ACTA ARITHMETICA
113.4 (2004)

Algebraic independence of elements from $\mathbb{C}_p$ over $\mathbb{Q}_p$, II

by

PETER BUNDSCHUH (Cologne) and VLADIMIR G. CHIRSKII (Moscow)

Dedicated to Rob Tijdeman
on the occasion of his sixtieth birthday

1. Introduction, main results, applications. Let $\mathbb{Q}_p$ be the p-adic completion of $\mathbb{Q}$ for a prime p. Denote by $\mathbb{Z}_p$ the ring of p-adic integers, i.e. of those elements $x \in \mathbb{Q}_p$ with $|x|_p \leq 1$. The unit group of $\mathbb{Q}_p$, i.e. the set of $x \in \mathbb{Q}_p$ with $|x|_p = 1$, will be denoted by U_p. Let $\overline{\mathbb{Q}}_p$ be the algebraic closure of $\mathbb{Q}_p$ and $\mathbb{C}_p$ its p-adic completion, which is an algebraically closed complete field with a valuation uniquely extended from $\mathbb{Q}_p$.

Whereas the questions of transcendence or algebraic independence of elements from $\mathbb{Q}_p$ or even from $\mathbb{C}_p$ over $\mathbb{Q}$ are rather well investigated, the corresponding question for $\mathbb{C}_p$ over $\mathbb{Q}_p$ has been studied in the past only occasionally. For a brief survey on what was published on this topic so far, we refer the reader to our recent paper [3]. The main result there gives sufficient conditions for the algebraic independence over $\mathbb{Q}_p$ of numbers from $\mathbb{C}_p$ defined by infinite series of the form $\sum a_k p^{r_k}$, where (r_k) is a sequence of positive rational numbers and the coefficients a_k are p-adic integers.

In our present paper, we propose two new such criteria, where the hypotheses on the a_k, r_k are now slightly stronger. But, on the other hand, we no longer need, as in [3], conditions on determinants involving certain of the coefficients a occurring in the different series under consideration. Both of these criteria have the same appearance, typical in algebraic independence theory: Under appropriate assumptions on functions $f_1, \ldots, f_l$ and points $\alpha_1, \ldots, \alpha_m$, the $l \cdot m$ numbers $f_\lambda(\alpha_\mu)$ from $\mathbb{C}_p$ are algebraically independent over $\mathbb{Q}_p$.

2000 *Mathematics Subject Classification*: 11J85, 11J61.

The main part of this work was carried out during the authors' Oberwolfach stay in 2002 within the scope of the RiP-program. They are grateful for this opportunity to complete their joint research which began during visits of the second author to Cologne University supported by INTAS-RFBR grant IR-97-1904.

Using the notation $\mathbb{N} := \{1, 2, \ldots\}$ and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$, we now are going on to formulate our first main result, which concerns the particular case $l = 1$.

THEOREM 1. *Let*

$$f(z) := \sum_{j=0}^{\infty} c_j z^j \in \mathbb{Z}_p[[z]]$$

satisfy $c_j \neq 0$ *for at least one* $j \in \mathbb{N}$. *Suppose*

$$\alpha_\mu := \sum_{k=1}^{\infty} a_{k,\mu}\, p^{r_{k,\mu}} \qquad (\mu = 1, \ldots, m)$$

with $a_{k,\mu} \in U_p$ *for any possible pair* (k, μ), *and where the sequences* $(r_{k,\mu})_k \in \mathbb{Q}_+^{\mathbb{N}}$ *satisfy the following technical conditions for* $\mu = 1, \ldots, m$:

(i) $(r_{k,\mu})_k$ *increases eventually strictly and is unbounded.*

(ii) *There exist infinitely many* $n \in \mathbb{N}$ *such that* $r_{n+1,\mu}$ *cannot be expressed as a finite linear combination with rational integer coefficients of the numbers* $1, r_{1,\mu}, \ldots, r_{n,\mu}$ *and the* $r_{k,\mu'}$ *with* $\mu' \neq \mu$.

Then the elements $f(\alpha_1), \ldots, f(\alpha_m) \in \mathbb{C}_p$ *are algebraically independent over* $\mathbb{Q}_p$. *In particular*, $\alpha_1, \ldots, \alpha_m$ *are algebraically independent over* $\mathbb{Q}_p$.

REMARK. Since $|\alpha_\mu|_p < 1$, the series f converges at all points $\alpha_1, \ldots, \alpha_m$.

After the proof of Theorem 1, at the end of Section 3, we briefly discuss how far the conditions on the r's are necessary.

Before giving an application of Theorem 1, we point out that we shall denote by $\operatorname{ord}_p x$ the highest power of p dividing $x \in \mathbb{Z} \setminus \{0\}$, and this notion can be extended to $x \in \mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ as well. Then the p-adic value of x is given by

$$|x|_p = p^{-\operatorname{ord}_p x}$$

for $x \in \mathbb{Q}^\times$, which we may use to define $\operatorname{ord}_p x$ more generally for any $x \in \mathbb{Q}_p^\times$ (or even $x \in \mathbb{C}_p^\times$). The above equation allows us to jump back and forth as we please between the two notions $|\ |_p$ and ord_p.

COROLLARY 1. *For* $\mu = 1, \ldots, m$, *let* $(q_{n,\mu})_{n \in \mathbb{N}}$ *be an arbitrary sequence of integers with* $q_{n,\mu} \neq 0$ *for infinitely many* n, *and suppose* $r_\mu \in \mathbb{Q}$, $r_\mu > 1$ *such that there exists a prime* p_μ *with* $-\operatorname{ord}_{p_\mu} r_\mu \in \mathbb{N}$ *and* $\operatorname{ord}_{p_\mu} r_{\mu'} \in \mathbb{N}_0$ *for any* $\mu' \neq \mu$ (*if* $m > 1$). *Then the elements*

$$\alpha_\mu := \prod_{n=1}^{\infty} (1 + p^{r_\mu^n})^{q_{n,\mu}} \qquad (\mu = 1, \ldots, m)$$

from $\mathbb{C}_p$ *are algebraically independent over* $\mathbb{Q}_p$.

Whereas in Theorem 1 our function f had only to be non-constant, our second main result needs, even in the case $l = 1$, a stronger hypothesis.

THEOREM 2. *Let the functions*

$$f_\lambda(z) := \sum_{j=0}^{\infty} c_{j,\lambda} z^j \in \mathbb{Z}_p[[z]] \quad (\lambda = 1, \ldots, l)$$

be algebraically independent over $\mathbb{Q}_p$. *Suppose that the elements*

$$\alpha_\mu := \sum_{k=1}^{\infty} a_{k,\mu} p^{r_{k,\mu}} \quad (\mu = 1, \ldots, m)$$

satisfy the conditions of Theorem 1. *Then the* $l \cdot m$ *elements* $f_\lambda(\alpha_\mu)$ $(\lambda = 1, \ldots, l,\ \mu = 1, \ldots, m)$ *from* $\mathbb{C}_p$ *are algebraically independent over* $\mathbb{Q}_p$.

REMARK 1. Clearly, for any λ there exists a $j_\lambda \in \mathbb{N}$ with $c_{j_\lambda,\lambda} \neq 0$ such that every f_λ satisfies the conditions on f in Theorem 1.

REMARK 2. The proof of Theorem 2 in Section 5 will use induction on m. The particular case $m = 1$ is stated in Section 2 as Proposition.

REMARK 3. In what follows, we shall need on several occasions the following fact. If $L|K$ is any field extension, then the power series $f_1, \ldots, f_l \in K[[z]]$ are algebraically independent over L if and only if they are so over K. Whereas one of these implications is trivial, the proof of the converse can be modeled exactly upon the procedure shown in Shidlovskii's monograph [7, p. 83] in the particular case where $L = \mathbb{C}$ and K is an algebraic number field.

Our first application of Theorem 2 concerns the case $l = 3$, more precisely the identity on $\mathbb{C}_p$, the p-adic exponential function $\exp_p$ and the p-adic logarithm $\log_p$. The last two are defined in $\mathbb{C}_p$ by the following power series:

$$\exp_p z := \sum_{k=0}^{\infty} \frac{z^k}{k!} \qquad \text{iff } |z|_p < p^{-1/(p-1)},$$

$$\log_p(1+z) := -\sum_{k=1}^{\infty} \frac{(-z)^k}{k} \qquad \text{iff } |z|_p < 1$$

respectively; compare e.g. [4]. These power series on the right-hand sides having rational coefficients are exactly as in the complex case. Therefore we can say: Since the complex functions z, $\exp z$, $\log(1+z)$ are algebraically independent over $\mathbb{C}$, they are so over $\mathbb{Q}$ as well, and thus the p-adic functions z, $\exp_p z$, $\log_p(1+z)$ living in $|z|_p < p^{-1/(p-1)}$ are algebraically independent over $\mathbb{C}_p$, or equivalently, over $\mathbb{Q}_p$. By the way, the algebraic independence of these three functions can be easily proved, even by a purely algebraic reasoning. We leave the corresponding details to the reader.

After these intermediate considerations, we are going to give a first application of Theorem 2. Two others, more involved in their formulation, will be discussed in Section 6.

Corollary 2. *If* $\alpha_1, \ldots, \alpha_m$ *satisfy the conditions of Theorem* 1, *then the* $3m$ *elements* α_μ, $\exp_p(p\alpha_\mu)$, $\log_p(1+\alpha_\mu)$ $(\mu = 1, \ldots, m)$ *from* $\mathbb{C}_p$ *are algebraically independent over* $\mathbb{Q}_p$.

We may combine Corollaries 1 and 2 as follows. Write the infinite products α_μ from Corollary 1 as $1 + \alpha_\mu^*$, where the α_μ^* satisfy the conditions of Theorem 1 (compare the beginning of Section 4). As a consequence of Corollary 2, the α_μ^*, $\log_p(1+\alpha_\mu^*)$ $(\mu = 1, \ldots, m)$ are algebraically independent over $\mathbb{Q}_p$, which is equivalent to the algebraic independence over $\mathbb{Q}_p$ of the α_μ, $\log_p \alpha_\mu$ $(\mu = 1, \ldots, m)$.

2. Some lemmas and a proposition. For the proof of Theorem 1 we shall need Lemma 2 below, which will be an easy consequence of the following

Lemma 1. *Let the power series*

$$\varphi(z) := \sum_{j=0}^{\infty} d_j z^j \in \mathbb{Z}_p[[z]]$$

satisfy $d_j \neq 0$ *for at least one* $j \in \mathbb{N}$. *Suppose*

$$\alpha := \sum_{k=1}^{\infty} a_k \, p^{r_k}$$

with $a_k \in U_p$ *for any* $k \in \mathbb{N}$, *and where* $(r_k) \in \mathbb{Q}_+^{\mathbb{N}}$ *satisfies the following technical conditions*:

(i) *The sequence* (r_k) *increases eventually strictly and is unbounded.*

(ii) *There exist infinitely many* $n \in \mathbb{N}$ *such that* r_{n+1} *cannot be expressed as a linear combination with rational integer coefficients of the numbers* $1, r_1, \ldots, r_n$.

Then $\varphi'(\alpha) \neq 0$ *implies* $\varphi(\alpha) \neq 0$.

Proof. The ith formal derivative of φ is defined, of course, by

$$\varphi^{(i)}(z) = \sum_{j=i}^{\infty} j \ldots (j-i+1) d_j z^{j-i}.$$

Since $\left|\binom{j}{i} d_j \alpha^{j-i}\right|_p \leq |\alpha|_p^{j-i}$ and $|\alpha|_p < 1$, all $\varphi^{(i)}(\alpha)/i!$ exist.

Suppose that, under the conditions of Lemma 1, we have $\varphi'(\alpha) \neq 0$ but $\varphi(\alpha) = 0$. Defining $\alpha^{(n)}$ to be the nth partial sum $\sum_{k=1}^{n} a_k p^{r_k}$ of α, we have

$\mathrm{ord}_p(\alpha^{(n)} - \alpha) = r_{n+1}$ for all large n. Since $\varphi(\alpha) = 0$ we get

$$\varphi(\alpha^{(n)}) = \varphi(\alpha + (\alpha^{(n)} - \alpha)) = \varphi'(\alpha)(\alpha^{(n)} - \alpha) + \frac{\varphi''(\alpha)}{2!}(\alpha^{(n)} - \alpha)^2 + \ldots$$

From $\varphi'(\alpha) \neq 0$ it is evident that, for n large enough, the p-order of the right-hand side is exactly $\mathrm{ord}_p(\varphi'(\alpha)(\alpha^{(n)} - \alpha))$, and therefore we find

$$\mathrm{ord}_p\, \varphi(\alpha^{(n)}) = \mathrm{ord}_p\, \varphi'(\alpha) + r_{n+1} \tag{1}$$

for all large n. This equation is our basic information leading finally to the desired contradiction. From

$$\varphi'(\alpha) = \sum_{j=1}^{\infty} jd_j \Big(\sum_{k=1}^{\infty} a_k p^{r_k}\Big)^{j-1}$$

we see that each summand occurring on the right-hand side has a p-order being a finite linear combination of $1, r_1, r_2, \ldots$ with non-negative integer coefficients. Since $\varphi'(\alpha) \neq 0$ we know that $\mathrm{ord}_p\, \varphi'(\alpha)$ is such a finite linear combination. Let us call it $u + u_1 r_1 + \ldots + u_h r_h$ with $u, u_1, \ldots, u_h \in \mathbb{N}_0$ but $u_h \neq 0$ without loss of generality. We fix this linear combination for $\mathrm{ord}_p\, \varphi'(\alpha)$.

Now we investigate

$$\varphi(\alpha^{(n)}) = \sum_{j=0}^{\infty} d_j \Big(\sum_{k=1}^{n} a_k p^{r_k}\Big)^{j}.$$

Here every summand occurring on the right-hand side has a p-order being a linear combination of $1, r_1, \ldots, r_n$ again with non-negative coefficients.

These considerations, combined with (1), lead to the following fact. r_{n+1} is a linear combination of $1, r_1, \ldots, r_n$ with integer coefficients if $n \geq h$ is large enough. But this contradicts condition (ii) of Lemma 1.

REMARK. Of course, admitting here and in what follows the usual convention $\mathrm{ord}_p\, 0 = \infty$, equation (1) implies $\varphi(\alpha^{(n)}) \neq 0$ for any large n.

A rather immediate consequence of Lemma 1 is

LEMMA 2. *If f satisfies the conditions of Theorem* 1, *and α those of Lemma* 1, *then $f'(\alpha) \neq 0$.*

Proof. Let q be the smallest positive integer with $f^{(q)}(\alpha) \neq 0$. Such a q must exist, by the condition on f in Theorem 1. Assuming $q > 1$, we put

$$\varphi(z) := f^{(q-1)}(z) \in \mathbb{Z}_p[[z]],$$

leading us to $\varphi(\alpha) = 0$ and $\varphi'(\alpha) \neq 0$. This contradicts Lemma 1.

Another application of Lemma 1 is the following

PROPOSITION. *Let $f_1, \ldots, f_l$, of the form*

$$f_\lambda(z) := \sum_{j=0}^{\infty} c_{j,\lambda} z^j \in \mathbb{Z}_p[[z]],$$

be algebraically independent over $\mathbb{Q}_p$. Suppose

$$\alpha := \sum_{k=1}^{\infty} a_k p^{r_k}$$

is as in Lemma 1. Then $f_1(\alpha), \ldots, f_l(\alpha)$ are algebraically independent over $\mathbb{Q}_p$.

REMARK. If the functions $f_1, \ldots, f_l$ are algebraically dependent over $\mathbb{Q}_p$, then, of course, so are the values $f_1(\alpha), \ldots, f_l(\alpha)$.

Proof. Let $P \in \mathbb{Z}_p[X_1, \ldots, X_l]$ be non-constant, and define $\varphi(z) := P(f_1(z), \ldots, f_l(z))$. Clearly,

$$\varphi(z) = \sum_{j=0}^{\infty} d_j z^j \in \mathbb{Z}_p[[z]].$$

Clearly there exists a $q \in \mathbb{N}$ with $\varphi^{(q)}(\alpha) \neq 0$, since $\varphi'(\alpha) = \varphi''(\alpha) = \ldots = 0$ would imply that φ is constant, $\varphi(z) = d_0$, and thus

$$P(f_1(z), \ldots, f_l(z)) = d_0,$$

contradicting the algebraic independence of $f_1, \ldots, f_l$ over $\mathbb{Q}_p$.

Consider now the function $\varphi^{(q-1)}(z)$, which cannot be constant. Thus, we get $\varphi^{(q-1)}(\alpha) \neq 0$, by Lemma 1. If $q = 1$, then we have $\varphi(\alpha) \neq 0$, or equivalently $P(f_1(\alpha), \ldots, f_l(\alpha)) \neq 0$. If $q > 1$, we consider the non-constant function $\varphi^{(q-2)}(z)$ and conclude $\varphi^{(q-2)}(\alpha) \neq 0$, and so on.

The following two lemmas prepare the proof of Theorem 2. Since their proofs generalize those of the above two lemmas, we will be somewhat briefer.

LEMMA 3. *Let $\alpha_1, \ldots, \alpha_m$ satisfy the conditions of Theorem 1. For any $\mu = 1, \ldots, m$, let*

$$\varphi_\mu(z) := \sum_{j=0}^{\infty} d_{j,\mu} z^j,$$

where all $d_{j,\mu} \in \mathbb{Z}_p[[\alpha_1, \ldots, \widehat{\alpha}_\mu, \ldots, \alpha_m]]$ (*) and $d_{j,\mu} \neq 0$ for at least one $j = j(\mu) \in \mathbb{N}$. Then $\varphi'_\mu(\alpha_\mu) \neq 0$ implies $\varphi_\mu(\alpha_\mu) \neq 0$.

Proof. Suppose that our assertion is false, i.e. $\varphi'_\mu(\alpha_\mu) \neq 0$ but $\varphi_\mu(\alpha_\mu) = 0$ for some $\mu \in \{1, \ldots, m\}$. Defining $\alpha_\mu^{(n)}$ as the nth partial sum of the

(*) This is an abbreviation for $\mathbb{Z}_p[[\alpha_1, \ldots, \alpha_{\mu-1}, \alpha_{\mu+1}, \ldots, \alpha_m]]$.

series for α_μ in Theorem 1, we have

$$\varphi_\mu(\alpha_\mu^{(n)}) = \varphi'_\mu(\alpha_\mu)(\alpha_\mu^{(n)} - \alpha_\mu) + \frac{\varphi''_\mu(\alpha_\mu)}{2!}(\alpha_\mu^{(n)} - \alpha_\mu)^2 + \ldots$$

Since $\varphi'_\mu(\alpha_\mu) \neq 0$, it follows that the p-order of the right-hand side is $\mathrm{ord}_p(\varphi'_\mu(\alpha_\mu)(\alpha_\mu^{(n)} - \alpha_\mu))$ for any $n \geq n_\mu$. This implies, for any large n ($\geq n_\mu$),

$$\mathrm{ord}_p\, \varphi_\mu(\alpha_\mu^{(n)}) = \mathrm{ord}_p\, \varphi'_\mu(\alpha_\mu) + r_{n+1,\mu}. \tag{2}$$

To examine $\mathrm{ord}_p\, \varphi'_\mu(\alpha_\mu)$, we note that

$$\varphi'_\mu(\alpha_\mu) = \sum_{j=1}^{\infty} j d_{j,\mu} \alpha_\mu^{j-1} \quad \text{and} \quad d_{j,\mu} \in \mathbb{Z}_p[[\alpha_1, \ldots, \widehat{\alpha}_\mu, \ldots, \alpha_m]].$$

The definition of $\alpha_1, \ldots, \alpha_m$ in Theorem 1 shows us that $\varphi'_\mu(\alpha_\mu)$ is a sum of products of an element from U_p times a rational power of p, where the exponent of p is a finite linear combination (over $\mathbb{N}_0$) of 1 and the $r_{k,\mu}$ with $k \in \mathbb{N}$, $\mu \in \{1, \ldots, m\}$. Thus $\mathrm{ord}_p\, \varphi'_\mu(\alpha_\mu)$ is again such a linear combination, which we fix from now on. We denote by k_μ the maximal first subscript k such that $r_{k,\nu}$ appears for some $\nu \in \{1, \ldots, m\}$ with a positive integer coefficient in this fixed combination.

Just the same consideration provides us with the fact that $\mathrm{ord}_p\, \varphi_\mu(\alpha_\mu^{(n)})$ is a finite linear combination (over $\mathbb{N}_0$) of $1, r_{1,\mu}, \ldots, r_{n,\mu}$ and the $r_{k,\mu'}$ with $\mu' \in \{1, \ldots, \widehat{\mu}, \ldots, m\}$. Combined with (2), this leads us to the insight that, for each large $n \geq \max\{n_\mu, k_\mu\}$, the number $r_{n+1,\mu}$ is a finite linear combination (over $\mathbb{Z}$) of $1, r_{1,\mu}, \ldots, r_{n,\mu}$ and some of the $r_{k,\mu'}$ with $\mu' \neq \mu$. Again this contradicts our hypotheses on the α's.

From Lemma 3 we conclude

LEMMA 4. *For $\alpha_1, \ldots, \alpha_m$ and $\varphi_1, \ldots, \varphi_m$ as in Lemma 3,*

$$\varphi'_\mu(\alpha_\mu) \neq 0$$

for $\mu = 1, \ldots, m$.

Proof. The hypotheses imply the existence of a smallest $q_\mu \in \mathbb{N}$ with $\varphi_\mu^{(q_\mu)}(\alpha_\mu) \neq 0$. If $q_\mu > 1$, we consider

$$\psi_\mu(z) := \varphi_\mu^{(q_\mu - 1)}(z) \in \mathbb{Z}_p[[\alpha_1, \ldots, \widehat{\alpha}_\mu, \ldots, \alpha_m]][[z]],$$

which satisfies all conditions of Lemma 3. Since $\psi'_\mu(\alpha_\mu) \neq 0$, we get $\psi_\mu(\alpha_\mu) \neq 0$ or equivalently $\varphi_\mu^{(q_\mu - 1)}(\alpha_\mu) \neq 0$, contradicting our choice of q_μ.

3. Proof of Theorem 1. We will argue by induction on m. To start with $m = 1$, we simply write $\alpha := \alpha_1 = \sum_{k=1}^{\infty} a_k p^{r_k}$ as in Lemma 1. We put $\gamma := f(\alpha)$, and we let $P \in \mathbb{Z}_p[X]$ be of minimal degree such that $P(\gamma) = 0$, assuming, of course, that γ is algebraic over $\mathbb{Q}_p$. As in the proof of Lemma 1, let $\alpha^{(n)}$ denote the nth partial sum of the series for α, and put $\gamma^{(n)} := f(\alpha^{(n)})$.

Next we must investigate the differences $\gamma^{(n)} - \gamma$. Clearly

$$\gamma^{(n)} - \gamma = f(\alpha^{(n)}) - f(\alpha) = f'(\alpha)(\alpha^{(n)} - \alpha) + \frac{f''(\alpha)}{2!}(\alpha^{(n)} - \alpha)^2 + \ldots,$$

where we know $f'(\alpha) \neq 0$ from Lemma 2. Thus we get

$$\operatorname{ord}_p(\gamma^{(n)} - \gamma) = \operatorname{ord}_p f'(\alpha) + \operatorname{ord}_p(\alpha^{(n)} - \alpha) \tag{3}$$

for any large n.

From the above choice of P we deduce

$$\begin{aligned} P(\gamma^{(n)}) &= P'(\gamma)(\gamma^{(n)} - \gamma) + \frac{P''(\gamma)}{2!}(\gamma^{(n)} - \gamma)^2 + \ldots \\ &=: P'(\gamma)(\gamma^{(n)} - \gamma) + P^*(\gamma^{(n)} - \gamma), \end{aligned} \tag{4}$$

where the power series $P^*(X) := \sum_{i=2}^{\infty}(P^{(i)}(\gamma)/i!)X^i \in \mathbb{C}_p[[X]]$ has $\operatorname{ord}_p(P^{(i)}(\gamma)/i!) \geq 0$. For n large enough, the p-order of the right-hand side of (4) is $\operatorname{ord}_p(P'(\gamma)(\gamma^{(n)} - \gamma))$; compare (3) and $P'(\gamma) \neq 0$. Thus it follows from (3) and (4) that

$$\operatorname{ord}_p P(\gamma^{(n)}) = \operatorname{ord}_p P'(\gamma) + \operatorname{ord}_p f'(\alpha) + \operatorname{ord}_p(\alpha^{(n)} - \alpha) \tag{5}$$

for any large n.

Now we try to get the desired contradiction from (5). As in the proof of Lemma 1, we find the existence of an $h \in \mathbb{N}_0$ such that

$$\operatorname{ord}_p f'(\alpha) = u + u_1 r_1 + \ldots + u_h r_h, \qquad \operatorname{ord}_p P'(\gamma) = v + v_1 r_1 + \ldots + v_h r_h$$

with $u, u_1, \ldots, u_h, v, v_1, \ldots, v_h \in \mathbb{N}_0$. Clearly, $\operatorname{ord}_p(\alpha^{(n)} - \alpha) = r_{n+1}$ for every large n, under the hypotheses of Theorem 1. What about $\operatorname{ord}_p P(\gamma^{(n)})$? If $e_0, \ldots, e_J \in \mathbb{Z}_p$ are the coefficients of P, we see

$$P(\gamma^{(n)}) = \sum_{i=0}^{J} e_i f(\alpha^{(n)})^i = \sum_{i=0}^{J} e_i \Big(\sum_{j=0}^{\infty} c_j \Big(\sum_{k=1}^{n} a_k p^{r_k}\Big)^j\Big)^i.$$

Hence $\operatorname{ord}_p P(\gamma^{(n)})$ is a linear combination of $1, r_1, \ldots, r_n$ with non-negative integer coefficients. Then we deduce from (5) that, for any large $n \geq h$, r_{n+1} is a linear combination (over $\mathbb{Z}$) of $1, r_1, \ldots, r_n$, contradicting condition (ii) of Theorem 1.

To perform the inductive step, we define

$$\gamma_\mu := f(\alpha_\mu) \qquad (\mu = 1, \ldots, m).$$

We suppose $m > 1$, and assume that $\gamma_1, \ldots, \gamma_m$ are algebraically dependent over $\mathbb{Q}_p$, whereas any subset of $m-1$ elements is not. Let $P \in \mathbb{Z}_p[X_1, \ldots, X_m]$ be a non-constant polynomial of minimal total degree such that

$$P(\gamma_1, \ldots, \gamma_m) = 0. \tag{6}$$

By our hypothesis, P must depend on all variables X_μ and

$$\frac{\partial P}{\partial X_\mu}(\gamma_1, \ldots, \gamma_m) \neq 0 \quad (\mu = 1, \ldots, m), \tag{7}$$

by our minimality condition on P. From (6) we get

$$\begin{aligned} P(X_1, \ldots, X_m) \\ = \sum_{\mu=1}^{m} \frac{\partial P}{\partial X_\mu}(\gamma_1, \ldots, \gamma_m)(X_\mu - \gamma_\mu) + P^*(X_1 - \gamma_1, \ldots, X_m - \gamma_m), \end{aligned} \tag{8}$$

where all monomials in $X_1 - \gamma_1, \ldots, X_m - \gamma_m$ in the polynomial P^* have total degree at least 2 and coefficients from $\mathbb{C}_p$ of non-negative p-order.

Now defining

$$\alpha_\mu^{(n)} := \sum_{k=1}^{n} a_{k,\mu} p^{r_{k,\mu}}, \qquad A_\mu^{(n)} := \alpha_\mu^{(n)} - \alpha_\mu = -\sum_{k>n} a_{k,\mu}\, p^{r_{k,\mu}}, \tag{9}$$

and

$$\gamma_\mu^{(n)} := f(\alpha_\mu^{(n)}), \tag{10}$$

we find from the definition of γ_μ that

$$\gamma_\mu^{(n)} - \gamma_\mu = \sum_{i=1}^{\infty} \frac{f^{(i)}(\alpha_\mu)}{i!}\, (A_\mu^{(n)})^i. \tag{11}$$

With $n_1, \ldots, n_m \in \mathbb{N}_0$, to be specified later, we deduce from (8) and (11) that

$$\begin{aligned} P(\gamma_1^{(n_1)}, \ldots, \gamma_m^{(n_m)}) = {} & \sum_{\mu=1}^{m} f'(\alpha_\mu)\, \frac{\partial P}{\partial X_\mu}(\gamma_1, \ldots, \gamma_m) A_\mu^{(n_\mu)} \\ & + \sum_{\mu=1}^{m} \frac{\partial P}{\partial X_\mu}(\gamma_1, \ldots, \gamma_m) \sum_{i=2}^{\infty} \frac{f^{(i)}(\alpha_\mu)}{i!}\, (A_\mu^{(n_\mu)})^i \\ & + P^*(\gamma_1^{(n_1)} - \gamma_1, \ldots, \gamma_m^{(n_m)} - \gamma_m). \end{aligned} \tag{12}$$

From (7) and Lemma 2, we get

$$B_\mu := f'(\alpha_\mu)\, \frac{\partial P}{\partial X_\mu}(\gamma_1, \ldots, \gamma_m) \neq 0 \quad (\mu = 1, \ldots, m),$$

and, defining $b_\mu := \operatorname{ord}_p B_\mu$ for $\mu = 1, \ldots, m$, we may suppose without loss of generality that

$$b_1 \geq \ldots \geq b_m. \tag{13}$$

The different terms on the right-hand side of the non-vanishing

$$f'(\alpha_\mu)=\sum_{j=1}^{\infty} jc_j\alpha_\mu^{j-1}=\sum_{j=1}^{\infty} jc_j\Big(\sum_{k=1}^{\infty} a_{k,\mu}p^{r_{k,\mu}}\Big)^{j-1}$$

have p-adic orders being finite linear combinations (over $\mathbb{N}_0$) of $1, r_{1,\mu}$, $r_{2,\mu},\ldots$ Similarly, the terms on the right-hand side of

$$\frac{\partial P}{\partial X_\mu}(\gamma_1,\ldots,\gamma_m)=\sum e_\mu(i_1,\ldots,i_m)f(\alpha_1)^{i_1}\ldots f(\alpha_m)^{i_m}, \qquad e_\mu(\ldots)\in\mathbb{Z}_p,$$

where the sum is extended over finitely many $(i_1,\ldots,i_m)\in\mathbb{N}_0^m$, have p-orders which are finite linear combinations (over $\mathbb{N}_0$) of 1 and all $r_{k,\nu}$ ($k\in\mathbb{N}$, $\nu=1,\ldots,m$). Therefore, we can assert that each b_μ is a finite linear combination (over $\mathbb{N}_0$) of 1 and all $r_{k,\nu}$. For any $\mu=1,\ldots,m$, we may fix such a linear combination for b_μ, and we define n_0 to be the maximal $k\in\mathbb{N}$ such that at least one $r_{k,\nu}$ occurs in at least one of these m fixed linear combinations.

Now we select $n_1>n_0$ according to the following conditions:

$$r_{n_1+1,1}>b_1, \tag{14}$$

$$\begin{cases} r_{n_1+1,1} \text{ is not a finite linear combination over } \mathbb{Z} \text{ of}\\ \quad 1, r_{1,1},\ldots,r_{n_1,1} \text{ and the } r_{k,\mu'} \text{ with } \mu'\in\{2,\ldots,m\}.\end{cases} \tag{15}$$

Finally we fix $n_2,\ldots,n_m\in\mathbb{N}_0$ such that

$$b_1+r_{n_1+1,1}<\ldots<b_m+r_{n_m+1,m} \tag{16}$$

implying, by (13),

$$r_{n_1+1,1}<\ldots<r_{n_m+1,m}. \tag{17}$$

Since $\operatorname{ord}_p A_\mu^{(n_\mu)}=r_{n_\mu+1,\mu}$ for n_μ large enough, by (9) and our hypotheses on the r-sequences, we find from (16) that

$$\operatorname{ord}_p\Big(\sum_{\mu=1}^{m} f'(\alpha_\mu)\,\frac{\partial P}{\partial X_\mu}(\gamma_1,\ldots,\gamma_m)A_\mu^{(n_\mu)}\Big)=b_1+r_{n_1+1,1}. \tag{18}$$

It remains to investigate the p-order of the second and third term on the right-hand side of (12). Clearly, for any $i\ge 2$, $\mu=1,\ldots,m$ we have

$$\operatorname{ord}_p\Big(\frac{\partial P}{\partial X_\mu}(\gamma_1,\ldots,\gamma_m)\cdot\frac{f^{(i)}(\alpha_\mu)}{i!}\,(A_\mu^{(n_\mu)})^i\Big)\ge 2r_{n_i+1,1}>b_1+r_{n_1+1,1},$$

by (14) and (17). The different terms of $P^*(\gamma_1^{(n_1)}-\gamma_1,\ldots,\gamma_m^{(n_m)}-\gamma_m)$ have p-orders not less than $2r_{n_1+1,1}>b_1+r_{n_1+1,1}$. With these considerations and (18), we conclude from (12) that $P(\gamma_1^{(n_1)},\ldots,\gamma_m^{(n_m)})$ does not vanish and moreover has

$$\omega:=\operatorname{ord}_p P(\gamma_1^{(n_1)},\ldots,\gamma_m^{(n_m)})=b_1+r_{n_1+1,1}. \tag{19}$$

On the other hand, we see from (9) and (10) that

$$\gamma_\mu^{(n)} = f(\alpha_\mu^{(n)}) = \sum_{j=0}^{\infty} c_j \Big(\sum_{k=1}^{n} a_{k,\mu} p^{r_{k,\mu}}\Big)^j$$

such that ω is a linear combination (over $\mathbb{N}_0$) of $1, r_{1,1}, \ldots, r_{n_1,1}, \ldots, r_{1,m}, \ldots, r_{n_m,m}$. This and (19) gives us the desired contradiction, taking $n_1 > n_0$ and hypothesis (15) into account. Herewith Theorem 1 is proved.

Remark. We briefly discuss the necessity of the conditions on the sequences $(r_k) \in \mathbb{Q}_+^{\mathbb{N}}$ appearing in our series

$$\sum_{k=1}^{\infty} a_k p^{r_k} \qquad (= \alpha).$$

Since $a_k \in U_p$, the assumption $(r_k) \to \infty$ is necessary and sufficient for the convergence of these series. If, in contrast to condition (ii) of Theorem 1, the sequence of denominators of r_k is bounded above, then α and $f(\alpha)$ are both algebraic over $\mathbb{Q}_p$ for arbitrary series $f \in \mathbb{Z}_p[[z]]$. Namely, under this new hypothesis, one can write both of them as finite sums of the shape

$$\sum_{\tau=0}^{t-1} A_\tau p^{\tau/t}$$

with all A_τ belonging to $\mathbb{Z}_p$ and $t \in \mathbb{N}$ the common denominator of all r_k.

4. The infinite product. For the *proof of Corollary 1*, we shall finally use Theorem 1 with $f(z) = z$. But let us first consider a typical product

$$\prod_{n=1}^{\infty} (1 + p^{r^n})^{q_n}$$

with $r \in \mathbb{Q} \setminus \mathbb{N}, r > 1$ and all $q_n \in \mathbb{Z}$ with $q_n \neq 0$ infinitely often. Clearly, this infinite product converges. We expand it as a series of the form

$$1 + \sum_{k=1}^{\infty} a_k p^{r_k}$$

with all $a_k \in U_p$, and all $r_k \in \mathbb{Q}_+$ are finite linear combinations of $1, r, \ldots, r^n, \ldots$ with coefficients from $\mathbb{N}_0$. We may suppose the sequence (r_k) to be strictly increasing.

Since

$$(1 + p^{r^n})^{q_n} = 1 + q_n p^{r^n} + \sum_{i=2}^{\infty} \binom{q_n}{i} p^{ir^n} \tag{20}$$

(where the sum vanishes for $q_n = 1$, and is finite for $q_n \in \mathbb{N}$), we first note that in the case $q_n \neq 0$,

$$\omega_p(n) := \operatorname{ord}_p q_n + r^n < \operatorname{ord}_p \binom{q_n}{i} + ir^n \quad \text{for } i \geq 2. \tag{21}$$

This inequality is a consequence of $\operatorname{ord}_p i < (i-1)r^n$, and this last estimate follows at once from $\operatorname{ord}_p i \leq (\log i)/(\log 2) \leq i - 1$. Clearly, the $\omega_p(n)$ are distinct for distinct n with $q_n \neq 0$, by our conditions on r. Since $\omega_p(n)$ tends to infinity with n ($q_n \neq 0$), we may define N_1 to be such that $\omega_p(N_1) = \min_{n\in\mathbb{N}} \omega_p(n)$, and inductively, for any $s > 1$, let $\omega_p(N_s) = \min_{n>N_{s-1}} \omega_p(n)$. Clearly, $N_1 < N_2 < \ldots$

For $N \in \mathbb{N}$ with $q_N \neq 0$, let $k_N \in \mathbb{N}$ be defined by

$$r_{k_N} = \omega_p(N).$$

Such a number k_N exists for each N as above, since we can obtain the corresponding term $\operatorname{ord}_p q_N + r^N$ by multiplying $q_N p^{r^N}$ on the right-hand side of (20) by the 1 from all other factors $(1 + p^{r^n})^{q_n}$, $n \neq N$.

Next we note that if an r_k contains some r^N with $q_N \neq 0$ as a summand, then r_k contains it in the form

$$\operatorname{ord}_p \binom{q_N}{i} + ir^N \tag{22}$$

with appropriate $i \geq 2$. Further, we point out that none of the linear combinations $r_1, \ldots, r_{k_{N_s}-1}$ contains some r^n ($n \geq N_s$) with a positive integer coefficient. Namely, by definition of N_s, for $n \geq N_s$ with $q_n \neq 0$ one has

$$\omega_p(n) \geq \omega_p(N_s) = r_{k_{N_s}}.$$

The number k_{N_s} is the smallest k such that r_k contains r^{N_s} as a summand with a positive coefficient, since

$$r_1 < \ldots < r_{k_{N_s}-1} < r_{k_{N_s}}$$

and all other r_k containing r^{N_s} have subscript $k > k_{N_s}$; this follows from (21) and (22).

We assert that $r_{k_{N_s}}$ cannot be expressed as a linear combination of $1, r_1, \ldots, r_{k_{N_s}-1}$ with integral coefficients. Otherwise we could rewrite this linear form as

$$r^{N_s} = B_0 + B_1 r + \ldots + B_{N_s-1} r^{N_s-1}$$

with all B's in $\mathbb{Z}$, contradicting the hypotheses on r.

Now we are in a position to apply Theorem 1 to the series

$$\sum_{k=1}^{\infty} a_{k,\mu} p^{r_{k,\mu}} := \prod_{n=1}^{\infty} (1 + p^{r_\mu^n})^{q_{n,\mu}} - 1 \quad (\mu = 1, \ldots, m), \tag{23}$$

which are just the $\alpha_\mu - 1$ in terms of our corollary. Our above investigations on the $a_{k,\mu}, r_{k,\mu}$ occurring in (23) show that these have all properties assumed in Theorem 1. Plainly, the role of the $r_{n+1,\mu}$ from Theorem 1 is now played by the different $r_{k_{N_s}}$ arising when carrying out the above considerations with $r = r_\mu$, $(q_n)_n = (q_{n,\mu})_n$ for $\mu = 1, \ldots, m$. Thus, we conclude from Theorem 1 that the $\alpha_1 - 1, \ldots, \alpha_m - 1$ are algebraically independent over $\mathbb{Q}_p$, and therefore so are the $\alpha_1, \ldots, \alpha_m$ as well, proving Corollary 1.

REMARK 1. For special sequences (q_n), the considerations in the preceding proof become much simpler. For instance, let us briefly discuss the case $q_n = 1$ for each $n \in \mathbb{N}$. For this, we consider all sums $\sum_{n=0}^{\infty} \delta_n r^n$ with $\delta_n \in \{0, 1\}$, but $\delta_n = 0$ from some n on. By our hypotheses on r, all these finite sums are distinct. Therefore, we may order them following their size as

$$0 = r_0 < r_1 < \ldots < r_k < \ldots \to \infty,$$

and we finally get

$$\prod_{n=1}^{\infty} (1 + p^{r^n}) - 1 = \sum_{k=1}^{\infty} p^{r_k}.$$

Clearly, for each $N \in \mathbb{N}$, there exists exactly one $k_n \in \mathbb{N}$ for which $r_{k_N} = r^N$ holds. Furthermore, no r_k with $k < k_N$ can contain an r^n with $n \geq N$ with a coefficient $\delta_n = 1$.

REMARK 2. The special infinite products considered in the preceding remark arise, at least formally, from Mahler type functional equations as discussed thoroughly in the classical complex case in Nishioka's monograph [5]. Namely, if $F(z)$ denotes the infinite product $\prod_{n=0}^{\infty}(1 + z^{r^n})$, then we have $F(z) = (1 + z)F(z^r)$.

5. Proof of Theorem 2. Again we proceed by induction on m. In the Proposition from Section 2, we have already proved (a little more than) the case $m = 1$ of Theorem 2. Suppose $m > 1$, and assume that Theorem 2 is proved for any subset $\{\alpha_1, \ldots, \widehat{\alpha}_\mu, \ldots, \alpha_m\}$ of $\{\alpha_1, \ldots, \alpha_m\}$. Suppose that our assertion is false for the m points $\alpha_1, \ldots, \alpha_m$, i.e. that the $l \cdot m$ numbers $f_\lambda(\alpha_\mu)$ ($\lambda = 1, \ldots, l$, $\mu = 1, \ldots, m$) are algebraically dependent over $\mathbb{Q}_p$. Let the non-constant polynomial

$$P \in \mathbb{Z}_p[X_{1,1}, \ldots, X_{1,m}; \ldots; X_{l,1}, \ldots, X_{l,m}] \quad (=: \mathbb{Z}_p[\underline{X}], \text{ for short}) \tag{24}$$

be such that

$$P(\underline{\gamma}) := P(\gamma_{1,1}, \ldots, \gamma_{1,m}; \ldots; \gamma_{l,1}, \ldots, \gamma_{l,m}) = 0, \tag{25}$$

where $\gamma_{\lambda,\mu} := f_\lambda(\alpha_\mu)$. Clearly, no l-tuple $(X_{1,\mu}, \ldots, X_{l,\mu})$ of variables can be missing in (24), by our induction hypothesis.

From (24) and (25), we find

$$P(\underline{X}) = \sum_{\mu=1}^{m}\sum_{\lambda=1}^{l} \frac{\partial P}{\partial X_{\lambda,\mu}}(\underline{\gamma})(X_{\lambda,\mu} - \gamma_{\lambda,\mu}) + P^*(\underline{X} - \underline{\gamma}), \tag{26}$$

where all monomials in the $l \cdot m$ differences $X_{\lambda,\mu} - \gamma_{\lambda,\mu}$ entering into P^* have total degree at least 2 and coefficients from $\mathbb{C}_p$ with non-negative p-order.

Now, let $\alpha_\mu^{(n)}$ and $A_\mu^{(n)}$ be defined as in (9), and

$$\gamma_{\lambda,\mu}^{(n)} := f_\lambda(\alpha_\mu^{(n)}).$$

We want to substitute $\gamma_{\lambda,\mu}^{(n)}$ for $X_{\lambda,\mu}$ in (26). To get on after that, we first calculate

$$\gamma_{\lambda,\mu}^{(n)} - \gamma_{\lambda,\mu} = \sum_{i=1}^{\infty} \frac{f_\lambda^{(i)}(\alpha_\mu)}{i!}\,(A_\mu^{(n)})^i = f'_\lambda(\alpha_\mu)A_\mu^{(n)} + \sum_{i\ge 2}\cdots \tag{27}$$

Allowing here that n depends on μ (we therefore write n_μ instead of n), we find from (26) and (27) that

$$\begin{aligned} &P(\gamma_{1,1}^{(n_1)}, \ldots, \gamma_{1,m}^{(n_m)}; \ldots; \gamma_{l,1}^{(n_1)}, \ldots, \gamma_{l,m}^{(n_m)}) \\ &= \sum_{\mu=1}^{m}\sum_{\lambda=1}^{l} f'_\lambda(\alpha_\mu)\,\frac{\partial P}{\partial X_{\lambda,\mu}}(\underline{\gamma})A_\mu^{(n_\mu)} \\ &\quad + \sum_{\mu}\sum_{\lambda} \frac{\partial P}{\partial X_{\lambda,\mu}}(\underline{\gamma})\sum_{i\ge 2}\frac{f_\lambda^{(i)}(\alpha_\mu)}{i!}(A_\mu^{(n_\mu)})^i \\ &\quad + P^*(\gamma_{1,1}^{(n_1)} - \gamma_{1,1}, \ldots, \gamma_{1,m}^{(n_m)} - \gamma_{1,m}; \ldots; \gamma_{l,1}^{(n_1)} - \gamma_{l,1}, \ldots, \gamma_{l,m}^{(n_m)} - \gamma_{l,m}). \end{aligned} \tag{28}$$

At this moment, we need the following intermediate but crucial

LEMMA 5. *For $\mu = 1, \ldots, m$, the sum*

$$B_\mu^* := \sum_{\lambda=1}^{l} f'_\lambda(\alpha_\mu)\,\frac{\partial P}{\partial X_{\lambda,\mu}}(\underline{\gamma})$$

does not vanish.

To start with its *proof*, we consider the polynomial

$$\begin{aligned} &Q_\mu(X_{1,\mu}, \ldots, X_{l,\mu}) \\ &\qquad := P(\gamma_{1,1}, \ldots, X_{1,\mu}, \ldots, \gamma_{1,m}; \ldots; \gamma_{l,1}, \ldots, X_{l,\mu}, \ldots, \gamma_{l,m}), \end{aligned} \tag{29}$$

where $X_{\lambda,\mu}$ replaces $\gamma_{\lambda,\mu}$ for $\lambda = 1, \ldots, l$ on the left-hand side of (25). Of course, by what we have noted after (25), $Q_\mu(X_{1,\mu}, \ldots, X_{l,\mu})$ is a non-constant polynomial with coefficients from

$$\mathbb{Z}_p[\gamma_{1,1}, \ldots, \widehat{\gamma}_{1,\mu}, \ldots, \gamma_{1,m}; \ldots; \gamma_{l,1}, \ldots, \widehat{\gamma}_{l,\mu}, \ldots, \gamma_{l,m}].$$

Since the functions $f_1, \ldots, f_l$ are algebraically independent over $\mathbb{Q}_p$ by hypothesis, and thus over $\mathbb{C}_p$ also (compare Remark 3 after Theorem 2), each function

$$\varphi_\mu(z) := Q_\mu(f_1(z), \ldots, f_l(z)) \quad (\mu = 1, \ldots, m) \tag{30}$$

is non-constant. From this and (29), we get

$$\varphi'_\mu(\alpha_\mu) = \sum_{\lambda=1}^{l} f'_\lambda(\alpha_\mu) \, \frac{\partial Q_\mu}{\partial X_{\lambda,\mu}}(\gamma_{1,\mu}, \ldots, \gamma_{l,\mu}) = B^*_\mu. \tag{31}$$

On the other hand, one can easily rearrange $\varphi_\mu(z)$ from (30) as a power series as they appear in Lemma 3; then Lemma 4 gives us $\varphi'_\mu(\alpha_\mu) \neq 0$ for $\mu = 1, \ldots, m$, and therefore, by (31), the assertion of Lemma 5.

We are now in a position to *continue our proof of Theorem 2*. Since $B^*_\mu \neq 0$ for $\mu = 1, \ldots, m$, by Lemma 5, we may define $b^*_\mu := \operatorname{ord}_p B^*_\mu$ and order them in such a way that

$$b^*_1 \geq \ldots \geq b^*_m.$$

Again each b^*_μ is a finite linear combination (over $\mathbb{N}_0$) of 1 and all $r_{k,\nu}$. For any $\mu = 1, \ldots, m$, we fix such a linear combination for b^*_μ, and proceed from here on exactly as in the corresponding passage of the proof of Theorem 1, except that we have to replace the b's in (14) and (16) by the b^*'s. If our new $n_1, \ldots, n_m$ are large enough, we deduce

$$\operatorname{ord}_p\Big(\sum_{\mu=1}^{m} B^*_\mu A^{(n_\mu)}_\mu\Big) = b^*_1 + r_{n_1+1,1} \tag{32}$$

replacing formula (18). The sum in (32) is nothing else than the first double sum on the right-hand side of (28). From here on, we get a contradiction along the same lines as before.

6. Two more applications of Theorem 2. Here we discuss first hypergeometric series and then a q-analogue of Corollary 2. But before entering a little more into the details, let us describe in short a general principle for the search of such applications, which we used already in the proof of Corollary 2.

Suppose we are given power series

$$f_\lambda(z) := \sum_{j=0}^{\infty} c_{j,\lambda} z^j \quad (\lambda = 1, \ldots, l)$$

from $\mathbb{Q}[[z]]$, say, having positive radii of convergence R_λ and $R_{p,\lambda}$ in $\mathbb{C}$ and $\mathbb{C}_p$, respectively. If we have any method to prove the algebraic independence of the functions

$$z, f_1(z), \dots, f_l(z) \tag{33}$$

over $\mathbb{C}$ (or equivalently the algebraic independence of $f_1(z), \dots, f_l(z)$ over the rational function field $\mathbb{C}(z)$), then the functions (33) are also algebraically independent over $\mathbb{Q}$; see again Remark 3 after Theorem 2. But this implies their algebraic independence over $\mathbb{Q}_p$ (or over $\mathbb{C}_p$) as well, and we can conclude from Theorem 2 that the $(l+1) \cdot m$ elements

$$\alpha_\mu, f_1(\alpha_\mu), \dots, f_l(\alpha_\mu) \quad (\mu = 1, \dots, m)$$

from $\mathbb{C}_p$ are algebraically independent over $\mathbb{Q}_p$ if the α's satisfy the conditions of Theorem 1.

Hypergeometric series. We consider generalized hypergeometric series

$$\sum_{j=0}^{\infty} \frac{(\kappa_1)_j \dots (\kappa_u)_j}{(\lambda_1)_j \dots (\lambda_v)_j} z^j, \tag{34}$$

where $(X)_j := X(X+1)\dots(X+j-1)$, $j \in \mathbb{N}$, denotes the usual Pochhammer symbol, $(X)_0 := 1$. If $v > u$, and all κ's and λ's are rational, these series can be made Siegel E-functions by a change of variable. Such functions are considered in the Siegel–Shidlovskii theory (compare, e.g., [7]), and their algebraic independence over $\mathbb{C}(z)$ is intensively studied within the scope of this theory. Very precise conditions on the parameters κ and λ such that functions of type (34) are algebraically independent over $\mathbb{C}(z)$ can be found in the literature. Concerning this topic, we refer the reader to Salikhov [6] but we also mention the paper [1] of Beukers, Brownawell and Heckman.

A q-analogue of Corollary 1. It is explained in [2] in which sense we may consider the entire transcendental function

$$E_q(z) := \prod_{n=1}^{\infty} \left(1 - \frac{z}{q^n}\right) = \sum_{j=0}^{\infty} \frac{z^j}{(1-q)\dots(1-q^j)} \tag{35}$$

as a q-analogue of the classical exponential function, supposing $q \in \mathbb{C}$, $|q| > 1$. Further, we may consider the meromorphic function

$$L_q(z) := \sum_{n=1}^{\infty} \frac{z}{q^n - z} \tag{36}$$

as a q-analogue of the complex logarithm. Namely, we easily see from (36), expanding $(q^n - z)^{-1}$ into a power series about $z = 0$, that

$$L_q(z) = \sum_{j=1}^{\infty} \frac{z^j}{q^j - 1} \tag{37}$$

in $|z| < |q|$, and therefore $(q-1)L_q(z) = \sum z^j/(q^{j-1} + \ldots + 1)$, which tends, at least formally, to $\sum z^j/j = -\log(1-z)$ as $q \to 1$. As is obvious from (35) and (36), the connection between the functions E_q and L_q is

$$\frac{E_q'(z)}{E_q(z)} = -\frac{L_q(z)}{z}. \tag{38}$$

Now we assert that, for fixed q as above, the three functions

$$z, E_q(z), L_q(z) \tag{39}$$

are algebraically independent over $\mathbb{C}$, or even over $\mathbb{Q}(q)$, since the series in (35) and (37) have their coefficients in that field. Suppose, to the contrary, that the functions (39) are algebraically dependent over $\mathbb{C}$. Then $z, E_q(z), E_q'(z)$ would be algebraically dependent as well, by (38). In other words, $E_q(z)$ would satisfy an algebraic differential equation of the first order. But then, following a result attributed by Valiron [8], [9] to Wiman, the function E_q would have growth order $\varrho(E_q) \in \mathbb{Q}_+$. On the other hand, it is well known (compare, e.g., [2] or [8]) that E_q has $\varrho(E_q) = 0$. For his convenience we remind the reader that the growth order $\varrho(f)$ of an entire function f is defined by $\limsup_{r\to\infty} (\log\log|f|_r)/(\log r)$, where $|f|_r$ denotes the maximum of $|f(z)|$ on $|z| = r$.

Choosing now $q \in \mathbb{Q}\backslash\mathbb{Z}$, $|q| > 1$, we may select a prime p with $\operatorname{ord}_p q < 0$. Then the product and the series in (35) define the same entire function in $\mathbb{C}_p$, which we denote by $E_{q,p}(z)$. The series in (37), converging for $z \in \mathbb{C}_p$, $|z|_p < |q|_p$, may be called $L_{q,p}(z)$. Then our above considerations on the functions (39) give the algebraic independence of their p-adic analogues

$$z, E_{q,p}(z), L_{q,p}(z),$$

and we can deduce from Theorem 2 a q-analogue of Corollary 2.

Acknowledgements. The authors thank the referee for careful reading of the manuscript.

References

[1] F. Beukers, W. D. Brownawell and G. Heckman, *Siegel normality*, Ann. of Math. (2) 127 (1988), 279–308.

[2] P. Bundschuh, *Arithmetic properties of the solutions of certain functional equations*, in: Number Theory (Turku, 1999), de Gruyter, 2001, 25–42.

[3] P. Bundschuh and V. G. Chirskii, *Algebraic independence of elements from $\mathbb{C}_p$ over $\mathbb{Q}_p$, I*, Arch. Math. (Basel) 79 (2002), 345–352.

[4] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, 2nd ed., Springer, 1984.

[5] K. Nishioka, *Mahler Functions and Transcendence*, Lecture Notes in Math. 1631, Springer, 1996.

[6] V. Kh. Salikhov, *Algebraic independence of values of hypergeometric E-functions*, Dokl. Akad. Nauk SSSR 307 (1989), 284–287 (in Russian); English transl.: Soviet Math. Dokl. 40 (1990), 71–74.
[7] A. B. Shidlovskii, *Transcendental Numbers*, de Gruyter, 1989.
[8] G. Valiron, *Lectures on the General Theory of Integral Functions*, Chelsea, New York, 1949.
[9] —, *Fonctions entières d'ordre fini et fonctions méromorphes*, Monogr. Enseign. Math. 8, Inst. Math. Univ. Genève, 1960.

Mathematisches Institut
Universität zu Köln
Weyertal 86-90
50931 Köln, Germany
E-mail: pb@mi.uni-koeln.de

Mech.-Math. Faculty
Moscow State University
Vorob'evy Hills
119899 Moscow, Russia
E-mail: chirskii@mech.math.msu.su

Received on 25.11.2002
and in revised form on 27.10.2003 (4414)