrases: conjugate polynomials, decomposition of polynomials.

Research of S. Spodzieja was partially supported by KBN Grant No. 2 P03A 050 10.

independent coefficients in the factors. The problem has been suggested by Professor A. Schinzel in a talk with the third author.

The key role in the proof is played by Proposition 1 (Section 2) on a multilinear form in the coefficients of polynomials.

The estimation obtained is a natural generalization of the one-parameter case because, for $m = 1$ and an irreducible polynomial F with $\deg_X F > 0$, we have $\gamma_\Lambda(F) = \deg_{\Lambda_1} F + 1$ (i.e. the number of coefficients of a polynomial in one variable with given degree). Moreover, in this estimation equality is attainable (Example 1), and it easy to see that $\gamma_\Lambda(F)$ does not exceed certain numbers which may be generalizations of the number mentioned above:

- $\gamma_\Lambda(F) \le \binom{\deg_\Lambda F + m}{m}$, i.e. $\gamma_\Lambda(F)$ does not exceed the number of coefficients of a polynomial with a given degree,
- $\gamma_\Lambda(F) \le \prod_{i=1}^{m} (\deg_{\Lambda_i} F + 1)$, i.e. $\gamma_\Lambda(F)$ does not exceed the number of coefficients of a polynomial with given degrees with respect to all variables.

Additionally we have $\gamma_\Lambda(F) \le (\deg_\Lambda F)^m + m$.

Theorem 2 does not fully explain the generalization of Bertini's Theorem ([Sc, Theorem 18]) to the case of polynomials with arbitrary degree with respect to the parameters. Such a generalization was claimed by Riehle in [R] (inaccessible to the authors), but Krull [Kr] objected to the validity of the proof. Riehle claimed that the number of linearly independent coefficients in the above mentioned factors does not exceed $1 + \prod_{i=1}^{m} \deg_{\Lambda_i} F$.

2. Multilinear forms in the coefficients of polynomials. For $A, B \subset \mathbb{R}^m$ we write

$$A + B = \{a + b : a \in A,\ b \in B\} \quad \text{and} \quad nA = \underbrace{A + \ldots + A}_{n \text{ times}}.$$

Thus, if A is convex, then $nA = \{na : a \in A\}$.

LEMMA 1. *Let $A \subset \mathbb{R}^m$ be bounded and convex. If $G, Q_1, \ldots, Q_N \in \mathbb{K}[\Lambda]$ are polynomials such that*

$$\Delta_\Lambda(Q_i) \subset iA \quad \text{for } i = 1, \ldots, N, \tag{1}$$

and

$$G^N + Q_1 G^{N-1} + \ldots + Q_N = 0, \tag{2}$$

then $\Delta_\Lambda(G) \subset A$.

Proof. Since $\Delta_\Lambda(G^i) = i\Delta_\Lambda(G)$ for $i = 1, \ldots, N$, from (1) and (2) we obtain

$$N\Delta_\Lambda(G) \subset \operatorname{conv}\Big(\bigcup_{i=1}^{N} [(N-i)\Delta_\Lambda(G) + iA]\Big). \tag{3}$$

Assume that, on the contrary, $\Delta_\Lambda(G) \not\subset A$. Then there exist $J_0 \in \Delta_\Lambda(G)\setminus A$ and a linear form $L : \mathbb{R}^m \to \mathbb{R}$ such that

$$L(J_0) \ge L(J) \qquad \text{for } J \in \Delta_\Lambda(G), \tag{4}$$

$$L(J_0) > L(J') \qquad \text{for } J' \in A. \tag{5}$$

By (3) there exist $J_1, \ldots, J_s \in \Delta_\Lambda(G)$, $J_1', \ldots, J_s' \in A$, $0 < i_1, \ldots, i_s \le N$ and $t_1, \ldots, t_s \in \mathbb{R}$, $t_i \ge 0$, $t_1 + \ldots + t_s = 1$, such that

$$NJ_0 = \sum_{k=1}^{s} t_k[(N - i_k)J_k + i_k J_k'].$$

Hence, from (4) and (5) we have

$$\begin{aligned} NL(J_0) &= \sum_{k=1}^{s} t_k[(N - i_k)L(J_k) + i_k L(J_k')] \\ &< \sum_{k=1}^{s} t_k[(N - i_k)L(J_0) + i_k L(J_0)] = NL(J_0), \end{aligned}$$

which is impossible. This ends the proof.

We are going to formulate a proposition which plays a crucial role in the proof of Theorem 1. First we define multilinear forms in the coefficients of polynomials which will be used in the proof of Proposition 1.

For a multiindex $I = (i_1, \ldots, i_n)$, let $\|I\| = i_1 + \ldots + i_n$ and $X^I = X_1^{i_1} \ldots X_n^{i_n}$. Let $F_j \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[X]$, $j = 1, \ldots, k$, be of the form

$$F_j = \sum_{\|I\| \le v} \alpha_{j,I} X^I, \tag{6}$$

where $v \in \mathbb{Z}$, $v \ge 0$, $\alpha_{j,I} \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$ for $j = 1, \ldots, k$, $\|I\| \le v$. Let $Y_j = (Y_{j,I}; \|I\| \le v)$, $j = 1, \ldots, k$. If $g \in \mathbb{Z}[Y_1, \ldots, Y_k]$ is a homogeneous form of degree k such that $\deg_{Y_j} g = 1$, $j = 1, \ldots, k$, then

$$G = g(\alpha_{j,I} : \|I\| \le v,\ j = 1, \ldots, k) \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$$

is called a *multilinear form in the coefficients of the polynomials* $F_1, \ldots, F_k$ (where for $r \in \mathbb{Z}$ we put $r \cdot 1 \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$).

Let $F_j \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[X]$, $j = 1, \ldots, k$, be all the conjugates of F_1 over $\mathbb{K}(\Lambda)$. Then there exist polynomials $P_1, \ldots, P_d \in \mathbb{K}[X]$ and $\mathring{\alpha}_{j,i} \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$ such that

$$F_j = \mathring{\alpha}_{j,1} P_1 + \ldots + \mathring{\alpha}_{j,d} P_d \tag{7}$$

for $j = 1, \ldots, k$ (and $\mathring{\alpha}_{1,i}, \ldots, \mathring{\alpha}_{k,i}$ are all the conjugates of $\mathring{\alpha}_{1,i}$ over $\mathbb{K}(\Lambda)$ for $i = 1, \ldots, d$). Let $Z = (Z_1, \ldots, Z_d)$ be a system of variables and

$$E_j = \mathring{\alpha}_{j,1} Z_1 + \ldots + \mathring{\alpha}_{j,d} Z_d \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[Z], \qquad j = 1, \ldots, k.$$

PROPOSITION 1. *Let $f \in \mathbb{K}(\Lambda)$, $f \neq 0$. If d is the minimal number in* (7) *and*

$$F = fF_1 \ldots F_k \in \mathbb{K}[\Lambda, X],$$

then

$$E = fE_1 \ldots E_k \in \mathbb{K}[\Lambda, Z] \quad \text{and} \quad \Delta_\Lambda(E) = \Delta_\Lambda(F).$$

Proof. From the choice of d we see that the polynomials $P_1, \ldots, P_d$ are linearly independent over $\mathbb{K}$. Since $\mathbb{K}$ is an infinite field, there exist $x^1, \ldots, x^d \in \mathbb{K}^n$ such that

$$\det[P_i(x^j)]_{i,j=1,\ldots,d} \neq 0. \tag{8}$$

From (6) and (7) we have

$$\sum_{\|I\| \le v} \alpha_{i,I}(x^j)^I = \mathring{\alpha}_{i,1} P_1(x^j) + \ldots + \mathring{\alpha}_{i,d} P_d(x^j), \quad j = 1, \ldots, d.$$

So, by (8), from Cramer's formulae we find that there exist $\xi_{i,I} \in \mathbb{K}$, $\|I\| \le v$, $i = 1, \ldots, d$, such that

$$\mathring{\alpha}_{s,i} = \sum_{\|I\| \le v} \alpha_{s,I} \xi_{i,I}.$$

Thus any multilinear form in the coefficients of $fE_1, \ldots, E_k$ is a linear combination over $\mathbb{K}$ of multilinear forms in the coefficients of $fF_1, \ldots, F_k$. Hence, since $F \in \mathbb{K}[\Lambda, X]$, by Kronecker's Theorem ([K], [Sc, Theorem 10], [Kö, VI, §2]), the multilinear forms in the coefficients of $fE_1, \ldots, E_k$ are integer over $\mathbb{K}[\Lambda]$. Since $F_1, \ldots, F_k$ are all the conjugates of F_1 over $\mathbb{K}(\Lambda)$, it follows that $E_1, \ldots, E_k$ are all the conjugates of E_1 over $\mathbb{K}(\Lambda)$. In consequence $E \in \mathbb{K}(\Lambda)[X]$, thus $E \in \mathbb{K}[\Lambda, X]$.

The inclusion $\Delta_\Lambda(E) \supset \Delta_\Lambda(F)$ is obvious. We prove that $\Delta_\Lambda(E) \subset \Delta_\Lambda(F)$. Let $E = \sum_J A_J Z^J$, where $A_J \in \mathbb{K}[\Lambda]$ for every multiindex J. Since

$$\Delta_\Lambda(E) = \operatorname{conv}\Big(\bigcup_J \Delta_\Lambda(A_J)\Big),$$

it suffices to prove that $\Delta_\Lambda(A_J) \subset \Delta_\Lambda(F)$ for all J. Take any coefficient $G = A_J \in \mathbb{K}[\Lambda]$ of the polynomial E. Obviously G is a multilinear form in the coefficients of $fE_1, \ldots, E_k$. Then there exist multilinear forms $G_1, \ldots, G_M$ in the coefficients of $fF_1, \ldots, F_k$ and $\xi_1, \ldots, \xi_M \in \mathbb{K}$ such that

$$G = \xi_1 G_1 + \ldots + \xi_M G_M. \tag{9}$$

By Kronecker's Theorem ([Sc, Theorem 9], [Kö, VI, §2]) there exists a non-empty set of non-zero forms $h_1, \ldots, h_N$ in the coefficients of $fF_1, \ldots, F_k$ such that every multilinear form G_s in the coefficients of $fF_1, \ldots, F_k$ satisfies

$$G_s h_i = \sum_{j=1}^{N} b_{i,j,G_s} h_j, \quad i = 1, \ldots, N,$$

where b_{i,j,G_s} are some linear forms in the coefficients of F. Hence (9) yields

$$\sum_{j=1}^{N}\Big(\delta_{i,j}G-\sum_{s=1}^{M}\xi_s b_{i,j,G_s}\Big)h_j=0,\qquad i=1,\dots,N, \tag{10}$$

where $\delta_{i,j}$ is the Kronecker symbol. Since $h_1,\dots,h_N$ are non-zero, the determinant of the linear system (10) vanishes. Thus we have

$$G^N+Q_1G^{N-1}+\dots+Q_N=0, \tag{11}$$

where $Q_j\in\mathbb{K}[\Lambda]$ is a homogeneous form of degree j in the coefficients of F, $j=1,\dots,N$. Thus $\Delta_\Lambda(Q_j)\subset j\Delta_\Lambda(F)$. By Lemma 1, $\Delta_\Lambda(G)\subset\Delta_\Lambda(F)$, which ends the proof.

3. Generalization of Salomon's Theorem. Let $F\in\mathbb{K}[\Lambda,X]$. The main result of the paper will be preceded by

THEOREM 1. *Let $F_j\in\overline{\mathbb{K}(\Lambda)}^{\text{sep}}[X]$, $j=1,\dots,k$, be all the conjugates of F_1 over $\mathbb{K}(\Lambda)$ and let $f\in\mathbb{K}(\Lambda)$, $f\neq 0$, be such that*

$$F=fF_1\dots F_k\in\mathbb{K}[\Lambda,X].$$

Then the number of linearly independent coefficients (over $\mathbb{K}$) of any F_j does not exceed $\gamma_\Lambda(F)$.

P r o o f. Let F_j, $j=1,\dots,k$, be of the form (6). Let d be the dimension of the following linear space over $\mathbb{K}$:

$$\Big\{\sum_{\|I\|\le v}\xi_I\alpha_{1,I}:\xi_I\in\mathbb{K}\text{ for }\|I\|\le v\Big\},$$

and $\mathring{\alpha}_{1,1},\dots,\mathring{\alpha}_{1,d}$ be its basis. Then there exist $P_1,\dots,P_d\in\mathbb{K}[X]$ such that

$$F_1=\mathring{\alpha}_{1,1}P_1+\dots+\mathring{\alpha}_{1,d}P_d.$$

Since $F_1,\dots,F_k$ are conjugate over $\mathbb{K}(\Lambda)$, we have

$$F_j=\mathring{\alpha}_{j,1}P_1+\dots+\mathring{\alpha}_{j,d}P_d$$

for $j=2,\dots,k$ (and $\mathring{\alpha}_{1,i},\dots,\mathring{\alpha}_{k,i}$ are all the conjugates of $\mathring{\alpha}_{1,i}$ over $\mathbb{K}(\Lambda)$ for $i=1,\dots,d$). Let

$$E_j=\mathring{\alpha}_{j,1}Z_1+\dots+\mathring{\alpha}_{j,d}Z_d\in\overline{\mathbb{K}(\Lambda)}^{\text{sep}}[Z],\qquad j=1,\dots,k,$$

where $Z=(Z_1,\dots,Z_d)$. By Proposition 1 we have $E=fE_1\dots E_k\in\mathbb{K}[\Lambda,Z]$ and $\Delta_\Lambda(E)\subset\Delta_\Lambda(F)$. Thus $\gamma_\Lambda(E)\le\gamma_\Lambda(F)$. In consequence there exist homogeneous forms $H_i\in\mathbb{K}[Z]$ and polynomials $B_i\in\mathbb{K}[\Lambda]$, $i=1,\dots,\gamma_\Lambda(F)$, such that

$$E=\sum_{i=1}^{\gamma_\Lambda(F)}B_iH_i.$$

Assume, contrary to our claim, that $\gamma_\Lambda(F) < d$. Then the forms $H_1, \ldots, H_{\gamma_\Lambda(F)}$ have a common non-trivial zero $(\xi_1, \ldots, \xi_d) \in \mathbb{K}^d$ and so

$$0 = f \prod_{j=1}^{k} (\mathring{\alpha}_{j,1}\xi_1 + \ldots + \mathring{\alpha}_{j,d}\xi_d).$$

In consequence, at least one factor of the right-hand side is zero. This contradicts the definition of d (since for any $j = 1, \ldots, k$ the elements $\mathring{\alpha}_{j,1}, \ldots, \mathring{\alpha}_{j,d}$ are linearly independent over $\mathbb{K}$). This ends the proof.

For F irreducible, the above theorem immediately yields the following generalization of Salomon's Theorem to the case of several parameters.

THEOREM 2. *If* $F \in \mathbb{K}[\Lambda, X]$ *is irreducible over* $\mathbb{K}(\Lambda)$ *then all monic factors in* $\overline{\mathbb{K}(\Lambda)}^{\text{sep}}[X]$ *of* F *irreducible over* $\overline{\mathbb{K}(\Lambda)}^{\text{sep}}$ *are conjugate over* $\mathbb{K}(\Lambda)$ *and the number of linearly independent coefficients* (*over* $\mathbb{K}$) *of any such factor does not exceed* $\gamma_\Lambda(F)$.

Proof. Let F_1 be a monic factor of F irreducible over $\overline{\mathbb{K}(\Lambda)}^{\text{sep}}$ and $F_2, \ldots, F_k$ be all its conjugates over $\mathbb{K}(\Lambda)$. Since $\overline{\mathbb{K}(\Lambda)}^{\text{sep}}$ is Galois over $\mathbb{K}(\Lambda)$, F_j are all irreducible over $\mathbb{K}(\Lambda)$ and since they are monic, they are pairwise relatively prime. Hence F_j is a divisor of F, $j = 1, \ldots, k$. It follows that $\prod_{j=1}^k F_j$ is a divisor of F. However, $\prod_{j=1}^k F_j$ is invariant with respect to any automorphism φ of $\overline{\mathbb{K}(\Lambda)}^{\text{sep}}$ over $\mathbb{K}(\Lambda)$, hence $\prod_{j=1}^k F_j \in \mathbb{K}(\Lambda)[X]$ and, by the irreducibility of F over $\mathbb{K}(\Lambda)$, there is an $f \in \mathbb{K}(\Lambda)$ such that

$$F = f \prod_{j=1}^{k} F_j. \tag{12}$$

Hence, by Theorem 1, we have the assertion.

The upper bound given by Theorem 2 can be attained, as shown by the following

EXAMPLE 1. Let $X = (X_0, \ldots, X_n)$ be a system of variables and $P(t_1, t_2, X) = \sum_{r+s=n} t_1^r t_2^s X_r$. Let ε be a primitive root of unity of degree n. Then the polynomials

$$F_j = P(\sqrt[n]{\Lambda_2 \ldots \Lambda_m}, \varepsilon^j \sqrt[n]{\Lambda_1}, X) \in \overline{\mathbb{K}(\Lambda)}^{\text{sep}}[X], \quad j = 1, \ldots, n,$$

are all the conjugates of F_1 over $\mathbb{K}(\Lambda)$. Hence $F = \prod_{j=1}^n F_j \in \mathbb{K}[\Lambda, X]$ is irreducible over $\mathbb{K}(\Lambda)$. Moreover, $\gamma_\Lambda(F) = n+1$ and the F_j have each $n+1$ coefficients linearly independent over $\mathbb{K}$.

In the above example the polyhedron of F is a segment and one can reduce this example to the case of one parameter Λ_1 (puting $\Lambda_2 = \ldots = \Lambda_m = 1$). The authors do not know such examples with $\Delta_\Lambda(F)$ m-dimensional.

From Theorem 2 we obtain the following

THEOREM 3. *Let $F \in \mathbb{K}[\Lambda, X]$. Then the number of linearly independent coefficients* (*over* $\mathbb{K}$) *of any factor of F irreducible over $\overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$ does not exceed $\gamma_\Lambda(F)$.*

Proof. Let $F_1 \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[X]$ be any factor of F irreducible over $\overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$. Without loss of generality we may assume that F_1 is monic. Let $F = R_1 \ldots R_k$ be the decomposition of F into irreducible factors in $\mathbb{K}[\Lambda, X]$. From Ostrowski's Theorem ([O, Theorem VI]) we have

$$\Delta_\Lambda(R_1) + \ldots + \Delta_\Lambda(R_k) = \Delta_\Lambda(F).$$

So, $\gamma_\Lambda(R_j) \le \gamma_\Lambda(F)$, $j = 1, \ldots, k$. Since F_1 is a divisor of at least one R_j, Theorem 2 yields the assertion.

The above theorem is not true for arbitrary factors, as is shown by the following

EXAMPLE 2. For $F = X_1^s - \Lambda_1$ we have $\gamma_\Lambda(F) = 2$ and

$$F = (X_1 - \sqrt[s]{\Lambda_1})(X_1^{s-1} + X_1^{s-1}\sqrt[s]{\Lambda_1} + \ldots + (\sqrt[s]{\Lambda_1})^{s-1}).$$

It is easy to see that the last factor has s coefficients linearly independent over $\mathbb{K}$.

REMARK 1. The above results hold for arbitrary Galois extensions of $\mathbb{K}(\Lambda)$ in place of $\overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$, with no change in the proofs.

4. A corollary. In this section we give a particular version of Theorem 2.

Assume that $\mathbb{K}$ is an algebraically closed field of characteristic zero. Then $\overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}$ is the algebraic closure of $\mathbb{K}(\Lambda)$.

In Theorems 1–3 the reducibility of the polynomial F in $\overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[X]$, by Emma Noether's Theorem ([N], [Sc, Theorem 15]), is equivalent to the reducibility of $F(\lambda, X)$ in $\mathbb{K}[X]$ for all $\lambda \in \mathbb{K}^m$ such that $\deg F(\lambda, X) = \deg_X F$. We now give a version of Theorem 2 in the case when $F(\lambda, X) - z$ is reducible in $\mathbb{K}[X]$ for all $z \in \mathbb{K}$ and $\lambda \in \mathbb{K}^m$ such that $\deg F(\lambda, X) = \deg_X F$.

COROLLARY 1. *Let $F \in \mathbb{K}[\Lambda, X]$ be an irreducible polynomial monic with respect to X_1. If $F(\lambda, X) - z$ is reducible for all $z \in \mathbb{K}$ and $\lambda \in \mathbb{K}^m$ such that $\deg F(\lambda, X) = \deg_X F$, then there exists a representation*

$$F = F_1 \ldots F_k,$$

where $F_j \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[X]$ are all the conjugates of F_1 over $\mathbb{K}(\Lambda)$, $\deg F_j < \deg_X F$ and the number of linearly independent coefficients (*over* $\mathbb{K}$) *of any F_j does not exceed $2^{-m}(\deg_{\Lambda_1} F + 2) \ldots (\deg_{\Lambda_m} F + 2)$.*

Proof. By [FS, Corollary 6] there exist $R \in \mathbb{K}[\Lambda, X]$, $\deg_X R < \deg_X F$, $a_i \in \mathbb{K}[\Lambda]$, $i = 0, \ldots, s$, $s \ge 2$, such that

$$F = a_0 R^s + a_1 R^{s-1} + \ldots + a_s.$$

Moreover, one can assume that $R(\Lambda, 0) = 0$. Hence

$$\begin{aligned}\deg_{\Lambda_j} F \geq\ & \deg_{\Lambda_j}(F - a_{s-1}R - a_s)\\ \geq\ & \deg_{\Lambda_j}(a_0R^{s-2} + a_1R^{s-3} + \ldots + a_{s-2}) + 2\deg_{\Lambda_j} R,\end{aligned}$$

and so

$$\deg_{\Lambda_j} R \leq \frac{\deg_{\Lambda_j} F}{2} \quad \text{for } j = 1, \ldots, m. \tag{15}$$

Since F is monic with respect to X_1, we may assume that R is monic with respect to X_1 and $a_0 = 1$. From the irreducibility of F we see that $h = a_0Z^s + a_1Z^{s-1} + \ldots + a_s$ is irreducible in $\mathbb{K}[\Lambda, Z]$, hence,

$$h = (Z - f_1)\ldots(Z - f_s)$$

where $Z - f_j \in \overline{\mathbb{K}(\Lambda)}^{\mathrm{sep}}[Z]$ are conjugate over $\mathbb{K}(\Lambda)$. Taking $F_j = R - f_j$ we see that F_j are conjugate over $\mathbb{K}(\Lambda)$ and, by (15), the number of linearly independent coefficients (over $\mathbb{K}$) of any F_j does not exceed $2^{-m}(\deg_{\Lambda_1} F + 2) \ldots (\deg_{\Lambda_m} F + 2)$. This gives the assertion.

REFERENCES

[FS] M. Frontczak, P. Skibiński and S. Spodzieja, *On factorization of polynomials with holomorphic coefficients*, Bull. Polish Acad. Sci. Math. 46 (1998), 39–54.

[Kö] J. König, *Einleitung in die allgemeine Theorie der algebraischen Größen*, Teubner, Leipzig, 1903.

[K] L. Kronecker, *Zur Theorie der Formen höherer Stufen*, Monatsber. Akad. Wiss. Berlin 37 (1883), 957–960; Werke 2, Chelsea, 1968, 417–424.

[Kr] W. Krull, *Über einen Irreduzibilitätssatz von Bertini*, J. Reine Angew. Math. 177 (1937), 94–104.

[N] E. Noether, *Ein algebraisches Kriterium für absolute Irreduzibilität*, Math. Ann. 85 (1922), 26–33.

[O] A. M. Ostrowski, *On multiplication and factorization of polynomials. I. Lexicographic orderings and extreme aggregates of terms*, Aequationes Math. 13 (1975), 201–228.

[R] A. Riehle, *Über den Bertinischen Satz und seine Erweiterung*, Diss. Tübingen, 1919.

[Sa] G. Salomon, *Über das Zerfallen von Systemen von Polynomen*, Jahresber. Deutsche Math.-Verein. 24 (1915), 225–246.

[Sc] A. Schinzel, *Selected Topics on Polynomials*, The Univ. of Michigan Press, Ann Arbor, 1982.

Faculty of Mathematics
University of Łódź
Banacha 22
90-238 Łódź, Poland
E-mail: spodziej@imul.uni.lodz.pl

Received 16 June 1998;
revised 10 September 1998