[4] Ю. В. Нестеренко, *Оценки порядков нулей функций некоторого класса*. Матем. заметки 33 (2) (1983), 195–205.
[5] — *Оценки характеристической функции простого идеала*, Матем. сборник 123 (165) (1) (1984), 11–34.
[6] — *Об алгебраической независимости алгебраических степеней алгебраических чисел*, ibid. 123 (165) (4) (1984), 435–459.
[7] — *О мере алгебраической независимости значений эллиптической функции в алгебраических точках*, Успехи матем. наук, 40 (4) (1985), 221–222.
[8] — *О мере алгебраической независимости значений некоторых функций*, Матем. сборник, 128 (170) (4) (1985), 545–568.
[9] Нгуен Тьен Тай, *Об оценках порядков нулей многочленов от аналитических функций и их приложении к оценкам мер взаимной трансцендентности значений E-функций*, ibid. 120 (162) (1) (1983), 112–142.
[10] W. L. Chow, B. L. Van der Waerden, *Zur algebraischen Geometrie, IX*, Math. Ann. 113 (1937), 692–704.
[11] K. Hentzelt, *Zur Theorie der Polynomideale und Resultanten*, ibid. 88 (1923), 53–79.
[12] W. Krull, *Parameterspezialisierung in Polynomringen II*, Arch. Math. 1 (2) (1984), 129–137.
[13] E. Noether, *Eliminationstheorie und allgemeine Idealtheorie*, Math. Ann. 90 (1923), 229–261.
[14] D. Bertrand, F. Beukers, *Equations différentielles linéaires et majorations de multiplicités*, Ann. Scient. Ec. Norm. Sup., 4 sér., 18 (1985), 181–192.
[15] W. D. Brownawell, *Effectivity in independence measures for values of E-functions*, J. Austral. Math. Soc., ser. A, 39 (1985), 227–240.
[16] P. Philippon, *Critères d'indépendence algébrique*, Publ. Math. IHES 64 (1986).

Поступило 29.9.1986
и в исправленной форме 21.1.1987 (1675)

ACTA ARITHMETICA
LIII (1989)

Reducibility of lacunary polynomials, X

by

A. SCHINZEL (Warszawa)

In memory of V. G. Sprindžuk

1. Introduction. The main aim of this paper is to study the reducibility over the rational field Q of polynomials $F(x^{n_1}, x^{n_2}, \ldots, x^{n_k})$, where $k \geqslant 3$ and $F \in Z[x_1, \ldots, x_k]$ is a non-reciprocal polynomial. For $k = 3$ we shall establish a special case of the conjecture formulated in [8] and give a necessary and sufficient condition for reducibility over Q, apart from cyclotomic factors, of every non-reciprocal $F(x^{n_1}, x^{n_2}, x^{n_3})$. For $k > 3$ we estimate the number of integer vectors $\boldsymbol{n} = [n_1, n_2, \ldots, n_k]$ satisfying $h(\boldsymbol{n}) = \max_{1 \leqslant i \leqslant k} |n_i| \leqslant N$, for which the said conjecture fails. This estimate leads to an analogue of Hilbert's irreducibility theorem. The starting point is the following theorem, which seems of independent interest.

THEOREM 1. *Let K be any field, $P, Q \in K[x_1, \ldots, x_k]$, $(P, Q) = 1$ and either* $\operatorname{char} K > 0$ *or* $\operatorname{char} K = 0$, $k \leqslant 3$. *There exists a number $c_1(P, Q)$ with the following property. If $\boldsymbol{n} = [n_1, n_2, \ldots, n_k] \in Z^k$, $\xi \neq 0$ is in the algebraic closure of K and*

$$P(\xi^{n_1}, \xi^{n_2}, \ldots, \xi^{n_k}) = Q(\xi^{n_1}, \xi^{n_2}, \ldots, \xi^{n_k}) = 0 \tag{1}$$

then either $\xi^q = 1$ for a suitable integer $q > 0$ or there is a vector $\gamma \in Z^k$ such that

$$0 < h(\gamma) \leqslant c_1(P, Q)$$

and

$$\gamma \boldsymbol{n} = 0.$$

For $K = Q$, k arbitrary, the special case $(P, Q) = 1$ of Lemma 9 in [9] asserts under the same assumption (1) that either ξ is conjugate over Q to ξ^{-1} or $\boldsymbol{\beta n} = 0$ with $\boldsymbol{\beta} \in Z^k$,

$$0 < h(\boldsymbol{\beta}) < c_1^*(P, Q), \tag{2}$$

where $c_1^*(P, Q)$ is explicitly given in terms of the degree and of the coefficients of P, Q supposed integral.

From the proof of Theorem 1 given below an explicit expression for $c_1(P, Q)$, in the case $k = 3$, $P, Q \in \mathbf{Z}[x_1, x_2, x_3]$, can also be derived and preliminary calculations show that it is smaller than $c_1^*(P, Q)$. However the calculations are cumbersome and therefore not included.

For $k > 3$ the method of proof of Theorem 1 gives the following

THEOREM 2. *Let $P, Q \in \mathbf{C}[x_1, \ldots, x_k]$, $(P, Q) = 1$. The number of integer vectors $\mathbf{n} = [n_1, n_2, \ldots, n_k]$ such that*

$$\max_{1 \leqslant i \leqslant k} |n_i| \leqslant N,$$

and for some ξ (1) holds, but $\xi^q \neq 0, 1$ for every integer $q > 0$, is less than

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

where for $k < 6$ the logarithmic factors can be omitted.

Formulating precisely the consequences of Theorem 1 and 2 concerning reducibility of polynomials over $\mathbf{Q}$ we shall use the notation introduced in the former papers of this series, which we recall for the convenience of the reader.

For a field $\mathbf{K}$ and a non-zero polynomial $F \in \mathbf{K}[x_1, \ldots, x_k]$ the notation

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

means, in addition to the equality, that polynomials F_σ are irreducible over $\mathbf{K}$ and relatively prime in pairs. If $\mathbf{K} = \mathbf{Q}$ the letter $\mathbf{K}$ is omitted from the symbol $\overset{\text{can}}{\underset{\mathbf{K}}{=}}$. Reducibility without qualification means reducibility over $\mathbf{Q}$.

If $\phi = \prod_{i=1}^{k} x_i^{\alpha_i} F(x_1, \ldots, x_k)$ where α_i are integers, not necessarily positive, $F \in \mathbf{K}[x_1, \ldots, x_k]$ and $(F, \prod_{i=1}^{k} x_i) = 1$ we set

$$J\phi = F.$$

A polynomial $F \in \mathbf{K}[x_1, \ldots, x_k]$ is called *reciprocal* if

$$JF(x_1^{-1}, \ldots, x_k^{-1}) = \pm F(x_1, \ldots, x_k).$$

If

$$J\phi \overset{\text{can}}{\underset{\mathbf{K}}{=}} \text{const} \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$$

we set

$$LF = \text{const} \prod_{\sigma=1}^{s}{}^{*} F_\sigma^{e_\sigma} \quad (\text{only for } \mathbf{K} = \mathbf{Q}), \qquad KF = \text{const} \prod_{\sigma=1}^{s}{}^{**} F_\sigma^{e_\sigma},$$

where $\prod^*$ is extended over all factors F_σ that are not reciprocal, $\prod^{**}$ is extended over all factors F_σ not dividing $J(\prod_{i=1}^{k} x_i^{\delta_i} - 1)$, for any vector $[\delta_1, \ldots, \delta_k] \neq [0, \ldots, 0]$.

In particular, if $F \in \mathbf{Q}[x]$, KF is JF deprived of all its cyclotomic factors. The leading coefficient of KF is by definition equal to that of F. $J0 = K0 = L0 = 0$. For a polynomial $F \in \mathbf{Q}[x_1, \ldots, x_k]$ $\|F\|$ is the sum of the squares of the coefficients of F,

$$|F| = \max_i \deg_{x_i} F.$$

For a vector $\mathbf{a} \in \mathbf{R}^k$ its coordinates are denoted by $a_1, \ldots, a_k$; $h(\mathbf{a}) = \max_{1 \leqslant i \leqslant k} |a_i|$. The scalar product of vectors $\mathbf{a}$, $\mathbf{b}$ is denoted by $\mathbf{ab}$, the vector product by $\mathbf{a} \times \mathbf{b}$, otherwise vectors are treated as matrices with one row. For a matrix $\mathbf{A} = [a_{ij}]$, $h(\mathbf{A}) = \max |a_{ij}|$, for an algebraic number θ $h(\theta)$ is the usual height. Small bold face letters denote vectors, capital bold face letters sets, fields or matrices, $c_1(P, Q), \ldots, c_{65}(k, \mathbf{S})$ denote real numbers depending only on the specified arguments.

We have

THEOREM 3. *Let $F \in \mathbf{Z}[x_1, x_2, x_3]$ be irreducible and non-reciprocal. There exists a number $c_3(F)$ with the following property. For every vector $\mathbf{n} \in \mathbf{Z}^3$ there exists an integral square matrix $\mathbf{M} = [\mu_{ij}]$ of order three and a vector $\mathbf{v} = [v_1, v_2, v_3] \in \mathbf{Z}^3$ such that*

$$(3_1) \qquad 0 \leqslant \mu_{ij} \leqslant \mu_{jj} < \exp 27 \cdot 2^{\|F\|-5} \quad (i \neq j), \qquad \mu_{ij} = 0 \quad (i < j),$$

$$(3_2) \qquad \mathbf{n} = \mathbf{vM}$$

and either

$$(4_1) \qquad JF\Big(\prod_{i=1}^{3} y_i^{\mu_{i1}}, \prod_{i=1}^{3} y_i^{\mu_{i2}}, \prod_{i=1}^{3} y_i^{\mu_{i3}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, y_2, y_3)^{e_\sigma}$$

implies $e_\sigma = 1$ $(1 \leqslant \sigma \leqslant s)$,

$$(4_2) \qquad KF(x^{n_1}, x^{n_2}, x^{n_3}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} KF_\sigma(x^{v_1}, x^{v_2}, x^{v_3})$$

or there exists a vector $\gamma \in \mathbf{Z}^3$ such that

$$0 < h(\gamma) \leqslant c_3(F)$$

and

$$\gamma \mathbf{n} = 0.$$

THEOREM 4. *For every polynomial $F \in \mathbf{Z}[x_1, x_2, x_3]$ there exist numbers $c_4(r, F)$ $(1 \leqslant r \leqslant 3)$ with the following property.*

If $\mathbf{n} = [n_1, n_2, n_3] \in \mathbf{Z}^3$ and $JF(x^{n_1}, x^{n_2}, x^{n_3})$ is not reciprocal

$KF(x^{n_1}, x^{n_2}, x^{n_3})$ is reducible if and only if there exist an integral matrix $N = [\nu_{ij}]_{\substack{i \le r\\ j\le 3}}$ of rank r and a vector $v \in Z^r$ such that

$$0 < h(N) \leqslant c_4(r, F),$$
$$n = vN,$$
$$KF\Big(\prod_{i=1}^{r} y_i^{\nu_{i1}}, \prod_{i=1}^{r} y_i^{\nu_{i2}}, \prod_{i=1}^{r} y_i^{\nu_{i3}}\Big) = G_1 G_2, \quad G_i \in Z[y_1, \ldots, y_r] \quad (i = 1, 2)$$

and

$$KG_i(x^{v_1}, \ldots, x^{v_r}) \notin Z \quad (i = 1, 2).$$

A result similar to Theorem 3, but concerning polynomials in two variables has been given as Theorem 2 of [8]. The comparison shows two differences. First that theorem asserted for every vector $n \in (Z^+)^2$ the existence of an integral non-singular matrix M with properties similar to (3) and (4) (M not necessarily triangular) and with nonnegative entries, while in Theorem 3 above the components of v may be negative. Secondly, on the right-hand side of the equality corresponding to (4_2) the factors occurred with exponents e_σ, while in (4_2) they occur with exponent 1. In fact the exponents must be 1 for every non-singular matrix M, as it has been shown in [9], p. 148. As to the first difference, in virtue of the results of Schmidt [15] and Low [7] the nonnegativity of the components of v can be achieved for $n \in (Z^+)^3$ at the cost of loosing the triangular form of M, but the additional complicacy in the proof would obscure the idea of the argument.

A result similar to Theorem 4, but concerning polynomials in two variables has been given as Theorem 3 in [9]. The comparison shows again two differences. First, the assumption of the present theorem is, at least for an irreducible F, stronger: it is assumed that $JF(x^{n_1}, x^{n_2}, x^{n_3})$ is not reciprocal, while in [9] it was assumed only that $KF(x_1, x_2) = LF(x_1, x_2)$. Secondly, the assertion of the present theorem is weaker: it gives only a necessary and sufficient condition for reducibility of $KF(x^{n_1}, x^{n_2}, x^{n_3})$, while in [9] the factorization of $KF(x^{n_1}, x^{n_2})$ into irreducible factors was completely described. These deficiences are inherent in the present approach.

Theorem 2 has the following application to reducibility of polynomials over Q.

THEOREM 5. *Let $k > 1$, $F \in Z[x_1, \ldots, x_k]$ be a non-reciprocal irreducible polynomial. There exists a subset $S(F)$ of Z^k with the following properties:*

(i) card $\{n \in S(F)\colon h(n) \leqslant N\} = O\Big(N^{k - \frac{\min\{k,6\}}{2(k-1)}} \dfrac{(\log N)^{10}}{(\log\log N)^9}\Big)$, *where for $k < 6$ the logarithmic factors can be omitted.*

(ii) *For every $n \in Z^k \setminus S(F)$ there exists an integral square matrix $M = [\mu_{ij}]$ of order k and a vector $v \in Z^k$ such that*

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

(5) $$n = vM$$

and

(6_1) $$JF\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, \ldots, y_k)^{e_\sigma}$$

implies $e_\sigma = 1$ $(1 \leqslant \sigma \leqslant s)$ and

(6_2) $$KF(x^{n_1}, \ldots, x^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} KF_\sigma(x^{v_1}, \ldots, x^{v_k}).$$

This theorem implies easily

THEOREM 6. *Let S be a set of positive integers with the counting function $S(x) = \Omega(x^{1-\varepsilon})$ for every $\varepsilon > 0$. If $F_g \in Q[x_1, \ldots, x_k]$ $(1 \leqslant g \leqslant h)$ are non-reciprocal polynomials such that $F_g(x_1^d, \ldots, x_k^d)$ is irreducible for all $g \leqslant h$, and all integers $d > 0$, then there exist infinitely many vectors $n = [n_1, \ldots, n_k] \in S^k$ such that $KF_g(x^{n_1}, \ldots, x^{n_k})$ is irreducible for all $g \leqslant h$.*

This theorem shows some similarity both to Theorem 3 of [12] (which can be deduced from it, if in the notation of that paper $[K_g : Q] < \infty$ for all $g \leqslant h$) and to Hilbert's irreducibility theorem. The condition that $F_g(x_1^d, \ldots, x_k^d)$ is irreducible for all $d > 0$ cannot be replaced even for $h = 1$ by the condition that F_g is itself irreducible. We shall give a relevant counterexample at the end of the paper. Also there we shall explain the difficulty of extending Theorem 6 to the case where the coefficients of F_g are irrational and the irreducibility is considered over the field generated by the ratios of these coefficients.

2. Twelve lemmata.

LEMMA 1. *For every non-zero vector $n \in Z^k$ there exists two linearly independent vectors p, $q \in Z^k$ and integers u, v such that*

$$n = up + vq,$$
$$h(p)h(q) \leqslant c_0(k)\, h(n)^{(k-2)/(k-1)}$$

where $c_0(3) = \sqrt{\tfrac{4}{3}}$ and $c_0(k) \leqslant 2$ for $k > 3$.

Proof, see [3] and [14].

LEMMA 2. *Let S be a finite subset of $C[y_1, y_2]$, $\text{g.c.d.}_{F \in S} F = 1$. There exists a constant $c_6(S)$ with the following property.*

If $[n_1, n_2] \in Z^2$ and

(7) $$\text{g.c.d.}_{F \in S}\, KF(x^{n_1}, x^{n_2}) \neq 1$$

then

$$\max\{|n_1|, |n_2|\} \leqslant c_6(S)(n_1, n_2),$$

where $(0, 0) = 0$.

Proof. We begin with an observation already used in [13] that an equation $\alpha_1^{n_2} = \alpha_2^{n_1}$, where α_1, α_2 are complex numbers different from 0 and roots of unity and n_1, n_2 are non-zero integers, determines uniquely the fraction n_1/n_2. The height of this number will be denoted by $C(\alpha_1, \alpha_2)$. If the equation $\alpha_1^{n_2} = \alpha_2^{n_1}$ implies $n_1 = n_2 = 0$ we set $C(\alpha_1, \alpha_2) = 0$.

By the choice of S there exist only finitely many zeros $(\alpha_{j1}, \alpha_{j2})$ $(1 \leqslant j \leqslant j_0)$ common to all $F \in S$ and if (7) holds then for some ξ different from 0 and roots of unity and a suitable $j \leqslant j_0$ we have

$$\xi^{n_1} = \alpha_{j1}, \quad \xi^{n_2} = \alpha_{j2}.$$

If $n_1 n_2 \neq 0$ it follows that α_{j1}, α_{j2} are not roots of unity,

$$\alpha_{j1}^{n_2} = \alpha_{j2}^{n_1}$$

and

$$\frac{\max\{|n_1|, |n_2|\}}{(n_1, n_2)} = C(\alpha_{j1}, \alpha_{j2}).$$

If $n_1 n_2 = 0$ we have $\max\{|n_1|, |n_2|\} = (n_1, n_2)$. Therefore it suffices to take

$$c_6(S) = \max\{\max_{j \leqslant j_0} C(\alpha_{j1}, \alpha_{j2}), 1\}.$$

LEMMA 3. *Let* $P, Q \in C[x_1, \ldots, x_k]$, $(P, Q) = 1$. *If* $p, q \in Z^k$,

$$D(y, z) = \big(JP(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k}), JQ(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k})\big) \in C[y, z] \setminus C[z],$$

then there exist two linearly independent vectors $l_1, l_2 \in Z^k$ *such that*

$$h(l_1) \leqslant \min\{|P|, |Q|\},$$

$$h(l_2) \leqslant 2|P||Q|,$$

$$(l_1 p)(l_2 q) = (l_1 q)(l_2 p)$$

and

$$l_2 q = 0 \quad \text{if} \quad l_2 p = 0.$$

Proof. Without loos of generality we may assume that

$$|P| \leqslant |Q|.$$

Let

$$P = \sum_{\alpha \in A} \pi_\alpha \sum_{j=1}^{k} x_j^{\alpha_j},$$

where $A \subset Z^k$ and $\pi_\alpha \neq 0$ for $\alpha \in A$. We have

$$JP(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k}) = \sum_{\alpha \in A} \pi_\alpha y^{(\alpha - \alpha_1)p} z^{(\alpha - \alpha_2)q}, \tag{8}$$

for some $\alpha_1, \alpha_2 \in A$. Let

$$D(y, z) = \sum_{\langle a,b \rangle \in D} d_{ab} y^a z^b, \quad \text{where } d_{ab} \neq 0 \text{ for } \langle a, b \rangle \in D.$$

By the assumption

$$D(y, z) \in C[y, z] \setminus C[z],$$

hence D is not contained in a line $a = \text{const}$ and we can find for it a supporting line L, i.e. such a line $a\lambda + b = \mu$ on the plane ab containing two or more points of D that all the remaining points of D lie above it. Let

$$D_0(y, z) = \sum_{\langle a,b \rangle \in D \cap L} d_{ab} y^a z^b.$$

Define the weight of a term $cy^a z^b$ $(c \neq 0)$ as $a\lambda + b$. Clearly D_0 divides the part P_0 of $JP(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k})$ consisting of all terms with the minimal weight. Since D_0 contains at least two terms, also P_0 contains at least two terms. However, by (8)

$$P_0(y, z) = \sum_{\alpha \in A_0} \pi_\alpha y^{(\alpha - \alpha_1)p} z^{(\alpha - \alpha_2)q},$$

where $A_0 \subset A$. Taking two distinct elements α_3, α_4 of A_0 we get

$$\lambda(\alpha_3 - \alpha_1)p + (\alpha_3 - \alpha_2)q = \lambda(\alpha_4 - \alpha_1)p + (\alpha_4 - \alpha_2)q,$$

thus

$$\lambda(\alpha_4 - \alpha_3)p + (\alpha_4 - \alpha_3)q = 0.$$

Putting $l_1 = \alpha_4 - \alpha_3$ we get

$$0 < h(l_1) \leqslant |P| = \min\{|P|, |Q|\}$$

and

$$\lambda l_1 p + l_1 q = 0. \tag{9}$$

Since $l_1 \neq 0$ we may assume without loss of generality that $l_{1k} \neq 0$. Let us consider the resultant of P and Q with respect to x_k. Since $(P, Q) = 1$ this resultant $R \in C[x_1, \ldots, x_{k-1}]$ is different from 0. By Lemma 5 of [9] we have

$$|R| \leqslant 2|P||Q|. \tag{10}$$

From the fundamental property of resultants

$$R = UP + VQ, \quad \text{where } U, V \in C[x_1, x_2, \ldots, x_k].$$

Hence by the definition of D

$$D(y, z) \mid JR(y^{p_1}z^{q_1}, \ldots, y^{p_{k-1}}z^{q_{k-1}}).$$

By the same argument about D_0 as before it follows that for some vectors $\gamma_1, \gamma_2 \in Z^{k-1}\times\{0\}$ we have

$$0 < h(\gamma_2-\gamma_1) \leqslant |R|, \tag{11}$$

$$\lambda(\gamma_2-\gamma_1)p+(\gamma_2-\gamma_1)q = 0. \tag{12}$$

Putting $l_2 = \gamma_2-\gamma_1$ we get by (10) and (11)

$$0 < h(l_2) \leqslant 2|P||Q|$$

and by (12)

$$\lambda l_2 p + l_2 q = 0.$$

Thus by (9)

$$(l_1 p)(l_2 q) = (l_1 q)(l_2 p)$$

and $l_2 p = 0$ implies $l_2 q = 0$.

Moreover the vectors l_1, l_2 are linearly independent since $l_{1k} \neq 0$, while $l_{2k} = 0$ and $l_2 \neq 0$.

LEMMA 4. *Let $P, Q \in C[x_1, x_2, \ldots, x_k]$, $(P, Q) = 1$. If $p, q \in Z^k$,*

$$\big(JP(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k}), JQ(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k})\big) = D(z) \in C[z]$$

and $KD(z) \neq 1$ then there exist $d \geqslant 2$ linearly independent vectors $m_1, \ldots, m_d \in Z^k$ such that for $i \leqslant d$

$$h(m_i) \leqslant i \max\{|P|, |Q|\}, \qquad m_i p = 0$$

and either $d \geqslant 3$ or

$$\max\{|m_1 q|, |m_2 q|\} \leqslant c_7(P, Q)(m_1 q, m_2 q).$$

Proof. Let

$$P = \sum_{\alpha\in A} \pi_\alpha \prod_{j=1}^{k} x_j^{\alpha_j}, \qquad Q = \sum_{\alpha\in B} \varrho_\alpha \prod_{j=1}^{k} x_j^{\alpha_j}, \tag{13}$$

where $A, B \subset Z^k$, $\alpha = [\alpha_1, \ldots, \alpha_k]$ and $\pi_\alpha \neq 0$ for $\alpha \in A$, $\varrho_\alpha \neq 0$ for $\alpha \in B$.

Let A' be a subset of A saturated with respect to property that all numbers $\alpha' p$ for $\alpha' \in A'$ are distinct and let B' be defined similarly. We have

$$\begin{aligned} P &= \sum_{\alpha'\in A'} \prod_{j=1}^{k} x_j^{\alpha'_j} \sum_{\substack{\alpha\in A\\ (\alpha-\alpha')p=0}} \pi_\alpha \prod_{j=1}^{k} x_j^{\alpha_j-\alpha'_j},\\ Q &= \sum_{\alpha'\in B'} \prod_{j=1}^{k} x_j^{\alpha'_j} \sum_{\substack{\alpha\in B\\ (\alpha-\alpha')p=0}} \varrho_\alpha \prod_{j=1}^{k} x_j^{\alpha_j-\alpha'_j}; \end{aligned} \tag{14}$$

$$\begin{aligned} P(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k}) &= \sum_{\alpha'\in A'} y^{\alpha' p} z^{\alpha' q} \sum_{\substack{\alpha\in A\\ (\alpha-\alpha')p=0}} \pi_\alpha z^{(\alpha-\alpha')q},\\ Q(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k}) &= \sum_{\alpha'\in B'} y^{\alpha' p} z^{\alpha' q} \sum_{\substack{\alpha\in B\\ (\alpha-\alpha')p=0}} \varrho_\alpha z^{(\alpha-\alpha')q}. \end{aligned} \tag{15}$$

Since $D(z)$ has at least two terms or $D(z) = 0$, for each $\alpha' \in A'$ there exists at least one $\alpha \in A$, $\alpha \neq \alpha'$ such that $(\alpha-\alpha')p = 0$.

Let Λ be the sublattice of Z^k generated by all the vectors $\alpha-\alpha'$, where $(\alpha-\alpha')p = 0$ and $\alpha, \alpha' \in A$ or $\alpha, \alpha' \in B$; let $d = \dim\Lambda$.

Since $h(\alpha-\alpha') \leqslant \max\{|P|, |Q|\}$ for $\alpha, \alpha' \in A \cup B$ by virtue of Lemma 6 of [9] Λ has a basis $m_1, \ldots, m_d$ satisfying

$$h(m_i) \leqslant i \max\{|P|, |Q|\} \qquad (1 \leqslant i \leqslant d).$$

Let $M = [m_{ij}]_{i,j\leqslant d}$. Without loss of generality we may assume that

$$|M| > 0. \tag{16}$$

For every vector $\alpha-\alpha'$, where $\alpha, \alpha' \in A$ or $\alpha, \alpha' \in B$ we have

$$\alpha-\alpha' = \sum_{i=1}^{d} c^i_{\alpha\alpha'} m_i, \qquad c^i_{\alpha\alpha'} \in Z \qquad (1 \leqslant i \leqslant d). \tag{17}$$

It follows that

$$|c^i_{\alpha\alpha'}| \leqslant d^{d/2} h(\alpha-\alpha') \prod_{j=1, j\neq i}^{d} h(m_j) \leqslant (d^{3/2} \max\{|P|, |Q|\})^d. \tag{18}$$

Let us put

$$S = \bigcup_{\alpha'\in A'} \{J \sum_{\substack{\alpha\in A\\ (\alpha-\alpha')p=0}} \pi_\alpha \prod_{i=1}^{d} y_i^{c^i_{\alpha\alpha'}}\} \cup \bigcup_{\alpha'\in B'} \{J \sum_{\substack{\alpha\in B\\ (\alpha-\alpha')p=0}} \varrho_\alpha \prod_{i=1}^{d} y_i^{c^i_{\alpha\alpha'}}\},$$

$$\Delta = \operatorname*{g.c.d.}_{F\in S} F.$$

Substituting

$$y_i = \prod_{j=1}^{k} x_j^{m_{ij}} \qquad (1 \leqslant i \leqslant d)$$

we get by (17)

$$J\Delta\Big(\prod_{j=1}^{k} x_j^{m_{1j}}, \ldots, \prod_{j=1}^{k} x_j^{m_{dj}}\Big) \Big| \Big(\operatorname*{g.c.d.}_{\alpha'\in A'} J \sum_{\substack{\alpha\in A\\ (\alpha-\alpha')p=0}} \pi_\alpha \prod_{j=1}^{k} x_j^{\alpha_j-\alpha'_j},\ \operatorname*{g.c.d.}_{\alpha'\in B'} J \sum_{\substack{\alpha\in B\\ (\alpha-\alpha')p=0}} \varrho_\alpha \prod_{j=1}^{k} x_j^{\alpha_j-\alpha'_j}\Big)$$

hence by (14)

$$J\Delta\Big(\prod_{j=1}^{k} x_j^{m_{1j}}, \ldots, \prod_{j=1}^{k} x_j^{m_{dj}}\Big) \Big| (P, Q)$$

and by the assumption

$$JΔ\Big(\prod_{j=1}^{k} x_j^{m_{1j}}, \ldots, \prod_{j=1}^{k} x_j^{m_{dj}}\Big) \in C.$$

Let $|M|M^{-1} = [m'_{ij}]$. Substituting

$$x_i = \prod_{j=1}^{d} z_j^{m'_{ij}} \quad (1 \leqslant i \leqslant d), \qquad x_i = 1 \quad (d < i \leqslant k),$$

we get

$$JΔ(z_1^{|M|}, \ldots, z_d^{|M|}) \in C,$$

hence by (16)

$$JΔ(z_1, \ldots, z_d) \in C.$$

Since by the definition of $Δ$ its leading coefficient is 1 and $\big(Δ(z_1, \ldots, z_d), \prod_{i=1}^{d} z_i\big) = 1$, we have

$$(19) \qquad Δ(y_1, \ldots, y_d) = 1.$$

On the other hand, by (15) and (17)

$$D(z) | \operatorname*{g.c.d.}_{F \in S} JF(z^{m_1 q}, \ldots, z^{m_d q}).$$

If $d = 1$ the right-hand side of the above divisibility equals $JΔ(z^{m_1 q})$ contradicting (19). Therefore either $d \geqslant 3$ or $d = 2$ and the set S satisfies the assumption of Lemma 2.

Applying that lemma to the vector $[m_1 q, m_2 q]$ we get

$$\max\{|m_1 q|, |m_2 q|\} \leqslant c_6(S)(m_1 q, m_2 q).$$

By (18) the number of possibilities for the set S for fixed P and Q is finite. Hence $c_6(S)$ does not exceed a bound depending only on P and Q. Denoting this bound by $c_7(P, Q)$ we obtain

$$\max\{|m_1 q|, |m_2 q|\} \leqslant c_7(P, Q)(m_1 q, m_2 q)$$

and the proof of Lemma 4 is complete.

LEMMA 5. *Let* $P, Q \in K[x_1, x_2, x_3]$, $K \subset C$, $(P, Q) = 1$. *If* $[n_1, n_2, n_3] \in Z^3$, $(n_1, n_2, n_3) = 1$ *and* ξ *is a common zero of* $KP(x^{n_1}, x^{n_2}, x^{n_3})$ *and* $KQ(x^{n_1}, x^{n_2}, x^{n_3})$ *then either*

$$[K(\xi):K] < 12|P||Q|\sqrt{3h(n)}$$

or there is a vector $\gamma \in Z^3$ *such that*

$$(20) \qquad \gamma n = 0$$

and

$$0 < h(\gamma) \leqslant c_8(P, Q).$$

Proof. Let us choose a decomposition

$$(21) \qquad n = up + vq, \quad u, v \in Z,\ p, q \in Z^3,\ \dim(p, q) = 2$$

with the least possible value of $h(p)h(q)$. By Lemma 1 we have

$$(22) \qquad h(p)h(q) \leqslant \sqrt{\tfrac{4}{3}h(n)}.$$

Without loss of generality we may assume that

$$(23) \qquad h(p) \leqslant h(q).$$

It follows from $(n_1, n_2, n_3) = 1$ that $(u, v) = 1$. If we had $v = 0$ it would follow $u = \pm 1$, $h(n) = h(p)$ and thus

$$h(n)^2 \leqslant \sqrt{\tfrac{4}{3}h(n)}; \quad h(n)^3 \leqslant \tfrac{4}{3}, \quad h(n) = 1.$$

Since for $h(n) = 1$ we can choose a decomposition (21) with $h(p) = h(q) = 1$, $v = \pm 1$, we may assume that

$$(24) \qquad (u, v) = 1, \quad v \neq 0.$$

Let us consider polynomials

$$(25_1) \qquad G = JP(y^{p_1} z^{q_1}, y^{p_2} z^{q_2}, y^{p_3} z^{q_3}), \qquad H = JQ(y^{p_1} z^{q_1}, y^{p_2} z^{q_2}, y^{p_3} z^{q_3})$$

$$(25_2) \qquad D = (G, H).$$

For further reference we note that

$$(26) \qquad \begin{aligned} \deg_y G &\leqslant 3|P|h(p), & \deg_z G &\leqslant 3|P|h(q), \\ \deg_y H &\leqslant 3|Q|h(p), & \deg_z H &\leqslant 3|Q|h(q). \end{aligned}$$

If $D \in K[y, z] \setminus K[z]$ then by Lemma 3 there are two linearly independent vectors $l_1, l_2 \in Z^3$ such that

$$(27) \qquad h(l_1) \leqslant \min\{|P|, |Q|\}, \quad h(l_2) \leqslant 2|P||Q|$$

and

$$(l_1 p)(l_2 q) = (l_2 p)(l_1 q).$$

Hence

$$(l_1 p)(l_2 n) - (l_2 p)(l_1 n) = (l_1 p)(l_2 up + l_2 vq) - (l_2 p)(l_1 up + l_1 vq) = 0$$

and we get (20) with

$$(28_1) \qquad \gamma = (l_1 p) l_2 - (l_2 p) l_1 = (l_1 \times l_2) \times p \neq 0$$

unless

$$l_1 p = l_2 p = 0.$$

In the latter case $l_1 q = l_2 q = 0$ and we get

$$(28_2) \qquad l_i n = l_i(up + vq) = 0 \quad (i = 1, 2),$$

thus we take $\gamma = l_1 \neq 0$. In the first case

$$(29_1) \qquad h(\gamma) \leqslant 2h(l_1 \times l_2) h(p) \leqslant 4h(l_1) h(l_2) h(p).$$

In the second case the same inequality clearly holds. By (20) and (28)

$$n = u_1(l_1 \times l_2) + v_1 p, \quad \text{where } u_1, v_1 \in Q$$

and by the argument leading to Theorem 2 of [14]

$$n = u_0 p_0 + v_0 q_0, \quad \text{where } u_0, v_0 \in Z,\ p_0, q_0 \in Z^3,\ \dim(p_0, q_0) = 2$$

and

$$h(p_0) h(q_0) \leqslant h(l_1 \times l_2) h(p).$$

By the choice of p, q

$$h(p) h(q) \leqslant h(p_0) h(q_0) \leqslant h(l_1 \times l_2) h(p) \leqslant 2h(l_1) h(l_2) h(p).$$

It follows by (23) that

$$h(p) \leqslant h(q) \leqslant 2h(l_1) h(l_2)$$

and hence by (27) and (29_1)

$$(29_2) \qquad 0 < h(\gamma) \leqslant 32|P|^2|Q|^2 (\min\{|P|, |Q|\})^2.$$

Assume now that

$$D \in K[z] \setminus K, \quad KD \neq 1.$$

Since $p \neq 0$ we cannot have three linearly independent vectors $m_i \in Z^3$ such that $m_i p = 0$ $(1 \leqslant i \leqslant 3)$. Therefore, by Lemma 4 we have two vectors $m_1, m_2 \in Z^3$ linearly independent and such that

$$(30_1) \qquad h(m_i) \leqslant i \max\{|P|, |Q|\} \quad (i = 1, 2),$$

$$m_1 p = m_2 p = 0, \quad \text{and} \quad \max\{|m_1 q|, |m_2 q|\} \leqslant c_7(P, Q)(m_1 q, m_2 q).$$

Since p, q are linearly independent and m_1, m_2 are linearly independent, we cannot have $m_1 q = m_2 q = 0$.

Since $m_i n = m_i(up + vq) = v m_i q$ $(i = 1, 2)$ and by (24) $v \neq 0$, it follows that

$$\frac{\max\{|m_1 n|, |m_2 n|\}}{(m_1 n, m_2 n)} \leqslant c_7(P, Q).$$

We take in (20)

$$\gamma = \frac{(m_1 \times m_2) \times n}{(m_1 n, m_2 n)}$$

and obtain by (30_1)

$$(30_2) \qquad h(\gamma) \leqslant c_7(P, Q)(h(m_1) + h(m_2)) \leqslant 4 \max\{|P|, |Q|\} c_7(P, Q).$$

Finally, consider the case where

$$(31) \qquad D \in Q(z) \quad \text{and} \quad KD = 1.$$

Let $G_1 = GD^{-1}$, $H_1 = HD^{-1}$, R be the resultant of G_1, H_1 with respect to z. By (25_2) $(G_1, H_1) = 1$. By virtue of Lemma 4 of [9] and of (26) we have

$$\begin{aligned}\operatorname{card}\{\langle \eta, \zeta \rangle \in C^2 \colon G_1(\eta, \zeta) = H_1(\eta, \zeta) = 0\} &\leqslant |R| \\ &\leqslant \deg_y G_1 \cdot \deg_z H_1 + \deg_z G_1 \cdot \deg_y H_1 \\ &\leqslant 3|P| h(p) \cdot 3|Q| h(q) + 3|Q| h(p) \cdot 3|Q| h(p) = 18|P||Q| h(p) h(q).\end{aligned}$$

On the other hand if ξ is a common zero of $KP(x^{n_1}, x^{n_2}, x^{n_3})$ and $KQ(x^{n_1}, x^{n_2}, x^{n_3})$ in virtue of (21) and (25_1) $\langle \xi^u, \xi^v \rangle$ is a common zero of G and H, while in virtue of (24) and (31) it is not a zero of D. Therefore,

$$G_1(\xi^u, \xi^v) = H_1(\xi^u, \xi^v) = 0.$$

Since by (24) $\langle \xi^u, \xi^v \rangle$ determines ξ uniquely, it follows that the number of common zeros of $KP(x^{n_1}, x^{n_2}, x^{n_3})$ and $KQ(x^{n_1}, x^{n_2}, x^{n_3})$ does not exceed $18|P||Q| h(p) h(q)$. However together with ξ every number conjugate to ξ over K is a common zero in question, hence by (22)

$$[K(\xi) : K] \leqslant 18|P||Q| \sqrt{\tfrac{4}{3} h(n)} = 12|P||Q| \sqrt{3h(n)}.$$

In view of (29) and (30_2) the lemma holds with

$$c_8(P, Q) = \max\{32|P|^2|Q^2|(\min\{|P|, |Q|\})^2, 4\max\{|P||Q|\} c_7(P, Q)\}.$$

Lemma 6. *Let* $a = [a_0, \ldots, a_r] \in C^{r+1} \setminus \{0\}$,

$$A(z) = \sum_{i=0}^{r} a_i z^i = a_m \prod_{i=1}^{m} (z - z_i).$$

There exist two positive real numbers $c_9(a) \leqslant 1$ *and* $c_{10}(a)$ *with the following property. If*

$$(32) \qquad c_9(a) \geqslant \varepsilon > 0,$$

$$b = [b_0, \ldots, b_r] \in C^{r+1},$$

$$(33) \qquad h(b - a) < c_{10}(a) \varepsilon^r,$$

then for some $n \geqslant m$, $b_n \neq 0$

$$B(z) = \sum_{i=0}^{r} b_i z^i = b_n \prod_{i=1}^{n} (z - \zeta_i),$$

where

$$(34) \qquad |\zeta_i| > \varepsilon^{-1} \quad \textit{for} \quad m < i \leqslant n,$$

$$(35) \qquad |\zeta_i - z_i| < \varepsilon \quad \textit{for} \quad i \leqslant m.$$

Remark. Under the additional assumption that $b_m \neq 0, b_{m+1} = \ldots = b_r = 0$ the lemma is well known, see e.g. [6], p. 92.

Proof. Let us put

(36) $c_9(\boldsymbol{a}) = \min(\{\frac{1}{2}|z_j - z_i|: z_j \neq z_i\} \cup \{|z_i|: z_i \neq 0\} \cup \{\frac{1}{2}|z_i|^{-1}: z_i \neq 0\} \cup \{\frac{1}{2}\})$

and

(37) $$c_{10}(\boldsymbol{a}) = \frac{|a_m|}{(r+1)(\max\{1, c_9(\boldsymbol{a}) + \max_{1 \leqslant i \leqslant m} |z_i|\})^r},$$

where the maximum over an empty set equals $-\infty$.

We may assume without loss of generality that

$$\bigcup_{i=1}^{m} \{z_i\} = \{z_1, z_2, \ldots, z_\mu\},$$

where z_j $(1 \leqslant j \leqslant \mu)$ are distinct and z_j occurs in the sequence $\{z_i\}$ $(1 \leqslant i \leqslant m)$ ν_j times ($\mu = 0$ if $m = 0$).

For $|z| = \varepsilon^{-1}$ we find

$$|A(z)| \geqslant |a_m| \prod_{i=1}^{m} |\varepsilon^{-1} - |z_i|| \geqslant \frac{|a_m|}{2^m} \varepsilon^{-m} \geqslant |a_m|.$$

On the other hand, we have

$$c_{10}(\boldsymbol{a}) \leqslant a_m/(r+1),$$

hence by (33)

$$|B(z) - A(z)| \leqslant (r+1) h(\boldsymbol{b} - \boldsymbol{a}) \varepsilon^{-r} < (r+1) c_{10}(\boldsymbol{a}) \leqslant |a_m| \leqslant |A(z)|.$$

In follows from Rouché's theorem that $B(z)$ has as many zeros, counting multiplicity, in the disc $|z| \leqslant \varepsilon^{-1}$ as $A(z)$, hence m (note that by (32) and (36) $|z_i| \leqslant c_9(\boldsymbol{a})^{-1} \leqslant \varepsilon^{-1}$ for all $i \leqslant m$). In particular $B(z)$ is not identically 0 and has degree $n \geqslant m$. All the zeros of $B(z)$ outside $|z| \leqslant \varepsilon^{-1}$ which can be denoted, counting multiplicity, $\zeta_{m+1}, \ldots, \zeta_n$ satisfy (34).

The discs $|z - z_j| < \varepsilon$ $(1 \leqslant j \leqslant \mu)$ are disjoint and contained in the disc $|z| \leqslant \varepsilon^{-1}$. Indeed, by (32) and (36)

$$|z_i - z_j| \geqslant 2\varepsilon \quad (1 \leqslant i < j \leqslant \mu)$$

and

$$|z_j| + \varepsilon \leqslant \max\{\varepsilon, 2|z_j|\} \leqslant \varepsilon^{-1}.$$

For $|z - z_j| = \varepsilon$, $z_i \neq z_j$ we have in view of (32) and (36)

$$|z - z_i| \geqslant |z_i - z_j| - |z - z_j| \geqslant 2\varepsilon - \varepsilon = \varepsilon,$$

hence

$$|A(z)| = |a_m| \varepsilon^{\nu_j} \prod_{\substack{i=1 \\ z_i \neq z_j}}^{m} |z - z_i| \geqslant |a_m| \varepsilon^m.$$

On the other hand, by (33) and (37) for $|z - z_j| = \varepsilon$

$$|B(z) - A(z)| \leqslant (r+1) h(\boldsymbol{b} - \boldsymbol{a})(\max\{1, |z_j| + \varepsilon\})^r$$
$$< (r+1) c_{10}(\boldsymbol{a}) \varepsilon^r (\max\{1, |z_j| + c_9(\boldsymbol{a})\})^r \leqslant |a_m| \varepsilon^m.$$

It follows from Rouché's theorem that $B(z)$ has as many zeros, counting multiplicity, in the disc $|z - z_j| < \varepsilon$ as $A(z)$, hence ν_j. This accounts for $\sum_{j=1}^{\mu} \nu_j = m$ zeros of $B(z)$ in $|z| \leqslant \varepsilon^{-1}$. They can be denoted by $\zeta_1, \ldots, \zeta_m$, counting multiplicity so that (34) is satisfied.

Lemma 7. *Let $R \in \boldsymbol{K}[y_0, y_1, \ldots, y_s] \setminus \{0\}$, where $[\boldsymbol{K}:\boldsymbol{Q}] < \infty$. There exist nonnegative real numbers $c_i(R)$ $(11 \leqslant i \leqslant 16)$ satisfying*

$$1 \geqslant c_{11}(R) > 0, \quad c_{14}(R) \geqslant 1, \quad c_{15}(R) \geqslant 4, \quad c_{16}(R) > 0$$

and with the following property. For every $\varepsilon \in (0, c_{11}(R)]$, every η with $|\eta| > 1$, every integer v_0 and every vector $\boldsymbol{v} = [v_1, \ldots, v_s] \in \boldsymbol{Z}^s$ if

(38) $$R(\eta^{v_0}, \eta^{v_1}, \ldots, \eta^{v_s}) = 0$$

then either there exists a vector $\boldsymbol{\delta} \in \boldsymbol{Z}^s$ such that

(39) $$0 < h(\boldsymbol{\delta}) \leqslant |R|$$

and

(40) $$|\boldsymbol{\delta v}| \leqslant \frac{c_{12}(R)|\log \varepsilon| + c_{13}(R)}{\log|\eta|},$$

or

(41) $$|v_0| \log|\eta| > |\log \varepsilon|,$$

or there exists a real algebraic number $\theta > 0$ such that

(42) $$[\boldsymbol{Q}(\theta):\boldsymbol{Q}] \leqslant c_{14}(R),$$

(43) $$h(\theta) \leqslant c_{15}(R),$$

(44) $$|v_0 \log|\eta| - \log \theta| < c_{16}(R)\varepsilon.$$

Proof. Let

(45) $$R(y_0, y_1, \ldots, y_s) = \sum_{i=0}^{r} y^i \sum_{\boldsymbol{\beta} \in \boldsymbol{B}_i} \varrho_i(\boldsymbol{\beta}) \prod_{j=1}^{s} y_j^{\beta_j},$$

where $\boldsymbol{B}_r \neq \emptyset$ and $\varrho_i : \boldsymbol{Z}^s \to \boldsymbol{K}$ is such that $\varrho_i(\boldsymbol{\beta}) \neq 0$ for all $\boldsymbol{\beta} \in \boldsymbol{B}_i$ and $\varrho_i(\boldsymbol{\beta}) = 0$ for all $\boldsymbol{\beta} \notin \boldsymbol{B}_i$ $(0 \leqslant i \leqslant r)$. Put

(46) $$A(R) = \bigcup_{i=0}^{r} \bigcup_{\boldsymbol{\beta}\in \boldsymbol{B}_i} \{\langle \varrho_0(\boldsymbol{\beta}), \ldots, \varrho_r(\boldsymbol{\beta})\rangle\},$$

(47) $$\boldsymbol{Z}(R) = \bigcup_{i=0}^{r} \bigcup_{\boldsymbol{\beta}\in \boldsymbol{B}_i} \{z\colon \sum_{i=0}^{n} \varrho_i(\boldsymbol{\beta}) z^i = 0\}.$$

Clearly $\boldsymbol{0} \notin \boldsymbol{A}(R)$. Hence $\boldsymbol{Z}(R)$ is finite (empty if $r = 0$) and the following definitions make sense:

(48) $$c_{11}(R) = \min\{\min_{\boldsymbol{a}\in \boldsymbol{A}(R)} c_9(\boldsymbol{a}),\ \min_{z\in \boldsymbol{Z}(R)\setminus\{0\}} \tfrac{1}{2}|z|\},$$

(49) $$c_{12}(R) = r,$$

(50) $$c_{13}(R) = \max\{0, \max_{\boldsymbol{a}\in \boldsymbol{A}} |\log c_{10}(\boldsymbol{a})| + \max_{\substack{i\leqslant r\\ \boldsymbol{B}_i\neq\emptyset}} \log \sum_{\boldsymbol{\beta}\in \boldsymbol{B}_i} |\varrho_i(\boldsymbol{\beta})|\},$$

(51) $$c_{14}(R) = \max\{0, \max_{z\in \boldsymbol{Z}(R)} [\boldsymbol{Q}(|z|) : \boldsymbol{Q}]\},$$

(52) $$c_{15}(R) = \max\{4, \max_{z\in \boldsymbol{Z}(R)} h(|z|)\},$$

(53) $$c_{16}(R) = \max\{0, \max_{z\in \boldsymbol{Z}(R)\setminus\{0\}} 2|z|^{-1}\},$$

where minimum or maximum over an empty set equals ∞ or $-\infty$, respectively.

Let

(54) $$0 < \varepsilon \leqslant c_{11}(R)$$

and let us define vectors $\boldsymbol{\beta}_1$ and $\boldsymbol{\beta}_2$ by the equalities

$$\boldsymbol{\beta}_1 \boldsymbol{v} = \max_{\boldsymbol{\beta}\in \bigcup_{i=1}^{r} \boldsymbol{B}_i} \{\boldsymbol{\beta}\boldsymbol{v}\}, \quad \boldsymbol{\beta}_2 \boldsymbol{v} = \max_{\boldsymbol{\beta}\in \bigcup_{i=1}^{r} \boldsymbol{B}_i\setminus\{\boldsymbol{\beta}_1\}} \{\boldsymbol{\beta}\boldsymbol{v}\}.$$

Suppose first that

$$|\eta|^{\boldsymbol{\beta}_2\boldsymbol{v} - \boldsymbol{\beta}_1\boldsymbol{v}} \geqslant e^{-c_{13}(R)} \varepsilon^{c_{12}(R)}.$$

Then

$$0 \geqslant \boldsymbol{\beta}_2\boldsymbol{v} - \boldsymbol{\beta}_1\boldsymbol{v} \geqslant \frac{c_{12}(R)\log\varepsilon - c_{13}(R)}{\log|\eta|}$$

and putting $\boldsymbol{\delta} = \boldsymbol{\beta}_2 - \boldsymbol{\beta}_1$ we obtain (39) and (40).

Suppose now that

$$|\eta|^{\boldsymbol{\beta}_2\boldsymbol{v} - \boldsymbol{\beta}_1\boldsymbol{v}} < e^{-c_{13}(R)} \varepsilon^{c_{12}(R)}.$$

Then for all $\boldsymbol{\beta} \in \bigcup_{i=0}^{r} \boldsymbol{B}_i \setminus \{\boldsymbol{\beta}_1\}$

$$|\eta|^{\boldsymbol{\beta}\boldsymbol{v} - \boldsymbol{\beta}_1\boldsymbol{v}} < e^{-c_{13}(R)} \varepsilon^{c_{12}(R)},$$

thus we obtain using (49) and (50)

(55) $$\Big|\sum_{\boldsymbol{\beta}\in \boldsymbol{B}_i} \varrho_i(\boldsymbol{\beta}) \eta^{\boldsymbol{\beta}\boldsymbol{v} - \boldsymbol{\beta}_1\boldsymbol{v}} - \sum_{\substack{\boldsymbol{\beta}\in \boldsymbol{B}_i\\ \boldsymbol{\beta}\boldsymbol{v} = \boldsymbol{\beta}_1\boldsymbol{v}}} \varrho_i(\boldsymbol{\beta})\Big| \leqslant \sum_{\boldsymbol{\beta}\in \boldsymbol{B}_i} |\varrho_i(\boldsymbol{\beta})| e^{-c_{13}(R)} \varepsilon^{c_{12}(R)} \leqslant \varepsilon^r \min_{\boldsymbol{a}\in \boldsymbol{A}(R)} c_{10}(\boldsymbol{a}),$$

where the first inequality is sharp if $\boldsymbol{B}_i \neq \emptyset$ and the second inequality is sharp otherwise.

If for some $\boldsymbol{\beta} \in \bigcup_{i=0}^{r} \boldsymbol{B}_i \setminus \{\boldsymbol{\beta}_1\}$ we have $\boldsymbol{\beta}\boldsymbol{v} = \boldsymbol{\beta}_1\boldsymbol{v}$ then (39) and (40) hold with $\boldsymbol{\delta} = \boldsymbol{\beta} - \boldsymbol{\beta}_1$ and the left-hand side of (40) equal to 0. If for all $\boldsymbol{\beta} \in \bigcup_{i=0}^{r} \boldsymbol{B}_i \setminus \{\boldsymbol{\beta}_1\}$ we have $\boldsymbol{\beta}\boldsymbol{v} \neq \boldsymbol{\beta}_1\boldsymbol{v}$ then

(56) $$\sum_{\substack{\boldsymbol{\beta}\in \boldsymbol{B}_i\\ \boldsymbol{\beta}\boldsymbol{v} = \boldsymbol{\beta}_1\boldsymbol{v}}} \varrho_i(\boldsymbol{\beta}) = \varrho_i(\boldsymbol{\beta}_1) \qquad (0 \leqslant i \leqslant r).$$

We set in Lemma 6

$$a_i = \varrho_i(\boldsymbol{\beta}_1), \quad b_i = \sum_{\boldsymbol{\beta}\in \boldsymbol{B}_i} \varrho_i(\boldsymbol{\beta}) \eta^{\boldsymbol{\beta}\boldsymbol{v} - \boldsymbol{\beta}_1\boldsymbol{v}} \qquad (0 \leqslant i \leqslant r)$$

and let

$$A(z) = \sum_{i=0}^{r} a_i z^i = a_m \prod_{i=1}^{m} (z - z_i).$$

By (46) $\boldsymbol{a} \in \boldsymbol{A}(R)$, hence by (47)

(57) $$z_i \in \boldsymbol{Z}(R) \qquad (1 \leqslant i \leqslant m).$$

Moreover, by (48) and (54)

$$1 \geqslant c_9(\boldsymbol{a}) \geqslant c_{11}(R) > \varepsilon$$

and by (55) and (56)

$$h(\boldsymbol{b} - \boldsymbol{a}) < c_{10}(\boldsymbol{a}) \varepsilon^r.$$

The assumptions of Lemma 6 being satisfied we have in virtue of that lemma for an $n \geqslant m$,

$$B(z) = \sum_{i=0}^{r} b_i z^i = b_n \prod_{i=1}^{n} (z - \zeta_i),$$

where $b_n \neq 0$,

(58) $$|\zeta_i| > \varepsilon^{-1} \quad \text{for } m < i \leqslant n,$$

(59) $$|\zeta_i - z_i| < \varepsilon \quad \text{for } i \leqslant m.$$

However by (38) and (45)

$$B(\eta^{v_0}) = \sum_{i=0}^{r} \eta^{v_0 i} \sum_{\beta \in B_i} \varrho_i(\beta)\eta^{\beta v - \beta_1 v} = \eta^{-\beta_1 v} R(\eta^{v_0}, \eta^{v_1}, \ldots, \eta^{v_s}) = 0,$$

hence $\eta^{v_0} = \zeta_i$ for an $i \leqslant n$. If $i > m$ we have by (58)

$$|\eta|^{v_0} > \varepsilon^{-1}, \quad v_0 \log|\eta| > -\log\varepsilon = |\log\varepsilon|$$

hence (41) holds. If $i \leqslant m$ we set $\theta = |z_i|$ and obtain by (59)

$$\big||\eta|^{v_0} - \theta\big| < \varepsilon. \tag{60}$$

If $\theta = 0$ then

$$|\eta|^{v_0} < \varepsilon \leqslant 1, \quad v_0 \log|\eta| < \log\varepsilon = -|\log\varepsilon|,$$

hence (41) holds again. If $\theta \neq 0$ the inequalities (42) and (43) follow from (51), (52) and (57). Moreover by (48)

$$|\eta|^{v_0} > \tfrac{1}{2}\theta,$$

by (60) and (53)

$$\big|v_0 \log|\eta| - \log\theta\big| < \frac{\big||\eta|^{v_0} - \theta\big|}{\min\{|\eta|^{v_0}, \theta\}} < \frac{\varepsilon}{\frac{1}{2}\theta} \leqslant c_{16}(R)\varepsilon,$$

which gives (44) and completes the proof.

LEMMA 8. *Let* $P, Q \in K[x_1, \ldots, x_k]$, *where* $[K:Q] < \infty$ *and* $k \geqslant 3$. *If* $(P, Q) = 1$,

$$P(\xi^{n_1}, \ldots, \xi^{n_k}) = Q(\xi^{n_1}, \ldots, \xi^{n_k}) = 0 \tag{61}$$

and $|\xi| > 1$ *then there exist two linearly independent vectors* $r_1, r_2 \in Z^k$ *such that*

$$h(r_1) \leqslant \min\{|P|, |Q|\}, \tag{62}$$

$$h(r_2) \leqslant 2|P||Q|, \tag{63}$$

$$|r_\nu n| \leqslant c_{16+\nu}(P, Q)(\log|\xi|)^{-1} \quad (\nu = 1, 2) \tag{64}$$

and either

$$\max\{|r_1 n|, |r_2 n|\} \leqslant c_{19}(P, Q)(r_1 n, r_2 n), \tag{65}$$

or $|\xi| < e$ *and there exists a vector* $r_3 \in Z^k$ *linearly independent of* r_1, r_2 *such that*

$$h(r_3) \leqslant 128|P|^3|Q|^3(\min\{|P|, |Q|\})^2 \tag{66}$$

and

$$|r_3 n| \leqslant c_{20}(P, Q)(-\log\log|\xi|)(\log|\xi|)^{-1} + c_{21}(P, Q)(\log|\xi|)^{-1}. \tag{67}$$

Proof. Let

$$P = \sum_{\alpha \in A} \pi_\alpha \prod_{j=1}^{k} x_j^{\alpha_j}, \quad Q = \sum_{\alpha \in B} \varrho_\alpha \prod_{j=1}^{k} x_j^{\alpha_j},$$

where A, B are subsets of Z^k and $\pi_\alpha \neq 0$ for $\alpha \in A$, $\varrho_\alpha \neq 0$ for $\alpha \in B$. Let us put

$$c_{22}(P) = \log \frac{\sum_{\alpha \in A} |\pi_\alpha|}{\min_{\alpha \in A} |\pi_\alpha|}$$

and define $c_{22}(T)$ similarly for any non-zero polynomial T over C. Assume without loss of generality that $|P| \leqslant |Q|$.

Let $\alpha_5 \in A$, $\alpha_6 \in A \setminus \{\alpha_5\}$ be chosen so that

$$\alpha_5 n = \max_{\alpha \in A}\{\alpha n\}, \quad \alpha_6 n = \max_{\alpha \in A \setminus \{\alpha_5\}} \{\alpha n\}.$$

The equation (61) gives

$$|\pi_{\alpha_5} \xi^{\alpha_5 n}| = \Big|\sum_{\alpha \in A \setminus \{\alpha_5\}} \pi_\alpha \xi^{\alpha n}\Big| \leqslant |\xi|^{\alpha_6 n} \sum_{\alpha \in A \setminus \{\alpha_5\}} |\pi_\alpha|.$$

It follows that

$$0 \leqslant \alpha_5 n - \alpha_6 n \leqslant c_{22}(P)(\log|\xi|)^{-1},$$

thus taking $r_1 = \alpha_5 - \alpha_6$ we obtain (62) and (64) with $\nu = 1$ and $c_{17}(P, Q) = c_{22}(P)$ (under the assumption $|P| \leqslant |Q|$).

Let g be the least index such that $r_{1g} \neq 0$. Let R_j be the resultant of P and Q with respect to x_j $(1 \leqslant j \leqslant k)$. By Lemma 5 of [9]

$$|R_g| \leqslant 2|P||Q|$$

and by (61)

$$R_g(\xi^{n_1}, \ldots, \xi^{n_{g-1}}, \xi^{n_{g+1}}, \ldots, \xi^{n_k}) = 0.$$

Applying to the above equation the argument previously applied to $P(\xi^{n_1}, \ldots, \xi^{n_k}) = 0$ we infer the existence of two vectors $\gamma_3, \gamma_4 \in Z^k$ such that

$$\gamma_{3g} = \gamma_{4g} = 0,$$

$$0 < h(\gamma_3 - \gamma_4) \leqslant |R_g|,$$

$$|(\gamma_3 - \gamma_4)n| \leqslant c_{22}(R_g)(\log|\xi|)^{-1}.$$

Taking

$$r_2 = \gamma_3 - \gamma_4$$

we obtain (63) and (64) with $\nu = 2$ and

$$c_{18}(P, Q) = \max_{1 \leqslant j \leqslant k} c_{22}(R_j).$$

Moreover, the vectors $\mathbf{r}_1$ and $\mathbf{r}_2$ are linearly independent since $r_{1g} \neq 0$, while $r_{2g} = 0$ and $\mathbf{r}_2 \neq \mathbf{0}$. Let us choose the least $h \neq g$ such that $r_{2h} \neq 0$ and replace if necessary $\mathbf{r}_2$ by $-\mathbf{r}_2$ so that $r_{1g} r_{2h} > 0$. Assume first that $|\xi| < e$ and consider two auxiliary polynomials

(68) $$\tilde{P}(x_1, \ldots, x_k) = JP(\tilde{x}_1, \ldots, \tilde{x}_k), \quad \tilde{Q}(x_1, \ldots, x_k) = JQ(\tilde{x}_1, \ldots, \tilde{x}_k),$$

where

$$\tilde{x}_g = x_g x_h^{-r_{1h}} \prod_{j \neq g,h} x_j^{r_{1h} r_{2j} - r_{1j} r_{2h}},$$
$$\tilde{x}_h = x_h^{r_{1g}} \prod_{j \neq g,h} x_j^{-r_{1g} r_{2j}},$$
$$\tilde{x}_j = x_j^{r_{1g} r_{2h}} \quad \text{if } j \neq g, h.$$

For further reference we note that

(69) $$|\tilde{P}| \leqslant 4|P| h(\mathbf{r}_1) h(\mathbf{r}_2), \quad |\tilde{Q}| \leqslant 4|Q| h(\mathbf{r}_1) h(\mathbf{r}_2)$$

and the operation J is performed after the substitution. Let

$$(\tilde{P}, \tilde{Q}) = \tilde{D} \in \mathbf{K}[x_1, \ldots, x_k].$$

Substituting

(70) $$x_g = \prod_{j=1}^{k} y_j^{r_{1j} r_{2h}}, \quad x_h = \prod_{j \neq g} y_j^{r_{2j}}, \quad x_j = y_j \quad (j \neq g, h)$$

we obtain

(71) $$\tilde{x}_j = y_j^{r_{1g} r_{2h}},$$

hence

$$J\tilde{D}\Big(y_1, \ldots, \prod_{j=1}^{k} y_j^{r_{1j} r_{2h}}, \ldots, \prod_{j \neq g} y_j^{r_{2j}}, \ldots, y_k\Big) \Big| \big(JP(y_1^{r_{1g} r_{2h}}, \ldots, y_k^{r_{1g} r_{2h}}),$$
$$JQ(y_1^{r_{1g} r_{2h}}, \ldots, y_k^{r_{1g} r_{2h}})\big).$$

Since $(P, Q) = 1$, by Lemma 9 of [10] the greatest common divisor on the right-hand side of the divisibility equals 1, hence

$$J\tilde{D}\Big(y_1, \ldots, \prod_{j=1}^{k} y_j^{r_{1j} r_{2h}}, \ldots, \prod_{j \neq g} y_j^{r_{2j}}, \ldots, y_k\Big) \in \mathbf{K}.$$

Two distinct terms of $\tilde{D}$ cannot become similar after the substitution (70) since the matrix of exponents is nonsingular. Hence $\tilde{D}$ is a monomial and since $(\tilde{D}, x_1 \cdot \ldots \cdot x_k) = 1$ we have $\tilde{D} = 1$. Therefore, for all $j \leqslant k$ the resultant $\tilde{R}_j$ of $\tilde{P}$ and $\tilde{Q}$ with respect to x_j is non-zero. Let us take for η any value of $\xi^{1/r_{1g} r_{2h}}$ and put

(72) $$\eta_g = \eta^{(\mathbf{r}_1 \mathbf{n}) r_{2h}}, \quad \eta_h = \eta^{\mathbf{r}_2 \mathbf{n}}, \quad \eta_j = \eta^{n_j} \quad (j \neq g, h).$$

Clearly

(73) $$|\eta| = |\xi|^{1/r_{1g} r_{2h}} > 1.$$

By virtue of (61), (68) and of the implication $(70) \rightarrow (71)$ we have

$$\tilde{P}(\eta_1, \ldots, \eta_k) = \tilde{Q}(\eta_1, \ldots, \eta_k) = 0,$$

hence also

(74) $$\tilde{R}_g(\eta_1, \ldots, \eta_k) = 0, \quad \tilde{R}_h(\eta_1, \ldots, \eta_k) = 0.$$

Let φ be a unique one-to-one increasing function mapping $\{1, 2, \ldots, k\} \setminus \{g, h\}$ onto $\{1, 2, \ldots, k-2\}$ and $i = g$ or h. We set in Lemma 7 $s = k-2$,

$$R = R_i^*(y_0, y_1, \ldots, y_s) := \tilde{R}_i(x_1, \ldots, x_k),$$

where

$$x_j = y_{\varphi(j)} \quad \text{for } j \neq g, h,$$
$$x_{g+h-i} = y_0,$$

(note that $\tilde{R}_i$ is independent of x_i);

(75) $$\varepsilon = c_{23}(R_g^*, R_h^*) \min\left\{\max\{|\mathbf{r}_2 \mathbf{n}|, |\mathbf{r}_1 \mathbf{n}||r_{2h}|, 4\}^{-c_{24}(R_g^*, R_h^*)}, \frac{\log|\xi|}{r_{1g} r_{2h}}\right\},$$

where

(76) $$c_{23}(R_g^*, R_h^*) = \min\{c_{11}(R_g^*), c_{11}(R_h^*), (c_{16}(R_g^*) + c_{16}(R_h^*))^{-1}\} \leqslant 1,$$

(77) $$c_{24}(R_g^*, R_h^*) = 1 + (32 c_{14}(R_g^*) c_{14}(R_h^*))^{400} \log c_{15}(R_g^*) \log c_{15}(R_h^*)$$
$$\times \log\min\{\log c_{15}(R_g^*), \log c_{15}(R_h^*)\} > 1;$$

(78) $$v_0 = \begin{cases} \mathbf{r}_2 \mathbf{n} & \text{if } i = g, \\ (\mathbf{r}_1 \mathbf{n}) r_{2h} & \text{if } i = h, \end{cases}$$

(79) $$v_j = n_{\varphi^{-1}(j)} \quad (1 \leqslant j \leqslant k-2).$$

We have by (75), (76) and (77) $0 < \varepsilon < c_{11}(R_i^*)$, by (73) $|\eta| > 1$, by (72) and (74)

$$R_i^*(\eta^{v_0}, \eta^{v_1}, \ldots, \eta^{v_s}) = \tilde{R}_i(\eta_1, \ldots, \eta_k) = 0,$$

hence by Lemma 7 either there exists a vector $\boldsymbol{\delta}_i \in \mathbf{Z}^s$ such that

(80) $$0 < h(\boldsymbol{\delta}_i) \leqslant |R_i^*|$$

and

(81) $$|\boldsymbol{\delta}_i \mathbf{v}| \leqslant \frac{c_{12}(R_i^*)|\log\varepsilon| + c_{13}(R_i^*)}{\log|\eta|},$$

or

(82) $$|v_0| \log|\eta| > |\log\varepsilon|,$$

or finally there exists a real algebraic number $\theta_i > 0$ such that

(83) $$[Q(\theta_i):Q] \leqslant c_{14}(R_i^*),$$

(84) $$h(\theta_i) \leqslant c_{15}(R_i^*),$$

(85) $$|v_0 \log|\eta| - \log\theta_i| < c_{16}(R_i^*)\varepsilon.$$

We shall consider successively the following cases.

A. (80) and (81) hold for $i = g$ or for $i = h$,

B. (82) holds for $i = g$ or for $i = h$,

C. (83)–(85) hold for $i = g$ or for $i = h$ with $\theta_i = 1$,

D. (83)–(85) hold for $i = g$ and for $i = h$ with $\theta_i \neq 1$.

Case A. We define the components r_{3j} or $\boldsymbol{r}_3$ by the formulae

$$r_{3j} = \begin{cases} \delta_{i\varphi(j)} & \text{for } j \in \{1, 2, \ldots, k\} \setminus \{g, h\}, \\ 0 & \text{for } j \in \{g, h\}. \end{cases}$$

Clearly $\boldsymbol{r}_3 \in \boldsymbol{Z}^k$. The vector $\boldsymbol{r}_3$ is linearly independent of $\boldsymbol{r}_1, \boldsymbol{r}_2$ since $\boldsymbol{r}_1 \neq 0$, $r_{3g} = r_{3h} = 0$, while $r_{1g} \neq 0$, $r_{2g} = 0$, $r_{2h} \neq 0$. Further, by (80), Lemma 5 of [9], (69), (62) and (63)

$$h(\boldsymbol{r}_3) \leqslant |R_i^*| = |\tilde{R}_i| \leqslant 2|P||Q|$$
$$\leqslant 32|P||Q|\,h(\boldsymbol{r}_1)^2\,h(\boldsymbol{r}_2)^2 \leqslant 128|P|^3|Q|^3(\min\{|P|,|Q|\})^2,$$

which proves (66). Moreover by (79)

$$\boldsymbol{r}_3\boldsymbol{n} = \sum_{j=1}^{k} r_{3j}n_j = \sum_{\substack{i=1\\ j\neq g,h}}^{k} \delta_{i\varphi(j)}n_j = \sum_{j=1}^{k-2} \delta_{ij}n_{\varphi^{-1}(j)} = \boldsymbol{\delta}_i\boldsymbol{v},$$

hence by (81), (73) and (75)

$$|\boldsymbol{r}_3\boldsymbol{n}| \leqslant \frac{c_{12}(R_i^*)|\log\varepsilon| + c_{13}(R_i^*)}{\log|\eta|}$$
$$\leqslant r_{1g}r_{2h}(\log|\xi|)^{-1}\big(c_{12}(R_i^*)|\log c_{23}(R_g^*, R_h^*)| + c_{13}(R_i^*)$$
$$+ c_{12}(R_i^*)\max\{c_{24}(R_g^*, R_h^*)\log\max\{|\boldsymbol{r}_2\boldsymbol{n}|, |\boldsymbol{r}_1\boldsymbol{n}||r_{2h}|, 4\},$$
$$\log r_{1g}r_{2h} - \log\log|\xi|\}\big),$$

while by (64)

$$\log\max\{|\boldsymbol{r}_2\boldsymbol{n}|, |\boldsymbol{r}_1\boldsymbol{n}||r_{2h}|, 4\}$$
$$\leqslant \log\max\{c_{18}(P, Q), c_{17}(P, Q)|r_{2h}|, 4\} - \log\log|\xi|.$$

It follows that

$$|\boldsymbol{r}_3\boldsymbol{n}| \leqslant c_{25}(P, Q, \boldsymbol{r}_1, \boldsymbol{r}_2)(-\log\log|\xi|)(\log|\xi|)^{-1} + c_{26}(P, Q, \boldsymbol{r}_1, \boldsymbol{r}_2)(\log|\xi|)^{-1},$$

where

$$c_{25}(P, Q, \boldsymbol{r}_1, \boldsymbol{r}_2) = r_{1g}r_{2h}\max\{c_{12}(R_g^*), c_{12}(R_h^*)\}\,c_{24}(R_g^*, R_h^*),$$
$$c_{26}(P, Q, \boldsymbol{r}_1, \boldsymbol{r}_2) = r_{1g}r_{2h}\big(\max\{c_{12}(R_g^*), c_{12}(R_h^*)\}$$
$$\times(|\log c_{23}(R_g^*, R_h^*)| + c_{24}(R_g^*, R_h^*) + \log\max\{c_{18}(P, Q),$$
$$c_{17}(P, Q)|r_{2h}|, 4, r_{1g}r_{2h}\}) + \max\{c_{13}(R_g^*), c_{13}(R_h^*)\}\big).$$

(Note that g, h, R_g^*, R_h^* are uniquely determined by $P, Q, \boldsymbol{r}_1, \boldsymbol{r}_2$.) Since by (62), (63) for given P, Q there are only finitely many possibilities for $\boldsymbol{r}_1, \boldsymbol{r}_2$, the numbers $c_{25}(P, Q, \boldsymbol{r}_1, \boldsymbol{r}_2)$ and $c_{26}(P, Q, \boldsymbol{r}_1, \boldsymbol{r}_2)$ do not exceed bounds depending only on P and Q. Denoting these bounds by $c_{20}(P, Q)$ and $c_{21}(P, Q)$ we obtain (67).

Case B. Here we have by (73) and (75)–(77)

$$|v_0|\frac{\log|\xi|}{r_{1g}r_{2h}} = |v_0|\log|\eta| > |\log\varepsilon| > \log\max\{|\boldsymbol{r}_2\boldsymbol{n}|, |\boldsymbol{r}_1\boldsymbol{n}|\}.$$

However, by (78) and (64)

$$|v_0|\frac{\log|\xi|}{r_{1g}r_{2h}} \leqslant \max\{c_{17}(P, Q), c_{18}(P, Q)\},$$

hence we obtain

(86) $$\max\{|\boldsymbol{r}_1\boldsymbol{n}|, |\boldsymbol{r}_2\boldsymbol{n}|\} \leqslant \exp\max\{c_{17}(P, Q), c_{18}(P, Q)\}.$$

Case C. Here we have by (85), (75), (76) and (73)

$$|v_0|\log|\eta| < c_{16}(R_i^*)\varepsilon \leqslant \frac{\log|\xi|}{r_{1g}r_{2h}} = \log|\eta|,$$

hence $v_0 = 0$, by (78) $\min\{|\boldsymbol{r}_1\boldsymbol{n}|, |\boldsymbol{r}_2\boldsymbol{n}|\} = 0$ and

(87) $$\max\{|\boldsymbol{r}_1\boldsymbol{n}|, |\boldsymbol{r}_2\boldsymbol{n}|\} = (|\boldsymbol{r}_1\boldsymbol{n}|, |\boldsymbol{r}_2\boldsymbol{n}|).$$

Case D. Here we have by (78)

$$|(\boldsymbol{r}_2\boldsymbol{n})\log|\eta| - \log\theta_g| < c_{16}(R_g^*)\varepsilon,$$
$$|(\boldsymbol{r}_1\boldsymbol{n})r_{2h}\log|\eta| - \log\theta_h| < c_{16}(R_h^*)\varepsilon,$$

hence by (75) and (76)

(88) $$|(\boldsymbol{r}_1\boldsymbol{n})r_{2h}\log\theta_g - (\boldsymbol{r}_2\boldsymbol{n})\log\theta_h| < \big(c_{16}(R_g^*)|\boldsymbol{r}_1\boldsymbol{n}||r_{2h}| + c_{16}(R_h^*)|\boldsymbol{r}_2\boldsymbol{n}|\big)\varepsilon$$
$$< \max\{|\boldsymbol{r}_2\boldsymbol{n}|, |\boldsymbol{r}_1\boldsymbol{n}||r_{2h}|, 4\}^{1-c_{24}(R_g^*, R_h^*)}.$$

Now, by Theorem 2 of [1] (the case of two logarithms) we have either

(89) $$(\mathbf{r}_1\mathbf{n})r_{2h}\log\theta_g-(\mathbf{r}_2\mathbf{n})\log\theta_h=0$$

or

(90) $$|(\mathbf{r}_1\mathbf{n})r_{2h}\log\theta_g-(\mathbf{r}_2\mathbf{n})\log\theta_h|>B^{-C\Omega\log\Omega'},$$

where

$$B=\max\{|\mathbf{r}_1\mathbf{n}|r_{2h},|\mathbf{r}_2\mathbf{n}|,4\},$$
$$\Omega=\log\max\{h(\theta_g),4\}\log\max\{h(\theta_h),4\},$$
$$\Omega'=\min\{\log\max\{h(\theta_g),4\},\log\max\{h(\theta_h),4\}\}$$
$$C=(32d)^{400},\quad d=[\mathbf{Q}(\theta_g,\theta_h):\mathbf{Q}].$$

Since by (83)

$$d\leqslant c_{14}(R_g^*)c_{14}(R_h^*),$$

while by (84) and the inequality $c_{15}(R_i)\geqslant 4$ included in Lemma 7

$$\max\{h(\theta_i),4\}\leqslant c_{15}(R_i)\quad (i=g\text{ or }h),$$

we have by (77)

$$C\Omega\log\Omega'\leqslant c_{24}(R_g^*,R_h^*)-1.$$

Therefore (90) is incompatible with (88) and we are left with the equality (89). This implies

$$\theta_g^{(\mathbf{r}_1\mathbf{n})r_{2h}}=\theta_h^{(\mathbf{r}_2\mathbf{n})}.$$

Since θ_g and θ_h are not roots of unity (they are positive and different from 1) we have either $(\mathbf{r}_1\mathbf{n})r_{2h}=\mathbf{r}_2\mathbf{n}=0$ or

$$\frac{\max\{|(\mathbf{r}_1\mathbf{n})r_{2h}|,|\mathbf{r}_2\mathbf{n}|\}}{((\mathbf{r}_1\mathbf{n})r_{2h},\mathbf{r}_2\mathbf{n})}=C(\theta_g,\theta_h).$$

In both cases we have

(91) $$\max\{|\mathbf{r}_1\mathbf{n}|,|\mathbf{r}_2\mathbf{n}|\}\leqslant C(\theta_g,\theta_h)|r_{2h}|(\mathbf{r}_1\mathbf{n},\mathbf{r}_2\mathbf{n}).$$

In virtue of (83) and (84) for given R_g^*, R_h^* there are only finitely many possibilities for θ_g,θ_h, in turn for given P, Q there are only finitely many possibilities for r_{2h}, R_g^*, R_h^*. Hence $C(\theta_g,\theta_h)|r_{2h}|$ does not exceed a bound depending only on P, Q, which we denote by $c_{27}(P,Q)$. The inequality (91) implies

(92) $$\max\{|\mathbf{r}_1\mathbf{n}|,|\mathbf{r}_2\mathbf{n}|\}\leqslant c_{27}(P,Q)(\mathbf{r}_1\mathbf{n},\mathbf{r}_2\mathbf{n})$$

and (65) follows from (86), (87) and (92) with

$$c_{19}(P,Q)=\max\{\exp c_{17}(P,Q),\exp c_{18}(P,Q),c_{27}(P,Q)\}.$$

If $|\xi|\geqslant e$ (65) with the above value of $c_{19}(P,Q)$ follows from (64).

LEMMA 9. *Let $P,Q\in\mathbf{K}[x_1,\ldots,x_k]$, where $[\mathbf{K}:\mathbf{Q}]<\infty$ and $k\geqslant 3$. If $(P,Q)=1$ and $KP(x^{n_1},\ldots,x^{n_k})$, $KQ(x^{n_1},\ldots,x^{n_k})$ have as a common zero an algebraic integer ξ of degree at most $d>c_{28}(P,Q)$ then there exist two linearly independent vectors $\mathbf{r}_1,\mathbf{r}_2\in\mathbf{Z}^k$ such that*

(93) $$h(\mathbf{r}_1)\leqslant\min\{|P|,|Q|\},$$

(94) $$h(\mathbf{r}_2)\leqslant 2|P||Q|,$$

(95 $$|\mathbf{r}_\nu\mathbf{n}|\leqslant c_{28+\nu}(P,Q)d\left(\frac{\log d}{\log\log d}\right)^3\quad(\nu=1,2)$$

and either

(96) $$\max\{|\mathbf{r}_1\mathbf{n}|,|\mathbf{r}_2\mathbf{n}|\}\leqslant c_{31}(P,Q)(\mathbf{r}_1\mathbf{n},\mathbf{r}_2\mathbf{n}),\quad c_{31}(P,Q)\geqslant 1,$$

or there exists a vector $\mathbf{r}_3\in\mathbf{Z}^k$ linearly independent of $\mathbf{r}_1,\mathbf{r}_2$ such that

(97) $$h(\mathbf{r}_3)\leqslant 128|P|^3|Q|^3(\min\{|P|,|Q|\})^2$$

and

(98) $$|\mathbf{r}_3\mathbf{n}|\leqslant c_{32}(P,Q)d\frac{(\log d)^4}{(\log\log d)^3}.$$

Proof. Without loss of generality we may assume that $\mathbf{K}$ is the least field containing the coefficients of P and Q. Let $\mathbf{T}$ be the set of all isomorphic injections of $\mathbf{K}$ into $\mathbf{C}$. Since ξ is not a root of unity, by the result of Dobrowolski ([4], Corollary to Theorem 1) for every $\varepsilon>0$ and $d>d_0(\varepsilon)$ we have

$$\overline{|\xi|}>1+\frac{2-\varepsilon}{d}\left(\frac{\log\log d}{\log d}\right)^3,$$

hence for a suitable ξ' conjugate to ξ over $\mathbf{Q}$ and $d>d_0(\frac{1}{2})$

(99) $$\log|\xi'|>\frac{3}{2d}\left(\frac{\log\log d}{\log d}\right)^3+o\left(\frac{1}{d^2}\right):=E(d).$$

Let us choose $c_{28}(P,Q)\geqslant d_0(\frac{1}{2})$ so that for $d\geqslant c_{28}(P,Q)$

(100) $$\log d\geqslant 1,$$

(101) $$E(d)>\frac{1}{d}\left(\frac{\log\log d}{\log d}\right)^3,$$

(102) $$-\log E(d)<2\log d$$

and let us set

(103) $$c_{28+\nu}(P,Q)=\max_{\tau\in\mathbf{T}}c_{16+\nu}(P^\tau,Q^\tau)\quad(\nu=1,2),$$

(104) $$c_{31}(P,Q)=\max_{\tau\in\mathbf{T}}c_{19}(P^\tau,Q^\tau),$$

(105) $$c_{32}(P,Q)=\max_{\tau\in\mathbf{T}}\big(2c_{20}(P^\tau,Q^\tau)+c_{21}(P^\tau,Q^\tau)\big).$$

Clearly there exists an isomorphic injection τ of K into C such that ξ' is a common zero of

$$KP^{\tau}(x^{n_1}, \ldots, x^{n_k}) \quad \text{and} \quad KQ^{\tau}(x^{n_1}, \ldots, x^{n_k}).$$

Applying Lemma 8 with $K^{\tau}, P^{\tau}, Q^{\tau}, \xi'$ in place of K, P, Q, ξ, respectively we obtain (93), (94) as a consequence of (62), (63); (95) as a consequence of (64) and (99), (101); finally the alternative (96) or (97), (98) as a consequence of the alternative (65) or (66), (67) and of (99)–(102), (105).

LEMMA 10. *Let* $P, Q \in K[x_1, \ldots, x_k]$, $(P, Q) = 1$, K_0 *be the field generated by the coefficients of* P, Q *over the prime field of* K, Ω *a subfield of* K_0, $\hat{\Omega}$ *its algebraic closure. If* ξ *is a common zero of* $KP(x^{n_1}, \ldots, x^{n_k})$ *and* $KQ(x^{n_1}, \ldots, x^{n_k})$ *and either* $\Omega = Q$, $[K_0 : Q] < \infty$, ξ *is not an algebraic unit or* $\mathrm{tr.deg}\, K_0/\Omega = 1$, $\xi \notin \hat{\Omega}$ *then there exists a vector* $\gamma \in Z^k$ *such that*

$$(106) \qquad 0 < h(\gamma) \leqslant c_{33}(P, Q, \Omega),$$

$$(107) \qquad \gamma n = 0.$$

Proof. In both cases considered in the lemma there is a divisor theory for the extension K_0/Ω. For every non-zero polynomial $F \in K_0[x_1, \ldots, x_k]$ we set

$$(108) \qquad c_{34}(F, K_0, \Omega) = \max\{\max|\mathrm{ord}_{\mathfrak{p}} f_1 - \mathrm{ord}_{\mathfrak{p}} f_2|, 1\},$$

where the inner maximum is taken over all prime divisors $\mathfrak{p}$ of K_0/Ω and all pairs $\langle f_1, f_2 \rangle$ of non-zero coefficients of F (note that for every $f \neq 0$ there exist only finitely many prime divisors $\mathfrak{p}$ of K_0/Ω such that $\mathrm{ord}_{\mathfrak{p}} f \neq 0$). We shall prove the assertion of the lemma with

$$(109) \qquad c_{33}(P, Q, \Omega) = \max_{1 \leqslant j \leqslant k} \left(c_{34}(R_j, K_0, \Omega)|P| + c_{34}(P, K_0, \Omega)|R_j|\right),$$

where R_j is the resultant of P and Q with respect to x_j. Since both R_j and K_0 are determined uniquely by P and Q the above definition of $c_{33}(P, Q, \Omega)$ is correct. We assume $\xi \in \hat{K}_0$, otherwise $P(x^{n_1}, \ldots, x^{n_k}) = 0$ and (106)–(107) is trivial.

Let $K_1 = K_0(\xi)$. In both cases considered in the lemma there exists a prime divisor $\mathfrak{p}_1$ of K_1/Ω such that

$$e_1 = \mathrm{ord}_{\mathfrak{p}_1} \xi \neq 0.$$

Let $\mathfrak{p}_0$ be the divisor of K_0 divisible by $\mathfrak{p}_1$ and put

$$\mathrm{ord}_{\mathfrak{p}_1} \mathfrak{p}_0 = e_0.$$

Let P be again given by the formula

$$P = \sum_{\alpha \in A} \pi_\alpha \prod_{j=1}^{k} x_j^{\alpha_j} \quad (\pi_\alpha \neq 0 \text{ for } \alpha \in A)$$

and let

$$\mathrm{ord}_{\mathfrak{p}_0} \pi_\alpha = p_\alpha.$$

It follows from

$$0 = P(\xi^{n_1}, \ldots, \xi^{n_k}) = \sum_{\alpha \in A} \pi_\alpha \xi^{\alpha n}$$

that the minimal value of the function $e_0 p_\alpha + e_1 \alpha n$ on the set A is taken by this function at least twice. Thus there exist two distinct vectors $\alpha_7, \alpha_8 \in A$ such that

$$e_0 p_{\alpha_7} + e_1 \alpha_7 n = e_0 p_{\alpha_8} + e_1 \alpha_8 n,$$

i.e.

$$(110) \qquad e_1 s_1 n + e_0 \sigma_1 = 0,$$

where $s_1 = \alpha_8 - \alpha_7$, $\sigma_1 = p_{\alpha_8} - p_{\alpha_7}$. Hence

$$(111) \qquad 0 < h(s_1) \leqslant |P|,$$

$$(112) \qquad |\sigma_1| \leqslant c_{34}(P, K_0, \Omega).$$

Without loss of generality we may assume that $s_{1k} \neq 0$. Let us consider as in the proof of Lemma 3 the resultant R_k of P and Q with respect to x_k. We have

$$R_k(\xi^{n_1}, \ldots, \xi^{n_{k-1}}) = 0$$

and by the argument applied previously to P there exist a vector $s_2 \in Z^{k-1} \times \{0\}$ and an integer σ_2 such that

$$(113) \qquad e_1 s_2 n + e_0 \sigma_2 = 0,$$

$$(114) \qquad 0 < h(s_2) \leqslant |R_k|,$$

$$(115) \qquad |\sigma_2| \leqslant c_{34}(R_k, K_0, \Omega).$$

We put

$$\gamma = \begin{cases} s_1 \sigma_2 - s_2 \sigma_1 & \text{if } \sigma_2 \neq 0, \\ s_2 & \text{if } \sigma_2 = 0. \end{cases}$$

The inequality (106) follows from (108), (109), (111), (112), (114), and (115), while (107) follows from (110) and (113) on eliminating e_0 and e_1.

LEMMA 11. *Theorem* 1 *holds for* $k = 3$, $[K : Q] < \infty$.

Proof. We may assume without loss of generality that K is the field generated over Q by the coefficients of P, Q. Suppose first that $(n_1, n_2, n_3) = 1$. By Lemma 5 if $KP(x^{n_1}, x^{n_2}, x^{n_3})$, $KQ(x^{n_1}, x^{n_2}, x^{n_3})$ have a common zero ξ then either there exists a vector $\gamma \in Z^3$ such that

$$\gamma n = 0$$

and

$$0 < h(\gamma) < c_8(P, Q)$$

or

$$[K(\xi) : K] < 12|P||Q|\sqrt{3h(n)}.$$

In the former case we have the assertion of the theorem provided $c_1(P, Q) \geqslant c_8(P, Q)$. In the latter case

(116) $$[Q(\xi):Q] \leqslant 12[K:Q]|P||Q|\sqrt{3h(n)} = d.$$

We shall consider separately two cases:

A. ξ is an algebraic integer,

B. ξ is not an algebraic integer.

A. In virtue of Lemma 9 we have either

(117) $$d < c_{28}(P, Q),$$

or there exist two vectors $r_1, r_2 \in Z^3$ linearly independent and such that

(118) $$h(r_1) \leqslant \min\{|P|, |Q|\},$$

(119) $$h(r_2) \leqslant 2|P||Q|,$$

(120) $$\max\{|r_1 n|, |r_2 n|\} \leqslant c_{31}(P, Q)(r_1 n, r_2 n),$$

or there exist three vectors $r_1, r_2, r_3 \in Z^3$ linearly independent and such that in addition to (116), (117)

(121) $$h(r_3) \leqslant 128|P|^3|Q|^3(\min\{|P|, |Q|\})^2,$$

(122) $$|r_\nu n| \leqslant c_{28+\nu}(P, Q)\, d\left(\frac{\log d}{\log\log d}\right)^2 \quad (\nu = 1, 2),$$

(123) $$|r_3 n| \leqslant c_{32}(P, Q)\, d\frac{(\log d)^4}{(\log\log d)^3}.$$

(118), (119), (120) imply the assertion of the theorem with

$$\gamma = \begin{cases} \dfrac{(r_1 \times r_2)\times n}{(r_1 n, r_2 n)} & \text{if } r_1 n \neq 0, \\ r_1 & \text{if } r_1 n = 0, \end{cases}$$

provided $c_1(P,Q) \geqslant c_{31}(P,Q)(2|P||Q| + \min\{|P|,|Q|\})$. On the other hand (118), (119), (121), (122) and (123) imply via the Cramer formulae

(124) $$h(n) \leqslant 2h(r_1)h(r_2)h(r_3)\sum_{\nu=1}^{3}\frac{|r_\nu n|}{h(r_\nu)} \leqslant c_{35}(P, Q)\, d\frac{(\log d)^4}{(\log\log d)^3},$$

where

$$\begin{aligned} c_{35}(P, Q) = {} & 512|P|^4|Q|^4(\min\{|P|, |Q|\})^2 c_{29}(P, Q) \\ & + 256|P|^3|Q|^3(\min\{|P|, |Q|\})^3 c_{30}(P, Q) \\ & + 4|P||Q|\min\{|P|, |Q|\}\, c_{32}(P, Q). \end{aligned}$$

Now, by (116) and (124)

$$d \leqslant 12[K:Q]|P||Q|\sqrt{3c_{35}(P, Q)\, d\frac{(\log d)^4}{(\log\log d)^3}},$$

hence for a suitable $c_{36}(P, Q)$

(125) $$d \leqslant c_{36}(P, Q).$$

Let $c_{37}(P, Q) = \max\{c_{28}(P, Q), c_{36}(P, Q)\}$. The alternative (117) or (125) gives

$$d \leqslant c_{37}(P, Q)$$

and by (116), for a suitable $c_{38}(P, Q)$

$$h(n) \leqslant c_{38}(P, Q).$$

By the Bombieri–Vaaler theorem (see [2]), the assertion of Theorem 1 holds provided

$$c_1(P, Q) \geqslant \sqrt{\sqrt{3}c_{38}(P, Q)}.$$

B. In virtue of Lemma 10 the assertion of the theorem holds provided

$$c_1(P, Q) \geqslant c_{33}(P, Q, Q).$$

Summing up the considered cases we conclude that if $(n_1, n_2, n_3) = 1$ Theorem 1 holds with

$$\begin{aligned} & c_1(P, Q) \\ & = \max\{c_{31}(P, Q)(2|P||Q| + \min\{|P|, |Q|\}), \sqrt{\sqrt{3}c_{38}(P, Q)}\, c_{33}(P, Q, Q)\}. \end{aligned}$$

Suppose now that $(n_1, n_2, n_3) = d$, $n_i = dm_i$ $(1 \leqslant i \leqslant 3)$. If

$$(JP(x^{m_1}, x^{m_2}, x^{m_3}), JQ(x^{m_1}, x^{m_2}, x^{m_3})) = G(x)$$

then by Lemma 9 of [10]

$$(JP(x^{n_1}, x^{n_2}, x^{n_3}), JQ(x^{n_1}, x^{n_2}, x^{n_3})) = G(x^d).$$

The assumption implies that $KG(x^d) \neq 1$, hence $KG(x) \neq 1$. Since $(m_1, m_2, m_3) = 1$ the already proved case of Theorem 1 applies and gives the existence of a vector $\gamma \in Z^3$ such that

$$\sum_{i=1}^{3}\gamma_i m_i = 0 \quad \text{and} \quad 0 < h(\gamma) \leqslant c_1(P, Q).$$

Now,

$$\gamma n = d\sum_{i=1}^{s}\gamma_i m_i = 0$$

and the proof is complete.

Lemma 12. *If Theorem 1 is true for given* K *and* k *then for every finite subset* S *of* $K[x_1, \ldots, x_k]$ *and every vector* $n \in Z^k$ *if*

(126) $$\underset{F\in S}{\text{g.c.d.}}\, F = 1,$$

but

(127) $$\underset{F\in S}{\text{g.c.d.}}\, KF(x^{n_1}, x^{n_2}, \ldots, x^{n_k}) \neq 1$$

there exists a vector $\gamma \in Z^k$ *such that*

$$0 < h(\gamma) \leqslant c_{39}(S) \quad and \quad \gamma n = 0.$$

Proof. Let us choose $F_0 \in S$, $F_0 \neq 0$ and let

$$F_0 \overset{\text{can}}{\underset{K}{=}} \text{const} \prod_{\sigma=1}^{s} P_\sigma^{e_\sigma}.$$

By (126) for every index $\sigma \leqslant s$ there exists a polynomial $F_\sigma \in S$ such that $(P_\sigma, F_\sigma) = 1$. The condition (127) implies that for at least one $\varrho \leqslant s$

$$\big(KP_\varrho(x^{n_1}, \ldots, x^{n_k}), \operatorname*{g.c.d.}_{F \in S \setminus \{F_0\}} KF(x^{n_1}, \ldots, x^{n_k})\big) \neq 1$$

hence *a fortiori*

$$\big(KP_\varrho(x^{n_1}, \ldots, x^{n_k}), KF_\varrho(x^{n_1}, \ldots, x^{n_k})\big) \neq 1.$$

By the assumption there exists a vector $\gamma \in Z^k$ such that

$$0 < h(\gamma) < c_1(P_\varrho, F_\varrho), \quad \gamma n = 0.$$

Therefore, it suffices to take

$$c_{29}(S) = \max_{\sigma \leqslant s} c_1(P_\sigma, F_\sigma).$$

3. Proofs of Theorems 1 and 2.

Proof of Theorem 1. We shall proceed by induction on the transcendence degree r of K_0, the field generated by the coefficients of P and Q over the prime field Π of K.

If $r = 0$ and char $K = 0$ the theorem is contained in Lemma 11. If $r = 0$ and char $K > 0$ the theorem is trivial since then for every $P \in K_0[x] \setminus \{0\}$ we have $KP(x) \in K_0$.

Let us consider the case, where tr. deg. $K_0/\Pi = r \geqslant 1$ assuming that the theorem holds, whenever tr. deg. $K_0/\Pi < r$. The assumption implies the truth of the theorem for all K with tr. deg. $K/\Pi < r$ and $k = 3$ if char $K = 0$, k arbitrary if char $K > 0$. Let $t_1, \ldots, t_r$ be a transcendence basis of K_0 over Π so that $[K_0 : \Pi(t_1, \ldots, t_r)] < \infty$. Let us put $\Omega = \Pi(t_1, \ldots, t_{r-1})$ and let $b_1, \ldots, b_s$ be a basis of $K_0\hat{\Omega}(t_r)$ over $\hat{\Omega}(t_r)$, $\hat{\Omega}$ being the algebraic closure of Ω. We have for suitable polynomials $D \in \hat{\Omega}(t_r)$, $P_{\sigma i}$, $Q_{\sigma j} \in \hat{\Omega}[x_1, \ldots, x_k]$ $(1 \leqslant \sigma \leqslant s, 0 \leqslant i \leqslant p, 0 \leqslant j \leqslant q)$

$$P = D^{-1} \sum_{\sigma=1}^{s} \sum_{i=0}^{p} P_{\sigma i} t_r^i b_\sigma,$$
$$Q = D^{-1} \sum_{\sigma=1}^{s} \sum_{j=0}^{q} Q_{\sigma j} t_r^j b_\sigma.$$

Let $S = \bigcup_{\sigma=1}^{s} \bigcup_{i=0}^{p} \{P_{\sigma i}\} \cup \bigcup_{\sigma=1}^{s} \bigcup_{j=0}^{q} \{Q_{\sigma j}\}$. Since $(P, Q) = 1$ we have $\operatorname*{g.c.d.}_{F \in S} F = 1$.

If $KP(x^{n_1}, \ldots, x^{n_k})$ and $KQ(x^{n_1}, \ldots, x^{n_k})$ have a common zero ξ we have either $\xi \in \hat{\Omega}$ or $\xi \notin \hat{\Omega}$. In the former case since $t_r^i b_\sigma$ $(1 \leqslant \sigma \leqslant s, i = 0, 1, \ldots)$ are linearly independent over $\hat{\Omega}$ we obtain

$$P_{\sigma i}(\xi^{n_1}, \ldots, \xi^{n_k}) = 0, \quad Q_{\sigma j}(\xi^{n_1}, \ldots, \xi^{n_k}) = 0 \quad (1 \leqslant \sigma \leqslant s, 0 \leqslant i \leqslant p, 0 \leqslant j \leqslant q)$$

and since ξ is neither 0 nor a root of unity

$$\operatorname*{g.c.d.}_{F \in S} KF(x^{n_1}, \ldots, x^{n_k}) \neq 1.$$

Since tr.deg. $\hat{\Omega}/\Pi = r-1$ the inductive assumption implies by virtue of Lemma 12 the existence of a vector $\gamma \in Z^k$ such that

$$0 < h(\gamma) \leqslant c_{39}(S) \quad \text{and} \quad \gamma n = 0.$$

On the other hand, $\Omega \subset K_0$ and tr. deg. $K_0/\Omega = 1$, thus if $\xi \notin \hat{\Omega}$ Lemma 10 implies the existence of a vector $\gamma \in Z^k$ such that

$$0 < h(\gamma) \leqslant c_{33}(P, Q, \Omega) \quad \text{and} \quad \gamma n = 0.$$

The numbers $c_{39}(S)$ and $c_{33}(P, Q, \Omega)$ depend upon the choice of the transcendence basis $t_1, \ldots, t_r$ and the choice of the linear basis $b_1, \ldots, b_s$. Since this choice is arbitrary and $h(\gamma)$ takes only integer values we put

$$c_1(P, Q) = \inf \max \{c_{39}(S), c_{33}(P, Q, \Omega)\},$$

where the infimum is taken over all possible bases $t_1, \ldots, t_r$ and $b_1, \ldots, b_s$. The inductive proof is complete.

LEMMA 13. *Let* $P, Q \in C[x_1, \ldots, x_k]$, $(P, Q) = 1$. *If* $p, q \in Z^k$,

$$\big(JP(y^{p_1} z^{q_1}, \ldots, y^{p_k} z^{q_k}), JQ(y^{p_1} z^{q_1}, \ldots, y^{p_k} z^{q_k})\big) = D(z) \in C[z],$$

$KD(z) \neq 1$ *then there exist* $d \geqslant 2$ *linearly independent vectors* $m_1, \ldots, m_d \in Z^k$ *such that*

$$h(m_i) \leqslant i \max\{|P|, |Q|\} \quad (1 \leqslant i \leqslant d), \quad m_i p = 0$$

and either $d \geqslant 4$ *or there exists a vector* $\beta \in Z^d$ *such that*

$$0 < h(\beta) \leqslant c_{40}(P, Q), \quad \beta[m_1 q, \ldots, m_d q] = 0.$$

Proof. We follow step by step the proof of Lemma 4 retaining the notation introduced there. If $d = 2$ we take

$$\beta = \begin{cases} [1, 0] & \text{if} \quad m_1 q = 0, \\ \left[\dfrac{m_2 q}{(m_1 q, m_2 q)}, \dfrac{-m_1 q}{(m_1 q, m_2 q)}\right] & \text{if} \quad m_1 q \neq 0 \end{cases}$$

and obtain

$$0 < h(\beta) \leqslant \max\{1, c_7(P, Q)\}.$$

If $d = 3$ in virtue of Theorem 1 we can apply Lemma 12 taking in that lemma $\boldsymbol{K} = \boldsymbol{C}$, $k = 3$, $\boldsymbol{S}$ defined in the proof of Lemma 4 and $n_i = \boldsymbol{m}_i\boldsymbol{q}$ $(1 \leqslant i \leqslant 3)$. We obtain the existence of a vector $\boldsymbol{\beta} \in \boldsymbol{Z}^3$ such that

$$0 < h(\boldsymbol{\beta}) \leqslant c_{39}(\boldsymbol{S}), \quad \boldsymbol{\beta}[\boldsymbol{m}_1\boldsymbol{q}, \boldsymbol{m}_2\boldsymbol{q}, \boldsymbol{m}_3\boldsymbol{q}] = 0.$$

By (18) the number of possibilities for the set $\boldsymbol{S}$ for fixed P, Q and d is finite. Hence $c_{39}(\boldsymbol{S})$ does not exceed a bound depending only on P and Q. Denoting this bound by $c_{41}(P,Q)$ we put

$$c_{40}(P,Q) = \max\{1, c_7(P,Q), c_{41}(P,Q)\}.$$

LEMMA 14. *Let* $P, Q \in \boldsymbol{K}[x_1, \ldots, x_k], [\boldsymbol{K}:\boldsymbol{Q}] < \infty, (P,Q) = 1$. *If* $(n_1, \ldots, n_k) = 1$ *and*

$$(KP(x^{n_1}, \ldots, x^{n_k}), KQ(x^{n_1}, \ldots, x^{n_k})) \neq 1$$

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

$$0 < h(\boldsymbol{\gamma}) \leqslant c_{42}(P,Q), \tag{128}$$

$$\boldsymbol{\gamma}\boldsymbol{n} = 0, \tag{129}$$

or there exist two vectors $\boldsymbol{l}_1, \boldsymbol{l}_2 \in \boldsymbol{Z}^k$ *linearly independent and such that*

$$h(\boldsymbol{l}_1) \leqslant \min\{|P|, |Q|\}, \tag{130}$$

$$h(\boldsymbol{l}_2) \leqslant 2|P||Q|, \tag{131}$$

$$\max\{|\boldsymbol{l}_1\boldsymbol{n}|, |\boldsymbol{l}_2\boldsymbol{n}|\} \leqslant 2\sqrt{2}k|P||Q|h(\boldsymbol{n})^{(k-2)/(2k-2)}(\boldsymbol{l}_1\boldsymbol{n}, \boldsymbol{l}_2\boldsymbol{n}), \tag{132}$$

or there exist three vectors $\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \in \boldsymbol{Z}^k$ *linearly independent and such that*

$$h(\boldsymbol{r}_1) \leqslant \min\{|P|, |Q|\}, \tag{133}$$

$$h(\boldsymbol{r}_2) \leqslant 2|P||Q|, \tag{134}$$

$$h(\boldsymbol{r}_3) \leqslant 128|P|^3|Q|^3(\min\{|P|, |Q|\})^2, \tag{135}$$

$$|\boldsymbol{r}_i\boldsymbol{n}| \leqslant c_{42+i}(P, Q)\, h(\boldsymbol{n})^{(k-2)/(k-1)}\left(\frac{\log h(\boldsymbol{n})}{\log\log h(\boldsymbol{n})}\right)^3 \quad (i = 1, 2), \tag{136}$$

$$|\boldsymbol{r}_3\boldsymbol{n}| \leqslant c_{45}(P, Q)h(\boldsymbol{n})^{(k-2)/(k-1)}(\log h(\boldsymbol{n}))^4(\log\log h(\boldsymbol{n}))^{-3}, \tag{137}$$

or there exist four vectors $\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4 \in \boldsymbol{Z}^k$ *linearly independent and such that*

$$h(\boldsymbol{m}_i) \leqslant i\max\{|P|, |Q|\} \quad (1 \leqslant i \leqslant 4), \tag{138}$$

$$\max\{|\boldsymbol{m}_1\boldsymbol{n}|, |\boldsymbol{m}_2\boldsymbol{n}|, |\boldsymbol{m}_3\boldsymbol{n}|, |\boldsymbol{m}_4\boldsymbol{n}|\} \leqslant 8k\max\{|P|, |Q|\}h(\boldsymbol{n})^{(k-2)/(k-1)}(\boldsymbol{m}_1\boldsymbol{n}, \boldsymbol{m}_2\boldsymbol{n}, \boldsymbol{m}_3\boldsymbol{n}, \boldsymbol{m}_4\boldsymbol{n}). \tag{139}$$

Proof. Let us choose a decomposition

$$\boldsymbol{n} = u\boldsymbol{p} + v\boldsymbol{q}; \quad u, v \in \boldsymbol{Z}, \boldsymbol{p}, \boldsymbol{q} \in \boldsymbol{Z}^k, \dim(\boldsymbol{p}, \boldsymbol{q}) = 2, \tag{140}$$

$$h(\boldsymbol{p})h(\boldsymbol{q}) \leqslant 2h(\boldsymbol{n})^{(k-2)/(k-1)} \tag{141}$$

the existence of which is guaranteed by Lemma 1. In view of symmetry between $\boldsymbol{p}$ and $\boldsymbol{q}$ we may assume that $h(\boldsymbol{p}) \leqslant h(\boldsymbol{q})$, hence

$$h(\boldsymbol{p}) \leqslant \sqrt{2}h(\boldsymbol{n})^{(k-2)/(2k-2)}. \tag{142}$$

It follows from $(n_1, \ldots, n_k) = 1$ that $(u, v) = 1$. If we had $v = 0$ it would follow $u = \pm 1, h(\boldsymbol{n}) = h(\boldsymbol{p})$ and thus

$$h(\boldsymbol{n}) \leqslant \sqrt{2}h(\boldsymbol{n})^{(k-2)/(2k-2)}; \quad h(\boldsymbol{n}) \leqslant 2^{(k-1)/k} < 2, \quad h(\boldsymbol{n}) = 1.$$

Since for $h(\boldsymbol{n}) = 1$ we can choose a decomposition (140) with $h(\boldsymbol{p}) = h(\boldsymbol{q}) = 1, v = \pm 1$, we may assume that

$$(u, v) = 1, \quad v \neq 0. \tag{143}$$

Let us consider polynomials

$$G = JP(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k}), \quad H = JQ(y^{p_1}z^{q_1}, \ldots, y^{p_k}z^{q_k}), \tag{144}$$

$$D = (G, H). \tag{145}$$

If $D \in \boldsymbol{C}[y,z]\backslash\boldsymbol{C}[z]$ then by Lemma 3 there are two linearly independent vectors $\boldsymbol{l}_1, \boldsymbol{l}_2 \in \boldsymbol{Z}^k$ such that (131), (132) hold,

$$(\boldsymbol{l}_1\boldsymbol{p})(\boldsymbol{l}_2\boldsymbol{q}) = (\boldsymbol{l}_2\boldsymbol{p})(\boldsymbol{l}_1\boldsymbol{q})$$

and

$$\boldsymbol{l}_2\boldsymbol{q} = 0 \quad \text{if} \quad \boldsymbol{l}_2\boldsymbol{p} = 0.$$

Hence

$$(\boldsymbol{l}_1\boldsymbol{p})(\boldsymbol{l}_2\boldsymbol{n}) - (\boldsymbol{l}_2\boldsymbol{p})(\boldsymbol{l}_1\boldsymbol{n}) = (\boldsymbol{l}_1\boldsymbol{p})(\boldsymbol{l}_2u\boldsymbol{p} + \boldsymbol{l}_2v\boldsymbol{q}) - (\boldsymbol{l}_2\boldsymbol{p})(\boldsymbol{l}_1u\boldsymbol{p} + \boldsymbol{l}_1v\boldsymbol{q}) = 0$$

and either $\boldsymbol{l}_2\boldsymbol{n} \neq 0$, thus $\boldsymbol{l}_2\boldsymbol{p} \neq 0$ and by (130), (131), (142)

$$\frac{\max\{|\boldsymbol{l}_1\boldsymbol{n}|, |\boldsymbol{l}_2\boldsymbol{n}|\}}{(\boldsymbol{l}_1\boldsymbol{n}, \boldsymbol{l}_2\boldsymbol{n})} = \frac{\max\{|\boldsymbol{l}_1\boldsymbol{p}|, |\boldsymbol{l}_2\boldsymbol{p}|\}}{(\boldsymbol{l}_1\boldsymbol{p}, \boldsymbol{l}_2\boldsymbol{p})} \leqslant \max\{|\boldsymbol{l}_1\boldsymbol{p}|, |\boldsymbol{l}_2\boldsymbol{p}|\}$$

$$\leqslant k\max\{h(\boldsymbol{l}_1), h(\boldsymbol{l}_2)\}h(\boldsymbol{p}) \leqslant 2\sqrt{2}k|P||Q|h(\boldsymbol{n})^{(k-2)/(2k-2)},$$

or $\boldsymbol{l}_2\boldsymbol{n} = 0$ and then

$$\max\{|\boldsymbol{l}_1\boldsymbol{n}|, |\boldsymbol{l}_2\boldsymbol{n}|\} = (\boldsymbol{l}_1\boldsymbol{n}, \boldsymbol{l}_2\boldsymbol{n}).$$

In both cases the inequality (132) holds.

If $D \in \boldsymbol{C}[z]$ and $KD \neq 1$ then by Lemma 13 there exist $d \geqslant 2$ vectors $\boldsymbol{m}_i \in \boldsymbol{Z}^k$ $(1 \leqslant i \leqslant d)$ linearly independent such that (138) holds, $\boldsymbol{m}_i\boldsymbol{p} = 0 (1 \leqslant i \leqslant d)$ and either $d \geqslant 4$ or there exists a vector $\boldsymbol{\beta} \in \boldsymbol{Z}^d$ satisfying

$$0 < h(\boldsymbol{\beta}) \leqslant c_{40}(P, Q), \tag{146}$$

$$\boldsymbol{\beta}[\boldsymbol{m}_1\boldsymbol{q}, \ldots, \boldsymbol{m}_d\boldsymbol{q}] = 0. \tag{147}$$

Since by (140)

$$\boldsymbol{m}_i\boldsymbol{n} = v\boldsymbol{m}_i\boldsymbol{q} \quad (1 \leqslant i \leqslant d),$$

in the former case we find either $m_i n = 0$ $(1 \leqslant i \leqslant 4)$ which implies (139), or by (138), (141)

$$\frac{\max\{|m_1 n|, |m_2 n|, |m_3 n|, |m_4 n|\}}{(m_1 n, m_2 n, m_3 n, m_4 n)} = \frac{\max\{|m_1 q|, |m_2 q|, |m_3 q|, |m_4 q|\}}{(m_1 q, m_2 q, m_3 q, m_4 q)}$$
$$\leqslant \max_{1\leqslant i\leqslant 4} |m_i q| \leqslant k \max_{1\leqslant i\leqslant 4} h(m_i)h(q)$$
$$\leqslant 8k\max\{|P|, |Q|\}\, h(n)^{(k-2)/(k-1)}.$$

In the latter case we set

$$\gamma = \sum_{i=1}^{d} \beta_i m_i$$

and (129) follows from (147). On the other hand assuming, as we may, $d \leqslant 3$ we obtain from (138) and (145)

$$h(\gamma) \leqslant h(\beta) \sum_{i=1}^{d} h(m_i) \leqslant 6\, c_{40}(P, Q) \max\{|P|, |Q|\}.$$

Since m_i are linearly independent and $\beta \neq 0$ we have also $h(\gamma) > 0$ and (128) holds provided

$$c_{42}(P, Q) \geqslant 6 c_{40}(P, Q) \max\{|P|, |Q|\}.$$

It remains to consider the case

$$D \in C[z] \quad \text{and} \quad KD(z) = 1. \tag{148}$$

Let $G_1 = GD^{-1}$, $H_1 = HD^{-1}$, R be the resultant of G_1, H_1 with respect to z. By (145) $(G_1, H_1) = 1$. By virtue of Lemma 4 of [9] and of (144) we have

$$\operatorname{card}\{\langle\eta, \zeta\rangle \in C^2\colon G_1(\eta, \zeta) = H_1(\eta, \zeta) = 0\} \leqslant \deg R$$
$$\leqslant \deg_y G_1 \deg_z H_1 + \deg_z G_1 \deg_y H_1 \leqslant k|P|h(p)k|Q|h(q) + k|P|h(q)k|Q|h(p)$$
$$= 2k^2|P||Q|h(p)h(q).$$

On the other hand, if ξ is a common zero of $KP(x^{n_1}, \ldots, x^{n_k})$ and $KQ(x^{n_1}, \ldots, x^{n_k})$, by virtue of (140) and (144) $\langle\xi^u, \xi^v\rangle$ is a common zero of G and H, while by virtue of (143) and (148) it is not a zero of D. Therefore

$$G_1(\xi^u, \xi^v) = H_1(\xi^u, \xi^v) = 0.$$

Since by (143) $\langle\xi^u, \xi^v\rangle$ determines ξ uniquely, it follows that the number of common zeros of $KP(x^{n_1}, \ldots, x^{n_k})$, $KQ(x^{n_1}, \ldots, x^{n_k})$ does not exceed $2k^2|P||Q|h(p)h(q)$. However together with ξ every number conjugate to ξ over the field K_0 generated by the coefficients of P and Q is a common zero in question, hence by (141)

$$[K_0(\xi)\colon K_0] \leqslant 4k^2|P||Q|h(n)^{(k-2)/(k-1)}.$$

Since $[K_0\colon Q]$ depends only of P, Q we get

$$[Q(\xi)\colon Q] \leqslant c_{46}(P, Q) h(n)^{(k-2)/(k-1)}, \tag{149}$$

where we may assume without loss of generality that $c_{46}(P, Q) \geqslant c_{28}(P, Q)$. If ξ is an algebraic integer, we obtain from Lemma 9 the existence of three linearly independent vectors $r_1, r_2, r_3 \in Z^k$ satisfying (93)–(98) and either (96) or (97) and (98). Now (93), (94), (97) imply (133), (134), (135), respectively; (95) and (98) together with (149) imply (136) and (137), respectively, with suitable c_{43}, c_{44}, c_{45}. On the other hand, (96) imply (128) and (129) with

$$\gamma = \begin{cases} \dfrac{(r_1 \times r_2) \times n}{(r_1 n, r_2 n)} & \text{if} \quad r_1 n \neq 0, \\ r_1 & \text{if} \quad r_1 n = 0, \end{cases}$$

provided

$$c_{42}(P, Q) \geqslant c_{31}(P, Q)(2|P||Q| + \min\{|P|, |Q|\}).$$

In the remaining case, where ξ is not an algebraic integer we apply Lemma 10 with $\Omega = Q$ and obtain (128) and (129) provided

$$c_{42}(P, Q) \geqslant c_{33}(P, Q, Q).$$

LEMMA 15. *Theorem 2 holds if the coefficients of P, Q lie in a finite extension of Q.*

Proof. Let $S(P, Q, N)$ be the set of all integer vectors n such that $h(n) \leqslant N$ and

$$(KP(x^{n_1}, \ldots, x^{n_k}), KQ(x^{n_1}, \ldots, x^{n_k})) \neq 1,$$

and let $S_0(N)$ be the subset of $S(P, Q, N)$ consisting of all vectors satisfying $(n_1, \ldots, n_k) = 1$. If for a vector $n \in S(P, Q, N)$ we have $(n_1, \ldots, n_k) = d$, $n_j = dm_j$, then by Lemma 9 of [10]

$$(KP(x^{m_1}, \ldots, x^{m_k}), KQ(x^{m_1}, \ldots, x^{m_k})) \neq 1$$

hence $m \in S_0(N/d)$. Thus we have

$$S(P, Q, N) \subset \bigcup_{d=1}^{N} d\, S_0(N/d),$$

$$\operatorname{card} S(P, Q, N) \leqslant \sum_{d=1}^{N} \operatorname{card} S_0(N/d) \tag{150}$$

and it will be sufficient to estimate the cardinality of $S_0(N)$. In virtue of Lemma 14 we have

$$S_0(N) \subset \bigcup_{i=1}^{4} S_i(N), \tag{151}$$

where $S_i(N)$ $(1 \leqslant i \leqslant 4)$ is the set of all vectors $\boldsymbol{n} \in S_0(N)$ such that for $i = 1$ there exists a vector $\gamma \in \boldsymbol{Z}^k$ satisfying (128) and (129), for $i = 2$ there exist two vectors $\boldsymbol{l}_1, \boldsymbol{l}_2 \in \boldsymbol{Z}^k$ linearly independent and satisfying (130)–(132), for $i = 3$ there exist three vectors $\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \in \boldsymbol{Z}^k$ linearly independent and satisfying (133)–(137), for $i = 4$ there exist four vectors $\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4 \in \boldsymbol{Z}^k$ linearly independent and satisfying (138), (139). We shall estimate $\operatorname{card} S_i(N)$ for $i = 1, 2, 3, 4$ successively. The number of integer vectors $\boldsymbol{n}$ satisfying $h(\boldsymbol{n}) \leqslant N$ and (128), (129) with $\gamma_i \neq 0$, $\gamma_{i+1} = \gamma_{i+2} = \ldots = \gamma_k = 0$ does not exceed

$$2c_{42}(P, Q)(2c_{42}(P, Q)+1)^{i-1}(2N+1)^{k-1},$$

since the coordinates n_j for $j \neq i$ can be chosen in at most $2N+1$ ways each and then n_i in at most $2c_{42}(P, Q)(2c_{42}(P, Q)+1)^{i-1}$ ways. Hence

$$\operatorname{card} S_1(N) \leqslant \sum_{i=1}^{k} 2c_{42}(P, Q)(2c_{42}(P, Q)+1)^{i-1}(2N+1)^{k-1} \leqslant c_{47}(P, Q)N^{k-1}. \tag{152}$$

The number of integer vectors $\boldsymbol{n}$ satisfying $h(\boldsymbol{n}) \leqslant N$ and (132) for fixed $\boldsymbol{l}_1, \boldsymbol{l}_2$ does not exceed $(2N+1)^{k-2} \operatorname{card} T(\boldsymbol{l}_1, \boldsymbol{l}_2)$, where

$$T(\boldsymbol{l}_1, \boldsymbol{l}_2) = \{[\lambda_1, \lambda_2] \in \boldsymbol{Z}^2 \colon \ \forall_{i=1,2} \ |\lambda_i| \leqslant kh(\boldsymbol{l}_i)N;$$
$$\max_{1 \leqslant i \leqslant 2} |\lambda_i| \leqslant 2\sqrt{2}k|P||Q|N^{(k-2)/(2k-2)}(\lambda_1, \lambda_2)\}.$$

Indeed, since $\boldsymbol{l}_1, \boldsymbol{l}_2$ are linearly independent there exists a set $\boldsymbol{H} \subset \{1, 2, \ldots, k\}$ such that $\operatorname{card} \boldsymbol{H} = k-2$ and $\boldsymbol{l}_1\boldsymbol{n}, \boldsymbol{l}_2\boldsymbol{n}, n_h\ (h \in \boldsymbol{H})$ determine uniquely $\boldsymbol{n}$. Now, for each $h \in \boldsymbol{H}$, n_h can be chosen in $2N+1$ ways.

Thus we obtain

$$\operatorname{card} S_2(N) \leqslant (2N+1)^{k-2} \sum_{\langle \boldsymbol{l}_1, \boldsymbol{l}_2 \rangle}^{*} \operatorname{card} T(\boldsymbol{l}_1, \boldsymbol{l}_2),$$

where the sum $\sum^{*}$ is taken over all pairs $\langle \boldsymbol{l}_1, \boldsymbol{l}_2 \rangle$ satisfying (130) and (131). On the other hand, by Lemma 6 of [11] applied with $r = 2$, $A = 2k|P||Q|N$, $B = 2\sqrt{2}k|P||Q|N^{(k-2)/(2k-2)}$ we have

$$\operatorname{card} T(\boldsymbol{l}_1, \boldsymbol{l}_2) \leqslant 1 + 2kh(\boldsymbol{l}_1)N + 2kh(\boldsymbol{l}_2)N + 4 \cdot 2AB$$
$$\leqslant 1 + 2k\min\{|P|, |Q|\}N + 4k|P||Q|N + 32\sqrt{2}k^2|P|^2|Q|^2N^{(3k-4)/(2k-2)}.$$

The sum $1 + 2kh(\boldsymbol{l}_1)N + 2kh(\boldsymbol{l}_2)N$ is the number of vectors $[\lambda_1, \lambda_2]$ with at least one coordinate 0 and the factor 4 in front of $2AB$ reflects the fact that λ_1, λ_2 may be either positive or negative. It follows that

$$\operatorname{card} S_2(N) \leqslant (2N+1)^{k-2}(1 + 2k\min\{|P|, |Q|\} + 4k|P||Q| + 32\sqrt{2}k^2|P|^2|Q|^2)N^{(3k-4)/(2k-2)} \sum_{\langle \boldsymbol{l}_1, \boldsymbol{l}_2 \rangle}^{*} 1 \leqslant c_{48}(P, Q)N^{k-k/(2k-2)}. \tag{153}$$

The number of integer vectors $\boldsymbol{n} \in \boldsymbol{Z}^k$ satisfying $h(\boldsymbol{n}) \leqslant N$ and (136), (137) for fixed $\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3$ does not exceed $(2N+1)^{k-3} \operatorname{card} \boldsymbol{U}$, where

$$\boldsymbol{U} = \Big\{[\varrho_1, \varrho_2, \varrho_3] \in \boldsymbol{Z}^3 \colon \forall_{i \leqslant 2} \ |\varrho_i| \leqslant c_{42+i}(P, Q)N^{(k-2)/(k-1)}\left(\frac{\log N}{\log\log N}\right)^3,$$
$$|\varrho_3| \leqslant c_{45}(P, Q)N^{(k-2)/(k-1)}\frac{(\log N)^4}{(\log\log N)^3}\Big\}.$$

Indeed, since $\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3$ are linearly independent there exists a set $\boldsymbol{I} \subset \{1, 2, \ldots, k\}$ such that $\operatorname{card} \boldsymbol{I} = k-3$ and $\boldsymbol{r}_1\boldsymbol{n}, \boldsymbol{r}_2\boldsymbol{n}, \boldsymbol{r}_3\boldsymbol{n}$ and n_i $(i \in \boldsymbol{I})$ determine uniquely $\boldsymbol{n}$. Now, for each $i \in \boldsymbol{I}$, n_i can be chosen in $2N+1$ ways. Thus we obtain

$$\operatorname{card} S_3(N) \leqslant (2N+1)^{k-3} \sum_{\langle \boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \rangle}^{**} \operatorname{card} \boldsymbol{U},$$

where the sum $\sum^{**}$ is taken over all triples $\langle \boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \rangle$ satisfying (133)–(135). On the other hand, clearly

$$\operatorname{card} \boldsymbol{U} \leqslant \prod_{i=1}^{2}\left(1 + 2c_{42+i}(P, Q)N^{(k-2)/(k-1)}\left(\frac{\log N}{\log\log N}\right)^3\right) \times \left(1 + 2c_{45}(P, Q)N^{(k-2)/(k-1)}\frac{(\log N)^4}{(\log\log N)^3}\right).$$

It follows that

$$\operatorname{card} S_3(N) \leqslant c_{49}(P, Q)N^{k-\frac{3}{k-1}}\frac{(\log N)^{10}}{(\log\log N)^9}. \tag{154}$$

The number of integer vectors $\boldsymbol{n}$ satisfying $h(\boldsymbol{n}) \leqslant N$ and (138), (139) for fixed $\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4$ does not exceed

$$(2N+1)^{k-4} \operatorname{card} V(\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4),$$

where

$$V(\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4) = \{[\mu_1, \mu_2, \mu_3, \mu_4] \in \boldsymbol{Z}^4 \colon \ \forall_{i \leqslant 4} \ |\mu_i| \leqslant kh(\boldsymbol{m}_i)N;$$
$$\max_{1 \leqslant i \leqslant 4} |\mu_i| \leqslant 8k\max\{|P|, |Q|\}N^{(k-2)/(k-1)}(\mu_1, \mu_2, \mu_3, \mu_4)\}.$$

Indeed, since $\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4$ are linearly independent there exists a set $\boldsymbol{J} \subset \{1, \ldots, k\}$ such that $\operatorname{card} \boldsymbol{J} = k-4$ and $\boldsymbol{m}_1\boldsymbol{n}, \boldsymbol{m}_2\boldsymbol{n}, \boldsymbol{m}_3\boldsymbol{n}, \boldsymbol{m}_4\boldsymbol{n}$ and n_j $(j \in \boldsymbol{J})$ determine uniquely $\boldsymbol{n}$. Now, for each $j \in \boldsymbol{J}$, n_j can be chosen in $2N+1$ ways. Thus we obtain

$$\operatorname{card} S_4(N) \leqslant (2N+1)^{k-4} \sum_{\langle \boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4 \rangle}^{***} \operatorname{card} V(\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4),$$

where the sum $\sum^{***}$ is taken over all quadruples $\langle \boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4\rangle$ satisfying (138). On the other hand, by Lemma 6 of [12] applied with $r = 4$, $A = 4k\max\{|P|,|Q|\}N$, $B = 8k\max\{|P|,|Q|\}N^{(k-2)/(k-1)}$ we have

$$\operatorname{card} V(\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4) \leqslant \prod_{i=1}^{4}(2kh(\boldsymbol{m}_i)N+1) - \prod_{i=1}^{4}(2kh(\boldsymbol{m}_i)N) + 16\cdot 2AB^3$$
$$\leqslant 929k^3(\max\{|P|,|Q|\})^3N^3 + 65536k^4(\max\{|P|,|Q|\})^4 N^{(4k-7)/(k-1)}.$$

The expression $\prod_{i=1}^{4}(2kh(\boldsymbol{m}_i)N+1) - \prod_{i=1}^{4}(2kh(\boldsymbol{m}_i)N)$ estimates the number of vectors $[\mu_1, \mu_2, \mu_3, \mu_4]$ with at least one coordinate 0 and the factor 16 in front of $2AB^3$ reflects the fact that $\mu_1, \mu_2, \mu_3, \mu_4$ may be either positive or negative. It follows that

(155) $$\operatorname{card} S_4(N) \leqslant (2N+1)^{k-4}(929k^3(\max\{|P|,|Q|\})^3 + 65536k^4(\max\{P,Q\})^4) \times N^{(4k-7)/(k-1)} \sum_{\langle \boldsymbol{m}_1,\boldsymbol{m}_2,\boldsymbol{m}_3,\boldsymbol{m}_4\rangle}^{***} 1 \leqslant c_{50}(P,Q)N^{k-\frac{3}{k-1}}.$$

The inequalities (151)–(155) imply

$$\operatorname{card} S_0(N) \leqslant c_{48}N^{k-\frac{k}{2k-2}} + (c_{47}+c_{49}+c_{50})N^{k-\frac{3}{k-1}}\frac{(\log N)^{10}}{(\log\log N)^9},$$

hence

$$\operatorname{card} S_0(N) \leqslant c_{51}(P,Q)N^{k-\frac{\min(k,6)}{2k-2}}\frac{(\log N)^{10}}{(\log\log N)^9},$$

where the logarithmic factors can be omitted for $k<6$, and by (150)

$$\operatorname{card} S(P,Q,N) \leqslant c_1(P,Q)N^{k-\frac{\min(k,6)}{2k-2}}\frac{(\log N)^{10}}{(\log\log N)^9}$$

with the similar proviso, provided

$$c_2(P,Q) = c_{51}(P,Q)\zeta\left(k-\frac{\min\{k,6\}}{2k-2}\right).$$

Lemma 16. *Let an integer $k \geqslant 4$ and a field $\boldsymbol{K}\subset \boldsymbol{C}$ be given. If Theorem 2 holds for all $P,Q\in \boldsymbol{K}[x_1,\ldots,x_k]$, $(P,Q)=1$ then for every finite subset $\boldsymbol{S}$ of $\boldsymbol{K}[x_1,\ldots,x_k]$ such that*

(156) $$\underset{F\in S}{\text{g.c.d.}}\, F = 1,$$

the number of vectors $\boldsymbol{n}\in \boldsymbol{Z}^k$ such that $h(\boldsymbol{n})\leqslant N$ and

(157) $$\underset{F\in S}{\text{g.c.d.}}\, KF(x^{n_1}, x^{n_2},\ldots,x^{n_k}) \neq 1$$

does not exceed

$$c_{52}(S)N^{k-\frac{\min(k,6)}{2k-2}}\frac{(\log N)^{10}}{(\log\log N)^9},$$

where for $k<6$ the logarithmic factors can be omitted.

Proof is similar to that of Lemma 12. We choose an $F_0\in \boldsymbol{S}$, $F_0\neq 0$ and write

$$F_0 \underset{K}{\overset{\text{can}}{=}} \text{const}\prod_{\sigma=1}^{s}P_\sigma^{e_\sigma}.$$

For every index $\sigma\leqslant s$ there exists a polynomial $F_\sigma\in \boldsymbol{S}$ such that $(P_\sigma, F_\sigma) = 1$. It suffices to take

$$c_{52}(S) = \max_{\sigma\leqslant s} c_2(P_\sigma, F_\sigma).$$

Proof of Theorem 2. We shall proceed by induction on the transcendence degree r of $\boldsymbol{K}_0$, the field generated by the coefficients of P and Q over $\boldsymbol{Q}$.

If $r=0$ the theorem is contained in Lemma 15. Let us consider the case, where $\operatorname{tr.deg.} \boldsymbol{K}_0/\boldsymbol{Q} = r\geqslant 1$ assuming that the theorem holds, whenever $\operatorname{tr.deg.}\boldsymbol{K}_0/\boldsymbol{Q} < r$. Let $t_1,\ldots,t_r$ be a transcendence basis of $\boldsymbol{K}_0$ over $\boldsymbol{Q}$ so that $[\boldsymbol{K}_0:\boldsymbol{Q}(t_1,\ldots,t_r)] < \infty$. Let us put $\boldsymbol{\Omega} = \boldsymbol{Q}(t_1,\ldots,t_{r-1})$ and let $b_1,\ldots,b_s$ be a basis of $\boldsymbol{K}_0\hat{\boldsymbol{\Omega}}(t_r)$ over $\hat{\boldsymbol{\Omega}}(t_r)$, $\hat{\boldsymbol{\Omega}}$ being the algebraic closure of $\boldsymbol{\Omega}$. We have as in the proof of Theorem 1, for suitable polynomials $D\in\hat{\boldsymbol{\Omega}}[t_r]$, $P_{\sigma i}$, $Q_{\sigma j}\in\hat{\boldsymbol{\Omega}}[x_1,\ldots,x_k]$ $(1\leqslant\sigma\leqslant s,\ 0\leqslant i\leqslant p,\ 0\leqslant j\leqslant q)$

$$P = D^{-1}\sum_{\sigma=1}^{s}\sum_{i=0}^{p}P_{\sigma i}t_r^i b_\sigma, \quad Q = D^{-1}\sum_{\sigma=1}^{s}\sum_{j=0}^{q}Q_{\sigma j}t_r^j b_\sigma.$$

Let

$$S = \bigcup_{\sigma=1}^{s}\bigcup_{i=0}^{p}\{P_{\sigma i}\}\cup\bigcup_{\sigma=1}^{s}\bigcup_{j=0}^{q}\{Q_{\sigma j}\}.$$

Since $(P,Q)=1$ we have

$$\underset{F\in S}{\text{g.c.d.}}\, F = 1.$$

Let $S_5(N), S_6(N)$ be the set of vectors $\boldsymbol{n}\in\boldsymbol{Z}^k$ such that $h(\boldsymbol{n})\leqslant N$ and $KP(x^{n_1},\ldots,x^{n_k})$, $KQ(x^{n_1},\ldots,x^{n_k})$ have a common zero ξ satisfying $\xi\in\hat{\boldsymbol{\Omega}}$ or $\xi\notin\hat{\boldsymbol{\Omega}}$, respectively.

For $\boldsymbol{n}\in S_5(N)$, since $t_r^i b_\sigma$ $(1\leqslant\sigma\leqslant s,\ i=0,1,\ldots)$ are linearly independent over $\hat{\boldsymbol{\Omega}}$ we obtain

$$P_{\sigma i}(\xi^{n_1},\ldots,\xi^{n_k}) = 0,\quad Q_{\sigma j}(\xi^{n_1},\ldots,\xi^{n_k}) = 0\ (1\leqslant\sigma\leqslant s,\ 0\leqslant i\leqslant p,\ 0\leqslant j\leqslant q)$$

and since ξ is neither 0 nor a root of unity

$$\underset{F\in S}{\text{g.c.d.}}\, KF(x^{n_1},\ldots,x^{n_k}) \neq 1.$$

Since tr. deg. $\hat{\Omega}/Q = r-1$ the inductive assumption implies by virtue of Lemma 16 that

$$\operatorname{card} S_5(N) \leqslant c_{52}(S) N^{k-\frac{\min(k,6)}{2k-2}} \frac{(\log N)^{10}}{(\log\log N)^9},$$

where for $k < 6$ the logarithmic factors can be omitted.

On the other hand $\Omega \subset K_0$ and tr. deg. $K_0/\Omega = 1$, thus if $n \in S_6(N)$ Lemma 10 implies the existence of a vector $\gamma \in Z^k$ such that

$$0 < h(\gamma) \leqslant c_{33}(P, Q, \Omega) \quad \text{and} \quad \gamma n = 0.$$

By the argument used in the proof of Lemma 15 to estimate card $S_1(N)$ it follows that

$$\operatorname{card} S_6(N) \leqslant c_{53}(P, Q, \Omega) N^{k-1},$$

$$\operatorname{card}(S_5(N) \cup S_6(N)) \leqslant (c_{52}(S) + c_{53}(P, Q, \Omega)) N^{k-\frac{\min(k,6)}{2k-2}},$$

where for $k < 6$ the logarithmic factors can be omitted.

The constants $c_{52}(S)$ and $c_{33}(P, Q, \Omega)$ depend upon the choice of the transcendence basis $t_1, \ldots, t_r$ and the choice of the linear basis $b_1, \ldots, b_s$. Since this choice is arbitrary we put

$$c_2(P, Q) = \inf(c_{52}(S) + c_{33}(P, Q, \Omega)),$$

where the infimum is taken over all possible bases $t_1, \ldots, t_r$ and $b_1, \ldots, b_s$. The inductive proof is complete.

4. Proofs of Theorems 3 and 4.

LEMMA 17. *If $F \in Q[x_1, \ldots, x_k]$ is irreducible and non-reciprocal and an integral matrix $M = [\mu_{ij}]$ of order k is non-singular then*

$$(158) \qquad LF\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big) = JF\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big)$$

and the above polynomial is squarefree.

Proof. The fact that the polynomial on the left-hand side is squarefree is proved in the remark after Lemma 12 of [9]. If the equality (158) were false there would be an irreducible reciprocal polynomial $G \in Q[y_1, \ldots, y_k]$ such that

$$G \,|\, JF\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big),$$

hence

$$\Big(JF\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big), JF\Big(\prod_{i=1}^{k} y_i^{-\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{-\mu_{ik}}\Big)\Big) \neq 1.$$

Let $|M|M^{-1} = [\mu'_{ij}]$. By the substitution

$$y_i = \prod_{j=1}^{k} x_j^{\mu'_{ij}},$$

we obtain

$$(JF(x_1^{|M|}, x_2^{|M|}, \ldots, x_k^{|M|}), JF(x_1^{-|M|}, x_2^{-|M|}, \ldots, x_k^{-|M|})) \neq 1$$

and by Lemma 9 of [10]

$$(JF(x_1, x_2, \ldots, x_k), JF(x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1})) \neq 1$$

contrary to the assumption about F.

Proof of Theorem 3. By Lemma 12 of [9] either $F(x^{n_1}, x^{n_2}, x^{n_3}) = 0$ or there exist an integral square matrix $M = [\mu_{ij}]$ of order 3 and a vector $v = [v_1, v_2, v_3] \in Z^3$ satisfying (3) and such that

$$(159) \qquad LF\Big(\prod_{i=1}^{3} y_i^{\mu_{i1}}, \prod_{i=1}^{3} y_i^{\mu_{i2}}, \prod_{i=1}^{3} y_i^{\mu_{i3}}\Big) \stackrel{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, y_2, y_3)^{e_\sigma}$$

implies

$$LF(x^{n_1}, x^{n_2}, x^{n_3}) \stackrel{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} LF(x^{v_1}, x^{v_2}, x^{v_3})^{e_\sigma}$$

or there exists a vector $\gamma \in Z^3$ such that $\gamma n = 0$ and

$$0 < h(\gamma) < c_{53}(F),$$

where $c_{53}(F)$ is an explicitly given constant.

In the first case the relation $\gamma n = 0$ holds for a suitable $\gamma \in Z^3$ such that $0 < h(\gamma) \leqslant |F|$, thus in the first and third case the assertion of Theorem 3 holds provided

$$c_3(F) \geqslant \max\{|F|, c_{53}(F)\}.$$

In the second case, by virtue of Lemma 17, the left-hand side of (4_1) coincides with the left-hand side of (159) and $e_\sigma = 1$ for all $\sigma \leqslant s$. Hence the assertion of Theorem 3 holds provided

$$KF(x^{n_1}, x^{n_2}, x^{n_3}) = LF(x^{n_1}, x^{n_2}, x^{n_3}).$$

If the above equality does not hold, $KF(x^{n_1}, x^{n_2}, x^{n_3})$ has a reciprocal factor and thus

$$(KF(x^{n_1}, x^{n_2}, x^{n_3}), KF(x^{-n_1}, x^{-n_2}, x^{-n_3})) \neq 1.$$

Let us put in Theorem 1

$$P = F(x_1, x_2, x_3), \quad Q = JF(x_1^{-1}, x_2^{-1}, x_3^{-1}).$$

By the assumptions about F we have $(P,Q)=1$, hence the assumptions of Theorem 1 are satisfied and by virtue of that theorem there exists a vector $\gamma\in\mathbf{Z}^3$ such that $\gamma\mathbf{n}=0$ and

$$0<h(\gamma)\leqslant c_1(P,Q).$$

Therefore, Theorem 3 holds with

$$c_3(F)=\max\{|F|,\ c_{53}(F),\ c_1(P,Q)\}.$$

LEMMA 18. *Let $F\in\mathbf{Q}[x_1,\ldots,x_k]$, $KF\notin\mathbf{Q}$. If $\mathbf{n}\in\mathbf{Z}^k$ and $KF(x^{n_1},\ldots,x^{n_k})\in\mathbf{Q}$ then there exists a vector $\gamma\in\mathbf{Z}^k$ such that $\gamma\mathbf{n}=0$,*

$$0<h(\gamma)\leqslant c_{54}(F).$$

Proof. Since $KF\notin\mathbf{Q}$, F has at least one irreducible factor $F_1\in\mathbf{Z}[x_1,\ldots,x_k]$ which is not an extended cyclotomic polynomial in the sense of [5].

By virtue of Lemma 3 of [5] applied with $\mathbf{r}=\mathbf{n}$ either

$$\deg KF_1(x^{n_1},x^{n_2},\ldots,x^{n_k})\geqslant\tfrac12\deg JF_1(x^{n_1},x^{n_2},\ldots,x^{n_k})$$

or there exists a vector $\gamma\in\mathbf{Z}^k$ such that $\gamma\mathbf{n}=0$ and

$$0\leqslant h(\gamma)<2|F_1|j^5\prod_{p\leqslant j}p,$$

where j is the number of non-zero coefficients of F_1. In the former case either $KF_1(x^{n_1},\ldots,x^{n_k})\notin\mathbf{Q}$, hence $KF(x^{n_1},\ldots,x^{n_k})\in\mathbf{Q}$, or $JF_1(x^{n_1},\ldots,x^{n_k})\in\mathbf{Q}$, hence a vector γ with the above properties exists again. Since $|F_1|\leqslant|F|$, j is bounded in terms of F, the lemma follows.

LEMMA 19. *For every polynomial $F\in\mathbf{Z}[x_1,x_2,x_3]$ there exists a number $c_{55}(F)$ with the following property. For every vector $\mathbf{n}\in\mathbf{Z}^3$ there exists an integral square matrix $\mathbf{M}=[\mu_{ij}]$ of order 3 and a vector $\mathbf{v}\in\mathbf{Z}^3$ such that (3) holds and either $JF(x^{n_1},x^{n_2},x^{n_3})$ is reciprocal or $KF(x^{n_1},x^{n_2},x^{n_3})$ is irreducible or*

$$KF\Big(\prod_{i=1}^{3}y_i^{\mu_{i1}},\ \prod_{i=1}^{3}y_i^{\mu_{i2}},\ \prod_{i=1}^{3}y_i^{\mu_{i3}}\Big)=\prod_{i=1}^{2}G_i(y_1,y_2,y_3),\tag{160}$$

$$G_i\in\mathbf{Z}[y_1,y_2,y_3]$$

and

$$KG_i(x^{v_1},x^{v_2},x^{v_3})\notin\mathbf{Z}\quad(i=1,2),\tag{161}$$

or there exists a vector $\gamma\in\mathbf{Z}^3$ such that $\gamma\mathbf{n}=0$ and

$$0<h(\gamma)\leqslant c_{55}(F).$$

Proof. If JF is reciprocal then $JF(x^{n_1},x^{n_2},x^{n_3})$ is reciprocal and the lemma holds with $\mathbf{M}$ equal to the identity matrix, $\mathbf{v}=\mathbf{n}$. If JF is not reciprocal and KF is irreducible Theorem 3 applies to the polynomial $F_0=KF$. By virtue of that theorem there exist a matrix $\mathbf{M}$ and a vector $\mathbf{v}$ satisfying (3), and such that either (4_1) with F replaced by F_0 implies (4_2), or there exists a $\gamma_1\in\mathbf{Z}^3$ such that $\gamma_1\mathbf{n}=0$ and

$$0<h(\gamma_1)\leqslant c_3(KF).\tag{162}$$

In the former case if on the right-hand side of (4_1) we have just one factor ($s=1$) then by (4_2) $KF(x^{n_1},x^{n_2},x^{n_3})$ is irreducible, hence the lemma holds. If on the right-hand side of (4_2) we have $s\geqslant2$ factors then for a suitable choice of G_1,G_2 we have (160) and (161) unless for a $\sigma\leqslant s$

$$KF_\sigma(x^{v_1},x^{v_2},x^{v_3})\in\mathbf{Z};\tag{163}$$

However by Lemma 18 (163) implies the existence of a vector $\gamma_0\in\mathbf{Z}^3$ such that $\gamma_0\mathbf{v}=0$ and $0<h(\gamma_0)\leqslant c_{54}(F_\sigma)$. Since, by ($3_1$) $\mathbf{M}$ is taken from a finite set depending only on F and to each $\mathbf{M}$ there correspond only finitely many primitive $F_\sigma\in\mathbf{Z}[x_1,x_2,x_3]$ (it suffices to consider only these), we obtain

$$0<h(\gamma_0)\leqslant c_{56}(F).$$

Taking $\gamma_2=\gamma_0\mathbf{M}^{\mathrm{a}}$, where $\mathbf{M}^{\mathrm{a}}$ is the matrix adjoint to $\mathbf{M}$, we obtain from (3_2) $\gamma_2\mathbf{n}=0$ and from (3_1)

$$0<h(\gamma)\leqslant3h(\gamma_0)h(\mathbf{M}^{\mathrm{a}})\leqslant6h(\gamma_0)h(\mathbf{M})^2\leqslant6c_{56}(F)\exp27\cdot2^{\|F\|-4}=c_{57}(F).\tag{164}$$

If JF is not reciprocal and KF is reducible we take $\mathbf{M}$ equal to the identity matrix, $\mathbf{v}=\mathbf{n}$. We have

$$KF=G_1G_2,$$

where

$$G_i\in\mathbf{Z}[y_1,y_2,y_3]\backslash\mathbf{Z}\quad(i=1,2).$$

If $KG_i(x^{n_1},x^{n_2},x^{n_3})\notin\mathbf{Z}$ $(i=1,2)$ (160) and (161) hold. Otherwise, for an $i\leqslant2$

$$KG_i(x^{n_1},x^{n_2},x^{n_3})\in\mathbf{Z}.$$

By Lemma 18 there exists a vector $\gamma_3\in\mathbf{Z}^3$ such that $\gamma_3\mathbf{n}=0$ and

$$0<h(\gamma_3)\leqslant\max_{G|KF}c_{54}(G),\tag{165}$$

where the maximum is taken over all primitive polynomials $G\in\mathbf{Z}[y_1,y_2,y_3]\backslash\mathbf{Z}$ dividing KF. Therefore, by (162), (164) and (165) the lemma holds with $c_{55}(F)=0$ if JF is reciprocal, $c_{55}(F)=\max\{c_3(KF),c_{57}(F),\max_{G|KF}c_{54}(G)\}$, otherwise.

LEMMA 20. *An analogue of Theorem 4 holds for polynomials $F\in\mathbf{Z}[x_1,x_2]$ with $c_4(r,F)$ replaced by a suitable $c_{58}(r,F)\geqslant1$ $(r=1,2)$.*

Proof. The analogue of the condition for reducibility given in Theorem 4 is clearly sufficient. We proceed to prove that it is necessary assuming that

$KF(x^{n_1}, x^{n_2})$ is reducible; the value of $c_{58}(r, F)$ will be given later. If $KF = LF$ then by virtue of Theorem 3 of [9] there exist an integral matrix $N = [\nu_{ij}]_{i \leqslant 2, j \leqslant r}$ of rank $r \leqslant 2$ and a vector $\boldsymbol{v} = [v_1, v_r] \in \boldsymbol{Z}^r$ such that

$$h(N) \leqslant c_{59}(r, F), \qquad \boldsymbol{n} = \boldsymbol{n}\boldsymbol{v}$$

and

$$KF\Big(\prod_{i=1}^{r} y_i^{\nu_{i1}}, \prod_{i=1}^{r} y_i^{\nu_{i2}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, y_r)^{e_\sigma}$$

implies

$$KF(x^{n_1}, x^{n_2}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} KF_\sigma(x^{v_1}, x^{v_r})^{e_\sigma}.$$

The matrix N and the vector $\boldsymbol{v}$ have the required properties, provided

$$c_{58}(r, F) \geqslant c_{59}(r, F).$$

If $KF \neq LF$, and KF is irreducible, then KF is reciprocal, JF is reciprocal and $JF(x^{n_1}, x^{n_2})$ is reciprocal, contrary to the assumption. If $KF \neq LF$ and KF is reducible we have

$$KF = G_1 G_2, \qquad G_i \in \boldsymbol{Z}[y_1, y_2] \backslash \boldsymbol{Z} \quad (i = 1, 2).$$

If $KG_i(x^{n_1}, x^{n_2}) \notin \boldsymbol{Z}$ for $i = 1, 2$ the lemma holds with N equal to the identity matrix, $\boldsymbol{v} = \boldsymbol{n}$. Otherwise, for an $i \leqslant 2$

$$KG_i(x^{n_1}, x^{n_2}) = 1.$$

By Lemma 18 there exists a vector $\gamma \in \boldsymbol{Z}^2$ such that $\gamma \boldsymbol{n} = 0$ and

(166) $$0 < h(\gamma) \leqslant \max_{G|KF} c_{54}(G) = c_{60}(F),$$

where the maximum is taken over all primitive polynomials $G \in \boldsymbol{Z}[y_1, y_2] \backslash \boldsymbol{Z}$ dividing KF.

Let $\gamma = [\gamma_1, \gamma_2]$, where we assume without loss of generality that $(\gamma_1, \gamma_2) = 1$. We have then

$$n_1 = \gamma_2 n, \quad n_2 = -\gamma_1 n, \quad n \in \boldsymbol{Z}$$

and taking

(167) $$F_0(x) = JF(x^{\gamma_2}, x^{-\gamma_1})$$

we find

$$KF(x^{n_1}, x^{n_2}) = KF_0(x^n).$$

Now, by Theorem 1 of [9] if $KF_0(x^n)$ is reducible there exists a positive integer $\nu \leqslant c_{61}(F_0)$ such that $\nu | n$ and $KF_0(x^\nu)$ is reducible. In this case we take $r = 1$,

$$N = [\gamma_2 \nu, -\gamma_1 \nu], \qquad \boldsymbol{v} = [n/\nu]$$

and find

$$h(N) \leqslant h(\gamma)\nu \leqslant c_{60}(F) c_{61}(F_0).$$

However F_0 is uniquely determined by F and γ via (167) and by virtue of (166) γ runs through a finite set of vectors depending only on F. Hence

$$c_{61}(F_0) \leqslant c_{62}(F)$$

and the matrix N has the required properties, provided

$$c_{58}(1, F) \geqslant c_{60}(F) c_{62}(F).$$

Therefore, it suffices to take $c_{58}(2, F) = c_{59}(2, F)$, if $KF = LF$, 1 otherwise;

$$c_{58}(1, F) = \begin{cases} c_{59}(1, F) & \text{if } KF = LF, \\ c_{60}(F) c_{62}(F) & \text{otherwise.} \end{cases}$$

Proof of Theorem 4. The condition for reducibility given in Theorem 4 is clearly sufficient. We proceed to prove that it is necessary assuming that $KF(x^{n_1}, x^{n_2}, x^{n_3})$ is reducible; the value of $c_4(r, F)$ will be given later.

If the matrix $\boldsymbol{M}$ and the vector $\boldsymbol{v}$ appearing in Lemma 19 have the properties (160) and (161), we take $N = \boldsymbol{M}$, $r = 3$, $c_4(3, F) = \exp 27 \cdot 2^{\|F\| - 5}$.

Otherwise by the lemma in question there exists a vector $\gamma \in \boldsymbol{Z}^3$ such that $\gamma \boldsymbol{n} = 0$ and $0 < h(\gamma) \leqslant c_{55}(F)$.

Let Λ be the lattice consisting of all vectors $\boldsymbol{x} \in \boldsymbol{Z}^3$ such that $\boldsymbol{x}\gamma = 0$. We have $[\gamma_2, -\gamma_1, 0]$, $[\gamma_3, 0, -\gamma_1]$, $[0, \gamma_3, -\gamma_2] \in \Lambda$ and two among these vectors are linearly independent, hence by Lemma 6 of [9] there exists a basis $\boldsymbol{b}_1, \boldsymbol{b}_2$ of Λ such that

(168) $$h(\boldsymbol{b}_i) \leqslant i h(\gamma) \leqslant 2 c_{55}(F) \quad (i = 1, 2).$$

Let us put

(169) $$F_1 = JF(x_1^{b_{11}} x_2^{b_{21}}, x_1^{b_{12}} x_2^{b_{22}}, x_1^{b_{13}} x_2^{b_{23}}), \qquad \boldsymbol{B} = \begin{bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{bmatrix}.$$

Since $\boldsymbol{n} \in \Lambda$ we have $\boldsymbol{n} = \boldsymbol{m}\boldsymbol{B}$ for an $\boldsymbol{m} \in \boldsymbol{Z}^2$. Clearly

$$JF(x^{n_1}, x^{n_2}, x^{n_3}) = JF_1(x^{m_1}, x^{m_2}),$$

thus, by the assumption, $KF_1(x^{m_1}, x^{m_2})$ is reducible. Applying Lemma 20 we infer the existence of an integral matrix $N' = [\nu'_{ij}]_{i \leqslant 2, j \leqslant r}$ of rank $r \leqslant 2$ and of a vector $\boldsymbol{v} = [v_1, v_r] \in \boldsymbol{Z}^r$ such that

(170) $$h(N') \leqslant c_{58}(r, F_1),$$

(171) $$\boldsymbol{m} = \boldsymbol{v} N',$$

$$KF_1\Big(\prod_{i=1}^{r} y_i^{\nu'_{i1}}, \prod_{i=1}^{r} y_i^{\nu'_{i2}}\Big) = G_1 G_2, \qquad G_2 \in \boldsymbol{Z}[y_1, y_r] \quad (i = 1, 2)$$

and

$$KG_i(x^{v_1}, x^{v_r}) \notin \boldsymbol{Z} \quad (i = 1, 2).$$

Let us take $N = N'B$. It follows from (169) that

$$JF_1\Big(\prod_{i=1}^{r} y_i^{\nu'_{i1}}, \prod_{i=1}^{r} y_i^{\nu'_{i2}}\Big) = JF\Big(\prod_{i=1}^{r} y_i^{\nu_{i1}}, \prod_{i=1}^{r} y_i^{\nu_{i2}}, \prod_{i=1}^{r} y_i^{\nu_{i3}}\Big)$$

and from (171) that

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

moreover, since $\boldsymbol{B}$ is of rank 2, N is of rank r. Thus N and $\boldsymbol{v}$ have all properties required in the theorem apart from the inequality for $h(N)$ and it remains to establish that by an appropriate choice of $c_4(r, F)$.

We have by (168) and (170)

$$h(N) \leqslant 2h(N')h(\boldsymbol{B}) \leqslant 4c_{55}(\boldsymbol{F})c_{58}(r, F_1).$$

However, F_1 is determined by F and $\boldsymbol{B}$ via (169) and by virtue of (168) $\boldsymbol{B}$ runs through a finite set of matrices depending only on F. Hence

$$c_{58}(r, F_1) \leqslant c_{63}(r, F) \quad (r = 1, 2)$$

and the theorem holds with

$$c_4(3, F) = \exp 27 \cdot 2^{\|F\|-5},$$

$$c_4(r, F) = 4c_{35}(F)c_{63}(r, F) \quad (r = 1, 2).$$

5. Proofs of Theorems 5 and 6.

Proof of Theorem 5. Let $S(F)$ be the set of all vectors $\boldsymbol{n} \in \boldsymbol{Z}^k$ such that either

$$\big(KF(x^{n_1}, \ldots, x^{n_k}), KF(x^{-n_1}, \ldots, x^{-n_k})\big) \neq 1$$

or there exists a vector $\boldsymbol{\gamma} \in \boldsymbol{Z}^k$ satisfying $\boldsymbol{\gamma n} = 0$ and

$$0 < h(\boldsymbol{\gamma}) < \exp_{2k-4}(7k|F|^{*\|F\|-1}\log\|F\|),$$

where $|F|^* = \sqrt{\max(2,|F|)^2+2}$.

Let $\boldsymbol{T}(F)$ be the set of all vectors $\boldsymbol{n} \in \boldsymbol{Z}^k$ for which the second part of the above alternative holds and put

$$P = F(x_1, \ldots, x_k), \quad Q = JF(x_1^{-1}, \ldots, x_k^{-1}).$$

In the notation used in the proof of Lemma 15

$$\boldsymbol{S}(F) = \bigcup_{N=1}^{\infty} \boldsymbol{S}(P, Q; N) \cup \boldsymbol{T}(F),$$

hence, denoting by $[-N, N]$ the closed interval

$$\operatorname{card}(\boldsymbol{S}(F) \cap [-N, N]^k) \leqslant \operatorname{card} \boldsymbol{S}(P, Q; N) + \operatorname{card}(\boldsymbol{T}(F) \cap [-N, N]^k).$$

By Lemma 15 we have

$$\operatorname{card} \boldsymbol{S}(P, Q; N) \leqslant c_2(P, Q)N^{k-\frac{\min(k,6)}{2(k-1)}} \frac{(\log N)^{10}}{(\log\log N)^9},$$

where for $k < 6$ the logarithmic factors can be omitted.

Counting the elements of $\boldsymbol{T}(F)$ in the same way as elements of $\boldsymbol{S}_1(N)$ in the proof of Lemma 15 we obtain

$$\operatorname{card}(\boldsymbol{T}(F) \cap [-N, N]^k) \leqslant c_{56}(F)N^{k-1},$$

thus (i) follows.

If $\boldsymbol{n} \in \boldsymbol{Z}^k \setminus \boldsymbol{S}(F)$ then by Lemma 12 of [9] there exist an integral square matrix $M = [\mu_{ij}]$ of order k and a vector $\boldsymbol{v} \in \boldsymbol{Z}^k$ satisfying (5) and such that

$$LF\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big) \stackrel{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, \ldots, y_k)^{e_\sigma} \tag{172}$$

implies

$$LF(x^{n_1}, \ldots, x^{n_k}) \stackrel{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^{v_1}, \ldots, x^{v_k})^{e_\sigma}.$$

However, by Lemma 17 the left-hand side of (6_1) coincides with the left-hand side of (172) and $e_\sigma = 1$ for all $\sigma \leqslant s$, hence (6_1) implies (6_2) provided $KF(x^{n_1}, \ldots, x^{n_k}) = LF(x^{n_1}, \ldots, x^{n_k})$. Otherwise we have

$$\big(KF(x^{n_1}, \ldots, x^{n_k}), KF(x^{-n_1}, \ldots, x^{-n_k})\big) \neq 1;$$

thus $\boldsymbol{n} \in \boldsymbol{S}(F)$. The obtained contradiction proves (ii).

Proof of Theorem 6. Without loss of generality we may assume that $F_i \in \boldsymbol{Z}[x_1, \ldots, x_k]$ $(1 \leqslant i \leqslant h)$. By the assumption about S for $\varepsilon = \dfrac{\min\{k, 6\}}{3k(k-1)}$ there exists a number $c_{64}(k, S) > 0$ and infinitely many integers N such that

$$S(N) > c_{64}(k, S)N^{1-\varepsilon}.$$

Therefore, the number of vectors $\boldsymbol{n} \in S^k$ with $h(\boldsymbol{n}) \leqslant N$ exceeds

$$(c_{64}(k, S)N^{1-\varepsilon})^k > c_{64}(k, S)^k N^{(1-\varepsilon)k}.$$

The number of vectors $\boldsymbol{n} \in \boldsymbol{Z}^k \cap [-N, N]^k$ such that $\boldsymbol{n} \in \boldsymbol{S}(F_g)$ is by Theorem 5 less than

$$c_5(F_g)N^{k-\frac{\min(k,6)}{2(k-1)}} \frac{(\log N)^{10}}{(\log\log N)^9},$$

hence the number of vectors $\boldsymbol{n} \in \boldsymbol{Z}^k \cap [-N, N]^k$ such that $\boldsymbol{n} \in \bigcup_{j=1}^{h} \boldsymbol{S}(F_g)$ is

$$O\bigg(N^{k-\frac{\min(k,6)}{2(k-1)}} \frac{(\log N)^{10}}{(\log\log N)^9}\bigg).$$

However

$$\varepsilon k < \frac{\min\{k, 6\}}{2(k-1)},$$

hence for infinitely many integers N there exist more than $c_{65}(k, S)^{k-\varepsilon k} > 0$ vectors $\boldsymbol{n} \in \boldsymbol{Z}^k \cap [-N, N]^k \setminus \bigcup_{g=1}^{h} \boldsymbol{S}(F_g)$. By virtue of Theorem 5 for all these vectors and all $g \leqslant h$ the number Ω_g of irreducible factors of $KF_g(x^{n_1}, \ldots, x^{n_k})$ equals the number of irreducible factors of

(173) $$JF_g\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big)$$

for a suitable non-singular matrix $M_g = [\mu_{ij}]_{i,j\leqslant k}$ depending upon g.

If for some $g \leqslant h$ the polynomial (173) were reducible we would obtain by the substitution

$$y_i = \prod_{j=1}^{k} x_j^{\mu'_{ij}}, \quad [\mu'_{ij}] = |\det M_g| M_g^{-1}$$

the reducibility of

$$F_g(x_1^{|\det M_g|}, \ldots, x_k^{|\det M_g|}),$$

contrary to the assumption. Hence $\Omega_g = 1$ for all $g \leqslant h$ and the theorem follows.

6. Examples and comments. We shall give an example, announced in the introduction, of a polynomial $F \in \mathbf{Z}[x_1, x_2]$ which is non-reciprocal and irreducible, but $KF(x^{n_1}, x^{n_2})$ is reducible for all positive integers n_1, n_2. Take

$$F(x_1, x_2) = x_1^2 + x_2^2 - 2x_1x_2 - 2a^2x_1 - 2a^2x_2 + a^4,$$

where a is an integer $\geqslant 3$. F is not reciprocal and the only conceivable factorization of F over $\mathbf{Q}$ into two factors of positive degree would be

$$F(x_1, x_2) = (b(x_1 - x_2) + c)(b^{-1}(x_1 - x_2) + a^4c^{-1}), \qquad b, c \in \mathbf{Q},$$

whence it would follow $F(x, x) = a^4$, while $F(x, x) = -4a^2x + a^4$. Thus F is irreducible. On the other hand, if $n_i = 2m_i$ ($i = 1$ or 2) we have

$$F(x^{n_1}, x^{n_2}) = (x^{n_i} - x^{n_{3-i}} + a^2 + 2ax^{m_i})(x^{n_i} - x^{n_{3-i}} + a^2 - 2ax^{m_i}),$$

if $n_i = 2m_i + 1$ ($i = 1, 2$)

$$F(x^{n_1}, x^{n_2}) = (x^{n_1} + x^{n_2} - a^2 + 2x^{m_1+m_2+1})(x^{n_1} + x^{n_2} - a^2 - 2x^{m_1+m_2+1}).$$

The factors on the right-hand side have no root of unity as a zero, since $a^2 > 2a + 2$, thus $KF(x^{n_1}, x^{n_2})$ is reducible for all positive integers n_1, n_2.

In the special case of Theorem 6, where $F_g = \alpha_{g0} + \sum_{j=1}^{k} \alpha_{gj} x_j$ $(k > 1)$ it has been possible in [12] to extend the result to the situation, where $\alpha_{g0} \in \mathbf{Q}(\alpha_{g1}/\alpha_{g0}, \ldots, \alpha_{gk}/\alpha_{g0}) = \mathbf{K}_g$ and the irreducibility of $KF_g(x^{n_1}, \ldots, x^{n_k})$ is asserted over $\mathbf{K}_g$.

In general such extension is possible with a suitable modification of the notion of a reciprocal polynomial (cf. [13]) if, for all d, $F_g(x_1^d, \ldots, x_k^d)$ is irreducible over the normal closure over $\mathbf{Q}$ of the field $\mathbf{K}_g$, generated by the ratios of the coefficients of F_g. In particular, if $\mathbf{K}_g$ is normal over $\mathbf{Q}$ and the notion of a reciprocal polynomial is suitably redefined the theorem as it stands

extends to the reducibility over $\mathbf{K}_g$. Indeed, then the norm $N_{\mathbf{K}_g/\mathbf{Q}} F_g(x_1^d, \ldots, x_k^d)$ is for all d irreducible over $\mathbf{Q}$ and to obtain the irreducibility of $KF_g(x^{n_1}, \ldots, x^{n_k})$ over $\mathbf{K}_g$ it suffices to apply Theorem 6 to $N_{\mathbf{K}_g/\mathbf{Q}} F_g$, provided this polynomial is not reciprocal in the usual sense $(1 \leqslant g \leqslant h)$.

However if $\mathbf{K}_1$ is not a normal extension of $\mathbf{Q}$, the polynomial $N_{\mathbf{K}_1/\mathbf{Q}} F_1$ is not necessarily irreducible, it is up to a constant factor a power of an irreducible polynomial F_0. It could seem that, if $F_0(x_1^d, \ldots, x_k^d)$ is irreducible for all positive integers d and non-reciprocal, then by choosing $n_1, \ldots, n_k$ so that $KF_0(x^{n_1}, \ldots, x^{n_k})$ is irreducible over $\mathbf{Q}$ we may achieve the irreducibility of $KF_1(x^{n_1}, \ldots, x^{n_k})$ over $\mathbf{K}_1$. This is, however, not the case, even for $k = 1$. Take

$$F_1 = x^2 - 3\sqrt[3]{p^2}\,x + 9\sqrt[3]{p^4}, \qquad \text{where } p \text{ is a prime.}$$

We have $\mathbf{K}_1 = \mathbf{Q}(\sqrt[3]{p})$,

$$N_{\mathbf{K}_1/\mathbf{Q}} F_1 = (x^3 - 27p^2)^2 = F_0^2.$$

The polynomial $F_0(x^d) = KF_0(x^d)$ is irreducible for every positive integer d, but

$$F_1(x^2) = x^4 - 3\sqrt[3]{p^2}\,x^2 + 9\sqrt[3]{p^4} = (x^2 - 3\sqrt[3]{p}\,x + 3\sqrt[3]{p^2})(x^2 + 3\sqrt[3]{p}\,x + 3\sqrt[3]{p^2})$$

and, since the factors on the right-hand side have no root of unity as a zero, $KF_1(x^2)$ is reducible over $\mathbf{K}_1$.

It is possible to extend Theorem 6 in a different manner, replacing the rational field by any totally real field or any totally complex quadratic extension of a totally real field, or by a purely transcendental extension of one of such fields. However, these generalizations are not automatical and we postpone them to a later work.

Note concerning the paper [11]. The following two corrections are needed

1. p. 316. The argument given to show that $D(\xi^{v_0}) = 0$ is impossible works only if $v_0 \neq 0$. If $v_0 = 0$ we have

$$u_0 = \pm 1, \quad h(\mathbf{p}) = h(\mathbf{n}) = n_k \geqslant k > 1.$$

Hence, by (9) $k \geqslant 3$ and (5) holds with $\{g, h, i, j\} = \{0, 1, 2, 3\}$.

2. p. 329. The formula (47) should read

$$\mathbf{T} \subset \bigcup_{d=1}^{N/2} \bigcup_{\nu=1}^{7} d\,\mathbf{S}_\nu\Big(\frac{N}{d}\Big),$$

where for a set $\mathbf{S}$: $d\mathbf{S} = \{d\mathbf{x} \colon \mathbf{x} \in \mathbf{S}\}$.

Note added in proof. Theorem 1 admits the following extension.

THEOREM 7. *Let $\mathbf{K}$ be any field and V an algebraic variety of dimension $\leqslant 1$ in the affine space $A_k(\mathbf{K})$. For $k \geqslant 3$ there exists a number $c(V)$ with the following property. If $\mathbf{n} \in \mathbf{Z}^k$, $\xi \in \mathbf{K}^*$, $(\xi^{n_1}, \ldots, \xi^{n_k}) \in V$ then either $\xi^q = 1$ for a suitable integer $q > 0$ or there exist an integral matrix $\mathbf{M}$ of size $2 \times k$, rank 2 and a vector $\mathbf{v} \in \mathbf{Z}^2$ such that*

$$h(\mathbf{M}) \leqslant c(V) \quad \text{and} \quad \mathbf{n} = \mathbf{v}\mathbf{M}.$$

Proof by induction on k. For $k = 3$ the theorem follows from Theorem 1 and Lemma 12. Indeed if ξ is not a root of unity we take in the latter for $\mathbf{S}$ the set of polynomials defining

V and infer the existence of a vector $\gamma \in \mathbf{Z}^3$ such that

$$0 < h(\gamma) < c_{39}(S) \quad \text{and} \quad \gamma \mathbf{n} = 0.$$

The lattice Λ of vectors perpendicular to γ has a basis $\mathbf{m}_1, \mathbf{m}_2$ satisfying

$$h(\mathbf{m}_i) \leqslant ih(\gamma) \leqslant 2c_{39}(S)$$

(cf. the proof of (168)). Since $\mathbf{n} \in \Lambda$ we have $\mathbf{n} = v_1\mathbf{m}_1 + v_2\mathbf{m}_2, v_i \in \mathbf{Z}$.

We take

$$c(V) = 2c_{39}(S), \quad M = \begin{bmatrix} \mathbf{m}_1 \\ \mathbf{m}_2 \end{bmatrix}, \quad \mathbf{v} = [v_1, v_2],$$

Assume now that $k > 3$, the theorem holds for all algebraic varieties of dimension $\leqslant 1$ in $A_{k-1}(K)$ and consider such a variety V in $A_k(K)$ and $\xi \in K^*$ different from roots of unity such that

$$(\xi^{n_1}, \xi^{n_2}, \ldots, \xi^{n_k}) \in V. \tag{174}$$

The projection of V on the hyperplane $x_k = 0$ is contained in an algebraic variety $V' \subset A_{k-1}(K)$, where $\dim V' \leqslant 1$. We have $(\xi^{n_1}, \ldots, \xi^{n_{k-1}}) \in V'$, hence by the inductive assumption there exist an integral matrix

$$M' = [m'_{ij}]_{\substack{i \leqslant 2 \\ j \leqslant k-1}} \quad \text{of rank 2} \tag{175}$$

and a vector $\mathbf{v}' \in \mathbf{Z}^2$ such that

$$h(M') \leqslant c(V'), \tag{176}$$

$$\mathbf{n}' = [n_1, \ldots, n_{k-1}] = \mathbf{v}'M'. \tag{177}$$

Since the vectors $[\mathbf{m}'_1, 0], [\mathbf{m}'_2, 0], [\mathbf{0}, 1]$ are linearly independent the variety V'' obtained from V by the substitution

$$x_i = x^{m'_{1i}} y^{m'_{2i}} \quad (1 \leqslant i < k), \quad x_k = z \tag{178}$$

satisfies

$$\dim V'' \leqslant 1.$$

By (174) and (177), (178) we have $(\xi^{v'_1}, \xi^{v'_2}, \xi^{n_k}) \in V''$ and by the already proved case $k = 3$ of the theorem there exist an integral matrix M'' of size 2×3, rank 2 and a vector $\mathbf{v}'' \in \mathbf{Z}^2$ such that

$$h(M'') \leqslant c(V''), \tag{179}$$

$$[v'_1, v'_2, n_k] = \mathbf{v}''M''. \tag{180}$$

Let us take

$$M = M'' \begin{bmatrix} M' & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{v} = \mathbf{v}''.$$

It follows from (176) and (179) that

$$h(M) \leqslant 2c(V')c(V'')$$

and from (177) and (180) that $\mathbf{n} = \mathbf{v}M$. Moreover, since M' and M'' are of rank 2, M is of rank 2. To complete the inductive proof it suffices to take $c(V) = \inf 2c(V') \max c(V'')$, where infimum is taken over all varieties V' containing the projection of V on $x_k = 0$ and the maximum is taken over all varieties V'' obtained from V by means of a substitution (178) satisfying (175) and (176).

References

[1] A. Baker, *The theory of linear forms in logarithms*, Transcendence Theory: Advances and Applications, London 1977, pp. 1–27.

[2] E. Bombieri and J. D. Vaaler, *On Siegel's lemma*, Invent. Math. 73 (1983), 11–32.

[3] S. Chaładus and A. Schinzel, *A decomposition of integer vectors, II*, to appear in Analysis and Related Mathematical Fields, Sofia.

[4] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.

[5] E. Dobrowolski, W. Lawton, A. Schinzel, *On a problem of Lehmer*, Studies in Pure Mathematics, To the Memory of Paul Turán, Budapest 1983, pp. 135–144.

[6] R. Fricke, *Lehrbuch der Algebra*, Bd. I, Braunschweig 1924.

[7] L. Low, *A problem of Schinzel on lattice points*, Acta Arith. 31 (1976), 385–388.

[8] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), 1–34.

[9] — *Reducibility of lacunary polynomials, I*, ibid. 16 (1969), 123–159.

[10] — *Reducibility of lacunary polynomials, III*, ibid. 34 (1978), 227–266.

[11] — *Reducibility of lacunary polynomials, VII*, Monatsch. Math. 102 (1986), 309–337.

[12] — *Reducibility of lacunary polynomials, VIII*, Acta Arith. 50 (1988), 91–106.

[13] — *Reducibility of lacunary polynomials, IX*, New Advances in Transcendence Theory, London 1988, 313–336.

[14] — *A decomposition of integer vectors, I*, Bull. Polish Acad. Sci. Ser. Math. 35 (1987), 155–159.

[15] W. Schmidt, *A problem of Schinzel on lattice points*, Acta Arith. 15 (1969), 199–203.

Received on 27. 10. 1987 (1763)