JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Peter BUNDSCHUH et Kumiko NISHIOKA

Algebraic independence over $\mathbb{Q}_p$

Tome 16, n° 3 (2004), p. 519-533.

<http://jtnb.cedram.org/item?id=JTNB_2004__16_3_519_0>

Journal de Théorie des Nombres
de Bordeaux **16** (2004), 519–533

Algebraic independence over $\mathbb{Q}_p$

par Peter BUNDSCHUH et Kumiko NISHIOKA

Résumé. Soit $f(x)$ une série entière $\sum_{n\geq 1}\zeta(n)x^{e(n)}$, où $(e(n))$ est une suite récurrente linéaire d'entiers naturels, strictement croissante, et $(\zeta(n))$ une suite de racines de l'unité dans $\overline{\mathbb{Q}}_p$, qui satisfait à une hypothèse technique convenable. Alors nous nous sommes particulièrement intéressés à caractériser l'indépendance algébrique sur $\mathbb{Q}_p$ des éléments $f(\alpha_1),\dots,f(\alpha_t)$ de $\mathbb{C}_p$ en fonction des $\alpha_1,\dots,\alpha_t\in\mathbb{Q}_p$, deux à deux distincts, avec $0<|\alpha_\tau|_p<1$ pour $\tau=1,\dots,t$. Une application remarquable de notre résultat principal dit que, dans le cas $e(n)=n$, l'ensemble $\{f(\alpha)|\,\alpha\in\mathbb{Q}_p,\,0<|\alpha|_p<1\}$ est algébriquement indépendant sur $\mathbb{Q}_p$, si $(\zeta(n))$ satisfait à "l'hypothèse technique". Nous terminerons par une conjecture portant sur des suites $(e(n))$ plus générales.

Abstract. Let $f(x)$ be a power series $\sum_{n\geq 1}\zeta(n)x^{e(n)}$, where $(e(n))$ is a strictly increasing linear recurrence sequence of non-negative integers, and $(\zeta(n))$ a sequence of roots of unity in $\overline{\mathbb{Q}}_p$ satisfying an appropriate technical condition. Then we are mainly interested in characterizing the algebraic independence over $\mathbb{Q}_p$ of the elements $f(\alpha_1),\dots,f(\alpha_t)$ from $\mathbb{C}_p$ in terms of the distinct $\alpha_1,\dots,\alpha_t\in\mathbb{Q}_p$ satisfying $0<|\alpha_\tau|_p<1$ for $\tau=1,\dots,t$. A striking application of our basic result says that, in the case $e(n)=n$, the set $\{f(\alpha)|\,\alpha\in\mathbb{Q}_p,\,0<|\alpha|_p<1\}$ is algebraically independent over $\mathbb{Q}_p$ if $(\zeta(n))$ satisfies the "technical condition". We close with a conjecture concerning more general sequences $(e(n))$.

1. Introduction and results

Let p be a fixed prime, $\mathbb{Q}_p$ be the p-adic completion of $\mathbb{Q}$, let $\overline{\mathbb{Q}}_p$ be the algebraic closure of $\mathbb{Q}_p$, and $\mathbb{C}_p$ be the p-adic completion of $\overline{\mathbb{Q}}_p$, which is an algebraically closed complete field with a valuation uniquely extended from $\mathbb{Q}_p$.

Manuscrit reçu le 21 mars 2003.
This work was done during the second-named author's stay at the University of Cologne supported by the Alexander von Humboldt Foundation. Both authors are very grateful to the foundation for giving them the opportunity for collaboration.

The question of transcendence or algebraic independence of elements from $\mathbb{Q}_p$ or even from $\mathbb{C}_p$ over $\mathbb{Q}$ is rather well investigated in the literature. In contrast to this situation, the corresponding question for $\mathbb{C}_p$ over $\mathbb{Q}_p$ has been studied in the past only occasionally. Seemingly, the first sufficient criterion (of Liouville–type) for transcendence was stated implicitly by Amice [1, p.74] as an exercise. Concerning algebraic independence, there is a first article by Lampert [8], who used p-adic series of the form

$$\sum a_k\, p^{r_k} \tag{1}$$

with infinite sequences (r_k) of positive non-integral rational numbers to answer two questions of Koblitz [6, p.75] about the transcendence degrees of $\mathbb{C}_p$ over $\mathbb{C}_p^{unr}$ and of $\mathbb{C}_p^{unr}$ over $\mathbb{Q}_p$. Here $\mathbb{C}_p^{unr}$ denotes the p-adic closure of $\mathbb{Q}_p^{unr}$ in $\mathbb{C}_p$, where $\mathbb{Q}_p^{unr}$ is the maximal unramified extension field of $\mathbb{Q}_p$. A few years later, Nishioka [9], based on an approximation type criterion for algebraic independence, gave more explicit examples for algebraically independent elements from $\mathbb{C}_p$ over $\mathbb{C}_p^{unr}$ (and from $\mathbb{C}_p^{unr}$ over $\mathbb{Q}_p$ as well) than Lampert did.

Whereas the a_k in Lampert's series (1) were certain roots of unity in $\mathbb{C}_p$, the first-named author and Chirskii [2], [3] very recently proved a variety of results giving sufficient conditions for the algebraic independence over $\mathbb{Q}_p$ of numbers from $\mathbb{C}_p$, again defined by infinite series of type (1), but now with coefficients from the ring $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \,|\, |x|_p \le 1\}$ of p-adic integers.

In the present paper, we will be mainly interested in the algebraic independence of $f(\alpha_1), \ldots, f(\alpha_t)$ over $\mathbb{Q}_p$, where $\alpha_1, \ldots, \alpha_t \in \mathbb{Q}_p^\times := \mathbb{Q}_p \setminus \{0\}$ and $f(x)$ is a power series

$$\sum_{n=1}^{\infty} \zeta(n) x^{e(n)} \in \overline{\mathbb{Q}}_p[[x]] \tag{2}$$

with a strictly increasing sequence $(e(n))_{n=1,2,\ldots}$ of non-negative integers. Our motivation to consider series of type (2) originates from Gouvêa's book [4, p.165], where the transcendence of $\Sigma_{n\ge1}\zeta(n)p^n$ over $\mathbb{Q}_p$ is proved under assumptions which are much stronger than our's will be in the sequel.

Before writing down the precise statement of our principal result, it is useful to give the

Definition. A finite subset $\{\alpha_1, \ldots, \alpha_t\}$ of $\mathbb{C}_p^\times := \mathbb{C}_p \setminus \{0\}$ is called $(e(n))$-*dependent* if there exist $\alpha \in \mathbb{C}_p^\times$, roots of unity $\zeta_1, \ldots, \zeta_t$, and numbers $\delta_1, \ldots, \delta_t \in \mathbb{C}_p^\times$ such that the following conditions hold:

(i) $\alpha_\tau = \zeta_\tau \alpha$ for $\tau = 1, \ldots, t$,

(ii) $\sum\limits_{\tau=1}^{t} \delta_\tau\, \zeta_\tau^{e(n)} = 0$ for any large n.

We are now in a position to formulate our main result.

Theorem 1. *Let $(e(n))_{n=1,2,\ldots}$ be a strictly increasing sequence of non-negative integers forming a linear recurrence. Assume $(\zeta(n))_{n=1,2,\ldots}$ to be a sequence of roots of unity, whose orders are all prime to p, satisfying $\zeta(n) \notin \mathbb{Q}_p(\zeta(1), \ldots, \zeta(n-1))$ for any large $n \in \mathbb{N} := \{1, 2, \ldots\}$. Put*

$$f(x) := \sum_{n=1}^{\infty} \zeta(n) x^{e(n)}, \tag{3}$$

and let $\alpha_1, \ldots, \alpha_t \in \mathbb{Q}_p^{\times}$ be distinct with $|\alpha_\tau|_p < 1$ for $\tau = 1, \ldots, t$. Then $f(\alpha_1), \ldots, f(\alpha_t)$ are algebraically dependent [1] if and only if there exists a non-empty subset of $\{\alpha_1, \ldots, \alpha_t\}$ which is $(e(n))$-dependent.

Remark 1. An example of a ζ-sequence as in Theorem 1 is the following. Let ℓ be a prime $\neq p$, and let $\zeta(n)$ be a primitive ℓ^n-th root of unity for any $n \in \mathbb{N}$.

Since, by a Vandermonde argument, no non-empty finite subset of $\mathbb{C}_p^{\times}$ can be (n)-dependent, the case $e(n) = n$ yields our first application.

Corollary 1. *Let $(\zeta(n))$ be as in Theorem 1, and define*

$$f(x) := \sum_{n=1}^{\infty} \zeta(n) x^n.$$

Then the set $\{f(\alpha) | \alpha \in \mathbb{Q}_p^{\times}, |\alpha|_p < 1\}$ is algebraically independent.

Corollary 2. *Let $(\zeta(n))$ be as in Theorem 1, and define*

$$f_d(x) := \sum_{n=1}^{\infty} \zeta(n) x^{d^n}$$

for fixed $d \in \mathbb{N} \setminus \{1\}$. Suppose $\alpha_1, \ldots, \alpha_t \in \mathbb{Q}_p^{\times}$ to be distinct with $|\alpha_\tau|_p < 1$ for $\tau = 1, \ldots, t$. Then $f_d(\alpha_1), \ldots, f_d(\alpha_t)$ are algebraically dependent if and only if there exists a non-empty (d^n)-dependent subset of $\{\alpha_1, \ldots, \alpha_t\}$.

With regard to Corollary 2 we can even go one step further by allowing d to vary over $\mathbb{N} \setminus \{1\}$. The corresponding result, which we state as Theorem 2, is not a direct consequence of Theorem 1, but its proof is rather similar.

Theorem 2. *Assume $(\zeta(n))$ to be as in Theorem 1, and $f_d(x)$ as in Corollary 2. Suppose $\alpha_1, \ldots, \alpha_t \in \mathbb{Q}_p^{\times}$ to be distinct with $|\alpha_\tau|_p < 1$ for $\tau = 1, \ldots, t$. Then the set $\{f_d(\alpha_\tau) | d \in \mathbb{N} \setminus \{1\}, \tau = 1, \ldots, t\}$ is algebraically dependent if and only if there exist a $d_0 \in \mathbb{N} \setminus \{1\}$ and a non-empty subset of $\{\alpha_1, \ldots, \alpha_t\}$ which is (d_0^n)-dependent.*

An immediate consequence of Theorem 2 is

[1] In our paper "algebraically dependent or independent" means *always* "over $\mathbb{Q}_p$".

Corollary 3. *Suppose that no $\alpha_\tau/\alpha_{\tau'}$ $(1 \le \tau < \tau' \le t)$ is a root of unity. Then the set $\{f_d(\alpha_\tau) | d \in \mathbb{N} \setminus \{1\}, \tau = 1, \dots, t\}$ is algebraically independent.*

To conclude this introduction we propose the following

Conjecture. *Let $(e(n))_{n\in\mathbb{N}}$ be a strictly increasing sequence of non-negative integers, and let $(\zeta(n))_{n\in\mathbb{N}}$ be as in Theorem 1. Suppose f to be defined by (3), and let $\alpha_1, \dots, \alpha_t \in \mathbb{Q}_p^\times$ be distinct with $|\alpha_\tau|_p < 1$ for $\tau = 1, \dots, t$. Then $f(\alpha_1), \dots, f(\alpha_t)$ are algebraically dependent if and only if there exists a non-empty $(e(n))$-dependent subset of $\{\alpha_1, \dots, \alpha_t\}$.*

2. Theorem 1: The if-part and preparation of the only-if-part

Let $\{\alpha_1, \dots, \alpha_{t'}\}$ be an $(e(n))$-dependent subset of $\{\alpha_1, \dots, \alpha_t\} \subset \mathbb{Q}_p^\times$. By definition, there exist $\alpha \in \mathbb{C}_p^\times$, roots of unity $\zeta_1, \dots, \zeta_{t'}$, and numbers $\delta_1, \dots, \delta_{t'} \in \mathbb{C}_p^\times$ such that

(i) $\alpha_\tau = \zeta_\tau \alpha \quad (\tau = 1, \dots, t')$,

(ii) $\sum_{\tau=1}^{t'} \delta_\tau \zeta_\tau^{e(n)} = 0 \quad (n > n_0)$.

From (i) we see $\alpha \in \overline{\mathbb{Q}}_p^\times$, and from (ii) we may suppose $\delta_1, \dots, \delta_{t'} \in \overline{\mathbb{Q}}_p$, not all zero, compare the argument in [11, p.83].

To prove now the if-part, let $\alpha_1, \dots, \alpha_t$ satisfy the hypotheses of our Theorem 1, and let $\{\alpha_1, \dots, \alpha_{t'}\}$ be an $(e(n))$-dependent subset of $\{\alpha_1, \dots, \alpha_t\}$. Then, using (i) and (ii), we find

$$\sum_{\tau=1}^{t'} \delta_\tau f(\alpha_\tau) = \sum_{n=1}^{\infty} \zeta(n) \sum_{\tau=1}^{t'} \delta_\tau \alpha_\tau^{e(n)} = \sum_{n=1}^{\infty} \zeta(n) \alpha^{e(n)} \sum_{\tau=1}^{t'} \delta_\tau \zeta_\tau^{e(n)}$$
$$= \sum_{n=1}^{n_0} \zeta(n) \alpha^{e(n)} \sum_{\tau=1}^{t'} \delta_\tau \zeta_\tau^{e(n)}$$

with $\delta_1, \dots, \delta_{t'} \in \overline{\mathbb{Q}}_p$, not all zero. This last equation shows that $1, f(\alpha_1), \dots f(\alpha_{t'})$ are *linearly* dependent over $\overline{\mathbb{Q}}_p$, and the algebraic dependence of $f(\alpha_1), \dots, f(\alpha_{t'})$ (over $\mathbb{Q}_p$) follows. Clearly, this reasoning is independent of the fact that $(e(n))$ is a recurrence sequence.

To begin with the only-if-part, we suppose $f(\alpha_1), \dots, f(\alpha_t)$ to be algebraically dependent whereas, w.l.o.g., every $t-1$ of these numbers are algebraically independent. Then there exists a polynomial $F \in \mathbb{Z}_p[x_1, \dots, x_t] \setminus \{0\}$ with minimal total degree such that

$$F(f(\alpha_1), \dots, f(\alpha_t)) = 0. \tag{4}$$

Clearly, with $D_\tau = \partial/\partial x_\tau$, we have

$$D_\tau F(f(\alpha_1), \dots, f(\alpha_t)) \neq 0 \quad \text{for} \quad \tau = 1, \dots, t. \tag{5}$$

Assuming

$$0 < |\alpha_1|_p \le \cdots \le |\alpha_s|_p < |\alpha_{s+1}|_p = \cdots = |\alpha_t|_p < 1, \tag{6}$$

and defining

$$\beta_{\tau,k} := \sum_{n=1}^{k-1} \zeta(n)\alpha_\tau^{e(n)} \quad (k \in \mathbb{N}) \tag{7}$$

we have, with $\underline{f(\alpha)} := (f(\alpha_1), \dots, f(\alpha_t))$ and $\underline{\beta}_k := (\beta_{1,k}, \dots, \beta_{t,k})$,

$$\begin{aligned} F(\underline{f(\alpha)}) &= F(\underline{\beta}_k) + \Big(\sum_{\tau=1}^{s} + \sum_{\tau=s+1}^{t}\Big) D_\tau F(\underline{\beta}_k)(f(\alpha_\tau) - \beta_{\tau,k}) \\ &\quad + \sum_{\tau,\tau'=1}^{t} D_\tau D_{\tau'} F(\underline{\beta}_k)(f(\alpha_\tau) - \beta_{\tau,k})(f(\alpha_{\tau'}) - \beta_{\tau',k}) + \cdots \end{aligned} \tag{8}$$

From (7) we see $|\beta_{\tau,k}|_p \le 1$ and

$$|f(\alpha_\tau) - \beta_{\tau,k}|_p = \Big|\sum_{n=k}^{\infty} \zeta(n)\alpha_\tau^{e(n)}\Big|_p = |\alpha_\tau|_p^{e(k)}$$

for $\tau = 1, \dots, t$ and any $k \in \mathbb{N}$. Using this and (4) we deduce from (8)

$$F(\underline{\beta}_k) + \sum_{\tau=s+1}^{t} D_\tau F(\underline{\beta}_k) \sum_{n \ge k} \zeta(n)\alpha_\tau^{e(n)} = O(|\alpha_s|_p^{e(k)}) + O(|\alpha_t|_p^{2e(k)}). \tag{9}$$

With $K_k := \mathbb{Q}_p(\zeta(1), \dots, \zeta(k))$ for every large $k \in \mathbb{N}$, let $\sigma(k) \in \mathrm{Gal}(K_k | K_{k-1}), \sigma(k) \ne \mathrm{id}$. As we shall explain in Remark 2 below, we can extend $\sigma(k)$ to an isometric automorphism of $\mathbb{C}_p$ over $\mathbb{Q}_p$, and therefore we find from (9)

$$\begin{aligned} F(\underline{\beta}_k) + \sum_{\tau=s+1}^{t} D_\tau F(\underline{\beta}_k) \sum_{n \ge k} \zeta(n)^{\sigma(k)}\alpha_\tau^{e(n)} \\ = O(|\alpha_s|_p^{e(k)}) + O(|\alpha_t|_p^{2e(k)}). \end{aligned} \tag{10}$$

Subtracting (9) from (10) we get

$$\sum_{n \ge k} (\zeta(n)^{\sigma(k)} - \zeta(n)) \sum_{\tau=s+1}^{t} D_\tau F(\underline{\beta}_k)\alpha_\tau^{e(n)} = O(|\alpha_s|_p^{e(k)}) + O(|\alpha_t|_p^{2e(k)}).$$

Since $D_\tau F(\underline{\beta}_k) = D_\tau F(\underline{f(\alpha)}) + O(|\alpha_t|_p^{e(k)})$, the last line can be equivalently written as

$$\sum_{n\ge k}(\zeta(n)^{\sigma(k)}-\zeta(n))\Big(\sum_{\tau=s+1}^{t} D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{e(n)}\Big)\alpha_t^{e(n)-e(k)} = O\left(\Big|\frac{\alpha_s}{\alpha_t}\Big|_p^{e(k)}\right)+O(|\alpha_t|_p^{e(k)}). \tag{11}$$

We put

$$M(k) := \max_{n\ge k}\Big|\sum_{\tau=s+1}^{t} D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{e(n)}\Big|_p; \tag{12}$$

this maximum exists because of the discreteness of $|\cdot|_p$ on $\mathbb{C}_p^{unr}$. If $M(k)=0$, then

$$\sum_{\tau=s+1}^{t} D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{e(n)} = 0 \quad \text{for any} \quad n\ge k.$$

Assume $M(k)>0$, and let $k'\ge k$ be such that

$$M(k) = \Big|\sum_{\tau=s+1}^{t} D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{e(k')}\Big|_p. \tag{13}$$

Then, for any $n>k'$, we have

$$\Big|\Big(\sum_{\tau=s+1}^{t} D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{e(n)}\Big)\alpha_t^{e(n)-e(k')}\Big|_p < M(k).$$

Replacing in (11) k by k', and taking $|\zeta(k')^{\sigma(k')}-\zeta(k')|_p=1$ into account, we get

$$\begin{aligned}\Big|\sum_{\tau=s+1}^{t} D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{e(k')}\Big|_p &= \Big|\sum_{n\ge k'}(\zeta(n)^{\sigma(k')}-\zeta(n))\Big(\sum_{\tau=s+1}^{t} D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{e(n)}\Big)\alpha_t^{e(n)-e(k')}\Big|_p\\ &= O\left(\Big|\frac{\alpha_s}{\alpha_t}\Big|_p^{e(k')}\right)+O(|\alpha_t|_p^{e(k')}).\end{aligned}$$

Combining this with (13) we find, by $|\alpha_s/\alpha_t|_p,\ |\alpha_t|_p<1$,

$$M(k) = O(\vartheta^{e(k)}) \tag{14}$$

with $0<\vartheta := \max(|\frac{\alpha_s}{\alpha_t}|_p,\ |\alpha_t|_p)<1$. By (14) we have, in particular,

$$\lim_{k\to\infty} M(k) = 0. \tag{15}$$

Clearly, (14) and (15) hold both in the anticipated case $M(k) = 0$ as well.

Remark 2. Writing σ for the above $\sigma(k)$, we let σ be an automorphism of $\overline{\mathbb{Q}}_p$ over $\mathbb{Q}_p$. For each $x \in \overline{\mathbb{Q}}_p$, we define $|x|^* := |x^\sigma|_p$. Then $|\cdot|^*$ is an absolute value on $\overline{\mathbb{Q}}_p$ coinciding on $\mathbb{Q}_p$ with $|\cdot|_p$. Hence $|\cdot|^* = |\cdot|_p$, and thus $|x^\sigma|_p = |x|_p$ for any $x \in \overline{\mathbb{Q}}_p$.

In the above deduction of (10) from (9), we first extend $\sigma \in \mathrm{Gal}(K_k|K_{k-1})$ to $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$. Then σ is isometric, and it can be further extended to an isometric automorphism of $\mathbb{C}_p$ over $\mathbb{Q}_p$.

To finish the proof of the only-if-part of our Theorem 1 we need the following lemma concerning the quotients α_τ/α_t $(\tau = s+1, \ldots, t)$ from $\mathbb{Q}_p$ of p-adic value 1, compare (6).

Lemma 1. *Denoting $q := p$ for $p > 2$, and $q := 4$ for $p = 2$ there exist distinct $\gamma_1, \ldots, \gamma_m \in 1 + q\mathbb{Z}_p$, and $\varphi(q)$-th roots of unity $\zeta_{s+1}, \ldots, \zeta_t$ such that the representations*

$$\frac{\alpha_\tau}{\alpha_t} \;=\; \zeta_\tau \gamma_{\mu(\tau)} \quad (\tau = s+1, \ldots, t)$$

hold with appropriate $\mu(\tau) \in \{1, \ldots, m\}$.

The *proof* follows immediately from [4, Corollary 4.3.8]. Clearly, no quotient $\gamma_\mu/\gamma_{\mu'}$ $(\mu \neq \mu')$ can be a root of unity.

3. A pedagogical example

Before concluding the proof of Theorem 1 in section 4 in the general situation of linear recurrence sequences $(e(n))$, we treat, for pedagogical reasons, first the particular case $e(\cdot) = g(\cdot)$ with $g \in \mathbb{Z}[x]$. To do this we need

Lemma 2. *Suppose $G \in \mathbb{Z}[x]$ such that $(G(\nu))_{\nu\in\mathbb{N}}$ is a strictly increasing sequence of non-negative integers. Let $\gamma_1, \ldots, \gamma_m$ be as in Lemma 1, and assume $\delta_1, \ldots, \delta_m \in \mathbb{C}_p$, not all zero. Then*

$$\limsup_{\nu\to\infty} \Big| \sum_{\mu=1}^{m} \delta_\mu \gamma_\mu^{G(\nu)} \Big|_p \;>\; 0.$$

Proof. W.l.o.g. we may assume $|\delta_\mu|_p \leq 1$ for $\mu = 1, \ldots, m$. Then the Skolem-Lech-Mahler theorem (for relatively simple proofs compare, e.g., [5], or [10, Theorem 2.5.3]) implies that there are at most finitely many $k \in \mathbb{N}_0$ with $\sum_{\mu=1}^m \delta_\mu \gamma_\mu^k = 0$, since no quotient $\gamma_\mu/\gamma_{\mu'}$ $(\mu \neq \mu')$ is a root of unity. Thus, by our hypothesis on G, there exists $\nu_0 \in \mathbb{N}$ such that

$$\sum_{\mu=1}^{m} \delta_\mu \gamma_\mu^{G(\nu_0)} \;\neq\; 0,$$

and this sum has p-adic value p^{-v} with rational $v \geq 0$. Defining $M := [v] \in \mathbb{N}_0$ we see $\gamma_\mu^{p^M} - 1 \in p^{M+1}\mathbb{Z}_p$, and thus, for any $\ell \in \mathbb{N}$

$$\gamma_\mu^{G(\nu_0+\ell p^M)} \;=\; \gamma_\mu^{G(\nu_0)+p^M\lambda(\ell)} \;=\; \gamma_\mu^{G(\nu_0)}(1+p^{M+1}\rho_\mu(\ell))$$

with appropriate $\lambda(\ell) \in \mathbb{N},\ \rho_\mu(\ell) \in \mathbb{Z}_p$. From this we see

$$\begin{aligned}\Big|\sum_{\mu=1}^m \delta_\mu\gamma_\mu^{G(\nu_0+\ell p^M)} - \sum_{\mu=1}^m \delta_\mu\gamma_\mu^{G(\nu_0)}\Big|_p \;&=\; p^{-M-1}\Big|\sum_{\mu=1}^m \delta_\mu\rho_\mu(\ell)\gamma_\mu^{G(\nu_0)}\Big|_p \\ &\leq\; p^{-M-1} < p^{-v}\end{aligned}$$

for any $\ell \in \mathbb{N}$, and therefore

$$\Big|\sum_{\mu=1}^m \delta_\mu\gamma_\mu^{G(\nu)}\Big|_p \;=\; p^{-v} \quad \text{for} \quad \nu = \nu_0 + \ell p^M \quad (\ell = 0,1,2,\ldots).$$

This proves Lemma 2.

To prove the only-if-part of Theorem 1 in the particular case $e = g,\ g \in \mathbb{Z}[x]$, we write[2] $n = (p-1)\nu + r$ with $r \in \{0,\ldots,p-2\}$, thus getting $g(n) \equiv g(r) \pmod{p-1}$. Using this and Lemma 1 we deduce

$$\begin{aligned}\sum_{\tau=s+1}^t D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{g(n)} \;&=\; \sum_{\tau=s+1}^t D_\tau F(\underline{f(\alpha)})\zeta_\tau^{g(r)}\,\gamma_{\mu(\tau)}^{g(n)} \\ &=\; \sum_{\mu=1}^m \left(\sum_{\substack{\tau=s+1\\ \mu(\tau)=\mu}}^t D_\tau F(\underline{f(\alpha)})\zeta_\tau^{g(r)}\right)\gamma_\mu^{g(n)}. \qquad (16)\end{aligned}$$

Defining for any fixed $r \in \{0,\ldots,p-2\}$ the new integer-valued polynomial G_r by $G_r(\nu) := g((p-1)\nu + r)$, it is clear, that every G_r satisfies the conditions on G in Lemma 2. On the other hand, it follows from (12), (15) and (16) that for every $r \in \{0,\ldots,p-2\}$

$$\begin{aligned}0 \;&=\; \lim_{\substack{n\to\infty\\ n\equiv r \bmod (p-1)}} \Big|\sum_{\tau=s+1}^t D_\tau F(\underline{f(\alpha)})\left(\frac{\alpha_\tau}{\alpha_t}\right)^{g(n)}\Big|_p \\ &=\; \lim_{\substack{n\to\infty\\ n\equiv r \bmod (p-1)}} \Big|\sum_{\mu=1}^m \delta_\mu(r)\gamma_\mu^{g(n)}\Big|_p \;=\; \lim_{\nu\to\infty}\Big|\sum_{\mu=1}^m \delta_\mu(r)\gamma_\mu^{G_r(\nu)}\Big|_p,\end{aligned}$$

where we defined

$$\delta_\mu(r) \;:=\; \sum_{\substack{\tau=s+1\\ \mu(\tau)=\mu}}^t D_\tau F(\underline{f(\alpha)})\zeta_\tau^{g(r)} \quad (\mu = 1,\ldots,m). \qquad (17)$$

[2] Obviously, we leave the case $p = 2$ to the reader.

Using Lemma 2 we see for any $r \in \{0, \dots, p-2\}$

$$\sum_{\substack{\tau=s+1 \\ \mu(\tau)=\mu}}^{t} D_\tau F(\underline{f(\alpha)})\zeta_\tau^{g(r)} \;=\; 0 \quad (\mu = 1, \dots, m). \tag{18}$$

This leads to

$$\sum_{\substack{\tau=s+1 \\ \mu(\tau)=\mu}}^{t} D_\tau F(\underline{f(\alpha)})\zeta_\tau^{g(n)} \;=\; 0 \quad (\mu = 1, \dots, m) \tag{19}$$

for any $n \in \mathbb{N}$.

Fix now $\mu_0 \in \{1, \dots, m\}$ such that the set of $\tau \in \{s+1, \dots, t\}$ with $\mu(\tau) = \mu_0$ is not empty. Then we find for those τ with $\mu(\tau) = \mu_0$

$$\alpha_\tau \;=\; \alpha_t\zeta_\tau\gamma_{\mu(\tau)} \;=\; \alpha_t\zeta_\tau\gamma_{\mu_0} \;=\; (\alpha_t\gamma_{\mu_0})\zeta_\tau.$$

This, combined with equation (19) for $\mu = \mu_0$, shows that $\{\alpha_\tau | \mu(\tau) = \mu_0\}$ is a $(g(n))$-dependent subset of $\{\alpha_1, \dots, \alpha_t\}$. Here we recall the fact that $D_\tau F(\underline{f(\alpha)}) \neq 0$ $(\tau = s+1, \dots, t)$, see (5).

4. The general case

To finish the proof of the only-if-part of Theorem 1 in the general case of linear recurrence sequences $(e(n))_{n\in\mathbb{N}}$, we note the existence of n_0, $h \in \mathbb{N}$ such that $e(n+h) \equiv e(n) \pmod{(p-1)}$ (or (mod 2) if $p = 2$) holds for any $n \geq n_0$. Equivalently written, with $e(n) = e(h\nu + r) =: E_r(\nu)$ for any $\nu \in \mathbb{N}_0$, $r \in \{n_0, \dots, n_0 + h - 1\}$, this means $E_r(\nu) \equiv E_r(0) \pmod{(p-1)}$ (or (mod 2) if $p = 2$). Then we can proceed as in section 3: Combination of (12) and (14) yields, by reasoning parallel to (16),

$$\begin{aligned} \vartheta^{E_r(\nu)} \;=\; \vartheta^{e(n)} &\gg \Big| \sum_{\tau=s+1}^{t} D_\tau F(\underline{f(\alpha)}) \left(\frac{\alpha_\tau}{\alpha_t}\right)^{e(n)} \Big|_p \\ &= \Big| \sum_{\mu=1}^{m} \delta_\mu(r)\gamma_\mu^{E_r(\nu)} \Big|_p, \end{aligned} \tag{20}$$

where $\delta_\mu(r)$ is defined by (17) with $g(r)$ now replaced by $e(r) = E_r(0)$.

Using the postponed Lemma 3 we deduce from (20) that the m equations (18), with $g(r)$ again replaced by $e(r) = E_r(0)$, hold for any $r \in \{n_0, \dots, n_0 + h - 1\}$. Therefore the equations (19) hold for any $n \geq n_0$ with $g(n)$ replaced by $e(n)$, and from here on the proof terminates as explained at the end of section 3.

Remark 3. For the proof of Lemma 3 below we need a few facts on (homogeneous) linear recurrence sequences with constant coefficients, for short

recurrence sequences, which the reader may find in the introductory chapter "Recurrence Sequences" of the book of Shorey and Tijdeman [12].

First, for our integral recurrence sequence $(e(n))_{n\ge 1}$ there exists a unique recurrence relation of minimal order L, say,

$$e(n) \;=\; a_{L-1}e(n-1) + \cdots + a_0 e(n-L) \quad (n > L) \tag{21}$$

with $a_0 \neq 0$. As it is easily seen, the recurrence coefficients $a_0, \ldots, a_{L-1}$ are rational, in fact, by a theorem due to Fatou, integral. Secondly, from [12, Theorem C.1a)] we know

$$e(n) \;=\; \sum_{\lambda=1}^{\ell} g_\lambda(n) d_\lambda^n \quad (n \in \mathbb{N}), \tag{22}$$

where the distinct non-zero algebraic integers $d_1, \ldots, d_\ell$ are the roots of order $\rho_1, \ldots, \rho_\ell \in \mathbb{N}$ $(\rho_1 + \cdots + \rho_\ell = L)$ of the companion polynomial

$$x^L - a_{L-1}\, x^{L-1} - \cdots - a_0 \quad (\in \mathbb{Z}[x])$$

of the recurrence (21). The uniquely determined $g_\lambda \in \mathbb{Q}(d_1, \ldots, d_\ell)[x]$ have degrees $< \rho_\lambda$ $(\lambda = 1, \ldots, \ell)$. Thirdly, we have from [12, Theorem C.1b)]: If $d_1, \ldots, d_\ell \in \mathbb{C}^\times$ are distinct, $\rho_1, \ldots, \rho_\ell \in \mathbb{N}$, and if one defines $a_0, \ldots, a_{L-1}$ by

$$x^L - a_{L-1}\, x^{L-1} - \cdots - a_0 \;:=\; \prod_{\lambda=1}^{\ell} (x - d_\lambda)^{\rho_\lambda} \quad (L := \sum_{\lambda=1}^{\ell} \rho_\lambda),$$

and if the g_λ are any polynomials of degree $< \rho_\lambda$ $(\lambda = 1, \ldots, \ell)$, then the sequence $(e(n))$ defined by (22) satisfies the recurrence relation (21).

When we applied earlier Lemma 3 to the sequences $(E_r(\nu))_\nu$ for fixed r, we must be sure that these are recurrence sequences for every fixed r. But this follows easily from our above statement and

$$E_r(\nu) \;=\; e(h\nu + r) \;=\; \sum_{\lambda=1}^{\ell} g_\lambda(h\nu + r) d_\lambda^r (d_\lambda^h)^\nu \;=:\; \sum_{\lambda=1}^{\ell'} G_\lambda(\nu) D_\lambda^\nu,$$

where $D_1, \ldots, D_{\ell'}$ are the distinct numbers among the powers $d_1^h, \ldots, d_\ell^h$.

Lemma 3. *Let $\gamma_1, \ldots, \gamma_m \in \mathbb{C}_p$ be distinct and satisfy $|\gamma_\mu - 1|_p < p^{-1/(p-1)} =: R_p$ $(\mu = 1, \ldots, m)$. Let $(E(\nu))$ be a strictly increasing recurrence sequence of non-negative integers, and let $\delta_1, \ldots, \delta_m \in \mathbb{C}_p$. If*

$$\sum_{\mu=1}^{m} \delta_\mu \gamma_\mu^{E(\nu)} \;=\; O(\vartheta^{E(\nu)}) \tag{23}$$

holds for $\nu \to \infty$, with a fixed non-negative real number $\vartheta < 1$, then $\delta_1 = \cdots = \delta_m = 0$.

Remark 4. Obviously, if γ_μ is as in Lemma 1, then $|\gamma_\mu - 1|_p < R_p$ for any prime p. Furthermore, it should be pointed out that, under the conditions on the γ's in Lemma 3, no quotient $\gamma_\mu/\gamma_{\mu'}$ $(\mu \neq \mu')$ can be a root of unity, see [4, p.154, xiii)].

Proof. From Remark 3, and rewriting (22) a little, we know

$$E(\nu) \;=\; \sum_{\lambda=1}^{\ell} G_\lambda(\nu) D_\lambda^\nu$$

with distinct non-zero algebraic integers $D_1, \dots, D_\ell$ and with non-zero polynomials G_λ having their coefficients in $\mathbb{Q}(D_1, \dots, D_\ell)$. Therefore we know $0 < |D_\lambda|_p \leq 1$ $(\lambda = 1, \dots, \ell)$, and we may assume w.l.o.g.

$$1 \;=\; |D_1|_p = \cdots = |D_{\ell'}|_p \;>\; |D_\lambda|_p \quad (\lambda = \ell' + 1, \dots, \ell). \tag{24}$$

Denoting

$$A(\nu) \;:=\; \sum_{\lambda=1}^{\ell'} G_\lambda(\nu) D_\lambda^\nu, \quad B(\nu) \;:=\; \sum_{\lambda=\ell'+1}^{\ell} G_\lambda(\nu) D_\lambda^\nu,$$

we have $|B(\nu)|_p \to 0$ as $\nu \to \infty$, by (24). Since $|E(\nu)|_p \leq 1$ we may suppose $|A(\nu)|_p,\ |B(\nu)|_p \leq 1$ for every $\nu \in \mathbb{N}_0$. Defining $\beta_\mu := \log_p \gamma_\mu$ for $\mu = 1, \dots, m$, the $\beta_1, \dots, \beta_m$ are distinct, and the inequalities $|\beta_\mu|_p \leq |\gamma_\mu - 1|_p < R_p$ hold. The sum on the left-hand side of (23) is

$$\sum_{\mu=1}^{m} \delta_\mu \gamma_\mu^{E(\nu)} \;=\; \sum_{\mu=1}^{m} \delta_\mu \exp_p(\beta_\mu E(\nu)) \;=\; \sum_{\mu=1}^{m} \delta_\mu \exp_p(\beta_\mu A(\nu)) \cdot \exp_p(\beta_\mu B(\nu)).$$

W.l.o.g. we may suppose $|\delta_\mu|_p \leq 1$ $(\mu = 1, \dots, m)$. We assume further that at least one of the $\delta_1, \dots, \delta_m$ is non-zero, and derive a contradiction according to the cases $\ell' = \ell$ and $\ell' < \ell$.

Case $\ell' = \ell$. Then $B(\nu) = 0$ and $A(\nu) = E(\nu)$ for every ν. By the Skolem-Lech-Mahler theorem, there is a ν_0 with $\Sigma_{\mu=1}^m \delta_\mu \gamma_\mu^{A(\nu_0)} \neq 0$, say,

$$\Big|\sum_{\mu=1}^{m} \delta_\mu \gamma_\mu^{A(\nu_0)}\Big|_p \;=\; p^{-v}$$

with rational $v \geq 0$.

Suppose now $L \in \mathbb{N}$ large enough, to be specified later. Then there is an $N \in \mathbb{N}$ such that for any $\kappa \in \mathbb{N}_0$ the following inequalities hold

$$\max(|G_\lambda(\nu_0 + N\kappa) - G_\lambda(\nu_0)|_p,\ |D_\lambda^{N\kappa} - 1|_p) \;<\; p^{-L} \quad (\lambda = 1, \dots, \ell).$$

These imply

$$
\begin{aligned}
|A(\nu_0+N\kappa)-A(\nu_0)|_p \;&\le\; \max_{1\le\lambda\le\ell} |(G_\lambda(\nu_0+N\kappa)D_\lambda^{N\kappa}-G_\lambda(\nu_0))\cdot D_\lambda^{\nu_0}|_p \\
&\le \max_{1\le\lambda\le\ell} \max(|G_\lambda(\nu_0+N\kappa)-G_\lambda(\nu_0)|_p,\ |G_\lambda(\nu_0)|_p|D_\lambda^{N\kappa}-1|_p) \qquad (25)\\
&< c_1 p^{-L},
\end{aligned}
$$

where $c_1>0$ depends only on $G_1,\dots,G_\ell$. Then for $\nu=\nu_0+N\kappa$ we get

$$
\begin{aligned}
\Big|\sum_{\mu=1}^m \delta_\mu\gamma_\mu^{A(\nu)}-\sum_{\mu=1}^m \delta_\mu\gamma_\mu^{A(\nu_0)}\Big|_p \;&\le\; \max_{1\le\mu\le m} |\exp_p(\beta_\mu(A(\nu)-A(\nu_0)))-1|_p \\
&=\; \max_{1\le\mu\le m} |\beta_\mu|_p\,|A(\nu)-A(\nu_0)|_p <\; R_p c_1 p^{-L},
\end{aligned}
$$

by (25). Here the right-hand side is $\le p^{-v}$ if we take L large enough. Therefore

$$
\Big|\sum_{\mu=1}^m \delta_\mu\gamma_\mu^{E(\nu)}\Big|_p \;=\; \Big|\sum_{\mu=1}^m \delta_\mu\gamma_\mu^{A(\nu)}\Big|_p \;=\; p^{-v}
$$

for all large ν of the form $\nu_0+N\kappa,\ \kappa\in\mathbb{N}$. Since this contradicts hypothesis (23) of Lemma 3, we have $\delta_1=\cdots=\delta_m=0$ in the first case.

Case $\ell'<\ell$. If $B(\nu)=0$ holds infinitely often, then the infinite set $\{\nu\in\mathbb{N}_0 | \Sigma_{\lambda=\ell'+1}^{\ell} G_\lambda(\nu)D_\lambda^\nu=0\}$ is a union of a finite set and of finitely many (at least one) arithmetical progressions, by the Skolem-Lech-Mahler theorem. This implies the existence of $c,d\in\mathbb{N}$ such that $B(c+d\tilde\nu)=0$ for each $\tilde\nu\in\mathbb{N}_0$. Putting

$$
\tilde E(\tilde\nu) \;:=\; E(c+d\tilde\nu) \;=\; A(c+d\tilde\nu)
$$

we are back to the first case with $\tilde E$.

Therefore we may suppose from now on that $B(\nu)\ne 0$ for all but finitely many ν. Indeed, we may even assume w.l.o.g. $B(\nu)\ne 0$ for any $\nu\in\mathbb{N}_0$.

Next we transform a little the sum on the left-hand side of (23)

$$
\begin{aligned}
\sum_{\mu=1}^m \delta_\mu\gamma_\mu^{E(\nu)} \;&=\; \sum_{\mu=1}^m \delta_\mu \exp_p(\beta_\mu A(\nu)) \sum_{j=0}^\infty \frac{1}{j!}\beta_\mu^j B(\nu)^j \\
&=\; \sum_{j=0}^\infty \frac{1}{j!} B(\nu)^j \sum_{\mu=1}^m \delta_\mu\beta_\mu^j \exp_p(\beta_\mu A(\nu)). \qquad (26)
\end{aligned}
$$

For every $\nu\in\mathbb{N}_0$, at least one of the sums

$$
\sum_{\mu=1}^m \delta_\mu\beta_\mu^j \exp_p(\beta_\mu A(\nu)) \quad (j=0,\dots,m-1) \qquad (27)
$$

is non-zero, by a Vandermonde argument, and since not all $\delta_1, \dots, \delta_m$ vanish. Therefore, for any $\nu \in \mathbb{N}_0$, there exists $j(\nu) \in \{0, \dots, m-1\}$ such that (27) vanishes for $j = 0, \dots, j(\nu)-1$, but not for $j = j(\nu)$. Thus there exists a $j_0 \in \{0, \dots, m-1\}$ such that the sum (27) vanishes for any $\nu \in \mathbb{N}_0$ and $j = 0, \dots, j_0 - 1$ but

$$\sum_{\mu=1}^{m} \delta_\mu \beta_\mu^{j_0} \exp_p(\beta_\mu A(\nu_0)) \;\neq\; 0$$

for an appropriate $\nu_0 \in \mathbb{N}$. With some rational $w \geq 0$ we define

$$\big|\sum_{\mu=1}^{m} \delta_\mu \beta_\mu^{j_0} \exp_p(\beta_\mu A(\nu_0))\big|_p \;=\; p^{-w}.$$

As we saw in the first case there exists $N \in \mathbb{N}$ such that

$$\big|\sum_{\mu=1}^{m} \delta_\mu \beta_\mu^{j_0} \exp_p(\beta_\mu A(\nu_0 + N\kappa))\big|_p \;=\; p^{-w} \tag{28}$$

holds for every $\kappa \in \mathbb{N}_0$.

Replacing now the linear recurrence $(E(\nu))$ by the new one $(E^*(\kappa))_{\kappa\in\mathbb{N}_0}$, where $E^*(\kappa) := E(\nu_0 + N\kappa)$, we find from (26)

$$\sum_{\mu=1}^{m} \delta_\mu \gamma_\mu^{E^*(\kappa)} \;=\; \sum_{j=j_0}^{\infty} \frac{1}{j!} B(\nu_0 + N\kappa)^j \sum_{\mu=1}^{m} \delta_\mu \beta_\mu^j \exp_p(\beta_\mu A(\nu_0 + N\kappa)).$$

Using (28) and $|B(\nu_0 + N\kappa)|_p \to 0$ as $\kappa \to \infty$, the last equation yields

$$\big|\sum_{\mu=1}^{m} \delta_\mu \gamma_\mu^{E^*(\kappa)}\big|_p \;=\; \big|\frac{1}{j_0!} B(\nu_0 + N\kappa)^{j_0}\big|_p \cdot p^{-w} \tag{29}$$

for every large κ. This equation, combined with hypothesis (23) in Lemma 3, shows that the case $j_0 = 0$ is impossible. Hence we know $m > 1$ and $j_0 \in \{1, \dots, m-1\}$. Since

$$|\alpha|_p \;\geq\; (\lceil\overline{\alpha}\rceil \operatorname{den}\alpha)^{-\deg\alpha} \tag{30}$$

holds for any $\alpha \in \overline{\mathbb{Q}}^\times$ we find from our previous definition of $B(\nu)$

$$|B(\nu)|_p \;=\; \Big|\sum_{\lambda=\ell'+1}^{\ell} G_\lambda(\nu) D_\lambda^\nu\Big|_p \;\geq\; c_2^{-\nu}$$

with some real $c_2 > 1$ (independent of ν). Using this, (29) and (23) we find

$$c_3 \vartheta^{E^*(\kappa)} \;\geq\; |B(\nu_0 + N\kappa)|_p^{j_0} \;\geq\; c_2^{-(\nu_0+N\kappa)j_0}$$

and thus

$$E^*(\kappa)|\log\vartheta| \;\leq\; c_4 + j_0 N(\log c_2)\kappa \;\leq\; c_5\kappa \tag{31}$$

for every large $\kappa \in \mathbb{N}_0$.

On the other hand, since $\ell' < \ell$, there is a λ_0 with $0 < |D_{\lambda_0}|_p < 1$. From (30) follows $\overline{|D_{\lambda_0}|} > 1$, thus at least one of the conjugates of D_{λ_0} (which occur all among the $D_1, \ldots, D_\ell$) must be larger than 1 in absolute value, thus leading to

$$\triangle := \max_{1 \le \lambda \le \ell} |D_\lambda| > 1.$$

Estimating the positive $E^*(\kappa)$ from below, at least for infinitely many κ, (31) leads now quickly to the desired contradiction.

The precise conclusion is as follows. The representation of $E(\nu)$ from the very beginning of our proof and our definition of $E^*(\kappa)$ leads us to

$$E^*(\kappa) \;=\; E(\nu_0 + N\kappa) \;=\; \sum_{\lambda=1}^{\ell} G_\lambda(\nu_0 + N\kappa) D_\lambda^{\nu_0} (D_\lambda^N)^\kappa \;=:\; \sum_{\lambda=1}^{\tilde{\ell}} \tilde{G}_\lambda(\kappa) \tilde{D}_\lambda^\kappa,$$

where the non-zero $\tilde{D}_1, \ldots, \tilde{D}_{\tilde{\ell}}$ are the distinct among the $D_1^N, \ldots, D_\ell^N$. To this representation of the recurrence $(E^*(\kappa))_{\kappa \in \mathbb{N}_0}$ we apply Kubota's result [7, Corollary 3(ii)], and we deduce the existence of a constant $c_6 > 0$ such that

$$E^*(\kappa) \;\ge\; c_6 \kappa^d \triangle^{N\kappa}$$

holds for infinitely many κ, where $d := \max\{\deg \tilde{G}_\lambda \,|\, |\tilde{D}_\lambda| = \triangle^N\} \in \mathbb{N}_0$. Thus Lemma 3 is completely proved.

5. Sketch of proof of Theorem 2

Let $d_1, \ldots, d_m \in \mathbb{N} \setminus \{1\}$ be distinct; w.l.o.g. we may suppose $d_1 > \cdots > d_m > 1$. Since Corollary 2 allows us to assume $m > 1$, we may further assume inductively that the

$$f_{d_i}(\alpha_\tau) \quad (\tau = 1, \ldots, t; i = 1, \ldots, m-1)$$

are algebraically independent. For each $t' \in \{1, \ldots, t\}$ we have to prove that the $f_{d_m}(\alpha_\tau)$ $(\tau = 1, \ldots, t')$ are algebraically independent over the field

$$K \;:=\; \mathbb{Q}_p(f_{d_1}(\alpha_1), \ldots, f_{d_1}(\alpha_t), \ldots, f_{d_{m-1}}(\alpha_1), \ldots, f_{d_{m-1}}(\alpha_t)).$$

We suppose $f_{d_1}(\alpha_1), \ldots, f_{d_m}(\alpha_{t'})$ to be algebraically dependent over K, whereas, (if $t' > 1$) every $t' - 1$ of these are algebraically independent. Then there exists a polynomial

$$F \in \mathbb{Z}_p[f_{d_1}(\alpha_1), \ldots, f_{d_{m-1}}(\alpha_t)][x_1, \ldots, x_{t'}] \setminus \{0\}$$

with minimal total degree such that

$$F(f_{d_m}(\alpha_1), \ldots, f_{d_m}(\alpha_{t'})) \;=\; 0.$$

We may assume $|\alpha_1|_p \le \cdots \le |\alpha_{s'}|_p < |\alpha_{s'+1}|_p = \cdots = |\alpha_{t'}|_p$. If $a \in \mathbb{Z}_p[f_{d_1}(\alpha_1), \ldots, f_{d_{m-1}}(\alpha_t)]$ then, with $\sigma(k)$ and $n \ge k$ as in section 2,

$$|a^{\sigma(k)} - a|_p \;\le\; (\max_{1\le\tau\le t} |\alpha_\tau|_p)^{d^k_{m-1}} \;=\; O\big(|\alpha_{t'}|_p^{2d^k_m}\big)$$

taking $d_{m-1} > d_m$ into account. Hence, we have (11) with s', t' instead of s, t and can continue in the same way as in section 2.

References

[1] Y. Amice, *Les nombres p-adiques*. Presses Universitaires de France, Paris, 1975.

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

[3] P. Bundschuh, V.G. Chirskii, *Algebraic independence of elements from* $\mathbb{C}_p$ *over* $\mathbb{Q}_p$*, II* Acta Arith. **113** (2004), 309–326.

[4] F.Q. Gouvêa, *p-adic Numbers*. Springer-Verlag, Berlin et al., 1993.

[5] G. Hansel, *Une démonstration simple du théorème de Skolem-Mahler-Lech*. Theoret. Comput. Sci. **43** (1986), 91–98.

[6] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed. Springer-Verlag, New York, 1984.

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

[8] D. Lampert, *Algebraic p-adic Expansions*. J. Number Theory **23** (1986), 279–284.

[9] K. Nishioka, *p-adic transcendental numbers*. Proc. Amer. Math. Soc. **108** (1990), 39–41.

[10] K. Nishioka, *Mahler Functions and Transcendence*. LNM 1631, Springer-Verlag, Berlin et al., 1996.

[11] A.B. Shidlovskii, *Transcendental Numbers*. De Gruyter, Berlin et al., 1989.

[12] T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*. Cambridge Univ. Press, 1986.

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

Kumiko Nishioka
Mathematics, Hiyoshi Campus
Keio University
4-1-1 Hiyoshi, Kohoku-ku
Yokohama 223-8521, Japan
E-mail : nishioka@math.hc.keio.ac.jp