ACTA ARITHMETICA
L (1988)

Reducibility of lacunary polynomials, VIII

by

A. SCHINZEL (Warszawa)

The aim of this paper is to extend the results of the previous paper of this series concerning the reducibility of $\alpha_0+\sum_{j=1}^{k}\alpha_j x^{n_j}$ over $Q(\alpha_0, \ldots, \alpha_k)$ to the case, where $Q(\alpha_0, \ldots, \alpha_k)$ is a transcendental extension of Q. In order to do this we have to establish first a result about roots of unity, which seems of independent interest. L. Rédei [3] and H. B. Mann [2] considered representations of 0 by sums of roots of unity with rational coefficients, the present writer [4] and J. H. Loxton [1] considered such representations of an arbitrary algebraic number. Here we prove a theorem which generalizes all these theorems in their qualitative form.

THEOREM 1. *There exists a function $C(d, k)$: $N^2 \to \mathbf{R}$ with the following property. If $\mathbf{K}$ is an extension of $\mathbf{Q}$ of degree at most d, $a_0, a_1, \ldots, a_k \in \mathbf{K}$, ζ_N is a primitive root of unity of order N, $(N, p_1, \ldots, p_k) = 1$ and*

$$a_0+\sum_{i=1}^{k} a_i \zeta_N^{p_i} = 0, \tag{1}$$

then either there is a non-empty set $I \subset \{1, 2, \ldots, k\}$ such that

$$\sum_{i\in I} a_i \zeta_N^{p_i} = 0$$

or

$$N < C(d, k).$$

The proof of this theorem will be conducted by the method of [4], although to obtain a good explicit value of $C(d, k)$ the method of [1] seems more appropriate.

Let us denote for a given polynomial $f \in C[x]$ by $Kf(x)$ the polynomial $f(x)$ deprived of all its factors $x-\zeta$, where ζ is 0 or a root of unity. Since all conjugates of a root of unity are also such roots, the coefficients of $Kf(x)$ belong to the field generated by the coefficients of f.

Using Theorem 1 we shall obtain from the results of [6] the following theorems.

THEOREM 2. *Let $k > 1$ and $a_0, a_1, \ldots, a_k$ be non-zero complex numbers such that $a_0 \in K_0 = Q(a_1/a_0, \ldots, a_k/a_0)$. The number of integer vectors $n = [n_1, n_2, \ldots, n_k]$ such that $0 = n_0 < n_1 < \ldots < n_k \leqslant N$ $(N \geqslant 3)$ and $K(a_0 + \sum_{j=1}^{k} a_j x^{n_j})$ is reducible over K_0 is less than*

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

where $C(a) \in R$ depends only on $a_0, a_1, \ldots, a_k$ and for $k < 6$ the logarithmic factors can be omitted.

THEOREM 3. *Let S be a set of positive integers with the counting function $S(x) = \Omega(x^{1-\varepsilon})$ for every $\varepsilon > 0$. If vectors $[a_{i0}, \ldots, a_{ik}] \in C^{k+1}$ $(1 \leqslant i \leqslant h)$ satisfy for each $i \leqslant h$ the conditions*

(i) $\quad a_{i0} \neq 0$ *and* $a_{ij} \neq 0$ *for at least two* $j > 0$

and

(ii) $\quad a_{i0} \in Q(a_{i1}/a_{i0}, \ldots, a_{ik}/a_{i0}) = K_i$

then there exist infinitely many vectors $[n_1, \ldots, n_k]$ such that

$$n_j \in S \quad (1 \leqslant j \leqslant k), \qquad n_1 < n_2 < \ldots < n_k$$

and for all $i \leqslant h$

$$K(a_{i0} + \sum_{j=1}^{k} a_{ij} x^{n_j}) \quad \text{is irreducible over } K_i.$$

Remarks. 1. Since every finitely generated field of characteristic 0 is isomorphic to a subfield of C, the complex numbers $a_0, \ldots, a_k$ in Theorem 2 and $a_{i0}, \ldots, a_{ik}$ in Theorem 3 can be replaced by elements of any field of characteristic 0.

2. It is clear that if $\sum_{j=0}^{k} a_{ij} = 0$ for some $i \leqslant h$ we cannot require in Theorem 3 the irreducibility of $a_{i0} + \sum_{j=1}^{k} a_{ij} x^{n_j}$.

At the end of the paper we give an example showing that the said irreducibility cannot be claimed even if $\sum_{j=0}^{k} a_{ij} \neq 0$ for all $i \leqslant h$.

The proofs of the above theorems are based on several lemmata. The proof of Theorem 1 has been simplified by J. Browkin.

LEMMA 1. *For all positive integers h and $N \geqslant 3$ there exists an integer D satisfying the conditions*

$$1 \leqslant D \leqslant (\log N)^{20h},$$

$$(iD+1, N) = 1 \quad \textit{for} \quad i = 1, 2, \ldots, h.$$

Proof, see [4], Lemma 1.

LEMMA 2. *There exist functions $C_i(g, l)\colon N^2 \to R$ $(i = 1, 2)$ non decreasing with respect of each of the variables and with the following property. For every $l \geqslant 1$, $N \geqslant 3$ and every subgroup G of $(Z/NZ)^*$ of index g there exist positive integers A and B such that*

(2) $$\max\{A, B\} < C_1(g, l)(\log N)^{C_2(g,l)}$$

and

(3) $$A + Bj \in G \bmod N \quad (j = 0, 1, \ldots, l).$$

Proof. In virtue of van der Waerden's theorem there exists a number $W(g, l)$ with the following property: if all positive integers not exceeding $W(g, l)$ are partitioned into g classes then at least one class contains an arithmetic progression of $l+1$ terms.

By Lemma 1 there exists an integer D satisfying the conditions

(4) $$1 \leqslant D \leqslant (\log N)^{20(W(g,l)-1)},$$

(5) $$(iD+1, N) = 1 \quad \text{for} \quad i = 1, 2, \ldots, W(g, l)-1.$$

The condition (5) is clearly satisfied also for $i = 0$. Let

$$(Z/NZ)^* = \bigcup_{i=1}^{g} H_i,$$

where H_i are cosets with respect to G and let us assign a positive integer $i \leqslant W(g, l)$ to the class A_i $(1 \leqslant i \leqslant g)$ if $(i-1)D+1 \in H_i \bmod N$. By the choice of $W(g, l)$ at least one of the classes A_i, say A_h, contains an arithmetic progression of $l+1$ terms $a+bj$ $(j = 0, 1, \ldots, l)$, where

(6) $$1 \leqslant a < a+bl \leqslant W(g, l).$$

Since $a+bj \in A_h$, we have

(7) $$(a+bj-1)D+1 \in H_h \bmod N \quad (j = 0, 1, \ldots, l)$$

and in particular

$$(a-1)D+1 \in H_h \bmod N.$$

The cosets H_i form a group of order g, hence

$$((a-1)D+1)^{g-1} \in H_h^{-1} \bmod N.$$

This together with (7) gives

$$((a-1)D+1)^{g-1}((a+bj-1)D+1) \in G \bmod N \quad (j = 0, 1, \ldots, l)$$

and the condition (3) is satisfied with

$$A = ((a-1)D+1)^g, \quad B = ((a-1)D+1)^{g-1} bD.$$

Using (4) and (6) we verify that (2) holds with

$$C_1(g, l) = W(g, l)^g, \quad C_2(g, l) = 20gW(g, l).$$

LEMMA 3. *Let $f_j(x_1, \ldots, x_n)$ $(1 \leqslant j \leqslant n)$ be polynomials of degrees $m_1, m_2, \ldots, m_n$ respectively, with coefficients in a field $K_1 \subset C$. If*

$$f_j(\xi_1, \ldots, \xi_n) = 0 \quad (1 \leqslant j \leqslant n)$$

and

$$\frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}(\xi_1, \ldots, \xi_n) \neq 0$$

then $[K_1(\xi_1, \ldots, \xi_n) : K_1] \leqslant m_1 m_2 \ldots m_n$.

Proof, see [4], Lemma 2 with a proof due to H. Davenport.

Proof of Theorem 1. Let us consider the equation (1) assuming $a_i \in K$ $(0 \leqslant i \leqslant k)$, $[K:Q] \leqslant d$, $N \geqslant 3$, $(N, p_1, \ldots, p_k) = 1$.

Let G be the Galois group of $K(\zeta_N)$ over K. G can clearly be represented as a subgroup of $(Z/NZ)^*$. For its index g, we have the inequality

$$g = [(Z/NZ)^* : G] = \frac{[Q(\zeta_N) : Q]}{[K(\zeta_N) : K]} = \frac{[K:Q]}{[K(\zeta_N) : Q(\zeta_N)]} \leqslant [K:Q] \leqslant d.$$

In virtue of Lemma 2 there exist positive integers A and B such that

$$\max\{A, B\} < C_1(d, k-1)(\log N)^{C_2(d,k-1)} \tag{8}$$

and

$$A + Bj \in G \bmod N \quad (j = 0, 1, \ldots, k-1). \tag{9}$$

Among the numbers p_i let there be exactly n that are distinct mod $N_1 = N/(N, B)$. By a suitable permutation of the terms of (1) we can achieve that $p_{s_1}, p_{s_2}, \ldots, p_{s_n}$ are all distinct mod N_1, $0 = s_0 < s_1 < \ldots < s_n = k$ and

$$p_i \equiv p_{s_\nu} \bmod N_1 \quad \text{if} \quad s_{\nu-1} < i \leqslant s_\nu \quad (1 \leqslant \nu \leqslant n). \tag{10}$$

Let us choose integers q_ν, such that

$$q_\nu \equiv p_{s_\nu} \bmod N_1, \quad (q_\nu, N) = (p_{s_\nu}, N_1) \quad (1 \leqslant \nu \leqslant n). \tag{11}$$

It follows from elementary congruence considerations that such choice is possible.

We write equation (1) in the form

$$\alpha_0 + \sum_{\nu=1}^{n} \zeta_N^{q_\nu} S_\nu = 0, \tag{12}$$

where $n \leqslant k$,

$$S_\nu = \sum_{i=s_{\nu-1}+1}^{s_\nu} \alpha_i \zeta_N^{p_i - q_\nu} \quad (1 \leqslant \nu \leqslant n).$$

By (9) ζ_N^{A+Bj} is for all nonnegative $j < k$ a conjugate of ζ_N. By (10) and (11)

$$\zeta_N^{(p_i - q_\nu)(A+Bj)} = \zeta_N^{(p_i - q_\nu)A} \quad (s_{\nu-1} < i \leqslant s_\nu).$$

Substituting ζ_N^{A+Bj} for ζ_N in (12) we get

$$\alpha_0 + \sum_{\nu=1}^{n} \zeta_N^{q_\nu(A+Bj)} S'_\nu = 0 \quad (0 \leqslant j < n),$$

where

$$S'_\nu = \sum_{i=s_{\nu-1}+1}^{s_\nu} \alpha_i \zeta_N^{(p_i - q_\nu)A} \in K(\zeta_B)$$

is a conjugate of S_ν.

We take in Lemma 3

$$f_j(x_1, \ldots, x_n) = \alpha_0 + \sum_{\nu=1}^{n} x_\nu^{A+Bj-B} S'_\nu \quad (1 \leqslant j \leqslant n),$$

$$K_1 = K(\zeta_B), \quad \xi_\nu = \zeta_N^{q_\nu} \quad (1 \leqslant \nu \leqslant n).$$

Hence

$$\frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}(\xi_1, \ldots, \xi_n) \tag{13}$$

$$= \prod_{j=1}^{n} (A+Bj-B) \prod_{\nu=1}^{n} S'_\nu \zeta_N^{q_\nu(A-1)} \prod_{1 \leqslant \mu < \nu \leqslant n} (\zeta_N^{q_\nu B} - \zeta_N^{q_\mu B}).$$

If $S'_\nu = 0$ for some $\nu \leqslant n$ then also

$$\sum_{i=s_{\nu-1}+1}^{s_\nu} \alpha_i \zeta_N^{p_i} = S_\nu = 0$$

and the theorem holds with $I = \{s_{\nu-1}+1, \ldots, s_\nu\}$.

If $S'_\nu \neq 0$ for all $\nu \leqslant n$, then by (13) and the choice of q_ν we have

$$\frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}(\xi_1, \ldots, \xi_n) \neq 0.$$

Therefore, by Lemma 3 and (8)

$$[K(\zeta_N^{q_1}, \zeta_N^{q_2}, \ldots, \zeta_N^{q_n}) : K] \leqslant [K(\zeta_B) : K] \prod_{j=0}^{n-1} (A+Bj) \tag{14}$$

$$< n! \max\{A, B\}^{n+1} \leqslant k! \max\{A, B\}^{k+1}$$

$$\leqslant k!\, C_1(d, k-1)^{k+1} (\log N)^{(k+1)C_2(d,k-1)}.$$

On the other hand, by (10) and (11)

$$(N, q_\nu) = (N_1, p_{s_\nu}) = (N_1, p_{s_{\nu-1}+1}, \ldots, p_{s_\nu}) \quad (1 \leqslant \nu \leqslant n),$$

hence

$$(N, q_1, \ldots, q_n) = (N_1, p_1, \ldots, p_k) = 1$$

and

$$[K(\zeta_N^{q_1}, \zeta_N^{q_2}, \ldots, \zeta_N^{q_n}) : K] = [K(\zeta_N) : K] = \frac{[K(\zeta_N) : Q(\zeta_N)][Q(\zeta_N) : Q]}{[K : Q]} \geqslant \frac{\varphi(N)}{d}.$$

It follows now from (14) that

$$\varphi(N) \leqslant k!\, dC_1(d, k-1)^{k+1} (\log N)^{(k+1)C_2(d,k-1)}.$$

Since for $N \geqslant 1$ we have $\varphi(N) > \frac{1}{2}\sqrt{N}$ it follows that $N < C(d, k)$ for a suitable function $C(d, k)$ and the proof is complete.

LEMMA 4. *Let $\alpha_0, \ldots, \alpha_k$ be non-zero algebraic numbers. If $\alpha_0 + \sum_{i=1}^{k} \alpha_i x^{n_i}$ has ζ_N as a multiple zero then there is a linear relation*

$$\sum_{i=1}^{k} \gamma_i n_i = 0,$$

where γ_i are integers, $0 < \max_{1 \leqslant i \leqslant k} |\gamma_i| \leqslant C_0(\boldsymbol{\alpha})$ and $C_0(\boldsymbol{\alpha}) \in \boldsymbol{R}$ depends only on $\alpha_0, \ldots, \alpha_k$.

Proof. Let $\omega_1, \ldots, \omega_s$ be an integral basis of the field $K = Q(\alpha_0, \ldots, \alpha_k)$ and let A be a positive integer such that $A\alpha_i$ are algebraic integers $(0 \leqslant i \leqslant k)$. We shall express $C_0(\boldsymbol{\alpha})$ in terms of ω_r's and $A\alpha_i$'s. If $\alpha_0 + \sum_{i=1}^{k} \alpha_i x^{n_i}$ has ζ_N as a multiple zero we get by differentiation

$$\sum_{i=1}^{k} \alpha_i n_i \zeta_N^{n_i} = 0.$$

Let S be a subset of $\{1, 2, \ldots, k\}$ irreducible with respect to the property that

$$\sum_{i \in S} \alpha_i n_i \zeta_N^{n_i} = 0.$$

We may assume without loss of generality that $1 \in S$. Since

$$(15) \qquad \alpha_1 n_1 + \sum_{i \in S \setminus \{1\}} \alpha_i n_i \zeta_N^{n_i - n_1} = 0,$$

it follows from Theorem 1 that either

$$(16) \qquad N_0 = \frac{N}{(N, \operatorname{g.c.d.}_{i \in S}(n_i - n_1))} < C(s, k-1)$$

or there exists a non-empty subset I of $S \setminus \{1\}$ such that

$$\sum_{i \in I} \alpha_i n_i \zeta_N^{n_i - n_1} = 0.$$

However in the latter case

$$\alpha_1 n_1 + \sum_{i \in S \setminus \{1\} \setminus I} \alpha_i n_i \zeta_N^{n_i - n_1} = 0$$

and

$$\sum_{i \in S \setminus I} \alpha_i n_i \zeta_N^{n_i} = 0,$$

contrary to the choice of S. Therefore, (16) holds. Taking the trace from $K(\zeta_{N_0})$ to K we get from (15)

$$(17) \qquad [K(\zeta_{N_0}) : K]\alpha_1 n_1 + \sum_{i \in S \setminus \{1\}} \alpha_i n_i \operatorname{Tr}(\zeta_N^{n_i - n_1}) = 0.$$

The numbers $A\alpha_i \operatorname{Tr}(\zeta_N^{n_i - n_1})$ are algebraic integers. Hence for suitable $b_{ir} \in \boldsymbol{Z}$ we have

$$(18) \qquad A\alpha_i \operatorname{Tr}(\zeta_N^{n_i - n_1}) = \sum_{r=1}^{s} b_{ir} \omega_r \quad (i \in S).$$

Passing to the conjugates with respect to Q and applying the Cramer formulae we get

$$(19) \qquad |b_{ir}| \leqslant s^{s/2} A \overline{|\alpha_i \operatorname{Tr}(\zeta_N^{n_i - n_1})|} \left(\max_{1 \leqslant r \leqslant s} \overline{|\omega_r|}\right)^{s-1},$$

where for an algebraic number α with conjugates $\alpha^{(1)}, \ldots, \alpha^{(d)}$

$$\overline{|\alpha|} = \max_{1 \leqslant i \leqslant d} |\alpha^{(i)}|.$$

However, by (16)

$$(20) \qquad \overline{|\operatorname{Tr}(\zeta_N^{n_i - n_1})|} \leqslant [K(\zeta_{N_0}) : K] \leqslant \varphi(N_0) < C(s, k-1).$$

Substituting (18) into (17) we get

$$\sum_{i \in S} n_i \sum_{r=1}^{s} b_{ir} \omega_r = 0,$$

hence

$$\sum_{r=1}^{s} \omega_r \sum_{i \in S} n_i b_{ir} = 0$$

and since $\omega_1, \ldots, \omega_s$ are linearly independent over Q

(21) $$\sum_{i\in S} n_i b_{ir} = 0 \quad (1 \leqslant r \leqslant s).$$

Taking

$$C_0(\boldsymbol{\alpha}) = s^{s/2} A \max_{0\leqslant i\leqslant k} \overline{|\alpha_i|}\, C(s, k-1)\big(\max_{1\leqslant r\leqslant s} \overline{|\omega_r|}\big)^{s-1}$$

we get from (19), (20) and (21) the assertion of the lemma unless $b_{ir} = 0$ for all $i \in S$ and all $r \leqslant s$. However in that case we get for $i = 1$ from (18)

$$A\alpha_1 [K(\zeta_{N_0}) : K] = 0$$

contrary to the assumption that $\alpha_1 \neq 0$.

LEMMA 5. *For every $k+1$ non-zero complex numbers $a_0, \ldots, a_k$ such that $a_0 \in K_0 = Q(a_1/a_0, \ldots, a_k/a_0)$ there exist $k+1$ algebraic numbers $\alpha_0, \ldots, \alpha_{k-1}$, $\alpha_k = 1$ such that if $0 = n_0 < n_1 < \ldots < n_k$ and $K(\sum_{i=0}^{k} a_i x^{n_i})$ is reducible over K_0 then either $K(\sum_{i=0}^{k} \alpha_i x^{n_i})$ is reducible over $K_0^* = Q(\alpha_0, \ldots, \alpha_{k-1})$ or there is a linear relation*

(22) $$\sum_{i=1}^{k} \gamma_i n_i = 0,$$

where γ_i are integers,

(23) $0 < \max_{1\leqslant i\leqslant k} |\gamma_i| \leqslant C_1(\boldsymbol{a})$ *and $C_1(\boldsymbol{a}) \in R$ depends only on $a_0, a_1, \ldots, a_k$.*

Remark. Note that K_0^* is not the set of invertible elements of K_0.

Proof. Let $b_1, \ldots, b_r$ be a transcendence basis for K_0, $\boldsymbol{b} = [b_1, \ldots, b_r]$ and let us choose for $K_0/Q(\boldsymbol{b})$ a generator θ of degree d, integral over $Q[\boldsymbol{b}]$ (such choice is always possible). By Theorem 7 of Chapter V of [7] the integral closure of $Q[\boldsymbol{b}]$ in K_0 is contained in a certain $Q[\boldsymbol{b}]$-module $[y_1, \ldots, y_d]$. Let us choose $D(\boldsymbol{b})$ so that

(24) $$D(\boldsymbol{b}) \in Q[\boldsymbol{b}] \setminus \{0\},$$

(25) $$D(\boldsymbol{b})\, y_i \in Q[\boldsymbol{b}, \theta] \quad (1 \leqslant i \leqslant d).$$

We have $a_i \in K_0$ $(0 \leqslant i \leqslant k)$. *Let*

(26) $$a_i = \frac{A_i(\boldsymbol{b}, \theta)}{B(\boldsymbol{b})} \quad (0 \leqslant i \leqslant k),$$

where

(27) $$A_i \in Q[\boldsymbol{b}, t] \quad (0 \leqslant i \leqslant k), \qquad B \in Q[\boldsymbol{b}] \setminus \{0\}.$$

Clearly

$$K_0 = Q(a_0/a_k, \ldots, a_{k-1}/a_k).$$

Let further

(28) $$\theta = \frac{\Phi(a_0/a_k, \ldots, a_{k-1}/a_k)}{\Psi(a_0/a_k, \ldots, a_{k-1}/a_k)}, \qquad \Psi(a_0/a_k, \ldots, a_{k-1}/a_k) \neq 0,$$

where

$$\Phi, \Psi \in Q[x_0, \ldots, x_{k-1}].$$

Let us denote by M the least common multiple of all positive integers less than $C(d, k-1)$, by k_0 the field of all algebraic numbers contained in K_0 and let $f \in k_0(\boldsymbol{b}, \zeta_M)[t]$ be the minimal polynomial of θ over $k_0(\boldsymbol{b}, \zeta_M)$,

(29) $$f = \frac{F}{G}, \qquad G \in k_0(\zeta_M)[\boldsymbol{b}] \setminus \{0\},$$

where $F \in k_0(\zeta_M)[\boldsymbol{b}, t]$ is irreducible over $k_0(\zeta_M)$.

For every subset S of $\{0, 1, \ldots, k\}$, every positive integer $N < C(d, k-1)$ and every function p: $S \to \{0, 1, \ldots, N-1\}$ we have either

$$F \mid \sum_{i\in S} A_i \zeta_N^{p(i)}$$

or

$$\Big(\sum_{i\in S} A_i \zeta_N^{p(i)}, F\Big) = 1.$$

In the latter case the resultant of the polynomials F and $\sum_{i\in S} A_i \zeta_N^{p(i)}$ with respect to t, which we denote by $R\langle S, N, p\rangle(\boldsymbol{b})$ is different from 0. Since by (26) and (27)

$$A_k(\boldsymbol{b}, \theta) = a_k B(\boldsymbol{b}) \neq 0$$

and by (28)

$$\Psi(a_0/a_k, \ldots, a_{k-1}/a_k) \neq 0$$

the resultant of F and of $A_k^{\deg\Psi}\Psi\left(\frac{A_0}{A_k}, \ldots, \frac{A_{k-1}}{A_k}\right)$ with respect to t, to be denoted by $R_0(\boldsymbol{b})$, is also different from 0.

Let us choose an integer vector $\boldsymbol{b}^* = [b_1^*, \ldots, b_r^*]$ such that

(30) $$B(\boldsymbol{b}^*) D(\boldsymbol{b}^*) G(\boldsymbol{b}^*) R_0(\boldsymbol{b}^*) \prod_{R\langle S,N,p\rangle \neq 0} R\langle S, N, p\rangle(\boldsymbol{b}^*) \neq 0.$$

Let us take for θ^* any zero of $F(\boldsymbol{b}^*, t)$. Then

(31) $$[Q(\theta^*):Q] \leqslant [Q(\boldsymbol{b}, \theta):Q(\boldsymbol{b})] = d.$$

Also

$$A_i(\boldsymbol{b}^*, \theta^*) \neq 0 \quad (0 \leqslant i \leqslant k),$$

since otherwise we should have

$$R\langle\{i\}, 1, 0\rangle(\boldsymbol{b}^*) = 0$$

and by (30)

$$R\langle\{i\}, 1, 0\rangle = 0,$$

contrary to the assumption $a_i \neq 0$. Let us set

(32) $$\alpha_i = \frac{A_i(\boldsymbol{b}^*, \theta^*)}{A_k(\boldsymbol{b}^*, \theta^*)} \quad (0 \leqslant i \leqslant k), \qquad \boldsymbol{\alpha} = [\alpha_0, \ldots, \alpha_{k-1}].$$

The numbers α_i are non-zero and algebraic, $\alpha_k = 1$;

(33) $$K_0^* = Q(\boldsymbol{\alpha}) \subset Q(\theta^*).$$

We proceed to show that the α_i's have the property asserted in the lemma. To this end we shall show first that $\theta^* \in K_0^*$. Indeed, by (26) and (28)

$$\theta\Psi\left(\frac{A_0(\boldsymbol{b}, \theta)}{A_k(\boldsymbol{b}, \theta)}, \ldots, \frac{A_{k-1}(\boldsymbol{b}, \theta)}{A_k(\boldsymbol{b}, \theta)}\right) - \Phi\left(\frac{A_0(\boldsymbol{b}, \theta)}{A_k(\boldsymbol{b}, \theta)}, \ldots, \frac{A_{k-1}(\boldsymbol{b}, \theta)}{A_k(\boldsymbol{b}, \theta)}\right) = 0$$

hence in view of (29) and of the irreducibility of F over $k_0(\zeta_M)$

$$F \mid A_k^{\max(\deg\Phi, \deg\Psi)}\left(t\Psi\left(\frac{A_0}{A_k}, \ldots, \frac{A_{k-1}}{A_k}\right) - \Phi\left(\frac{A_0}{A_k}, \ldots, \frac{A_{k-1}}{A_k}\right)\right),$$

where the divisibility holds in the ring $k_0(\zeta_M)[\boldsymbol{b}, t]$. Substituting $\boldsymbol{b}^*$, θ^* for $\boldsymbol{b}$, t respectively we get by (32)

$$\theta^* \Psi(\boldsymbol{\alpha}) - \Phi(\boldsymbol{\alpha}) = 0.$$

If we had $\Psi(\boldsymbol{\alpha}) = 0$ it would follow from $F(\boldsymbol{b}^*, \theta^*) = 0$ that $R_0(\boldsymbol{b}^*) = 0$ contrary to (30). Thus $\Psi(\boldsymbol{\alpha}) \neq 0$ and

(34) $$\theta^* = \frac{\Phi(\boldsymbol{\alpha})}{\Psi(\boldsymbol{\alpha})} \in K_0^*.$$

If $K(\sum_{i=0}^{k} a_i x^{n_i})$ is reducible over K_0 then

(35) $$\sum_{i=0}^{k} a_i x^{n_i} = a_k P_0(x) P_1(x) P_2(x),$$

where

(36) $$P_0, P_1, P_2 \in K_0[x], \quad KP_0(x) = 1, \quad KP_\nu(x) = P_\nu(x), \quad \deg P_\nu > 0$$
$(\nu = 1, 2)$ and P_ν are monic.

By (26)

$$\sum_{i=0}^{k} A_i(\boldsymbol{b}, \theta) A_k(\boldsymbol{b}, \theta)^{n_k - 1} x^{n_i} = A_k(\boldsymbol{b}, \theta)^{n_k} \prod_{\nu=0}^{2} P_\nu(x)$$

hence

$$\sum_{i=0}^{k} A_i(\boldsymbol{b}, \theta) A_k(\boldsymbol{b}, \theta)^{n_k - n_i - 1} x^{n_i} = \prod_{\nu=0}^{2} A_k(\boldsymbol{b}, \theta)^{\deg P_\nu} P_\nu\left(\frac{x}{A_k(\boldsymbol{b}, \theta)}\right).$$

The polynomial on the left-hand side and the three factors on the right-hand side are monic. In virtue of a theorem of Kronecker (see [5], Theorem 10, p. 48) the coefficients of the factors are integral over the ring generated over $\boldsymbol{Z}$ by the coefficients of the product, hence they are integral over the ring $Q[\boldsymbol{b}, \theta]$. Since θ has been chosen integral over $Q[\boldsymbol{b}]$ we get that the coefficients of

$$A_k(\boldsymbol{b}, \theta)^{\deg P_\nu} P_\nu\left(\frac{x}{A_k(\boldsymbol{b}, \theta)}\right)$$

are integral over $Q[\boldsymbol{b}]$. By (25) it follows that

$$D(\boldsymbol{b}) A_k(\boldsymbol{b}, \theta)^{\deg P_\nu} P_\nu\left(\frac{x}{A_k(\boldsymbol{b}, \theta)}\right) \in Q[\boldsymbol{b}, \theta, x] \quad (0 \leqslant \nu \leqslant 2)$$

and thus

(37) $$P_\nu(x) = \frac{R_\nu(\boldsymbol{b}, \theta, x)}{D(\boldsymbol{b}) A_k(\boldsymbol{b}, \theta)^{\deg P_\nu}},$$

where

(38) $$R_\nu \in Q[\boldsymbol{b}, t, x] \quad (0 \leqslant \nu \leqslant 2).$$

It follows from (26), (35) and (37) that

$$\left(D^3 A_k^{n_k - 1} \sum_{i=0}^{k} A_i x^{n_i} - R_0 R_1 R_2\right)\Big|_{t=\theta} = 0.$$

In view of (24), (27) and (38) the polynomial in the parenthesis belongs to $Q[\boldsymbol{b}, t, x]$. From (29) and the irreducibility of F over $k_0(\zeta_M)$ it follows that

$$F \mid D^3 A_k^{n_k - 1} \sum_{i=0}^{k} A_i x^{k_i} - R_0 R_1 R_2,$$

where the divisibility holds in the ring $k_0(\zeta_M)[\boldsymbol{b}, t, x]$. Substituting $\boldsymbol{b}^*$, θ^* for

b, t respectively, we get in view of (32)

$$D(\boldsymbol{b}^*)^3 A_k(\boldsymbol{b}^*, \theta^*)^{n_k} \sum_{i=0}^{k} \alpha_i x^{n_i} - \prod_{\nu=0}^{2} R_\nu(\boldsymbol{b}^*, \theta^*, x) = 0,$$

hence

$$\sum_{i=0}^{k} \alpha_i x^{n_i} = \prod_{\nu=0}^{2} P_\nu^*(x), \tag{39}$$

where

$$P_\nu^*(x) = \frac{R_\nu(\boldsymbol{b}^*, \theta^*, x)}{D(\boldsymbol{b}^*) A_k(\boldsymbol{b}^*, \theta^*)^{\deg P_\nu}} \quad (0 \leqslant \nu \leqslant 2), \tag{40}$$

and thus

$$\deg P_\nu^* \leqslant \deg P_\nu \quad (0 \leqslant \nu \leqslant 2).$$

Since

$$\sum_{\nu=0}^{2} \deg P_\nu^* = n_k = \sum_{\nu=0}^{2} \deg P_\nu$$

it follows that

$$\deg P_\nu^* = \deg P_\nu \quad (0 \leqslant \nu \leqslant 2).$$

Moreover, by (34) $P_\nu^* \in K_0^*[x]$. To complete the proof of the lemma it suffices to show that either

$$KP_\nu^*(x) = P_\nu^*(x) \quad (\nu = 1, 2)$$

or the conditions (22) and (23) hold. To this end we show first that

$$P_0^*(x) = P_0(x). \tag{41}$$

By (36) the coefficients of $P_0(x)$ are algebraic, hence $P_0(x) \in \boldsymbol{k}_0[x]$.

By (37)

$$\left(D(\boldsymbol{b}) A_k(\boldsymbol{b}, t)^{\deg P_0} P_0(x) - R_0(\boldsymbol{b}, t, x)\right)\Big|_{t=\theta} = 0.$$

By (24), (27) and (38) the polynomial in the parenthesis belongs to $\boldsymbol{k}_0[\boldsymbol{b}, t, x]$. From (29) and the irreducibility of F over $\boldsymbol{k}_0(\zeta_M)$ it follows that

$$F | D(\boldsymbol{b}) A_k(\boldsymbol{b}, t)^{\deg P_0} P_0(x) - R_0(\boldsymbol{b}, t, x),$$

where the divisibility holds in the ring $\boldsymbol{k}_0(\zeta_M)[\boldsymbol{b}, t, x]$. Substituting $\boldsymbol{b}^*, \theta^*$ for $\boldsymbol{b}, t$ respectively we get

$$D(\boldsymbol{b}^*) A_k(\boldsymbol{b}^*, \theta^*)^{\deg P_0} P_0(x) - R_0(\boldsymbol{b}^*, \theta^*, x) = 0$$

and (40) implies (41).

Since $\alpha_0 \neq 0$ we have by (39) $P_\nu^*(0) \neq 0$ $(0 \leqslant \nu \leqslant 2)$ hence if $KP_\nu^*(x) \neq P_\nu^*(x)$ $(\nu = 1$ or $2)$ it follows that for a certain root of unity ζ_N we have

$$P_\nu^*(\zeta_N) = 0 \quad (\nu = 1 \text{ or } 2). \tag{42}$$

By (39)

$$\sum_{i=0}^{k} \alpha_i \zeta_N^{n_i} = 0$$

and there is a decomposition

$$\{0, 1, \ldots, k\} = \bigcup_{\mu=1}^{m} \boldsymbol{I}_\mu \tag{43}$$

where $\boldsymbol{I}_\mu$ are non-empty disjoint sets such that

$$\sum_{i \in \boldsymbol{I}_\mu} \alpha_i \zeta_N^{n_i} = 0 \quad (1 \leqslant \mu \leqslant m). \tag{44}$$

We choose a decomposition with the maximal m and for all $\mu \leqslant m$ we choose an element i_μ in $\boldsymbol{I}_\mu$. Since by (31) and (33) $[\boldsymbol{K}_0^* : \boldsymbol{Q}] \leqslant d$ it follows from Theorem 1 that putting

$$d_\mu = (N, \underset{i \in \boldsymbol{I}_\mu}{\text{g.c.d.}} (n_i - n_{i_\mu}))$$

we have

$$N_\mu = \frac{N}{d_\mu} < C(d, k) \quad (1 \leqslant \mu \leqslant m). \tag{45}$$

The number $\zeta_N^{d_\mu}$ is a primitive root of unity of order N_μ, we denote it by ζ_{N_μ}. It follows from (44) that

$$\sum_{i \in \boldsymbol{I}_\mu} \alpha_i \zeta_{N_\mu}^{(n_i - n_{i_\mu})/d_\mu} = 0,$$

hence by (32)

$$\sum_{i \in \boldsymbol{I}_\mu} A_i(\boldsymbol{b}^*, \theta^*) \zeta_{N_\mu}^{(n_i - n_{i_\mu})/d_\mu} = 0.$$

Since $F(\boldsymbol{b}^*, \theta^*) = 0$ we have

$$R\langle \boldsymbol{I}_\mu, N_\mu, p_\mu \rangle(\boldsymbol{b}^*) = 0,$$

where $p_\mu(i)$ is defined for $i \in \boldsymbol{I}_\mu$ as the residue mod N_μ of $(n_i - n_{i_\mu})/d_\mu$. In view of (30) this implies

$$R\langle \boldsymbol{I}_\mu, N_\mu, p_\mu \rangle = 0,$$

thus

$$\Big(F, \sum_{i \in \boldsymbol{I}_\mu} A_i \zeta_{N_\mu}^{(n_i - n_{i_\mu})/d_\mu}\Big) \neq 1.$$

However by (45) and the remark after (29), the last formula implies

$$F\Big|\sum_{i\in I_\mu} A_i \zeta_{N_\mu}^{(n_i-n_{i_\mu})/d_\mu},$$

where the divisibility holds in the ring $k_0(\zeta_M)[b, t]$. Substituting θ for t we get by (26)

$$\sum_{i\in I_\mu} a_i \zeta_{N_\mu}^{(n_i-n_{i_\mu})/d_\mu} = 0.$$

Hence

$$\sum_{i\in I_\mu} a_i \zeta_N^{n_i} = 0 \quad (1 \leqslant \mu \leqslant m)$$

and by (43)

$$\sum_{i=0}^{k} a_i \zeta_N^{n_i} = 0.$$

It follows from (35) and (36) that $P_0(\zeta_N) = 0$, hence by (41)

$$P_0^*(\zeta_N) = 0.$$

By (39) and (42) ζ_N is a multiple zero of $\sum_{i=0}^{k} \alpha_i x^{n_i}$. The conditions (22) and (23) follow now from Lemma 4 with $C_1(a) = C_0(\alpha, 1)$.

Proof of Theorem 2. Let $\alpha_0, \ldots, \alpha_{k-1}$, $\alpha_k = 1$ be $k+1$ algebraic numbers the existence of which is asserted in Lemma 5, $\alpha = [\alpha_0, \ldots, \alpha_{k-1}]$. In virtue of that lemma if $0 = n_0 < n_1 < \ldots < n_k$ and $K\big(\sum_{j=0}^{k} a_j x^{n_j}\big)$ is reducible over K_0 then either $K\big(\sum_{j=0}^{k} \alpha_j x^{n_j}\big)$ is reducible over $K_0^* = Q(\alpha_0, \ldots, \alpha_{k-1})$ or the conditions (22) and (23) hold. Since $K_0^* = Q(\alpha_1/\alpha_0, \ldots, \alpha_k/\alpha_0)$, in virtue of Theorem 1 of [6] the number of integer vectors $[n_1, \ldots, n_k]$ satisfying

(46) $$0 < n_1 < \ldots < n_k \leqslant N,$$

for which the first possibility holds is for $N \geqslant 3$ less than

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

where for $k < 6$ the logarithmic factors can be omitted. On the other hand, the number of vectors in question for which the conditions (22) and (23) hold with $\gamma_i \neq 0$, $\gamma_{i+1} = \gamma_{i+2} = \ldots = \gamma_k = 0$ does not exceed

$$2C_1(a)\big(2C_1(a)+1\big)^{i-1} N^{k-1},$$

since the coordinates n_j for $j \neq i$ can be chosen in at most N ways each and then n_i in at most

$$2C_1(a)\big(2C_1(a)+1\big)^{i-1}$$

ways. Since

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

and

$$\sum_{i=1}^{k} 2C_1(a)\big(2C_1(a)+1\big)^{i-1} < \big(2C_1(a)+1\big)^k,$$

Theorem 2 holds with

$$C(a) = C(\alpha, 1) + \big(2C_1(a)+1\big)^k.$$

Proof of Theorem 3. By the assumption about S for $\varepsilon = \dfrac{\min\{k, 6\}}{3k(k-1)}$ there exists a constant $\gamma(k) > 0$ and infinitely many integers N such that

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

Therefore, the number of vectors $[n_1, \ldots, n_k]$ such that $n_j \in S$ $(1 \leqslant j \leqslant k)$ and

(47) $$0 = n_0 < n_1 < \ldots < n_k \leqslant N$$

exceeds

$$\big(\gamma(k)\, N^{1-\varepsilon}\big)^k > \gamma_1(k)\, N^{(1-\varepsilon)k}.$$

The number of vectors $[n_1, \ldots, n_k] \in Z^k$ such that (47) holds and $K\big(\sum_{j=0}^{k} a_{ij} x^{n_j}\big)$ is reducible over K_i is by Theorem 2 less than

$$U_i = C(a_i)\, N^{l_i - \frac{\min\{l_i, 6\}}{2(l_i-1)}} \frac{(\log N)^{10}}{(\log\log N)^9} \cdot N^{k-l_i},$$

where $a_i \in C^{l_i+1}$ is the vector obtained from $[a_{i0}, \ldots, a_{ik}]$ by leaving out all coordinates equal to 0 and the factor N^{k-l_i} reflects the free choice of n_j for all j with $a_{ij} = 0$.

Further, by Theorem 2 of [6] the number of vectors $[m_1, \ldots, m_k] \in Z^k$ such that (47) holds and $K\big(\sum_{j=0}^{k} a_{ij} x^{n_j}\big) \in K_0$ is less than

$$V_i = c(l_i)\, N^{\left[\frac{l_i+1}{2}\right]} N^{k-l_i} = c(l_i)\, N^{k-\left[\frac{l_i}{2}\right]}.$$

Since by the assumption $l_i \geqslant 2$ for all $i \leqslant h$ and $2 \leqslant l \leqslant k$ implies

$$\frac{\max\{l, 6\}}{2(l-1)} \geqslant \frac{\min\{k, 6\}}{2(k-1)} > \varepsilon k, \qquad \left[\frac{l}{2}\right] \geqslant \frac{\min\{k, 6\}}{2(k-1)} > \varepsilon k$$

we have for N large enough

$$\gamma_1(k)\,N^{k(1-\varepsilon)} > \sum_{i=1}^{h} (U_i+V_i)$$

and the theorem follows.

EXAMPLE. Take $k = 2$, $k = 3$;

$$a_{ij} = \begin{cases} 2 & \text{if} \quad i-j = 1, \\ 1 & \text{if} \quad i-j \neq 1. \end{cases}$$

We assert that for every choice of n_1, n_2, where $0 < n_1 < n_2$ at least one of the polynomials $f_i(x) = a_{i0} + \sum_{j=1}^{2} a_{ij} x^{n_j}$ $(1 \leqslant i \leqslant 3)$ is reducible over Q. Indeed, let $(n_1, n_2) = d$, $n_j = dm_j$ $(j = 1, 2)$. We cannot have $m_1 \equiv m_2 \equiv 0 \bmod 2$.

If $m_1 \equiv 1$, $m_2 \equiv 1 \bmod 2$, then $x^d+1 | f_1(x)$;

if $m_1 \equiv 1$, $m_2 \equiv 0 \bmod 2$, then $x^d+1 | f_2(x)$;

if $m_1 \equiv 0$, $m_2 \equiv 1 \bmod 2$, then $x^d+1 | f_3(x)$.

Since $\deg f_i = n_2 > d$, the claim follows.

Note added in proof. U. Zannier in the paper *On the linear dependence of roots of unity over finite extensions of Q*, due to appear in Acta Arithmetica, vol. 52, gives the following bound for $C(d, k)$

$$C(d, k) \leqslant \exp\left(c\frac{\tau(d)\,d}{\varphi(d)}\log(dk)\frac{k}{\log k}\right),$$

where c is an absolute constant and $\tau(d)$ the number of divisors of d.

References

[1] J. H. Loxton, *On two problems of R. M. Robinson about sums of roots of unity*, Acta Arith. 26 (1974), pp. 159–174.

[2] H. B. Mann, *On linear relations between roots of unity*, Mathematika 12 (1965), pp. 107–117.

[3] L. Rédei, *Natürliche Basen des Kreisteilungskörpers, I*, Abh. Math. Sem. Univ. Hamburg 23 (1959), pp. 180–200.

[4] A. Schinzel, *On sums of roots of unity. Solution of two problems of R. M. Robinson*, Acta Arith. 11 (1966), pp. 419–432.

[5] — *Selected Topics on Polynomials*, Ann Arbor 1982.

[6] — *Reducibility of lacunary polynomials, VII*, Monatsh. Math. 102 (1986), pp. 309–337.

[7] O. Zariski and P. Samuel, *Commutative algebra*, vol. 1, Princeton 1958.

Received on 2.6.1986 (1644)