COMPOSITIO MATHEMATICA

KUMIKO NISHIOKA

Algebraic independence by Mahler's method and S-unit equations

Compositio Mathematica, tome 92, nº 1 (1994), p. 87-110
<http://www.numdam.org/item?id=CM_1994__92_1_87_0>

Compositio Mathematica **92**: 87–110, 1994.

Algebraic independence by Mahler's method and *S*-unit equations

KUMIKO NISHIOKA
College of Humanities and Sciences, Nihon University, Tokyo, Japan

Received 13 November 1992; accepted in final form 29 May 1993

1. Introduction

Let $\Omega = (o_{ij})$ be an $n \times n$ matrix with nonnegative integer entries. If $z = (z_1, \ldots, z_n)$ is a point of $\mathbb{C}^n$, we define a transformation $\Omega: \mathbb{C}^n \to \mathbb{C}^n$ by

$$\Omega z = \left(\prod_{j=1}^{n} z_j^{o_{1j}}, \ldots, \prod_{j=1}^{n} z_j^{o_{nj}} \right).$$

Let K be an algebraic number field and $f_1(z), \ldots, f_m(z)$ convergent power series of n variables with coefficients in K. We say that $f_1(z), \ldots, f_m(z)$ are Mahler functions if they satisfy

$$\begin{pmatrix} f_1(z) \\ f_2(z) \\ \vdots \\ f_m(z) \end{pmatrix} = A(z) \begin{pmatrix} f_1(\Omega z) \\ f_2(\Omega z) \\ \vdots \\ f_m(\Omega z) \end{pmatrix} + B(z),$$

where $A(z)$ and $B(z)$ are respectively an $n \times n$ matrix and an n-dimensional vector with entries in the rational function field $K(z) = K(z_1, \ldots, z_n)$. Mahler [11], [12], [13] started to study the algebraic independence of the values $f_1(\alpha), \ldots, f_m(\alpha)$ at an algebraic point $\alpha = (\alpha_1, \ldots, \alpha_n)$ and later Kubota [5], Loxton and van der Poorten [6–10] extended Mahler's method. It is our aim here to give an extension in another direction by using Evertse's theorem [3] on S-unit equations. Before mentioning our results, we shall briefly summarize the results which have been obtained up to now. In case $n = 1$, the following theorem is proved by using Nesterenko's method [15].

THEOREM A. *Suppose that $\Omega = (d)$ with a single entry $d > 1$. Let α be an algebraic number such that $0 < |\alpha| < 1$, $A(\alpha^{d^k})$, $B(\alpha^{d^k})$ are defined and $A(\alpha^{d^k})$ is non-singular for all $k \geqq 0$, and $f_1(\alpha), \ldots, f_m(\alpha)$ converge. Then we have*

$$\begin{aligned}&\operatorname{tr.deg}_{\mathbb{Q}} \mathbb{Q}(f_1(\alpha), \ldots, f_m(\alpha))\\ &\quad = \operatorname{tr.deg}_{K(z)} K(z)(f_1(z), \ldots, f_m(z))\\ &\quad (= \operatorname{tr.deg}_{\mathbb{C}(z)} \mathbb{C}(z)(f_1(z), \ldots, f_m(z))).\end{aligned}$$

Further in Amou [1], Becker [2], Nishioka [16], [17], [18], the algebraic independence measures and the algebraic independence at a transcendental number are studied. For the general case $n \geqq 2$, we can only treat diagonal matrices as $A(z)$. Summarizing the results by Kubota, Loxton and van der Poorten, we have the following. Let Ω be a nonsingular matrix such that none of its eigenvalues is a root of unity, and ρ the maximum of the absolute values of the eigenvalues of Ω. Then $\rho > 1$ and ρ is an eigenvalue of Ω (see [4]). We suppose that all the eigenvalues of modulus ρ are simple roots of the minimal polynomial of Ω. Let

$$A(z) = \begin{pmatrix} a_1(z) & 0 & \cdots & 0 \\ 0 & a_2(z) & \cdots & 0 \\ & & \vdots & \\ 0 & 0 & \cdots & a_m(z) \end{pmatrix},$$

each $a_i(z)$ defined and nonzero at $z = 0$.

THEOREM B. *Suppose that* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *is an algebraic point which satisfies the following three properties.*

(i) *None of* α_i *is zero,* $A(z)$ *and* $B(z)$ *are defined at* $\Omega^k\alpha$, $A(\Omega^k\alpha)$ *is nonsingular for all* $k \geqq 0$, *and* $f_1(z), \ldots, f_m(z)$ *converge at* α.

(ii) *For all sufficiently large* $k \in \mathbb{N}$,

$$\log |\alpha_i^{(k)}| \leqq -c\rho^k, \; 1 \leqq i \leqq n,$$

where $\Omega^k\alpha = (\alpha_1^{(k)}, \ldots, \alpha_n^{(k)})$ *and* c *is a positive constant.*

(iii) *If* $f(z)$ *is a convergent power series with complex coefficients such that* $f(\Omega^k\alpha) = 0$ *for all sufficiently large* $k \in \mathbb{N}$, *then* $f(z) \equiv 0$.

If $f_1(z), \ldots, f_m(z)$ *are algebraically independent over* $K(z)$, *then* $f_1(\alpha), \ldots, f_m(\alpha)$ *are algebraically independent.*

In connection with assumption (iii), Masser [14] proves the following, improving Kubota's result [5] which is proved by using Baker's theorem on linear forms in the logarithms of algebraic numbers.

THEOREM C. *In the above notation, a necessary and sufficient condition for* α *not to satisfy the property* (iii) *is that there exists a nonzero difference of monomials* $D(z)$ *and an arithmetic progression* R *such that* $D(\Omega^k\alpha) = 0$ *for all* $k \in R$.

One of the simplest examples of Mahler function is $f_r(z) = \Sigma_{h=0}^{\infty} z^{r^h}$, $r \geqq 2$, which satisfies $f_r(z) = f_r(z^r) + z$. By the results above, we see that $f_r(\alpha_1), \ldots, f_r(\alpha_n)$ are algebraically independent if $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent algebraic numbers with $0 < |\alpha_i| < 1$, $i = 1, \ldots, n$. (A more precise result is proved in [9].) But we can not deduce the algebraic independence of the values $f_2(\alpha)$, $f_3(\alpha)$, $f_4(\alpha), \ldots$, from the results above. Further, as far as we know, it has not been determined whether the functions $f_r(z)$ $(r \geqq 2)$ are algebraically independent over $\mathbb{C}(z)$. These problems are treated in [9], but their proofs of Theorem 1 and Lemma 5 therein are unreadable.

The objective of this paper is thus to prove a general theorem which includes the algebraic independence of $f_r(\alpha)$ $(r \geqq 2)$. Evertse's theorem [3] plays an essential role in the proof.

2. The main theorem

Let Ω_i, $i = 1, \ldots, t$, be $n_i \times n_i$ matrices with nonnegative integer entries, and the characteristic polynomials of Ω_i irreducible over $\mathbb{Q}$. We assume that for each i, Ω_i has a real and positive eigenvalue ρ_i which is a simple root of the characteristic polynomial and exceeds the moduli of all the other eigenvalues. Let K be an algebraic number field and $f_{i1}, \ldots, f_{iM_i}$ $(1 \leqq i \leqq t)$ power series belonging to $K[\![z_i]\!] = K[\![z_{i1}, \ldots, z_{in_i}]\!]$, and satisfy

$$f_{ij}(z_i) = a_{ij}(z_i) f_{ij}(\Omega_i z_i) + b_{ij}(z_i),\ 1 \leqq i \leqq t,\ 1 \leqq j \leqq M_i,$$

where $a_{ij}(z_i)$ and $b_{ij}(z_i)$ are in the rational function field $K(z_i)$ and $a_{ij}(0) = 1$. Let α be an algebraic number with $0 < |\alpha| < 1$. We call a vector $\beta = (\beta_1, \ldots, \beta_n)$ an α-point, if each β_i is a nonnegative power of α and at least one of $\beta_1, \ldots, \beta_n$ is not unity.

THEOREM 1. *Suppose that* $\log \rho_i / \log \rho_j \notin \mathbb{Q}$ *for any distinct* i, j $(1 \leqq i, j \leqq t)$. *Let* $\beta_1, \ldots, \beta_t$ *be* α*-points such that* a_{ij} *and* b_{ij} *are defined at* $\Omega_i^k \beta_i$, $a_{ij}(\Omega_i^k \beta_i) \neq 0$ *for all* $k \geqq 0$, *and* $f_{ij}(z_i)$ *converges at* β_i *for every* i, j. *If* $f_{i1}(z_i), \ldots, f_{iM_i}(z_i)$ *are algebraically independent over* $K(z_i)$ *for every* i, *then the values*

$$f_{ij}(\beta_i)\ (1 \leqq i \leqq t,\ 1 \leqq j \leqq M_i)$$

are algebraically independent.

COROLLARY. *Let* $\log \rho_i / \log \rho_j \notin \mathbb{Q}$ *for any distinct* i, j $(1 \leqq i, j \leqq t)$, *and put* $N = \max_{1 \leq i \leq t} n_i$. *If the functions* $f_{i1}(z_1, \ldots, z_{n_i}), \ldots, f_{iM_i}(z_1, \ldots, z_{n_i})$ *are algebraically independent over* $K(z_1, \ldots, z_{n_i})$ *for every* i, *then the functions*

$$f_{ij}(z_1, \ldots, z_{n_i})\ (1 \leqq i \leqq t,\ 1 \leqq j \leqq M_i)$$

are algebraically independent over $K(z_1, \dots, z_N)$.

This is deduced from the theorem by taking $\beta_i = (\alpha^{r_1}, \dots, \alpha^{r_{n_i}})$, where α is a nonzero algebraic number and $r_1, \dots, r_N$ are suitable natural numbers.

PROPOSITION. *Let* $f_r(z) = \Sigma_{h=0}^{\infty} z^{r^h}$ *and* $g_r(z) = \Pi_{h=0}^{\infty}(1 - z^{r^h})$, $r \geqq 2$. *Let* $\{\omega_i\}_{i \geq 1}$ *be a set of real quadratic irrational numbers such that* $\mathbb{Q}(\omega_i) \neq \mathbb{Q}(\omega_j)$ *if* $i \neq j$ *and put* $F_{\omega_i}(z) = \Sigma_{h=1}^{\infty} [h\omega_i] z^h$. *Then for any algebraic number* α *with* $0 < |\alpha| < 1$,

$$f_r(\alpha) \ (r \geqq 2),\ g_r(\alpha) \ (r \geqq 2),\ F_{\omega_i}(\alpha) \ (i \geqq 1)$$

are algebraically independent.

3. A vanishing theorem

We prepare some notations and lemmas. In what follows K denotes an algebraic number field. An equivalence class of nontrivial valuations on K is called a prime on K. S_K and S_∞ denote the set of all primes and the set of all infinite primes on K, respectively. For every prime v on K lying above a prime p on $\mathbb{Q}$, we choose a valuation $|\ |_v$ such that

$$|\alpha|_v = |\alpha|_p^{[K_v : \mathbb{Q}_p]} \quad (\alpha \in \mathbb{Q}),$$

where K_v and $\mathbb{Q}_p$ denote the completions of K at v and $\mathbb{Q}$ at p, respectively. Then we have the product formula

$$\prod_{v \in S_K} |\alpha|_v = 1 \quad (\alpha \in K,\ \alpha \neq 0).$$

For any projective point $x = (x_0 : x_1 : \cdots : x_n)$ in $P^n(K)$, we define the height of x by

$$H(x) = H_K(x) = \prod_{v \in S_K} \max(|x_0|_v, |x_1|_v, \dots, |x_n|_v),$$

which is well-defined because of the product formula. We put

$$h(\alpha) = h_K(\alpha) = H(1 : \alpha) \quad (\alpha \in K).$$

Then we have the fundamental inequality

$$-\log h(\alpha) \leqq \sum_{v \in S} \log |\alpha|_v \leqq \log h(\alpha) \quad (\alpha \in K,\ \alpha \neq 0),$$

where S is any subset of S_K. If $\alpha \in K$, then $h(\alpha) = 1$ if and only if α is a root of unity or 0, $h(\alpha) = h(\alpha^{-1})$, and $h(\alpha^m) = h(\alpha)^m$. Furthermore, if $\alpha_1, \dots, \alpha_m \in K$,

$$h(\alpha_1 + \cdots + \alpha_m) \leqq m^d h(\alpha_1) \cdots h(\alpha_m), \quad d = [K:\mathbb{Q}],$$
$$h(\alpha_1 \cdots \alpha_m) \leqq h(\alpha_1) \cdots h(\alpha_m). \tag{1}$$

Let S be a finite subset of S_K including S_∞ and let c, d be constants with $c > 0$, $d \geqq 0$. A projective point $x \in P^n(K)$ is called (c, d, S)-admissible if its homogeneous coordinates $x_0, x_1, \dots, x_n$ can be chosen such that all x_i are S-integers, i.e., $|x_i|_v \leqq 1$ for $v \notin S$, and

$$\prod_{v \in S} \prod_{i=0}^{n} |x_i|_v \leqq cH(x)^d.$$

The following theorem is due to Evertse [3]: Let c, d be constants with $c > 0$, $0 \leqq d < 1$. Then there are only finitely many (c, d, S)-admissible points $x = (x_0 : x_1 : \cdots : x_n) \in P^n(K)$ satisfying

$$x_0 + x_1 + \cdots + x_n = 0$$

but

$$x_{i_0} + x_{i_1} + \cdots + x_{i_s} \neq 0$$

for each proper, non-empty subset $\{i_0, i_1, \dots, i_s\}$ of $\{0, 1, \dots, n\}$.

LEMMA 1 (Nishioka-Shiokawa-Tamura [19], Lemma 4). *Let ω be real and irrational. If α and β are nonzero elements in an algebraic number field K such that at least one of α and β is not a root of unity, then*

$$|\alpha|_v > |\beta|_v^{\omega}$$

for some $v \in S_K$.

LEMMA 2. *Let $\rho_1, \dots, \rho_n$ be nonzero elements of K and none of them a root of unity. Let $\{e_i(k)\}_{k=1}^{\infty}$ $(1 \leqq i \leqq n)$ be sequences of positive integers with* $\lim_{k\to\infty} e_i(k) = \infty$ $(1 \leqq i \leqq n)$ *such that for each $i \neq 1$, $e_1(k)/e_i(k)$ converges to an irrational number as $k \to \infty$. Let $\{A_i(k)\}_{k=1}^{\infty}$ $(1 \leqq i \leqq n)$ be sequences of elements in K satisfying the following conditions* (i) *and* (ii);

(i) $A_1(k) \neq 0 \quad (k \geqq 1)$,
(ii) $\lim_{k\to\infty} (\log h(A_i(k)))/e_i(k) = 0 \quad (1 \leqq i \leqq n)$.

Let $0 < \gamma < 1$. *Then we have*

$$\left|\sum_{i=1}^{n} A_i(k)\rho_i^{e_i(k)}\right| > |\rho_1|^{e_1(k)}\gamma^{e_1(k)} \tag{2}$$

for all large k.

Proof. We may assume $\sqrt{-1} \in K$ and $|\ |^2 = |\ |_{v_0}$ for some $v_0 \in S_\infty$. Let S be a finite subset of S_K containing S_∞ and all the divisors of ρ_i ($1 \leqq i \leqq n$). We may assume without loss of generality that all $A_i(k)$ ($1 \leqq i \leqq n$, $k \geqq 1$) are algebraic integers, since for each k there is an integer D_k with $1 \leqq D_k \leqq \prod_{i=1}^{n} h(A_i(k))$ such that $D_k A_1(k), \ldots, D_k A_n(k)$ are algebraic integers. Therefore $A_i(k)\rho_i^{e_i(k)}$ ($1 \leqq i \leqq n$, $k \geqq 1$) are S-integers. We prove the lemma by induction on n. If $n = 1$, the statement follows from (i), (ii) and the fundamental inequality. Let $n \geqslant 2$. We assume that

$$\sum_{i=1}^{n} A_i(k)\rho_i^{e_i(k)} = 0 \tag{3}$$

holds for all k belonging to an infinite set Λ_1 of positive integers. By the induction hypothesis, no proper subsum of the left-hand side of (3) vanishes, provided $k \in \Lambda_1$ is large. In particular, $A_i(k) \neq 0$ ($1 \leqq i \leqq n$) for all large $k \in \Lambda_1$. Then, putting

$$H_k = H(A_1(k)\rho_1^{e_1(k)} : \cdots : A_n(k)\rho_n^{e_n(k)}),$$

we have

$$\begin{aligned} H_k &\geqq \left(\prod_{i=1}^{n} h(A_i(k))\right)^{-1} H(\rho_1^{e_1(k)} : \cdots : \rho_n^{e_n(k)}) \\ &\geqq \left(\prod_{i=1}^{n} h(A_i(k))\right)^{-1} H(\rho_1^{e_1(k)} : \rho_2^{e_2(k)}), \end{aligned} \tag{4}$$

for all large $k \in \Lambda_1$. Here we can find a constant $C > 1$ independent of k such that

$$H(\rho_1^{e_1(k)} : \rho_2^{e_2(k)}) = H(\rho_1^{e_1(k)}\rho_2^{-e_2(k)} : 1) > C^{e_1(k)} \tag{5}$$

holds for all large k. Inded, it follows from Lemma 1 that

$$|\rho_1|_v > |\rho_2|_v^{\omega}$$

for some $v \in S_K$, where $\omega = \lim_{k\to\infty} e_2(k)/e_1(k)$. If $|\rho_2|_v > 1$, we choose $\eta > 0$ such that $|\rho_1|_v > |\rho_2|_v^{\omega+2\eta}$. Then

$$\begin{aligned}|\rho_1|_v|\rho_2|_v^{-e_2(k)/e_1(k)} &\geqq |\rho_2|_v^{\omega+2\eta-e_2(k)/e_1(k)}\\ &\geqq |\rho_2|_v^{\eta} > 1\end{aligned}$$

for all large k. If $|\rho_2|_v = 1$, then

$$|\rho_1|_v|\rho_2|_v^{-e_2(k)/e_1(k)} = |\rho_1|_v > 1.$$

Finally, if $|\rho_2|_v < 1$, we choose $\eta > 0$ such that $|\rho_1|_v > |\rho_2|_v^{\omega-2\eta}$. Then

$$\begin{aligned}|\rho_1|_v|\rho_2|_v^{-e_2(k)/e_1(k)} &\geqq |\rho_2|_v^{\omega-2\eta-e_2(k)/e_1(k)}\\ &\geqq |\rho_2|_v^{-\eta} > 1\end{aligned}$$

for all large k. In any case, we can choose a constant $C > 1$ satisfying (5). Combining (4), (5) and (ii), we have

$$\lim_{\Lambda_1 \ni k\to\infty} H_k = \infty.$$

Therefore it follows from Evertse's theorem that $(A_1(k)\rho_1^{e_1(k)}:\cdots:A_n(k)\rho_n^{e_n(k)})$ is not (1, 1/2, S)-admissible; namely

$$\prod_{i=1}^{n} h(A_i(k)) \geqq \prod_{v\in S}\prod_{i=1}^{n} |A_i(k)\rho_i^{e_i(k)}|_v > H_k^{1/2},$$

for all large $k \in \Lambda_1$. This together with (4) and (5) implies that

$$\left(\prod_{i=1}^{n} h(A_i(k))\right)^3 > C^{e_1(k)},$$

for all large $k \in \Lambda_1$, which contradicts the condition (ii). Therefore we have

$$\sum_{i=1}^{n} A_i(k)\rho_i^{e_i(k)} \neq 0 \tag{6}$$

for all large k. Now we assume that the inequality

$$\left|\sum_{i=1}^{n} A_i(k)\rho_i^{e_i(k)}\right| < |\rho_1|^{e_1(k)}\gamma^{e_1(k)} \tag{7}$$

holds for all k belonging to an infinite set Λ_2 of positive integers. Let δ_k be defined by

$$\sum_{i=1}^{n} A_i(k)\rho_i^{e_i(k)} + \delta_k = 0. \tag{8}$$

Then δ_k is an S-integer. By the induction hypothesis, (6) and (7), no proper subsum of the left-hand side of (8) vanishes for any sufficiently large $k \in \Lambda_2$. Noticing that $A_i(k) \neq 0\,(1 \leqq i \leqq n)$ for all large $k \in \Lambda_2$, we have again (4), which together with (5) and (ii) yields $\lim_{\Lambda_2 \ni k \to \infty} H_k = \infty$, so that

$$H_k \leqq H(A_1(k)\rho_1^{e_1(k)}:\cdots:A_n(k)\rho_1^{e_n(k)}:\delta_k) \to \infty(\Lambda_2 \ni k \to \infty).$$

It follows from Evertse's theorem that, if $0 < \varepsilon < 1$, then

$$(A_1(k)\rho_1^{e_1(k)}:\cdots:A_n(k)\rho_n^{e_n(k)}:\delta_k) \in P^n(K)$$

is not $(1, 1-\varepsilon, S)$-admissible, namely

$$\left(\prod_{v\in S}\prod_{i=1}^{n} |A_i(k)\rho_i^{e_i(k)}|_v\right)\left(\prod_{v\in S}|\delta_k|_v\right) > H_k^{1-\varepsilon} \tag{9}$$

for all large $k \in \Lambda_2$. Here we have

$$\prod_{v\in S}\prod_{i=1}^{n} |A_i(k)\rho_i^{e_i(k)}|_v \leqq \prod_{i=1}^{n} h(A_i(k)),$$

and by (7), (8)

$$\prod_{v\in S}|\delta_k|_v \leqq n^d\left(\prod_{i=1}^{n} h(A_i(k))\right) H(\rho_1^{e_1(k)}:\cdots:\rho_n^{e_n(k)}) \times\left(\max_{1\leq i\leq n} |\rho_i^{e_i(k)}|\right)^{-2} |\rho_1^{e_1(k)}|^2\gamma^{2e_1(k)},$$

so that the left-hand side of the inequality (9) is not greater than

$$n^d\left(\prod_{i=1}^{n} h(A_i(k))\right)^2 H(\rho_1^{e_1(k)}:\cdots:\rho_n^{e_n(k)})\gamma^{2e_1(k)}$$

for all large $k \in \Lambda_2$. This together with (4) and (9) implies that

$$n^d \left(\prod_{i=1}^{n} h(A_i(k)) \right)^3 \gamma^{2e_1(k)} \geqq H(\rho_1^{e_1(k)}:\cdots:\rho_n^{e_n(k)})^{-\varepsilon}$$

holds for all large $k \in \Lambda_2$. Therefore, using the condition (ii), we get

$$2 \log \gamma \geqq -\varepsilon \varlimsup_{\Lambda_2 \ni k \to \infty} (\log H(\rho_1^{e_1(k)}:\cdots:\rho_n^{e_n(k)}))/e_1(k).$$

Noticing that $(\log H(\rho_1^{e_1(k)}:\cdots:\rho_n^{e_n(k)}))/e_1(k)$ is bounded and letting $\varepsilon \to 0$, we obtain

$$\log \gamma \geqq 0,$$

which contradicts the assumption $0 < \gamma < 1$.

In the notation introduced in Section 2, we define

$$e_i(k) = [k \log \rho_1/\log \rho_i], \quad k \geqq 0.$$

If $z = (z_1, \ldots, z_t)$ is a point of $\mathbb{C}^{n_1 + \cdots + n_t}$, we define transformations $\Omega(k): \mathbb{C}^{n_1 + \cdots + n_t} \to \mathbb{C}^{n_1 + \cdots + n_t}$ $(k \geqslant 0)$ by

$$\Omega(k)z = (\Omega_1^{e_1(k)} z_1, \ldots, \Omega_t^{e_t(k)} z_t).$$

Now we prove the vanishing theorem.

THEOREM 2. *Let* $\log \rho_i/\log \rho_j \notin \mathbb{Q}$ *for any distinct* i, j *and* $\beta = (\beta_1, \ldots, \beta_t)$ *with* $\beta_1, \ldots, \beta_t$ *being* α*-points. If* $f(z)$ *is a convergent power series with complex coefficients such that* $f(\Omega(k)\beta) = 0$ *for all sufficiently large* $k \in \mathbb{N}$, *then* $f(z) \equiv 0$.

Proof. Choose a real number γ such that $0 < \gamma < 1$ and for each i, $\rho_i \gamma$ is larger than 1 and than the modulus of any other eigenvalues of Ω_i. From Mahler [11], Chap. 1, we have

$$\Omega_i^k = \rho_i^k \Gamma_i + o((\rho_i \gamma)^k), \quad \Gamma_i = B_i (B_{1p}^{(i)} B_{q1}^{(i)})_{p,\, q = 1, \ldots, n_i},$$

where B_i, $B_{1p}^{(i)}$ and $B_{q1}^{(i)}$ are positive algebraic numbers and $B_{11}^{(i)}, \ldots, B_{1n_i}^{(i)}$ are linearly independent over $\mathbb{Q}$. Let $\beta_i = (\alpha^{r_{i1}}, \ldots, \alpha^{r_{in_i}})$ and $h_i = (h_{i1}, \ldots, h_{in_i}) \in \mathbb{Z}^{n_i}$. Then we have

$$(\Omega_i^{e_i(k)} \beta_i)^{h_i} = \alpha^{\left(\sum_{q=1}^{n_i} B_{q1}^{(i)} r_{iq}\right) \rho_i^{e_i(k)} B_i \sum_{p=1}^{n_i} B_{1p}^{(i)} h_{ip} + o((\rho_i \gamma)^{e_i(k)})} \tag{10}$$

Therefore

$$(\Omega_i^{e_i(k)}\beta_i)^{h_i} = \alpha^{A_i\rho_i^{e_i(k)}} + o((\rho_i\gamma)^{e_i(k)}), \qquad A_i \neq 0, \quad \text{if } h_i \neq 0,$$
$$= 1, \quad \text{otherwise.}$$

If $h = (h_1, \ldots, h_t) \neq 0$, then

$$|(\Omega(k)\beta)^h| = |\alpha|^{\sum_{i:h_i \neq 0}(A_i\rho_i^{e_i(k)} + o((\rho_i\gamma)^{e_i(k)}))},$$

where

$$\left|\sum_{i:h_i \neq 0}(A_i\rho^{e_i(k)} + o((\rho_i\gamma)^{e_i(k)}))\right| \to \infty \quad (k \to \infty),$$

by Lemma 2. Let $f(z) = \Sigma_{h \geqq 0} c_h z^h (c_h \in \mathbb{C})$. Assume that the set $S = \{h \mid c_h \neq 0\}$ is not empty. By Lemma 3 in Kubota [5], S has a finite subset T such that every element of S majorizes some element of T. We can choose an element $h_0 \in T$ and an infinite subset Λ of $\mathbb{N}$ such that if h is an element of T distinct from h_0,

$$|(\Omega(k)\beta)^{h-h_0}| \to 0 \quad (\Lambda \ni k \to \infty).$$

If $h_1 \in T$, $\Sigma_{h \geqq h_1} c_h(\Omega(k)\beta)^{h-h_1}$ is bounded independently of k. Therefore

$$f(\Omega(k)\beta)/(\Omega(k)\beta)^{h_0} \to c_{h_0} \quad (\Lambda \ni k \to \infty),$$

which completes the proof.

4. Algebraic independence of functions

Let C be a field of characteristic zero, L and M the rational function field $C(z_1, \ldots, z_n)$ and the quotient field $C((z_1, \ldots, z_n))$ of the ring of formal power series, respectively, in n indeterminants over C. Let Ω be a nonsingular $n \times n$ matrix with nonnegative integer entries such that none of its eigenvalues is a root of unity. We define an endmorphism τ of the field M by

$$(z_1^\tau, \ldots, z_n^\tau) = \Omega(z_1, \ldots, z_n) \qquad \text{and} \qquad x^\tau = x \quad \text{for } x \in C,$$

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

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

Although the following theorem is essentially equivalent to Theorem 2 in Kubota [5], here we shall prove it in a different way.

THEOREM 3. *In the above notation, let* f_{ij} $(1 \leqq i \leqq h,\ 1 \leqq j \leqq n(i))$ *be a family of elements of* M *satisfying*

$$f_{ij}^{\tau} = a_i f_{ij} + b_{ij}, \quad a_i \in L^{\times},\ b_{ij} \in L \tag{11}$$

where $a_i a_j^{-1} \notin H$ *for all* $i \neq j$ $(1 \leqq i, j \leqq h)$. *Let* f_i $(h+1 \leqq i \leqq m)$ *be a family of elements of* $M^{\times}$ *satisfying*

$$f_i^{\tau} = a_i f_i, \quad a_i \in L^{\times}. \tag{12}$$

Suppose that b_{ij} *and* a_i *satisfying the following properties.*

(i) *If* $c_{ij} \in C$ $(1 \leqq j \leqq n(i))$ *are not all zero, then there exists no element* g *of* L *such that*

$$a_i g - g^{\tau} = \sum_{j=1}^{n(i)} c_{ij} b_{ij}.$$

(ii) $a_{h+1}, \ldots, a_m$ *are multiplicatively independent modulo* H. *Then the functions* f_{ij} $(1 \leqq i \leqq h,\ 1 \leqq j \leqq n(i))$ *and* f_i $(h+1 \leqq i \leqq m)$ *are algebraically independent over* L.

LEMMA 3 (Loxton-van der Poorten [8], Lemma 1). *Let* c *be a nonzero constant. If* $g \in M$ *and* $g^{\tau} = cg$, *then* $g \in C$.

Proof of Theorem 3. First we prove that f_{ij} $(1 \leqq i \leqq h,\ 1 \leqq j \leqq n(i))$ are algebraically independent over L by induction on $\Sigma_{i=1}^{h} n(i)$. Let X_{ij} $(1 \leqq i \leqq h,\ 1 \leqq j \leqq n(i))$ be indeterminants and define an endmorphism T of the polynomial ring $L[\{X_{ij}\}]$ by

$$TX_{ij} = a_i X_{ij} + b_{ij} \qquad \text{and} \qquad Ta = a^{\tau} \quad \text{for } a \in L.$$

We assume that $\{f_{ij}\}$ are algebraically dependent over L. Then there exists a nonconstant polynomial $F \in L[\{X_{ij}\}]$ such that

$$F(\{f_{ij}\}) = 0.$$

We may assume F is irreducible. By the equality (11), we get

$$TF(\{f_{ij}\}) = 0.$$

By the induction hypothesis, F divides TF. Comparing the degrees of F and TF, we know that

$$TF = aF \quad \text{for some } a \in L. \tag{13}$$

Let P be a polynomial with the least total degree among the nonconstant elements of $L[\{X_{ij}\}]$ satisfying (13). We denote by D_{ij} the derivation $\partial/\partial X_{ij}$. Then we have

$$a_i T D_{ij} P = D_{ij} T P = a D_{ij} P.$$

Since the total degree of $D_{ij}P$ is less than that of P, $D_{ij}P$ must belong to L for all i, j, which implies

$$P = \sum_{i=1}^{h} \sum_{j=1}^{n(i)} c_{ij} X_{ij} + c, \quad c_{ij}, c \in L.$$

Hence

$$\begin{aligned} TP &= \sum_{i=1}^{h} \sum_{j=1}^{n(i)} c_{ij}^{\tau}(a_i X_{ij} + b_{ij}) + c^{\tau} \\ &= a\left(\sum_{i=1}^{h} \sum_{j=1}^{n(i)} c_{ij} X_{ij}\right) + ac. \end{aligned}$$

Comparing the coefficients of the both sides, we get

$$c_{ij}^{\tau} a_i = a c_{ij}, \quad \sum_{i=1}^{h} \sum_{j=1}^{n(i)} c_{ij}^{\tau} b_{ij} + c^{\tau} = ac. \tag{14}$$

Since P is not constant, we may assume that $c_{i_0 j_0} = 1$ for some i_0, j_0. Therefore

$$a_{i_0} = a \quad \text{and} \quad c_{i_0 j}^{\tau} = c_{i_0 j} \quad (1 \leqq j \leqq n(i_0)).$$

By Lemma 3, we conclude $c_{i_0 j} \in C$ for $j = 1, \ldots, n(i_0)$. If $i \neq i_0$, by (14)

$$c_{ij}^{\tau} a_i = a_{i_0} c_{ij}.$$

Since $a_i a_{i_0}^{-1} \notin H$, c_{ij} must be zero for any i distinct from i_0. Hence by (14)

$$\sum_{j=1}^{n(i_0)} c_{i_0 j} b_{i_0 j} + c^{\tau} = a_{i_0} c,$$

where $c_{i_0 j} \in C$, $c_{i_0 j_0} = 1$, and $c \in L$. This contradicts (i), and so $\{f_{ij}\}$ are algebraically independent over L.

Next, we prove by induction $f_{h+1}, \ldots, f_m$ are algebraically independent over $R = L(\{f_{ij}\})$ which is the subfield of M generated by $\{f_{ij}\}$ over L. Let $X_{h+1}, \ldots, X_m$ be indeterminants and define an endmorphism T of the polynomial ring $R[X_{h+1}, \ldots, X_m]$ by

$$TX_i = a_i X_i \qquad \text{and} \qquad Ta = a^\tau \quad \text{for } a \in \mathrm{R}.$$

We assume that $f_{h+1}, \ldots, f_m$ are algebraically dependent over the field R. Then there exists a nonconstant element F of $R[X_{h+1}, \ldots, X_m]$ such that

$$F(f_{h+1}, \ldots, f_m) = 0.$$

We may assume F is irreducible, and so F must divide TF in the same way as above. Put

$$F = \sum_{i_{h+1}, \ldots, i_m} b_{i_{h+1} \cdots i_m} X_{h+1}^{i_{h+1}} \cdots X_m^{i_m} = \sum_{I = (i_{h+1}, \ldots, i_m)} b_I X^I,$$

where $b_{i_{h+1} \cdots i_m} = b_I \in R$. We may assume $b_J = 1$ for some $J = (j_{h+1}, \ldots, j_m)$. Then we have

$$TF = a_{h+1}^{j_{h+1}} \cdots a_m^{j_m} F = a^J F.$$

Comparing the coefficients of both sides above, we get

$$b_I^\tau a^I = a^J b_I, \tag{15}$$

Since none of f_i is zero, there exists I distinct from J with $b_I \neq 0$. We have a representation

$$b_I = A(\{f_{ij}\})/B(\{f_{ij}\}),$$

where A, $B \in L[\{X_{ij}\}]$ and A, B are relatively prime. By (15) we obtain

$$B(\{f_{ij}\}) TA(\{f_{ij}\}) a^{I-J} = A(\{f_{ij}\}) TB(\{f_{ij}\}).$$

Since $\{f_{ij}\}$ are algebraically independent over L, we have

$$B(TA) a^{I-J} = A(TB),$$

and so A and B divide TA and TB, respectively. In the same fashion as the first part of the proof, we can conclude that $A, B \in L$. This with (15) contradicts (ii), which completes the proof.

Now we shall prove that in the main theorem, we may assume without loss of generality, the power series $\Pi_{k=0}^{\infty} a_{ij}(\Omega_i^k z_i)$ $(1 \leqq j \leqq M_i)$ are power products of $f_{i,m_i+1}, \ldots, f_{iM_i}$ $(m_i \geqq 0)$, which satisfy

$$f_{ij}(z_i) = a_{ij}(z_i) f_{ij}(\Omega_i z_i), \quad m_i + 1 \leqq j \leqq M_i.$$

We assume that Ω has a real eigenvalue ρ which is greater than any of the absolute values of the other eigenvalues of Ω. Let K be an algebraic number field and $f_1, \ldots, f_m$ convergent power series belonging to $K[[z_1, \ldots, z_n]]$ and satisfying

$$f_i^\tau = a_i f_i + b_i,\ a_i,\ b_i \in L = K(z_1, \ldots, z_n), \quad 1 \leqslant i \leqslant m.$$

We assume $a_i(0) = 1$. Since $a_i(z) \equiv a_i(\Omega z) \mod H$, replacing Ω with any convenient power of Ω, we may assume the subgroup of $L^\times/H$ generated by $a_1, \ldots, a_m$ is torsion free. Let β be an α-point, a_i, b_i defined at $\Omega^k\beta$ and $a_i(\Omega^k\beta) \neq 0$ for all $k \geqq 0$. Suppose that $f_1, \ldots, f_m$ are algebraically independent over L. If $a_i a_j^{-1} = a^\tau a^{-1}$ for some $a \in L$, then

$$(af_j)^\tau = a^\tau f_j^\tau = a_i(af_j) + a^\tau b_j.$$

Put $a = A/B$, where A, B are relatively prime elements of $K[z_1, \ldots, z_n]$. We assert $A(\Omega^k\beta) \neq 0$ and $B(\Omega^k\beta) \neq 0$ for all $k \geqq 0$. Assume the assertion was false, i.e., for example $A(\Omega^k\beta) = 0$ for a certain $k \geqq 0$. Then there is a prime divisor P of A such that $P(\Omega^k\beta) = 0$, and so P must divide A^τ, since $a_i a_j^{-1} = (A^\tau B)/(AB^\tau)$, $a_i(\Omega^k\beta) \neq 0$ and $a_j(\Omega^k\beta) \neq 0$. Therefore

$$0 = A^\tau(\Omega^k\beta) = A(\Omega^{k+1}\beta).$$

Continuing this, we obtain

$$A(\Omega^{k'}\beta) = 0 \quad \text{for all } k' \geqq k.$$

By Theorem 2, $A = 0$, which is a contradiction. Replacing f_j by af_j, we may assume $\{f_i\}_{1 \leqq i \leqq m} = \{f_{ij}\}_{1 \leqq i \leqq h, 1 \leqq j \leqq n(i)}$, where f_{ij} satisfies

$$f_{ij}^\tau = a_i f_{ij} + b_{ij}, \quad a_i,\ b_{ij} \in L,$$

and $a_i a_j^{-1} \notin H$ for all $i \neq j$. Suppose that there are $c_{ij} \in K$ $(1 \leqq j \leqq n(i))$ not all zero such that

$$\sum_{j=1}^{n(i)} c_{ij} b_{ij} = a_i g - g^\tau, \quad g \in L.$$

We may assume $c_{in(i)} = 1$. Putting

$$f_i = g + \sum_{j=1}^{n(i)} c_{ij} f_{ij},$$

we obtain $f_i^\tau = a_i f_i$. In the same way as above, we can see that g is defined at $\Omega^k \beta$ for all $k \geqq 0$. We put $n'(i) = n(i) - 1$ in this case, $n'(i) = n(i)$, otherwise. It is easily seen that the functions $\{f_{ij}\}_{1 \leqq i \leqq h, 1 \leqq j \leqq n'(i)}$ have the property (i) in Theorem 3, since the functions $\{f_{ij}\}_{1 \leqq i \leqq h, 1 \leqq j \leqq n'(i)} \cup \{f_i\}_{n'(i) \neq n(i)}$ are algebraically independent over L. Let $\{e_1, \ldots, e_S\}$ be a base of the subgroup generated by $a_1, \ldots, a_h$ in $L^\times/H$. We may assume $e_i(0) = 1$ and $e_i(\Omega^k \beta) \neq 0$ for all $k \geqq 0$. Putting

$$g_i(z) = \prod_{k=0}^{\infty} e_i(\Omega^k z)^{-1},$$

we have $g_i(z) \in K[\![z_1, \ldots, z_n]\!]$ and

$$g_i^\tau = e_i g_i, \quad 1 \leqq i \leqq s.$$

Since $e_1, \ldots, e_S$ are multiplicatively independent modulo H, by Theorem 3, the functions $\{f_{ij}\}_{1 \leqq i \leqq h, 1 \leqq j \leqq n'(i)} \cup \{g_i\}_{1 \leqq i \leqq s}$ are algebraically independent over L. We may assume that $a_1, \ldots, a_h$ are power products of $e_1, \ldots, e_S$. Therefore $\prod_{k=0}^{\infty} a_i(\Omega^k z)$ $(1 \leqq i \leqq h)$ are power products of $g_1, \ldots, g_S$. By the equality $f_i^\tau = a_i f_i$ and Lemma 3, we know that f_i equals $\prod_{k=0}^{\infty} a_i(\Omega^k z)^{-1}$ multiplied by an element of K. These complete the proof.

5. Proof of the main theorem

In addition to the assumption of Theorem 1, we suppose that

$$\prod_{k=0}^{\infty} a_{ij}(\Omega_i^k z_i) \ (1 \leqq j \leqq M_i)$$

are power products of $f_{i,m_i+1},\dots,f_{iM_i}$ $(m_i \geqq 0)$, which satisfy

$$f_{ij}(z_i) = a_{ij}(z_i) f_{ij}(\Omega_i z_i), \quad m_i + 1 \leqq j \leqq M_i.$$

Define the transformation $\Omega(k)$ as in Theorem 2. We assume that $f_{ij}(\beta_i)$ $(1 \leqq i \leqq t,\ 1 \leqq j \leqq M_i)$ are algebraically dependent. There is a relation of algebraic dependence

$$\sum_{\mu=(\mu_{11},\dots,\mu_{tM_t})} \omega_\mu f_{11}(\beta_1)^{\mu_{11}} \cdots f_{tM_t}(\beta_t)^{\mu_{tM_t}} = 0, \tag{16}$$

where ω_μ are nonzero rational integers. To each of the finitely many ω_μ, associate a new indeterminant w_μ and define

$$F(z; w) = \sum_\mu w_\mu f_{11}(z_1)^{\mu_{11}} \cdots f_{tM_t}(z_t)^{\mu_{tM_t}}. \tag{17}$$

Iterating the functional equation of f_{ij}, we get

$$f_{ij}(z_i) = a_{ij}^{(k)}(z_i) f_{ij}(\Omega_i^{e_i(k)} z_i) + b_{ij}^{(k)}(z_i), \tag{18}$$

where

$$a_{ij}^{(k)}(z_i) = \prod_{r=0}^{e_i(k)-1} a_{ij}(\Omega_i^r z_i),$$

$$b_{ij}^{(k)}(z_i) = \sum_{r=0}^{e_i(k)-1} \left(\prod_{s=0}^{r-1} a_{ij}(\Omega_i^s z_i) \right) b_{ij}(\Omega_i^r z_i). \tag{19}$$

We define $w^{(k)} = (w_\mu^{(k)})_\mu$ and $\omega^{(k)} = (\omega_\mu^{(k)})_\mu$ by

$$w_\mu^{(k)} = \left(\prod_{i=1}^t \prod_{j=1}^{M_i} a_{ij}^{(k)}(z_i)^{\mu_{ij}} \right) \sum_\nu \left\{ \prod_{i=1}^t \prod_{j=1}^{m_i} \binom{\nu_{ij}}{\mu_{ij}} b_{ij}^{(k)}(z_i)^{\nu_{ij}-\mu_{ij}} \right\} w_\nu, \tag{20}$$

$$\omega_\mu^{(k)} = \left(\prod_{i=1}^t \prod_{j=1}^{M_i} a_{ij}^{(k)}(\beta_i)^{\mu_{ij}} \right) \sum_\nu \left\{ \prod_{i=1}^t \prod_{j=1}^{m_i} \binom{\nu_{ij}}{\mu_{ij}} b_{ij}^{(k)}(\beta_i)^{\nu_{ij}-\mu_{ij}} \right\} \omega_\nu. \tag{21}$$

Substituting (18) into (17), we have

$$F(z; w) = F(\Omega(k) z; w^{(k)}),$$

and by (16)

$$0 = F(\beta; \omega) = F(\Omega(k)\beta; \omega^{(k)}).$$

DEFINITION 1. If $P(z;w) \in K[z,w]$ is a polynomial, then we write $P(z;w) \sim O(\beta;\omega)$ to indicate that for all sufficiently large integers k, $P(\Omega(k)\beta\,;\,\omega^{(k)}) = 0$.

The negation is written $P(z;\,w) \not\sim O(\beta;\,\omega)$.

LEMMA 4. *The set* $V(\omega)$ *of polynomials* $P(z;w)$ *satisfying* $P(z;w) \sim O(\beta:\omega)$ *is independent of the choice of* α*-point* β *and is a prime ideal of* $K[z,w]$ *with basis in* $K[w]$.

Proof. Clearly $V(\omega)$ is an ideal of $K[z,\,w]$. Put

$$A_{ij}(z) = \prod_{r=0}^{\infty} a_{ij}(\Omega_i^r z_i),$$

$$A_\mu(z) = \prod_{i=1}^{t}\prod_{j=1}^{M_i} A_{ij}(z)^{\mu_{ij}}.$$

By assumption $A_{ij}(z)$ and $A_\mu(z)$ are power products of f_{ij}, $1 \leqq i \leqq t$, $m_i + 1 \leqq j \leqq M_i$, and

$$\omega_\mu^{(k)} = A_\mu(\beta)A_\mu(\Omega(k)\beta)^{-1}$$
$$\times \sum_\nu \left\{\prod_{i=1}^{t}\prod_{j=1}^{m_i}\binom{\nu_{ij}}{\mu_{ij}}(f_{ij}(\beta) - A_{ij}(\beta)A_{ij}(\Omega(k)\beta)^{-1} f_{ij}(\Omega(k)\beta))^{\nu_{ij}-\mu_{ij}}\right\}\omega_\nu. \quad (22)$$

If $P(z;\,w) \in K[z;\,w]$, by (22)

$$P(\Omega(k)\beta\,;\,\omega^{(k)}) = \sum_{\lambda=(\lambda_{11},\ldots,\lambda_{tm_t})} Q_{\beta\lambda}(f_{11}(\Omega(k)\beta),\ldots,f_{tM_t}(\Omega(k)\beta))(\Omega(k)\beta)^\lambda,$$

where $Q_{\beta\lambda}$ are rational functions in indeterminants $X_{11},\ldots,X_{tM_t}$ with complex coefficients. Put

$$Q_\beta(z) = \sum_\lambda Q_{\beta\lambda}(f_{11}(z_1),\ldots,f_{tM_t}(z_t))z^\lambda.$$

By Theorem 2, $P(z;w) \in V(\omega)$ if and only if $Q_\beta(z) \equiv 0$. Since $f_{11}(z_1),\ldots,f_{tM_t}(z_t)$ are algebraically independent over $\mathbb{C}(z)$, $Q_\beta(z) \equiv 0$ if and only if $Q_{\beta\lambda} = 0$ for all λ. We define new indeterminants Y_{ij} by

$$Y_{ij} = X_{ij}/f_{ij}(\beta), \quad 1 \leqq i \leqq t,\ m_i + 1 \leqq j \leqq M_i,$$

$$Y_{ij} = f_{ij}(\beta) - X_{ij}M_{ij}(\{Y_{ij}\}),\ 1 \leqq i \leqq t,\ 1 \leqq j \leqq m_i,$$

where $M_{ij}(\{Y_{ij}\})$ are power products of Y_{ij} $(1 \leqq i \leqq t,\ m_i + 1 \leqslant j \leqq M_i)$ such that $A_{ij}(z)^{-1} = M_{ij}(\{f_{ij}\})$. By (22) we obtain

$$Q_{\beta\lambda}(X_{11}, \ldots, X_{tM_t}) = Q_\lambda(Y_{11}, \ldots, Y_{tM_t}),$$

where Q_λ are rational functions independent of β. The lemma follows easily by these facts.

DEFINITION 2. If $P(z; w) = \Sigma_\lambda P_\lambda(w) z^\lambda \in K[w][\![z]\!]$ is a power series, then the index of $P(z; w)$ is defined to be the least integer h for which there are nonnegative integers $h_{11}, \ldots, h_{tn_t}$ satisfying $h_{11} + \cdots + h_{tn_t} = h$ and $P_{h_{11}, \ldots, h_{tnt}}(w) \not\sim O(\beta; \omega)$. If there are no such integers, we define the index of $P(z; w)$ is ∞.

By Lemma 4, we have

$$\text{index}\,(P_1(z;\, w) P_2(z;\, w)) = \text{index}\, P_1(z;\, w) + \text{index}\, P_2(z;\, w).$$

LEMMA 5. *The power series $F(z; w)$ defined by* (17) *is of finite index.*

Proof. Substituting $w = \omega$ into $F(z; w)$, we get a nonzero power series $F(z; \omega)$, since $f_{11}(z_1), \ldots, f_{tM_t}(z_t)$ are algebraically independent over $\mathbb{C}(z)$. By Theorem 2, there exists a nonnegative integer k_0 such that $F(\Omega(k_0)\beta; \omega) \neq 0$. Here $\beta' = \Omega(k_0)\beta$ is also an α-point. Suppose that index $F(z; w) = \infty$. If $F(z; w) = \Sigma_\lambda F_\lambda(w) z^\lambda$, then $F_\lambda(w) \sim O(\beta'; \omega)$ for all λ. We define $\omega'^{(k)}$ substituting $z = \beta'$ and $w = \omega$ into (20). Since the ideal $V(\omega) \cap K[w]$ is finitely generated, if k is sufficiently large, then $F_\lambda(\omega'^{(k)}) = 0$ for all λ. Therefore

$$O = F(\Omega(k)\beta';\, \omega'^{(k)}) = F(\beta';\, \omega).$$

This is a contradiction.

Let p be a nonnegative integer, $R(p)$ the K-vector space of polynomials in $K[w]$ of degree at most p in each w_μ, and $d(p)$ the dimension over K of the factor space $R(p)/(R(p) \cap V(\omega))$.

LEMMA 6. *Let $|\{w_\mu\}| = M$. Then*

$$d(2p) \leqq 2^M d(p).$$

Proof. Every polynomial $P(w) \in R(2p)$ can be written in the form

$$P(w) = \sum_\varepsilon \left(\prod_\mu w_\mu^{\varepsilon(\mu)p} \right) Q_\varepsilon(w),$$

where ε ranges through the 2^M functions into the set $\{0, 1\}$ and $Q_\varepsilon(w) \in R(p)$. The lemma follows from this.

LEMMA 7. *Let $N = \Sigma_{i=1}^{t} n_i$, and p be a sufficiently large natural number. Then there are polynomials $P_0(z;w),\ldots,P_p(z;w) \in K[z,w]$ with algebraic integer coefficients and degrees at most p in each z_{ij} and each w_μ such that $P_0(z;w) \not\equiv O(\beta;\omega)$ and such that the index I of*

$$E(z;w) = \sum_{h=0}^{p} P_h(z;w)F(z;w)^h = \sum_{\lambda} E_\lambda(w)z^\lambda \tag{23}$$

is at least $c_1(p+1)^{1+N^{-1}}$, where c_1 is a positive constant not depending on p.

Proof. The coset of a polynomial $P(w)$ of $R(p)$ in $\bar{R}(p) = R(p)/(R(p) \cap V(\omega))$ is denoted by $\bar{P}(w)$. Letting $\bar{Q}_i^p(w)$ for $i = 1,\ldots,d(p)$, be a K-basis of $\bar{R}(p)$, the typical polynomial $P_h(z;w)$ can be expressed in the form

$$P_h(z;w) = \sum_{\lambda} P_\lambda^h(w)z^\lambda, \qquad \bar{P}_\lambda^h(w) = \sum_{i=1}^{d(p)} q_{h\lambda i}\bar{Q}_i^p(w) \tag{24}$$

where the variables $q_{h\lambda i}$ range through K. Since $F(z;w)$ is a linear form in the w_μ, the polynomials $E_\lambda(w)$ are all in $R(2p)$. Substituting the equation (24) into the equation (23), we obtain expressions for the $\bar{E}_\lambda(w)$ which can be written in terms of the $\bar{Q}_j^{2p}(w)$. The coefficients of $\bar{Q}_j^{2p}(w)$ as $j = 1,\ldots,d(2p)$ are a system of $d(2p)$ homogeneous linear expressions in the $q_{h\lambda i}$ whose simultaneous vanishing is equivalent to $\bar{E}_\lambda(w) = 0$. In particular, if we wish $E(z;w)$ to have index at least equal to $J = [2^{-MN^{-1}}(p+1)^{1+N^{-1}}] - 1$, then we need to solve a system of $\binom{J+N-1}{N} d(2p)$ $(\leqq J^N d(2p))$ homogeneous linear equations in $(p+1)^{N+1}d(p)$ variables $q_{h\lambda i}$. By Lemma 6, we have $J^N d(2p) \leqq J^N 2^M d(p) < (p+1)^{N+1}d(p)$. This implies that there is a function $E(z;w)$ of the form (23) with index $I \geqq J$ and such that $P_h(z;w) \not\equiv O(\beta;\omega)$ for at least one value of h. By construction, we know that there is a least index r such that $P_r(z;w) \not\equiv O(\beta;\omega)$. Let

$$E_0(z;w) = \sum_{h=r}^{p} P_h(z;w)F(z;w)^{h-r}.$$

Since the index of $E(z;w) - F(z;w)^r E_0(z;w)$ is ∞, the function $F(z;w)^r E_0(z;w)$ must have the same index I as $E(z;w)$. If I_0 denotes the index of $E_0(z;w)$, then we have $I = r$ (index $F(z;w)) + I_0$ by Lemma 5. Therefore, if p is taken sufficiently large, then

$$I_0 = I - r(\text{index } F(z;w)) \geqq J - p(\text{index } F(z;w)) > c_1(p+1)^{1+N^{-1}}.$$

We can take $E_0(z;w)$ as $E(z;w)$ in the lemma.

In what follows, $c_2, c_3, \ldots$ denote positive constants which do not depend on p, k.

LEMMA 8. *If k is larger than a certain constant depending on p, then*

$$\log |E(\Omega(k)\beta; \omega^{(k)})| \leqq -c_2(p+1)^{1+N^{-1}} \rho_1^k.$$

Proof. By (22) we have

$$|\omega_\mu^{(k)}| \leqslant c_3 \quad \text{for all } k \geqq 0.$$

Since the power series f_{ij} converge at β_i, using (17) and (23) we have

$$|E_\lambda(\omega^{(k)})| \leqq S_p c_4^{|\lambda|},$$

where S_p is a positive constant depending on p. By (10) we get

$$|(\Omega(k)\beta)^\lambda| \leqq |\alpha|^{c_5 \rho_1^k |\lambda|}.$$

These imply

$$\begin{aligned} |E(\Omega(k)\beta ; \omega^{(k)})| &\leqq S_p \sum_{|\lambda| \geq I} (c_4 |\alpha|^{c_5 \rho_1^k})^{|\lambda|} \\ &\leqq S_p c_6 (c_4 |\alpha|^{c_5 \rho_1^k})^{c_1 (p+1)^{1+N-1}} \\ &\leqq \exp(-c_2(p+1)^{1+N^{-1}} \rho_1^k), \end{aligned}$$

if k is larger than a certain constant depending on p.

By construction of $E(z; w)$, $E(\Omega(k)\beta ; \omega^{(k)}) = P_0(\Omega(k)\beta ; \omega^{(k)})$ and there exists an infinite set Λ of natural numbers such that $P_0(\Omega(k)\beta ; \omega^{(k)}) \neq 0$ for any $k \in \Lambda$.

LEMMA 9. *If k is larger than a certain constant depending on p, then*

$$h(E(\Omega(k)\beta ; \omega)) \leqq c_7^{p\rho_1^k}.$$

Proof. If we put

$$P_0(z; w) = \sum_{\nu, \lambda} p_{\nu\lambda} w^\nu z^\lambda,$$

then

$$E(\Omega(k)\beta\,;\,\omega^{(k)}) = P_0(\Omega(k)\beta\,;\,\omega^{(k)})$$
$$= \sum_{\nu,\lambda} p_{\nu\lambda}(\omega^{(k)})^{\nu}(\Omega(k)\beta)^{\lambda}.$$

Therefore, by the inequality (1),

$$h(E(\Omega(k)\beta\,;\,\omega^{(k)})$$
$$\leqq (p+1)^{(M+N)[K:\mathbb{Q}]}\prod_{\nu,\lambda} h(p_{\nu\lambda})h((\omega^{(k)})^{\nu})h\,((\Omega(k)\beta)^{\lambda}).$$

Since $h(a_{ij}(\Omega_i^r\beta_i))$, $h(b_{ij}(\Omega_i^r\beta_i)) \leqq c_8^{\rho_i^r}$, we have

$$h(\omega_\mu^{(k)}) \leqq c_9^{\rho_1^k}$$

by (19) and (21). On the other hand

$$h((\Omega(k)\beta)^{\lambda}) \leqq c_{10}^{p\rho_1^k}.$$

Therefore

$$h(E(\Omega(k)\beta\,;\,\omega^{(k)})) \leqq T_p c_{11}^{p\rho_1^k},$$

where T_p is a positive constant depending only on p. This implies the lemma.

If $k\in\Lambda$ is larger than a certain constant depending on p, then Lemma 8, Lemma 9 and the fundamental inequality imply the inequality

$$-p\rho_1^k \log c_7 \leqq -2c_2(p+1)^{1+N^{-1}}\rho_1^k.$$

Dividing both sides above by ρ_1^k, we obtain

$$-p \log c_7 \leqq -2c_2(p+1)^{1+N^{-1}}.$$

This is a contradiction if p is sufficiently large. Hence we complete the proof of Theorem 1.

6. Proof of proposition

First we shall prove that the functions $f_r, f_{r^2}, \ldots, f_{r^n}$ have the property (i) in Theorem 3. Put $N = n!$. Since $f_{r^j}(z^{r^j}) = f_{r^j}(z) - z$, we get

$$f_{r^j}(z^{r^N}) = f_{r^j}(z) - z - z^{r^j} - z^{r^{2j}} - \cdots - z^{(Nj^{-1}-1)j}$$
$$= f_{r^j}(z) + b_j(z) \quad \text{(say)}.$$

Assume that there are $c_j \in \mathbb{Q}$ not all zero such that

$$\sum_{j=1}^{n} c_j b_j(z) = g(z) - g(z^{r^N})$$

for some $g \in \mathbb{Q}(z)$. The function g can be written in the form $g = P/Q$, where P and Q are relatively prime polynomials in z. Hence we have

$$Q(z)Q(z^{r^N}) \sum_{j=1}^{n} c_j b_j(z) = Q(z^{r^N})P(z) - Q(z)P(z^{r^N}).$$

Since $P(z^{r^N})$ and $Q(z^{r^N})$ are relatively prime, $Q(z^{r^N})$ divides $Q(z)$. Then we may assume $Q(z) = 1$, which implies

$$P(z) - P(z^{r^N}) = \sum_{j=1}^{n} c_j b_j(z).$$

This is a contradiction, since the degree of $b_j(z)$ is r^{N-j} for each j.

Second we shall prove that the functions $g_r, g_{r^2}, \ldots, g_{r^n}$ have the property (ii) in Theorem 3. Put $N = n!$. Since $g_r(z) = (1 - z)g_r(z^r)$, we obtain

$$g_{r^i}(z) = (1 - z)(1 - z^{r^i})\cdots(1 - z^{(Ni^{-1}-1)i})g_{r^i}(z^{r^N})$$
$$= a_i(z)g_{r^i}(z^{r^N}) \quad \text{(say)}.$$

Suppose that for some integers $j_1, \ldots, j_n$ not all zero and $a(z) \in \mathbb{Q}(z)^\times$, the equality

$$a_1(z)^{j_1} \cdots a_n(z)^{j_n} = a(z)a(z^{r^N})^{-1}$$

holds. We write $a(z) = P(z)/Q(z)$, where P and Q are relatively prime polynomials in z. Then we have

$$a_1(z)^{j_1} \cdots a_n(z)^{j_n} = P(z)Q(z^{r^N})/Q(z)P(z^{r^N}). \tag{25}$$

Assume the degree of P is positive and ζ is a root of $P(z)$ such that the argument θ $(0 < \theta \leqq 2\pi)$ of ζ is least among the roots of $P(z)$. Since ζ^{1/r^N} $(0 < \arg.\zeta^{1/r^N} = \theta/r^N \leqq 2\pi/r^N)$ is a root of $P(z^{r^N})$ and $P(z^{r^N})$, $Q(z^{r^N})$ are relatively prime, by (25) ζ^{1/r^N} must be a root of $a_i(z)$ for some i. This is a contradiction, since any root of $a_i(z)$ is an r^{N-i}th root of unity. Therefore $P(z) \in \mathbb{Q}^\times$. In the same way, $Q(z) \in \mathbb{Q}^\times$. Then the right-hand side of (25) is constant. Let h be the least number with $j_h \neq 0$. Then any primitive r^{N-h}th root of unity is a zero or a pole of the left-hand side of (25), which is a contradiction.

Third we consider the power series

$$\bar{F}_\omega(z_1, z_2) = \sum_{h_1=1}^{\infty} \sum_{h_2=1}^{[h_1\omega]} z_1^{h_1} z_2^{h_2},$$

where $F_{\omega_i}(z) = \bar{F}_{\omega_i}(z, 1)$. Let ω be expanded in the continued fraction

$$\omega = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}.$$

Define $\theta_1, \theta_2, \dots$ by

$$\omega = \frac{1}{a_1 + \theta_1}, \quad \theta_1 = \frac{1}{a_2 + \theta_2}, \dots$$

Because of the equality (see Mahler [11])

$$\bar{F}_\omega(z_1, z_2) = \sum_{\mu=0}^{\nu-1} (-1)^\mu \frac{z_1^{p_{\mu+1}+p_\mu} z_2^{q_{\mu+1}+q_\mu}}{(1 - z_1^{p_{\mu+1}} z_2^{q_{\mu+1}})(1 - z_1^{p_\mu} z_2^{q_\mu})}$$
$$+ (-1)^\nu \bar{F}_{\theta_\nu}(z_1^{p_\nu} z_2^{q_\nu}, z_1^{p_{\nu-1}} z_2^{q_{\nu-1}}),$$

where q_ν/p_ν is the νth convergent of ω, we may assume that each of ω_i is expanded in a purely periodic continued fraction. Let ν_i be an even period of the continued fraction of ω_i and $\Omega_i = \begin{pmatrix} p_{\nu_i} & q_{\nu_i} \\ p_{\nu_i - 1} & q_{\nu_i - 1} \end{pmatrix}$. Then we have

$$\bar{F}_{\omega_i}(z_1, z_2) = \bar{F}_{\omega_i}(\Omega_i(z_1, z_2)) + b_i(z_1, z_2), \; b_i(z_1, z_2) \in \mathbb{Q}(z_1, z_2).$$

The eigenvalue $\rho_i = p_{\nu_i} + p_{\nu_i - 1}\omega_i > 1$ of Ω_i is greater than the other eigenvalue of Ω_i. Since each ρ_i is a nontrivial unit of $\mathbb{Q}(\omega_i)$, $\log \rho_i / \log \rho_j \notin \mathbb{Q}$ for all $i \neq j$.

Now we can prove the proposition applying Theorem 1 to the above functions.

References

[1] M. Amou: Algebraic independence of the values of certain functions at a transcendental number. *Acta Arith.* 59 (1991) 71–82.

[2] P.-G. Becker: Effective measures for algebraic independence of the values of Mahler type functions. To appear in Acta Arith.

[3] J.-H. Evertse: On sums of S-units and linear recurrences, *Compositio Math.* 53 (1984)225–244.

[4] F. R. Gantmacher: *Applications of the Theory of Matrices.* New York, Wiley, 1959.

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

[6] J. H. Loxton and A. J. van der Poorten: Arithmetic properties of certain functions in several variables. *J. Number Theory* 9 (1977) 87–106.

[7] J. H. Loxton and A. J. van der Poorten: Arithmetic properties of certain functions in several variables. II. *J. Austral. Math. Soc. Ser.* A 24 (1977) 393–408.

[8] J. H. Loxton and A. J. van der Poorten: A class of hypertranscendental functions. *Aequationes Math.* 16 (1977) 93–106.

[9] 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.

[10] J. H. Loxton and A. J. van der Poorten: Arithmetic properties of automata; regular sequences. *J. reine angew. Math.* 392 (1988) 57–69.

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

[12] K. Mahler: Über das Verschwinden von Potenzreihen mehrerer Veränderlichen in speziellen Punktfolgen. *Math. Ann.* 103 (1930) 573–587.

[13] K. Mahler: Arithmetische Eigenschaften einer Klasse transzendental-transzendenter Funktionen. *Math. Z.* 32 (1930) 545–585.

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

[15] Yu. V. Nesterenko: On a measure of the algebraic independence of the values of certain functions. *Mat. Sb.* 128 (170) (1985); English transl. in Math. USSR Sb. 56 (1987) 545–567.

[16] K. Nishioka: New approach in Mahler's method. *J. reine angew. Math.* 407 (1990) 202–219.

[17] K. Nishioka: On an estimate for the orders of zeros of Mahler type functions. *Acta Arith.* 56 (1990) 249–256.

[18] K. Nishioka: Algebraic independence measures of the values of Mahler functions. *J. reine angew. Math.* 420 (1991) 203–214.

[19] K. Nishioka, Y. Shiokawa and J. Tamura: Arithmetic properties of a certain power series. *J. Number Theory* 42 (1992) 61–87.