ACTA ARITHMETICA
XC.3 (1999)

# Reducibility of lacunary polynomials XII

by

A. Schinzel (Warszawa)

*In memory of Paul Erdős*

E. Bombieri and U. Zannier [1] have recently proved an important theorem which permits improving most of the results of papers VII, VIII, X and XI of this series. In order to state the results I shall use the same notation as in those papers, explained below, together with a new usage of the matrix notation.

$\mathbb{N}$ and $\mathbb{N}_0$ are the sets of positive and non-negative integers, respectively, $\overline{\mathbb{Q}}$ is the field of algebraic numbers.

Bold face letters denote vectors written horizontally, $\boldsymbol{x} = [x_1, \ldots, x_k]$, $\boldsymbol{x}^{-1} = [x_1^{-1}, \ldots, x_k^{-1}]$ and similarly for $\boldsymbol{z}$; $\boldsymbol{ab}$ is the scalar product of $\boldsymbol{a}$ and $\boldsymbol{b}$.

The set of $k \times l$ integral matrices is denoted by $\mathfrak{M}_{k,l}(\mathbb{Z})$, and the identity matrix of order $k$ by $\boldsymbol{I}_k$. For a matrix $\boldsymbol{A} = (a_{ij}) \in \mathfrak{M}_{k,l}(\mathbb{Z})$ we put

$$h(\boldsymbol{A}) = \max_{i,j} |a_{ij}|, \qquad \boldsymbol{x}^{\boldsymbol{A}} = \Big[\prod_{i=1}^{k} x_i^{a_{i1}}, \ldots, \prod_{i=1}^{k} x_i^{a_{il}}\Big].$$

For a Laurent polynomial $F \in \boldsymbol{K}[\boldsymbol{x}, \boldsymbol{x}^{-1}]$, where $\boldsymbol{K}$ is any field, if $F = \prod_{i=1}^{k} x_i^{\alpha_i} F_0(\boldsymbol{x})$, where $F_0 \in \boldsymbol{K}[\boldsymbol{x}]$ and $(F_0, \prod_{i=1}^{k} x_i) = 1$, we put

$$JF = F_0.$$

A polynomial $F$ is *reciprocal* if $JF(\boldsymbol{x}^{-1}) = \pm F(\boldsymbol{x})$.

A polynomial is *irreducible* over $\boldsymbol{K}$ if it is not reducible over $\boldsymbol{K}$ and not a constant. For $\boldsymbol{K} = \mathbb{Q}$ we omit the words "over $\mathbb{Q}$". If $F = c\prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$, where $c \in \boldsymbol{K}^*$, $F_\sigma$ are irreducible over $\boldsymbol{K}$ and pairwise coprime, and $e_\sigma \ge 1$ $(1 \le \sigma \le s)$, we write

$$F \overset{\text{can}}{\underset{\boldsymbol{K}}{=}} \text{const} \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$$

1991 *Mathematics Subject Classification*: Primary 11R09.

and call this a *canonical factorization* of $F$ over $\boldsymbol{K}$. If $\boldsymbol{K}=\mathbb{Q}$, then $\overset{\mathrm{can}}{\underset{\boldsymbol{K}}{=}}$ is replaced by $\overset{\mathrm{can}}{=}$. If

$$JF \overset{\mathrm{can}}{\underset{\boldsymbol{K}}{=}} \mathrm{const}\prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$$

we put

$$KF = \mathrm{const}\prod\nolimits^{*} F_\sigma^{e_\sigma},$$

and if $\boldsymbol{K}=\mathbb{Q}$

$$LF = \mathrm{const}\prod\nolimits^{**} F_\sigma^{e_\sigma},$$

where $\prod^{*}$ is taken over all $F_\sigma$ that do not divide $J(\boldsymbol{x}^{{}^t\boldsymbol{\alpha}}-1)$ for any $\boldsymbol{\alpha}\in\mathbb{Z}^k\setminus\{\mathbf{0}\}$ and $\prod^{**}$ is taken over all $F_\sigma$ that are not reciprocal. The leading coefficients (i.e. the coefficients of the first term in the antilexicographic order) of $KF$ and $LF$ are equal to that of $F$. Note that $KF$ depends only on $F$ and the prime field of $\boldsymbol{K}$, which in this paper is always $\mathbb{Q}$.

If $T$ is any transformation of $\boldsymbol{K}[\boldsymbol{x},\boldsymbol{x}^{-1}]$ into itself and $F\in\boldsymbol{K}[\boldsymbol{x},\boldsymbol{x}^{-1}]$ then

$$KF(T\boldsymbol{x}) = K(F(T\boldsymbol{x})),$$

and if $\boldsymbol{K}=\mathbb{Q}$

$$LF(T\boldsymbol{x}) = L(F(T\boldsymbol{x})).$$

The Bombieri–Zannier theorem can be stated as follows.

THEOREM BZ. *Let $P,Q\in\overline{\mathbb{Q}}[\boldsymbol{x}]$ and $\boldsymbol{n}\in\mathbb{Z}^k$. If $(P,Q)=1$, but $(KP(x^{\boldsymbol{n}}),KQ(x^{\boldsymbol{n}}))\neq 1$, then there exists a $\boldsymbol{\gamma}\in\mathbb{Z}^k$ such that*

$$\boldsymbol{\gamma}\boldsymbol{n}=0 \quad \textit{and} \quad 0<h(\boldsymbol{\gamma})\le c_1(P,Q),$$

*where $c_1(P,Q)$ depends only on $P$ and $Q$.*

In the sequel $c_i(\ldots)$ denote effectively computable positive numbers depending only on parameters displayed in parentheses. Theorem BZ extends Theorem 1 of [7] from $k\le 3$ to arbitrary $k$ in the crucial case $[\boldsymbol{K}:\mathbb{Q}]<\infty$ and immediately implies that in Theorem 2 of [7],

$$c_2(P,Q)N^{k-\min\{k,6\}/(2k-2)}\frac{(\log N)^{10}}{(\log\log N)^9}$$

can be replaced by

$$c_2(P,Q)N^{k-1}.$$

Theorems 3 and 5 of [7] can now be extended in the following manner.

THEOREM 1. *Let $F\in\mathbb{Z}[\boldsymbol{x}]\setminus\{0\}$, $k_0$ be the number of variables with respect to which $F$ is of positive degree, and $\|F\|$ be the sum of squares of the coefficients of $F$. Assume $KF=LF$. For every vector $\boldsymbol{n}\in\mathbb{Z}^k$ such that*

*$F(x^{\boldsymbol{n}}) \neq 0$ there exist a matrix $\boldsymbol{M} = (\mu_{ij}) \in \mathfrak{M}_{k,k}(\mathbb{Z})$ and a vector $\boldsymbol{v} \in \mathbb{Z}^k$ such that*

$$0 \le \mu_{ij} < \mu_{jj} \le \exp(9k_0) \cdot 2^{\|F\|-5} \quad (i \neq j), \qquad \mu_{ij} = 0 \quad (i < j), \tag{1}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}, \tag{2}$$

*and either*

$$KF(\boldsymbol{z}^{\boldsymbol{M}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(\boldsymbol{z})^{e_\sigma} \tag{3}$$

*implies*

$$KF(x^{\boldsymbol{n}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^{\boldsymbol{v}})^{e_\sigma}, \tag{4}$$

*or there exists a $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that*

$$\boldsymbol{\gamma}\boldsymbol{n} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}) \le c_3(F, \boldsymbol{M}). \tag{5}$$

Theorem 4 of [7] is extended as follows.

THEOREM 2. *Let $F \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$ and $\boldsymbol{n} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$. If $JF(x^{\boldsymbol{n}})$ is not reciprocal, then $KF(x^{\boldsymbol{n}})$ is reducible if and only if there exists a matrix $\boldsymbol{N} \in \mathfrak{M}_{r,k}(\mathbb{Z})$ of rank $r$ and a vector $\boldsymbol{v} \in \mathbb{Z}^r$ such that*

$$h(\boldsymbol{N}) \le c_4(F), \tag{6}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}, \tag{7}$$

$$KF(\boldsymbol{y}^{\boldsymbol{N}}) = F_1F_2, \qquad \boldsymbol{y} = [y_1, \ldots, y_r], \qquad F_i \in \mathbb{Q}[\boldsymbol{y}] \quad (i = 1, 2), \tag{8}$$

$$KF_i(x^{\boldsymbol{v}}) \notin \mathbb{Q} \quad (i = 1, 2). \tag{9}$$

Further we have

THEOREM 3. *Let $F \in \overline{\mathbb{Q}}[\boldsymbol{x}] \setminus \{0\}$, $\boldsymbol{n} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$, $\boldsymbol{K}$ be the field generated over $\mathbb{Q}$ by the ratios of the coefficients of $F(x^{\boldsymbol{n}})$ and $\widehat{\boldsymbol{K}}$ be its normal closure. Assume that $F \in \boldsymbol{K}[\boldsymbol{x}]$, $F(x^{\boldsymbol{n}}) \neq 0$ and for all embeddings $\tau$ of $\boldsymbol{K}$ into $\widehat{\boldsymbol{K}}$,*

$$\frac{JF(x^{-\boldsymbol{n}})}{JF^\tau(x^{\boldsymbol{n}})} \notin \widehat{\boldsymbol{K}}. \tag{10}$$

*If $KF(x^{\boldsymbol{n}})$ is reducible over $\boldsymbol{K}$ there exist a matrix $\boldsymbol{N} \in \mathfrak{M}_{r,k}(\mathbb{Z})$ of rank $r$ and a vector $\boldsymbol{v} \in \mathbb{Z}^r$ such that*

$$h(\boldsymbol{N}) \le c_5(F), \tag{11}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N} \tag{12}$$

*and $JF(\boldsymbol{y}^{\boldsymbol{N}})$ is reducible over $\widehat{\boldsymbol{K}}$, where $\boldsymbol{y} = [y_1, \ldots, y_r]$.*

This theorem implies

Corollary 1. *Let* $\boldsymbol{a} = [a_0, \ldots, a_k] \in \overline{\mathbb{Q}}^{*k+1}$, $\boldsymbol{n} = [n_1, \ldots, n_k] \in \mathbb{N}^k$, $0 < n_1 < \ldots < n_k$ *and let* $\boldsymbol{K} = \mathbb{Q}(a_1/a_0, \ldots, a_k/a_0)$. *If* $a_0 \in \boldsymbol{K}$ *and* $K(a_0 + \sum_{j=1}^k a_j x^{n_j})$ *is reducible over* $\boldsymbol{K}$, *then there exist a matrix* $\boldsymbol{N}_0 \in \mathfrak{M}_{[(k+1)/2],k}(\mathbb{Z})$ *and a vector* $\boldsymbol{v}_0 \in \mathbb{Z}^{[(k+1)/2]}$ *such that*

$$h(\boldsymbol{N}_0) \le c_6(\boldsymbol{a}) \tag{13}$$

*and*

$$\boldsymbol{n} = \boldsymbol{v}_0 \boldsymbol{N}_0. \tag{14}$$

Corollary 2. *Under the assumptions of Corollary* 1 *the number of vectors* $\boldsymbol{n}$ *such that* $n_k \le N$ *and* $K(a_0 + \sum_{j=1}^k a_j x^{n_j})$ *is reducible over* $\boldsymbol{K}$ *is less than* $c_7(\boldsymbol{a}) N^{[(k+1)/2]}$.

Corollary 3. *Let* $\boldsymbol{a} = [a_0, \ldots, a_k] \in \mathbb{C}^{*k+1}$ *be such that* $a_0 \in \boldsymbol{K} = \mathbb{Q}(a_1/a_0, \ldots, a_k/a_0)$. *The number of integer vectors* $\boldsymbol{n} = [n_1, \ldots, n_k]$ *such that* $0 < n_1 < \ldots < n_k \le N$ *and* $K(a_0 + \sum_{j=1}^k a_j x^{n_j})$ *is reducible over* $\boldsymbol{K}$ *is less than* $c_8(\boldsymbol{a}) N^{k-1}$.

Corollary 1 improves in the case $\boldsymbol{K} = \mathbb{Q}$ and extends Theorem 2 of [3], while Corollary 2 drastically improves Theorem 1 of [5]. The exponent $[(k+1)/2]$ cannot be further improved, as will be shown by an example, the gist of which is in [3]. Corollary 3 improves Theorem 2 of [6] and the Theorem of [8].

Further we have

Theorem 4. *Let* $F \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$. *There exist two finite subsets* $R$ *and* $S$ *of* $\bigcup_{r=1}^k \mathfrak{M}_{r,k}(\mathbb{Z})$ *with the following property. If* $\boldsymbol{n} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$ *and* $JF(x^{\boldsymbol{n}})$ *is not reciprocal*, *then* $KF(x^{\boldsymbol{n}})$ *is reducible if and only if the equation* $\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}$ *is soluble in* $\boldsymbol{v} \in \mathbb{Z}^r$ *and* $\boldsymbol{N} \in R \cap \mathfrak{M}_{r,k}(\mathbb{Z})$ *but unsoluble in* $\boldsymbol{v} \in \mathbb{Z}^s$ *and* $\boldsymbol{N} \in S \cap \mathfrak{M}_{s,k}(\mathbb{Z})$ *for each* $s < r$.

The reducibility condition given in Theorem 4 is more readily verifiable than that of Theorem 2, because of the relation (9) occurring in the latter. It is conjectured that a similar reducibility condition holds without the assumption that $JF(x^{\boldsymbol{n}})$ is not reciprocal and over any finite extension of $\mathbb{Q}$.

The proofs of Theorems 1–4 are based on several lemmas.

Lemma 1. *For every polynomial* $P \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$,

$$LKP = LP.$$

Proof. See [2], Lemma 11.

Lemma 2. *For every polynomial* $F \in \mathbb{Z}[\boldsymbol{x}]$ *and every vector* $\boldsymbol{n} \in \mathbb{Z}^k$ *such that* $F(x^{\boldsymbol{n}}) \ne 0$ *there exist a matrix* $\boldsymbol{M} = (\mu_{ij}) \in \mathfrak{M}_{k,k}(\mathbb{Z})$ *and a vector*

$\boldsymbol{v} \in \mathbb{Z}^k$ *such that*

$$0 \le \mu_{ij} < \mu_{jj} \le \exp(9k) \cdot 2^{\|F\|-5} \quad (i \ne j), \qquad \mu_{ij} = 0 \quad (i < j), \tag{15}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}, \tag{16}$$

*and either*

$$LF(\boldsymbol{z}^{\boldsymbol{M}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$$

*implies*

$$LF(x^{\boldsymbol{n}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^{\boldsymbol{v}})^{e_\sigma},$$

*or there exists a vector* $\boldsymbol{\gamma} \in \mathbb{Z}^k$ *such that*

$$\boldsymbol{\gamma}\boldsymbol{n} = 0 \quad \textit{and} \quad 0 < h(\boldsymbol{\gamma}) \le c_9(k, F).$$

P r o o f. See [2], Lemma 12, where $c_9(k, F)$ is given explicitly.

LEMMA 3. *If* $F \in \mathbb{Q}[\boldsymbol{x}]$ *is irreducible and non-reciprocal and a matrix* $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ *is non-singular*, *then*

$$LF(\boldsymbol{z}^{\boldsymbol{M}}) = JF(\boldsymbol{z}^{\boldsymbol{M}}).$$

P r o o f. See [7], Lemma 17.

LEMMA 4. *If* $F \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$, $KF = LF$, $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ *and* $\det \boldsymbol{M} \ne 0$, *then*

$$KF(\boldsymbol{z}^{\boldsymbol{M}}) = LF(\boldsymbol{z}^{\boldsymbol{M}}). \tag{17}$$

P r o o f. By Lemma 1 we have, for every polynomial $P \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$,

$$LP \mid KP \mid JP. \tag{18}$$

Assume first that $F$ is irreducible. If $F = cx_i$, $c \in \mathbb{Q}$, then $JF(\boldsymbol{z}^{\boldsymbol{M}}) = c$, hence $KF(\boldsymbol{z}^{\boldsymbol{M}}) = LF(\boldsymbol{z}^{\boldsymbol{M}}) = c$. If $F \mid J(\boldsymbol{x}^{{}^t\boldsymbol{\alpha}} - 1)$ for an $\boldsymbol{\alpha} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$, then $F(\boldsymbol{z}^{\boldsymbol{M}}) \mid J(\boldsymbol{z}^{\boldsymbol{M}{}^t\boldsymbol{\alpha}} - 1)$, hence $KF(\boldsymbol{z}^{\boldsymbol{M}}) \in \mathbb{Q}$ and (18) implies (17). If $F \ne cx_i$ for all $c \in \mathbb{Q}$ and all $i \le k$, and $F \nmid J(\boldsymbol{x}^{{}^t\boldsymbol{\alpha}} - 1)$ for all $\boldsymbol{\alpha} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$, then $KF = F$, hence $KF = LF$ implies that $F$ is not reciprocal. By Lemma 3 we have $LF(\boldsymbol{z}^{\boldsymbol{M}}) = JF(\boldsymbol{z}^{\boldsymbol{M}})$ and (18) implies (17).

Assume now that

$$F \overset{\text{can}}{=} c \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}, \qquad c \in \mathbb{Q}^*.$$

Then

$$KF = c \prod_{\sigma=1}^{s} KF_\sigma^{e_\sigma}, \qquad LF = c \prod_{\sigma=1}^{s} LF_\sigma^{e_\sigma},$$

which together with $KF = LF$ and (18) implies

$$KF_\sigma = LF_\sigma \quad (1 \le \sigma \le s).$$

By the part of the lemma already proved, $KF_\sigma(\boldsymbol{z}^{\boldsymbol{M}}) = LF_\sigma(\boldsymbol{z}^{\boldsymbol{M}})$, hence

$$KF(\boldsymbol{z}^{\boldsymbol{M}}) = c\prod_{\sigma=1}^{s} KF_\sigma(\boldsymbol{z}^{\boldsymbol{M}})^{e_\sigma} = c\prod_{\sigma=1}^{s} LF_\sigma(\boldsymbol{z}^{\boldsymbol{M}})^{e_\sigma} = LF(\boldsymbol{z}^{\boldsymbol{M}}).$$

LEMMA 5. *Let* $\Phi \in \mathbb{Q}[x]$ *be irreducible*, $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_k) \in \mathbb{Z}^k$ *and* $(\gamma_1, \ldots, \gamma_k) = 1$. *Then* $J\Phi(\boldsymbol{x}^{{}^t\gamma})$ *is irreducible.*

Proof. See [4], Lemma 11.

LEMMA 6. *If* $F \in \mathbb{Q}[\boldsymbol{x}]$ *and* $KF \in \mathbb{Q}$, *then for every vector* $\boldsymbol{v} \in \mathbb{Z}^k$ *we have* $KF(x^{\boldsymbol{v}}) \in \mathbb{Q}$.

Proof. It is enough to prove the lemma for $F$ irreducible and different from $cx_i$ $(1 \le i \le k)$, $c \in \mathbb{Q}^*$. The condition $KF \in \mathbb{Q}$ gives

$$F \mid J(\boldsymbol{x}^{{}^t\boldsymbol{\alpha}} - 1), \quad \text{where } \boldsymbol{\alpha} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}.$$

If $\boldsymbol{\alpha v} \ne 0$ the conclusion follows at once, but the case $\boldsymbol{\alpha v} = 0$ remains to be considered.

Let $\boldsymbol{\alpha} = a\boldsymbol{\gamma}$, where $a \in \mathbb{N}$, $\boldsymbol{\gamma} \in \mathbb{Z}^k$ and the coordinates of $\boldsymbol{\gamma}$ are relatively prime. We have

$$J(\boldsymbol{x}^{{}^t\boldsymbol{\alpha}} - 1) = \prod_{d \mid a} J\phi_d(\boldsymbol{x}^{{}^t\gamma}),$$

where $\phi_d$ is the cyclotomic polynomial of order $d$. By Lemma 5, $J\phi_d(\boldsymbol{x}^{{}^t\gamma})$ is irreducible. Hence $F = cJ\phi_d(\boldsymbol{x}^{{}^t\gamma})$ for a $c \in \mathbb{Q}^*$ and a divisor $d$ of $a$. The equality $\boldsymbol{\alpha v} = 0$ gives $\boldsymbol{v}^t\boldsymbol{\gamma} = (0)$, hence $JF(x^{\boldsymbol{v}}) = c\phi_d(1) \in \mathbb{Q}$.

*Proof of Theorem 1.* Let $c_1$ have the meaning of Theorem BZ and $c_9$ the meaning of Lemma 2. We may assume without loss of generality that $F \in \mathbb{Q}[x_1, \ldots, x_{k_0}]$ and apply Lemma 2 with $k$ replaced by $k_0$, $\boldsymbol{n}$ replaced by $\boldsymbol{n}_0 = [n_1, \ldots, n_{k_0}]$, and $\boldsymbol{z}$ replaced by $\boldsymbol{z}_0 = [z_1, \ldots, z_{k_0}]$. Let $\boldsymbol{M}_0$ and $\boldsymbol{v}_0$ be the matrix and the vector the existence of which is asserted in Lemma 2. We put

$$(\mu_{ij})_{i,j \le k_0} = \boldsymbol{M}_0, \quad \mu_{ii} = 1 \text{ if } i > k_0, \quad \mu_{ij} = 0 \text{ if } i > k_0 \text{ or } j > k_0 \text{ and } i \ne j;$$
$$[v_1, \ldots, v_{k_0}] = \boldsymbol{v}_0, \quad v_i = n_i \text{ if } i > k_0.$$

This together with (15) and (16) gives (1) and (2). Moreover, by Lemma 2, either

$$LF(\boldsymbol{z}^{\boldsymbol{M}}) = LF(\boldsymbol{z}_0^{\boldsymbol{M}_0}) \stackrel{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s_0} F_\sigma^0(\boldsymbol{z}_0)^{e_\sigma^0} \tag{19}$$

implies

$$LF(x^{\boldsymbol{n}}) = LF(x^{\boldsymbol{n}_0}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s_0} F_\sigma^0(x^{\boldsymbol{v}_0})^{e_\sigma^0}, \tag{20}$$

or there exists a $\boldsymbol{\gamma}_0 \in \mathbb{Z}^{k_0}$ such that

$$\boldsymbol{\gamma}_0 \boldsymbol{n}_0 = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}_0) \le c_9(k_0, F). \tag{21}$$

By Lemma 4 the left-hand sides of (3) and (19) coincide. Since the canonical factorization is essentially unique we have $s = s_0$ and we may assume that $F_\sigma = F_\sigma^0$, $e_\sigma = e_\sigma^0$ $(1 \le \sigma \le s)$. Therefore $(JF_\sigma(\boldsymbol{z}^{-1}), F_\sigma(\boldsymbol{z})) = 1$ for all $\sigma \le s$ and the number

$$c_3(F, \boldsymbol{M}) = \max\{c_9(k_0, F), \max_{1 \le \sigma \le s} c_1(JF_\sigma(\boldsymbol{z}^{-1}), F_\sigma(\boldsymbol{z}))\} \tag{22}$$

is well defined. We now show that it has the property claimed in the theorem.

By (3) we have

$$F(\boldsymbol{z}^{\boldsymbol{M}}) = F_0(\boldsymbol{z}) \prod_{\sigma=1}^{s} F_\sigma(\boldsymbol{z})^{e_\sigma}, \tag{23}$$

where $KF_0 \in \mathbb{Q}$. Hence on substitution $\boldsymbol{z} = x^{\boldsymbol{v}}$ we obtain, by (2),

$$F(x^{\boldsymbol{n}}) = F_0(x^{\boldsymbol{v}}) \prod_{\sigma=1}^{s} F_\sigma(x^{\boldsymbol{v}})^{e_\sigma},$$

and, on applying $K$ to both sides, by Lemma 6 we infer that

$$KF(x^{\boldsymbol{n}}) = \text{const} \prod_{\sigma=1}^{s} KF_\sigma(x^{\boldsymbol{v}})^{e_\sigma}.$$

If $KF_\sigma(x^{\boldsymbol{v}}) = LF_\sigma(x^{\boldsymbol{v}})$ for all $\sigma \le s$, then since $F_\sigma(x^{\boldsymbol{v}}) = F_\sigma^0(x^{\boldsymbol{v}_0})$, (20) implies (4), while (21) and (22) imply (5) with $\boldsymbol{\gamma} = [\boldsymbol{\gamma}_0, 0, \ldots, 0]$. If $KF_\sigma(x^{\boldsymbol{v}}) \ne LF_\sigma(x^{\boldsymbol{v}})$ for at least one $\sigma \le s$, then $KF_\sigma(x^{\boldsymbol{v}})$ has an irreducible reciprocal factor. Hence

$$(KF_\sigma(x^{-\boldsymbol{v}}), KF_\sigma(x^{\boldsymbol{v}})) \ne 1$$

and by Theorem BZ there is a $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that $\boldsymbol{\gamma}\boldsymbol{n} = 0$ and $0 < h(\boldsymbol{\gamma}) \le c_1(JF_\sigma(\boldsymbol{z}^{-1}), F_\sigma(\boldsymbol{z}))$, which gives (5) by virtue of (22).

Lemma 7. *Let $F \in \mathbb{Q}[\boldsymbol{x}]$ with $KF \notin \mathbb{Q}$. If $\boldsymbol{n} \in \mathbb{Z}^k$ and $KF(x^{\boldsymbol{n}}) \in \mathbb{Q}$, then there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that*

$$\boldsymbol{\gamma}\boldsymbol{n} = 0 \quad \textit{and} \quad 0 < h(\boldsymbol{\gamma}) \le c_{10}(F). \tag{24}$$

Proof. See [7], Lemma 18.

Lemma 8. *Let $G \in \overline{\mathbb{Q}}[\boldsymbol{x}]\backslash\{0\}$, $\boldsymbol{n} \in \mathbb{Z}^k\backslash\{\boldsymbol{0}\}$, $\boldsymbol{K}$ be the field generated over $\mathbb{Q}$ by the ratios of the coefficients of $G(x^{\boldsymbol{n}})$ and $\widehat{\boldsymbol{K}}$ be its normal closure.*

*Assume that* $G \in \boldsymbol{K}[\boldsymbol{x}]$, $G(x^{\boldsymbol{n}}) \neq 0$ *and*

$$JG(x^{-\boldsymbol{n}})/JG^{\tau}(x^{\boldsymbol{n}}) \notin \widehat{\boldsymbol{K}} \quad \textit{for all embeddings } \tau \textit{ of } \boldsymbol{K} \textit{ into } \widehat{\boldsymbol{K}}. \tag{25}$$

*There exist a matrix* $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ *and a vector* $\boldsymbol{v} \in \mathbb{Z}^k$ *such that*

$$\det \boldsymbol{M} \neq 0, \quad h(\boldsymbol{M}) \leq c_{11}(G), \tag{26}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}, \tag{27}$$

*and either*

$$KG(x^{\boldsymbol{n}}) \textit{ is irreducible over } \boldsymbol{K}, \tag{28}$$

*or there exists a vector* $\boldsymbol{\gamma} \in \mathbb{Z}^k$ *such that*

$$\boldsymbol{\gamma}\boldsymbol{n} = 0 \quad \textit{and} \quad 0 < h(\boldsymbol{\gamma}) \leq c_{12}(G), \tag{29}$$

*or*

$$JG(\boldsymbol{z}^{\boldsymbol{M}}) = G_1 G_2, \quad G_i \in \widehat{\boldsymbol{K}}[\boldsymbol{z}] \setminus \widehat{\boldsymbol{K}} \tag{30}$$

*and if* $\boldsymbol{K} = \mathbb{Q}$

$$KG_i(x^{\boldsymbol{v}}) \notin \mathbb{Q} \quad (i = 1, 2). \tag{31}$$

P r o o f. Let $T$ be the set of all embeddings of $\boldsymbol{K}$ into $\widehat{\boldsymbol{K}}$. The assumption (25) implies

$$\frac{JG(\boldsymbol{x}^{-1})}{JG^{\tau}(\boldsymbol{x})} \notin \widehat{\boldsymbol{K}} \quad \text{for all } \tau \in T, \tag{32}$$

hence, in particular, $JG \notin \widehat{\boldsymbol{K}}$. If $JG$ is reducible over $\widehat{\boldsymbol{K}}$ or $\boldsymbol{K} = \mathbb{Q}$ and $KG$ is reducible we have (26), (27) and (30) with $\boldsymbol{M} = \boldsymbol{I}_k$, $\boldsymbol{v} = \boldsymbol{n}$ (provided $c_{11}(G) \geq 1$) and for $\boldsymbol{K} = \mathbb{Q}$ we may additionally assume that

$$KG_i \notin \mathbb{Q} \quad (i = 1, 2). \tag{33}$$

In this last case we have either (31) or, denoting by $l_i$ the leading coefficient of $G$,

$$Kl_i^{-1}G_i(x^{\boldsymbol{n}}) \in \mathbb{Q} \quad \text{for an } i \leq 2.$$

However, $l_i^{-1}G_i$ belongs to a finite set $S$ of monic non-constant divisors $D$ of $JG$ in $\mathbb{Q}[\boldsymbol{z}]$ satisfying $KD \notin \mathbb{Q}$ by virtue of (33). Hence, by Lemma 7, (29) holds provided

$$c_{12}(G) \geq \max_{D \in S} c_{10}(D).$$

It remains to consider the case where $JG$ is irreducible over $\widehat{\boldsymbol{K}}$, or $\boldsymbol{K} = \mathbb{Q}$ and $KG$ is irreducible.

If $JG$ is irreducible over $\widehat{\boldsymbol{K}}$, let $l$ be the leading coefficient of $JG(x^{\boldsymbol{n}})$. Since $JG(x^{\boldsymbol{n}})$ has the same coefficients as $G(x^{\boldsymbol{n}})$, by the definition of $\boldsymbol{K}$, $\tau_1 \neq \tau_2$ implies that for all $\tau_1, \tau_2 \in T$,

$$(l^{-1}JG(x^{\boldsymbol{n}}))^{\tau_1} \neq (l^{-1}JG(x^{\boldsymbol{n}}))^{\tau_2}$$

and since both sides are monic,

$$\frac{(l^{-1}JG(x^{\boldsymbol{n}}))^{\tau_2}}{(l^{-1}JG(x^{\boldsymbol{n}}))^{\tau_1}} \notin \widehat{\boldsymbol{K}}. \tag{34}$$

It follows that $JG^{\tau_2}/JG^{\tau_1} \notin \widehat{\boldsymbol{K}}$, and since $JG^{\tau_1}$, $JG^{\tau_2}$ are both irreducible over $\widehat{\boldsymbol{K}}$, $(JG^{\tau_1}, JG^{\tau_2}) = 1$. If $F$ is the polynomial over $\mathbb{Z}$ with the least positive leading coefficient divisible by $JG$ and irreducible over $\mathbb{Q}$ we find that

$$JN_{\boldsymbol{K}/\mathbb{Q}}G = \prod_{\tau\in T} JG^{\tau} \mid F$$

and, since $JN_{\boldsymbol{K}/\mathbb{Q}}G \in \mathbb{Q}[\boldsymbol{x}] \setminus \mathbb{Q}$, we infer that

$$JN_{\boldsymbol{K}/\mathbb{Q}}G/F \in \mathbb{Q}^*. \tag{35}$$

Moreover, by (32),

$$(JF(\boldsymbol{x}^{-1}), F) = 1,$$

which implies $LF = F$ and, by (18), $KF = LF$.

If $\boldsymbol{K} = \mathbb{Q}$ and $KG$ is irreducible we define $F$ as the polynomial over $\mathbb{Z}$ which is a scalar multiple of $G$ with the least positive leading coefficient. Thus we have (34) and infer, by (32) and (18), that $KF = LF$.

Hence in any case Theorem 1 applies to $F$. By virtue of that theorem and of (34) there exist a matrix $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ and a vector $\boldsymbol{v} \in \mathbb{Z}^k$ such that (26), with $c_{11}(G) = 9k_0 \cdot 2^{\|F\|-5}$, and (27) hold and either

$$KN_{\boldsymbol{K}/\mathbb{Q}}G(\boldsymbol{z}^{\boldsymbol{M}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_{\sigma}(\boldsymbol{z})^{e_{\sigma}} \tag{36}$$

implies

$$KN_{\boldsymbol{K}/\mathbb{Q}}G(x^{\boldsymbol{n}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_{\sigma}(x^{\boldsymbol{v}})^{e_{\sigma}}, \tag{37}$$

or there exists a $\boldsymbol{\gamma}_1 \in \mathbb{Z}^k$ such that

$$\boldsymbol{\gamma}_1\boldsymbol{n} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}_1) \le c_3(F, \boldsymbol{M}) = c_{13}(G, \boldsymbol{M}).$$

In the latter case we have (29) provided

$$c_{12}(G) \ge \max c_{13}(G, \boldsymbol{M}),$$

where the maximum is taken over all matrices $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ satisfying (26). In the former case on the right-hand side of (36) we have $\sum_{\sigma=1}^{s} e_{\sigma} \ge 1$. Indeed, if $\boldsymbol{K} \ne \mathbb{Q}$, then by Lemma 3,

$$LF(\boldsymbol{z}^{\boldsymbol{M}}) = JF(\boldsymbol{z}^{\boldsymbol{M}}),$$

hence by (18),

$$KF(\boldsymbol{z}^{\boldsymbol{M}}) = JF(\boldsymbol{z}^{\boldsymbol{M}}) \notin \mathbb{Q}.$$

If $\boldsymbol{K} = \mathbb{Q}$ the same argument works with $F$ replaced by $KG$.

If $\sum_{\sigma=1}^{s} e_\sigma = 1$, then by (37), $KN_{\boldsymbol{K}/\mathbb{Q}}G(x^{\boldsymbol{n}})$ is irreducible, hence we have (28). If $\sum_{\sigma=1}^{s} e_\sigma \geq 2$, then we have (30). Indeed, otherwise $JG(\boldsymbol{z}^{\boldsymbol{M}})$ would be irreducible over $\widehat{\boldsymbol{K}}$ and would satisfy

$$JG(\boldsymbol{z}^{\boldsymbol{M}}) \mid F_\sigma(\boldsymbol{z}) \tag{38}$$

for a $\sigma \leq s$. Since

$$JG(x^{\boldsymbol{n}}) = JG((x^{\boldsymbol{v}})^{\boldsymbol{M}}),$$

(34) implies that $JG(\boldsymbol{z}^{\boldsymbol{M}})^{\tau_2}/JG(\boldsymbol{z}^{\boldsymbol{M}})^{\tau_1} \notin \widehat{\boldsymbol{K}}$ for any two distinct elements $\tau_1$, $\tau_2$ of $T$. Since $JG(\boldsymbol{z}^{\boldsymbol{M}})^{\tau_1}$, $JG(\boldsymbol{z}^{\boldsymbol{M}})^{\tau_2}$ are both irreducible over $\widehat{\boldsymbol{K}}$,

$$(JG(\boldsymbol{z}^{\boldsymbol{M}})^{\tau_1}, JG(\boldsymbol{z}^{\boldsymbol{M}})^{\tau_2}) = 1$$

and by (38),

$$JN_{\boldsymbol{K}/\mathbb{Q}}G(\boldsymbol{z}^{\boldsymbol{M}}) = \prod_{\tau \in T} JG(\boldsymbol{z}^{\boldsymbol{M}})^{\tau} \mid F_\sigma(\boldsymbol{z}),$$

contrary to (36) under the assumption $\sum_{\sigma=1}^{s} e_\sigma \geq 2$. The contradiction obtained shows (30). If $\boldsymbol{K} = \mathbb{Q}$ the same assumption together with (37) shows the existence of a factorization (30) satisfying (31). Indeed, according to the definition of canonical factorization, $F_\sigma(x^{\boldsymbol{v}}) \notin \mathbb{Q}$ for all $\sigma \leq s$.

*Proof of Theorem 2.* The reducibility condition given in the theorem is clearly sufficient. We proceed to prove that it is necessary. Assume that the condition is necessary for $\mathbb{Q}[x_1, \ldots, x_{k-1}]$, $c_4(F)$ being defined for all polynomials in less than $k$ variables for which it is needed (for $k = 1$ this is an empty statement); assume that $F \in \mathbb{Q}[\boldsymbol{x}]$, $JF(x^{\boldsymbol{n}})$ is not reciprocal and $KF(x^{\boldsymbol{n}})$ is reducible.

Consider first the case where $F$ is of positive degree with respect to all $k$ variables, so that $k$ is determined by $F$. For $k = 1$ this is the only case.

If the matrix $\boldsymbol{M}$ and the vector $\boldsymbol{v}$ appearing in Lemma 8 for $G = F$ have the properties (30) and (31) we take $\boldsymbol{N} = \boldsymbol{M}$, $r = k$, $F_i = (KF, G_i)$ $(i = 1, 2)$ and obtain $h(\boldsymbol{N}) \leq c_{11}(F)$. Otherwise, by Lemma 8, there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that $\boldsymbol{\gamma}\boldsymbol{n} = 0$ and $0 < h(\boldsymbol{\gamma}) \leq c_{12}(F)$. For $k = 1$ this completes the proof, since $\boldsymbol{\gamma}\boldsymbol{n} = 0$ implies $\boldsymbol{n} = \boldsymbol{0}$.

For $k > 1$ the integer vectors perpendicular to $\boldsymbol{\gamma}$ form a lattice, say $\boldsymbol{\Lambda}$. It is easily seen (cf. for instance Lemma 6 in [2]) that $\boldsymbol{\Lambda}$ has a basis that written in the form of a matrix $\boldsymbol{B} \in \mathfrak{M}_{k-1,k}(\mathbb{Z})$ satisfies

$$h(\boldsymbol{B}) \leq \frac{k}{2} c_{12}(F). \tag{39}$$

Let us put

$$\widetilde{F} = JF(\widetilde{\boldsymbol{x}}^{\boldsymbol{B}}), \qquad \text{where } \widetilde{\boldsymbol{x}} = [x_1, \ldots, x_{k-1}]. \tag{40}$$

Since $\boldsymbol{n} \in \boldsymbol{\Lambda}$ we have $\boldsymbol{n} = \boldsymbol{m}\boldsymbol{B}$ for an $\boldsymbol{m} \in \mathbb{Z}^{k-1}$. Clearly

$$JF(x^{\boldsymbol{n}}) = J\widetilde{F}(x^{\boldsymbol{m}}), \tag{41}$$

thus, by assumption, $J\widetilde{F}(x^{\boldsymbol{m}})$ is not reciprocal and $K\widetilde{F}(x^{\boldsymbol{m}})$ is reducible. By the inductive assumption there exist a matrix $\widetilde{\boldsymbol{N}} \in \mathfrak{M}_{r,k-1}(\mathbb{Z})$ of rank $r \le k-1$ and a vector $\boldsymbol{v} \in \mathbb{Z}^r$ such that

$$h(\widetilde{\boldsymbol{N}}) \le c_4(\widetilde{F}), \tag{42}$$

$$\boldsymbol{m} = \boldsymbol{v}\widetilde{\boldsymbol{N}}; \tag{43}$$

$$K\widetilde{F}(\boldsymbol{y}^{\widetilde{\boldsymbol{N}}}) = F_1F_2, \qquad F_i \in \mathbb{Q}[\boldsymbol{y}], \qquad KF_i(x^{\boldsymbol{v}}) \notin \mathbb{Q} \qquad (i = 1, 2).$$

Let us take $\boldsymbol{N} = \widetilde{\boldsymbol{N}}\boldsymbol{B}$. It follows from (40) that $J\widetilde{F}(\boldsymbol{y}^{\widetilde{\boldsymbol{N}}}) = JF(\boldsymbol{y}^{\boldsymbol{N}})$ and from (43) that $\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}$; moreover, since rank $\boldsymbol{B} = k-1$, rank $\boldsymbol{N} = r$. Thus $\boldsymbol{N}$ and $\boldsymbol{v}$ have all the properties required in the theorem apart from (6); it remains to establish (6) by an appropriate choice of $c_4(F)$. We have, by (39) and (42),

$$h(\boldsymbol{N}) \le (k-1)h(\widetilde{\boldsymbol{N}})h(\boldsymbol{B}) \le \binom{k}{2} c_4(\widetilde{F})c_{12}(F).$$

However, $\widetilde{F}$ is determined by $F$ and $\boldsymbol{B}$ via (40) and, by virtue of (39), $\boldsymbol{B}$ runs through a finite set of matrices depending only on $F$. Hence $c_4(\widetilde{F}) \le c_{14}(F)$ and the theorem holds with

$$c_4(F) = \max\left\{c_{11}(F), \binom{k}{2} c_{12}(F)c_{14}(F)\right\}.$$

Consider now the case where $F$ is of positive degree with respect to less than $k$ variables. We may assume that $F \in \mathbb{Q}[\widetilde{\boldsymbol{x}}]$. By the inductive assumption there exist a matrix $\boldsymbol{N}_0 \in \mathfrak{M}_{k-1,r_0}(\mathbb{Z})$ of rank $r_0$ and a vector $\boldsymbol{v}_0 \in \mathbb{Z}^{r_0}$ such that

$$\begin{gathered} h(\boldsymbol{N}_0) \le c_4(F), \qquad [n_1, \ldots, n_k] = \boldsymbol{v}_0\boldsymbol{N}_0, \\ KF(\boldsymbol{y}_0^{\boldsymbol{N}_0}) = F_1F_2, \qquad \boldsymbol{y}_0 = [y_1, \ldots, y_{r_0}], \\ F_i \in \mathbb{Q}[\boldsymbol{y}_0], \qquad KF_i(x^{\boldsymbol{v}_0}) \notin \mathbb{Q} \qquad (i = 1, 2). \end{gathered}$$

We put $r = r_0+1$, $\boldsymbol{N} = \left(\begin{smallmatrix} \boldsymbol{N}_0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\boldsymbol{v} = [\boldsymbol{v}_0, n_k]$ and easily verify that conditions (6)–(9) are satisfied.

*Proof of Theorem 3.* We proceed in the same way as in the proof of the necessity part of Theorem 2, with $\boldsymbol{K}$ instead of $\mathbb{Q}$, using Lemma 8 without the formula (31). Therefore we point out only the argument not needed in the proof of Theorem 2. Before applying the inductive assumption to $\widetilde{F}(x^{\boldsymbol{m}})$

we have to check that $\widetilde{F} \in \boldsymbol{K}[\widetilde{\boldsymbol{x}}]$ and that

$$\frac{J\widetilde{F}(\widetilde{\boldsymbol{x}}^{-\boldsymbol{m}})}{J\widetilde{F}^{\tau}(\widetilde{\boldsymbol{x}}^{\boldsymbol{m}})} \notin \widehat{\boldsymbol{K}} \tag{44}$$

for all embeddings $\tau$ of $\boldsymbol{K}$ into $\widehat{\boldsymbol{K}}$.

Now $\widetilde{F} \in \boldsymbol{K}[\widetilde{\boldsymbol{x}}]$ follows from $F \in \boldsymbol{K}[\boldsymbol{x}]$ and from the definition of $\widetilde{F}$ by the formula (40), while (44) follows from (10) and (41).

LEMMA 9. *If $a_j \neq 0$ $(0 \le j \le k)$ are complex numbers and the rank of a matrix $(\nu_{ij}) \in \mathfrak{M}_{r,k}(\mathbb{Z})$ is greater than $(k+1)/2$, then*

$$J\Big(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{r} x_i^{\nu_{ij}}\Big)$$

*is absolutely irreducible.*

Proof. See [3], Corollary to Theorem 1. The proof of Theorem 1 given there shows less than stated in the theorem, but only in the case of positive characteristic of the ground field, so the Corollary is fully justified.

*Proof of Corollary 1.* We apply Theorem 3 with $F = a_0 + \sum_{j=1}^{k} a_j x_j$ and infer that if $K(a_0 + \sum_{j=1}^{k} a_j x^{n_j})$ is irreducible over $\boldsymbol{K}$, then either

$$\frac{J(a_0 + \sum_{j=1}^{k} a_j x^{-n_j})}{a_0^{\tau} + \sum_{j=1}^{k} a_j^{\tau} x^{n_j}} \in \widehat{\boldsymbol{K}} \tag{45}$$

for an embedding $\tau$ of $\boldsymbol{K}$ into $\widehat{\boldsymbol{K}}$, or there exist a matrix $\boldsymbol{N} = (\nu_{ij}) \in \mathfrak{M}_{r,k}(\mathbb{Z})$ of rank $r$ and a vector $\boldsymbol{v} \in \mathbb{Z}^r$ such that $h(\boldsymbol{N}) \le c_4(F)$, $\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}$ and

$$J\Big(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{r} y_i^{\nu_{ij}}\Big) \text{ is reducible over } \widehat{\boldsymbol{K}}. \tag{46}$$

Let us put $c_6(\boldsymbol{a}) = \max\{2, c_4(F)\}$.

If (45) holds, then $n_j + n_{k-j} = n_k$ $(1 \le j < k)$ and we satisfy (13) and (14) by taking

$$\boldsymbol{v}_0 = \begin{cases} [n_1, \ldots, n_{k/2}] & \text{if } k \text{ is even,} \\ [n_1, \ldots, n_{(k-1)/2}, n_k] & \text{if } k \text{ is odd;} \end{cases}$$

$$\boldsymbol{N}_0 = \begin{pmatrix} 1 & & & & & & & -1 \\ & 1 & & & & & \iddots & \\ & & \ddots & & & -1 & & \\ & & & 1 & -1 & & & \\ & & & & 1 & 2 & 2 \; \ldots & 2 & 2 \end{pmatrix} \quad \text{if } k \text{ is even,}$$

$$N_0 = \begin{pmatrix} 1 & & & & & & & -1 & \\ & 1 & & & & & \iddots & & \\ & & \ddots & & & -1 & & & \\ & & & 1 & 1 & & & & \\ & & & & 1 & 1 & \dots & 1 & 1 \end{pmatrix} \quad \text{if } k \text{ is odd,}$$

where the empty places (but not the dots) denote zeros.

If (46) holds, then by Lemma 9, $r \le (k+1)/2$. If $r = [(k+1)/2]$ we take $\boldsymbol{N}_0 = \boldsymbol{N}$, $\boldsymbol{v}_0 = \boldsymbol{v}$; if $r < (k+1)/2$ we amplify $\boldsymbol{N}$ and $\boldsymbol{v}$ by inserting zeros.

*Proof of Corollary 2.* For each matrix $\boldsymbol{N}_0 \in \mathfrak{M}_{[(k+1)/2],k}(\mathbb{Z})$ the number of vectors $\boldsymbol{n} \in \mathbb{Z}^k$ with $h(\boldsymbol{n}) \le N$ for which there exists a $\boldsymbol{v}_0 \in \mathbb{Z}^{[(k+1)/2]}$ satisfying (14) is less than $c_{15}(\boldsymbol{N}_0)N^{[(k+1)/2]}$. Hence Corollary 2 follows from Corollary 1 with

$$c_7(\boldsymbol{a}) = \sum c_{15}(\boldsymbol{N}_0),$$

where the sum is taken over all matrices $\boldsymbol{N}_0 \in \mathfrak{M}_{[(k+1)/2],k}$ satisfying (13).

REMARK 1. If $k > 1$ and $\sum_{j=0}^{k} a_j = 0$, then the polynomial $a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ is reducible for all vectors $\boldsymbol{n}$ in question. This shows that replacing $a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ by $K(a_0 + \sum_{j=1}^{k} a_j x^{n_j})$ is really needed in order to obtain a non-trivial result.

EXAMPLE. Here is the example announced in the introduction showing that the exponent $[(k+1)/2]$ is best possible in Corollary 2, and hence also in Corollary 1.

If $k = 2l-1$ we take $a_0 = 4$, $a_j = 2$ $(1 \le j \le l)$, $a_j = 1$ $(l < j < 2l)$, $n_j = n_l + n_{j-l}$ $(l < j < 2l)$. It follows that

$$a_0 + \sum_{j=1}^{k} a_j x^{n_j} = \Big(2 + \sum_{j=1}^{l-1} x^{n_j}\Big)(2 + x^{n_l}).$$

The two factors on the right-hand side are not reciprocal, hence $K(a_0 + \sum_{j=1}^{k} a_j x^{n_j})$ is reducible. The number $X$ of relevant vectors $\boldsymbol{n}$ with $n_k \le N$ is at least equal to the number of increasing sequences $n_1 < \ldots < n_l$ with $n_l \le [N/2]$, hence

$$X \ge \binom{[N/2]}{l} \ge c_{16}(l)N^l \quad \text{for } N \ge 2l,$$

where $c_{16}(l) > 0$.

If $k = 2l$ we take $a_0 = 4$, $a_j = 2$ $(1 \le j \le l)$, $a_{l+1} = 3$, $a_j = 1$ $(l+1 < j \le 2l)$, $n_j = n_l + n_{j-l}$ $(l < j < 2l)$, $n_{2l} = 2n_l + n_1$. It follows that

$$a_0 + \sum_{j=1}^{k} a_j x^{n_j} = \Big(2 + \sum_{j=1}^{l-1} x^{n_j} + x^{n_l+n_1}\Big)(2 + x^{n_l}).$$

The two factors on the right-hand side are not reciprocal, hence $K(a_0 + \sum_{j=1}^{k} a_j x^{n_j})$ is reducible. The number $X$ of relevant vectors $\boldsymbol{n}$ with $n_k \le N$ is at least equal to the number of increasing sequences $n_1 < \ldots < n_l$ with $n_l \le [N/3]$, hence

$$X \ge \binom{[N/3]}{l} \ge c_{17}(l) N^l \quad \text{for } N \ge 3l,$$

where $c_{17}(l) > 0$.

LEMMA 10. *For any $k+1$ non-zero complex numbers $a_0, \ldots, a_k$ such that $a_0 \in \boldsymbol{K} = \mathbb{Q}(a_1/a_0, \ldots, a_k/a_0)$ there exist $k+1$ algebraic numbers $\alpha_0, \ldots, \alpha_{k-1}$, $\alpha_k = 1$ such that if $0 = n_0 < n_1 < \ldots < n_k$ and $K(\sum_{j=0}^{l} a_j x^{n_j})$ is reducible over $\boldsymbol{K}$ then either $K(\sum_{j=0}^{l} \alpha_j x^{n_j})$ is reducible over $\boldsymbol{K}_0 = \mathbb{Q}(\alpha_0, \ldots, \alpha_{k-1})$, or there is a vector $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that $\boldsymbol{\gamma}\boldsymbol{n} = 0$ and*

$$0 < h(\boldsymbol{\gamma}) \le c_{18}(\boldsymbol{a}). \tag{47}$$

Proof. See [6], Lemma 5.

*Proof of Corollary 3.* Let $\alpha_i$ have the meaning of Lemma 10. By Corollary 2 the number of relevant vectors $\boldsymbol{n}$ for which $n_k \le N$ and $K(\sum_{j=0}^{k} \alpha_j x^{n_j})$ is reducible over $\mathbb{Q}(\alpha_0, \ldots, \alpha_{k-1})$ is less than $c_7(\boldsymbol{\alpha}) N^{[(k+1)/2]}$. For a fixed $\boldsymbol{\alpha} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$ the number of relevant vectors $\boldsymbol{n} \in \mathbb{Z}^k$ with $n_k \le N$ such that $\boldsymbol{\gamma}\boldsymbol{n} = 0$ is less than $c_{19}(\boldsymbol{\gamma}) N^{k-1}$. Hence Corollary 3 holds with

$$c_8(\boldsymbol{a}) = c_7(\boldsymbol{\alpha}) + \sum c_{19}(\boldsymbol{\gamma}),$$

where the sum is taken over all vectors $\boldsymbol{\gamma} \in \mathbb{Z}^k$ satisfying (47).

REMARK 2. It seems likely that by improving Lemma 10 one can replace the exponent $k-1$ in Corollary 3 by $[(k+1)/2]$.

*Proof of Theorem 4.* We begin by defining subsets $S_i$ and $R_i$ of $\mathfrak{M}_{k-i,k}(\mathbb{Z})$ $(0 \le i < k)$ inductively, as follows:

$$S_0 = \{\boldsymbol{I}_k\}, \tag{48}$$

and supposing that $S_i$ is already defined and $\boldsymbol{y} = [y_1, \ldots, y_{k-i}]$,

$$\begin{aligned} R_i = \{\boldsymbol{M}\boldsymbol{N} : \boldsymbol{N} \in S_i,\ \boldsymbol{M} \in \mathfrak{M}_{k-i,k-i}(\mathbb{Z}),\ \det \boldsymbol{M} \ne 0,\\ h(\boldsymbol{M}) \le c_{11}(F(\boldsymbol{y}^{\boldsymbol{N}})),\ KF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}}) \text{ is reducible}\}, \end{aligned} \tag{49}$$

and for $i < k-1$,

$$\begin{aligned} S_{i+1} = \big\{\boldsymbol{N} \in \mathfrak{M}_{k-i-1,k}(\mathbb{Z}) : \operatorname{rank} \boldsymbol{N} = k-i-1,\\ h(\boldsymbol{N}) \le \tfrac{1}{2}(k-i)^2 \max_{\boldsymbol{N}_1 \in S_i} \{h(\boldsymbol{N}_1) \max\{\max c_{12}(F(\boldsymbol{y}^{\boldsymbol{N}_1})),\\ \max{}^*(k-1) c_{10}(D) h(\boldsymbol{M})\}\}\big\} \end{aligned} \tag{50}$$

where $\max^*$ is taken over all $\boldsymbol{M} \in \mathfrak{M}_{k-i,k-i}(\mathbb{Z})$ with $\det \boldsymbol{M} \neq 0$, $h(\boldsymbol{M}) \leq c_{11}(F(\boldsymbol{y}^{\boldsymbol{N}_1}))$ and all monic irreducible divisors $D$ of $KF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1})$. (If $KF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1}) \in \mathbb{Q}$ we take $\max^* = 0$.)

In this way $R_i$ and $S_i$ are defined for all $i < k$ and we put

$$R = \bigcup_{i=0}^{k-1} R_i, \qquad S = \bigcup_{i=1}^{k-1} S_i.$$

We first prove that the condition given in the theorem is necessary. By (48) there exist indices $i$ such that

$$\boldsymbol{n} = \boldsymbol{u}\boldsymbol{U}, \quad \boldsymbol{U} \in S_{k-i}, \quad \boldsymbol{u} \in \mathbb{Z}^i.$$

Let $r$ be the least such index and

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}, \quad \boldsymbol{N} \in S_{k-r}, \quad \boldsymbol{v} \in \mathbb{Z}^r. \tag{51}$$

By Lemma 8 if $KF(x^{\boldsymbol{n}}) = KF(x^{\boldsymbol{v}\boldsymbol{N}})$ is reducible, then there exists a matrix $\boldsymbol{M} \in \mathfrak{M}_{r,r}(\mathbb{Z})$ such that

$$\det \boldsymbol{M} \neq 0, \quad h(\boldsymbol{M}) \leq c_{11}(F(\boldsymbol{y}^{\boldsymbol{N}})), \quad \boldsymbol{y} = [y_1, \ldots, y_r], \tag{52}$$

$$\boldsymbol{v} = \boldsymbol{v}_1\boldsymbol{M}, \quad \boldsymbol{v}_1 \in \mathbb{Z}^r \tag{53}$$

and either $KF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}})$ is reducible, or there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^r$ such that

$$\boldsymbol{\gamma}\boldsymbol{v} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}) \leq c_{12}(F(\boldsymbol{y}^{\boldsymbol{N}})).$$

The second possibility can only hold for $r > 1$ since for $r = 1$ it gives $\boldsymbol{v} = \boldsymbol{0}$ and by (51), $\boldsymbol{n} = \boldsymbol{0}$. For $r > 1$ the vectors $\boldsymbol{v}$ perpendicular to $\boldsymbol{\gamma}$ form a lattice $\boldsymbol{\Lambda}$ in $\mathbb{Z}^r$. This lattice has a basis that written in the form of a matrix $\boldsymbol{B} \in \mathfrak{M}_{r-1,r}(\mathbb{Z})$ satisfies

$$\operatorname{rank} \boldsymbol{B} = r - 1, \tag{54}$$

$$h(\boldsymbol{B}) \leq \frac{r}{2} h(\boldsymbol{\gamma}) \leq \frac{r}{2} c_{12}(F(\boldsymbol{y}^{\boldsymbol{N}})) \tag{55}$$

(cf. Lemma 6 in [2]). Since $\boldsymbol{v} \in \boldsymbol{\Lambda}$ we have

$$\boldsymbol{v} = \boldsymbol{w}\boldsymbol{B}, \quad \boldsymbol{w} \in \mathbb{Z}^{r-1},$$

hence, by (51),

$$\boldsymbol{n} = \boldsymbol{w}\boldsymbol{B}\boldsymbol{N}, \quad \boldsymbol{B}\boldsymbol{N} \in \mathfrak{M}_{r-1,k}(\mathbb{Z}). \tag{56}$$

Since, by (50) and (51), $\operatorname{rank} \boldsymbol{N} = r$, it follows from (54), by linear algebra, that

$$\operatorname{rank} \boldsymbol{B}\boldsymbol{N} = r - 1.$$

Moreover, by (55),

$$h(\boldsymbol{B}\boldsymbol{N}) \leq r h(\boldsymbol{B}) h(\boldsymbol{N}) \leq \frac{r^2}{2} h(\boldsymbol{N}) c_{12}(F(\boldsymbol{y}^{\boldsymbol{N}}))$$

and, by (50), $\boldsymbol{B}\boldsymbol{N} \in S_{k-r+1}$, contrary, in view of (56), to the definition of $r$. The contradiction obtained proves that $KF(\boldsymbol{y}^{\boldsymbol{MN}})$ is reducible, hence $\boldsymbol{MN} \in R_{k-r}$ by (49). By (51) and (53) we have

$$\boldsymbol{n} = \boldsymbol{v}_1 \boldsymbol{MN},$$

while by the definition of $r$ the equation $\boldsymbol{n} = \boldsymbol{uU}$ in unsoluble in $\boldsymbol{u} \in \mathbb{Z}^i$, $\boldsymbol{U} \in S_{k-i}$ for $i < r$. Thus the condition given in the theorem is necessary.

Now we prove that it is sufficient. Assume that for a certain matrix $\boldsymbol{N} \in R_{k-r}$ $(1 \le r \le k)$,

$$\boldsymbol{n} = \boldsymbol{vN}, \quad \boldsymbol{v} \in \mathbb{Z}^r, \tag{57}$$

but

$$\boldsymbol{n} \ne \boldsymbol{uU} \quad \text{for all } s < r, \quad \boldsymbol{u} \in \mathbb{Z}^s, \quad \boldsymbol{U} \in S_{k-s}. \tag{58}$$

Then by (49),

$$\boldsymbol{n} = \boldsymbol{vMN}_1, \quad \boldsymbol{N}_1 \in S_{k-r}, \quad \boldsymbol{M} \in \mathfrak{M}_{r,r}(\mathbb{Z}), \quad \det \boldsymbol{M} \ne 0,$$
$$h(\boldsymbol{M}) \le c_{11}(F(\boldsymbol{y}^{\boldsymbol{N}_1})), \quad \boldsymbol{y} = [y_1, \ldots, y_r]$$

and

$$KF(\boldsymbol{y}^{\boldsymbol{MN}_1}) = F_1 F_2, \quad F_1, F_2 \in \mathbb{Q}[\boldsymbol{y}] \setminus \mathbb{Q}.$$

Hence

$$KF(x^{\boldsymbol{n}}) = KF_1(x^{\boldsymbol{v}})KF_2(x^{\boldsymbol{v}}). \tag{59}$$

Suppose that for an $i \le 2$ we have $KF_i(x^{\boldsymbol{v}}) \in \mathbb{Q}$. Then $KD(x^{\boldsymbol{v}}) \in \mathbb{Q}$ for an irreducible monic factor $D$ of $KF$, hence by Lemma 7 there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^r$ such that

$$\boldsymbol{\gamma v} = 0, \quad 0 < h(\boldsymbol{\gamma}) \le c_{10}(D).$$

Again this can occur only for $r > 1$ and, repeating the argument about the lattice given above, we find a matrix $\boldsymbol{B} \in \mathfrak{M}_{r-1,r}(\mathbb{Z})$ such that

$$\operatorname{rank} \boldsymbol{B} = r - 1, \quad h(\boldsymbol{B}) \le \frac{r}{2} h(\boldsymbol{\gamma}) \le \frac{r}{2} c_{10}(D);$$
$$\boldsymbol{v} = \boldsymbol{wB}, \quad \boldsymbol{w} \in \mathbb{Z}^{r-1}.$$

It follows that

$$\boldsymbol{n} = \boldsymbol{wBMN}_1, \quad \boldsymbol{BMN}_1 \in \mathfrak{M}_{r-1,k}(\mathbb{Z}), \tag{60}$$
$$\operatorname{rank} \boldsymbol{BMN}_1 = r - 1,$$
$$h(\boldsymbol{BMN}_1) \le r^2 h(\boldsymbol{B}) h(\boldsymbol{M}) h(\boldsymbol{N}_1) \le \frac{r^3}{2} c_{10}(D) h(\boldsymbol{M}) h(\boldsymbol{N}_1),$$

hence by (50),

$$\boldsymbol{BMN}_1 \in S_{k-r+1},$$

which together with (59) contradicts (58). The contradiction obtained shows that $KF_i(x^{\boldsymbol{v}}) \notin \mathbb{Q}$ $(i = 1, 2)$, hence by (59), $KF(x^{\boldsymbol{n}})$ is reducible.

**References**

[1] E. Bombieri and U. Zannier, *Intersections of varieties with* 1*-dimensional tori and a conjecture of Schinzel*, preprint; see also U. Zannier, *Proof of Conjecture 1*, appendix in the book by A. Schinzel, *Polynomials with Special Regard to Reducibility*, to be published by Cambridge University Press.
[2] A. Schinzel, *Reducibility of lacunary polynomials I*, Acta Arith. 16 (1969), 123–159.
[3] —, *A general irreducibility criterion*, J. Indian Math. Soc. (N.S.) 37 (1973), 1–8.
[4] —, *Reducibility of lacunary polynomials III*, Acta Arith. 34 (1978), 227–266.
[5] —, *Reducibility of lacunary polynomials VII*, Monatsh. Math. 102 (1986), 309–337.
[6] —, *Reducibility of lacunary polynomials VIII*, Acta Arith. 50 (1988), 91–106.
[7] —, *Reducibility of lacunary polynomials X*, ibid. 53 (1989), 47–97.
[8] —, *Reducibility of lacunary polynomials XI*, ibid. 57 (1991), 165–175.

Institute of Mathematics
Polish Academy of Sciences
P.O. Box 137
00-950 Warszawa, Poland
E-mail: schinzel@impan.gov.pl

*Received on 20.11.1998* (3512)