ACTA ARITHMETICA
LXXIV.2 (1996)

Algebraic independence of the values of power series generated by linear recurrences

by

TAKA-AKI TANAKA (Yokohama)

1. Introduction. Let $\{a_k\}_{k\ge 0}$ be a linear recurrence of nonnegative integers defined by

$$(1) \qquad a_{k+n} = c_1 a_{k+n-1} + \ldots + c_n a_k \quad (k = 0, 1, 2, \ldots),$$

where $a_0, \ldots, a_{n-1}$ are not all zero and $c_1, \ldots, c_n$ are nonnegative integers with $c_n \neq 0$. Put

$$(2) \qquad \Phi(X) = X^n - c_1 X^{n-1} - \ldots - c_n.$$

In what follows, $\mathbb{Q}$ and $\overline{\mathbb{Q}}$ denote the fields of rational and algebraic numbers respectively. In 1929, Mahler [4] proved the following theorem: Let $\{a_k\}_{k\ge 0}$ be a linear recurrence satisfying (1). Suppose that $\Phi(X)$ is irreducible over $\mathbb{Q}$ and the roots $\varrho_1, \ldots, \varrho_n$ of $\Phi(X)$ satisfy $\varrho_1 > \max\{1, |\varrho_2|, \ldots, |\varrho_n|\}$. If α is an algebraic number with $0 < |\alpha| < 1$, then the number $\sum_{k=0}^{\infty} \alpha^{a_k}$ is transcendental.

In this paper, we establish two theorems on the algebraic independence of the values of power series generated by linear recurrences with conditions on $\Phi(X)$ weaker than those of Mahler (see Remark 1 below).

Let $\{a_k\}_{k\ge 0}$ and $\{b_k\}_{k\ge 0}$ be linear recurrences satisfying (1). We write $\{a_k\}_{k\ge 0} \sim \{b_k\}_{k\ge 0}$ if there is a nonnegative integer l such that

$$a_k = b_{k+l} \ (0 \le k \le n-1) \quad \text{or} \quad b_k = a_{k+l} \ (0 \le k \le n-1).$$

Then $\sim$ is an equivalence relation. Its negation is written as $\{a_k\}_{k\ge 0} \not\sim \{b_k\}_{k\ge 0}$. We denote by $f^{(l)}(z)$ the lth derivative of a function $f(z)$.

THEOREM 1. *Let $\{a_k^{(i)}\}_{k\ge 0}$ $(i = 1, \ldots, s)$ be linear recurrences satisfying* (1). *Suppose that $\Phi(\pm 1) \neq 0$ and the ratio of any pair of distinct roots of $\Phi(X)$ is not a root of unity. Let*

$$f_i(z) = \sum_{k=0}^{\infty} z^{a_k^{(i)}} \quad (1 \le i \le s)$$

and let α *be an algebraic number with* $0<|\alpha|<1$. *Then* $\{f_i^{(l)}(\alpha)\}_{1\le i\le s,\, l\ge 0}$ *are algebraically independent if and only if* $\{a_k^{(i)}\}_{k\ge 0}\not\sim\{a_k^{(j)}\}_{k\ge 0}$ $(1\le i<j\le s)$.

THEOREM 2. *Let* $\{a_k\}_{k\ge 0}$ *be a linear recurrence satisfying the same conditions as in Theorem* 1. *Suppose that* $\{a_k\}_{k\ge 0}$ *is not a geometric progression. Let*

$$f(z)=\sum_{k=0}^{\infty} z^{a_k}$$

and let $\alpha_1,\ldots,\alpha_r$ *be algebraic numbers with* $0<|\alpha_i|<1$ $(1\le i\le r)$. *Then the following three properties are equivalent*:

(i) $\{f^{(l)}(\alpha_i)\}_{1\le i\le r,\, l\ge 0}$ *are algebraically dependent.*

(ii) $1, f(\alpha_1),\ldots,f(\alpha_r)$ *are linearly dependent over* $\overline{\mathbb{Q}}$.

(iii) *There exist a nonempty subset* $\{\alpha_{i_1},\ldots,\alpha_{i_s}\}$ *of* $\{\alpha_1,\ldots,\alpha_r\}$, *roots of unity* $\zeta_1,\ldots,\zeta_s$, *an algebraic number* γ *with* $\alpha_{i_q}=\zeta_q\gamma$ $(1\le q\le s)$, *and algebraic numbers* $\xi_1,\ldots,\xi_s$, *not all zero*, *such that*

$$\sum_{q=1}^{s}\xi_q\zeta_q^{a_k}=0$$

for all sufficiently large k.

Remark 1. Since we do not assume that $\Phi(X)$ is irreducible over $\mathbb{Q}$, our assumption on $\Phi(X)$ is weaker than that of Mahler, because of the following fact: Suppose that the polynomial $\Phi(X)$ defined by (2) with $n\ge 2$ is irreducible over $\mathbb{Q}$. Then the roots $\varrho_1,\ldots,\varrho_n$ of $\Phi(X)$ satisfy the condition $\varrho_1>\max\{1,|\varrho_2|,\ldots,|\varrho_n|\}$ if and only if none of ϱ_i/ϱ_j $(i\ne j)$ is a root of unity. (A proof of this statement will be given in Section 2.)

Remark 2. In the case where $\{a_k\}_{k\ge 0}$ is a geometric progression, Loxton and van der Poorten [3] obtained the following result: Let $f(z)=\sum_{k=0}^{\infty} z^{d^k}$, where d is an integer greater than 1, and let $\alpha_1,\ldots,\alpha_r$ be algebraic numbers with $0<|\alpha_i|<1$ $(1\le i\le r)$. Then the following three properties are equivalent:

(i) $\{f^{(l)}(\alpha_i)\}_{1\le i\le r,\, l\ge 0}$ are algebraically dependent.

(ii) $1, f(\alpha_1),\ldots,f(\alpha_r)$ are linearly dependent over $\overline{\mathbb{Q}}$.

(iii) There exist a nonempty subset $\{\alpha_{i_1},\ldots,\alpha_{i_s}\}$ of $\{\alpha_1,\ldots,\alpha_r\}$, nonnegative integers $k_1,\ldots,k_s$, roots of unity $\zeta_1,\ldots,\zeta_s$, an algebraic number γ with $\alpha_{i_q}^{d^{k_q}}=\zeta_q\gamma$ $(1\le q\le s)$, and algebraic numbers $\xi_1,\ldots,\xi_s$, not all zero, such that

$$\sum_{q=1}^{s}\xi_q\zeta_q^{d^k}=0\qquad (k=0,1,2,\ldots).$$

Remark 3. As a special case of the result of Nishioka [6], the three properties (i)–(iii) in Theorem 2 are equivalent also for gap series $\sum_{k=0}^{\infty} z^{a_k}$, where $\{a_k\}_{k\ge 0}$ is an increasing sequence of nonnegative integers such that $\lim_{k\to\infty} a_{k+1}/a_k = \infty$. In the case of a linear recurrence $\{a_k\}_{k\ge 0}$ satisfying the conditions of Theorem 1, we have $\lim_{k\to\infty} a_{k+1}/a_k = \varrho > 1$ (see Remark 4 in Section 2).

The author is grateful to Prof. K. Nishioka for her valuable advice.

2. Lemmas. Let $\Omega = (\omega_{ij})$ be an $n\times n$ matrix with nonnegative integer entries. Then the maximum ϱ of the absolute values of the eigenvalues of Ω is itself an eigenvalue (cf. Gantmacher [2, p. 66, Theorem 3]). If $\mathbf{z} = (z_1,\dots,z_n)$ is a point of $\mathbb{C}^n$ with $\mathbb{C}$ the set of complex numbers, we define a transformation $\Omega : \mathbb{C}^n \to \mathbb{C}^n$ by

$$\Omega\mathbf{z} = \Big(\prod_{j=1}^{n} z_j^{\omega_{1j}}, \dots, \prod_{j=1}^{n} z_j^{\omega_{nj}}\Big). \tag{3}$$

We suppose that the matrix Ω and an algebraic point $\boldsymbol{\alpha} = (\alpha_1,\dots,\alpha_n)$, where α_i are nonzero algebraic numbers, have the following four properties:

(I) Ω is nonsingular and none of its eigenvalues is a root of unity, so that in particular $\varrho > 1$.

(II) Every entry of the matrix Ω^k is $O(\varrho^k)$ as k tends to infinity.

(III) If we put $\Omega^k\boldsymbol{\alpha} = (\alpha_1^{(k)},\dots,\alpha_n^{(k)})$, then

$$\log|\alpha_i^{(k)}| \le -c\varrho^k \quad (1\le i\le n)$$

for all sufficiently large k, where c is a positive constant.

(IV) If $f(\mathbf{z})$ is any nonzero power series in n variables with complex coefficients which converges in some neighborhood of the origin, then there are infinitely many positive integers k such that $f(\Omega^k\boldsymbol{\alpha}) \ne 0$.

We note that the property (II) is satisfied if every eigenvalue of Ω of absolute value ϱ is a simple root of the minimal polynomial of Ω.

Let K be an algebraic number field. In what follows, the rings of polynomials and formal power series in variables $z_1,\dots,z_n$ with coefficients in K are denoted by $K[z_1,\dots,z_n]$ and $K[[z_1,\dots,z_n]]$, respectively.

Lemma 1 (Nishioka [7]). *Assume that* $f_1(\mathbf{z}),\dots,f_m(\mathbf{z}) \in K[[z_1,\dots,z_n]]$ *converge in an n-polydisc U around the origin and satisfy a functional equation of the form*

$$\begin{pmatrix} f_1(\mathbf{z}) \\ \vdots \\ f_m(\mathbf{z}) \end{pmatrix} = A \begin{pmatrix} f_1(\Omega\mathbf{z}) \\ \vdots \\ f_m(\Omega\mathbf{z}) \end{pmatrix} + \begin{pmatrix} b_1(\mathbf{z}) \\ \vdots \\ b_m(\mathbf{z}) \end{pmatrix}, \tag{4}$$

where A is an $m\times m$ matrix with entries in K and $b_i(\mathbf{z})\in K[z_1,\ldots,z_n]$ $(1\le i\le m)$. Suppose that the $n\times n$ matrix Ω and a point $\boldsymbol{\alpha}$ whose components are nonzero algebraic numbers have the properties (I)–(IV) *and* $\boldsymbol{\alpha}\in U$. *If $f_1(\mathbf{z}),\ldots,f_r(\mathbf{z})$ $(r\le m)$ are linearly independent over K modulo $K[z_1,\ldots,z_n]$, then $f_1(\boldsymbol{\alpha}),\ldots,f_r(\boldsymbol{\alpha})$ are algebraically independent.*

In what follows, $\mathbb{N}_0$ denotes the set of nonnegative integers.

LEMMA 2 (Skolem–Mahler–Lech's theorem, cf. Cassels [1]). *Let C be a field of characteristic zero. Let $\varrho_1,\ldots,\varrho_d$ be nonzero distinct elements in C and $P_1(X),\ldots,P_d(X)$ nonzero polynomials of X with coefficients in C. Then*

$$R=\Big\{k\in\mathbb{N}_0\,\Big|\,f(k)=\sum_{i=1}^{d}P_i(k)\varrho_i^k=0\Big\}\tag{5}$$

is the union of a finite set and a finite number of arithmetic progressions. If R is an infinite set, then ϱ_i/ϱ_j is a root of unity for some distinct i and j.

LEMMA 3 (Masser [5]). *Let Ω be an $n\times n$ matrix with nonnegative integer entries for which the property* (I) *holds. Let $\boldsymbol{\alpha}$ be an n-dimensional vector whose components $\alpha_1,\ldots,\alpha_n$ are nonzero algebraic numbers such that $\Omega^k\boldsymbol{\alpha}\to(0,\ldots,0)$ as k tends to infinity. Then the negation of the property* (IV) *is equivalent to the following*:

There exist integers $i_1,\ldots,i_n$ not all zero and positive integers a, b such that

$$(\alpha_1^{(k)})^{i_1}\ldots(\alpha_n^{(k)})^{i_n}=1$$

for all $k=a+lb$ $(l=0,1,2,\ldots)$.

Let $\{a_k\}_{k\ge0}$ be a linear recurrence satisfying (1). We put

$$\Omega=\begin{pmatrix} c_1 & 1 & 0 & \ldots & 0\\ c_2 & 0 & 1 & \ddots & \vdots\\ \vdots & \vdots & & \ddots & 0\\ & & & \ddots & 1\\ c_n & 0 & & \ldots & 0\end{pmatrix}.\tag{6}$$

LEMMA 4. *Suppose that $\Phi(\pm1)\ne0$ and the ratio of any pair of distinct roots of $\Phi(X)$ is not a root of unity. If α is an algebraic number with $0<|\alpha|<1$, then the matrix Ω defined by* (6) *and $\boldsymbol{\alpha}=(\underbrace{1,\ldots,1}_{n-1},\alpha)$ have the properties* (I)–(IV).

Proof. The property (I) is satisfied, since the characteristic polynomial of the matrix Ω defined by (6) is $\Phi(X)$. Let $\varrho_1,\ldots,\varrho_d$ be the distinct eigenvalues of Ω. Since every entry of Ω is nonnegative, we may assume

$\varrho_1 \geq \max\{|\varrho_2|, \ldots, |\varrho_d|\}$ and then $\varrho_1 > 1$. For each i $(0 \leq i \leq n-1)$, we define the sequence $\{a_k^{(i)}\}_{k \geq 0}$ by

$$a_{k+n}^{(i)} = c_1 a_{k+n-1}^{(i)} + \ldots + c_n a_k^{(i)} \qquad (k = 0, 1, 2, \ldots)$$

with

$$a_0^{(i)} = 0,\ \ldots,\ a_{i-1}^{(i)} = 0,\ a_i^{(i)} = 1,\ a_{i+1}^{(i)} = 0,\ \ldots,\ a_{n-1}^{(i)} = 0.$$

Then

$$\Omega^k = \begin{pmatrix} a_{k+n-1}^{(n-1)} & \ldots & a_k^{(n-1)} \\ \ldots & \ldots & \ldots \\ a_{k+n-1}^{(0)} & \ldots & a_k^{(0)} \end{pmatrix} \qquad (k = 0, 1, 2, \ldots).$$

Since each $a_k^{(i)}$ can be expressed as an $f(k)$ in (5), the sequence $\{a_k^{(i)}\}_{k \geq 0}$ has only finitely many zeros by Lemma 2. Hence the entries of Ω^λ are positive for sufficiently large λ. By Perron's theorem (cf. Gantmacher [2, p. 53, Theorem 1]), it follows that ϱ_1 is a simple root of $\Phi(X)$ and has the property $\varrho_1 > \max\{|\varrho_2|, \ldots, |\varrho_d|\}$. Therefore the property (II) is satisfied.

We can write

$$a_k^{(i)} = b^{(i)} \varrho_1^k + o(\varrho_1^k) \qquad (0 \leq i \leq n-1), \tag{7}$$

where at least one of $b^{(i)}$ is not zero. Since $a_k^{(i)} \geq 0$ $(k = 0, 1, 2, \ldots)$, all the $b^{(i)}$ are nonnegative. Noting

$$\begin{pmatrix} a_{k+n}^{(n-1)} & \ldots & a_{k+1}^{(n-1)} \\ \ldots & \ldots & \ldots \\ a_{k+n}^{(0)} & \ldots & a_{k+1}^{(0)} \end{pmatrix} = \begin{pmatrix} c_1 & 1 & 0 & \ldots & 0 \\ c_2 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ & & & \ddots & 1 \\ c_n & 0 & \ldots & & 0 \end{pmatrix} \begin{pmatrix} a_{k+n-1}^{(n-1)} & \ldots & a_k^{(n-1)} \\ \ldots & \ldots & \ldots \\ a_{k+n-1}^{(0)} & \ldots & a_k^{(0)} \end{pmatrix},$$

we have

$$a_{k+1}^{(i)} = c_{n-i} a_k^{(n-1)} + a_k^{(i-1)} \quad (1 \leq i \leq n-1), \quad a_{k+1}^{(0)} = c_n a_k^{(n-1)}.$$

Thus

$$b^{(i)} \varrho_1 = c_{n-i} b^{(n-1)} + b^{(i-1)} \quad (1 \leq i \leq n-1), \quad b^{(0)} \varrho_1 = c_n b^{(n-1)},$$

so that

$$b^{(i)} \geq b^{(i-1)}/\varrho_1 \quad (1 \leq i \leq n-1), \quad b^{(0)} \geq b^{(n-1)}/\varrho_1.$$

This implies that $b^{(i)} > 0$ for any i, since at least one of $b^{(i)}$ is positive. Put $\Omega^k \boldsymbol{\alpha} = (\alpha_{n-1}^{(k)}, \ldots, \alpha_0^{(k)})$. Then

$$\alpha_i^{(k)} = (a_{n-1}^{(i)}, \ldots, a_0^{(i)})\Omega^k \boldsymbol{\alpha} = \alpha^{a_k^{(i)}} \qquad (0 \le i \le n-1).$$

Hence the property (III) is satisfied.

Assume that there exist integers $i_0, \ldots, i_{n-1}$ not all zero and positive integers a, b such that

$$(\alpha_{n-1}^{(k)})^{i_{n-1}} \ldots (\alpha_0^{(k)})^{i_0} = 1$$

for all $k = a + lb$ $(l = 0, 1, 2, \ldots)$. Let $\{a_k^*\}_{k \ge 0}$ be a linear recurrence defined by (1) with $a_0 = i_0, \ldots, a_{n-1} = i_{n-1}$. Then

$$\alpha^{a_k^*} = (i_{n-1}, \ldots, i_0)\Omega^k \boldsymbol{\alpha} = 1,$$

namely $a_k^* = 0$ for all $k = a + lb$ $(l = 0, 1, 2, \ldots)$. Since $\{a_k^*\}_{k \ge 0}$ is nonzero linear recurrence, there are distinct i and j such that ϱ_i/ϱ_j is a root of unity by Lemma 2. This contradicts the assumption in the lemma. Therefore the property (IV) is satisfied. This completes the proof of the lemma.

Remark 4. Let $\{a_k\}_{k \ge 0}$ be as in Theorem 1. Then we have

$$a_k = b\varrho_1^k + o(\varrho_1^k),$$

where $b = \sum_{i=0}^{n-1} a_i b^{(i)} > 0$, since $a_k = \sum_{i=0}^{n-1} a_i a_k^{(i)}$ and $a_0, \ldots, a_{n-1}$ are not all zero.

Proof of the statement in Remark 1. We only have to prove that none of ϱ_i/ϱ_j $(i \ne j)$ is a root of unity if $\varrho_1 > \max\{1, |\varrho_2|, \ldots, |\varrho_n|\}$, since the converse is already proved in the proof of Lemma 4. Suppose that ϱ_i/ϱ_j is a root of unity for some distinct i and j. We choose an automorphism σ of the field $\overline{\mathbb{Q}}$ such that $\varrho_i^\sigma = \varrho_1$. Then $\varrho_1/\varrho_j^\sigma$ is a root of unity, and so $\varrho_1 = |\varrho_j^\sigma|$, which contradicts the inequality $\varrho_1 > \max\{1, |\varrho_2|, \ldots, |\varrho_n|\}$.

LEMMA 5. *Let $\{a_k^{(i)}\}_{k \ge 0}$ $(i = 1, 2)$ be linear recurrences satisfying* (1). *Suppose that $\Phi(\pm 1) \ne 0$ and the ratio of any pair of distinct roots of $\Phi(X)$ is not a root of unity. Denote by $\{a_k^{(i)}\}_{k \ge 0}^*$ the set of numbers appearing in $\{a_k^{(i)}\}_{k \ge 0}$, so that $\{a_k^{(i)}\}_{k \ge 0}^*$ $(i = 1, 2)$ are infinite sets by Lemma 2. Then $\{a_k^{(1)}\}_{k \ge 0}^* \cap \{a_k^{(2)}\}_{k \ge 0}^*$ is an infinite set if and only if $\{a_k^{(1)}\}_{k \ge 0} \sim \{a_k^{(2)}\}_{k \ge 0}$.*

Proof. We only have to prove that $\{a_k^{(1)}\}_{k \ge 0} \sim \{a_k^{(2)}\}_{k \ge 0}$ if $\{a_k^{(1)}\}_{k \ge 0}^* \cap \{a_k^{(2)}\}_{k \ge 0}^*$ is an infinite set. Assume that there are infinitely many pairs k_1 and k_2 such that $a_{k_1}^{(1)} = a_{k_2}^{(2)}$. By Remark 4, we have

$$a_k^{(i)} = b^{(i)}\varrho_1^k + o(\varrho_1^k) \qquad (i = 1, 2),$$

where $\varrho_1 > 1$ and $b^{(1)}, b^{(2)} > 0$. For any positive number ε there is a non-negative integer $k_0 = k_0(\varepsilon)$ such that

$$(b^{(i)} - \varepsilon)\varrho_1^k \le a_k^{(i)} \le (b^{(i)} + \varepsilon)\varrho_1^k \quad (i = 1, 2)$$

for all $k \ge k_0$. Then we have

$$(b^{(1)} - \varepsilon)\varrho_1^{k_1} \le (b^{(2)} + \varepsilon)\varrho_1^{k_2}, \quad (b^{(2)} - \varepsilon)\varrho_1^{k_2} \le (b^{(1)} + \varepsilon)\varrho_1^{k_1}$$

for infinitely many $k_1, k_2 \ge k_0$. Choosing $\varepsilon < \min\{b^{(1)}, b^{(2)}\}$, we get

$$0 < \frac{b^{(1)} - \varepsilon}{b^{(2)} + \varepsilon} \le \varrho_1^{k_2 - k_1} \le \frac{b^{(1)} + \varepsilon}{b^{(2)} - \varepsilon}.$$

Hence there are infinitely many pairs k_1 and k_2 such that $k_2 - k_1 = l$ for some integer l. Letting

$$b_k = a_k^{(1)} - a_{k+l}^{(2)} \quad (k \ge \max\{0, -l\}),$$

we see that the linear recurrence $\{b_k\}$ satisfies (1) and has infinitely many zeros. By Lemma 2, $b_k = 0$ for any $k \ge \max\{0, -l\}$, and the lemma is proved.

3. Proofs of Theorems 1 and 2

P r o o f o f T h e o r e m 1. We only have to prove that $\{f_i^{(l)}(\alpha)\}_{1\le i\le s, l\ge 0}$ are algebraically independent if $\{a_k^{(i)}\}_{k\ge 0} \not\sim \{a_k^{(j)}\}_{k\ge 0}$ $(1 \le i < j \le s)$. Let

$$P_i(\mathbf{z}) = z_1^{a_{n-1}^{(i)}} \dots z_n^{a_0^{(i)}} \quad (1 \le i \le s)$$

be monomials of $z_1, \dots, z_n$, which we denote similarly to (3) by

$$P_i(\mathbf{z}) = (a_{n-1}^{(i)}, \dots, a_0^{(i)})\mathbf{z}. \tag{8}$$

By (3) and (8), we get

$$P_i(\Omega^k \mathbf{z}) = z_1^{a_{k+n-1}^{(i)}} \dots z_n^{a_k^{(i)}} \quad (k = 0, 1, 2, \dots),$$

where Ω is the matrix defined by (6), and then define the power series

$$g_i(\mathbf{z}) = \sum_{k=0}^{\infty} P_i(\Omega^k \mathbf{z}) \quad (1 \le i \le s).$$

Then $f_i(z) = g_i(1, \dots, 1, z)$ and $g_i(\mathbf{z})$ satisfies the functional equation

$$g_i(\mathbf{z}) = g_i(\Omega \mathbf{z}) + P_i(\mathbf{z}) \quad (1 \le i \le s).$$

Letting

$$D_1 = z_1 \frac{\partial}{\partial z_1}, \; \dots, \; D_n = z_n \frac{\partial}{\partial z_n},$$

we see that $D_1^{k_1} \dots D_n^{k_n} g_i(\mathbf{z})$ $(k_1 + \dots + k_n = L)$ is a linear combination of $\{D_1^{l_1} \dots D_n^{l_n} g_i(\Omega \mathbf{z})\}_{l_1+\dots+l_n=L}$ over $\mathbb{Q}$ modulo $\mathbb{Q}[z_1, \dots, z_n]$. Hence

$\{D_1^{l_1}\ldots D_n^{l_n}g_i(\mathbf{z})\}_{k_1+\ldots+k_n\le L}$ satisfy the functional equation of the form (4) for any nonnegative integer L. By Lemma 4, the matrix Ω and $\boldsymbol{\alpha}=(1,\ldots,1,\alpha)$ have the properties (I)–(IV). If $\{f_i^{(l)}(\alpha)\}_{1\le i\le s,\,0\le l\le L}$ are algebraically dependent, then so are $\{D_n^l g_i(\boldsymbol{\alpha})\}_{1\le i\le s,\,0\le l\le L}$. It follows that $\{D_n^l g_i(\mathbf{z})\}_{1\le i\le s,\,0\le l\le L}$ are linearly dependent over $\mathbb{Q}$ modulo $\mathbb{Q}[z_1,\ldots,z_n]$ by Lemma 1. Thus there are rational numbers ξ_{il} $(1\le i\le s,\ 0\le l\le L)$, not all zero, such that

$$h(\mathbf{z})=\sum_{i=1}^{s}\sum_{l=0}^{L}\xi_{il}D_n^l g_i(\mathbf{z})\in\mathbb{Q}[z_1,\ldots,z_n].$$

Letting

$$R_i(X)=\sum_{l=0}^{L}\xi_{il}X^l\qquad(1\le i\le s),$$

we get

$$h(\mathbf{z})=\sum_{i=1}^{s}\sum_{k=0}^{\infty}R_i(a_k^{(i)})z_1^{a_{k+n-1}^{(i)}}\ldots z_n^{a_k^{(i)}}.$$

Put

$$S=\{i\in\{1,\ldots,s\}\mid R_i(X)\ne 0\}.$$

Then S is not empty. For any $i\in S$, $R_i(a_k^{(i)})\ne 0$ for all sufficiently large k, since $\{a_k^{(i)}\}_{k\ge 0}$ is strictly increasing ultimately. Hence, if S has only one element, $h(\mathbf{z})\notin\mathbb{Q}[z_1,\ldots,z_n]$. This is a contradiction. Suppose that S has at least two elements. Since $h(\mathbf{z})\in\mathbb{Q}[z_1,\ldots,z_n]$, there are distinct $i,j\in S$ such that $\{a_k^{(i)}\}_{k\ge 0}^{*}\cap\{a_k^{(j)}\}_{k\ge 0}^{*}$ is an infinite set, where the notation is the same as in Lemma 5, thereby we have $\{a_k^{(i)}\}_{k\ge 0}\sim\{a_k^{(j)}\}_{k\ge 0}$. This completes the proof of the theorem.

Proof of Theorem 2. Obviously (iii) implies (ii), and (ii) implies (i). We only have to prove that (i) implies (iii).

There exist multiplicatively independent algebraic numbers $\beta_1,\ldots,\beta_m$ with $0<|\beta_j|<1$ $(1\le j\le m)$ such that

$$\alpha_i=\zeta_i\prod_{j=1}^{m}\beta_j^{l_{ij}}\qquad(1\le i\le r),$$

where $\zeta_1,\ldots,\zeta_r$ are roots of unity and l_{ij} $(1\le i\le r, 1\le j\le m)$ are nonnegative integers (cf. Loxton and van der Poorten [3]). Let y_{jp} $(1\le j\le m, 1\le p\le n)$ be variables and let $\mathbf{y}=(y_{11},\ldots,y_{1n},\ldots,y_{m1},\ldots,y_{mn})$. Define

$$g_i(\mathbf{y})=\sum_{k=0}^{\infty}\zeta_i^{a_k}\prod_{j=1}^{m}(y_{j1}^{a_{k+n-1}}\ldots y_{jn}^{a_k})^{l_{ij}}\qquad(1\le i\le r).$$

Then we have

$$f(\alpha_i) = g_i(\underbrace{1,\dots,1}_{n-1},\beta_1,\dots,\underbrace{1,\dots,1}_{n-1},\beta_m) \qquad (1 \le i \le r).$$

Take a positive integer N such that $\zeta_i^N = 1$ for $i = 1,\dots,r$. We can choose a positive integer t and a nonnegative integer u such that $a_{k+t} \equiv a_k \pmod N$ for any $k \ge u$. Let

$$\Omega_1 = \begin{pmatrix} c_1 & 1 & 0 & \dots & 0 \\ c_2 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ & & & & 1 \\ c_n & 0 & & \dots & 0 \end{pmatrix} \tag{9}$$

and set

$$\Omega = \mathrm{diag}(\underbrace{\Omega_1^t,\dots,\Omega_1^t}_{m}). \tag{10}$$

It follows that

$$g_i(\Omega\mathbf{y}) = \sum_{k=0}^{\infty} \zeta_i^{a_k} \prod_{j=1}^{m} (y_{j1}^{a_{k+t+n-1}} \dots y_{jn}^{a_{k+t}})^{l_{ij}} \qquad (1 \le i \le r).$$

Let

$$\begin{aligned} h_i(\mathbf{y}) &= \sum_{k=u}^{\infty} \zeta_i^{a_k} \prod_{j=1}^{m} (y_{j1}^{a_{k+t+n-1}} \dots y_{jn}^{a_{k+t}})^{l_{ij}} \\ &= \sum_{k=t+u}^{\infty} \zeta_i^{a_k} \prod_{j=1}^{m} (y_{j1}^{a_{k+n-1}} \dots y_{jn}^{a_k})^{l_{ij}} \qquad (1 \le i \le r). \end{aligned}$$

Then

$$g_i(\mathbf{y}) - h_i(\mathbf{y}) = \sum_{k=0}^{t+u-1} \zeta_i^{a_k} \prod_{j=1}^{m} (y_{j1}^{a_{k+n-1}} \dots y_{jn}^{a_k})^{l_{ij}},$$

$$g_i(\Omega\mathbf{y}) - h_i(\mathbf{y}) = \sum_{k=0}^{u-1} \zeta_i^{a_k} \prod_{j=1}^{m} (y_{j1}^{a_{k+t+n-1}} \dots y_{jn}^{a_{k+t}})^{l_{ij}}.$$

Hence

$$g_i(\mathbf{y}) - g_i(\Omega\mathbf{y}) \in \overline{\mathbb{Q}}[\mathbf{y}] \qquad (1 \le i \le r). \tag{11}$$

For each i, there exists at least one of j such that $l_{ij} \ne 0$, since $|\alpha_i|$ is less than 1. Choosing such a j for each i and letting

$$D_{i1} = l_{ij}^{-1} y_{j1} \frac{\partial}{\partial y_{j1}}, \dots, D_{in} = l_{ij}^{-1} y_{jn} \frac{\partial}{\partial y_{jn}},$$

we see that $D_{i1}^{k_1}\dots D_{in}^{k_n}g_i(\mathbf{y})$ $(k_1+\dots+k_n=L)$ is a linear combination of $\{D_{i1}^{l_1}\dots D_{in}^{l_n}g_i(\Omega\mathbf{y})\}_{l_1+\dots+l_n=L}$ over $\mathbb{Q}$ modulo $\overline{\mathbb{Q}}[\mathbf{y}]$.

We shall verify that the matrix Ω defined by (10) and

$$\boldsymbol{\beta}=(\underbrace{1,\dots,1}_{n-1},\beta_1,\dots,\underbrace{1,\dots,1}_{n-1},\beta_m)$$

have the properties (I)–(IV). By the proof of Lemma 4, the matrix Ω_1 defined by (9) has the property (I), its eigenvalues $\varrho_1,\dots,\varrho_d$ satisfy $\varrho_1>\max\{|\varrho_2|,\dots,|\varrho_d|\}$, and ϱ_1 is a simple root of the characteristic polynomial of it. Hence Ω also has the properties (I) and (II). Put

$$\Omega^k\boldsymbol{\beta}=(\beta_{11}^{(k)},\dots,\beta_{1n}^{(k)},\dots,\beta_{m1}^{(k)},\dots,\beta_{mn}^{(k)})\qquad(k=0,1,2,\dots).$$

Define $\{a_k^{(i)}\}_{k\ge0}$ $(i=0,\dots,n-1)$ as in the proof of Lemma 4. Then we have

$$\beta_{jp}^{(k)}=\beta_j^{a_{kt}^{(n-p)}}\qquad(1\le j\le m,\ 1\le p\le n).$$

Since

$$a_{kt}^{(n-p)}=b^{(n-p)}(\varrho_1^t)^k+o((\varrho_1^t)^k)\qquad(1\le p\le n),$$

where $b^{(n-p)}>0$ for every p, Ω and $\boldsymbol{\beta}$ have the property (III). Assume that there exist mn integers $i_{11},\dots,i_{1n},\dots,i_{m1},\dots,i_{mn}$, not all zero, and positive integers a, b such that

$$\prod_{j=1}^{m}\prod_{p=1}^{n}{\beta_{jp}^{(k)}}^{i_{jp}}=1$$

for all $k=a+lb$ $(l=0,1,2,\dots)$. Let $\{a_k^{(j)}\}_{k\ge0}$ $(j=1,\dots,m)$ be linear recurrences defined by

$$a_{k+n}^{(j)}=c_1a_{k+n-1}^{(j)}+\dots+c_na_k^{(j)}\qquad(k=0,1,2,\dots)$$

with $a_0^{(j)}=i_{jn},\dots,a_{n-1}^{(j)}=i_{j1}$. Then

$$\prod_{j=1}^{m}\beta_j^{a_{kt}^{(j)}}=1$$

holds for all $k=a+lb$ $(l=0,1,2,\dots)$. Here $\{a_k^{(j)}\}_{k\ge0}$ is nonzero for at least one of j, and for such j there is a positive integer $k_0=a+l_0b$ $(l_0\in\mathbb{N}_0)$ such that $a_{k_0t}^{(j)}\ne0$ by Lemma 2. This contradicts the fact that $\beta_1,\dots,\beta_m$ are multiplicatively independent. Therefore the property (IV) is satisfied.

If $\{f^{(l)}(\alpha_i)\}_{1\le i\le r,\,0\le l\le L}$ are algebraically dependent, then so are $\{D_{in}^lg_i(\boldsymbol{\beta})\}_{1\le i\le r,\,0\le l\le L}$. Hence $\{D_{in}^lg_i(\mathbf{y})\}_{1\le i\le r,\,0\le l\le L}$ are linearly dependent over $\overline{\mathbb{Q}}$ modulo $\overline{\mathbb{Q}}[\mathbf{y}]$ by Lemma 1. Thus there are algebraic numbers

ξ_{il} $(1 \le i \le r,\ 0 \le l \le L)$, not all zero, such that

$$G(\mathbf{y}) = \sum_{i=1}^{r}\sum_{l=0}^{L} \xi_{il} D_{in}^{l} g_i(\mathbf{y}) \in \overline{\mathbb{Q}}[\mathbf{y}].$$

Letting

$$R_i(X) = \sum_{l=0}^{L} \xi_{il} X^l \qquad (1 \le i \le r),$$

we get

$$G(\mathbf{y}) = \sum_{i=1}^{r}\sum_{k=0}^{\infty} R_i(a_k)\zeta_i^{a_k} \prod_{j=1}^{m} (y_{j1}^{a_{k+n-1}} \ldots y_{jn}^{a_k})^{l_{ij}}.$$

Hence

$$G(\underbrace{1,\ldots,1}_{n-1}, y_1, \ldots, \underbrace{1,\ldots,1}_{n-1}, y_m) = \sum_{i=1}^{r}\sum_{k=0}^{\infty} R_i(a_k)\zeta_i^{a_k} \Big(\prod_{j=1}^{m} y_j^{l_{ij}}\Big)^{a_k} \in \overline{\mathbb{Q}}[y_1, \ldots, y_m]. \tag{12}$$

Put

$$S = \{i \in \{1, \ldots, r\} \mid R_i(X) \ne 0\}.$$

Then S is not empty. Suppose that $\lambda \in S$. Let

$$\{i_1, \ldots, i_s\} = \{i \in S \mid l_{ij} = l_{\lambda j}\ (1 \le j \le m)\}.$$

We assert that

$$\sum_{q=1}^{s} R_{i_q}(a_k)\zeta_{i_q}^{a_k} = 0 \tag{13}$$

for all sufficiently large k. To the contrary we assume that there exist infinitely many k such that (13) does not hold. Then by (12), there exist some index $\mu \in S \setminus \{i_1, \ldots, i_s\}$ and infinitely many pairs k_1, k_2 such that

$$\Big(\prod_{j=1}^{m} y_j^{l_{\lambda j}}\Big)^{a_{k_1}} = \Big(\prod_{j=1}^{m} y_j^{l_{\mu j}}\Big)^{a_{k_2}}.$$

Since $l_{\lambda j} a_{k_1} = l_{\mu j} a_{k_2}$ $(1 \le j \le m)$, either $l_{\lambda j} = l_{\mu j} = 0$ or $l_{\lambda j} l_{\mu j} > 0$ holds for each j. Put

$$T = \{j \in \{1, \ldots, m\} \mid l_{\lambda j} l_{\mu j} > 0\}.$$

Then T is not empty. For any $j \in T$, $\{l_{\lambda j} a_k\}_{k \ge 0} \sim \{l_{\mu j} a_k\}_{k \ge 0}$ by Lemma 5 and $l_{\lambda j}/l_{\mu j}$ is equal to a constant c. Hence there exists a nonnegative integer l such that

$$a_{k+l} = c a_k \qquad (k = 0, 1, 2, \ldots).$$

(We replace c by c^{-1} if necessary.) If $l=1$, then $a_k = a_0 c^k$ $(k=0,1,2,\ldots)$. This contradicts the assumption in the theorem. If we assume $l \geq 2$, then at least two of the roots of $\Psi(X) = X^l - c$ are those of $\Phi(X)$. This also contradicts the assumption, since the ratio of any pair of distinct roots of $\Psi(X)$ is a root of unity. Hence $l=0$ and so $c=1$. Therefore $l_{\lambda j} = l_{\mu j}$ $(1 \leq j \leq m)$, which contradicts the choice of μ. Hence (13) holds. Set

$$\gamma = \prod_{j=1}^{m} \beta_j^{l_{i_1 j}}.$$

Then γ is an algebraic number with $\alpha_{i_q} = \zeta_{i_q}\gamma$ $(1 \leq q \leq s)$. Let

$$L = \max_{1 \leq q \leq s} \deg R_{i_q}(X).$$

By (13), we have

$$\sum_{l=0}^{L} \Big(\sum_{q=1}^{s} \xi_{i_q l} \zeta_{i_q}^{a_k} \Big) a_k^l = 0$$

for all sufficiently large k, where $\xi_{i_q l} = 0$ if $l > \deg R_{i_q}$. We rewrite the above equation as follows:

$$\sum_{q=1}^{s} \xi_{i_q L} \zeta_{i_q}^{a_k} = -\sum_{l=0}^{L-1} \Big(\sum_{q=1}^{s} \xi_{i_q l} \zeta_{i_q}^{a_k} \Big) a_k^{l-L}.$$

Then the right-hand side converges to 0 as k tends to infinity, but the left-hand side takes only finitely many values. Therefore the left-hand side is equal to 0 for all sufficiently large k. This completes the proof of the theorem.

4. Examples

Example 1. Let $\{a_k^{(i)}\}_{k \geq 0}$ $(i = 1,2,3,4)$ be linear recurrences defined by

$$a_{k+3}^{(i)} = a_{k+2}^{(i)} + 16a_{k+1}^{(i)} + 20a_k^{(i)} \qquad (k=0,1,2,\ldots, i=1,2,3,4) \tag{14}$$

with

$$a_0^{(1)} = 1,\ a_1^{(1)} = 3,\ a_2^{(1)} = 33, \quad a_0^{(2)} = 0,\ a_1^{(2)} = 5,\ a_2^{(2)} = 29,$$
$$a_0^{(3)} = 2,\ a_1^{(3)} = 3,\ a_2^{(3)} = 29, \quad a_0^{(4)} = 1,\ a_1^{(4)} = 5,\ a_2^{(4)} = 25.$$

Then the polynomial

$$\Phi(X) = X^3 - X^2 - 16X - 20 = (X-5)(X+2)^2$$

satisfies the conditions in Theorem 1. By (14), we see that $\{a_k^{(i)}\}_{k \geq 0}$ is a strictly increasing sequence for each i. Hence $\{a_k^{(i)}\}_{k \geq 0} \not\sim \{a_k^{(j)}\}_{k \geq 0}$ $(1 \leq$

$i < j \le 4$). Define

$$f_1(z) = \sum_{k=0}^{\infty} z^{a_k^{(1)}} = \sum_{k=0}^{\infty} z^{5^k + k(-2)^k},$$

$$f_2(z) = \sum_{k=0}^{\infty} z^{a_k^{(2)}} = \sum_{k=0}^{\infty} z^{5^k + (k-1)(-2)^k},$$

$$f_3(z) = \sum_{k=0}^{\infty} z^{a_k^{(3)}} = \sum_{k=0}^{\infty} z^{5^k + (-2)^k},$$

$$f_4(z) = \sum_{k=0}^{\infty} z^{a_k^{(4)}} = \sum_{k=0}^{\infty} z^{5^k}.$$

If α is an algebraic number with $0 < |\alpha| < 1$, then $\{f_i^{(l)}(\alpha)\}_{1\le i\le 4,\, l\ge 0}$ are algebraically independent.

Example 2. Let $\{a_k\}_{k\ge 0}$ be a linear recurrence defined by

$$a_{k+3} = 2a_{k+2} + (m-1)(3m+1)a_{k+1} + 2m(m-1)^2 a_k \quad (k = 0, 1, 2, \ldots)$$

with

$$a_0 = 1, \quad a_1 = m+1, \quad a_2 = 6m^2 - 4m + 2,$$

where m is an integer greater than 2.

Since we have

$$a_k = (2m)^k + k(1-m)^k, \tag{15}$$

the conditions in Theorem 2 are satisfied. Define $f(z) = \sum_{k=0}^{\infty} z^{a_k}$ and set $\zeta = e^{2\pi\sqrt{-1}/m}$. If α is an algebraic number with $0 < |\alpha| < 1$, then $\{f^{(l)}(\zeta^j \alpha)\}_{j=0,\ldots,m-1,\, l\ge 0}$ are algebraically independent. In fact, if this is not the case, there are algebraic numbers $\xi_0, \ldots, \xi_{m-1}$, not all zero, such that

$$\sum_{j=0}^{m-1} \xi_j (\zeta^j)^{a_k} = 0 \tag{16}$$

for all sufficiently large k by Theorem 2. On the other hand, we see that $a_k \equiv k \pmod m$ for any $k \ge 1$ by (15). Therefore (16) holds only if $\xi_0 = \ldots = \xi_{m-1} = 0$. This is a contradiction.

For any given distinct algebraic numbers $\alpha_1, \ldots, \alpha_r$ with $0 < |\alpha_i| < 1$ ($i = 1, \ldots, r$), we can choose an integer m greater than 2 for which the linear recurrence $\{a_k\}_{k\ge 0}$ in this example does not have the property (iii) in Theorem 2. Then the values $\{f^{(l)}(\alpha_i)\}_{i=1,\ldots,r,\, l\ge 0}$ defined by the power series $f(z) = \sum_{k=0}^{\infty} z^{a_k}$ are algebraically independent.

References

[1] J. W. S. Cassels, *Local Fields*, Cambridge University Press, 1986.

[2] F. R. Gantmacher, *Applications of the Theory of Matrices*, Vol. II, Interscience, New York, 1959.

[3] J. H. Loxton and A. J. van der Poorten, *Algebraic independence properties of the Fredholm series*, J. Austral. Math. Soc. Ser. A 26 (1978), 31–45.

[4] K. Mahler, *Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen*, Math. Ann. 101 (1929), 342–366.

[5] D. W. Masser, *A vanishing theorem for power series*, Invent. Math. 67 (1982), 275–296.

[6] K. Nishioka, *Conditions for algebraic independence of certain power series of algebraic numbers*, Compositio Math. 62 (1987), 53–61.

[7] —, *Algebraic independence of Mahler functions and their values*, Tôhoku Math. J., to appear.

DEPARTMENT OF MATHEMATICS
KEIO UNIVERSITY
3-14-1, HIYOSHI, KOHOKU-KU
YOKOHAMA 223 JAPAN
E-mail: TAKAAKI@MATH.KEIO.AC.JP

Received on 20.3.1995 (2759)