Nihonkai Math. J.
Vol.14(2003), 83-93

A TRANSCENDENCE CRITERION OVER p-ADIC FIELDS

VICTOR ALEXANDRU AND ALEXANDRU ZAHARESCU

ABSTRACT. Let p be a prime number, $\mathbf{Q}_p$ the field of p-adic numbers, $\bar{\mathbf{Q}}_p$ a fixed algebraic closure of $\mathbf{Q}_p$, $\mathbf{C}_p$ the completion of $\bar{\mathbf{Q}}_p$ with respect to the p-adic valuation, and $O_{\mathbf{C}_p}$ the ring of integers of $\mathbf{C}_p$. We provide a criterion which characterizes the elements of $O_{\mathbf{C}_p}$ which are transcendental over $\mathbf{Q}_p$.

1. INTRODUCTION

Let p be a prime number, $\mathbf{Q}_p$ the field of p-adic numbers, $\mathbf{Z}_p$ the ring of p-adic integers, $\bar{\mathbf{Q}}_p$ a fixed algebraic closure of $\mathbf{Q}_p$, $\mathbf{C}_p$ the completion of $\bar{\mathbf{Q}}_p$ with respect to the unique extension to $\bar{\mathbf{Q}}_p$ of the p-adic valuation on $\mathbf{Q}_p$, and $O_{\mathbf{C}_p}$ the ring of integers of $\mathbf{C}_p$. The theory of saturated distinguished chains of polynomials, developed in [8], [9], [12], [1], [10], [11], plays an important role in the problem of describing the structure of irreducible polynomials in one variable over $\mathbf{Q}_p$, or more generally over a local field K. Knowing a saturated distinguished chain for a given element $\alpha \in \bar{K}$, where $\bar{K}$ denotes a fixed algebraic closure of K, can be helpful in various problems. One reason is that we can use such a chain to construct an integral basis of $K(\alpha)$ over K. The shape of such a basis may be useful in practice, for instance it has been used in [7] in order to show that the Ax-Sen constant vanishes for deeply ramified extensions (in the sense of [4]). Another instance when saturated distinguished chains of polynomials can be successfully used as tools to understand various questions on the structure of $\mathbf{C}_p$ is described in the present paper. If t is an element of $O_{\mathbf{C}_p}$ and $(P_n(X))_{n\in\mathbf{N}}$ is a sequence of polynomials in $\mathbf{Z}_p[X]$, of any degrees, such that $P_n(t) \to 0$ as $n \to \infty$, we consider for each $n \in \mathbf{N}$ the derivative $P_n'(X)$, and investigate convergence properties of the sequence $(P_n'(t))_{n\in\mathbf{N}}$. It turns out that in general the sequence $(P_n'(t))_{n\in\mathbf{N}}$ behaves differently when t is transcendental over $\mathbf{Q}_p$, than in the case when t is algebraic over $\mathbf{Q}_p$. This allows us to establish a criterion which characterizes the elements $t \in O_{\mathbf{C}_p}$ which are transcendental over $\mathbf{Q}_p$, and to derive some consequences of this result. The key ingredients in investigating such questions come from the properties of saturated distinguished chains of polynomials over $\mathbf{Q}_p$.

2. DISTINGUISHED SEQUENCES OF POLYNOMIALS OVER $\mathbf{Q}_p$

In this section we present the basic properties of the so-called distinguished sequences of polynomials. We work in the following context. We let p be a fixed prime number, $\mathbf{Q}_p$ the field of p-adic numbers, $\mathbf{Z}_p$ the ring of p-adic integers, and

2000 *Mathematics Subject Classification.* 11S99.
Key words and phrases: p-adic fields, transcendental elements.

we denote by v the p-adic valuation on $\mathbf{Q}_p$, normalized by $v(p) = 1$. Next, we let $\bar{\mathbf{Q}}_p$ be a fixed algebraic closure of $\mathbf{Q}_p$, and $\mathbf{C}_p$ the completion of $\bar{\mathbf{Q}}_p$ with respect to the unique extension of v to $\bar{\mathbf{Q}}_p$. We continue to denote by v the corresponding valuations on $\bar{\mathbf{Q}}_p$ and $\mathbf{C}_p$.

A pair (a, b) of elements from $\bar{\mathbf{Q}}_p$ is said to be a distinguished pair (relative to $\mathbf{Q}_p$), provided that one has

$$\deg a > \deg b,$$

$$v(a - c) \leq v(a - b)$$

for any $c \in \bar{\mathbf{Q}}_p$ with $\deg c < \deg a$, and

$$v(a - c) < v(a - b)$$

for any $c \in \bar{\mathbf{Q}}_p$ with $\deg c < \deg b$. Here $\deg a$, $\deg b$ and $\deg c$ denote the degrees of a, b and respectively c over $\mathbf{Q}_p$.

Given two irreducible polynomials $f, g \in \mathbf{Q}_p[X]$, one says that (g, f) is a distinguished pair if there exist a root a of g and a root b of f such that (a, b) is a distinguished pair. It is easy to see that if (g, f) is a distinguished pair of polynomials, then for any root a of g there exists a root b of f such that (a, b) is a distinguished pair, and for any root b of f there exists a root a of g such that (a, b) is a distinguished pair.

Let $a \in \bar{\mathbf{Q}}_p$. If $a_0, \ldots, a_s \in \bar{\mathbf{Q}}_p$, one says that $(a_0, \ldots, a_s)$ is a distinguished chain for a if $a_0 = a$ and (a_{i-1}, a_i) is a distinguished pair for any $i \in \{1, \ldots, s\}$. The integer s is called the length of the chain $(a_0, \ldots, a_s)$. A distinguished chain $(a_0, \ldots, a_s)$ for a is said to be saturated if there is no distinguished chain $(b_0, \ldots, b_r)$ for a, with $r > s$, such that $\{a_0, \ldots, a_s\} \subseteq \{b_0, \ldots, b_r\}$. One shows that $(a_0, \ldots, a_s)$ is saturated if and only if $a_s \in \mathbf{Q}_p$.

Let $f_0 = f, f_1, \ldots, f_s$ be monic, irreducible polynomials over $\mathbf{Q}_p$. One says that $(f_0, \ldots, f_s)$ is a (saturated) distinguished chain for f if there exist roots $a_0 = a, a_1, \ldots, a_s$ of $f_0, f_1, \ldots, f_s$ respectively such that $(a_0, \ldots, a_s)$ is a (saturated) distinguished chain for a. The following results capture some of the basic properties of saturated distinguished chains.

Theorem 1. ([12], Proposition 4.1). *If $(a_0, \ldots, a_s)$ is a distinguished chain, then*

$$G(\mathbf{Q}_p(a_s)) \subseteq G(\mathbf{Q}_p(a_{s-1})) \subseteq \cdots \subseteq G(\mathbf{Q}_p(a_0)),$$

and

$$R(\mathbf{Q}_p(a_s)) \subseteq R(\mathbf{Q}_p(a_{s-1})) \subseteq \cdots \subseteq R(\mathbf{Q}_p(a_0)),$$

where, for any $j \in \{0, 1, \ldots, s\}$, $G(\mathbf{Q}_p(a_j)) = \{v(x) : x \in \mathbf{Q}_p(a_j)\}$ is the value group of $\mathbf{Q}_p(a_j)$, and $R(\mathbf{Q}_p(a_j))$ denotes the residue field of $\mathbf{Q}_p(a_j)$.

Corollary 1. *If $(a_0, \ldots, a_s)$ is a distinguished chain, then $\deg a_i$ divides $\deg a_{i-1}$, for any $i \in \{1, \ldots, s\}$.*

Theorem 2. ([12], Proposition 4.2). *Let $(a_0, \ldots, a_s)$ and $(b_0, \ldots, b_r)$ be two saturated distinguished chains for a. Then $s = r$. Moreover if $c_i \in \{a_i, b_i\}$, $1 \leq i \leq s$, then $(c_0, \ldots, c_s)$ is also a saturated distinguished chain for a.*

Theorem 3. ([12], Proposition 4.3). *Let $a \in \bar{\mathbf{Q}}_p$, let $(a_0, \ldots, a_s)$ and $(b_0, \ldots, b_s)$ be two saturated distinguished chains for a, and let f_i, g_j be the minimal polynomials of a_i and respectively b_j over $\mathbf{Q}_p$. Then for any $i \in \{1, \ldots, s\}$ one has*

$$v(a_{i-1} - a_i) = v(b_{i-1} - b_i),$$

$$v(f_i(a_{i-1})) = v(g_i(b_{i-1})),$$

$$G(\mathbf{Q}_p(a_i)) = G(\mathbf{Q}_p(b_i)),$$

and

$$R(\mathbf{Q}_p(a_i)) = R(\mathbf{Q}_p(b_i)).$$

Moreover if we replace the condition $b_0 = a$ in the hypothesis by the condition $b_0 = \sigma(a)$ where $\sigma \in Gal(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ then all the above relations remain valid, with the only exception that in the last relation instead of equality we have a canonical $R(\mathbf{Q}_p)-$isomorphism.

A sequence $(\alpha_n)_{n \in \mathbf{N}}$ of elements from $\bar{\mathbf{Q}}_p$ is said to be distinguished over $\mathbf{Q}_p$, provided that

$$\alpha_0 \in \mathbf{Q}_p, \tag{2.1}$$

$$(\alpha_n, \alpha_{n-1}) \text{ is a distinguished pair,} \tag{2.2}$$

for any $n \geq 1$, and

$$v(\alpha_n - \alpha_{n-1}) \to \infty, \text{ as } n \to \infty. \tag{2.3}$$

Note that any distinguished sequence is a Cauchy sequence in $\bar{\mathbf{Q}}_p$, and so it has a limit in $\mathbf{C}_p$.

Theorem 4. ([1], Proposition 2.1). *Let $t \in \mathbf{C}_p$ be the limit of a distinguished sequence $(\alpha_n)_{n \in \mathbf{N}}$. Then t is transcendental over $\mathbf{Q}_p$.*

Theorem 5. ([1], Proposition 2.2). *Let $t \in \mathbf{C}_p$ be transcendental over $\mathbf{Q}_p$. Then there exists a distinguished sequence $(\alpha_n)_{n \in \mathbf{N}}$ such that $t = \lim_{n \to \infty} \alpha_n$.*

Theorem 6. ([1], Proposition 2.3). *Let $t \in \mathbf{C}_p$ be transcendental over $\mathbf{Q}_p$. Let $(\alpha_n)_{n \in \mathbf{N}}$ and $(\alpha'_n)_{n \in \mathbf{N}}$ be distinguished sequences over $\mathbf{Q}_p$ such that $t = \lim_{n \to \infty} \alpha_n = \lim_{n \to \infty} \alpha'_n$. Then*

$$\deg \alpha_n = \deg \alpha'_n \text{ and } v(t - \alpha_n) = v(t - \alpha'_n), \tag{2.4}$$

for any $n \in \mathbf{N}$. If f_n and $\bar{f}_n$ denote the minimal polynomial of α_n and respectively α'_n over $\mathbf{Q}_p$, then

$$v(f_n(\alpha_{n+1})) = v(\bar{f}_n(\alpha'_{n+1})), \tag{2.5}$$

for any $n \in \mathbf{N}$. Also,

$$e(\mathbf{Q}_p(\alpha_n)/\mathbf{Q}_p) = e(\mathbf{Q}_p(\alpha'_n)/\mathbf{Q}_p) \text{ and } f(\mathbf{Q}_p(\alpha_n)/\mathbf{Q}_p) = f(\mathbf{Q}_p(\alpha'_n)/\mathbf{Q}_p), \tag{2.6}$$

for any $n \in \mathbf{N}$, where $e(./.)$ and $f(./.)$ denote the ramification index and respectively the inertial degree of the corresponding field extension.

By Theorem 6 it follows that, given an element $t \in \mathbf{C}_p$ which is transcendental over $\mathbf{Q}_p$, the numbers

$$D_n := \deg \alpha_n, \quad n \in \mathbf{N}, \tag{2.7}$$

$$E_n := e(\mathbf{Q}_p(\alpha_n)/\mathbf{Q}_p), \quad n \in \mathbf{N}, \tag{2.8}$$

$$F_n := f(\mathbf{Q}_p(\alpha_n)/\mathbf{Q}_p), \quad n \in \mathbf{N}, \tag{2.9}$$

$$\delta_n := v(t - \alpha_n), \quad n \in \mathbf{N}, \tag{2.10}$$

and

$$\gamma_n := v(f_n(\alpha_{n+1})), \quad n \in \mathbf{N}, \tag{2.11}$$

depend on t only, and not on the particular choice of the distinguished sequence $(\alpha_n)_{n\in\mathbf{N}}$ with $\lim_{n\to\infty} \alpha_n = t$.

Let us fix now a transcendental element t and a distinguished sequence $(\alpha_n)_{n\in\mathbf{N}}$ with $\lim_{n\to\infty} \alpha_n = t$. For any $n \in \mathbf{N}$, let f_n denote the monic minimal polynomial of α_n over $\mathbf{Q}_p$, and let $D_n = \deg \alpha_n = \deg f_n$. By Corollary 1 we know that D_n divides D_{n+1}, for any $n \in \mathbf{N}$.

We will denote by $\mathcal{A}$ the set of sequences of nonnegative integers of the form $\mathbf{s} = (s_0, s_1, \ldots, s_n, \ldots)$ such that $s_n < D_{n+1}/D_n$ for any n, and $s_n = 0$ for all but finitely many values of n. On $\mathcal{A}$ we have a natural order, defined by

$$\mathbf{s} = (s_0, s_1, \ldots, s_n, \ldots) < \mathbf{s}' = (s_0', s_1', \ldots, s_n', \ldots)$$

if there exists a natural number m such that $s_n = s_n'$ for any $n > m$, and $s_m < s_m'$. With respect to this order, $\mathcal{A}$ becomes a well ordered set. To any $\mathbf{s} = (s_0, s_1, \ldots, s_n, \ldots) \in \mathcal{A}$ one associates the polynomial

$$H_\mathbf{s}(X) = f_0^{s_0}(X) f_1^{s_1}(X) \cdots f_n^{s_n}(X) \cdots .$$

Denote by $q_\mathbf{s}$ the integer part of the rational number $v(H_\mathbf{s}(t))$, and let

$$M_\mathbf{s}(X) = \frac{H_\mathbf{s}(X)}{p^{q_\mathbf{s}}}.$$

We consider the elements $M_\mathbf{s}(t) \in \mathbf{C}_p$, for $\mathbf{s} \in \mathcal{A}$, and arrange them in a sequence, according to the order on $\mathcal{A}$. In order to simplify the notation, we write the elements of this sequence as $M_0, M_1, \ldots, M_n, \ldots$. Thus for any $n \geq 0$, M_n stands for that element $M_\mathbf{s}(t)$ for which $\mathbf{s}$ is the $(n+1)-$th element of $\mathcal{A}$, according to the order on $\mathcal{A}$. It is easy to see that for each $n \geq 0$, M_n is a polynomial of degree exactly n in t. Note also that $0 \leq v(M_n) < 1$, for any $n \in \mathbf{N}$.

If $(a_n)_{n\in\mathbf{N}}$ is a sequence in $\mathbf{Q}_p$ such that $v(a_n) \to \infty$, then the series $\sum_{n\in\mathbf{N}} a_n M_n$ converges in $\mathbf{C}_p$. Let $\mathcal{H}(t)$ denote the set of elements of $\mathbf{C}_p$ of the form $\sum_{n\in\mathbf{N}} a_n M_n$, where $(a_n)_{n\in\mathbf{N}}$ is a sequence in $\mathbf{Q}_p$ which converges to 0.

Theorem 7. ([1], Proposition 6.1). *$\mathcal{H}(t)$ is a subring of $\mathbf{C}_p$. Moreover for any $x = \sum_{n\in\mathbf{N}} a_n M_n$, where $(a_n)_{n\in\mathbf{N}}$ is a sequence in $\mathbf{Q}_p$ which converges to 0, one has*

$$v(x) = \inf_{n\in\mathbf{N}} (v(a_n) + v(M_n)).$$

Theorem 8. ([1], Proposition 6.2). *For any element t of $\mathbf{C}_p$, transcendental over $\mathbf{Q}_p$, the ring $\mathbf{Q}_p[t]$ and the field $\mathbf{Q}_p(t)$ have the same topological closure in $\mathbf{C}_p$.*

Theorem 9. ([1], Proposition 6.3). *For any element t of $\mathbf{C}_p$, transcendental over $\mathbf{Q}_p$, $\mathcal{H}(t)$ coincides with the topological closure of $\mathbf{Q}_p(t)$ in $\mathbf{C}_p$.*

Theorems 7, 8 and 9 above show that for any element t of $\mathbf{C}_p$, transcendental over $\mathbf{Q}_p$, and any distinguished sequence $(\alpha_n)_{n\in\mathbf{N}}$ over $\mathbf{Q}_p$, with $\lim_{n\to\infty}\alpha_n = t$, the corresponding sequence $(M_n)_{n\in\mathbf{N}}$ forms an integral basis of the topological closure of $\mathbf{Q}_p(t)$ in $\mathbf{C}_p$, over $\mathbf{Q}_p$.

We also mention that for any complete subfield E of $\mathbf{C}_p$, in particular for $\mathbf{C}_p$ itself, there exists an element t such that $\mathbf{Q}_p(t)$ is dense in E (see [6] and [2]).

3. A TRANSCENDENCE CRITERION OVER $\mathbf{Q}_p$

Denote by $O_{\bar{\mathbf{Q}}_p}$ and $O_{\mathbf{C}_p}$ the ring of integers of $\bar{\mathbf{Q}}_p$ and respectively the ring of integers of $\mathbf{C}_p$, thus $O_{\bar{\mathbf{Q}}_p} = \{x \in \bar{\mathbf{Q}}_p : v(x) \geq 0\}$ and $O_{\mathbf{C}_p} = \{x \in \mathbf{C}_p : v(x) \geq 0\}$. We will prove the following theorem.

Theorem 10. *Let $t \in O_{\mathbf{C}_p}$, t transcendental over $\mathbf{Q}_p$. Then, for any sequence $(t_n)_{n\in\mathbf{N}}$ in $\mathbf{C}_p$ with $\lim_{n\to\infty} t_n = t$, and any sequence of polynomials $(P_n(X))_{n\in\mathbf{N}}$ in $\mathbf{Z}_p[X]$, such that*

$$\lim_{n\to\infty} P_n(t_n) = 0, \tag{3.1}$$

we have

$$\lim_{n\to\infty} P_n'(t_n) = 0. \tag{3.2}$$

By taking $t_n = t$ for any $n \in \mathbf{N}$, we obtain the following corollary.

Corollary 2. *Let $t \in O_{\mathbf{C}_p}$, t transcendental over $\mathbf{Q}_p$. Then, for any sequence of polynomials $(P_n(X))_{n\in\mathbf{N}}$ in $\mathbf{Z}_p[X]$, such that*

$$\lim_{n\to\infty} P_n(t) = 0, \tag{3.3}$$

we have

$$\lim_{n\to\infty} P_n'(t) = 0. \tag{3.4}$$

Note that this result fails for any $t \in O_{\mathbf{C}_p}$ which is algebraic over $\mathbf{Q}_p$. Indeed, if $t = \alpha \in O_{\mathbf{C}_p}$ is algebraic over $\mathbf{Q}_p$, and if $f_\alpha(X)$ denotes the monic minimal polynomial of α over $\mathbf{Q}_p$, then, if we let $P_n(X) = f_\alpha(X)$ for any $n \in \mathbf{N}$, equality (3.3) will be satisfied, while (3.4) will not hold true. Thus Corollary 2 characterizes the elements $t \in O_{\mathbf{C}_p}$ which are transcendental over $\mathbf{Q}_p$.

Corollary 3. *Let $(\alpha_n)_{n\in\mathbf{N}}$ be a Cauchy sequence of elements in $O_{\bar{\mathbf{Q}}_p}$, and for each $n \in \mathbf{N}$ let $f_{\alpha_n}(X)$ denote the monic minimal polynomial of α_n over $\mathbf{Q}_p$. Assume that either the sequence $\left(f'_{\alpha_n}(\alpha_n)\right)_{n\in\mathbf{N}}$ is not a Cauchy sequence, or that this sequence is Cauchy but it does not converge to 0. Then the limit $\lim_{n\to\infty}\alpha_n$ is an element of $\mathbf{C}_p$ which is algebraic over $\mathbf{Q}_p$.*

Corollary 3 follows immediately from Theorem 10. Indeed, let $t = \lim_{n\to\infty} \alpha_n \in O_{C_p}$, and assume that t is transcendental over $\mathbf{Q}_p$. Then, by taking $t_n = \alpha_n$ and $P_n(X) = f_{\alpha_n}(X)$ for any $n \in \mathbf{N}$ in the statement of Theorem 10, the condition (3.1) will be satisfied, while (3.2) will fail, by the assumptions from the statement of Corollary 3.

Corollary 4. *Let $t \in O_{\mathbf{C}_p}$, t transcendental over $\mathbf{Q}_p$, and let $(P_n(X))_{n\in\mathbf{N}}$ be a sequence of polynomials in $\mathbf{Z}_p[X]$ such that the sequence $(P_n(t))_{n\in\mathbf{N}}$ is convergent, and its limit belongs to $\bar{\mathbf{Q}}_p$. Then $\lim_{n\to\infty} P_n'(t) = 0$.*

Proof of Corollary 4. Denote $\beta = \lim_{n\to\infty} P_n(t) \in \bar{\mathbf{Q}}_p$, and let $f_\beta(X)$ be the monic minimal polynomial of β over $\mathbf{Q}_p$. Then one has

$$0 = f_\beta(\beta) = f_\beta(\lim_{n\to\infty} P_n(t)) = \lim_{n\to\infty} f_\beta(P_n(t)). \tag{3.5}$$

By Corollary 2, with $P_n(X)$ replaced by $f_\beta(P_n(X))$, it follows from (3.5) that

$$0 = \lim_{n\to\infty} (f_\beta \circ P_n)'(t) = \lim_{n\to\infty} \Big(f_\beta'(P_n(t)) \cdot P_n'(t)\Big). \tag{3.6}$$

Since

$$\lim_{n\to\infty} f_\beta'(P_n(t)) = f_\beta'\Big(\lim_{n\to\infty} P_n(t)\Big) = f_\beta'(\beta) \neq 0, \tag{3.7}$$

by (3.6) and (3.7) we obtain

$$\lim_{n\to\infty} P_n'(t) = 0,$$

which completes the proof of Corollary 4.

Proof of Theorem 10. The proof goes in three steps. The first step is to show that Theorem 10 is implied by Corollary 2. The second step deals with the particular case of Corollary 2 when the sequence $(P_n(X))_{n\in\mathbf{N}}$ is a distinguished sequence of polynomials associated to t. In the third step we consider a general sequence of polynomials $(P_n(X))_{n\in\mathbf{N}}$ in $\mathbf{Z}_p[X]$ with $\lim_{n\to\infty} P_n(t) = 0$, and complete the proof of the theorem.

We now proceed with the first step. Assume that Corollary 2 holds true and prove that Theorem 10 also holds true. Fix an element $t \in O_{\mathbf{C}_p}$, t transcendental over $\mathbf{Q}_p$. Let $(t_n)_{n\in\mathbf{N}}$ be a sequence of elements in $\mathbf{C}_p$ with $\lim_{n\to\infty} t_n = t$, and choose a sequence of polynomials $(P_n(X))_{n\in\mathbf{N}}$ in $\mathbf{Z}_p[X]$ which satisfies (3.1). For each $n \in \mathbf{N}$, we write

$$P_n(X) = a_{n,0}X^{d_n} + a_{n,1}X^{d_n-1} + \cdots + a_{n,d_n},$$

with $a_{n,0}, a_{n,1}, \ldots, a_{n,d_n} \in \mathbf{Z}_p$, $a_{n,0} \neq 0$. Note that $t_n \in O_{\mathbf{C}_p}$ for n large enough. Since

$$v(P_n(t_n) - P_n(t)) = v\Big(\sum_{j=0}^{d_n-1} a_{n,j}(t_n^{d_n-j} - t^{d_n-j})\Big)$$

$$\geq \min_{0\leq j\leq d_n-1} \Big(v(a_{n,j}) + v(t_n^{d_n-j} - t^{d_n-j})\Big) \geq \min_{0\leq j\leq d_n-1} v(t_n^{d_n-j} - t^{d_n-j}) \geq v(t_n - t),$$

which tends to ∞ as $n \to \infty$, and since $P_n(t_n) \to 0$ as $n \to \infty$, it follows that $P_n(t) \to 0$ as $n \to \infty$. Then Corollary 2 implies that $P_n'(t) \to 0$ as $n \to \infty$. Combining this with the inequalities

$$v(P_n'(t_n) - P_n'(t)) = v\Big(\sum_{j=0}^{d_n-2}(d_n - j)a_{n,j}(t_n^{d_n-j-1} - t^{d_n-j-1})\Big)$$

$$\geq \min_{0\leq j\leq d_n-2}\Big(v(d_n - j) + v(a_{n,j}) + v(t_n^{d_n-j-1} - t^{d_n-j-1})\Big) \geq v(t_n - t),$$

we find that $P_n'(t_n) \to 0$ as $n \to \infty$. In conclusion Theorem 10 follows from Corollary 2.

In order to prove Corollary 2, let us fix a transcendental element $t \in O_{\mathbf{C}_p}$ as before, and let us first consider the particular case when $P_n(X) = f_{\alpha_n}(X)$ for any $n \in \mathbf{N}$, where $(\alpha_n)_{n\in\mathbf{N}}$ is a distinguished sequence with $\lim_{n\to\infty}\alpha_n = t$, and for each n, $f_{\alpha_n}(X)$ denotes the monic minimal polynomial of α_n over $\mathbf{Q}_p$. We need to show that $f_{\alpha_n}'(t) \to 0$ as $n \to \infty$. By an argument as above we know that

$$v(f_{\alpha_n}'(t) - f_{\alpha_n}'(\alpha_n)) \geq v(t - \alpha_n), \tag{3.8}$$

for any $n \in \mathbf{N}$. If $\alpha_{n,1} = \alpha_n, \alpha_{n,2}, \ldots, \alpha_{n,d_n}$ denote the conjugates of α_n over $\mathbf{Q}_p$, then, since $v(\alpha_n - \alpha_{n,j}) \geq 0$ for any j, we see that

$$v(f_{\alpha_n}'(\alpha_n)) = v\Big(\prod_{j=2}^{d_n}(\alpha_n - \alpha_{n,j})\Big) = \sum_{j=2}^{d_n} v(\alpha_n - \alpha_{n,j}) \tag{3.9}$$

$$\geq \max_{2\leq j\leq d_n} v(\alpha_n - \alpha_{n,j}).$$

Let $G = Gal_{cont}(\mathbf{C}_p/\mathbf{Q}_p)$, the group of continuous automorphisms of $\mathbf{C}_p$ over $\mathbf{Q}_p$, which is canonically isomorphic to $Gal(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$. The map from G to $\mathbf{C}_p$ given by $\sigma \mapsto \sigma(t)$ is continuous, and its image $C(t) = \{\sigma(t) : \sigma \in G\}$ is a compact subset of $\mathbf{C}_p$. Fix an $\epsilon > 0$, and cover $C(t)$ with a finite union of balls of radius ϵ, say $C(t) \subseteq \cup_{1\leq i\leq N_\epsilon} B_i$. The element t belongs to at least one of these balls, say $t \in B_1$. Then, for all large n, α_n will belong to B_1. Note also that if n is large enough so that $\deg \alpha_n > N_\epsilon$, there will be two distinct conjugates of α_n, say $\alpha_{n,r}$ and $\alpha_{n,s}$, which belong to the same ball B_i. Since any continuous automorphism of $\mathbf{C}_p$ over $\mathbf{Q}_p$ is an isometry, if we choose $\sigma \in G$ such that $\sigma(\alpha_n) = \alpha_{n,r}$, then $\sigma^{-1}(\alpha_{n,s})$ is a conjugate of α_n, distinct from α_n, which belongs to B_1. By letting $\epsilon \to 0$, and choosing n large enough in terms of ϵ, we deduce that the far right side of (3.9) goes to ∞ as $n \to \infty$. Therefore $f_{\alpha_n}'(\alpha_n) \to 0$ as $n \to \infty$, and combining this with (3.8), it follows that $f_{\alpha_n}'(t) \to 0$ as $n \to \infty$.

We now turn to the general case of Corollary 2. Fix a transcendental element $t \in O_{\mathbf{C}_p}$ as before, and let $\big(P_k(X)\big)_{k\in\mathbf{N}}$ be a sequence of polynomials in $\mathbf{Z}_p[X]$ such that $P_k(t) \to 0$ as $k \to \infty$. We need to show that $P_k'(t) \to 0$ as $k \to \infty$. We know from Theorem 5 that there exists a distinguished sequence $(\alpha_n)_{n\in\mathbf{N}}$ over $\mathbf{Q}_p$ such that $\lim_{n\to\infty}\alpha_n = t$, and from Theorems 7, 8 and 9 we know that the corresponding sequence $(M_n)_{n\in\mathbf{N}}$ forms an integral basis over $\mathbf{Q}_p$ of the topological closure of $\mathbf{Q}_p(t)$ in $\mathbf{C}_p$. Here for each $n \in \mathbf{N}$ we denote by $f_n(X)$ the monic minimal polynomial of

α_n. Then define, for $\mathbf{s} \in \mathcal{A}$, $H_\mathbf{s}(X)$, $q_\mathbf{s}$, $M_\mathbf{s}(X)$, and arrange the elements $M_\mathbf{s}(t)$, $\mathbf{s} \in \mathcal{A}$ in a sequence $(M_n)_{n\in\mathbf{N}}$, as in the previous section.

Next, we write each of the elements $P_k(t)$ in terms of this basis,

$$P_k(t) = \sum_{\mathbf{s}\in\mathcal{A}} a_{k,\mathbf{s}} M_\mathbf{s}(t). \tag{3.10}$$

Then

$$v(P_k(t)) = \min_{\mathbf{s}\in\mathcal{A}} \big(v(a_{k,\mathbf{s}}) + v(M_\mathbf{s}(t))\big). \tag{3.11}$$

Let us note, as a consequence of (3.11) and of the inequality $v(M_\mathbf{s}(t)) < 1$, for any $\mathbf{s} \in \mathcal{A}$, that

$$v(a_{k,\mathbf{s}}) \geq v(P_k(t)) - 1, \tag{3.12}$$

for any $\mathbf{s} \in \mathcal{A}$.

Since $P_k(X) \in \mathbf{Z}_p[X]$, and since each of the polynomials $f_j(X)$, $j \in \mathbf{N}$, is monic, with coefficients in $\mathbf{Z}_p$, which in turn implies that each polynomial $H_\mathbf{s}$, $\mathbf{s} \in \mathcal{A}$, is monic, with coefficients in $\mathbf{Z}_p$, it is easy to see that each polynomial $P_k(X)$ has a representation of the form

$$P_k(X) = \sum_{\mathbf{s}\in\mathcal{A}} c_{k,\mathbf{s}} H_\mathbf{s}(X), \tag{3.13}$$

with $c_{k,\mathbf{s}} \in \mathbf{Z}_p$ for any $\mathbf{s} \in \mathcal{A}$, and $c_{k,\mathbf{s}} = 0$ for any $\mathbf{s} = (s_0, s_1, \dots, s_n, \dots) \in \mathcal{A}$ for which $\sum_{n\in\mathbf{N}} s_n \deg f_n(X) > \deg P_k(X)$. Thus, if n_k is the largest positive integer for which $\deg f_{n_k}(X) \leq \deg P_k(X)$, then any $\mathbf{s} \in \mathcal{A}$ which appears with a nonzero coefficient $c_{k,\mathbf{s}}$ on the right side of (3.13), has the form $\mathbf{s} = (s_0, s_1, \dots, s_n, \dots)$, with $s_n = 0$ for $n > n_k$. By (3.10), (3.13) and the definition of $H_\mathbf{s}(X)$, $q_\mathbf{s}$ and $M_\mathbf{s}(X)$, we see that for any $\mathbf{s} \in \mathcal{A}$, $q_\mathbf{s}$ is a nonnegative integer and $a_{k,\mathbf{s}} = p^{q_\mathbf{s}} c_{k,\mathbf{s}}$.

Let us note that for any $m \in \mathbf{N}$, there exists an element $\mathbf{s}(m) \in \mathcal{A}$ such that any $\mathbf{s} \in \mathcal{A}$ with $\mathbf{s} > \mathbf{s}(m)$, $\mathbf{s} = (s_0, s_1, \dots, s_n, \dots)$, has at least one nonzero component s_n for which $n > m$. Then, for each $\mathbf{s} \in \mathcal{A}$ with $\mathbf{s} > \mathbf{s}(m)$, $H_\mathbf{s}(X)$ will have at least one factor of the form $f_{m+i}(X)$, with $i \geq 1$.

Let now L be an arbitrary positive number, and choose a positive integer $m(L)$ such that for any $m > m(L)$ one has simultaneously that $v(f_m(t)) > L$ and $v(f'_m(t)) > L$. Here for this last inequality one uses the second step in our proof, which proved Corollary 2 in the particular case of a distinguished sequence of polynomials associated to t.

Next, we consider the finite set

$$\mathcal{A}_1 = \{\mathbf{s} \in \mathcal{A} : \mathbf{s} \leq \mathbf{s}(m(L))\}.$$

Let $q = \max\{q_\mathbf{s} : \mathbf{s} \in \mathcal{A}_1\}$. Since $P_k(t) \to 0$, there exists $k_q \in \mathbf{N}$, such that for any $k > k_q$, one has $v(P_k(t)) > 1 + q + L$. Then, using (3.12), we see that for any $k > k_q$ and any $s \in \mathcal{A}_1$, one has

$$v(c_{k,\mathbf{s}}) = v\Big(\frac{a_{k,\mathbf{s}}}{p^{q_\mathbf{s}}}\Big) \geq v(P_k(t)) - 1 - q > L. \tag{3.14}$$

Let now $k > \max\{k_q, m(L)\}$. By (3.13) we have

$$P_k'(t) = \sum_{\mathbf{s}\in\mathcal{A}_1} c_{k,\mathbf{s}} H_{\mathbf{s}}'(t) + \sum_{\mathbf{s}>\mathbf{s}(m(L))} c_{k,\mathbf{s}} H_{\mathbf{s}}'(t). \tag{3.15}$$

Clearly $v(H_{\mathbf{s}}'(t)) \geq 0$ for any $\mathbf{s} \in \mathcal{A}$, since each polynomial $H_{\mathbf{s}}(X)$ has coefficients in $\mathbf{Z}_p$. Therefore, by (3.14), we find that

$$v\Big(\sum_{\mathbf{s}\in\mathcal{A}_1} c_{k,\mathbf{s}} H_{\mathbf{s}}'(t)\Big) \geq \min_{\mathbf{s}\in\mathcal{A}_1} v(c_{k,\mathbf{s}}) > L. \tag{3.16}$$

In order to deal with the second sum on the right side of (3.15), recall that each coefficient $c_{k,\mathbf{s}}$ belongs to $\mathbf{Z}_p$, hence

$$v\Big(\sum_{\mathbf{s}>\mathbf{s}(m(L))} c_{k,\mathbf{s}} H_{\mathbf{s}}'(t)\Big) \geq \inf_{\mathbf{s}>\mathbf{s}(m(L))} v(H_{\mathbf{s}}'(t)). \tag{3.17}$$

Let us also recall that for each $\mathbf{s} > \mathbf{s}(m(L))$, the polynomial $H_{\mathbf{s}}(X)$ factors as a product of polynomials $f_j(X)$, which appear with various multiplicities in $H_{\mathbf{s}}(X)$, but such that at least one factor has the form $f_{m(L)+i}(X)$, with $i \geq 1$. Therefore $H_{\mathbf{s}}'(X)$ will equal a sum, in which each term is a product of factors of the form $f_j(X)$, and exactly one factor of the form $f_j'(X)$. All these factors are polynomials with coefficients in $\mathbf{Z}_p$. Moreover, in each term as above, we have at least one factor of the form $f_{m(L)+i}(X)$, or of the form $f_{m(L)+i}'(X)$, with $i \geq 1$. We deduce that for any $\mathbf{s} > \mathbf{s}(m(L))$,

$$v(H_{\mathbf{s}}'(t)) \geq \inf_{i\geq 1} \min\{v(f_{m(L)+i}(t)), v(f_{m(L)+i}'(t))\}. \tag{3.18}$$

By our choice of $m(L)$ it follows that the right side of (3.18) is $\geq L$. Using this bound in (3.17), we obtain

$$v\Big(\sum_{\mathbf{s}>\mathbf{s}(m(L))} c_{k,\mathbf{s}} H_{\mathbf{s}}'(t)\Big) \geq L. \tag{3.19}$$

Relations (3.15), (3.16) and (3.19) imply that

$$v(P_k'(t)) \geq L, \tag{3.20}$$

for any $k > \max\{k_q, m(L)\}$. We now let $L \to \infty$, and then from (3.20) it follows that $P_k'(t) \to 0$ as $k \to \infty$. This completes the proof of the theorem.

We end the paper with an application, concerning elements $\beta \in O_{\bar{\mathbf{Q}}_p}$ for which the differential $d\beta$ vanishes. Let $K = \mathbf{Q}_p^{ur}$ be the maximal unramified extension of $\mathbf{Q}_p$ in $\bar{\mathbf{Q}}_p$, and let L be any algebraic (finite or infinite) extension of K in $\bar{\mathbf{Q}}_p$, which is not deeply ramified over K. Consider the module Ω_{O_L/O_K} of differentials of O_L over O_K, where O_K and O_L denote the ring of integers in K and L respectively, and let d denote the canonical derivation $d : O_L \to \Omega_{O_L/O_K}$. This map has various subtle arithmetical properties (see for instance the Appendix of [5]). If L/K is not deeply ramified then Ω_{O_L/O_K} is annihilated by a suitable power of p (see [7], Theorem 2.2). In this case the above map d is locally constant on O_L, and hence it can be extended by continuity to a map $d : O_E \to \Omega_{O_L/O_K}$, where E denotes the topological closure of L in $\mathbf{C}_p$, and O_E denotes the ring of integers in E.

We remark in passing that if one replaces L by the entire field $\bar{\mathbf{Q}}_p$, which is deeply ramified over K, then one can not extend the canonical derivation $d : O_{\bar{\mathbf{Q}}_p} \to \Omega_{O_{\bar{\mathbf{Q}}_p}/O_K}$ by continuity, from $O_{\bar{\mathbf{Q}}_p}$ to $O_{\mathbf{C}_p}$.

Returning to our extension L/K which is not deeply ramified, we know that there exists an element $t \in O_E$, t transcendental over $\mathbf{Q}_p$, such that the topological closure of the ring $\mathbf{Q}_p[t]$ in $\mathbf{C}_p$, coincides with E. Therefore any element of E, and in particular any element of L, is the limit of a sequence of the form $(P_n(t))_{n\in\mathbf{N}}$, where $P_n(X) \in \mathbf{Q}_p[X]$ for any $n \in \mathbf{N}$. This does not mean, and in general it is not true, that any element of O_E is the limit of a sequence of the form $(P_n(t))_{n\in\mathbf{N}}$, with $P_n(X) \in \mathbf{Z}_p[X]$ for any $n \in \mathbf{N}$. Thus, if we take an element $t \in O_E$, t transcendental over $\mathbf{Q}_p$, and if we denote by A_t the topological closure of the ring $\mathbf{Z}_p[t]$ in $\mathbf{C}_p$, then A_t will be a closed subring of $\mathbf{C}_p$ which in general will be strictly contained in O_E. Let β be an element of A_t which is algebraic over $\mathbf{Q}_p$. By Galois theory in $\mathbf{C}_p$ (see [3], [13], [14]), we know that any algebraic element of E belongs to L. Thus $\beta \in A_t \cap O_L$. We claim that β belongs to the kernel of the canonical derivation $d : O_L \to \Omega_{O_L/O_K}$. Indeed, choose a sequence of polynomials $(P_n(X))_{n\in\mathbf{N}}$ in $\mathbf{Z}_p[X]$ such that $P_n(t) \to \beta$ as $n \to \infty$. By the continuity of the map d on O_E, we have that $d(P_n(t)) \to d\beta$, as $n \to \infty$. Now, for each $n \in \mathbf{N}$ we have $d(P_n(t)) = P_n'(t)dt$. Since the sequence $(P_n(t))_{n\in\mathbf{N}}$ converges to β, which is algebraic over $\mathbf{Q}_p$, by Corollary 4 it follows that $P_n'(t) \to 0$ as $n \to \infty$. Therefore

$$d\beta = \lim_{n\to\infty} d(P_n(t)) = \lim_{n\to\infty} P_n'(t)dt = 0 \cdot dt = 0,$$

which proves the claim. We have obtained the following result.

Corollary 5. *Let L be an algebraic extension of $K = \mathbf{Q}_p^{ur}$, L not deeply ramified over K. Let E be the topological closure of L in $\mathbf{C}_p$, let $t \in O_E$, t transcendental over $\mathbf{Q}_p$, and denote by A_t the topological closure of $\mathbf{Z}_p[t]$ in $\mathbf{C}_p$. Then the ring $A_t \cap O_L$ is contained in the kernel of the canonical derivation $d : O_L \to \Omega_{O_L/O_K}$.*

References

[1] V. Alexandru, N. Popescu and A. Zaharescu, *On the closed subfields of* $\mathbf{C}_p$, J. Number Theory **68** (1998), no. 2, 131–150.

[2] V. Alexandru, N. Popescu and A. Zaharescu, *The generating degree of* $\mathbf{C}_p$, Canad. Math. Bull. **44** (2001), no. 1, 3–11.

[3] J. Ax, *Zeros of Polynomials Over Local Fields. The Galois Action*, J. Algebra **15** (1970), 417–428.

[4] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), no. 1-3, 129–174.

[5] J.-M. Fontaine, *Le corps des périodes p-adique (avec une appendice par P. Colmez)*, Astérisque **223** (1994), 59-111.

[6] A. Iovita and A. Zaharescu, *Completions of r.a.t.-valued fields of rational functions*, J. Number Theory **50** (1995), no. 2, 202–205.

[7] A. Iovita and A. Zaharescu, *Galois theory of* B_{dR}^+, Compositio Math. **117** (1999), no. 1, 1–31.

[8] K. Okutsu, *Construction of Integral Basis I - IV*, Proc. Japan Acad. Ser. A Math. Sci. **58** (1982), 47–49, 87–89, 117–119, 167–169.

[9] K. Okutsu, *Integral Basis of the Field* $Q(\sqrt[\ell]{a})$, Proc. Japan Acad. Ser. A Math. Sci. **58** (1982), 219–222.

[10] K. Ota, *On saturated distinguished chains over a local field*, J. Number Theory **79** (1999), no. 2, 217–248.
[11] A. Popescu, N. Popescu, M. Vajaitu and A. Zaharescu, *Chains of metric invariants over a local field*, Acta Arith. **103** (2002), no. 1, 27–40.
[12] N. Popescu and A. Zaharescu, *On the structure of the irreducible polynomials over local fields*, J. Number Theory **52** (1995), no. 1, 98–118.
[13] S. Sen, *On Automorphisms of local fields*, Ann. of Math. **90** (1969), 33–46.
[14] J. Tate, *p-divisible groups*, 1967 Proc. Conf. Local Fields (Driebergen, 1966) pp. 158–183 Springer, Berlin.

V. ALEXANDRU: UNIVERSITY OF BUCHAREST, DEPARTMENT OF MATHEMATICS, STR. ACADEMIEI 14, RO-70109, BUCHAREST, ROMANIA

A. ZAHARESCU: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 1409 W. GREEN STREET, URBANA, IL, 61801, USA
E-mail address: `zaharesc@math.uiuc.edu`

Received May 7, 2003 Revised October 9, 2003