Tanaka, T.
Osaka J. Math.
42 (2005), 487–497

ALGEBRAIC INDEPENDENCE OF THE VALUES OF POWER SERIES, LAMBERT SERIES, AND INFINITE PRODUCTS GENERATED BY LINEAR RECURRENCES

TAKA-AKI TANAKA

(Received January 5, 2004)

Abstract

In Theorem 1 of this paper, we establish the necessary and sufficient condition for the values of a power series, a Lambert series, and an infinite product generated by a linear recurrence at the same set of algebraic points to be algebraically dependent. In Theorem 4, from which Theorems 1–3 are deduced, we obtain an easily confirmable condition under which the values more general than those considered in Theorem 1 are algebraically independent, improving the method of [5].

1. Introduction and results

Let $\{a_k\}_{k\geq 0}$ be a linear recurrence of positive integers satisfying

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

where $c_1, \ldots, c_n$ are nonnegative integers with $c_n \neq 0$. We define a polynomial associated with (1) by

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

In this paper, we always assume that $\Phi(\pm 1) \neq 0$ and the ratio of any pair of distinct roots of $\Phi(X)$ is not a root of unity and that $\{a_k\}_{k\geq 0}$ is not a geometric progression.

In what follows, let

$$f(z) = \sum_{k=0}^{\infty} z^{a_k}, \quad g(z) = \sum_{k=0}^{\infty} \frac{z^{a_k}}{1 - z^{a_k}}, \quad h(z) = \prod_{k=0}^{\infty} (1 - z^{a_k})$$

and let $\mathbb{Q}$ and $\overline{\mathbb{Q}}$ denote the fields of rational and algebraic numbers, respectively. The author [5] proved the following theorem: Let $\alpha_1, \ldots, \alpha_r$ be algebraic numbers with $0 < |\alpha_i| < 1$ $(1 \leq i \leq r)$ such that none of α_i/α_j $(1 \leq i < j \leq r)$ is a root of unity. Then the $3r$ numbers $f(\alpha_i), g(\alpha_i), h(\alpha_i)$ $(1 \leq i \leq r)$ are algebraically independent.

On the other hand, the author [4] obtained the necessary and sufficient condition for the numbers $f(\alpha_1), \ldots, f(\alpha_r)$ to be algebraically dependent.

DEFINITION 1. We say that the algebraic numbers $\alpha_1, \dots, \alpha_r$ with $0 < |\alpha_i| < 1$ $(1 \le i \le r)$ are $\{a_k\}_{k\ge 0}$-*dependent* if there exist a non-empty subset $\{\alpha_{i_1}, \dots, \alpha_{i_t}\}$ of $\{\alpha_1, \dots, \alpha_r\}$, roots of unity $\zeta_1, \dots, \zeta_t$, an algebraic number γ with $\alpha_{i_l} = \zeta_l \gamma$ $(1 \le l \le t)$, and algebraic numbers $\xi_1, \dots, \xi_t$, not all zero, such that

$$\sum_{l=1}^{t} \xi_l \zeta_l^{a_k} = 0$$

for all sufficiently large k.

REMARK 1. If the algebraic numbers $\alpha_1, \dots, \alpha_r$ with $0 < |\alpha_i| < 1$ $(1 \le i \le r)$ are $\{a_k\}_{k\ge 0}$-dependent, then the numbers $1, f(\alpha_1), \dots, f(\alpha_r)$ are linearly dependent over $\overline{\mathbb{Q}}$, namely $\sum_{l=1}^{t} \xi_l f(\alpha_{i_l}) \in \overline{\mathbb{Q}}$.

The author [4] proved that the numbers $f(\alpha_1), \dots, f(\alpha_r)$ are algebraically dependent if and only if the algebraic numbers $\alpha_1, \dots, \alpha_r$ are $\{a_k\}_{k\ge 0}$-dependent. In this paper we establish the necessary and sufficient condition for the $3r$ numbers $f(\alpha_i), g(\alpha_i), h(\alpha_i)$ $(1 \le i \le r)$ to be algebraically dependent:

Theorem 1. *Let $\{a_k\}_{k\ge 0}$ be a linear recurrence satisfying* (1). *Let $\alpha_1, \dots, \alpha_r$ be algebraic numbers with $0 < |\alpha_i| < 1$ $(1 \le i \le r)$. Then the numbers $f(\alpha_i), g(\alpha_i)$, $h(\alpha_i)$ $(1 \le i \le r)$ are algebraically dependent if and only if the algebraic numbers $\alpha_1, \dots, \alpha_r$ are $\{a_k\}_{k\ge 0}$-dependent.*

Combining Theorem 1 and the above-mentioned result of [4], we immediately have the following:

Theorem 2. *Let $\alpha_1, \dots, \alpha_r$ be algebraic numbers with $0 < |\alpha_i| < 1$ $(1 \le i \le r)$. If the numbers $f(\alpha_1), \dots, f(\alpha_r)$ are algebraically independent, then so are the numbers $f(\alpha_i), g(\alpha_i), h(\alpha_i)$ $(1 \le i \le r)$.*

Theorem 2 implies the following:

Theorem 3. *Let $\alpha_1, \dots, \alpha_r$ be algebraic numbers with $0 < |\alpha_i| < 1$ $(1 \le i \le r)$. Then*

$$\begin{aligned} &\operatorname{trans.deg}_{\mathbb{Q}} \mathbb{Q}(f(\alpha_1), \dots, f(\alpha_r), g(\alpha_1), \dots, g(\alpha_r), h(\alpha_1), \dots, h(\alpha_r)) \\ &\ge 3 \operatorname{trans.deg}_{\mathbb{Q}} \mathbb{Q}(f(\alpha_1), \dots, f(\alpha_r)). \end{aligned} \tag{3}$$

The following is an example in which the equality of (3) holds:

EXAMPLE 1. Let $\{a_k\}_{k\geq 0}$ be a linear recurrence defined by

$$a_0 = 1, \quad a_1 = 2, \quad a_{k+2} = 3a_{k+1} + a_k \qquad (k = 0, 1, 2, \ldots).$$

We put

$$f(z) = \sum_{k=0}^{\infty} z^{a_k}, \quad g(z) = \sum_{k=0}^{\infty} \frac{z^{a_k}}{1 - z^{a_k}}, \quad h(z) = \prod_{k=0}^{\infty}(1 - z^{a_k}).$$

Let α be an algebraic number with $0 < |\alpha| < 1$ and let $\omega = e^{2\pi\sqrt{-1}/3} = (-1+\sqrt{-3})/2$. Since $a_{2k} \equiv 1 \pmod 3$ and $a_{2k+1} \equiv 2 \pmod 3$ for any $k \geq 0$, the numbers $\alpha, \omega\alpha$, and α^3 are not $\{a_k\}_{k\geq 0}$-dependent. Therefore the numbers $f(\alpha)$, $f(\omega\alpha)$, $f(\alpha^3)$, $g(\alpha)$, $g(\omega\alpha)$, $g(\alpha^3)$, $h(\alpha)$, $h(\omega\alpha)$, $h(\alpha^3)$ are algebraically independent by Theorem 1. Noting that $f(\alpha) + f(\omega\alpha) + f(\omega^2\alpha) = 0$, $g(\alpha) + g(\omega\alpha) + g(\omega^2\alpha) = 3g(\alpha^3)$ and $h(\alpha)h(\omega\alpha)h(\omega^2\alpha) = h(\alpha^3)$, we see that

$$\begin{aligned}
&\operatorname{trans.deg}_{\mathbb{Q}} \mathbb{Q}(f(\alpha), f(\omega\alpha), f(\omega^2\alpha), f(\alpha^3)) = 3,\\
&\operatorname{trans.deg}_{\mathbb{Q}} \mathbb{Q}(g(\alpha), g(\omega\alpha), g(\omega^2\alpha), g(\alpha^3)) = 3,\\
&\operatorname{trans.deg}_{\mathbb{Q}} \mathbb{Q}(h(\alpha), h(\omega\alpha), h(\omega^2\alpha), h(\alpha^3)) = 3,
\end{aligned}$$

and

$$\begin{aligned}
\operatorname{trans.deg}_{\mathbb{Q}} \mathbb{Q}(&f(\alpha), f(\omega\alpha), f(\omega^2\alpha), f(\alpha^3),\\
&g(\alpha), g(\omega\alpha), g(\omega^2\alpha), g(\alpha^3), h(\alpha), h(\omega\alpha), h(\omega^2\alpha), h(\alpha^3)) = 9.
\end{aligned}$$

As shown in the example above or in Remark 4 of [5], it seems complicated to state the necessary and sufficient condition for the values of the Lambert series $g(z)$ and the infinite product $h(z)$ at $\{a_k\}_{k\geq 0}$-dependent algebraic numbers $\alpha_1, \ldots, \alpha_r$ to be algebraically independent. In Theorem 4 below we establish an easily confirmable condition under which such values are algebraically independent.

DEFINITION 2. We say that the algebraic numbers $\alpha_1, \ldots, \alpha_r$ with $0 < |\alpha_i| < 1$ $(1 \leq i \leq r)$ are *strongly* $\{a_k\}_{k\geq 0}$*-dependent* if there exist a non-empty subset $\{\alpha_{i_1}, \ldots, \alpha_{i_t}\}$ of $\{\alpha_1, \ldots, \alpha_r\}$, N-th roots of unity $\zeta_1, \ldots, \zeta_t$, an algebraic number γ with $\alpha_{i_l} = \zeta_l\gamma$ $(1 \leq l \leq t)$, and algebraic numbers $\xi_1, \ldots, \xi_t$, not all zero, such that

$$\sum_{l=1}^{t} \xi_l \zeta_l^{ma_k} = 0, \qquad m = 1, \ldots, N-1, \qquad \text{g.c.d.}(m, N) = 1,$$

for all sufficiently large k.

It is clear that, if the algebraic numbers $\alpha_1, \ldots, \alpha_r$ with $0 < |\alpha_i| < 1$ $(1 \leq i \leq r)$ are strongly $\{a_k\}_{k\geq 0}$-dependent, then they are $\{a_k\}_{k\geq 0}$-dependent.

The following theorem is more precise than Theorem 2 above.

Theorem 4. *Let $\{a_k\}_{k\ge 0}$ be a linear recurrence satisfying* (1). *Let $\alpha_1,\dots,\alpha_r$ be algebraic numbers with $0<|\alpha_i|<1$ $(1\le i\le r)$. Suppose that the algebraic numbers $\alpha_1,\dots,\alpha_r$ are not strongly $\{a_k\}_{k\ge 0}$-dependent. Assume further that $\alpha_1,\dots,\alpha_\rho$ $(\rho\le r)$ are not $\{a_k\}_{k\ge 0}$-dependent or equivalently that the numbers $f(\alpha_1),\dots,f(\alpha_\rho)$ are algebraically independent. Then the numbers $f(\alpha_1),\dots,f(\alpha_\rho), g(\alpha_1),\dots,g(\alpha_r), h(\alpha_1),\dots, h(\alpha_r)$ are algebraically independent.*

Using Theorem 4, we have an example in which the strict inequality of (3) holds:

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

$$a_0=1,\quad a_1=3,\quad a_{k+2}=3a_{k+1}+a_k \qquad (k=0,1,2,\dots).$$

We put

$$f(z)=\sum_{k=0}^{\infty} z^{a_k},\quad g(z)=\sum_{k=0}^{\infty}\frac{z^{a_k}}{1-z^{a_k}},\quad h(z)=\prod_{k=0}^{\infty}(1-z^{a_k}).$$

Let α be an algebraic number with $0<|\alpha|<1$ and let $\omega=e^{2\pi\sqrt{-1}/3}=(-1+\sqrt{-3})/2$. Since $a_{2k}\equiv 1 \pmod 3$ and $a_{2k+1}\equiv 0 \pmod 3$ for any $k\ge 0$, the numbers $\alpha,\omega\alpha,\omega^2\alpha$ and α^3 are not strongly $\{a_k\}_{k\ge 0}$-dependent and the numbers $\alpha,\omega\alpha$ and α^3 are not $\{a_k\}_{k\ge 0}$-dependent. Therefore the numbers $f(\alpha), f(\omega\alpha), f(\alpha^3), g(\alpha), g(\omega\alpha), g(\omega^2\alpha), g(\alpha^3), h(\alpha), h(\omega\alpha), h(\omega^2\alpha), h(\alpha^3)$ are algebraically independent by Theorem 4 with $\rho=3$ and $r=4$. Noting that $\omega f(\alpha)-(\omega+1)f(\omega\alpha)+f(\omega^2\alpha)=0$, we see that

$$\begin{aligned}
&\operatorname{trans.deg}_{\mathbb{Q}}\mathbb{Q}(f(\alpha), f(\omega\alpha), f(\omega^2\alpha), f(\alpha^3))=3,\\
&\operatorname{trans.deg}_{\mathbb{Q}}\mathbb{Q}(f(\alpha), f(\omega\alpha), f(\omega^2\alpha), f(\alpha^3),\\
&\qquad g(\alpha), g(\omega\alpha), g(\omega^2\alpha), g(\alpha^3), h(\alpha), h(\omega\alpha), h(\omega^2\alpha), h(\alpha^3))=11,
\end{aligned}$$

and so

$$\begin{aligned}
&\operatorname{trans.deg}_{\mathbb{Q}}\mathbb{Q}(f(\alpha), f(\omega\alpha), f(\omega^2\alpha), f(\alpha^3),\\
&\qquad g(\alpha), g(\omega\alpha), g(\omega^2\alpha), g(\alpha^3), h(\alpha), h(\omega\alpha), h(\omega^2\alpha), h(\alpha^3))\\
&> 3\operatorname{trans.deg}_{\mathbb{Q}}\mathbb{Q}(f(\alpha), f(\omega\alpha), f(\omega^2\alpha), f(\alpha^3)).
\end{aligned}$$

2. Lemmas

Let $F(z_1,\dots,z_n)$ and $F[[z_1,\dots,z_n]]$ denote the field of rational functions and the ring of formal power series in the variables $z_1,\dots,z_n$ with coefficients in a field F, respectively, and $F^\times$ the multiplicative group of nonzero elements of F. 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 [1, p.66, Theorem 3]). If $\boldsymbol{z} = (z_1, \dots, z_n)$ is a point of $\mathbb{C}^n$ with $\mathbb{C}$ the set of complex numbers, we define the transformation $\Omega\colon \mathbb{C}^n \to \mathbb{C}^n$ by

$$\Omega\boldsymbol{z} = \left(\prod_{j=1}^{n} z_j{}^{\omega_{1j}}, \prod_{j=1}^{n} z_j{}^{\omega_{2j}}, \dots, \prod_{j=1}^{n} z_j{}^{\omega_{nj}}\right). \tag{4}$$

We suppose that 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 non-singular and none of its eigenvalues is a root of unity, so that in particular $\rho > 1$.

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

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

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

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

(IV) For any nonzero $f(\boldsymbol{z}) \in \mathbb{C}[[z_1, \dots, z_n]]$ which converges in some neighborhood of the origin, there are infinitely many positive integers k such that $f(\Omega^k\boldsymbol{\alpha}) \neq 0$.

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.

Lemma 1 (Tanaka [4, Lemma 4, Proof of Theorem 2]). *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, where* $\Phi(X)$ *is the polynomial defined by* (2). *Let*

$$\Omega = \begin{pmatrix} c_1 & 1 & 0 & \cdots & 0 \\ c_2 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ \vdots & \vdots & & \ddots & 1 \\ c_n & 0 & \cdots & \cdots & 0 \end{pmatrix} \tag{5}$$

and let $\beta_1, \dots, \beta_s$ *be multiplicatively independent algebraic numbers with* $0 < |\beta_j| < 1$ $(1 \le j \le s)$. *Let* p *be a positive integer and put*

$$\Omega' = \mathrm{diag}(\underbrace{\Omega^p, \dots, \Omega^p}_{s}).$$

Then the matrix Ω' *and the point*

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

have the properties (I)–(IV).

Lemma 2 (Kubota [2], see also Nishioka [3]). *Let K be an algebraic number field. Suppose that $f_1(\boldsymbol{z}), \dots, f_m(\boldsymbol{z}) \in K[[z_1, \dots, z_n]]$ converge in an n-polydisc U around the origin and satisfy the functional equations*

$$f_i(\Omega \boldsymbol{z}) = a_i(\boldsymbol{z}) f_i(\boldsymbol{z}) + b_i(\boldsymbol{z}) \qquad (1 \le i \le m),$$

where $a_i(\boldsymbol{z}), b_i(\boldsymbol{z}) \in K(z_1, \dots, z_n)$ and $a_i(\boldsymbol{z})$ $(1 \le i \le m)$ are defined and nonzero at the origin. Assume that the $n \times n$ matrix Ω and a point $\boldsymbol{\alpha} \in U$ whose components are nonzero algebraic numbers have the properties (I)–(IV) *and that $a_i(\boldsymbol{z})$ $(1 \le i \le m)$ are defined and nonzero at $\Omega^k \boldsymbol{\alpha}$ for all $k \ge 0$. If $f_1(\boldsymbol{z}), \dots, f_m(\boldsymbol{z})$ are algebraically independent over $K(z_1, \dots, z_n)$, then the values $f_1(\boldsymbol{\alpha}), \dots, f_m(\boldsymbol{\alpha})$ are algebraically independent.*

Lemma 2 is essentially due to Kubota [2] and improved by Nishioka [3].

In what follows, C denotes a field of characteristic 0. Let $L = C(z_1, \dots, z_n)$ and let M be the quotient field of $C[[z_1, \dots, z_n]]$. Let Ω be an $n \times n$ matrix with nonnegative integer entries having the property (I). We define an endomorphism $\tau : M \to M$ by

$$f^\tau(\boldsymbol{z}) = f(\Omega \boldsymbol{z}) \qquad (f(\boldsymbol{z}) \in M)$$

and a subgroup H of $L^\times$ by

$$H = \{g^\tau g^{-1} \mid g \in L^\times\}.$$

Lemma 3 (Kubota [2], see also Nishioka [3]). *Let $f_i \in M$ $(i = 1, \dots, h)$ satisfy*

$$f_i^\tau = f_i + b_i,$$

where $b_i \in L$ $(1 \le i \le h)$, and let $f_i \in M^\times$ $(i = h+1, \dots, m)$ satisfy

$$f_i^\tau = a_i f_i,$$

where $a_i \in L^\times$ $(h+1 \le i \le m)$. Suppose that a_i and b_i have the following properties:
(i) *If $c_i \in C$ $(1 \le i \le h)$ are not all zero, there is no element g of L such that*

$$g - g^\tau = \sum_{i=1}^{h} c_i b_i.$$

(ii) *$a_{h+1}, \dots, a_m$ are multiplicatively independent modulo H.*
Then the functions f_i $(1 \le i \le m)$ are algebraically independent over L.

Let $\{a_k\}_{k\geq 0}$ be a linear recurrence satisfying (1) with the conditions stated in the beginning of this paper. We define a monomial

$$P(\boldsymbol{z}) = z_1^{a_{n-1}} \cdots z_n^{a_0}, \tag{6}$$

which is denoted similarly to (4) by

$$P(\boldsymbol{z}) = (a_{n-1}, \ldots, a_0)\boldsymbol{z}. \tag{7}$$

Let Ω be the matrix defined by (5). It follows from (1), (4), and (7) that

$$P(\Omega^k \boldsymbol{z}) = z_1^{a_{k+n-1}} \cdots z_n^{a_k} \qquad (k \geq 0).$$

In what follows, let $\overline{C}$ be an algebraically closed field of characteristic 0.

Lemma 4 (Tanaka [5]). *Suppose that $G(\boldsymbol{z}) \in \overline{C}[[z_1, \ldots, z_n]]$ satisfies the functional equation of the form*

$$G(\boldsymbol{z}) = \alpha G(\Omega^p \boldsymbol{z}) + \sum_{k=q}^{p+q-1} Q_k(P(\Omega^k \boldsymbol{z})),$$

where $\alpha \neq 0$ is an element of $\overline{C}$, Ω is defined by (5), *$p > 0$, $q \geq 0$ are integers, and $Q_k(X) \in \overline{C}(X)$ $(q \leq k \leq p+q-1)$ are defined at $X = 0$. If $G(\boldsymbol{z}) \in \overline{C}(z_1, \ldots, z_n)$, then $G(\boldsymbol{z}) \in \overline{C}$ and $Q_k(X) \in \overline{C}$ $(q \leq k \leq p+q-1)$.*

Lemma 5 (Tanaka [5]). *Suppose that $G(\boldsymbol{z})$ is an element of the quotient field of $\overline{C}[[z_1, \ldots, z_n]]$ satisfying the functional equation of the form*

$$G(\boldsymbol{z}) = \left(\prod_{k=q}^{p+q-1} Q_k(P(\Omega^k \boldsymbol{z})) \right) G(\Omega^p \boldsymbol{z}),$$

where Ω, p, q, and $Q_k(X)$ are as in Lemma 4. *Assume that $Q_k(0) \neq 0$. If $G(\boldsymbol{z}) \in \overline{C}(z_1, \ldots, z_n)$, then $G(\boldsymbol{z}) \in \overline{C}$ and $Q_k(X) \in \overline{C}^{\times}$ $(q \leq k \leq p+q-1)$.*

3. Proof of Theorems 1 and 4

Proof of Theorem 1. If the algebraic numbers $\alpha_1, \ldots, \alpha_r$ are $\{a_k\}_{k\geq 0}$-dependent, then the numbers $f(\alpha_i), g(\alpha_i), h(\alpha_i)$ $(1 \leq i \leq r)$ are algebraically dependent, since so are the numbers $f(\alpha_i)$ $(1 \leq i \leq r)$ by Remark 1. Conversely, if the algebraic numbers $\alpha_1, \ldots, \alpha_r$ are not $\{a_k\}_{k\geq 0}$-dependent, then by Theorem 4 with $\rho = r$ the numbers $f(\alpha_i), g(\alpha_i), h(\alpha_i)$ $(1 \leq i \leq r)$ are algebraically independent. This completes the proof of the theorem. □

Proof of Theorem 4. Suppose on the contrary that the numbers $f(\alpha_1),\dots,f(\alpha_\rho)$, $g(\alpha_1),\dots,g(\alpha_r),h(\alpha_1),\dots,h(\alpha_r)$ are algebraically dependent. There exist multiplicatively independent algebraic numbers $\beta_1,\dots,\beta_s$ with $0<|\beta_j|<1$ $(1\le j\le s)$ such that

$$\alpha_i=\zeta_i\prod_{j=1}^{s}\beta_j^{e_{ij}}\qquad(1\le i\le r), \tag{8}$$

where $\zeta_1,\dots,\zeta_r$ are roots of unity and e_{ij} $(1\le i\le r,\ 1\le j\le s)$ are nonnegative integers (cf. Nishioka [3, Lemma 3.4.9]). Take a positive integer N such that $\zeta_i^N=1$ for any i $(1\le i\le r)$. We can choose a positive integer p and a nonnegative integer q such that $a_{k+p}\equiv a_k \pmod N$ for any $k\ge q$. Let $y_{j\lambda}$ $(1\le j\le s,\ 1\le\lambda\le n)$ be variables and let $\boldsymbol{y}_j=(y_{j1},\dots,y_{jn})$ $(1\le j\le s)$, $\boldsymbol{y}=(\boldsymbol{y}_1,\dots,\boldsymbol{y}_s)$. Define

$$f_i(\boldsymbol{y})=\sum_{k=q}^{\infty}\zeta_i^{a_k}\prod_{j=1}^{s}P(\Omega^k\boldsymbol{y}_j)^{e_{ij}}\qquad(1\le i\le\rho),$$

$$g_i(\boldsymbol{y})=\sum_{k=q}^{\infty}\frac{\zeta_i^{a_k}\prod_{j=1}^{s}P(\Omega^k\boldsymbol{y}_j)^{e_{ij}}}{1-\zeta_i^{a_k}\prod_{j=1}^{s}P(\Omega^k\boldsymbol{y}_j)^{e_{ij}}}\qquad(1\le i\le r),$$

and

$$h_i(\boldsymbol{y})=\prod_{k=q}^{\infty}\left(1-\zeta_i^{a_k}\prod_{j=1}^{s}P(\Omega^k\boldsymbol{y}_j)^{e_{ij}}\right)\qquad(1\le i\le r),$$

where $P(\boldsymbol{z})$ and Ω are defined by (6) and (5), respectively. Letting

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

we see by (8) that

$$f_i(\boldsymbol{\beta})=\sum_{k=q}^{\infty}\alpha_i^{a_k},\quad g_i(\boldsymbol{\beta})=\sum_{k=q}^{\infty}\frac{\alpha_i^{a_k}}{1-\alpha_i^{a_k}},\quad h_i(\boldsymbol{\beta})=\prod_{k=q}^{\infty}(1-\alpha_i^{a_k}).$$

Hence the values $f_1(\boldsymbol{\beta}),\dots,f_\rho(\boldsymbol{\beta}),g_1(\boldsymbol{\beta}),\dots,g_r(\boldsymbol{\beta}),h_1(\boldsymbol{\beta}),\dots,h_r(\boldsymbol{\beta})$ are algebraically dependent. Let

$$\Omega'=\mathrm{diag}(\underbrace{\Omega^p,\dots,\Omega^p}_{s}).$$

Then $f_1(\boldsymbol{y}),\dots,f_\rho(\boldsymbol{y}),g_1(\boldsymbol{y}),\dots,g_r(\boldsymbol{y}),h_1(\boldsymbol{y}),\dots,h_r(\boldsymbol{y})$ satisfy the functional equations

$$f_i(\boldsymbol{y}) = f_i(\Omega'\boldsymbol{y}) + \sum_{k=q}^{p+q-1} \zeta_i^{a_k} \prod_{j=1}^{s} P(\Omega^k \boldsymbol{y}_j)^{e_{ij}},$$

$$g_i(\boldsymbol{y}) = g_i(\Omega'\boldsymbol{y}) + \sum_{k=q}^{p+q-1} \frac{\zeta_i^{a_k} \prod_{j=1}^{s} P(\Omega^k \boldsymbol{y}_j)^{e_{ij}}}{1 - \zeta_i^{a_k} \prod_{j=1}^{s} P(\Omega^k \boldsymbol{y}_j)^{e_{ij}}},$$

and

$$h_i(\boldsymbol{y}) = \left(\prod_{k=q}^{p+q-1} \left(1 - \zeta_i^{a_k} \prod_{j=1}^{s} P(\Omega^k \boldsymbol{y}_j)^{e_{ij}} \right) \right) h_i(\Omega'\boldsymbol{y}),$$

where $\Omega'\boldsymbol{y} = (\Omega^p \boldsymbol{y}_1, \dots, \Omega^p \boldsymbol{y}_s)$. By Lemmas 1 and 2 the functions $f_1(\boldsymbol{y}), \dots, f_\rho(\boldsymbol{y})$, $g_1(\boldsymbol{y}), \dots, g_r(\boldsymbol{y}), h_1(\boldsymbol{y}), \dots, h_r(\boldsymbol{y})$ are algebraically dependent over $\overline{\mathbb{Q}}(\boldsymbol{y})$. Hence by Lemma 3 at least one of the following two cases arises:

(i) There are algebraic numbers $b_1, \dots, b_\rho, c_1, \dots, c_r$, not all zero, and $F(\boldsymbol{y}) \in \overline{\mathbb{Q}}(\boldsymbol{y})$ such that

$$\begin{aligned} F(\boldsymbol{y}) &= F(\Omega'\boldsymbol{y}) \\ &\quad + \sum_{k=q}^{p+q-1} \left(\sum_{i=1}^{\rho} b_i \zeta_i^{a_k} \prod_{j=1}^{s} P(\Omega^k \boldsymbol{y}_j)^{e_{ij}} + \sum_{i=1}^{r} \frac{c_i \zeta_i^{a_k} \prod_{j=1}^{s} P(\Omega^k \boldsymbol{y}_j)^{e_{ij}}}{1 - \zeta_i^{a_k} \prod_{j=1}^{s} P(\Omega^k \boldsymbol{y}_j)^{e_{ij}}} \right). \end{aligned} \tag{9}$$

(ii) There are rational integers d_i $(1 \le i \le r)$, not all zero, and $G(\boldsymbol{y}) \in \overline{\mathbb{Q}}(\boldsymbol{y}) \setminus \{0\}$ such that

$$G(\boldsymbol{y}) = \left(\prod_{k=q}^{p+q-1} \prod_{i=1}^{r} \left(1 - \zeta_i^{a_k} \prod_{j=1}^{s} P(\Omega^k \boldsymbol{y}_j)^{e_{ij}} \right)^{d_i} \right) G(\Omega'\boldsymbol{y}). \tag{10}$$

Let M be a positive integer and let

$$\boldsymbol{y}_j = (y_{j1}, \dots, y_{jn}) = (z_1^{M^j}, \dots, z_n^{M^j}) \qquad (1 \le j \le s),$$

where M is so large that the following two properties are both satisfied:

(A) If $(e_{i1}, \dots, e_{is}) \neq (e_{i'1}, \dots, e_{i's})$, then $\sum_{j=1}^{s} e_{ij} M^j \neq \sum_{j=1}^{s} e_{i'j} M^j$.

(B) $F^*(\boldsymbol{z}) = F(z_1^M, \dots, z_n^M, \dots, z_1^{M^s}, \dots, z_n^{M^s}) \in \overline{\mathbb{Q}}(z_1, \dots, z_n)$, $G^*(\boldsymbol{z}) = G(z_1^M, \dots, z_n^M, \dots, z_1^{M^s}, \dots, z_n^{M^s}) \in \overline{\mathbb{Q}}(z_1, \dots, z_n) \setminus \{0\}$.

Then by (9) and (10), at least one of the following two functional equations holds:

$$F^*(\boldsymbol{z}) = F^*(\Omega^p \boldsymbol{z}) + \sum_{k=q}^{p+q-1} \left(\sum_{i=1}^{\rho} b_i \zeta_i^{a_k} P(\Omega^k \boldsymbol{z})^{E_i} + \sum_{i=1}^{r} \frac{c_i \zeta_i^{a_k} P(\Omega^k \boldsymbol{z})^{E_i}}{1 - \zeta_i^{a_k} P(\Omega^k \boldsymbol{z})^{E_i}} \right), \tag{11}$$

$$G^*(z) = \left(\prod_{k=q}^{p+q-1} \prod_{i=1}^{r} \left(1 - \zeta_i^{a_k} P(\Omega^k z)^{E_i}\right)^{d_i} \right) G^*(\Omega^p z), \tag{12}$$

where $E_i = \sum_{j=1}^{s} e_{ij} M^j > 0$ $(1 \le i \le r)$. By Lemmas 4, 5, and the property (B), at least one of the following two properties are satisfied:
(i) For any k $(q \le k \le p + q - 1)$,

$$\begin{aligned} &\sum_{i=1}^{\rho} b_i \zeta_i^{a_k} X^{E_i} + \sum_{i=1}^{r} \frac{c_i \zeta_i^{a_k} X^{E_i}}{1 - \zeta_i^{a_k} X^{E_i}} \\ &= \sum_{i=1}^{\rho} b_i \zeta_i^{a_k} X^{E_i} + \sum_{i=1}^{r} c_i \sum_{h=1}^{\infty} (\zeta_i^{a_k} X^{E_i})^h \in \overline{\mathbb{Q}}. \end{aligned} \tag{13}$$

(ii) For any k $(q \le k \le p + q - 1)$,

$$\prod_{i=1}^{r} (1 - \zeta_i^{a_k} X^{E_i})^{d_i} = \gamma_k \in \overline{\mathbb{Q}}^{\times}. \tag{14}$$

Suppose first that (11) is satisfied with $c_i = 0$ $(1 \le i \le r)$. Let $S = \{i \in \{1, \dots, \rho\} \mid b_i \ne 0\}$ and let $\{i_1, \dots, i_t\}$ be a subset of S such that $E_{i_1} = \cdots = E_{i_t}$ and $E_{i_1} < E_j$ for any $j \in S \setminus \{i_1, \dots, i_t\}$. Then by (13)

$$\sum_{l=1}^{t} b_{i_l} \zeta_{i_l}^{a_k} = 0 \qquad (q \le k \le p + q - 1)$$

and hence

$$\sum_{l=1}^{t} b_{i_l} \zeta_{i_l}^{a_k} = 0 \qquad (k \ge q)$$

since $a_{k+p} \equiv a_k \pmod N$ for any $k \ge q$. By the property (A), $E_{i_1} = \cdots = E_{i_t}$ implies $(e_{i_1 1}, \dots, e_{i_1 s}) = \cdots = (e_{i_t 1}, \dots, e_{i_t s})$. Putting $\gamma = \prod_{j=1}^{s} \beta_j^{e_{i_1 j}}$, we have $\alpha_{i_l} = \zeta_{i_l} \gamma$ $(1 \le l \le t)$ by (8). Therefore the algebraic numbers $\alpha_1, \dots, \alpha_\rho$ are $\{a_k\}_{k \ge 0}$-dependent, which contradicts the assumption.

Secondly suppose that (11) is satisfied with $c_1, \dots, c_r$ not all zero. Let $T = \{i \in \{1, \dots, r\} \mid c_i \ne 0\}$ and let $\{i_1, \dots, i_u\}$ be a subset of T such that $E_{i_1} = \cdots = E_{i_u}$ and $E_{i_1} < E_j$ for any $j \in T \setminus \{i_1, \dots, i_u\}$. Let m be any integer with $0 \le m \le N - 1$ such that g.c.d.$(m, N) = 1$. By Dirichlet's theorem on arithmetical progressions, there exists a prime number P_m such that $P_m \equiv m \pmod N$ and $P_m > \max_{1 \le i \le r} E_i$. Since $P_m E_{i_1}$ is not divided by any E_j with $j \in T \setminus \{i_1, \dots, i_u\}$, the term $\sum_{l=1}^{u} c_{i_l} (\zeta_{i_l}^{a_k} X^{E_{i_1}})^{P_m}$ must vanish in (13). Hence

$$\sum_{l=1}^{u} c_{i_l}\zeta_{i_l}^{ma_k} = 0 \qquad (q \le k \le p+q-1)$$

and so the algebraic numbers $\alpha_1, \dots, \alpha_r$ are strongly $\{a_k\}_{k\ge 0}$-dependent, which contradicts the assumption.

Finally suppose that (12) is satisfied. Taking the logarithmic derivative of (14), we get

$$\sum_{i=1}^{r} \frac{-d_i E_i \zeta_i^{a_k} X^{E_i-1}}{1-\zeta_i^{a_k} X^{E_i}} = 0 \qquad (q \le k \le p+q-1)$$

and so

$$\sum_{i=1}^{r} \frac{d_i E_i \zeta_i^{a_k} X^{E_i}}{1-\zeta_i^{a_k} X^{E_i}} = \sum_{i=1}^{r} d_i E_i \sum_{h=1}^{\infty} (\zeta_i^{a_k} X^{E_i})^h = 0 \qquad (q \le k \le p+q-1).$$

Therefore the algebraic numbers $\alpha_1, \dots, \alpha_r$ are strongly $\{a_k\}_{k\ge 0}$-dependent also in this case by the same way as above. This completes the proof of the theorem. $\square$

References

[1] F.R. Gantmacher: Applications of the Theory of Matrices, Interscience, New York, 1959.

[2] K.K. Kubota: *On the algebraic independence of holomorphic solutions of certain functional equations and their values*, Math. Ann. **227** (1977), 9–50.

[3] K. Nishioka: Mahler Functions and Transcendence, Lecture Notes in Mathematics **1631**, Springer-Verlag, Berlin, 1996.

[4] T. Tanaka: *Algebraic independence of the values of power series generated by linear recurrences*, Acta Arith. **74** (1996), 177–190.

[5] T. Tanaka: *Algebraic independence results related to linear recurrences*, Osaka J. Math. **36** (1999), 203–227.

Department of Mathematics
Keio University
Hiyoshi 3-14-1, Kohoku-ku
Yokohama 223-8522, Japan
e-mail: takaaki@math.keio.ac.jp