

ALGEBRAIC INDEPENDENCE BY A METHOD OF MAHLER

YUVAL Z. FLICKER

(Received 14 July 1977; revised 28 August 1978)

(Communicated by J. Coates)

Abstract

We establish a general algebraic independence theorem for the solutions of a certain kind of functional equations. As a particular application, we prove that for any real irrational ζ , the numbers

$$\sum_1^{\infty} [h\zeta] \alpha_1^h, \dots, \sum_1^{\infty} [h\zeta] \alpha_n^h$$

are algebraically independent, for multiplicatively independent algebraic numbers α_i with $0 < |\alpha_i| < 1$.

Subject classification (Amer. Math. Soc. (MOS) 1970): 10 F 35, 10 F 45, 39 A 30.

0. Introduction

Let $T = (t_{ij})$ be an $n \times n$ matrix with non-negative integer entries, and for any field F define a transformation $T: F^n \rightarrow F^n$ by $\mathbf{z}' = T\mathbf{z}$, where

$$z'_i = z_1^{t_{i1}} \dots z_n^{t_{in}} \quad (1 \leq i \leq n) \quad \text{and} \quad \mathbf{z} = (z_1, \dots, z_n).$$

Studies concerning the arithmetic properties of functions $f(\mathbf{z})$ of n complex variables, for which $f(T\mathbf{z})$ can be expressed as a rational function in $f(\mathbf{z})$ and \mathbf{z} , were initiated by Mahler in 1929–30. It follows from his work that functions of the complex variable z , such as

$$g(z) = \sum_{r=0}^{\infty} z^{2^r}, \quad h_{\zeta}(z) = \sum_{r=0}^{\infty} [r\zeta] z^r,$$

where ζ is a quadratic irrational, obtain transcendental values at algebraic numbers α with $0 < |\alpha| < 1$. Moreover he demonstrated the algebraic independence of, for

instance, $g(\alpha_1), \dots, g(\alpha_m)$, and further $h_\zeta(\alpha_1), \dots, h_\zeta(\alpha_m)$, for any multiplicatively independent algebraic numbers $\alpha_1, \dots, \alpha_m$, with $0 < |\alpha_i| < 1$.

The method has received considerable attention recently from various authors, especially Kubota, Loxton and van der Poorten. In particular they obtained transcendence and algebraic independence results for functions which satisfy functional equations with transformation matrices T which are more general than those considered by Mahler; see, for example, Loxton and van der Poorten (1977). Further, in answer to a question by Mahler (1969) (see p. 520), Loxton and van der Poorten (1977a) proved the transcendence of values of functions which satisfy a sequence of functional equations, rather than a single one. Their work furnishes as a notable corollary the transcendence of $h_\zeta(\alpha)$, where now ζ is an arbitrary real irrational. Furthermore, Kubota (1977a) generalized Mahler's algebraic independence techniques to deal with functions that satisfy a sequence of functional equations, but in which all of the transformations T are given by scalar matrices.

Loxton and van der Poorten (1977b) (see p. 20) posed the problem of extending their transcendence results in order to establish algebraic independence theorems similar to those obtained by Mahler in the case when ζ is a quadratic irrational. Here we shall extend the scope of Kubota's (1977a) methods, in order to deal with a wider class of transformation formulae; we shall obtain thereby a general algebraic independence theorem (Theorem 2), from which we shall deduce the following corollary. Let Q be the field of rational numbers.

THEOREM 1. *For any real irrational number ζ there exists a number $\lambda = \lambda(\zeta)$, with the following property. If $\alpha_1, \dots, \alpha_m$ are algebraic numbers with $0 < |\alpha_i| < 1$, such that $\log |\alpha_1|, \dots, \log |\alpha_m|$ are linearly independent over $Q + \lambda Q$, then the numbers $h_\zeta(\alpha_1), \dots, h_\zeta(\alpha_m)$ are algebraically independent over Q .*

Note that ζ is an arbitrary real irrational number, and that $Q + \lambda Q$ denotes the set of all numbers of the form $u + \lambda v$ with rational u and v . In fact we shall specify in Section 5 the value of λ when the partial quotients in the continued fraction expansion of ζ are bounded. When these partial quotients are not bounded we obtain indeed a stronger algebraic independence result, for in that case we need assume only that $\alpha_1, \dots, \alpha_m$ are algebraic numbers with $0 < |\alpha_i| < 1$, whose absolute values are distinct. In the special case $m = 1$ we obtain again the result of Loxton and van der Poorten (1977a) which is mentioned above, namely the transcendence of $h_\zeta(\alpha)$. Simple cardinality arguments show that there are sets of $\alpha_1, \dots, \alpha_m$, which satisfy the conditions of the Theorem with arbitrary large m . Furthermore, we shall carry out our studies over any completion of an arbitrary number field, thus establishing the p -adic analogue of a major part of the work mentioned above.

In the p -adic case, when ζ has continued fraction with bounded partial quotients, we can obtain only the transcendence of $h_\zeta(\alpha)$. This is essentially because the (p -adic) valuation group of a number field is cyclic and discrete in the real numbers; see Section 5.

In (1977a) (see Theorems 7 and 8; and see also Section 4.3 of (1977b)), Loxton and van der Poorten suggested that their work can be generalized to yield the transcendence of numbers such as $\sum p([r\zeta])\alpha^r$, with arbitrary ζ and α as above, where p is any non-constant polynomial with algebraic coefficients. Unfortunately, however, when the degree of p is greater than 1, and when the continued fraction of ζ has bounded partial quotients, the functional equations satisfied by the associated sequence of functions is not as simple as asserted there (see p. 42), and thus their technique (like ours) is insufficient, as it stands, to establish the result.

Further we mention the related problem of establishing the algebraic independence of $h_1(\alpha), \dots, h_m(\alpha)$, where h_1, \dots, h_m are algebraically independent functions associated with distinct ζ_1, \dots, ζ_m . Such a result does not seem to follow from our studies here, but we note that the methods which were announced by Kubota (1977b) may possibly be useful in this context.

1. The auxiliary functions

Let K be a finite algebraic extension of the field \mathcal{Q} of rational numbers, and denote by K_p its completion by a p -adic valuation $||_p$ on K . We include the field \mathbf{C} of the complex numbers in this scheme by writing $p = \infty$ and $K_p = \mathbf{C}$ when we deal with the archimedean valuation $|| (= ||_\infty)$.

Our main theorem (Theorem 2, below) will relate to a sequence $\mathbf{f}_0, \mathbf{f}_1, \dots$, of m -tuples

$$\mathbf{f}_j(\mathbf{z}) = (f_{1j}(\mathbf{z}), \dots, f_{mj}(\mathbf{z})) \quad (j \geq 0),$$

where $f_{ij}(\mathbf{z})$ are power series in n variables $\mathbf{z} = (z_1, \dots, z_n)$ with coefficient in K . For any n -tuple $\mathbf{m} = (m_1, \dots, m_n)$ of non-negative integers we put

$$\mathbf{z}^{\mathbf{m}} = z_1^{m_1} \dots z_n^{m_n}.$$

As usual, we measure the proximity to 0 of a power series in n variables by the minimal total degree of the terms with non-zero coefficients; by the total degree of the term $\mathbf{z}^{\mathbf{m}}$ we mean $|\mathbf{m}| = m_1 + \dots + m_n$. Now suppose that the sequence $\{\mathbf{f}_j\}$ admits a subsequence S which converges in the above topology to a limit function \mathbf{f} . We shall assume that the components $f_i(\mathbf{z})$ ($1 \leq i \leq m$) of \mathbf{f} are algebraically independent over the ring $K_p[\mathbf{z}]$ of polynomials in n variables with coefficients in K_p .

For the proof of Theorem 2 we shall further assume that there is an n -tuple α in K_p^d , and elements $\omega_{\mathbf{k}}$ of K , not all 0, such that

$$(1) \quad \sum_{\mathbf{k} \leq \mathbf{h}} \omega_{\mathbf{k}} f_{10}(\alpha)^{k_1} \dots f_{m0}(\alpha)^{k_m} = 0,$$

where $\mathbf{h} = (h_1, \dots, h_m)$ is a fixed m -tuple of non-negative integers, and $\mathbf{k} = (k_1, \dots, k_m)$ satisfies $0 \leq k_i \leq h_i$ ($1 \leq i \leq m$). We shall write $\omega = (\omega_{\mathbf{k}})$, so that ω is a vector of $h = (h_1 + 1) \dots (h_m + 1)$ elements $\omega_{\mathbf{k}}$ of K , not all 0. We shall denote by \mathbf{w} a vector of h independent variables in K_p . For convenience we shall rewrite (1) in the form

$$(1') \quad F(\mathbf{f}_0(\alpha), \omega) = 0,$$

where

$$F(\mathbf{z}, \mathbf{w}) = \sum_{\mathbf{k} \leq \mathbf{h}} w_{\mathbf{k}} z^{\mathbf{k}}$$

is a polynomial in $n + h$ variables.

We shall eventually deduce a contradiction by estimating certain values of well-chosen auxiliary functions; to describe these functions we need the notion of index. Let $\omega_j = (\omega_{j\mathbf{k}})$ ($j = 1, 2, \dots$) be a sequence of vectors whose h components $\omega_{j\mathbf{k}}$ ($0 \leq \mathbf{k} \leq \mathbf{h}$) are elements of K , and put $\omega_0 = \omega$. We say that a polynomial $P(\mathbf{w})$ with coefficients in K has the property $A(\omega)$ if $P(\omega_j) = 0$ for all $j \geq 0$. Let $P(\mathbf{z}, \mathbf{w}) = \sum P_{\mathbf{m}}(\mathbf{w}) z^{\mathbf{m}}$ be a power series in \mathbf{z} , with coefficients $P_{\mathbf{m}}(\mathbf{w})$ in $K[\mathbf{w}]$. We define the index $I(P)$ (with respect to $\{\omega_j\}$) of the power series $P(\mathbf{z}, \mathbf{w})$, to be the minimum of the numbers $|\mathbf{m}|$ over \mathbf{m} such that $P_{\mathbf{m}}(\mathbf{w})$ does not have the property $A(\omega)$. Thus we say that $P(\mathbf{z}, \mathbf{w})$ has the property $A(\omega)$, and that $I(P) = \infty$, if all coefficients $P_{\mathbf{m}}(\mathbf{w})$ of $P(\mathbf{z}, \mathbf{w})$ have the property $A(\omega)$.

To define the auxiliary functions we need the following:

LEMMA 1. For any natural number r there are polynomials $P_i(\mathbf{z}, \mathbf{w})$ ($0 \leq i \leq r$) with coefficients in K and with degrees at most r in each of its $n + h$ variables, not all with the property $A(\omega)$, such that the function

$$(2) \quad E'_j(\mathbf{z}, \mathbf{w}) = \sum_{i=0}^r P_i(\mathbf{z}, \mathbf{w}) F(\mathbf{f}_j(\mathbf{z}), \mathbf{w})^i,$$

has index $\gg r^{1+1/n}$ for any $j \geq j_0$ ($j_0 = j_0(r)$) for which \mathbf{f}_j belongs to S . Further, the coefficients of P_i may depend on r , but not on j .

Here and below the constant implied by \ll is independent of r and j . Before proving the lemma we define the auxiliary functions that we actually require; namely

$$E_j(\mathbf{z}, \mathbf{w}) = \sum_{i=q}^r P_i(\mathbf{z}, \mathbf{w}) F(\mathbf{f}_j(\mathbf{z}), \mathbf{w})^{i-q},$$

for j as specified in the lemma, where q is the minimal integer such that $P_q(\mathbf{z}, \mathbf{w})$ does not have the property $A(\omega)$.

PROOF. Let r be a natural number, and suppose that P_i are polynomials with coefficients, variables and degrees as in the lemma. We expand E'_j as a power series in \mathbf{z} , thus

$$E'_j(\mathbf{z}, \mathbf{w}) = \sum_{\mathbf{m}} C_{j\mathbf{m}}(\mathbf{w}) \mathbf{z}^{\mathbf{m}},$$

where $C_{j\mathbf{m}}(\mathbf{w})$ are polynomials with degrees at most $2r$ in the components of \mathbf{w} , whose coefficients may depend on the coefficients of \mathbf{f}_j , but not on the variable \mathbf{z} . But the function \mathbf{f}_j belongs to the convergent subsequences S ; hence there is a function $j_0 = j_0(r)$ of r , such that for any \mathbf{m} with $|\mathbf{m}| \leq r^{1+1/n}$, the polynomial $C_{j\mathbf{m}}(\mathbf{w})$ is independent of j , provided that $j \geq j_0$.

It remains for us to choose polynomials P_i for which the lemma holds. We reduce this problem to a simple question in linear algebra. Let $V(r)$ denote the vector space of polynomials in $K[\mathbf{w}]$ with degrees at most r in each of its h variables. Denote by $V_{\omega}(r)$ the set of polynomials in $V(r)$ with the property $A(\omega)$. We denote the dimension of the factor space

$$\bar{V}(r) = V(r)/V_{\omega}(r)$$

by $d(r)$, and let v_{kr} ($1 \leq k \leq d(r)$) be a basis for $\bar{V}(r)$ over K . We can write

$$P_i(\mathbf{z}, \mathbf{w}) = \sum_{\mathbf{m} \leq \mathbf{r}} p_{i\mathbf{m}}(\mathbf{w}) \mathbf{z}^{\mathbf{m}}, \quad \text{where } \mathbf{r} = (r, \dots, r),$$

and where $p_{i\mathbf{m}}(\mathbf{w})$ is in $V(r)$. Now the image of $p_{i\mathbf{m}}(\mathbf{w})$ in $\bar{V}(r)$ is given by

$$\bar{p}_{i\mathbf{m}}(\mathbf{w}) = \sum_{k=1}^r p_{ikm} v_{kr} \quad (p_{ikm} \text{ in } K).$$

Substituting the last two equations in the defining equation (2) of E'_j , we see that for any fixed \mathbf{m}' the image $\bar{C}_{j\mathbf{m}'}$ in $\bar{V}(2r)$ of the element $C_{j\mathbf{m}'}(\mathbf{w})$ of $V(2r)$ is a linear form in $v_{k,2r}$ ($1 \leq k \leq d(2r)$), whose coefficients are linear forms in

$$p_{ikm} \quad (1 \leq k \leq d(r), 0 \leq i \leq r, \mathbf{m} \leq \mathbf{r}).$$

Thus each equation $\bar{C}_{j\mathbf{m}'} = 0$ is equivalent to a system of $d(2r)$ homogeneous linear equations

$$\sum_{i=0}^r \sum_{k=1}^{d(r)} \sum_{\mathbf{m} \leq \mathbf{r}} a_{ijkm} p_{ikm} = 0 \quad (1 \leq j \leq d(2r)),$$

in the $(r+1)^{n+1}d(r)$ unknowns p_{ikm} , with coefficients a_{ijkm} in K . It follows that the requirement that the index of $E'_j(\mathbf{z}, \mathbf{w})$ be at least I is equivalent to a system of at most $I^n d(2r)$ equations in the unknowns p_{ikm} . Note that if $I \leq r^{1+1/n}$ then the system is independent of the choice of j , for any j as in the statement of the lemma.

Clearly each polynomial in $\bar{V}(2r)$ can be written as a linear form in 2^h polynomials in $\bar{V}(r)$, whose coefficients are of the form

$$\prod_{\mathbf{k} \leq \mathbf{h}} w_{\mathbf{k}}^{r d_{\mathbf{k}}}, \quad \text{with } d_{\mathbf{k}} = 0 \text{ or } 1.$$

Hence $d(2r) \leq 2^h d(r)$, and further

$$I^n d(2r) \leq I^n 2^h d(r) < (r+1)^{n+1} d(r),$$

if $I = [2^{-h/n} r^{1+1/n}]$. Therefore the number of unknowns exceeds the number of equations in the homogeneous system above, and so we can choose polynomials $P_i(\mathbf{z}, \mathbf{w})$ for which the lemma holds. This completes the proof.

2. A dominance lemma

In this section we shall establish technical instruments which are useful in estimating values of the auxiliary functions.

We introduce a sequence of $n \times n$ non-degenerate matrices T_0, T_1, \dots , with non-negative integer entries, and such that T_0 is the identity matrix. We shall assume that the maximum entry r_j of T_j satisfies

$$(3) \quad r' = \liminf_{j \rightarrow \infty} (r_j/j) > 0,$$

and that there exist arbitrary large j 's with $r_j/j \neq r'$. Further, we assume that there is an open neighbourhood D of the origin in K_p^n such that $f_{ij}(\mathbf{z})$ are convergent on D . Also we assume that $\mathbf{z}_j = T_j \mathbf{z}$ belongs to D for any \mathbf{z} in D , where we use the notations of Section 1. Furthermore, we assume that (i) and (ii) below are satisfied.

(i) $|f_{ij}(\mathbf{z})|_p$ are uniformly bounded for \mathbf{z} in D and for all j .

(ii) For any \mathbf{z} in D there exists an n -tuple \mathbf{s} with real positive components, such that for any \mathbf{m} we have

$$\log |z_j^{\mathbf{m}}|_p \sim -r_j \langle \mathbf{m}, \mathbf{s} \rangle, \quad \text{as } j \rightarrow \infty;$$

here and below $\langle \mathbf{m}, \mathbf{s} \rangle$ is the usual vector dot product, that is

$$\langle \mathbf{m}, \mathbf{s} \rangle = m_1 s_1 + \dots + m_n s_n.$$

Now let $\gamma_1, \dots, \gamma_l$ be a finite set of non-zero p -adic numbers with distinct valuations. Let g_1, \dots, g_l be polynomials in $m+n$ variables, with coefficients in K_p , and which are not all 0. We put

$$G_{jk}(\mathbf{z}) = \sum_{i=1}^l g_i(\mathbf{f}_k(\mathbf{z}_j), \mathbf{z}_j) \gamma_i^j \quad (k \geq 0).$$

We denote by $c_{\mathbf{m}}$ the coefficient of the term $\mathbf{z}^{\mathbf{m}}$ in the power series expansion of $g_i(\mathbf{f}(\mathbf{z}), \mathbf{z})$ at the origin, that is

$$g_i(\mathbf{f}(\mathbf{z}), \mathbf{z}) = \sum_{\mathbf{m}} c_{\mathbf{m}} \mathbf{z}^{\mathbf{m}}.$$

Finally we let α be an n -tuple in D , with non-zero algebraic components $\alpha_i (1 \leq i \leq n)$, and we suppose that the real vector $\mathbf{s} = \mathbf{s}(\alpha)$ has components which are linearly independent over Q . For brevity we put $\alpha_j = T_j \alpha$.

LEMMA 2. *There is an integer $i (1 \leq i \leq l)$ and an n -tuple \mathbf{m} with $c_{\mathbf{m}} \neq 0$, such that*

$$G_{jk}(\alpha) \sim c_{\mathbf{m}} \alpha_j^{\mathbf{m}} \gamma_i^j, \text{ as } j \rightarrow \infty,$$

uniformly in k , provided that f_k belongs to S , and $k \gg 1$.

PROOF. The proof is based on arguments of Kubota (1977a); in fact we merely have to show that Kubota's methods can be applied in our slightly more general situation.

It suffices to prove the lemma in the case that $l = 1$; for then we obtain the asymptotic formula for $G_{jk}(\alpha)$ as a finite sum of terms with the required shape, and one of these is dominating by virtue of the assumptions that $\gamma_1, \dots, \gamma_l$ have distinct valuations and that there exist arbitrary large j 's with $r_j \neq jr'$. It suffices in fact to prove that

$$g(\mathbf{f}_k(\alpha_j), \alpha_j) \sim c_{\mathbf{m}} \alpha_j^{\mathbf{m}}, \text{ as } j \rightarrow \infty.$$

Let M be the set of \mathbf{m} for which $c_{\mathbf{m}} \neq 0$. We define a partial order relation on M by writing $\mathbf{m} \leq \mathbf{m}'$ if and only if $m_i \leq m'_i$ for all i with $1 \leq i \leq n$. The subset L of minimal elements of M is clearly finite. Since \mathbf{s} has linearly independent components over Q , there is some \mathbf{t} in L such that for any $\mathbf{m} \neq \mathbf{t}$ in L we have $\langle \mathbf{m} - \mathbf{t}, \mathbf{s} \rangle > 0$. It now follows from (ii) and (3) that $\alpha_j^{\mathbf{m} - \mathbf{t}}$ tends to 0 as $j \rightarrow \infty$. Let q' be an integer which is greater than the maximum of $|\mathbf{m}|$ over all \mathbf{m} in L . Then there is an integer $k_0 = k_0(q')$, such that for any $k \geq k_0$ for which \mathbf{f}_k belongs to S , the coefficients of the terms with total degree $\leq q'$ in the power series $f_{ik} - f_i (1 \leq i \leq m)$ are zero; in particular $c_{k\mathbf{t}} = c_{\mathbf{t}}$, where

$$g(\mathbf{f}_k(\mathbf{z}), \mathbf{z}) = \sum_{\mathbf{m}} c_{k\mathbf{m}} \mathbf{z}^{\mathbf{m}}.$$

It follows that we can write

$$g(\mathbf{f}_k(\alpha_j), \alpha_j) = c_{\mathbf{t}} \alpha_j^{\mathbf{t}} + \sum_{\mathbf{m} \neq \mathbf{t}} c_{k\mathbf{m}} \alpha_j^{\mathbf{m}},$$

and it suffices to show that

$$C_j = \sum_{\mathbf{m} \neq \mathbf{t}} (c_{k\mathbf{m}}/c_{\mathbf{t}}) \alpha_j^{\mathbf{m}-\mathbf{t}}$$

tends to 0 as $j \rightarrow \infty$.

By virtue of (i) the functions $g(\mathbf{f}_k(\mathbf{z}), \mathbf{z})$ are uniformly bounded for \mathbf{z} in D and for all k . Thus it follows from Cauchy's inequality that there is a real positive vector \mathbf{c} such that

$$|c_{k\mathbf{m}}|_p \ll c^{\mathbf{m}},$$

where the implied constant is independent of k and \mathbf{m} . Now if $\mathbf{m} > \mathbf{t}$ then there is an i with $\alpha_j^{\mathbf{m}-\mathbf{t}} = \alpha_{ij} \alpha_j^{\mathbf{m}'}$, where α_{ij} is the i th component of α_j , and where $\mathbf{m}' \geq \mathbf{0}$. Also if $\mathbf{m} \geq \mathbf{t}'$, where $\mathbf{t}' \neq \mathbf{t}$ in L , then $\alpha_j^{\mathbf{m}-\mathbf{t}} = \alpha_j^{\mathbf{t}'-\mathbf{t}} \alpha_j^{\mathbf{m}'}$, where $\mathbf{m}' \geq \mathbf{0}$. Since any \mathbf{m} which appears in the sum C_j satisfies at least one of the conditions $\mathbf{m} > \mathbf{t}$ or $\mathbf{m} \geq \mathbf{t}'$, for some $\mathbf{t}' \neq \mathbf{t}$ in L , it follows that

$$|C_j|_p \ll \left(\sum_{i=1}^n |\alpha_{ij}|_p + \sum_{\mathbf{t}' \neq \mathbf{t}} |\alpha_j^{\mathbf{t}'-\mathbf{t}}|_p \right) \left(\sum_{\mathbf{m}'} c^{\mathbf{m}'} |\alpha_j^{\mathbf{m}'}|_p \right).$$

But by virtue of (ii) and (3) the sum over \mathbf{m}' converges for all $j \geq 1$, and it is uniformly bounded in j ; further, α_{ij} and $\alpha_j^{\mathbf{t}'-\mathbf{t}}$ tend to 0 as $j \rightarrow \infty$. Since L is finite, it follows that $C_j \rightarrow 0$ as $j \rightarrow \infty$, and the proof is complete.

3. The choice of ω_j

To proceed further we assume that the numbers $f_{ij}(\omega_j)$ satisfy the equations

$$(4) \quad f_{i0}(\alpha) = a_i^j f_{ij}(\alpha_j) + b_{ij};$$

here a_i and b_{ij} are elements of K which may depend on α . We shall assume that the a_i 's are non-zero and that the multiplicative subgroup of K generated by the a_i 's does not contain any element on the unit circle in K_p , except roots of unity. We can then assume without loss of generality that in fact this subgroup does not contain any element on the unit circle in K_p , except the element 1; for there exists a positive integer d such that the set a_1^d, \dots, a_m^d has this property, and we may restrict our attention to a subsequence of $\{\mathbf{f}_j\}$, whose members \mathbf{f}_j are indexed by all j congruent to a fixed i ($0 \leq i < d$) modulo d . We choose i with the property that the intersection of the corresponding subsequence with S is infinite; then $|a_1^{j_1} \dots a_m^{j_m}|_p = 1$ if, and only if, $a_1^{j_1} \dots a_m^{j_m} = 1$, where j_1, \dots, j_m are rational integers, as required.

In the next section we shall estimate the numbers $e_j = E_j(\alpha_j, \omega_j)$. We shall deal with h -tuples ω_j for which

$$(5) \quad F(f_j(\alpha_j), \omega_j) = F(f_0(\alpha), \omega),$$

for all j ; by virtue of (1') we then deduce that

$$(6) \quad e_j = P_q(\alpha_j, \omega_j),$$

and therefore that the e_j are algebraic numbers. Moreover, the next lemma implies that the e_j are non-zero for infinitely many j . Substituting the value of $f_0(\alpha)$, which is obtained from (4), in the right-hand side of (5), we deduce that in fact (5) is satisfied with the ω_j occurring on the left given by

$$(7) \quad \omega_{jk} = a^{jk} \sum_{l \geq k} \omega_l \binom{l}{k} b_j^{l-k} \quad (0 \leq k \leq h),$$

where $a^j = (a_1^j \dots a_m^j)$, $b_j = (b_{1j}, \dots, b_{mj})$, and $\binom{l}{k} = \binom{l_1}{k_1} \dots \binom{l_m}{k_m}$. Substituting the value of b_j obtained from (4), namely $b_j = f_0(\alpha) - a^j f_j(\alpha_j)$, in (7), we obtain

$$(8) \quad \omega_{jk} = a^{jk} \sum_{l \geq k} \omega_l \binom{l}{k} (f_0(\alpha) - a^j f_j(\alpha_j))^{l-k}.$$

In the sequel we assume that the property $A(\omega)$ and the index are defined with respect to the sequence $\omega_j = (\omega_{jk})$ of (7) and (8).

LEMMA 3. (i) *The polynomial $P(z, w)$ has the property $A(\omega)$ if $P(\alpha_j, \omega_j) = 0$ for all $j \geq 1$,*

(ii) *The set of polynomials in $K[w]$ with the property $A(\omega)$ is a prime ideal of the ring $K[w]$.*

We deduce from the second part of the lemma that

$$(9) \quad I(P_1 P_2) \leq I(P_1) + I(P_2),$$

for any power series P_1 and P_2 in z , with coefficients in $K[w]$. The inequality (9) can be replaced by an equality, since the complementary inequality is easy to obtain; however, we shall not need it here.

PROOF. Let $P(z, w)$ be a polynomial in z and w for which $P(\alpha_j, \omega_j) = 0$ for all sufficiently large j . By virtue of (8) we deduce that there are finitely many polynomials g_1, \dots, g_t in $m+n$ variables, whose coefficients (which lie in K) may depend on α , but not on j ; also there are monomials $\gamma_1, \dots, \gamma_t$ in a_1, \dots, a_m , whose values

are distinct, such that

$$P(\alpha_j, \omega_j) = \sum_{i=1}^l g_i(f_j(\alpha_j), \alpha_j) \gamma_j^i \quad (j \geq 0).$$

Since $\{f_j\}$ admits a subsequence S which converges to a function f , we can apply Lemma 2 to deduce that $g_i(f(z), z) = 0$ ($1 \leq i \leq l$), identically in z . Since the components of f are algebraically independent we conclude that $g_i(\mathbf{x}, z) = 0$ for all i , identically in $\mathbf{x} = (x_1, \dots, x_m)$ and z . It follows that if we define x_{jk} by the right-hand side of (8), replacing $f_{ij}(\alpha_j)$ by x_i , and if we put $\mathbf{x}_j = (x_{jk})$, then

$$(10) \quad P(\mathbf{z}_j, \mathbf{x}_j) = \sum_{i=1}^l g_i(\mathbf{x}, z_j) \gamma_j^i = 0, \quad \text{for all } j \geq 0.$$

Now if

$$P(\mathbf{z}, \mathbf{w}) = \sum_{\mathbf{m}} P_{\mathbf{m}}(\mathbf{w}) z^{\mathbf{m}},$$

then on substituting $x_i = f_{ij}(\alpha_j)$ in (10) we obtain

$$0 = P(\mathbf{z}_j, \omega_j) = \sum_{\mathbf{m}} P_{\mathbf{m}}(\omega_j) z_j^{\mathbf{m}} \quad (j \geq 0).$$

Since T_j is non-singular for all $j \geq 0$ it follows that $z_j^{\mathbf{m}} \neq z_j^{\mathbf{m}'}$ for any $\mathbf{m} \neq \mathbf{m}'$. Hence $P_{\mathbf{m}}(\omega_j) = 0$ for all $j \geq 0$, and $P(\mathbf{z}, \mathbf{w})$ has the property $A(\omega)$.

To prove (ii) we take two polynomials $P_1(\mathbf{w})$ and $P_2(\mathbf{w})$ which do not have the property $A(\omega)$, and deduce a contradiction from the assumption that their product P does have the property $A(\omega)$. Arguing as above we can write

$$P_k(\omega_j) = \sum_{i=1}^l g_{ik}(f_j(\alpha_j)) \gamma_j^i \quad (k = 1, 2),$$

in the usual notations. The polynomials

$$h_k(\mathbf{x}) = \sum_{i=1}^l g_{ik}(\mathbf{x}) \gamma_i^j \quad (k = 1, 2),$$

and their product

$$h_1(\mathbf{x}) h_2(\mathbf{x}) = \sum_{i=1}^l g_i(\mathbf{x}) \gamma_i^{j'j},$$

are non-zero by our assumption. But the supposition that $P(\mathbf{w}) = P_1(\mathbf{w}) P_2(\mathbf{w})$ has the property $A(\omega)$ implies that

$$\sum_{i=1}^l g_i(f_j(\alpha_j)) \gamma_i^{j'j} = 0,$$

for all $j \geq 0$. Applying Lemma 2 as above we deduce that $g_i(\mathbf{x}, \mathbf{z}) = 0$ ($1 \leq i \leq l$), identically in \mathbf{x} and \mathbf{z} . This is a contradiction which establishes the lemma.

4. Estimates

It remains for us to estimate the numbers $e_j = E_j(\boldsymbol{\alpha}_j, \boldsymbol{\omega}_j)$.

LEMMA 4. For any $r \geq 1$, and for infinitely many $j \geq j_1$, where $j_1 = j_1(r)$, we have:
 (i) $I(F(\mathbf{f}_j(\mathbf{z}), \boldsymbol{\omega})) \leq 1$, (ii) $I(E_j(\mathbf{z}, \boldsymbol{\omega})) \geq r^{1+1/n}$, (iii) $0 < |e_j|_p < \exp(-cr, r^{1+1/n})$, where $c \geq 1$.

PROOF. Since F is a non-zero polynomial, and f_1, \dots, f_m are algebraically independent, the function $F(\mathbf{f}(\mathbf{z}), \boldsymbol{\omega})$ is non-zero. Denote by i (resp. i_j) the minimal total degree of the terms $\mathbf{z}^{\mathbf{m}}$ in the power series expansion of $F(\mathbf{f}(\mathbf{z}), \boldsymbol{\omega})$ (resp. $F(\mathbf{f}_j(\mathbf{z}), \boldsymbol{\omega}_j)$) at the origin, whose coefficients are non-zero. For any large enough j for which \mathbf{f}_j belongs to S we have $i_j = i$. Define $P_{jk\mathbf{m}}$ by

$$F(\mathbf{f}_j(\mathbf{z}), \boldsymbol{\omega}_k) = \sum_{\mathbf{m}} P_{jk\mathbf{m}} \mathbf{z}^{\mathbf{m}}.$$

If $I(F(\mathbf{f}_j(\mathbf{z}), \boldsymbol{\omega})) \geq i$ then for any \mathbf{m} with $|\mathbf{m}| < i$ we have $P_{jk\mathbf{m}} = 0$, for any $k \geq 0$. Noting that $\boldsymbol{\omega} = \boldsymbol{\omega}_0$ we deduce that $I(F(\mathbf{f}_j(\mathbf{z}), \boldsymbol{\omega})) \leq i$, and (i) follows.

By the minimality of q we see that for any j as in Lemma 3 the power series

$$E'_j(\mathbf{z}, \boldsymbol{\omega}) - F(\mathbf{f}_j(\mathbf{z}), \boldsymbol{\omega})^q E_j(\mathbf{z}, \boldsymbol{\omega})$$

has the property $A(\boldsymbol{\omega})$. Thus the two members have equal indices, and by (9) we deduce that

$$I(E_j(\mathbf{z}, \boldsymbol{\omega})) \geq I(E'_j(\mathbf{z}, \boldsymbol{\omega})) - qI(F(\mathbf{f}_j(\mathbf{z}), \boldsymbol{\omega})).$$

Since $q \leq r$, Lemma 1 implies that the right-hand side of the inequality above is

$$\geq r^{1+1/n} - ir \geq r^{1+1/n},$$

and (ii) follows.

Finally, in order to prove (iii) we note that (6) and Lemma 3(i) imply that e_j are non-zero for infinitely many j . By (8), and by (6) again, we may write

$$e_j = \sum_{i=1}^l g_i(\mathbf{f}_j(\boldsymbol{\alpha}_j), \boldsymbol{\alpha}_j) \alpha_j^i,$$

where γ_i are monomials in a_1, \dots, a_m of degrees $\ll r$ and with distinct non-zero valuations; g_i are non-zero polynomials which are independent of j . Now for any r

and for infinitely many $j \geq j_1$, Lemma 2 and (ii) of Section 2 imply that

$$\log |e_j|_p \leq j \max(\log |\gamma_i|_p) - c_1 r_j |t|.$$

Lemma 4(ii), and later (3), imply that the right-hand side above is

$$\leq c_2 j^r - c_3 r_j r^{1+1/n} \ll -r_j r^{1+1/n},$$

where $1 \ll c_i \ll 1$ ($1 \leq i \leq 3$). Thus (iii) follows.

To establish our last estimates we need to define the size $s(\alpha)$ of any algebraic number $\alpha \neq 0$. This is given by

$$s(\alpha) = \max(\|\alpha\|, \text{den } \alpha),$$

where $\|\alpha\|$ denotes the maximum of the archimedean absolute values of the conjugates of α , and $\text{den } \alpha$ is the minimal natural number for which $(\alpha \text{den } \alpha)$ is an algebraic integer. For any valuation we have

$$(11) \quad |\alpha|_p \geq (s(\alpha))^{-2d},$$

where d denotes the degree of the field K over \mathcal{Q} , provided that α belongs to K . We assume that

$$(12) \quad \log s(b_{ij}) \ll r_j.$$

On extending K if necessary we may assume without loss of generality that all components of α lie in K .

LEMMA 5. *For any j and any r as in Lemma 4 we have*

$$\log s(e_j) \ll rr_j.$$

PROOF. By (3), (7) and (12) we deduce that $\log s(\omega_{jk}) \ll r_j$. Since r_j is the maximal entry of T_j we have $\log s(\alpha_{ij}) \ll r_j$, where α_{ij} denotes the i th component of α_j . Lemma 1 implies that the polynomial $P_q(\mathbf{z}, \mathbf{w})$ has degree at most r in each of its variables, and its coefficients are K -integers whose sizes do not exceed a real positive number c , which may depend on r , but not on j . Thus $P_q(\mathbf{z}, \mathbf{w})$ is majorized by

$$c \left(\prod_{i=1}^n (1 + z_i)^r \right) \left(\prod_{k \leq h} (1 + w_k)^r \right).$$

We deduce that

$$\log s(P_q(\alpha_j, \omega_j)) \ll \log c + rr_j \ll rr_j,$$

for $r \gg 1$ and $j \geq j_2 (= j_2(r))$. The lemma now follows from (6).

Finally we establish the following:

THEOREM 2. *The numbers $f_{10}(\alpha), \dots, f_{m0}(\alpha)$ are algebraically independent over \mathbb{Q} .*

PROOF. We merely have to show that no relation of the form (1) can hold. But this is easy, since if the relation (1) did hold, we would obtain for any $r \gg 1$ and for infinitely many j ,

$$rr_j \gg \log s(e_j) \gg -\log |e_j|_p \gg r^{1+1/n} r_j;$$

the inequalities follow from Lemma 5, (11) and Lemma 4(iii), respectively. We obtain a contradiction, if r is large enough, which establishes the theorem.

As we remarked in the introduction, a variant of Theorem 2 has been obtained by Mahler in the special case that the transformation matrices T_j are equal to the j th power T^j of a fixed matrix T , and by Kubota (1977a), when all of the matrices T_j are scalars, provided that $\liminf(\log r_j/j) > 0$. Loxton and van der Poorten (1977a) established Theorem 2 in the case $m = 1$. However, we need Theorem 2 in its full generality in order to deduce Theorem 1.

5. Proof of Theorem 1

We shall now deduce Theorem 1 from Theorem 2, using the analysis of Loxton and van der Poorten (1977a), pp. 39–45.

Let ζ be a real irrational with $0 < \zeta < 1$, and denote by a_1, a_2, \dots , the partial quotients of the simple continued fraction of ζ . Put

$$\zeta_j = \frac{1}{a_{j+1} + \frac{1}{a_{j+2} + \dots}} \quad (j \geq 0);$$

hence $\zeta = \zeta_0$ and $\zeta_{j+1} = \zeta_j^{-1} - a_{j+1}$. The convergents p_j/q_j of ζ are determined by

$$p_0 = 1, \quad q_0 = 0; \quad p_1 = 0, \quad q_1 = 1;$$

$$p_{j+1} = a_j p_j + p_{j-1}, \quad q_{j+1} = a_j q_j + q_{j-1} \quad (j \geq 1).$$

We have

$$\frac{p_{j+1}}{q_{j+1}} = \frac{1}{a_1 + a_2 + \dots + a_j}, \quad \frac{q_j}{q_{j+1}} = \frac{1}{a_j + \dots + a_1}.$$

Put $n = 2m$, and let $\mathbf{z} = (z_1, \dots, z_n)$ be a vector of n variables. The function

$$f_{ij}(\mathbf{z}) = \sum_{k=0}^{\infty} \sum_{1 \leq h < k \leq j} z_{2i-1}^k z_{2i}^h \quad (1 \leq i \leq m, j \geq 0),$$

converges for all \mathbf{z} with $l_i < 0$, where we put

$$l_i = \log |z_{2i-1}|_p + \zeta \log |z_{2i}|_p.$$

Denote by T'_j and T_j the $n \times n$ matrices with

$$\begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} q_{j+1} & p_{j+1} \\ q_j & p_j \end{pmatrix} \quad (j \geq 1),$$

along their main diagonals, respectively. We denote by T'_0 and by T_0 the identity $n \times n$ matrix, and note that $T_j = T'_j T_{j-1}$ ($j \geq 1$). Condition (3) now follows with $r_j = q_{j+1}$, and we note that since $r_j = a_j r_{j-1} + r_{j-2}$ and a_j are rational integers, we cannot have $jr_{j+1} = (j+1)r_j$ for all $j \geq 1$. It is easy to verify that

$$f_{ij}(\mathbf{z}'_j) = -f_{i,j-1}(\mathbf{z}) + z'_{2i-1,j} z'_{2i,j} / (1 - z'_{2i-1,j})(1 - z'_{2i,j}),$$

where $\mathbf{z}'_j = T'_j \mathbf{z} = (z'_{1j}, \dots, z'_{nj})$, and further that

$$(13) \quad f_{i0}(\mathbf{z}) = (-1)^j f_{ij}(\mathbf{z}_j) + \sum_{k=1}^j (-1)^{k-1} z_{2i-1,k} z_{2i,k} / (1 - z_{2i-1,k})(1 - z_{2i,k}),$$

where $\mathbf{z}_j = T_j \mathbf{z} = (z_{1j}, \dots, z_{nj})$. We deduce that (4) and (12) hold for any n -tuple $\mathbf{z} = \boldsymbol{\alpha}$ with non-zero (algebraic) components such that

$$l_i = l_i(\boldsymbol{\alpha}) < 0 \quad \text{and} \quad \alpha_{2i-1}^{q_i} \alpha_{2i}^{p_i} \neq 1 \quad (1 \leq i \leq m).$$

Henceforth we shall assume that $|\alpha_i|_p \leq 1$ ($1 \leq i \leq 2m$), and we distinguish between the two cases.

Case I. Suppose that the partial quotients a_j are bounded. Thus $\lambda = \liminf q_{j+1}/q_j$ is finite, greater than 1, and irrational. This is the number λ which is mentioned in the statement of Theorem 1. On restricting j to a subsequence with $q_{j+1}/q_j \rightarrow \lambda$, condition (ii) of Section 2 obtains for any vector $\mathbf{z} = \boldsymbol{\alpha}$ with non-zero components, with \mathbf{s} proportional to an n -tuple whose $(2i-j)$ th component is equal to $-\lambda^j l_i$ ($1 \leq i \leq m; j = 0, 1$). Loxton and van der Poorten (1977a), pp. 43–4, proved that the sequence $\mathbf{f}_j = (f_{1j}, \dots, f_{mj})$ admits a subsequence which converges to an m -tuple of non-constant functions, each of which is transcendental over $K_p[\mathbf{z}]$. But f_{ij} ($1 \leq i \leq m$) are functions of independent variables, hence the limit functions

are algebraically independent over $K_p[z]$. Theorem 2 now holds for any n -tuple $\alpha = (\alpha_1, \dots, \alpha_n)$ of non-zero algebraic numbers, with $\alpha_{2i-1}^{l_i} \alpha_{2i}^{l_i} \neq 1$, such that l_i are negative and linearly independent over $Q + \lambda Q$. We obtain Theorem 1 in this case on putting $\alpha_{2i} = 1$ ($1 \leq i \leq m$). Note that when λ is algebraic it suffices to assume that $\log|\alpha_{2i-1}|_p$ ($1 \leq i \leq m$) are linearly independent over Q ; this follows from Baker's theorem on linear forms in the logarithms of algebraic numbers.

In the complex case the linear independence assumption can be satisfied with arbitrary large m . In the nonarchimedean case we can take $m = 1$ only, since the p -adic valuation of any algebraic number is equal to some rational power of p . Thus we obtain the transcendence of $\sum [r\zeta] z^r$ at $z = \alpha$, in the p -adic sense, where α is any algebraic number with $0 < |\alpha|_p < 1$. It would be of interest to obtain a general algebraic independence result in the p -adic case, analogous to the one which we obtained in the complex case.

Case II. It remains to deal with the case that the partial quotients a_j are not bounded. In this case we shall establish the algebraic independence of $f_{10}(\alpha) \dots f_{m0}(\alpha)$ when $l_1 \dots l_m$ are distinct and negative, in the complex as well as in the p -adic case. We deduce from (13) that

$$f_{i0}(z) = \sum_{j=0}^{\infty} h_{ij}(z),$$

where

$$h_{ij}(z) = (-1)^{j-1} z_{2i-1,j} z_{2i,j} / (1 - z_{2i-1,j})(1 - z_{2i,j}),$$

and for any $j \geq 1$ we put for brevity

$$c_i = \sum_{k=1}^{j-1} h_{ik}(\alpha) \quad d_i = \sum_{k=j}^{\infty} h_{ik}(\alpha);$$

hence we have $c_i + d_i = f_{i0}(\alpha)$. Suppose that (ω_k) is a finite set of algebraic numbers, not all 0, such that

$$\sum_{k \leq h} \omega_k (c_1 + d_1)^{k_1} \dots (c_m + d_m)^{k_m} = 0.$$

Then

$$(14) \quad - \sum_k \omega_k c_1^{k_1} \dots c_m^{k_m} = \sum_k \omega_k (d_1 c'_1 + \dots + d_m c'_m) + \delta,$$

where δ is a linear form in products of at least two distinct d_i 's with bounded coefficients and where

$$c'_i = \left(\sum_{l=1}^{k_i} \binom{k_i}{l} c_i^{k_i-l} d_i^{l-1} \right) \left(\prod_{i \neq i} f_{i0}(\alpha) \right)^{k_i}.$$

On noting that the c_i are rational functions in $\alpha'_{ik} = \alpha_{2i-1}^{q_k} \alpha_{2i}^{q_k}$ ($1 \leq i \leq m, 1 \leq k \leq j$), we deduce that the left-hand side of (14) is an algebraic number, say t_j , with

$$(15) \quad \log s(t_j) \ll q_j.$$

We shall now find an upper bound for the valuation of the right-hand side of (14), where we restrict our attention to a subsequence of j with $q_{j+1}/q_j \rightarrow \infty$. We note that d_i can be expressed as a power series in $\alpha'_{ij}, \alpha'_{i,j+1}, \dots$, whose dominant term is $\alpha''_{i,j} = \alpha'_{ij} \alpha'_{i,j+1}$. Since $c_i = f_{i0}(\alpha) - d_i$, and $f_{i0}(\alpha) \neq 0$, the dominant term in $d_i c'_i$ is $\alpha'_{ij} k_i f_{i0}(\alpha)^{k_i-1} \prod_{l \neq i} f_{l0}(\alpha)^{k_l}$. Now if l_1, \dots, l_m are distinct, it is clear that the dominant term in the right-hand side of (14) is given by the product of α'_{ij} (with a fixed $i, 1 \leq i \leq m$) and

$$\sum_k \omega_k k_i f_{i0}(\alpha)^{k_i-1} \prod_{l \neq i} f_{l0}(\alpha)^{k_l}.$$

The last expression is certainly non-zero if we assume as we may that the algebraic dependence relation which is satisfied by the $f_{i0}(\alpha)$ is of minimal (total) degree. It follows that t_j is non-zero and that

$$(16) \quad \log |t_j|_p \ll -q_{j+1}.$$

But since $q_{j+1}/q_j \rightarrow \infty$, the inequalities (15) and (16) violate the fundamental inequality (11). Thus we obtain a contradiction to the assumption that $f_{10}(\alpha), \dots, f_{m0}(\alpha)$ are algebraically dependent. Theorem 1 follows in this case on taking $\alpha_{2i} = 1$ ($1 \leq i \leq m$).

References

K. K. Kubota (1977a), 'On Mahler's algebraic independence method', preprint.
 K. K. Kubota (1977b), 'Linear functional equations and algebraic independence', in *Transcendence theory: advances and applications*, edited by A. Baker and D. W. Masser (Academic Press).
 J. H. Loxton and A. J. van der Poorten (1977), 'Arithmetic properties of certain functions in several variables II', *J. Austral. Math. Soc.* **24**, 393–408.
 J. H. Loxton and A. J. van der Poorten (1977a), 'Arithmetic properties of certain functions in several variables III', *Bull. Austral. Math. Soc.* **16**, 15–47.
 J. H. Loxton and A. J. van der Poorten (1977b), 'Transcendence and algebraic independence by a method of Mahler', in *Transcendence theory: advances and applications*, edited by A. Baker and D. W. Masser (Academic Press).
 K. Mahler (1969), 'Remarks on a paper by W. Schwarz', *J. Number Theory* **1**, 512–521.

Institute for Advanced Study
 Princeton, New Jersey 08540
 U.S.A.