Proceedings of the Edinburgh Mathematical Society (2016) **59**, 1–10
DOI:10.1017/S0013091514000376

ON p-ADIC ANALYTIC CONTINUATION WITH APPLICATIONS TO GENERATING ELEMENTS

VICTOR ALEXANDRU[1], MARIAN VÂJÂITU[2] AND ALEXANDRU ZAHARESCU[3]

[1] *Department of Mathematics, University of Bucharest, 14 Academiei Street, 010014 Bucharest, Romania*
[2] *Simion Stoilow Institute of Mathematics of the Romanian Academy, Research Unit 5, PO Box 1-764, 014700 Bucharest, Romania* (marian.vajaitu@imar.ro)
[3] *Department of Mathematics, University of Illinois at Urbana-Champaign, Altgeld Hall, 1409 W Green Street, Urbana, IL 61801, USA*

(Received 11 December 2012)

Dedicated to the memory of Professor Nicolae Popescu

Abstract Given a prime number p and the Galois orbit $O(T)$ of an integral transcendental element T of $\mathbb{C}_p$, the topological completion of the algebraic closure of the field of p-adic numbers, we study the p-adic analytic continuation around $O(T)$ of functions defined by limits of sequences of restricted power series with p-adic integer coefficients. We also investigate applications to generating elements for $\mathbb{C}_p$ or for some classes of closed subfields of $\mathbb{C}_p$.

Keywords: p-adic analytic functions; local fields; generating elements

2010 *Mathematics subject classification:* Primary 11S99

1. Introduction

Let p be a prime number, let $\mathbb{Z}_p$ be the ring of p-adic integers, let $\mathbb{Q}_p$ be the field of p-adic numbers, let $\bar{\mathbb{Q}}_p$ be a fixed algebraic closure of $\mathbb{Q}_p$ and let $\mathbb{C}_p$ be the completion of $\bar{\mathbb{Q}}_p$ with respect to the p-adic valuation. Denote by $O(T)$ the orbit of an element $T \in \mathbb{C}_p$ with respect to the Galois group $\mathrm{G} = \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/\mathbb{Q}_p)$. In this paper we study the p-adic analytic continuation around $O(T)$ of functions defined by limits of sequences of restricted power series with p-adic integer coefficients. We also provide applications to generating elements for some closed subfields of $\mathbb{C}_p$. Generating elements are quite useful in the study of $\mathbb{C}_p$ and its closed subfields. It is a non-trivial fact that $\mathbb{C}_p$ has a generating element over $\mathbb{Q}_p$, that is, there exists an element T of $\mathbb{C}_p$ (which is necessarily transcendental over $\mathbb{Q}_p$) for which the ring $\mathbb{Q}_p[T]$ is dense in $\mathbb{C}_p$ (see [**4**, Theorem 1]). This means that $\mathbb{C}_p$ can be viewed as the completion of the ring of polynomials in one variable over $\mathbb{Q}_p$ with respect to a suitable absolute value. In order to better understand how this absolute value works on this polynomial ring, one usually makes use of so-called saturated distinguished chains associated with the given generating element T. Generating elements and distinguished chains have been intensively studied in various contexts. For more on these topics the reader is referred to [**2**, **4**, **5**, **11**, **12**, **15**–**25**, **28**]. Here we restrict ourselves to explaining the basic reason why these two entirely different topics, concerned with generating elements and, respectively, distinguished chains, connect naturally with each other. Let us consider the simple case of a finite field extension K of $\mathbb{Q}_p$. Oversimplifying things, we could say that one of the two topics mentioned above, namely, the one concerning generating elements, aims at producing (explicitly, if possible) generating elements T of K over $\mathbb{Q}_p$. In this case the condition simply means that K is obtained by adjoining T to $\mathbb{Q}_p$. Then $1, T, \dots, T^{[K:\mathbb{Q}_p]-1}$ form a basis of K over $\mathbb{Q}_p$ and each element α of K can be uniquely written as a linear combination $\alpha = \sum_{0 \leqslant j \leqslant [K:\mathbb{Q}_p]} c_j T^j$ with coefficients in $\mathbb{Q}_p$. This does not immediately enable one to compute the p-adic valuation of α. Now, if T comes equipped with an associated saturated distinguished chain, then one can replace the above basis $\{1, T, \dots, T^{[K:\mathbb{Q}_p]-1}\}$ by a more convenient basis defined in terms of the given saturated distinguished chain, which enables one to compute the valuation of any element of K (see, for example, [**23**, Remark 4.7]). This explains the relationship between generating elements and saturated distinguished chains. It also shows that for papers such as the present one and others, where applications to generating elements are presented, a natural further problem that arises would be to investigate the saturated distinguished chains associated with those generating elements. Returning to the content of this paper, § 2 contains notation and some basic results. In § 3 we consider a sequence $\{f_n\}_{n \geqslant 1}$ of restricted power series with p-adic integer coefficients. If T_n is a sequence in $\mathbb{C}_p$ that converges to an element T that is a p-adic integral element of $\mathbb{C}_p$, and such that $f_n(T_n)$ converges to $f(T)$, then f defines a G-equivariant continuous function on $O(T)$ that has a unique G-equivariant analytic continuation around $O(T)$ (see Theorem 3.1). For an application, in Corollary 3.4 we show that $\widetilde{\mathbb{Z}_p[T]} \cap \bar{\mathbb{Q}}_p$ is a $\mathbb{Z}_p$-module of finite rank, where $\widetilde{\mathbb{Z}_p[T]}$ is the topological closure of $\mathbb{Z}_p[T]$ in $\mathbb{C}_p$. In the final section we present some applications to generating elements for $\mathbb{C}_p$ and for some classes of closed subfields of $\mathbb{C}_p$ (see Theorems 4.1, 4.3 and 4.5 and Corollaries 4.2, 4.4 and 4.6).

2. Background material

Let p be a prime number and let $\mathbb{Q}_p$ be the field of p-adic numbers endowed with the p-adic absolute value $|\cdot|$, normalized such that $|p| = 1/p$. Also, we denote by v_p the p-adic valuation. Let $\bar{\mathbb{Q}}_p$ be a fixed algebraic closure of $\mathbb{Q}_p$ and denote by the same symbol $|\cdot|$ the unique extension of $|\cdot|$ to $\bar{\mathbb{Q}}_p$. Furthermore, denote by $(\mathbb{C}_p, |\cdot|)$ the completion of $(\bar{\mathbb{Q}}_p, |\cdot|)$ (see [**6**, **7**]) and by $O_{\mathbb{C}_p}$ the ring of integers of $\mathbb{C}_p$. Consider the Galois group $\mathrm{G} = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ endowed with the Krull topology. The group G is canonically isomorphic with the group $\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/\mathbb{Q}_p)$ of all continuous automorphisms of $\mathbb{C}_p$ over $\mathbb{Q}_p$ (see, for example, [**3**, p. 17]). We shall identify these two groups. For any $T \in \mathbb{C}_p$ denote by $O(T) = \{\sigma(T) \colon \sigma \in \mathrm{G}\}$ the orbit of T and let $\widetilde{\mathbb{Q}_p[T]}$ be the topological closure of the ring $\mathbb{Q}_p[T]$ in $\mathbb{C}_p$.

By Galois theory in $\mathbb{C}_p$, as developed by Tate [**29**], Sen [**27**] and Ax [**8**], the closed subgroups of the Galois group G are in one-to-one correspondence with the closed subfields of $\mathbb{C}_p$. For any closed subgroup H of G denote by $\mathrm{Fix}(H) = \{T \in \mathbb{C}_p \colon$

$\sigma(T) = T$ for all $\sigma \in H\}$. Then $\mathrm{Fix}(H)$ is a closed subfield of $\mathbb{C}_p$. We define $H(T) = \{\sigma \in \mathrm{G} \colon \sigma(T) = T\}$. We then have that $H(T)$ is a closed subgroup of G. Also, we have that $\mathrm{Fix}(H(T)) = \widetilde{\mathbb{Q}_p[T]}$. For any $\varepsilon > 0$, $H(T, \varepsilon) := \{\sigma \in \mathrm{G} \colon |\sigma(T) - T| < \varepsilon\}$ is an open subgroup of G of finite index and $[\mathrm{G} : H(T, \varepsilon)] = N(T, \varepsilon)$ is the number of open balls of radius ε that cover $O(T)$. Moreover, when T is transcendental, the set $\{|\sigma(T) - T| \colon \sigma \in \mathrm{G}\}$ is a strictly decreasing sequence $\{\varepsilon_n\}_{n \geqslant 1}$ with limit zero. This sequence is called the fundamental sequence associated with the orbit of T (see [**24**]).

The map $\sigma \rightsquigarrow \sigma(T)$ from G to $O(T)$ is continuous and it defines a homeomorphism from $\mathrm{G}/H(T)$ (endowed with the quotient topology) to $O(T)$ (endowed with the induced topology from $\mathbb{C}_p$) (see [**2**, Remark 3.2 and Theorem 3.5]). In such a way $O(T)$ is a closed compact and totally disconnected subspace of $\mathbb{C}_p$ and the group G acts continuously on $O(T)$: if $\sigma \in \mathrm{G}$ and $\tau(T) \in O(T)$, then $\sigma \star \tau(T) := (\sigma\tau)(T)$.

Definition 2.1. Let $\mathbb{Q}_p \subseteq K$ be a closed subfield of $\mathbb{C}_p$. An element x of $\mathbb{C}_p$ is said to be a *generating element* (or a *generic element*) for K provided that $\widetilde{\mathbb{Q}_p[x]} = K$. (See [**2**, **11**].)

Definition 2.2. The radius of convergence of a power series $f(X) = \sum_{n \geqslant 0} a_n X^n \in \mathbb{C}_p[\![X]\!]$ is the extended real number $0 \leqslant r_f \leqslant \infty$ defined by $r_f = \sup\{r \geqslant 0 \colon |a_n| r^n \to 0\}$.

By Hadamard's formula, one has $r_f = 1/\limsup |a_n|^{1/n}$ (see [**26**, p. 283]).

Definition 2.3. A power series $f \in \mathbb{Z}_p[\![X]\!]$, $f(X) = \sum_{n \geqslant 0} a_n X^n$ with $a_n \in \mathbb{Z}_p$, is called a restricted power series if $\lim_{n \to \infty} a_n = 0$. Denote by $\mathbb{Z}_p\{X\}$ the ring of all restricted power series with p-adic integer coefficients (see [**26**, p. 233]).

In the case of a power series $f \in \mathbb{Z}_p[\![X]\!]$ we have $r_f \geqslant 1$ and f is convergent on $\{z \in \mathbb{C}_p \colon |z| = 1\}$ if and only if $f \in \mathbb{Z}_p\{X\}$.

Definition 2.4. A subset $D \subseteq \mathbb{C}_p$ is G-equivariant provided that $\sigma(x) \in D$ for any $x \in D$ and any $\sigma \in \mathrm{G}$. (An example is $D = O(x)$, where $x \in \mathbb{C}_p$.)

Definition 2.5. An analytic function f defined on a G-equivariant subset D of $\mathbb{C}_p$ is G-equivariant if $f(\sigma(x)) = \sigma(f(x))$ for any $x \in D$ and any $\sigma \in \mathrm{G}$.

We now recall the following result.

Theorem 2.6 (Alexandru and Zaharescu [1, Theorem 10]). *Let T be a transcendental element of $O_{\mathbb{C}_p}$. Then, for any sequence $\{T_n\}_{n \in \mathbb{N}}$ in $\mathbb{C}_p$ with $\lim_{n \to \infty} T_n = T$ and any sequence of polynomials $\{P_n(X)\}_{n \in \mathbb{N}}$ in $\mathbb{Z}_p[X]$ such that $\lim_{n \to \infty} P_n(T_n) = 0$, one has $\lim_{n \to \infty} P_n'(T_n) = 0$.*

3. On p-adic analytic continuation

Let T be a transcendental element of $O_{\mathbb{C}_p}$. For any positive integer n, let $P_n \in \mathbb{Z}_p[X]$ be a polynomial with p-adic integer coefficients such that the sequence $\{P_n(T)\}_{n \geqslant 1}$ is convergent. Define

$$u(T) = \lim_{n \to \infty} P_n(T) \in \widetilde{\mathbb{Z}_p[T]} \subseteq \mathbb{C}_p.$$

As a consequence of Theorem 2.6, we have a well-defined element

$$u^{(k)}(T) := \lim_{n\to\infty} P_n^{(k)}(T)$$

for any $k \geqslant 1$. Indeed, let us define $Q_n = P_{n+1} - P_n \in \mathbb{Z}_p[X]$. One has $\lim_{n\to\infty} Q_n(T) = 0$ so $\lim_{n\to\infty} Q'_n(T) = 0$ and by this we have that the sequence $\{P'_n(T)\}$ is convergent to an element $u'(T) \in \mathbb{Z}_p[T]$. The same is true for any $k \geqslant 1$. In what follows we will see that the element $u = u(T)$ defines, in a natural way, a G-equivariant analytic function $u\colon B[O(T), |p|^{1+\varepsilon}] \to \mathbb{C}_p$, where, for any $\varepsilon > 0$,

$$B[O(T), |p|^{1+\varepsilon}] := \{z \in \mathbb{C}_p \colon \operatorname{dist}(z, O(T)) \leqslant |p|^{1+\varepsilon}\}.$$

One has a more general result.

Theorem 3.1. *Let T be an integral transcendental element of $\mathbb{C}_p$ and let $\{T_n\}_{n\geqslant 1}$ be a sequence of elements of $\mathbb{C}_p$ such that T_n converges to T. Let $\{f_n\}_{n\geqslant 1}$ be a sequence of power series of $\mathbb{Z}_p[\![X]\!]$ such that for n large enough $f_n(T_n)$ exists and converges to $f = f(T) \in \mathbb{C}_p$. Then f defines a* G*-equivariant continuous function on $O(T)$ that has a unique* G*-equivariant analytic continuation to $B[O(T), |p|^{1+\varepsilon}]$ for any $\varepsilon > 0$.*

Proof. For the sake of simplicity we suppose that $|T_n| = |T|$ and that $f_n(T_n)$ exists for any $n \geqslant 1$. For the case in which $|T| = 1$ the existence and convergence of $f_n(T_n)$ means that $f_n \in \mathbb{Z}_p\{X\}$. Let us see that $f_n(T)$ is a convergent sequence with limit $f(T)$. Indeed, let us write f_n in the form

$$f_n(X) = \sum_{k\geqslant 0} a_k^{(n)} X^k, \quad a_k^{(n)} \in \mathbb{Z}_p. \tag{3.1}$$

From (3.1) one has

$$|f_n(T_n) - f_n(T)| = \left|\sum_{k\geqslant 0} a_k^{(n)}(T_n^k - T^k)\right| \leqslant |T_n - T|, \tag{3.2}$$

which converges to zero as n tends to infinity. Since $\lim_{n\to\infty} f_n(T_n) = f(T)$, we also have $\lim_{n\to\infty} f_n(T) = f(T)$.

Fix now an $\varepsilon > 0$ and define $g_n = f_{n+1} - f_n \in \mathbb{Z}_p[\![X]\!]$. To show that the sequence $\{f_n(z)\}_{n\in\mathbb{N}}$ is uniformly convergent on $B[T, |p|^{1+\varepsilon}]$, it is enough to prove that the sequence $\{g_n(z)\}_{n\in\mathbb{N}}$ converges uniformly to zero. We write g_n as a Taylor series about T,

$$g_n(z) = \sum_{k\geqslant 0} \frac{(z-T)^k}{k!} g_n^{(k)}(T). \tag{3.3}$$

We have that

$$v_p(k!) = \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \cdots < \frac{k}{p-1},$$

so

$$v_p\left(\frac{(z-T)^k}{k!}\right) > k(1+\varepsilon) - \frac{k}{p-1} = k\left(1 + \varepsilon - \frac{1}{p-1}\right) \geqslant k\varepsilon.$$

https://doi.org/10.1017/S0013091514000376 Published online by Cambridge University Press

From this inequality and (3.3) one obtains

$$|g_n(z)| \leqslant \sup_{k \geqslant 0}\{|p|^{k\varepsilon}|g_n^{(k)}(T)|\}. \tag{3.4}$$

By the p-adic Weierstrass preparation theorem, we can decompose g_n in the form

$$g_n = P_n \cdot h_n, \tag{3.5}$$

where $P_n \in \mathbb{Z}_p[X]$ and $h_n \in 1 + X\mathbb{Z}_p[\![X]\!]$. Moreover, h_n converges on $B[0, |T|]$, which is the closed ball of centre 0 and radius $|T|$, has no zeros on this ball and $\|h_n\|_{B[0,|T|]} = |h_n(x)| = 1$ for any $x \in B[0, |T|]$ (see also [**9**, Propositions 5.1.4.3 and 5.1.3.1]). Since $\lim_{n\to\infty} g_n(T) = 0$, by the above decomposition one has that $\lim_{n\to\infty} P_n(T) = 0$. From Theorem 2.6, $\lim_{n\to\infty} P_n'(T) = 0$ so $\lim_{n\to\infty} g_n'(T) = 0$. By repeating this argument, we have that

$$\lim_{n\to\infty} |g_n^{(k)}(T)| = 0 \quad \text{for any } k \geqslant 0. \tag{3.6}$$

Now, let us consider an arbitrary $\delta > 0$. There exists $k_1(\delta) \in \mathbb{N}$ such that $|p|^{k\varepsilon} < \delta$ for any $k \geqslant k_1(\delta)$, which means that $|p|^{k\varepsilon}|g_n^{(k)}(T)| < \delta$ for any $k \geqslant k_1(\delta)$ and any $n \in \mathbb{N}$. From (3.6) there exists $n(\delta) \in \mathbb{N}$ such that $|p|^{k\varepsilon}|g_n^{(k)}(T)| < \delta$ for any $0 \leqslant k < k_1(\delta)$ and any $n \geqslant n(\delta)$. It is easy to see that one has $|p|^{k\varepsilon}|g_n^{(k)}(T)| < \delta$ for any $k \geqslant 0$ and any $n \geqslant n(\delta)$. By (3.4), we have that $|g_n(z)| \leqslant \delta$ for any $n \geqslant n(\delta)$ and any $z \in B[T, |p|^{1+\varepsilon}]$. It is clear that

$$|f_m(z) - f_n(z)| \leqslant \delta \quad \text{for any } m, n \geqslant n(\delta) \text{ and any } z \in B[T, |p|^{1+\varepsilon}].$$

This means that the sequence $\{f_n\}_{n\geqslant 1}$ is Cauchy in the sup norm, which is the same as the Gauss norm in this case. Since the ring of analytic functions defined on $B[T, |p|^{1+\varepsilon}]$ is complete with respect to this norm (see [**10**, pp. 13–22] and [**26**, pp. 339–350]), one obtains that $f(z) = \lim_{n\to\infty} f_n(z)$ is analytic and G-equivariant on $B[O(T), |p|^{1+\varepsilon}]$. In fact, f_n has the following expansion about T:

$$f_n(z) = \sum_{k\geqslant 0} D^k f_n(T)(z - T)^k, \quad z \in B[T, |p|^{1+\varepsilon}],$$

with $D^k f_n(T) \in \widetilde{\mathbb{Z}_p[T]}$, where for a formal power series $F(z) = \sum A_j z^j$, $D^k F(z)$ is the kth Hasse derivative of F, defined by

$$D^k F(z) = \sum_{j\geqslant k} A_j \binom{j}{k} z^{j-k}.$$

The G-equivariant analytic function f, which is defined above, has the following expansion about T:

$$f(z) = \sum_{k\geqslant 0} D^k f(T)(z - T)^k, \quad z \in B[T, |p|^{1+\varepsilon}],$$

with $D^k f(T) \in \widetilde{\mathbb{Z}_p[T]}$. Because T is transcendental and all the points of $O(T)$ are limit points (see [**2**, Theorem 3.5]), the uniqueness of analytic continuation results by the identity theorem. The proof of the theorem is now complete. □

Corollary 3.2. *Let T be a transcendental element of $O_{\mathbb{C}_p}$. For any positive integer n let $P_n \in \mathbb{Z}_p[X]$ be a polynomial with p-adic integer coefficients such that the limit $u = u(T) := \lim_{n\to\infty} P_n(T)$ exists in $\mathbb{C}_p$. Then u defines a* G*-equivariant continuous function on $O(T)$ that has a unique* G*-equivariant analytic continuation to $B[O(T), |p|^{1+\varepsilon}]$ for any $\varepsilon > 0$.*

From the proof of Theorem 3.1 one has that $f(T)$ is in $\widetilde{\mathbb{Z}_p[T]}$ but it does not have a representation as a series in T with coefficients in $\mathbb{Z}_p$. Let now $\alpha \in \bar{\mathbb{Q}}_p \cap B[T, |p|^{1+\varepsilon}]$. By expanding f about α one has

$$f(z) = \sum_{k\geqslant 0} D^k f(\alpha)(z-\alpha)^k.$$

In particular, for $z = T$ we obtain

$$f(T) = \sum_{k\geqslant 0} D^k f(\alpha)(T-\alpha)^k,$$

where $D^k f(\alpha) \in \mathbb{Z}_p[\alpha]$, so $f(T)$ can be represented as a convergent power series in $T - \alpha$ with coefficients in $\mathbb{Z}_p[\alpha]$. Moreover, if $|T| < |p|$, then $|T| < |p|^{1+\varepsilon}$ for ε small enough and we can choose $\alpha = 0$ to obtain

$$f(T) = \sum_{k\geqslant 0} D^k f(0) T^k \in \mathbb{Z}_p[\![T]\!].$$

Corollary 3.3. *Let T be a transcendental element of $\mathbb{C}_p$ such that $|T| < |p|$. Then,*

$$\widetilde{\mathbb{Z}_p[T]} = \left\{ \sum_{n\geqslant 0} a_n T^n : a_n \in \mathbb{Z}_p \right\}.$$

An interesting application of Theorem 3.1 is the following result.

Corollary 3.4. *Let T be a transcendental element of $O_{\mathbb{C}_p}$. Then $\widetilde{\mathbb{Z}_p[T]} \cap \bar{\mathbb{Q}}_p$ is a $\mathbb{Z}_p$-module of finite rank.*

Proof. Let $u \in \widetilde{\mathbb{Z}_p[T]} \cap \bar{\mathbb{Q}}_p$. By Theorem 3.1, $u = u(T)$ has an analytic continuation on $B[T, |p|^{1+\varepsilon}]$ for any $\varepsilon > 0$. Let P be the minimal polynomial of u over $\mathbb{Q}_p$ (or $\mathbb{Z}_p$) and let $\alpha \in \bar{\mathbb{Q}}_p$ be an algebraic element such that $|T - \alpha| < |p|^{1+\varepsilon}$. By our hypothesis, T is transcendental, so it is a limit point of $O(T) \cap B[T, |p|^{1+\varepsilon}]$ (see [**2**, Theorem 3.5]). Because u is G-equivariant and $P(u(T)) = 0$, by the identity theorem one has that $P(u(z)) = 0$ for any $z \in B[T, |p|^{1+\varepsilon}]$. In particular, $P(u(\alpha)) = 0$, and so $\deg P \leqslant [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$ because $u(\alpha) \in \mathbb{Q}_p(\alpha)$. The degrees of algebraic elements $u(T)$ from $\widetilde{\mathbb{Z}_p[T]}$ are bounded by $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$ so we have that $\widetilde{\mathbb{Z}_p[T]} \cap \bar{\mathbb{Q}}_p$ is included in a finite extension of $\mathbb{Q}_p$ and the corollary is proved. □

Remark 3.5. It is not sure that one can choose $\alpha \in \mathbb{Q}_p^{ur}$ such that $|T - \alpha| < |p|^{1+\varepsilon}$, where $\mathbb{Q}_p^{ur}$ is the maximal unramified extension of $\mathbb{Q}_p$ in $\bar{\mathbb{Q}}_p$. By this, the fact that the differential is zero on $\widetilde{\mathbb{Z}_p[T]} \cap \bar{\mathbb{Q}}_p$ is non-trivial.

https://doi.org/10.1017/S0013091514000376 Published online by Cambridge University Press

Indeed, let $u \in \widetilde{\mathbb{Z}_p[T]} \cap \bar{\mathbb{Q}}_p$. By the proof of Corollary 3.4, we have that $P(u(z)) = 0$ for any $z \in B[T, |p|^{1+\varepsilon}]$, where P is the minimal polynomial of u over $\mathbb{Q}_p$. One obtains that $P'(u(z)) \cdot u'(z) = 0$ and, for $z = T$, one has $P'(u(T)) \cdot u'(T) = 0$ so $P'(u(T)) = 0$ or $u'(T) = 0$. Because u is G-equivariant and $P \in \mathbb{Z}_p[X]$, the functions u' and $P'(u)$ are G-equivariant. But T is transcendental, so it is a limit point of $O(T) \cap B[T, |p|^{1+\varepsilon}]$ and by the identity theorem we have $u' = 0$ or $P'(u) = 0$. We cannot have $P'(u) = 0$ and by this it is clear that u is constant, so it is in $\mathbb{Q}_p$.

4. Applications to generating elements

As we know from the previous section, if T is a transcendental element of $O_{\mathbb{C}_p}$ and $\{f_n\}_{n\geqslant 1}$ is a sequence of power series from $\mathbb{Z}_p[\![X]\!]$ such that for any $n \geqslant 1$ one has that $f_n(T)$ exists and the sequence $\{f_n(T)\}_{n\geqslant 1}$ is convergent to $f = f(T) \in \mathbb{C}_p$, then f defines a G-equivariant continuous function on $O(T)$ that has a unique G-equivariant analytic continuation to $B[O(T), |p|^{1+\varepsilon}]$ for any $\varepsilon > 0$. One has the following result.

Theorem 4.1. *Let T be a transcendental element of $O_{\mathbb{C}_p}$ and let $\{f_n\}_{n\geqslant 1}$ be a sequence of power series from $\mathbb{Z}_p[\![X]\!]$ such that $f_n(T)$ exists for any $n \geqslant 1$ and such that the sequence $\{f_n(T)\}_{n\geqslant 1}$ is convergent. Let $f\colon B[O(T), |p|^{1+\varepsilon}] \to \mathbb{C}_p$ be the analytic function defined by the sequence $\{f_n(T)\}_{n\geqslant 1}$ with limit $x := f(T) \in \widetilde{\mathbb{Q}_p[T]}$, where ε is a positive real number. If f is not a constant function, then the extension of fields $\widetilde{\mathbb{Q}_p[x]} \subseteq \widetilde{\mathbb{Q}_p[T]}$ is finite. Moreover, if T is a generating element for $\mathbb{C}_p$, then x is also a generating element for $\mathbb{C}_p$.*

Proof. For the closed subgroup of G, $H(T) = \{\sigma \in \mathrm{G}\colon \sigma(T) = T\}$, one has $\mathrm{Fix}(H(T)) = \widetilde{\mathbb{Q}_p[T]}$. To prove that the extension of fields $\widetilde{\mathbb{Q}_p[x]} \subseteq \widetilde{\mathbb{Q}_p[T]}$ is finite it is enough to prove that $[H(x) : H(T)] < \infty$. Let us denote by $S_{x,T}$ a system of representatives on the left for $H(x)/H(T)$. Let us suppose that $|S_{x,T}| = \infty$. Then there exists an infinite sequence of distinct elements $\sigma_n \in S_{x,T}$, $n \geqslant 1$, such that $\sigma_n \in H(x)$ and σ_n converges to $\sigma \in H(x)$. For any $n \geqslant 1$, define $T_n = \sigma_n(T)$. One has that $T_i \neq T_j$ for any $i, j \geqslant 1$, $i \neq j$. Let $F\colon B[O(T), |p|^{1+\varepsilon}] \to \mathbb{C}_p$ be the analytic function defined by $F(z) = f(z) - x, z \in B[O(T), |p|^{1+\varepsilon}]$. Because f is G-equivariant, one has that $F(T_n) = f(T_n) - x = \sigma_n(f(T)) - x = f(T) - x = 0$ for any $n \geqslant 1$. By the identity theorem, one has $F = 0$. This means that f is constant, which contradicts our assumption on f. For the last part of the theorem, let T be a generating element for $\mathbb{C}_p$. By the Artin–Schreier theorem (see [**13, 14**]), we must have $\widetilde{\mathbb{Q}_p[x]} = \mathbb{C}_p$ or $\widetilde{\mathbb{Q}_p[x]}$ is really closed. Since $\mathbb{Q}_p$ is not an ordered field we obtain $\widetilde{\mathbb{Q}_p[x]} = \mathbb{C}_p$. The proof of the theorem is complete. □

Corollary 4.2. *Let T be an integral transcendental element of $\mathbb{C}_p$ and let x be a transcendental element of $\widetilde{\mathbb{Z}_p[T]}$ such that the extension of fields $\mathbb{Q}_p \subset \mathbb{Q}_p[x]$ is normal. Then, for any transcendental element y of $\widetilde{\mathbb{Z}_p[T]}$, the extension of fields*

$$\widetilde{\mathbb{Q}_p[x]} \cap \widetilde{\mathbb{Q}_p[y]} \subset \widetilde{\mathbb{Q}_p[T]}$$

is finite.

https://doi.org/10.1017/S0013091514000376 Published online by Cambridge University Press

Proof. By the previous results, the extensions of fields

$$\widetilde{\mathbb{Q}_p[x]} \subset \widetilde{\mathbb{Q}_p[T]} \quad \text{and} \quad \widetilde{\mathbb{Q}_p[y]} \subset \widetilde{\mathbb{Q}_p[T]}$$

are finite. It is clear that $H(T) \leqslant H(x)$ and $H(T) \leqslant H(y)$. Moreover, $\mathrm{Fix}(H(T)) = \widetilde{\mathbb{Q}_p[T]}$, $\mathrm{Fix}(H(x)) = \widetilde{\mathbb{Q}_p[x]}$ and $\mathrm{Fix}(H(y)) = \widetilde{\mathbb{Q}_p[y]}$. By Galois theory one has that $[H(x) : H(T)] < \infty$ and $[H(y) : H(T)] < \infty$. Because $H(x)$ is a normal subgroup of G, one has that $H(x) \cdot H(y) = \{\sigma\tau \colon \sigma \in H(X),\ \tau \in H(y)\}$ is a subgroup of G and, moreover, we have

$$\mathrm{Fix}(H(x) \cdot H(y)) \subseteq \widetilde{\mathbb{Q}_p[x]} \cap \widetilde{\mathbb{Q}_p[y]}.$$

It is clear that $\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/\widetilde{\mathbb{Q}_p[x,y]}) = H(x) \cap H(y)$. By using an isomorphism theorem, we have that

$$\frac{H(y)}{H(x) \cap H(y)} \simeq \frac{H(x) \cdot H(y)}{H(x)}. \tag{4.1}$$

Since the extension of fields $\widetilde{\mathbb{Q}_p[y]} \subset \widetilde{\mathbb{Q}_p[x,y]}$ is finite, one has that $H(y)/H(x) \cap H(y)$ is finite. Through use of (4.1), we obtain that the extension of fields $\mathrm{Fix}(H(x) \cdot H(y)) \subset \widetilde{\mathbb{Q}_p[x]}$ is finite, so the extension of fields $\widetilde{\mathbb{Q}_p[x]} \cap \widetilde{\mathbb{Q}_p[y]} \subset \widetilde{\mathbb{Q}_p[x]}$ is finite. $\square$

Theorem 4.3. *Let $K = \widetilde{\mathbb{Q}_p[T]}$ be a closed subfield of $\mathbb{C}_p$. Then the set*

$$\{L \subset \mathbb{C}_p \colon L \text{ is a closed subfield of } \mathbb{C}_p,\ L \subset K \text{ and } [K : L] < \infty\}$$

is at most countable.

Proof. Let $L = \widetilde{\mathbb{Q}_p[u]} \subset K = \widetilde{\mathbb{Q}_p[T]}$ and $n = [K : L]$. Let $\mathrm{G}_K = H(T) = \{\sigma \in \mathrm{G} \colon \sigma(x) = x \text{ for any } x \in K\}$ and $\mathrm{G}_L = H(u) = \{\sigma \in \mathrm{G} \colon \sigma(x) = x \text{ for any } x \in L\}$. By Galois theory (see [**8**]) we have $\mathrm{Fix}(\mathrm{G}_K) = K$, $\mathrm{Fix}(\mathrm{G}_L) = L$ and $[\mathrm{G}_L : \mathrm{G}_K] = n = [K : L]$. Let us fix $S \subset \mathrm{G}$ a system of representatives for the left cosets of G/G_K such that S contains the identity e of G. There exists (and it is unique) $S_L = \{\sigma_1 = e, \dots, \sigma_n\} \subset S$ such that $\mathrm{G}_L = \bigcup_{i=1}^{n} \sigma_i \mathrm{G}_K$ with G_L and L well determined by S_L. The idea of the proof is to give an injective map from the set of the finite subsets of S of the form S_L into another set that is at most countable. First of all let us see that the map $S \to O(T)$ such that $\sigma \to \sigma(T)$ is injective. Indeed, if $\sigma(T) = \tau(T)$, then $\sigma \equiv \tau \pmod{\mathrm{G}_K}$ so $\sigma = \tau$. By this, one obtains that the map $S_L \to \{\sigma_1(T) = T, \dots, \sigma_n(T)\} \subset O(T)$ is also injective. Now, let us see that each $\sigma_i \in S_L$, $1 \leqslant i \leqslant n$, gives a permutation π_i of $(\sigma_1(T), \dots, \sigma_n(T))$ in the following way. For any $1 \leqslant j \leqslant n$ one has $\sigma_i\sigma_j \in \mathrm{G}_L = \bigcup_{m=1}^{n} \sigma_m \mathrm{G}_K$. There then exists a unique element $\sigma_{i(j)} \in S_L$, $1 \leqslant i(j) \leqslant n$, such that $\sigma_i\sigma_j \in \sigma_{i(j)}\mathrm{G}_K$. The permutation π_i of $(\sigma_1(T), \dots, \sigma_n(T))$ will be $(\sigma_{i(1)}(T), \dots, \sigma_{i(n)}(T))$. It is easy to see that the map $\sigma_i \to \pi_i$ is injective. Define $\varepsilon_L = \min\{|\sigma_i(T) - T| \colon 2 \leqslant i \leqslant n,\ \sigma_i \in S_L\} > 0$ and $H(T, \varepsilon_L) = \{\sigma \in \mathrm{G} \colon |\sigma(T) - T| < \varepsilon_L\}$. From the background material we have that ε_L is an element of the fundamental sequence associated with $O(T)$ and $H(T, \varepsilon_L)$ is an open subgroup of G of finite index. One considers the finite partition of the orbit of T with open balls of radius ε_L. In any such open ball there exists at most one element of $\{\sigma_1(T), \dots, \sigma_n(T)\}$. Define $s = [\mathrm{G} : H(T, \varepsilon_L)]$, which is in fact the number of disjoint open balls of radius ε_L that cover $O(T)$. One has that $s \geqslant n$. We can consider, via an ordered cover, that the first n balls are $B(\sigma_i(T), \varepsilon_L)$, $1 \leqslant i \leqslant n$, and the others, which exist only in the case $s > n$, are $B(\sigma_j(T), \varepsilon_L)$, $n+1 \leqslant j \leqslant s$. Now we associate with each permutation π_i of $(\sigma_1(T), \ldots, \sigma_n(T))$ the permutation $\bar{\pi}_i$ of the ordered set $\{B(\sigma_1(T), \varepsilon_L), \ldots, B(\sigma_n(T), \varepsilon_L), \ldots, B(\sigma_s(T), \varepsilon_L)\}$ that permutes the elements $B(\sigma_i(T), \varepsilon_L)$ as π_i permutes $(\sigma_1(T), \ldots, \sigma_n(T))$ and $\bar{\pi}_i$ fixes the other balls, if it is the case in which $s > n$. For any $\varepsilon > 0$, which is an element of the fundamental sequence $\{\varepsilon_n\}_{n \geqslant 1}$ associated with the orbit of T, we have a unique finite cover of $O(T)$ with $N(T, \varepsilon)$ open balls of radius ε so one has a finite number of permutations of the set of these balls. By this, when ε runs over the fundamental sequence $\{\varepsilon_n\}_{n \geqslant 1}$, the union of the sets of considered permutations is at most countable. In such a way, an injective map $\varPhi$ is defined from the set of finite subsets of S, which are in the form S_L, to the set of permutations of finite coverings of $O(T)$, in the form $\{B(\tau_1(T), \varepsilon), \ldots, B(\tau_s(T), \varepsilon)\}$ with $\varepsilon > 0$ an element of the fundamental sequence $\{\varepsilon_n\}_{n \geqslant 1}$. The proof of the theorem is finished. □

Corollary 4.4. *Let $\mathbb{Q}_p \subseteq K$ be a subfield of $\bar{\mathbb{Q}}_p$. Then the set of subfields of K of finite index, which contain $\mathbb{Q}_p$, is at most countable.*

Proof. The closed subfields of $\mathbb{C}_p$ are in one-to-one correspondence with the subfields of $\bar{\mathbb{Q}}_p$ that contain $\mathbb{Q}_p$ via the maps $K \to \tilde{K}$ and $\tilde{K} \to \tilde{K} \cap \bar{\mathbb{Q}}_p$ (see [**11**]). By this and Theorem 4.3, the proof is done. □

Theorem 4.5. *Let T be an integral transcendental element of $\mathbb{C}_p$ and let x and y be transcendental elements of $\mathbb{Z}_p[T]$. There then exists a generating element of $\mathbb{Q}_p[x, y]$ that can be written as a linear combination of x and y with coefficients in $\mathbb{Z}_p$. To be more precise, there exists $a \in \mathbb{Z}_p$ such that $\mathbb{Q}_p[x, y] = \mathbb{Q}_p[x + ay]$.*

Proof. It is easy to see that there exists an uncountable set of elements $a \in \mathbb{Z}_p$ for which $x+ay$ is transcendental. For any a in this set one has that $[\mathbb{Q}_p[T] : \mathbb{Q}_p[x + ay]] < \infty$. By this and Theorem 4.3, it follows that there exist two different elements $a, b \in \mathbb{Z}_p$ such that $\mathbb{Q}_p[x + ay] = \mathbb{Q}_p[x + by]$. It results that $x, y \in \mathbb{Q}_p[x + ay]$, and so we have that $\mathbb{Q}_p[x, y] = \mathbb{Q}_p[x + ay]$. □

Corollary 4.6. *Let ε_L be defined as in the proof of Theorem 4.3 and let* $\mathrm{Fix}\, H(T, \varepsilon_L) = \mathbb{Q}_p(\alpha)$. *Then, $K = \mathbb{Q}_p[u, \alpha] = L(\alpha)$.*

Proof. We have $L \subset L(\alpha) \subset K$. Let $\sigma \in \mathrm{G}_L$ be such that $\sigma(\alpha) = \alpha$. Then $|\sigma(T) - T| < \varepsilon_L$ and by this one has $\sigma \equiv e (\mathrm{mod}\, \mathrm{G}_K)$, so $\sigma \in \mathrm{G}_K$. It is easy to see that $\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/L(\alpha)) = \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K)$, so $K = L(\alpha) = \mathbb{Q}_p[u, \alpha]$. □

Acknowledgements. The authors are grateful to the referee for many useful comments and suggestions.

References

1. V. Alexandru and A. Zaharescu, A transcendence criterion over p-adic fields, *Nihonkai Math. J.* **14** (2003), 83–93.
2. V. Alexandru, N. Popescu and A. Zaharescu, On the closed subfields of $\mathbb{C}_p$, *J. Number Theory* **68**(2) (1998), 131–150.
3. V. Alexandru, N. Popescu and A. Zaharescu, Trace on $\mathbb{C}_p$, *J. Number Theory* **88**(1) (2001), 13–48.
4. V. Alexandru, N. Popescu and A. Zaharescu, The generating degree of $\mathbb{C}_p$, *Can. Math. Bull.* **44**(1) (2001), 3–11.
5. V. Alexandru, N. Popescu and A. Zaharescu, Metric invariants in B_{dR}^{+} associated to differential operators, *Rev. Roumaine Math. Pures Appl.* **46**(5) (2001), 551–564.
6. Y. Amice, *Les nombres p-adiques*, Collection SUP: le Mathématicien (in French) (Presse Universitaires de France, Paris, 1975).
7. E. Artin, *Algebraic numbers and algebraic functions* (Gordon and Breach, New York, 1967).
8. J. Ax, Zeros of polynomials over local fields: the Galois action, *J. Alg.* **15** (1970), 417–428.
9. S. Bosch, U. Güntzer and R. Remmert, *Non-Archimedean analysis* (Springer, 1984).
10. J. Fresnel and M. van der Put, *Rigid analytic geometry and its applications* (Birkhäuser, 2004).
11. A. Iovita and A. Zaharescu, Completions of r.a.t.-valued fields of rational functions, *J. Number Theory* **50**(2) (1995), 202–205.
12. A. Iovita and A. Zaharescu, Generating elements for B_{dR}^{+}, *J. Math. Kyoto Univ.* **39**(2) (1999), 233–248.
13. N. Jacobson, *Basic algebra II*, 2nd edn (W. H. Freeman and Co., New York, 1989).
14. S. Lang, *Algebra*, 3rd edn (Springer, 2002).
15. K. Okutsu, Construction of integral basis, I, *Proc. Jpn Acad.* A **58** (1982), 47–49.
16. K. Okutsu, Construction of integral basis, II, *Proc. Jpn Acad.* A **58** (1982), 87–89.
17. K. Okutsu, Construction of integral basis, III, *Proc. Jpn Acad.* A **58** (1982), 117–119.
18. K. Okutsu, Construction of integral basis, IV, *Proc. Jpn Acad.* A **58** (1982), 167–169.
19. K. Okutsu, Integral basis of the field $Q(\sqrt[n]{\alpha})$, *Proc. Jpn Acad.* A **58** (1982), 219–222.
20. K. Ota, On saturated distinguished chains over a local field, *J. Number Theory* **79** (1999), 217–248.
21. K. Ota, On saturated distinguished chains over a local field, II, *J. Number Theory* **111** (2005), 86–143.
22. K. Ota, On saturated distinguished chains over a local field, III, The case of p-extensions with two proper higher ramification groups, *Int. J. Math.* **17**(5) (2006), 493–604.
23. N. Popescu and A. Zaharescu, On the structure of the irreducible polynomials over local fields, *J. Number Theory* **52** (1995), 98–118.
24. A. Popescu, N. Popescu, M. Vâjâitu and A. Zaharescu, Chains of metric invariants over a local field, *Acta Arith.* **103**(1) (2002), 27–40.
25. A. Popescu, N. Popescu and A. Zaharescu, Metric invariants over Henselian valued fields, *J. Alg.* **266**(1) (2003), 14–26.
26. A. M. Robert, *A course in p-adic analysis* (Springer, 2000).
27. S. Sen, On automorphisms of local fields, *Annals Math. (2)* **90** (1969), 33–46.
28. A. P. Singh and S. K. Khanduja, On construction of saturated distinguished chains, *Mathematika* **54**(1–2) (2007), 59–65.
29. J. T. Tate, p-divisible groups, in *Proceedings of a conference on local fields: NUFFIC summer school held at Driebergen (the Netherlands) in 1966*, pp. 158–183 (Springer, 1967).