Tôhoku Math. J.
48 (1996), 51–70

ALGEBRAIC INDEPENDENCE OF MAHLER FUNCTIONS AND THEIR VALUES

KUMIKO NISHIOKA

(Received September 21, 1994, revised March 9, 1995)

Abstract. General theorems are proved on the algebraic independence of Mahler functions in several variables and their values at algebraic points.

1. Introduction and results. Using Nesterenko's results, we have a satisfactory result (Nishioka [9]) on the algebraic independence of the values of Mahler functions of one variable. However we have been unable to get such a result in the case of several variables (see Töpfer [11]). Here we study the algebraic independence of the following Mahler functions and their values by Mahler's method.

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

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

Let K be an algebraic number field, $f_1(z),\dots,f_m(z)$ power series of n variables $z_1,\dots,z_n$ with coefficients in K, convergent in an n-polydisc U around the origin. We assume that $f_1(z),\dots,f_m(z)$ satisfy a functional equation of the form

$$(1)\qquad \begin{pmatrix} f_1(z)\\ \vdots \\ f_m(z)\end{pmatrix}=A\begin{pmatrix} f_1(\Omega z)\\ \vdots \\ f_m(\Omega z)\end{pmatrix}+\begin{pmatrix} b_1(z)\\ \vdots \\ b_m(z)\end{pmatrix},$$

where A is an $m\times m$ matrix with entries in K and $b_i(z)$ are rational functions of $z_1,\dots,z_n$ with coefficients in K. Furthermore we suppose that the matrix Ω and an algebraic point $\alpha=(\alpha_1,\dots,\alpha_n)$, 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.

Let ρ be the maximum of the absolute values of the eigenvalues of Ω. Then ρ is an eigenvalue of Ω (Gantmacher [1]) and $\rho>1$.

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

If every eigenvalue of Ω of the absolute value ρ is a simple root of the minimal polynomial of Ω, then the property (II) is fulfilled.

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

1991 *Mathematics Subject Classification*. Primary 11J81.

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

for all sufficiently large k, where c is a positive constant.
(IV) If $f(z)$ is any nonzero power series of n variables with complex coefficients which converges in some neighborhood of the origin, then there are infinitely many natural numbers k such that $f(\Omega^k\alpha) \neq 0$.

Masser [7] gives a property which is equivalent to (IV).

The power series $f_1(z), \dots, f_r(z)$ are said to be linearly independent over K modulo $K(z_1, \dots, z_n)$ ($K[z_1, \dots, z_n]$) if $c_1 f_1(z) + \cdots + c_r f_r(z) \notin K(z_1, \dots, z_n)$ ($K[z_1, \dots, z_n]$) for any $c_1, \dots, c_r \in K$ which are not all zero.

THEOREM 1. *Suppose $\alpha \in U$. If $f_1(z), \dots, f_r(z)$ ($r \leq m$) are linearly independent over K modulo the rational function field $K(z_1, \dots, z_n)$, then $f_1(\alpha), \dots, f_r(\alpha)$ are algebraically independent.*

COROLLARY. *If $\alpha \in U$, then*

$$\text{trans.deg}_K K(f_1(\alpha), \dots, f_m(\alpha)) = \text{trans.deg}_{K(z)} K(z)(f_1(z), \dots, f_m(z)).$$

THEOREM 2. *Suppose that all $b_i(z)$ in the functional equation (1) are polynomials. If $f_1(z), \dots, f_r(z)$ ($r \leq m$) are linearly independent over K modulo the polynomial ring $K[z_1, \dots, z_n]$, then $f_1(\alpha), \dots, f_r(\alpha)$ are algebraically independent for $\alpha \in U$.*

Kubota [2] and Loxton-van der Poorten [3] study the case where the matrix A is diagonal. We note that they need the further assumption that $\Omega^k\alpha$ ($k \geq 0$) are not poles of $b_i(z)$.

In Section 2, we shall study the algebraic independence of the functions $f_1(z), \dots, f_m(z)$, and in Section 3, the algebraic independence of the values $f_1(\alpha), \dots, f_m(\alpha)$. Finally in Section 4, we shall give some examples.

ACKNOWLEDGEMENT. The author would like to express her gratitude to the referees for their suggestions.

2. Algebraic independence of Mahler functions. Let C be a field of characteristic 0, L the rational function field $C(z_1, \dots, z_n)$ and M the quotient field of the formal power series ring $C[[z_1, \dots, z_n]]$. Let Ω be an $n \times n$ matrix with nonnegative integer entries which is nonsingular and has no roots of unity as eigenvalues. We define an endomorphism $\tau: M \to M$ by

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

where Ωz is defined as in Section 1.

The following lemma, which is more general than Lemma 1 in Loxton-van der Poorten [4], can be proved in the same way.

LEMMA 1. *If $g \in M$ satisfies*

$$g^{\tau} = cg + d, \qquad c, d \in C,$$

then $g \in C$.

PROOF. From the theory of nonnegative matrices (cf. Gantmacher [1]), the matrix Ω has a positive eigenvalue $\rho(>1)$ such that no eigenvalue of Ω has modulus exceeding ρ, and to this dominant eigenvalue there corresponds a nonnegative eigenvector u such that $\Omega u = \rho u$. By renumbering the variables, if necessary, we may take $u = {}^t(u_1, \ldots, u_m, 0, \ldots, 0)$ with $u_1, \ldots, u_m > 0$. This forces Ω to have the partitioned form

$$\Omega = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix},$$

where A is $m \times m$ and D is $(n-m) \times (n-m)$ and A and D are nonsingular and have no roots of unity as eigenvalues.

We prove the lemma by induction on n. The lemma is immediate in the case $n=1$. We put

$$\{R = \langle \mu, u \rangle \mid \mu \in N^n\} = \{R_0, R_1, \ldots\}, \qquad 0 = R_0 < R_1 < \cdots,$$

where $\langle \mu, u \rangle = \mu_1 u_1 + \cdots + \mu_n u_n$ for $\mu = (\mu_1, \ldots, \mu_n)$, $u = (u_1, \ldots, u_n)$. If $f(z) \in C[[z_1, \ldots, z_n]]$, we can decompose it as follows:

$$f(z) = \sum_R f_R(z), \qquad \text{with} \quad f_R(z) = \sum_{\langle \mu, u \rangle = R} f_\mu z^\mu,$$

where R runs through the sequence $\{R_k\}_{k \geq 0}$ and each $f_R(z)$ is a polynomial in $z' = (z_1, \ldots, z_m)$ of which the coefficients are power series of $z'' = (z_{m+1}, \ldots, z_n)$. Note that, if we write $z_j = y_j s^{u_j}$ for $1 \leq j \leq n$, then

$$f_R(z) = f_R(y) s^R, \qquad f_R(\Omega z) = f_R(\Omega y) s^{\rho R}.$$

We suppose $g(z) \neq 0$ and

$$g(z) = p(z)/q(z), \qquad p(z), q(z) \in C[[z_1, \ldots, z_n]].$$

Letting $p(z) = \sum_R p_R(z)$, $q(z) = \sum_R q_R(z)$, we have

$$(*) \qquad \left(\sum_R p_R(\Omega y) s^{\rho R}\right)\left(\sum_R q_R(y) s^R\right)$$
$$= c\left(\sum_R p_R(y) s^R\right)\left(\sum_R q_R(\Omega y) s^{\rho R}\right) + d\left(\sum_R q_R(y) s^R\right)\left(\sum_R q_R(\Omega y) s^{\rho R}\right).$$

Take the least R_i and R_j such that $p_{R_i}(y) \neq 0$ and $q_{R_j}(y) \neq 0$, respectively. We observe that $R_i = R_j$. For if $R_i > R_j$, then the term with least degree in s on the left hand side above is $p_{R_i}(\Omega y) q_{R_j}(y) s^{\rho R_i + R_j}$ and that of the right hand side above is

$dq_{R_j}(y)q_{R_j}(\Omega y)s^{R_j+\rho R_j}$, a contradiction. In the case $R_i<R_j$, we can also deduce a contradiction. Hence $R_i=R_j$ and comparing the coefficients of the terms of lowest degree in s of both sides, we have

$$p_{R_i}(\Omega y)q_{R_i}(y)=cp_{R_i}(y)q_{R_i}(\Omega y)+dq_{R_i}(y)q_{R_i}(\Omega y)\,.$$

We shall show below that this implies $p_{R_i}(y)/q_{R_i}(y)\in C$. We omit the subscript R_i. We can write $p(y)$ and $q(y)$ as polynomials in $y'=(y_1,\dots,y_m)$, say,

$$p(y)=\sum_{\mu} p_\mu(y'')y'^{\mu}\,,\qquad q(y)=\sum_{\mu} q_\mu(y'')y'^{\mu}\,,$$

where the coefficients are power series in $y''=(y_{m+1},\dots,y_n)$. Then

$$p(\Omega^k y)=\sum_{\mu} p_\mu(D^k y'')y''^{\mu(BD^{k-1}+ABD^{k-2}+\cdots+A^{k-1}B)}y'^{\mu A^k}\,,$$

$$q(\Omega^k y)=\sum_{\mu} q_\mu(D^k y'')y''^{\mu(BD^{k-1}+ABD^{k-2}+\cdots+A^{k-1}B)}y'^{\mu A^k}\,.$$

We define the rank of a term ay'^{μ}, with $a\neq 0$, to be μ. Ranks are ordered lexicographically. For $k=0,1,2,\dots$, let $\mu_k A^k$ and $\nu_k A^k$ be the exponents of the terms of lowest rank in the polynomials $p(\Omega^k y)$ and $q(\Omega^k y)$, respectively. The ranks μ_k and ν_k are uniquely determined since A is nonsingular. Because ν_k has only finitely many possibilities, there are a vector ν and an infinite set Λ of nonnegative integers such that $\nu_k=\nu$ for any $k\in\Lambda$. Since μ_k also has only finitely many possibilities, there are nonnegative integers $h,k\in\Lambda$ such that $h<k$ and $\mu_h=\mu_k(=\mu)$. Since

$$\frac{p(\Omega^h y)}{q(\Omega^h y)}=c^h\frac{p(y)}{q(y)}+(c^{h-1}+c^{h-2}+\cdots+1)d\,,$$

$$\frac{p(\Omega^k y)}{q(\Omega^k y)}=c^k\frac{p(y)}{q(y)}+(c^{k-1}+c^{k-2}+\cdots+1)d\,,$$

we have

$$\frac{p(\Omega^k y)}{q(\Omega^k y)}=c^{k-h}\frac{p(\Omega^h y)}{q(\Omega^h y)}+d'\,.$$

Therefore

$$p(\Omega^k y)q(\Omega^h y)=c^{k-h}p(\Omega^h y)q(\Omega^k y)+d'q(\Omega^k y)q(\Omega^h y)\,.$$

The terms of lowest rank of $p(\Omega^k y)q(\Omega^h y)$, $p(\Omega^h y)q(\Omega^k y)$ and $q(\Omega^k y)q(\Omega^h y)$ are $\mu_k A^k+\nu_h A^h$, $\mu_h A^h+\nu_k A^k$ and $\nu_k A^k+\nu_h A^h$, respectively. Hence two of these are equal and so $\mu=\nu$. Comparing the coefficients of the terms of lowest rank on the left and right hand sides, we get

$$p_\mu(D^k y'')q_\mu(D^h y'')=c^{k-h}p_\mu(D^h y'')q_\mu(D^k y'')+d'q_\mu(D^k y'')q_\mu(D^h y'').$$

By the induction hypothesis, $p_\mu(D^h y'')=aq_\mu(D^h y'')$ for some $a\in C^\times$, and therefore $p_\mu(y'')=aq_\mu(y'')$. If we put $r(y)=p(y)-aq(y)$, then $r(y)$ has no term of rank $\mu=\nu$ and

$$\begin{aligned} r(\Omega y)q(y)&=p(\Omega y)q(y)-aq(\Omega y)q(y)\\ &=cp(y)q(\Omega y)+dq(y)q(\Omega y)-aq(\Omega y)q(y)\\ &=cr(y)q(\Omega y)+(ca+d-a)q(y)q(\Omega y). \end{aligned}$$

If $r(y)\neq 0$, we can apply the above construction to $r(y)$ in place of $p(y)$ and reach a contradiction. Thus $r(y)=0$ and $p_{R_i}(y)=aq_{R_i}(y)$, where $a=ca+d$. Next we shall prove that $p_{R_j}(y)=aq_{R_j}(y)$ for any $j\geq i$ by induction on j. We may assume $c\neq 0$. We compare the coefficients of $s^{\rho R_i+R_j}$ on both sides of $(*)$. If $\rho R_i+R_j=\rho R_{i'}+R_{j'}$ for some $(i',j')\neq(i,j)$, $(i',j'\geq i)$, we can easily see that $i',j'<j$. By the induction hypothesis, we get

$$p_{R_{i'}}(y)=aq_{R_{i'}}(y),\qquad p_{R_{j'}}(y)=aq_{R_{j'}}(y).$$

Hence

$$aq_{R_i}(\Omega y)q_{R_j}(y)=p_{R_i}(\Omega y)q_{R_j}(y)=cp_{R_j}(y)q_{R_i}(\Omega y)+dq_{R_j}(y)q_{R_i}(\Omega y).$$

Dividing both sides by $q_{R_i}(\Omega y)$, we get

$$aq_{R_j}(y)=cp_{R_j}(y)+dq_{R_j}(y).$$

Since $a-d=ca$ and $c\neq 0$, we have $p_{R_j}(y)=aq_{R_j}(y)$. Hence the assertion is proved and we get $g(z)=p(z)/q(z)=a$.

THEOREM 3. *Suppose that $f_{ij}\in M$ $(i=1,\dots,k,j=1,\dots,n(i))$ satisfy the functional equation*

$$\begin{pmatrix} f_{i1}^\tau\\ \vdots\\ \vdots\\ f_{i\,n(i)}^\tau \end{pmatrix}=\begin{pmatrix} a_i & & & 0\\ a_{21}^{(i)} & a_i & & \\ \vdots & & \ddots & \\ a_{n(i)1}^{(i)} & \cdots & a_{n(i)\,n(i)-1}^{(i)} & a_i \end{pmatrix}\begin{pmatrix} f_{i1}\\ \vdots\\ \vdots\\ f_{i\,n(i)} \end{pmatrix}+\begin{pmatrix} b_{i1}\\ \vdots\\ \vdots\\ b_{i\,n(i)} \end{pmatrix},$$

where a_i, $a_{st}^{(i)}\in C$, $a_i\neq 0$, $a_{s\,s-1}^{(i)}\neq 0$ and $b_{ij}\in L$. If f_{ij} $(i=1,\dots,k,j=1,\dots,n(i))$ are algebraically dependent over L, then there exist a nonempty subset $\{i_1,\dots,i_r\}$ of $\{1,\dots,k\}$ and nonzero elements $c_1,\dots,c_r$ of C such that

$$a_{i_1}=\cdots=a_{i_r},\qquad g=c_1f_{i_11}+\cdots+c_rf_{i_r1}\in L.$$

Here g satisfies $g^\tau=a_{i_1}g+c_1b_{i_11}+\cdots+c_rb_{i_r1}$.

PROOF. We prove the theorem by induction on $\sum_{i=1}^k n(i)$. We assume that $\sum_{i=1}^k n(i)\geq 1$ and that f_{ij} $(i=1,\dots\ k,j=1,\dots,n(i))$ are algebraically dependent over L.

By the induction hypothesis we may assume f_{ij} $(i=1,\dots,k,\ j=1,\dots,n(i))$ except $f_{kn(k)}$ are algebraically independent over L. Let X_{ij} $(i=1,\dots,k,\ j=1,\dots,n(i))$ be indeterminates and define an endomorphism T of the polynomial ring $M[X]$ by

$$Ta=a^{\tau} \qquad (a\in M),$$

$$\begin{pmatrix} TX_{i1} \\ \vdots \\ \vdots \\ TX_{i\,n(i)} \end{pmatrix} = \begin{pmatrix} a_i & & & 0 \\ a_{21}^{(i)} & a_i & & \\ \vdots & & \ddots & \\ a_{n(i)1}^{(i)} & \cdots & a_{n(i)\,n(i)-1}^{(i)} & a_i \end{pmatrix} \begin{pmatrix} X_{i1} \\ \vdots \\ \vdots \\ X_{i\,n(i)} \end{pmatrix} + \begin{pmatrix} b_{i1} \\ \vdots \\ \vdots \\ b_{i\,n(i)} \end{pmatrix}.$$

There exists a nonconstant polynomial $F\in L[X]$ such that $F(f)=0$. We may assume F to be irreducible. Put

$$F=\sum_I b_I X^I \qquad (b_I\in L).$$

Then

$$TF(f)=\sum_I b_I^{\tau}(f^{\tau})^I=\Big(\sum_I b_I f^I\Big)^{\tau}=0.$$

As a polynomial of $X_{kn(k)}$, F divides TF. Since F is irreducible in $L[X]$, F divides TF in $L[X]$. Comparing the total degrees of F and TF, we have

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

The nonzero monomials of F can be ordered lexicographically with

$$X_{11}<X_{12}<\cdots<X_{1n(i)}<X_{21}<\cdots<X_{kn(k)}.$$

We may assume that the coefficient of the largest term of F is 1. Comparing the coefficients of the largest terms of TF and aF, we get $a\in C$. Let P be a polynomial with the least total degree among the nonconstant elements of $L[X]$ such that

$$TF=aF+c \qquad \text{for some} \quad a,c\in C.$$

Suppose that

$$TP=aP+c, \qquad a,c\in C. \tag{2}$$

We denote by D_{ij} the derivation $\partial/\partial X_{ij}$. Then we have

$$a_i TD_{i\,n(i)}P=D_{i\,n(i)}TP=D_{i\,n(i)}(aP+c)=aD_{i\,n(i)}P.$$

Since

$$\text{total deg } D_{i\,n(i)}P<\text{total deg } P,$$

$D_{i\,n(i)}P$ must belong to L. By Lemma 1 we obtain

$$D_{i\,n(i)}P = c_{i\,n(i)} \in C\,.$$

Then $Q = P - \sum_{i=1}^{k} c_{i\,n(i)} X_{i\,n(i)}$ is a polynomial of X_{ij} $(i=1,\ldots,k,\, j=1,\ldots,n(i)-1)$ with coefficients in L. Since

$$D_{i\,n(i)-1}TQ = a_i T D_{i\,n(i)-1} Q = a_i T D_{i\,n(i)-1} P\,,$$

$$D_{i\,n(i)-1}TQ = D_{i\,n(i)-1}\left(aP + c - \sum_{r=1}^{k} c_{rn(r)}\left(\sum_{s=1}^{n(r)} a_{n(r)s}^{(r)} X_{rs} + b_{rn(r)}\right)\right)$$

$$= aD_{i\,n(i)-1}P - c_{i\,n(i)} a_{n(i)\,n(i)-1}^{(i)}$$

and

$$\text{total deg}\, D_{i\,n(i)-1}P < \text{total deg}\, P\,,$$

$D_{i\,n(i)-1}P$ must belong to L. By Lemma 1,

$$D_{i\,n(i)-1}P = c_{i\,n(i)-1} \in C\,.$$

Continuing this, we obtain

$$P = \sum_{i,j} c_{ij} X_{ij} + b \qquad (c_{ij} \in C,\, b \in L)\,.$$

By the equality (2),

$$TP = \sum_{i,j} c_{ij}(a_i X_{ij} + a_{j\,j-1}^{(i)} X_{i\,j-1} + \cdots + a_{j1}^{(i)} X_{i1} + b_{ij}) + b^{\tau} \tag{3}$$

$$= a\left(\sum_{i,j} c_{ij} X_{ij} + b\right) + c\,.$$

Let $\{i_1, \ldots, i_r\}$ be the set of i for which there exists nonzero c_{ij} for some j and define

$$J_h = \max\{\, j \mid c_{i_h j} \neq 0\}\,, \qquad 1 \leq h \leq r\,.$$

Comparing the coefficient of $X_{i_h J_h}$ on the left hand side with the right hand side in (3), we have $c_{i_h J_h} a_{i_h} = a c_{i_h J_h}$ and therefore $a_{i_1} = \cdots = a_{i_r} = a$. Assume $J_h > 1$ for some h. Comparing the coefficient of $X_{i_h\,J_h-1}$ in (3), we have

$$c_{i_h\,J_h} a_{J_h\,J_h-1}^{(i_h)} + c_{i_h\,J_h-1} a_{i_h} = a c_{i_h\,J_h-1}\,.$$

This contradicts the assumption $a_{J_h J_h-1}^{(i_h)} \neq 0$. Therefore $J_h = 1$ for every h and

$$P = \sum_{h=1}^{r} c_{i_h 1} X_{i_h 1} + b\,, \qquad c_{i_h 1} \neq 0\,, \quad b \in L\,.$$

By the equality (3),

$$TP=\sum_{h=1}^{r} c_{i_h1}(a_{i_h}X_{i_h1}+b_{i_h1})+b^\tau=a\left(\sum_{h=1}^{r} c_{i_h1}X_{i_h1}+b\right)+c$$

and therefore

$$\sum_{h=1}^{r} c_{i_h1}b_{i_h1}+b^\tau=ab+c\ .$$

By this we obtain

$$\left(\sum_{h=1}^{r} c_{i_h1}f_{i_h1}+b\right)^\tau=\sum_{h=1}^{r} c_{i_h1}(af_{i_h1}+b_{i_h1})+b^\tau=a\left(\sum_{h=1}^{r} c_{i_h1}f_{i_h1}+b\right)+c\ .$$

By Lemma 1, $\sum_{h=1}^{r} c_{i_h1}f_{i_h1}+b$ must belong to C. This completes the proof.

THEOREM 4. *Let $f_1(z),\dots,f_m(z)\in M$ satisfy the functional equation* (1), *where A is an $m\times m$ matrix with entries in C and $b_i(z)\in L$. If $f_1,\dots,f_m$ are algebraically dependent over L, then there exist $c_1,\dots,c_m\in C$, not all zero, such that*

$$\sum_{i=1}^{m} c_if_i\in L\ .$$

PROOF. When $\det A=0$, the assertion is trivial. Thus we assume $\det A\neq 0$. Let $B=P^{-1}A^{-1}P$ be the Jordan canonical form of the matrix A^{-1}, where B and P are $m\times m$ matrices with entries in the algebraic closure $\bar{C}$ of C. Then we have

$$P^{-1}\begin{pmatrix} f_1^\tau \\ \vdots \\ f_m^\tau \end{pmatrix}=P^{-1}\left(A^{-1}\begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}-A^{-1}\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}\right)=BP^{-1}\begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}-P^{-1}A^{-1}\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

By applying Theorem 3 to the matrix B, there exists a nonzero vector $(c_1,\dots,c_m)\in\bar{C}^m$ such that

$$g(z)=(c_1,\dots,c_m)P^{-1}\begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}\in\bar{C}(z_1,\dots,z_n)\ .$$

Putting $(d_1,\dots,d_m)=(c_1,\dots,c_m)P^{-1}$, we get

$$g=d_1f_1+\cdots+d_mf_m\ ,$$

where $d_1,\dots,d_m$ are not all zero. We can put

$$g=p/q\ ,\qquad p\in\bar{C}[z_1,\dots,z_n]\ ,\quad q\in C[z_1,\dots,z_n]\ .$$

Let $f\in C[[z_1,\dots,z_n]]$ be a common denominator of $f_1,\dots,f_m$. There exist elements $\beta_1,\dots,\beta_s$ of $\bar{C}$ which are linearly independent over C such that $d_1,\dots,d_m$ and the coefficients of p are linear combinations of $\beta_1, \ldots, \beta_s$ over C. Comparing the coefficients of β_i in the equality

$$fqf_1d_1 + \cdots + fqf_md_m = fp ,$$

we complete the proof.

LEMMA 2. *If $A, B \in C[z_1, \ldots, z_n]$ are coprime, then so are A^τ and B^τ.*

PROOF. We may assume C to be algebraically closed. Assume that an irreducible polynomial P divides both A^τ and B^τ. Let $x = (x_1, \ldots, x_n)$ be a generic point of the algebraic variety defined by P over C. Since $A^\tau(x) = B^\tau(x) = 0$, we know that Ωx is a zero of both A and B. By the fact that

$$\text{trans.deg}_C C(\Omega x) = \text{trans.deg}_C C(x) = n-1 ,$$

Ωx is a generic point of the algebraic variety defined by an irreducible polynomial Q over C. Hence Q divides both A and B, a contradiction.

THEOREM 5. *Let $f_1, \ldots, f_m \in M$ satisfy the assumptions of Theorem 4 and $b_i(z) \in C[z_1, \ldots, z_n]$ for every i. If $f_1, \ldots, f_m$ are algebraically dependent over L, then there exist $c_1, \ldots, c_m \in C$, not all zero, such that*

$$\sum_{i=1}^{m} c_i f_i \in C[z_1, \ldots, z_n] .$$

PROOF. When $\det A = 0$, the assertion is trivial. We thus assume $\det A \neq 0$. In the same way as in the proof of Theorem 4, we get $g \in \bar{C}(z_1, \ldots, z_n)$, where g satisfies a functional equation

$$g^\tau = ag + b , \qquad a \in \bar{C} , \quad b \in \bar{C}[z_1, \ldots, z_n] .$$

Put $g = A/B$, where $A, B \in \bar{C}[z_1, \ldots, z_n]$ are coprime. Then by Lemma 2, A^τ and B^τ are coprime and

$$BA^\tau = aAB^\tau + bBB^\tau .$$

Therefore B^τ divides B and B divides B^τ. Hence $B^\tau/B \in \bar{C}$. By Lemma 1, B must belong to $\bar{C}$ and so $g \in \bar{C}[z_1, \ldots, z_n]$. We can complete the proof in the same way as in the proof of Theorem 4.

3. Algebraic independence of the values of Mahler functions. The following lemma was proved by Loxton and van der Poorten (cf. [9]). We restate it here for the reader's convenience.

LEMMA 3. *Suppose that Ω, α satisfy the properties* (I)–(IV) *and*

$$\psi(z; x) = \sum_{i=1}^{q} \sum_{j=1}^{d_i} \theta_i^x x^{j-1} g_{ij}(z) ,$$

where θ_i *are distinct nonzero complex numbers and* $g_{ij}(z)\in \boldsymbol{C}[[z_1,\dots,z_n]]$ *are regular at the origin. If* $\psi(\Omega^k\alpha, k)=0$ *for all sufficiently large* k, *then* $g_{ij}(z)=0$ *for every* i, j.

PROOF. We prove this by induction on $\sum_{i=1}^q d_i$. If $\sum_{i=1}^q d_i=1$, the lemma is true by the property (IV). Let $\sum_{i=1}^q d_i>1$ and $g(z)=g_{qd_q}(z)\neq 0$. We may assume $\theta_q=1$. Consider

$$\xi(z;x)=g(\Omega z)\psi(z;x)-g(z)\psi(\Omega z;x+1)=\sum_{i=1}^{q-1}\sum_{j=1}^{d_i}\theta_i^x x^{j-1}h_{ij}(z)+\sum_{j=1}^{d_q-1}x^{j-1}h_j(x),$$

where

$$h_j(z)=g(\Omega z)g_{qj}(z)-g(z)\sum_{s=j}^{d_q}\binom{s-1}{j-1}g_{qs}(\Omega z)\qquad (j=1,\dots,d_q-1)$$

and

$$h_{ij}(z)=g(\Omega z)g_{ij}(z)-\theta_i g(z)\sum_{s=j}^{d_i}\binom{s-1}{j-1}g_{is}(\Omega z)\qquad (j=1,\dots,q-1, j=1,\dots,d_i).$$

Now, $\xi(\Omega^k\alpha;k)=0$ for all sufficiently large k, so by the induction hypothesis, $h_j(z)$ and $h_{ij}(z)$ are all identically zero. Since

$$h_{d_q-1}(z)=g(\Omega z)g_{q\,d_q-1}(z)-g(z)(g_{q\,d_q-1}(\Omega z)+(d_q-1)g_{qd_q}(\Omega z))=0,$$

we have

$$\frac{g_{q\,d_q-1}(z)}{g(z)}=\frac{g_{q\,d_q-1}(\Omega z)}{g(\Omega z)}+d_q-1.$$

By Lemma 1, $g_{q\,d_q-1}(z)/g(z)\in \boldsymbol{C}$, and so $d_q-1=0$. By the assumption $\sum_{i=1}^q d_i>1$, we know that $q\geq 2$ and

$$h_{1d_1}(z)=g(\Omega z)g_{1d_1}(z)-\theta_1 g(z)g_{1d_1}(\Omega z)=0.$$

Thus $g_{1d_1}(z)/g(z)\in \boldsymbol{C}$ by Lemma 1. Since $\theta_1\neq 1$, we have $g_{1d_1}(z)=0$. By the induction hypothesis, $g_{ij}(z)$ are all identically zero.

THEOREM 6. *Suppose that* $f_1(z),\dots,f_m(z)\in K[[z_1,\dots,z_n]]$ *satisfy the functional equation* (1), Ω, α *satisfy the properties* (I)–(IV) *and for all* $k\geq 0$, $\Omega^k\alpha\in U$ *and* $b_i(z)$ *are defined at* $\Omega^k\alpha$. *If* $f_1(z),\dots,f_m(z)$ *are algebraically independent over* $K(z_1,\dots,z_n)$, *then* $f_1(\alpha),\dots,f_m(\alpha)$ *are algebraically independent.*

We note that $f_1(z),\dots,f_m(z)$ are algebraically independent over $K(z_1,\dots,z_n)$ if and only if they are algebraically independent over $\boldsymbol{C}(z_1,\dots,z_n)$.

PROOF. We may assume that $\alpha_1,\dots,\alpha_n$ and the eigenvalues of A are all contained in K. Since $f_1(z),\dots,f_m(z)$ are algebraically independent over $K(z_1,\dots,z_n)$, we have $\det A\neq 0$. By the functional equation (1), we have

$$f(z)=A^k f(\Omega^k z)+\sum_{j=0}^{k-1} A^j b(\Omega^j z)=A^k f(\Omega^k z)+b^{(k)}(z)\,, \qquad b^{(k)}(z)=\sum_{j=0}^{k-1} A^j b(\Omega^j z)\,.$$

Replacing Ω by any convenient power of Ω, we may assume that the multiplicative subgroup generated by the eigenvalues of A is torsion free. Assume that $f_1(\alpha), \dots, f_m(\alpha)$ are algebraically dependent. Then there is a relation of algebraic dependence

$$\sum_{\substack{\mu=(\mu_1,\dots,\mu_m)\\ |\mu|=\mu_1+\cdots+\mu_m\le L}} \tau_\mu f_1(\alpha)^{\mu_1}\cdots f_m(\alpha)^{\mu_m}=0\,,$$

where τ_μ are integers not all zero. Let t_μ $(\mu=(\mu_1,\dots,\mu_m), |\mu|\le L)$ be indeterminates and put

$$F(z;t)=\sum_{\substack{\mu=(\mu_1,\dots,\mu_m)\\ |\mu|=\mu_1+\cdots+\mu_m\le L}} t_\mu f_1(z)^{\mu_1}\cdots f_m(z)^{\mu_m}=\sum_\mu t_\mu f(z)^\mu\,.$$

We define $t_\mu^{(k)}$ by the equality

$$F(z;t)=\sum_\mu t_\mu f(z)^\mu=\sum_\mu t_\mu(A^k f(\Omega^k z)+b^{(k)}(z))^\mu=\sum_\mu t_\mu^{(k)} f(\Omega^k z)^\mu\,.$$

Let $x_{11},\dots,x_{1m},\dots,x_{m1},\dots,x_{mm}, w_1,\dots,w_m, y_1,\dots,y_m$ be indeterminates and put

$$\sum_\mu t_\mu\left(\begin{pmatrix} x_{11} & \cdots & x_{1m}\\ \vdots & & \vdots\\ x_{m1} & \cdots & x_{mm}\end{pmatrix}\begin{pmatrix} w_1\\ \vdots\\ w_m\end{pmatrix}+\begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix}\right)^\mu=\sum_\mu T_\mu(t;x;y)w^\mu\,.$$

Then $t_\mu^{(k)}=T_\mu(t;A^k;b^{(k)}(z))$ and

$$F(z;t)=F(\Omega^k z;T(t;A^k;b^{(k)}(z)))\,.$$

Therefore

$$0=F(\alpha;\tau)=F(\Omega^k\alpha;T(\tau;A^k;b^{(k)}(\alpha)))\,. \tag{4}$$

We note that $T_\mu(\tau;A^0;b^{(0)}(z))=\tau_\mu$. Put

$$V(\tau)=\{Q(t)\in K[t]\,|\,Q(T(\tau;A^k;y))=0 \text{ for any } k\ge 0\}\,.$$

PROPOSITION 1. *$V(\tau)$ is a prime ideal of $K[t]$.*

PROOF. $Q(T(\tau;A^k;y))$ is a linear recurrence with characteristic roots in a torsion free group. Here a linear recurrence is a sequence of the form

$$\sum_{i=1}^q g_i(k)\theta_i^k\,, \qquad k\ge 0\,,$$

where $g_1(x),\dots,g_q(x)$ are polynomials in x and $\theta_1,\dots,\theta_q$ are the characteristic roots.

Suppose that $Q_1, Q_2 \in K[t]$ and $Q_1 Q_2 \in V(\tau)$. Then for every k, at least one of $Q_1(T(\tau; A^k; y))$ and $Q_2(T(\tau; A^k; y))$ is zero. Thus one of these linear recurrences has infinitely many zeros, and so it is a zero linear recurrence by Skolem-Lech-Mahler's theorem.

PROPOSITION 2. *If $P(z; t)$ is a polynomial in the variables $z=(z_1, \dots, z_n)$ and $t=(t_\mu)$, then the following assertions are equivalent.*

(i) $P(\Omega^k\alpha; T(\tau; A^k; b^{(k)}(\alpha)))=0$ *for all large* k.

(ii) *If* $P(z; t)=\sum_\lambda Q_\lambda(t) z^\lambda$, *then* $Q_\lambda(t) \in V(\tau)$ *for every* λ.

PROOF. Assume (i) and put

$$Q_\lambda(T(\tau; A^k; f(\alpha)-A^k w))=\sum_\mu R_{\lambda\mu}(k) w^\mu .$$

Then $R_{\lambda\mu}(k)$ are linear recurrences and since $b^{(k)}(\alpha)=f(\alpha)-A^k f(\Omega^k\alpha)$,

$$P(\Omega^k\alpha; T(\tau; A^k; b^{(k)}(\alpha)))=\sum_\lambda \sum_\mu R_{\lambda\mu}(k) f(\Omega^k\alpha)^\mu (\Omega^k\alpha)^\lambda .$$

By Lemma 3, $R_{\lambda\mu}(k)$ are zero linear recurrences since $z, f_1(z), \dots, f_m(z)$ are algebraically independent over K. Hence

$$Q_\lambda(T(\tau; A^k; f(\alpha)-A^k w))=0$$

for every $k \geq 0$. Since $w_1, \dots, w_m$ are variables,

$$Q_\lambda(T(\tau; A^k; y))=0$$

for every $k \geq 0$ and so $Q_\lambda(t) \in V(\tau)$. The converse is immediate.

DEFINITION. If $P(z; t)=\sum_\lambda p_\lambda(t) z^\lambda$ is a formal power series in the variables $z_1, \dots, z_n$ with coefficients in $K[t]$, then the *index* of $P(z; t)$ is defined to be the least integer $|\lambda|$ for which $P_\lambda(t) \notin V(\tau)$. If there are no such integers, we define the *index* of $P(z; t)$ is ∞.

By Proposition 1, we have

$$\operatorname{index}(P_1(z; t) P_2(z; t))=\operatorname{index} P_1(z; t)+\operatorname{index} P_2(z; t) .$$

PROPOSITION 3. $\operatorname{index} F(z; t)<\infty$.

PROOF. $F(z; \tau) \neq 0$, since $f_1(z), \dots, f_m(z)$ are algebraically independent. By the property (IV), there exists k_0 such that $F(\Omega^{k_0}\alpha; \tau) \neq 0$. Suppose that

$$F(z; t)=\sum_\lambda p_\lambda(t) z^\lambda$$

and $\operatorname{index} F(z; t)=\infty$. Then $p_\lambda(t) \in V(\tau)$ for every λ and therefore

$$F(\Omega^{k_0}\alpha; \tau)=\sum_\lambda p_\lambda(T(\tau; A^0; b^{(0)}(\Omega^{k_0}\alpha)))(\Omega^{k_0}\alpha)^\lambda=0 ,$$

a contradiction.

Let p be a nonnegative integer, $R(p)$ the K-vector space of polynomials in $K[t]$ of degree at most p in each t_μ, and $d(p)$ the dimension over K of the factor space $\bar{R}(p)=R(p)/(R(p)\cap V(\tau))$. The coset containing a polynomial $P(t)$ of $R(p)$ in $\bar{R}(p)$ is denoted by $\bar{P}(t)$.

PROPOSITION 4. $d(2p)\leq 2^{(L+1)^m}d(p)$.

PROOF. Every polynomial $Q(t)\in R(2p)$ can be written in the form

$$Q(t)=\sum_{\varepsilon}\left(\prod_{\mu} t_\mu^{\varepsilon(\mu)p}\right)Q_\varepsilon(t),$$

where ε ranges through the functions from $\{\mu\}_{|\mu|\leq L}$ to $\{0,1\}$ and $Q_\varepsilon(t)\in R(p)$. Let $P_\varepsilon(t)=\prod_\mu t_\mu^{\varepsilon(\mu)p}$. If $\{\bar{Q}_1(t),\dots,\bar{Q}_{d(p)}(t)\}$ is a basis of $\bar{R}(p)$, then $\{\bar{P}_\varepsilon(t)\bar{Q}_i(t)\}_{i,\varepsilon}$ generates $\bar{R}(2p)$.

PROPOSITION 5. *Let p be a sufficiently large natural number. Then there are polynomials $P_0(z;t),\dots,P_p(z;t)\in K[z;t]$ with algebraic integer coefficients and degrees at most p in each variable such that the following assumptions are satisfied.*

(i) index $P_0(z;t)<\infty$.

(ii) index$(\sum_{h=0}^{p}P_h(z;t)F(z;t)^h)\geq c_1(p+1)^{1+n^{-1}}$, *where c_1 is a positive constant.*

PROOF. If $\{\bar{Q}_1^{(p)}(t),\dots,\bar{Q}_{d(p)}^{(p)}(t)\}$ is a basis of $\bar{R}(p)$ over K, a typical polynomial $P_h(z;t)$ can be expressed in the form

$$P_h(z;t)=\sum_\lambda P_{h\lambda}(t)z^\lambda,\quad \bar{P}_{h\lambda}(t)=\sum_{i=1}^{d(p)}g_{h\lambda i}\bar{Q}_i^{(p)}(t)\qquad (q_{h\lambda i}\in K).$$

Let

$$E(z;t)=\sum_{h=0}^{p}P_h(z;t)F(z;t)^h=\sum_\lambda E_\lambda(t)z^\lambda.$$

Then $E_\lambda(t)\in R(2p)$ and we obtain expressions for the $\bar{E}_\lambda(t)$ which can be written in terms of $\bar{Q}_1^{(2p)}(t),\dots,\bar{Q}_{d(2p)}^{(2p)}(t)$. The coefficients of $\bar{Q}_i^{(2p)}(t)$ $(i=1,\dots,d(2p))$ are a system of $d(2p)$ homogeneous linear forms of $g_{h\lambda i}$ over K whose simultaneous vanishing is equivalent to $\bar{E}_\lambda(t)=\bar{0}$. If we wish $E(z;t)$ to have index at least equal to $J=[2^{-(L+1)^m n^{-1}}(p+1)^{1+n^{-1}}]-1$, then we have to solve a system of $\binom{J+n-1}{n}d(2p)\,(\leq J^n d(2p))$ homogeneous linear equations in $(p+1)^{n+1}d(p)$ variables $g_{h\lambda i}$. By Proposition 4, we have

$$(p+1)^{n+1}d(p)>J^n 2^{(L+1)^m}d(p)\geq J^n d(2p).$$

This implies that there is a function $E(z;t)$ with index $I\geq J$ such that index $P_h(z;t)\neq\infty$ for some h. Let r be the smallest among such h and put

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

Then

$$I=\operatorname{index} F(z;t)^r E_0(z;t)=r \operatorname{index} F(z;t)+\operatorname{index} E_0(z;t).$$

By Proposition 3, we have

$$\operatorname{index} E_0(z;t)\geq c_1(p+1)^{1+n^{-1}},$$

and so $E_0(z;t)$ satisfies (i) and (ii).

Let $E(z;t)$ be the $\sum_{h=0}^{p} P_h(z;t)F(z;t)^h$ in Proposition 5, and $I=\operatorname{index} E(z;t)$. In what follows, $c_1, c_2, \ldots$ are positive constants independent of k, p while $c_1(p), c_2(p), \ldots$ are positive constants depending on p and independent of k.

PROPOSITION 6. *If $k>c_2(p)$, then*

$$\log|E(\Omega^k\alpha;T(\tau;A^k;b^{(k)}(\alpha)))|\leq -c_3(p+1)^{1+n^{-1}}\rho^k.$$

PROOF. By the equality

$$f(\alpha)=A^k f(\Omega^k\alpha)+b^{(k)}(\alpha),$$

we have $|b_i^{(k)}(\alpha)|\leq c_4^k$ and

$$|T(\tau;A^k;b^{(k)}(\alpha))|\leq c_5^k.$$

$E(z;t)$ is a polynomial in the variables t with degree at most $2p$ in each variable whose coefficients are power series convergent in U. Letting

$$E(z;t)=\sum_{\nu} g_\nu(z)t^\nu, \qquad g_\nu(z)=\sum_{\lambda} g_{\nu\lambda}z^\lambda,$$

we have

$$|g_{\nu\lambda}|\leq c_6(p)c_7^{|\lambda|}$$

and

$$E(z;t)=\sum_{\lambda}\left(\sum_{\nu} g_{\nu\lambda}t^\nu\right)z^\lambda.$$

Therefore

$$|E(\Omega^k\alpha;T(\tau;A^k;b^{(k)}(\alpha)))|\leq \sum_{|\lambda|\geq I} c_8(p)c_7^{|\lambda|}c_9^{pk}|(\Omega^k\alpha)^\lambda|.$$

By the property (III), $|\alpha_i^{(k)}|\leq \varepsilon^{\rho^k}$ for some $\varepsilon<1$. Therefore, if $k>c_{10}(p)$, then

$$|E(\Omega^k\alpha;\, T(\tau;\, A^k;\, b^{(k)}(\alpha)))| \le c_8(p)c_9^{pk} \sum_{i=1}^{n} \sum_{\substack{\lambda_1,\dots,\lambda_n \ge 0 \\ \lambda_i \ge I/n}} (c_7\varepsilon^{\rho^k})^{\lambda_1+\cdots+\lambda_n}$$

$$\le nc_8(p)c_9^{pk}(c_7\varepsilon^{\rho^k})^{I/n}/(1-c_7\varepsilon^{\rho^k})^n\,.$$

This implies the proposition.

If α is an algebraic number, we denote by $\overline{|\alpha|}$ the maximum of the absolute values of the conjugates of α and by $\mathrm{den}(\alpha)$ the least positive integer such that $\mathrm{den}(\alpha)\alpha$ is an algebraic integer, and we set $\|\alpha\| = \max\{\overline{|\alpha|}, \mathrm{den}(\alpha)\}$. Let $\alpha \in K^\times$ and $D = \mathrm{den}(\alpha)$. $|N_{K/\boldsymbol{Q}}(D\alpha)| \ge 1$, since $N_{K/\boldsymbol{Q}}(D\alpha)$ is a nonzero integer. Hence we have the so-called fundamental inequality

$$|\alpha| \ge D^{-[K:\boldsymbol{Q}]}\overline{|\alpha|}^{-[K:\boldsymbol{Q}]+1} \ge \|\alpha\|^{-2[K:\boldsymbol{Q}]}\,.$$

If α^σ is a conjugate of α, then for the same reason,

$$|(\alpha^\sigma)^{-1}| \le D^{[K:\boldsymbol{Q}]}\overline{|\alpha|}^{[K:\boldsymbol{Q}]-1} \le \|\alpha\|^{2[K:\boldsymbol{Q}]}\,.$$

Since $N_{K/\boldsymbol{Q}}(D\alpha)\alpha^{-1}$ is an algebraic integer,

$$\mathrm{den}(\alpha^{-1}) \le |N_{K/\boldsymbol{Q}}(D\alpha)| \le \|\alpha\|^{2[K:\boldsymbol{Q}]}\,.$$

Therefore we have $\|\alpha^{-1}\| \le \|\alpha\|^{2[K:\boldsymbol{Q}]}$.

PROPOSITION 7. *If* $k > c_4(p)$, *then*

$$\log\|E(\Omega^k\alpha;\, T(\tau;\, A^k;\, b^{(k)}(\alpha)))\| \le c_5 p\rho^k\,.$$

PROOF. By the equality (4), we have

$$E(\Omega^k\alpha;\, T(\tau;\, A^k;\, b^{(k)}(\alpha))) = P_0(\Omega^k\alpha;\, T(\tau;\, A^k;\, b^{(k)}(\alpha)))\,.$$

Letting $A^k = (a_{ij}^{(k)})$, we have $\|a_{ij}^{(k)}\| \le c_6^k$. By the property (II), we obtain $\|b_i(\Omega^k\alpha)\| \le c_7^{\rho^k}$ and so

$$\|b_i^{(k)}(\alpha)\| \le k\prod_{j=0}^{k-1} m(c_6^j c_7^{\rho^j})^m \le c_8^{\rho^k}\,.$$

Therefore

$$\|T_\mu(\tau;\, A^k;\, b^{(k)}(\alpha))\| \le c_9^{\rho^k}$$

and

$$\|P_0(\Omega^k\alpha;\, T(\tau;\, A^k;\, b^{(k)}(\alpha)))\| \le c_{10}(p)c_{11}^{p\rho^k}\,.$$

This implies the proposition.

Now we can complete the proof of Theorem 6. By Proposition 2, there exists $k > \max(c_2(p), c_4(p))$ such that

$$P_0(\Omega^k\alpha\,;\,T(\tau\,;\,A^k\,;\,b^{(k)}(\alpha)))\neq 0\,.$$

By Propositions 6 and 7 and the fundamental inequality, we get

$$-c_3(p+1)^{1+n^{-1}}\rho^k \geq -2[K:\boldsymbol{Q}]c_5 p\rho^k\,.$$

Hence

$$c_3(p+1)^{1+n^{-1}} \leq 2[K:\boldsymbol{Q}]c_5 p\,,$$

a contradiction, if p is large.

LEMMA 4. *Let C be a field and F a subfield of C. If*

$$f(z_1,\ldots,z_n)\in C[[z_1,\ldots,z_n]]\cap F(z_1,\ldots,z_n)\,,$$

then there exist polynomials $A(z_1,\ldots,z_n)$, $B(z_1,\ldots,z_n)\in F[z_1,\ldots,z_n]$ such that

$$f(z_1,\ldots,z_n)=A(z_1,\ldots,z_n)/B(z_1,\ldots,z_n)\,,\qquad B(0,\ldots,0)\neq 0\,.$$

PROOF. There are relatively prime polynomials $A(z_1,\ldots,z_n)$ and $B(z_1,\ldots,z_n)$ in $F[z_1,\ldots,z_n]$ such that

$$f(z_1,\ldots,z_n)=A(z_1,\ldots,z_n)/B(z_1,\ldots,z_n)\,.$$

We shall show that every prime factor P of B satisfies $P(0,\ldots,0)\neq 0$. We may assume F to be algebraically closed. Then $F\{t\}=\bigcup_{n=1}^{\infty}F((t^{1/n}))$ is algebraically closed, where t is a variable. We have the expression

$$P=P_d+P_{d-1}+\cdots+P_0\,,\qquad P_d\neq 0\,,$$

where P_i is the sum of the terms of total degree i. Changing the variables z_i to z_i' as

$$z_1=z_1'\,,\quad z_i=z_i'+c_iz_1'\,,\quad c_i\in F\ (i\geq 2)\,,$$

we obtain

$$P(z_1,\ldots,z_n)=P_d(1,c_2,\ldots,c_n)z_1'^d+(\text{the sum of the terms of degree}\leq d-1\text{ in }z_1')\,.$$

We can choose $c_2,\ldots,c_n$ so that $P_d(1,c_2,\ldots,c_n)\neq 0$. Therefore we may assume

$$P(z_1,\ldots,z_n)=az_1^d+P_{d-1}(z_2,\ldots,z_n)z_1^{d-1}+\cdots+P_0(z_2,\ldots,z_n)\,,\qquad a\in F^\times\,.$$

We can choose $g_2,\ldots,g_n\in F[[t]]$ which are algebraically independent over F and satisfy $g_i(0)=0$. Then $P(X,g_2,\ldots,g_n)\in F[[t]][X]$ and the coefficient of the largest degree is a. Suppose that $P(0,\ldots,0)=0$. Then $P_0(0,\ldots,0)=0$ and therefore there exists a root $g_1\in F\{t\}$ of $P(X,g_2,\ldots,g_n)=0$ such that $g_1(0)=0$. $(g_1,\ldots,g_n)$ is a generic point of the algebraic variety defined by $P(X_1,\ldots,X_n)=0$ over F. By the equality

$$f(z_1,\ldots,z_n)B(z_1,\ldots,z_n)=A(z_1,\ldots,z_n)\,,$$

we have

$$0=f(g_1,\dots,g_n)B(g_1,\dots,g_n)=A(g_1,\dots,g_n).$$

Hence P must divide A, a contradiction.

PROOF OF THEOREMS 1 AND 2. Let $\{f_1(z),\dots,f_s(z)\}$ $(r\le s)$ be a maximal set whose elements are linearly independent over K modulo $K(z_1,\dots,z_n)$. Then $f_{s+1}(z),\dots,f_m(z)$ are linear combinations over K modulo $K(z_1,\dots,z_n)$. Therefore $f_1(z),\dots,f_s(z)$ satisfy a functional equation of the form (1) and we may assume $s=m$ without loss of generality. By Theorem 4, $f_1(z),\dots,f_m(z)$ are algebraically independent over $K(z_1,\dots,z_n)$. Since

$$b(z)=f(z)-Af(\Omega z)\in(K[[z_1,\dots,z_n]])^m,$$

by Lemma 4 we have expressions

$$b_i(z)=p_i(z)/q_i(z),\quad p_i(z),q_i(z)\in K[z_1,\dots,z_n],\quad q_i(0,\dots,0)\neq 0.$$

There exists a positive integer k_0 such that if $k\ge k_0$, then $\Omega^k\alpha\in U$ and $q_i(\Omega^k\alpha)\neq 0$ $(i=1,\dots,m)$. By Theorem 6, $f_1(\Omega^{k_0}\alpha),\dots,f_m(\Omega^{k_0}\alpha)$ are algebraically independent. Since

$$\sum_{j=0}^{k_0-1}A^jb(\Omega^jz)=f(z)-A^{k_0}f(\Omega^{k_0}z)\in C[[z_1-\alpha_1,\dots,z_n-\alpha_n]]\cap K(z_1-\alpha_1,\dots,z_n-\alpha_n),$$

we obtain

$$f(\alpha)=A^{k_0}f(\Omega^{k_0}\alpha)+B,\qquad B\in K^m,$$

by Lemma 4. The values $f_1(\alpha),\dots,f_m(\alpha)$ are algebraically independent, since $\det A\neq 0$. We can prove Theorem 2 similarly by using Theorem 5.

4. Examples. Let d be an integer greater than 1 and put

$$f(x,z)=\sum_{k=0}^{\infty}x^kz^{d^k}.$$

Then $f(x,z)$, $\partial f/\partial x(x,z),\dots,\partial^l f/\partial x^l(x,z)$ satisfy

$$f(x,z)=xf(x,z^d)+z$$

$$\frac{\partial f}{\partial x}(x,z)=x\frac{\partial f}{\partial x}(x,z^d)+f(x,z^d)$$

$$\vdots$$

$$\frac{\partial^l f}{\partial x^l}(x,z)=x\frac{\partial^l f}{\partial x^l}(x,z^d)+l\frac{\partial^{l-1}f}{\partial x^{l-1}}(x,z^d).$$

Let $a_1,\dots,a_n$ be distinct nonzero algebraic numbers. By Theorem 3, $\partial^l f/\partial x^l(a_i,z)$ $(i=1,\dots,n,\ l\ge 0)$ are algebraically independent over $C(z)$, since $a_1,\dots,a_n$ are distinct and $f(a_i,z)\notin C(z)$. $\Omega=(d)$ and a nonzero algebraic number α with absolute value less than 1 satisfy the properties (I)–(IV). Therefore $\partial^l f/\partial x^l(a_i, \alpha)$ $(i=1,\dots,n, l\geq 0)$ are algebraically independent by Theorem 1. Hence we have the following theorem.

THEOREM 7. *Let d be an integer greater than* 1, *α a nonzero algebraic number with absolute value less than* 1, *and $g(x)=\sum_{k=0}^{\infty}\alpha^{d^k}x^k$. Then $g(x)$ is an entire function and $g^{(l)}(a)$ $(a\in\bar{Q}^{\times}, l\geq 0)$ are algebraically independent.*

Nishioka [8] proved that the function $\sum_{k=0}^{\infty}\alpha^{k!}x^k$ has the same property as the function $g(z)$.

Next we consider the power series

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

where ω is quadratic irrational and $0<\omega<1$. $F_\omega(z_1, z_2)$ converges in the domain $\{|z_1|<1, |z_1||z_2|^\omega<1\}$ and

$$F_\omega(z, 1)=\sum_{k=1}^{\infty}[k\omega]z^k.$$

For suitable algebraic numbers α_1, α_2, the transcendence of $F_\omega(\alpha_1, \alpha_2)$ is proved in Mahler [5]. Now we shall prove the following theorem:

THEOREM 8. *Let α_1, α_2 be algebraic numbers with $0<|\alpha_1|<1$, $0<|\alpha_1||\alpha_2|^\omega<1$. Then*

$$\frac{\partial^{l_1+l_2}F_\omega}{\partial z_1^{l_1}\partial z_2^{l_2}}(\alpha_1, \alpha_2) \qquad (l_1\geq 0, l_2\geq 0)$$

are algebraically independent.

COROLLARY. *Let $f(z)=F_\omega(z, 1)$, and let α be an algebraic number with $0<|\alpha|<1$. Then $f^{(l)}(\alpha)$ $(l\geq 0)$ are algebraically independent.*

PROOF. Let ω be expanded in continued fraction

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

Define $\omega_0, \omega_1, \dots$ by

$$\omega=\omega_0=\frac{1}{a_1+\omega_1}, \quad \omega_1=\frac{1}{a_2+\omega_2}, \dots.$$

Because of the equality (see Mahler [5]),

$$F_{\omega}(z_1, z_2)=(-1)^{\nu}F_{\omega_\nu}(z_1^{p_\nu}z_2^{q_\nu}, z_1^{p_{\nu-1}}z_2^{q_{\nu-1}})+\sum_{\mu=0}^{\nu-1}(-1)^{\mu}\frac{z_1^{p_{\mu+1}+p_\mu}z_2^{q_{\mu+1}+q_\mu}}{(1-z_1^{p_{\mu+1}}z_2^{q_{\mu+1}})(1-z_1^{p_\mu}z_2^{q_\mu})},$$

where q_ν/p_ν is the ν-th convergent of ω, we may assume without loss of generality that $0<|\alpha_1|, |\alpha_2|<1$ and ω is expanded in a purely periodic continued fraction. Let ν be an even period of the continued fraction of ω and

$$\Omega=\begin{pmatrix} p_\nu & q_\nu \\ p_{\nu-1} & q_{\nu-1} \end{pmatrix}.$$

Then we have

$$F_{\omega}(z_1, z_2)=F_{\omega}(\Omega(z_1, z_2))+b(z_1, z_2), \qquad b(z_1, z_2)\in \boldsymbol{Q}(z_1, z_2).$$

Letting $D_1=z_1\partial/\partial z_1$, $D_2=z_2\partial/\partial z_2$, we know that $D_1^{l_1}D_2^{l_2}F_{\omega}(z_1, z_2)$ is a linear combination of $\{D_1^{h_1}D_2^{h_2}F_{\omega}(\Omega(z_1, z_2))\}_{h_1+h_2=l_1+l_2}$ modulo $\boldsymbol{Q}(z_1, z_2)$. We need the following:

THEOREM (Mahler [5]). *Suppose that the characteristic polynomial of Ω is irreducible over $\boldsymbol{Q}$ and that Ω has an eigenvalue ρ which is greater than the absolute values of all other eigenvalues. We denote by A_{ij}, the (i, j)-cofactor of the matrix $\Omega-\rho I$. If*

$$\sum_{i=1}^{n}|A_{i1}|\log|\alpha_i|<0,$$

then Ω and $\alpha=(\alpha_1, \ldots, \alpha_n)$ satisfy the properties (I)–(IV).

Nishioka [10] proves the algebraic independence of the functions $D_1^{l_1}D_2^{l_2}F_{\omega}(z_1, z_2)$ ($l_1\geq 0, l_2\geq 0$). By Theorem 1 we complete the proof.

REFERENCES

[1] F. R. GANTMACHER, Applications of the theory of matrices, New York, Interscience, 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] 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.

[4] J. H. LOXTON AND A. J. VAN DER POORTEN, A class of hypertranscendental functions, Aequationes Math. 16 (1977), 93–106.

[5] K. MAHLER, Arithmetische Eigenschaften der Lösungen einer Klasse von Funktion-algleichungen, Math. Ann. 101 (1929), 342–366.

[6] K. MAHLER, Arithmetische Eigenschaften einer Klasse transzendental-transzendenter Funktionen, Math. Z. 32 (1930), 545–585.

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

[8] K. NISHIOKA, Algebraic independence of certain power series of algebraic numbers, J. Number Theory 23 (1986), 353–364.

[9] K. NISHIOKA, New approach in Mahler's method, J. reine angew. Math. 407 (1990), 202–219.

[10] K. NISHIOKA, Note on a paper by Mahler, Tsukuba J. Math. 17 (1993), 455–459.

[11] T. TÖPFER, An axiomatization of Nesterenko's method and applications on Mahler functions, J. Number Theory 49 (1994), 1–26.

KEIO UNIVERSITY
4–1 HIYOSHI 4-CHOME, KOHOKU-KU
YOKOHAMA, 223
JAPAN