ACTA ARITHMETICA
123.3 (2006)

On the structure of compact subsets of $\mathbb{C}_p$

by

A. D. R. Choudary (Lahore and Ellensburg, WA),
Angel Popescu (Bucureşti) and Nicolae Popescu (Bucureşti)

Introduction. Let $\mathbb{Q}$ be the rational number field and let p be a fixed prime integer. Let v_p be the p-adic valuation on $\mathbb{Q}$ and let $\mathbb{Q}_p$ be the p-adic number field, i.e. the completion of $\mathbb{Q}$ with respect to v_p. Let $\overline{\mathbb{Q}}_p$ be a fixed algebraic closure of $\mathbb{Q}_p$ and let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\overline{\mathbb{Q}}_p$. Let $\overline{v}_p$ be the unique extension of v_p to $\overline{\mathbb{Q}}_p$ and let v be the restriction of $\overline{v}_p$ to $\overline{\mathbb{Q}}$. Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Set $K_p = \overline{\mathbb{Q}} \cap \mathbb{Q}_p$ and $G'_p = \mathrm{Gal}(\overline{\mathbb{Q}}/K_p)$. Since the restriction map from G_p to G'_p is injective and surjective ($\overline{\mathbb{Q}}$ is dense in $\overline{\mathbb{Q}}_p$) we can view G_p as a subgroup of G. Here we used the fact that $v(\sigma(x)) = v(x)$ for every x in $\overline{\mathbb{Q}}$ and for every $\sigma \in G_p$ ($\mathbb{Q}_p$ is a Henselian field).

For any subfield L of $\overline{\mathbb{Q}}$ we denote by $\widetilde{L}$ the completion of L with respect to the *p-adic spectral norm*

$$\|x\|_p = \max\{|\sigma(x)|_p \mid \sigma \in G\}$$

where $|\cdot|_p$ is the corresponding absolute value of v (see also [P1], [PN], [PPV], [PPZ1]–[PPZ5]).

Denote by $\widetilde{\overline{\mathbb{Q}}}_p$ the completion of $(\overline{\mathbb{Q}}, \|\cdot\|_p)$; we shall continue to use the same notation $\|\cdot\|_p$ for the unique extension of $\|\cdot\|_p$ to $\widetilde{\overline{\mathbb{Q}}}_p$. This last completion is a regular commutative ring (a von Neumann regular ring). It has many other interesting properties (see [PPV]). An element in $\widetilde{\overline{\mathbb{Q}}}_p$ is a class $\widehat{x}$ of Cauchy sequences, where $x = \{x_n\}_n$, $x_n \in \overline{\mathbb{Q}}$, $n = 1, 2, \ldots$, is a representative of $\widehat{x}$. It is easy to see that if $x = \{x_n\}_n$, $x_n \in \overline{\mathbb{Q}}$, is a Cauchy sequence relative to the p-adic spectral norm, then $\{x_n\}_n$ is a Cauchy sequence with

2000 *Mathematics Subject Classification*: Primary 11R99, 12J10; Secondary 12J20, 13A18.

Key words and phrases: Galois groups, number fields, Banach algebras, compact sets.

This research is supported by a grant from the Higher Education Commission of Pakistan.

respect to the absolute value $|\cdot|_{v\circ\sigma}$, $\sigma \in G$, i.e. the sequence $\{\sigma(x_n)\}_n$ has a limit in $\mathbb{C}_p$, the complex p-adic field (the completion of $\overline{\mathbb{Q}}_p$ relative to $\overline{v}_p$). Denote this limit by

$$x_{(\sigma)} = \lim_{n\to\infty} \sigma(x_n).$$

We call $x_{(\sigma)}$ the σ-*component* of x. Let $C(x)$ denote the set of all σ-components of x and call it the *pseudo-orbit* of x.

Since $\{\sigma(x_n)\}_n$ is also a Cauchy sequence relative to the p-adic spectral norm, we denote by $\sigma(x)$ its limit in $\widetilde{\overline{\mathbb{Q}}}_p$ for any σ in G. The subset $O(x) = \{\sigma(x) \mid \sigma \in G\}$ of $\widetilde{\overline{\mathbb{Q}}}_p$ is said to be the *orbit* of x in $\widetilde{\overline{\mathbb{Q}}}_p$. By $(\sigma, x) \mapsto \sigma(x)$, G acts continuously on $\widetilde{\overline{\mathbb{Q}}}_p$ if we consider the Krull topology on G (see [PPV]). The same is true for the mapping $(\sigma, z) \mapsto z_{(\sigma)}$ defined on $G \times \widetilde{\overline{\mathbb{Q}}}_p$ with values in $\mathbb{C}_p$. In general we have a homeomorphism $\sigma(x) \mapsto x_{(\sigma)}$ from the orbit of x *onto* the pseudo-orbit of the same x.

Three main results are proved relative to these completions:

1) Any compact subset M of $\mathbb{C}_p$ which is invariant under the group G_p $(= \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/\mathbb{Q}_p))$ is of the form $M = C(x)$, where $x \in \widetilde{\overline{\mathbb{Q}}}_p$ and $C(x)$ is the pseudo-orbit of x (Theorem 2.2).

2) The completion $\widetilde{L}$ of a finite or infinite algebraic number field L, relative to the p-adic spectral norm, is a $\mathbb{Q}_p$-Banach algebra isomorphic to the $\mathbb{Q}_p$-Banach algebra of all the G_p-equivariant continuous functions $f : G/H_L \to \mathbb{C}_p$, where $H_L = \mathrm{Fix}\, L$. Here f is said to be G_p-*equivariant* if $f(\widehat{\sigma\mu}) = \sigma(f(\widehat{\mu}))$ for all $\mu \in G$ and $\sigma \in G_p$ (Theorem 2.4).

3) Any algebraic number field (finite or infinite) has a topological generic element x in $\widetilde{\overline{\mathbb{Q}}}_p$ with respect to the p-adic spectral norm, i.e. $\widetilde{L} = \widetilde{\mathbb{Q}[x]}$ (Theorem 3.1). This result is a version of the “Primitive Element Theorem” for infinite algebraic number fields.

There is a nice connection between the topological generic elements $x \in \widetilde{\overline{\mathbb{Q}}}_p$ of an algebraic number field L and the so-called Cantor compact subsets of $\mathbb{C}_p$ (Remark 2.1, Proposition 2.3, Theorem 3.3 and Theorem 3.4). At the end of the paper we give an explicit computation of a Galois action of G on the compact set $\mathbb{Z}_p$, the p-adic integers, and we associate to it an algebraic number field, unique up to $\mathbb{Q}_p$-isomorphism (Section 4).

In a forthcoming paper we shall completely describe the structure of all compact subsets of $\mathbb{C}_p$ in connection with algebraic number fields and spectral norms.

1. Some general results. In this section we use the notations and definitions from the introduction. Now we recall a classical result in valuation theory (see for instance [Neu, pp. 161–167]):

THEOREM 1.1. *Let L/K be an algebraic extension of fields and let v be a fixed valuation on K. Let K_v be the completion of K with respect to v and let $\overline{K}_v$ be an algebraic closure of K_v which contains L. Let $\overline{v}$ be the unique extension of v to $\overline{K}_v$. Let $\overline{K}$ be the algebraic closure of K in $\overline{K}_v$. Then*:

(i) *Any extension w of v to L is of the form $w = \overline{v} \circ \tau$, where τ is a K-embedding of L into $\overline{K}_v$.*
(ii) *If τ and τ' are two K-embeddings of L into $\overline{K}_v$, then $\overline{v} \circ \tau = \overline{v} \circ \tau'$ if and only if τ and τ' are conjugate by a K_v-automorphism of $\overline{K}_v$, i.e. $\tau' = \sigma \circ \tau$ for some $\sigma \in \mathrm{Gal}(\overline{K}_v/K_v)$. In particular, if L/K is a Galois extension and if $H = \mathrm{Gal}(L/K)$, then any extension w' of v to L is of the form $w' = w \circ \mu$, where w is a fixed extension of v to L and $\mu \in H$. Moreover, $w \circ \mu = w \circ \mu'$ for $\mu, \mu' \in H$ if and only if $\mu' = \varrho \circ \mu$ for some $\varrho \in \mathrm{Gal}(\overline{K}_v/K_v) = \mathrm{Gal}(\overline{K}/\overline{K} \cap K_v)$.*

We give here an elementary result which will be useful in the following (see [PPV]).

PROPOSITION 1.2. *Let v be the restriction of $\overline{v}_p$ to $\overline{\mathbb{Q}}$ and let σ be an automorphism of G. Then the following assertions are equivalent*:

(i) *v and $v \circ \sigma$ are equivalent (they induce the same topology on $\overline{\mathbb{Q}}$).*
(ii) *$\sigma \in G_p$.*
(iii) *σ is a continuous mapping with respect to v.*

We need the following result, which partially appears in [PL].

PROPOSITION 1.3. *There exists a maximal extension $L^{(p)}$ of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ such that v_p has only one extension w to $L^{(p)}$ (for any finite extension K of $L^{(p)}$, w has at least two distinct extensions to K). This $L^{(p)}$ is dense in $\mathbb{C}_p$. Moreover, any automorphism μ of G can be uniquely written in the form $\mu = \sigma\tau$, where $\sigma \in G_p$ and $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/L^{(p)})$.*

Proof. According to [PL] we only have to prove the last statement. Since $L^{(p)}$ is dense in $\overline{\mathbb{Q}}_p$ one can use Krasner's lemma [Neu] to prove that $L^{(p)}\mathbb{Q}_p = \overline{\mathbb{Q}}_p$. Hence any embedding λ of $L^{(p)}$ in $\overline{\mathbb{Q}}$ gives rise to a unique automorphism $\overline{\lambda}$ of $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. If we start with a $\mu \in G$, then $\mu|_{L^{(p)}}$ is such a λ. Hence $\overline{\lambda}^{-1}\mu \in \mathrm{Gal}(\overline{\mathbb{Q}}/L^{(p)})$. In the end we get $\mu = \overline{\lambda}\tau$ with $\overline{\lambda} \in G_p$ and $\tau = \overline{\lambda}^{-1}\mu \in \mathrm{Gal}(\overline{\mathbb{Q}}/L^{(p)})$. The unicity follows from the equality $L^{(p)}\mathbb{Q}_p = \overline{\mathbb{Q}}_p$. ∎

REMARK 1.1. For any natural number n, it is not difficult to construct an algebraic extension T of $L^{(p)}$ of degree n such that the valuation w

from the above proposition has exactly n extensions to T. Namely, take an extension R of $\mathbb{Q}$ of degree n such that the valuation v_p splits completely into n valuations on R (see the theorem of Hasse [R]). Then we can consider the compositum $T = L^{(p)}R$, which is an extension of degree n over $L^{(p)}$ and w splits exactly into n distinct valuations on T.

2. G_p-equivariant compact subsets of $\mathbb{C}_p$. Let $G_p = \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/\mathbb{Q}_p)$ denote the group of continuous automorphisms of the p-adic complex number field $\mathbb{C}_p$ over $\mathbb{Q}_p$. A compact subset M of $\mathbb{C}_p$ is said to be G_p-*equivariant* if $\sigma(x) \in M$ for any $\sigma \in G_p$ and $x \in M$.

PROPOSITION 2.1. *For any $x \in \widetilde{\overline{\mathbb{Q}}}_p$, the pseudo-orbit $C(x)$ of x is a G_p-equivariant compact subset of $\mathbb{C}_p$. Moreover, G_p acts continuously on $C(x)$ by $\sigma(x_{(\mu)}) = x_{(\sigma\mu)}$.*

Let M be a G_p-equivariant compact subset of $\mathbb{C}_p$. For any $\varrho > 0$ we consider the covering of M with $n_{(\varrho)}$ disjoint closed balls of radius ϱ:

$$\mathcal{S}_{(\varrho)} = \{B[x_{\varrho 1}, \varrho], \ldots, B[x_{\varrho n_{(\varrho)}}, \varrho]\}$$

where $B[x, \varrho] = \{y \in \mathbb{C}_p \mid |x - y|_p \le \varrho\}$ and such that $x_{\varrho j} \in M$ for any $j = 1, \ldots, n_{(\varrho)}$. For any fixed ϱ the balls of $\mathcal{S}_{(\varrho)}$ are uniquely determined. Since the mapping $\varrho \mapsto n_{(\varrho)}$ has discrete values, the real interval $(0, \infty)$ can be written as a union

$$(0, \infty) = (\infty, \varepsilon_1] \cup (\varepsilon_1, \varepsilon_2] \cup \cdots \cup (\varepsilon_{n-1}, \varepsilon_n] \cup \cdots$$

where $\{\varepsilon_n\}_n$ is a decreasing sequence and $\varepsilon_n \to 0$. We briefly write $\mathcal{S}_n$ instead of $\mathcal{S}_{(\varepsilon_n)}$ and n_k for n_{ε_k}. The two sequences $\{\varepsilon_k\}_k$ and $\{n_k\}_k$ are called the *configuration numbers* (sequences) of M. They are invariants for M. The set M is said to be a *Cantor compact subset* if all the balls from $\mathcal{S}_k$ contain the same number of balls from $\mathcal{S}_{k+1}$.

Let now M be a G_p-equivariant compact of $\mathbb{C}_p$. We shall construct a new compact subset N of M and we shall call it a *p-reduction* of M. It will be the projective limit of the following projective system of balls. Set $\mathcal{S}'_1 = \mathcal{S}_1$. Assume we have constructed $\mathcal{S}'_k$. We now define $\mathcal{S}'_{k+1}$ to be a least subset of balls of $\mathcal{S}_{k+1}$ which are contained in $\mathcal{S}'_k$ and such that for any two balls of $\mathcal{S}'_{k+1}$ no σ in G_p carries one ball into the other. Take now $N = \varprojlim \mathcal{S}'_k$. This N can be obtained as the intersection of a tower of balls $B'_{1i_1} \supset B'_{2i_2} \supset \cdots$, all of them from the initial configuration of M. Briefly we say that N is a reduction of M.

DEFINITION 2.1. A G_p-equivariant Cantor compact subset of $\mathbb{C}_p$ is said to be (p-) *strong compact* if it has a Cantor compact reduction $N \subset M$.

THEOREM 2.2. *Let M be a G_p-equivariant compact subset of $\mathbb{C}_p$. Then there exists an x in $\widetilde{\overline{\mathbb{Q}}}_p$ whose pseudo-orbit is exactly M.*

Proof. Let $\{\mathcal{S}_k\}_k$ and $\{\mathcal{S}'_k\}_k$ be the projective systems constructed above for M and for one of its reductions N respectively.

Let $n'_1, n'_2, \ldots,$ be the corresponding numbers of distinct balls which cover only the subset N. Fix a $k = 1, 2, \ldots$. If every ball $B'[x_{kj}, \varepsilon_k] \in \mathcal{S}'_k$, $j = 1, \ldots, n'_k$, where $n'_1 = 1$, contains the same number of balls of radius ε_{k+1}, namely n'_{k+1}/n'_k, we put $n''_{k+1} = n'_{k+1}$. If this last fraction is not a natural number, we denote by $p(k, j)$ the number of balls of radius ε_{k+1} which are contained in $B'[x_{kj}, \varepsilon_k]$ and put $m_k = \text{l.c.m.}\{p(k, j)\}_j$. Finally, we change n'_{k+1} to $n''_{k+1} = n''_k m_k$. In this way we must count some of the true balls of radius ε_{k+1} which are contained in $B'[x_{kj}, \varepsilon_k]$ many times, i.e. we must consider them "with multiplicities". We obtain inductively a new sequence of natural numbers, $n''_1, n''_2, \ldots,$ such that n''_k divides n''_{k+1} for any $k = 1, 2, \ldots$. For every $k = 1, 2, \ldots,$ denote by $\mathcal{S}^*_k$ the set of all n''_k balls $B'[x_{kj}, \varepsilon_k]$ in N (for convenience we assume that only the first one, $B'[x_{k1}, \varepsilon_k]$, may appear many times). It is now clear that the sets $\{\mathcal{S}^*_k\}_k$ can be organized as a projective system of balls and its projective limit is exactly $N = \varprojlim \mathcal{S}^*_k$, i.e. every element of N can be realized as the intersection of a tower of balls, one from every $\mathcal{S}^*_k$, $k = 1, 2, \ldots$.

We now want to associate to this projective system of balls in N a tower of algebraic fields:

$$L^{(p)} = L_1 \subset L_2 \subset \cdots \subset \overline{\mathbb{Q}}$$

where $L^{(p)}$ is the subfield considered in Proposition 1.3. For $\mathcal{S}^*_1 = \{B'[x_1, \varepsilon_1]\}$, $x_1 \in N$, we take simply $L_1 = L^{(p)}$. Consider now an extension L_2 of L_1 of degree n''_2 such that the unique extension of the p-adic valuation v_p to L_1 decomposes exactly into n''_2 distinct valuations $v_{21}, v_{22}, \ldots, v_{2n''_2}$ on L_2 (this can be done as in Remark 1.1). Since L_2 is dense in $\mathbb{C}_p$ (in fact $L^{(p)}$ is dense in $\mathbb{C}_p$ as we saw in Proposition 1.3) we can take $z_{2j} \in B'[x_{2j}, \varepsilon_2]$ such that $\sigma_{2j}^{-1}(z_{2j}) \in L_2$ for every $B'[x_{2j}, \varepsilon_2] \in \mathcal{S}^*_2$, where $\{\sigma_{2j}\}_j$ are all the $L^{(p)}$-embeddings of L_2 into $\overline{\mathbb{Q}}$ and $v_{2j} = v \circ \sigma_{2j}$. We now use the Approximation Theorem to find an element w_2 in L_2 such that $|w_2 - \sigma_{2j}^{-1}(z_{2j})|_{v_{2j}} \le \varepsilon_2$ for every $j = 1, \ldots, n''_2$. This means that in every ball $B'[x_{2j}, \varepsilon_2]$ from $\mathcal{S}^*_2$ we have exactly one conjugate of w_2 over $L^{(p)}$. It is easy to see that $L_2 = L^{(p)}[w_2]$.

Assume that we have constructed the field L_k, n''_k distinct valuations $v_{kj} = v \circ \sigma_{kj}$ on it and a generator w_k of it such that $\sigma_{kj}(w_k) \in B'[x_{kj}, \varepsilon_k]$ for every $j = 1, \ldots, n''_k$. Here σ_{kj} are all the $L^{(p)}$-embeddings of L_k into $\overline{\mathbb{Q}}$.

We now consider an extension L_{k+1} of L_k of degree $q_k = n''_{k+1}/n''_k$ such that every valuation v_{kj} decomposes exactly into q_k valuations on L_{k+1} (Remark 1.1). Then $v_{k+1,j} = v \circ \sigma_{k+1,j}$, $j = 1, \ldots, n''_{k+1}$, are all the distinct valuations on L_{k+1} which extend v_p. Here $\sigma_{k+1,j}$, $j = 1, \ldots, n''_{k+1}$, are all the $L^{(p)}$-embeddings of L_{k+1} into $\overline{\mathbb{Q}}$. We must be careful with the notation of $\sigma_{k+1,j}$. Namely, the restriction of $\sigma_{k+1,j}$ to L_k must be $\sigma_{k,j'}$ such that

$\sigma_{k+1,j}(w_{k+1})$ is in the ball $B'[x_{k,j'},\varepsilon_k]$ which also contains $\sigma_{k,j'}(w_k)$. For any $j=1,\dots,n''_{k+1}$, take $z_{k+1,j}\in B'[x_{k+1,j},\varepsilon_{k+1}]$ such that $\sigma^{-1}_{k+1,j}(z_{k+1,j})\in L_{k+1}$. Using the Approximation Theorem we find $w_{k+1}\in L_{k+1}$ whose conjugates over $L^{(p)}$ all belong to a ball of the form $B'[z_{k+1,j},\varepsilon_{k+1}]$. Hence $L_{k+1}=L^{(p)}[w_{k+1}]=L_k[w_{k+1}]$.

Let now $\mu\in G$. From Proposition 1.3 we can write $\mu=\sigma\tau$, where $\sigma\in G_p$ and $\tau\in \mathrm{Gal}(\overline{\mathbb{Q}}/L^{(p)})$. Therefore, every conjugate $\mu(w_k)$ of w_k belongs to a ball from $\mathcal{S}_k$, where $\{\mathcal{S}_k\}_k$ is the projective system of balls which gives the whole compact subset M. Moreover, any ball B_{kj} of $\mathcal{S}_k$ contains at least one such $\mathbb{Q}$-conjugate of w_k. We now prove that $\{w_k\}_k$ is a Cauchy sequence relative to the p-adic spectral norm. Indeed,

$$\|w_{k+n}-w_k\|_p=\max\{|\mu(w_{k+n}-w_k)|_p \mid \mu\in G\}.$$

But $|\mu(w_{k+n}-w_k)|_p=|\tau(w_{k+n}-w_k)|_p$, where $\tau\in \mathrm{Gal}(\overline{\mathbb{Q}}/L^{(p)})$. Since $w_k,w_{k+n}\in L_{k+n}$, τ is one of the $L^{(p)}$-embeddings $\sigma_{k+n,j}$ of L_{k+n} in $\overline{\mathbb{Q}}$ considered above. Because of the special choice of $\sigma_{k+1,j},\dots,\sigma_{k+n,j}$, we see that $\sigma_{k+n,j}(w_{k+n})$ and $\sigma_{k+n,j}(w_k)$ are in the same ball $B'[x_{kj},\varepsilon_k]$, i.e.

$$|\mu(w_{k+n}-w_k)|_p\le\varepsilon_k$$

for every $n=1,2,\dots$ and $\mu\in G$. This means that

$$\|w_{k+n}-w_k\|_p\le\varepsilon_k$$

for every $n=1,2,\dots$ and so $\{w_k\}_k$ is a Cauchy sequence with respect to the p-adic spectral norm. Let

$$x\overset{\|\cdot\|_p}{=}\lim_{n\to\infty}w_n\quad\text{ in }\widetilde{\overline{\mathbb{Q}}}_p.$$

It is not difficult to see that any element y of M is the intersection of a tower of balls of the form $B[x_1,\varepsilon_1]\supset B[x_{2j_2},\varepsilon_2]\supset\cdots\supset B[x_{kj_k},\varepsilon_k]\supset\cdots$ and each such ball contains an element of the form $\mu(w_k)\in B[x_{x_kj_k},\varepsilon_k]$ for the same $\mu\in G$ (see the construction of $\sigma_{k+1,j}$ from $\sigma_{k,j}$). Hence

$$x_{(\mu)}\overset{|\cdot|_p}{=}\lim_{n\to\infty}\mu(w_k),$$

i.e. $M=C(x)$ and the proof of the theorem is finished. ∎

Remark 2.1. In the proof of Theorem 2.2 we have constructed an element $x\in\widetilde{L}$, the p-adic completion of $L=\bigcup_{k=1}^{\infty}L_k$, such that $M=C(x)$. Let M be a p-strong compact subset of $\mathbb{C}_p$. Let $\sigma,\mu\in G$ with $\sigma(x)\ne\mu(x)$ (in $\widetilde{\overline{\mathbb{Q}}}_p$), i.e. $x_{(\tau\sigma)}\ne x_{(\tau\mu)}$ for at least one $\tau\in G$ (two elements in $\widetilde{\overline{\mathbb{Q}}}_p$ are equal if and only if their components are equal). If $\tau\in G_p$ then $x_{(\tau\sigma)}=\tau(x_{(\sigma)})\ne\tau(x_{(\mu)})=x_{(\tau\mu)}$ if and only if $x_{(\sigma)}\ne x_{(\mu)}$. If $\tau\notin G_p$, then we can consider τ,σ,μ to be $L^{(p)}$- embeddings of L into $\overline{\mathbb{Q}}$ (see Proposition 1.3). In this last case, since N is a Cantor compact subset of $\mathbb{C}_p$, $x_{(\tau\sigma)}\ne x_{(\tau\mu)}$ means that the two towers of balls which define $x_{(\sigma)}$ and $x_{(\mu)}$ respectively do not coincide, i.e. $x_{(\sigma)} \neq x_{(\mu)}$. So we have proved that the continuous mapping $\sigma(x) \mapsto x_{(\sigma)}$ from $O(x)$ to $C(x)$ is a homeomorphism.

PROPOSITION 2.3. *Let M be a p-strong compact subset of $\mathbb{C}_p$. Then M is homeomorphic to a factor set of left cosets of the form G/H, where H is a closed subgroup of the absolute Galois group of $\mathbb{Q}$.*

Proof. Let $M = C(x)$ for $x \in \widetilde{\overline{\mathbb{Q}}}_p$ (Theorem 2.2). Let $H_x = \{\mu \in G \mid \mu(x) = x \text{ in } \widetilde{\overline{\mathbb{Q}}}_p\}$. It is easy to see that H_x is a closed subgroup of G. The orbit $O(x)$ is homeomorphic to G/H_x through the mapping $\sigma \mapsto \sigma(x)$. Take $H = H_x$ and the proof is finished. ∎

Let K be a subfield of $\overline{\mathbb{Q}}$ and let $H_K = \{\sigma \in G \mid \sigma(x) = x \text{ for all } x \text{ in } K\}$ be the closed subgroup of G which fixes K. Let G/H_K be the compact space of all left cosets of H_K in G. A continuous function f: $G/H_K \to \mathbb{C}_p$ is said to be G_p-*equivariant* if $f(\mu\sigma H_K) = \mu(f(\sigma H_K))$ for every $\mu \in G_p$ and for all cosets σH_K in G/H_K. We denote by $C_{G_p}(G/H_K, \mathbb{C}_p)$ the $\mathbb{Q}_p$-Banach algebra of all continuous G_p-equivariant functions $f : G/H_K \to \mathbb{C}_p$.

THEOREM 2.4. *With the notations and the hypotheses above, let $\widetilde{K}$ be the completion of K relative to the p-adic spectral norm. Then the continuous mapping $\varphi : K \to C_{G_p}(G/H_K, \mathbb{C}_p)$, defined by $\varphi(x) = \varphi_x$, where $\varphi_x(\sigma H_K) = \sigma(x)$ $(= x_{(\sigma)})$, can be uniquely extended to an isometric homomorphism of $\mathbb{Q}_p$-algebras, denoted also by φ: $\widetilde{K} \to C_{G_p}(G/H_K, \mathbb{C}_p)$, $\varphi(z) = \varphi_z$, where $\varphi_z(\sigma H_K) = z_{(\sigma)}$.*

Proof. Since $\|z\|_p = \sup_{\sigma\in G} |z_{(\sigma)}|_p$, the isometric property is clear (for $f \in C_{G_p}(G/H_K, \mathbb{C}_p)$, $\|f\| = \sup_{\sigma\in G} |f(\sigma H_K)|_p$, the usual sup-norm in a Banach algebra of continuous functions defined on a compact space). The continuity of φ comes from the continuity of the mapping $\sigma \mapsto x_{(\sigma)}$ (see also [PPV]). It remains to prove the surjectivity of φ. Let $f \in C_{G_p}(G/H_K, \mathbb{C}_p)$ and let M be the G_p-equivariant compact subset $f(G/H_K)$. Let "$\sim$" be the following equivalence relation on G/H_K:

$$\mu_1 H_K \sim \mu_2 H_K \ \text{ if } \ \mu_2 H_K = \sigma\mu_1 H_K \text{ for some } \sigma \text{ in } G_p.$$

Choose a representative $\mu_t H_K$ in each equivalence class of this relation. Denote this set of representatives by $\{\mu_t H_K\}_{t\in T}$. It is clear that the $\{\mu_t\}_t$ give rise to a set of inequivalent independent absolute values on K: $|z|_{\mu_t} = |\mu_t(z)|_p$, $t \in T$. Let now

$$\mathbb{Q} = K_1 \subset K_2 \subset \cdots \subset K, \qquad \bigcup_{n=1}^{\infty} K_n = K,$$

be a tower of (finite) algebraic number fields which cover the whole K.

Let $\varepsilon_1 > \varepsilon_2 > \cdots > 0$ be a sequence of real numbers convergent to zero and let n_k be the least number of balls $B[x_{kj}, \varepsilon_k]$, $j = 1, \ldots, n_k$, which cover N, a reduction of M (see definition before Definition 2.1). We suppose that $n_1 = 1$ and $n_1 < n_2 < \cdots$. Consider now the next $n_2 > 1$ balls of radius ε_2 which cover N, and take an element $f(\mu_{2j}H_K)$, $j = 1, \ldots, n_2$, of N in every such ball, where μ_{2j} is one of the above chosen $\{\mu_t\}_{t\in T}$. Since $|\cdot|_{\mu_{2j}}$, $j = 1, \ldots, n_2$, are independent absolute values on K, they are also independent on at least one field K_{k_2} from the above tower. Choose the smallest K_{k_2}.

Now assume that we have already constructed $K_{k_2} \subset \cdots \subset K_{k_n}$ such that for any $i = 2, \ldots, n$ and any set of elements $\{f(\mu_{ij}H_K)\}$, $j = 1, \ldots, n_i$, in N and, at the same time, in a ball $B[x_{ij}, \varepsilon_i]$, the corresponding absolute values $\{|\cdot|_{\mu_{ij}}\}$, $j = 1, \ldots, n_i$, are independent on the subfield K_{k_i}. If the set N is finite, the above construction must stop at a subfield K_{k_m}, for an $m \in \mathbb{N}$. If N is infinite, we consider the set $\{B[x_{n+1,j}, \varepsilon_n]\}_j$ of balls which cover N, some elements $f(\mu_{n+1,j}H_K)$ from N, each in one of these balls, and take a subfield K_h with sufficiently large $h \in \mathbb{N}$ such that $K_{k_n} \subset K_h$ and the absolute values $\{|\cdot|\mu_{n+1,j}\}_j$ are independent on K_h. Then we restrict the absolute values $\{|\cdot|_{\mu_{n+1,j}}\}_j$ to K_{k_n}. Let k_{n+1} be the least h with this property. Now we apply the Approximation Theorem on any K_{k_n} and find an element $w_n \in K_{k_n}$ such that

$$|\mu_{nj}(w_n) - f(\mu_{nj}H_K)|_p < \varepsilon_n$$

for any $j = 1, \ldots, n_{k_n}$ and $n = 2, 3, \ldots$. Since f is G_p-equivariant we can extend these inequalities to the whole $M = f(G/H_K)$ and to the whole G/H_K.

Now it is easy to see that $\{w_n\}_n$ is a Cauchy sequence in K relative to the p-adic spectral norm. Let $w = \lim_{n\to\infty} w_n$ be its limit in $\widetilde{K}$. From the last inequality and from the way we have chosen the set $\{\mu_t\}_t$ one finds that $w_{(\tau)} = f(\tau H_K)$, i.e. $f = \varphi_w$ and the proof is finished. ∎

3. Topological generic elements in the p-adic case

THEOREM 3.1. *Any algebraic number field L (finite or infinite) has a topological generic element $x \in \widetilde{\overline{\mathbb{Q}}}_p$, relative to the p-adic spectral norm, i.e. $\widetilde{L} = \widetilde{\mathbb{Q}[x]}$. Moreover, this x is such that $\varphi_x : G/H_L \to \mathbb{C}_p$ is a topological embedding, where H_L is the subgroup of G which corresponds to L (in the Galois correspondence).*

Proof. From Theorem 2.4 we can work in $C_{G_p}(G/H_L, \mathbb{C}_p) \cong \widetilde{L}$, where $H_L = \operatorname{Fix} L = \{\sigma \in G \mid \sigma(z) = z \text{ for any } z \in L\}$. In order to find an element $x \in \widetilde{L}$ with $\widetilde{L} = \widetilde{\mathbb{Q}[x]}$ it is enough to find $f \in C_{G_p}(G/H_L, \mathbb{C}_p)$ which separates the elements of G/H_L, i.e. $\sigma H_L \neq \mu H_L$ implies $f(\sigma H_L) \neq f(\mu H_L)$. Indeed, using the p-adic version of the Stone–Weierstrass theorem (see [Sch, Appendix]) for the $\mathbb{Q}_p$-subalgebra $\widetilde{\mathbb{Q}[f]}$ of $C_{G_p}(G/H_L, \mathbb{C}_p)$ we will then obtain $\widetilde{\mathbb{Q}[f]} = C_{G_p}(G/H_L, \mathbb{C}_p)$. Then the generic topological element of $\widetilde{L}$ will be the $x \in \widetilde{L}$ with $\varphi_x = f$.

Let us construct such an embedding $f : G/H_L \to \mathbb{C}_p$. Since f must be a G_p-equivariant continuous function on G/H_L, first of all we take a subset N of representatives $\{\tau_i\}_{i\in I}$ in G/H_L such that for any $i \neq j$, $i, j \in I$, there is no $\sigma \in G_p$ with $\sigma\tau_i = \tau_j$. We construct N exactly as in the case of a G_p-equivariant compact subset M of $\mathbb{C}_p$. Namely, first of all let us organize G/H_L as a profinite Cantor compact set, considering a tower of finite algebraic number fields:

$$\mathbb{Q} = L_1 \subset L_2 \subset \cdots \subset L$$

where $L = \bigcup_{i=1}^{\infty} L_i$ and taking the corresponding tower of subgroups:

$$H_L \subset \cdots \subset H_2 \subset H_1 = G$$

where $\bigcap_{i=1}^{\infty} H_i = H_L$ and $H_n = H_{L_n} = \operatorname{Fix} L_n$. Now $G/H_L = \varprojlim G/H_n$ and we construct the compact subset N of G/H_L as follows. Consider the partition $G = \mu_{21}H_2 \cup \cdots \cup \mu_{2n_2}H_2$. If $\mu_{22}H_2 = \sigma\mu_{21}H_2$ for some $\sigma \in G_p$ we remove $\mu_{22}H_2$ from this partition. We proceed in this way in order to obtain a "reduced" subset of $\{\mu_{2i}H_2\}_i$, $i = 1, \ldots, n_2$, with respect to G_p. Denote by

$$\mathcal{S}_2^* = \{\mu_{21}^* H_2, \mu_{2i_2}^* H_2, \ldots, \mu_{2i_{k_2}}^* H_2\}$$

this "reduced" subset. Consider now the partition $H_2 = \tau_{31}H_3 \cup \cdots \cup \tau_{3m_3}H_3$. Take $\mu_{21}^* H_2 \in \mathcal{S}_2^*$ and find a corresponding partition:

$$\mu_{21}^* H_2 = \mu_{21}^* \tau_{31} H_3 \cup \mu_{21}^* \tau_{32} H_3 \cup \cdots \cup \mu_{21}^* \tau_{3m_3} H_3.$$

We now consider the "reduction" of the set $\{\mu_{21}^*\tau_{3j}H_3\}_j$ relative to G_p. We do the same with all $\mu_{2i_j}^* H_2$ of $\mathcal{S}_2^*$ and finally obtain $\mathcal{S}_3^* = \{\mu_{31}^* H_3, \ldots, \mu_{3k_3}^* H_3\}$. We continue in this way and obtain $\mathcal{S}_4^*, \mathcal{S}_5^*, \ldots$. Since any set in $\mathcal{S}_{n+1}^*$ is a subset of a set in $\mathcal{S}_n^*$ we can organize $\{\mathcal{S}_n^*\}_n$ into a projective system of finite sets. Let N be its projective limit. It is clear that N is a compact subset of G/H_L and $\bigcup_{\sigma\in G_p} \sigma(N) = G/H_L$. The compact subset N has a "configuration"

$$k_1 = 1 < k_2 < k_3 < \cdots$$

where $k_j = |\mathcal{S}_j^*|$ for any $j = 1, 2, \ldots$. Let $\varepsilon_1 > \varepsilon_2 > \cdots > 0$ be a sequence of positive real numbers which tends to zero. Let Z be the following compact subset of $\mathbb{C}_p$ with the configuration $(\{\varepsilon_n\}_n, \{k_n\}_n)$. Take a collection $\mathcal{U}_n = \{B_{n1}, \ldots, B_{nk_n}\}$ of disjoint balls such that any ball $B_{n+1,i}$ of $\mathcal{U}_{n+1}$ is contained in one ball $B_{n,j}$ of $\mathcal{U}_n$. Moreover we assume that for any $n = 1, 2, \ldots$ and $i \neq j$, $i, j \in \{1, \ldots, k_n\}$ there is no $\sigma \in G_p$, $\sigma \neq e$, such that $B_{nj} = \sigma(B_{ni})$. We also suppose that any two distinct towers of balls $B_{11} \supset B_{2i_2} \supset B_{3i_3} \supset \cdots$ and $B_{11} \supset B_{2j_2} \supset B_{3j_3} \supset \cdots$ have distinct intersection points. We consider the mapping $f_n : \mathcal{S}_n^* \to \mathcal{U}_n$,

$f_n(\mu^*_{nj}H_n) = z_{nj}$, where z_{nj} is a fixed point of B_{nj}, $j = 1, \ldots, k_n$. If $\sigma \in G_p$ we put $f_n(\sigma\mu^*_{nj}H_n) = \sigma(z_{nj})$.

In this way we have obtained a continuous function from G/H_n to $\mathbb{C}_p$ which separates the elements of G/H_n. The projective limit of $\{f_n\}_n$ gives rise to a continuous function $f \in C_{G_p}(G/H_L, \mathbb{C}_p)$, with $\operatorname{Im} f = Z$, which separates the elements of G/H_L, and the proof of the theorem is finished. ∎

In the course of the above proof we obtained in fact another important result.

COROLLARY 3.2. *The element $x \in \widetilde{\overline{\mathbb{Q}}}_p$ is a generic element for L if and only if $\varphi_x : G \to \mathbb{C}_p$ induces a continuous embedding $\overline{\varphi}_x$: $G/H_L \to \mathbb{C}_p$, i.e. $\mu^{-1}\sigma \in H_L$ if and only if $x_{(\sigma)} = x_{(\mu)}$.*

REMARK 3.1. An alternative proof for Theorem 3.1 can be given exactly as in the archimedean case (see [PPZ1]).

THEOREM 3.3. *Let L be a subfield of $\overline{\mathbb{Q}}$. Assume that there exists a topological generic element x for L, i.e. $\widetilde{L} = \widetilde{\mathbb{Q}[x]}$. Then the pseudo-orbit $C(x)$ of x is a Cantor compact subset of $\mathbb{C}_p$.*

Proof. We prove that the continuous surjection $\sigma(x) \mapsto x_{(\sigma)}$ from $O(x)$ to $C(x)$ is a bijection, i.e. $C(x) \overset{\text{top}}{\cong} G/H_x$, where $H_x = \{\mu \in G \mid \mu(x) = x\}$. Let $\sigma, \mu \in G$ be such that $x_{(\sigma)} = x_{(\mu)}$, let $z \in L$ and let $\varepsilon > 0$ be a small real number. Then $z \overset{\|\cdot\|}{=} \lim_{n\to\infty} P_n(x)$, where $P_n(x) \in \mathbb{Q}[x]$. Let $\{x_m\}_m$ be a Cauchy sequence in L which defines x. Then, for fixed n,

$$\lim_{m\to\infty} P_n(\sigma(x_m)) = P_n(x_{(\sigma)}) = P_n(x_{(\mu)}) = \lim_{m\to\infty} P_n(\mu(x_m)).$$

Choose n such that $\|z - P_n(x)\|_p < \varepsilon/6$. Then

$$\|\sigma(z) - P_n(\sigma(x))\|_p < \varepsilon/6, \qquad \|\mu(z) - P_n(\mu(x))\|_p < \varepsilon/6.$$

For this n we choose m such that

$$\|P_n(\sigma(x)) - P_n(\sigma(x_m))\|_p < \varepsilon/6, \qquad \|P_n(\mu(x)) - P_n(\mu(x_m))\|_p < \varepsilon/6.$$

It follows that

$$\|\sigma(z) - P_n(\sigma(x_m))\|_p < \varepsilon/3, \qquad \|\mu(z) - P_n(\mu(x_m))\|_p < \varepsilon/3.$$

Possibly increasing m we have

$$\|P_n(\sigma(x_m)) - P_n(\mu(x_m))\|_p < \varepsilon/3.$$

Finally, we see that $\|\sigma(z) - \mu(z)\|_p < \varepsilon$ for any $\varepsilon > 0$. This means that $\sigma(z) = \mu(z)$ for any $z \in L$. Hence $\sigma(x) = \mu(x)$, i.e. the mapping $\sigma(x) \mapsto x_{(\sigma)}$ is an injection and the proof is finished. ∎

THEOREM 3.4. *Let x in $\widetilde{\overline{\mathbb{Q}}}_p$ be such that $C(x)$ is a Cantor compact subset of $\mathbb{C}_p$. Let $H_x = \{\sigma \in G \mid \sigma(x) = x\}$ and $L = \{y \in \overline{\mathbb{Q}} \mid \mu(y) = y$ for every $\mu \in H_x\}$. Then $\widetilde{L} = \widetilde{\mathbb{Q}[x]}$, i.e. x is a topological generic element for $\widetilde{L}$.*

Proof. Since $\widetilde{L} \overset{\text{top}}{\cong} C_{G_p}(G/H_x, \mathbb{C}_p)$ and $x \in \widetilde{L}$ ($\operatorname{Ker}\varphi_x = H_x$, where $\varphi_x : G \to \mathbb{C}_p$, $\varphi_x(\sigma) = x_{(\sigma)}$). Since $C(x)$ is a Cantor compact subset, φ_x separates the elements of G/H_x. Hence we can apply the p-adic version of the Stone–Weierstrass theorem (see [Sch]) for the subalgebra $\widetilde{\mathbb{Q}[x]}$ of $C_{G_p}(G/H_x, \mathbb{C}_p)$ to conclude that $\widetilde{L} \cong \widetilde{\mathbb{Q}[x]}$. ∎

REMARK 3.2. If we start with a Cantor compact subset M of $\mathbb{C}_p$, it is not difficult to find the least G_p-equivariant Cantor compact subset M' which contains M, namely,

$$M' = \bigcup_{\sigma \in G_p} \sigma(M).$$

This is a consequence of a general observation. If G is a compact group which acts continuously on a metric space M, that is, $(g, m) \mapsto g \cdot m$ is a continuous mapping, and if N is a compact subset of M, then $\{g \cdot n \mid g \in G, n \in N\}$ is a compact subset of M.

Another remark is that an element x can be a topological generic element only for one algebraic number field. Indeed, if $\widetilde{L} = \widetilde{\mathbb{Q}[x]} = \widetilde{L'}$ then, according to [PPV], $L = \widetilde{L} \cap \overline{\mathbb{Q}} = \widetilde{L'} \cap \overline{\mathbb{Q}} = L'$.

If one puts together Theorems 3.1, 3.3, 3.4 and the method used in the proof of Theorem 3.1, one obtains the following basic result.

THEOREM 3.5. *Let* $x \in \widetilde{\overline{\mathbb{Q}}}_p$, *let* H_x *be its invariant subgroup in* G *and* $L = \operatorname{Inv} H_x$. *Then the following assertions are equivalent*:

(i) $C(x)$ *is a Cantor compact subset of* $\widetilde{\overline{\mathbb{Q}}}_p$.

(ii) x *is a topological generic element for* $\widetilde{L}$.

(iii) $x \overset{\|\cdot\|}{=} \lim_{n\to\infty} x_n$, *where* $x_n \in \overline{\mathbb{Q}}$, $\mathbb{Q}(x_n) \subset \mathbb{Q}(x_{n+1})$, *any valuation on* $\mathbb{Q}(x_n)$ *which extends* v_p *splits completely in* $\mathbb{Q}(x_{n+1})$ *for every* $n = 1, 2, \ldots$, *and* $L = \bigcup_{n=1}^{\infty} \mathbb{Q}(x_n)$.

4. Unusual Galois actions on compact subsets of $\mathbb{C}_p$. In this section we use freely the notations and results of the previous sections.

Let $M \subset \mathbb{C}_p$ be a p-strong compact subset of $\mathbb{C}_p$ and let $x \in \widetilde{\overline{\mathbb{Q}}}_p$ be such that $C(x) = M$ (Theorem 2.2). Since the continuous mapping $\sigma(x) \mapsto x_{(\sigma)}$ from $O(x)$ to $C(x)$ is a homeomorphism (Remark 2.1), the map

$$(\sigma, x_{(\tau)}) \mapsto \sigma * x_{(\tau)} := x_{(\sigma\tau)}$$

is a continuous group action of the absolute Galois group $G = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the compact subset M. We call such actions *Galois actions on compact subsets of* $\mathbb{C}_p$. It is easy to see that if the above defined function is a group action of G on $M = C(x)$, then M must be a Cantor compact subset. If M

is not G_p-equivariant or if M is not a Cantor compact subset, we cannot define such a Galois action on it.

The usual compact subsets of $\mathbb{C}_p$ are the rings of integers of finite extensions of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$. The ring $\mathbb{Z}_p$ of p-adic integers is a p-strong compact subset of $\mathbb{C}_p$. Let us describe such a Galois action on $\mathbb{Z}_p$. $\mathbb{Z}$ itself is dense in $\mathbb{Z}_p$ (relative to the p-adic valuation). Consider a fixed tower of subfields of $\overline{\mathbb{Q}}$:

$$K_0 = \mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K, \quad \text{where} \quad K = \bigcup K_n \subset \overline{\mathbb{Q}},$$

such that $[K_{n+1} : K_n] = p$ and the p-adic valuation splits completely in K_n (see the theorem of Hasse [R]). Let $H_n = \{\mu \in G \mid \mu(y) = y \text{ for every } y \in K_n\}$ be the corresponding closed subgroup of G. As in the proof of Theorem 2.2 we shall connect the natural profinite structure of $\mathbb{Z}_p$ to the profinite structure of G.

We denote by $\mathcal{S}_1 = \{B_{10}, B_{11}, \ldots, B_{1,p-1}\}$ the set of "closed" balls in $\mathbb{Z}_p$ of radius $1/p$, with centres at $0, 1, 2, \ldots, p-1$, respectively. For instance $B_{1i} = B[i, 1/p] = \{z \in \mathbb{Z}_p \mid |z-i|_p \le 1/p\}$. It is clear that $\mathbb{Z}_p = \bigcup_{i=0}^{p-1} B_{1i}$ and this is a disjoint union. The ball B_{1i} is the disjoint union of the following p balls of radius $1/p^2$: $B_{1i} = \bigcup_{j=0}^{p-1} B_{2j}^{(i)}$, where $B_{2j}^{(i)} = B[i+jp, 1/p^2]$, $0 \le j < p$. We put together all these balls of radius $1/p^2$ for any $i = 0, 1, \ldots, p-1$ and obtain $\mathcal{S}_2 = \{B_{20}, B_{21}, \ldots, B_{2,p^2-1}\}$; the first p balls are contained in B_{10}, the next p in B_{11}, etc. In this way we can construct $\mathcal{S}_n$ from $\mathcal{S}_{n-1}$ for every $n = 2, 3, \ldots$ and it is clear that $\mathbb{Z}_p = \varprojlim \mathcal{S}_n$.

Let $|\cdot|_{10}, \ldots, |\cdot|_{1,p-1}$ be the p-adic absolute values on K_1, which extend the usual p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$.

Let $\sigma_{10}, \sigma_{11}, \ldots, \sigma_{1,p-1}$ be a fixed set of representatives of the left cosets in G/H_1 and we assume (after a suitable permutation of the above p absolute values) that $|y_1|_{1j} = |\sigma_{1j}(y_1)|_v$ for any $y_1 \in K_1$ and $j = 0, 1, \ldots, p-1$. Exactly as in the case of $\mathcal{S}_2$, we consider a set of representatives $\sigma_{20}, \sigma_{21}, \ldots, \sigma_{2,p^2-1}$ of cosets in G/H_2, the first p of which extend σ_{10}, the next p extend σ_{11}, etc. At the same time we consider the p^2 absolute values: $|y_2|_{2j} = |\sigma_{2j}(y_2)|_v$ for any $y_2 \in K_2$ and $j = 0, 1, \ldots, p^2-1$.

We continue in this way for every $K_3, K_4, \ldots$. We obtain three "isomorphic" projective systems: of balls, $\{\mathcal{S}_n\}_n$, of automorphisms of G, and of absolute values. Using the Approximation Theorem on K_n we can find $x_n \in K_n$ such that $|\sigma_{nj}(x_n) - j|_v \le 1/p^n$ for every $j = 0, 1, \ldots, p^n - 1$. This means that x_n has exactly $p^n = [K_n : \mathbb{Q}]$ conjugates (in particular $\mathbb{Q}(x_n) = K_n$) and each of them belongs to a ball from $\mathcal{S}_n$. Since any automorphism σ of G, when restricted to K_n, is one of the σ_{nj}, $j = 0, 1, \ldots, p^n - 1$, the sequence $\{x_n\}_n$ is a Cauchy sequence relative to the p-adic spectral norm on $\overline{\mathbb{Q}}$. Let $x \overset{\|\cdot\|_p}{=} \lim_{n\to\infty} x_n$, $x \in \widetilde{K}$. In fact we have a representation of the Cantor compact subset $\mathbb{Z}_p$ as the pseudo-orbit of this x: $\mathbb{Z}_p = C(x)$.

Now, the Galois action $\sigma * x_{(\mu)} = x_{(\sigma\mu)}$ of G on $C(x) = \mathbb{Z}_p$ is easy to describe. Take a p-adic integer

$$\alpha = a_0 + a_1 p + \cdots, \quad a_i \in \{0, 1, \ldots, p-1\} \text{ for all } i = 0, 1, \ldots.$$

This α corresponds to a tower of balls $B_{1i_1} \supset B_{2i_2} \supset \cdots$, namely $B_{1i_1} = B[a_0, 1/p]$, $B_{2i_2} = B[a_0 + a_1 p, 1/p^2], \ldots, B_{ni_n} = B[a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}, 1/p^n], \ldots$. Moreover $B_{ni_n} \in \mathcal{S}_n$ for $n = 1, 2, \ldots$ and $\{\alpha\} = \bigcap_n B_{ni_n}$. We associate to this α the unique $\mathbb{Q}$-embedding $\mu_{(\alpha)}$ of $K = \bigcup_n K_n$ into $\overline{\mathbb{Q}}$, such that the restriction of $\mu_{(\alpha)}$ to K_n is exactly $\sigma_{nj_{n,\alpha}}$ (where $j_{n,\alpha} = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}$) constructed above. It is easy to see that this assignment $\alpha \mapsto \mu_{(\alpha)}$ is a one-to-one and onto correspondence between $\mathbb{Z}_p$ and the topological space G/H (with its Krull topology), where $H = \operatorname{Fix} K$. Moreover, this last mapping is a homeomorphism between $\mathbb{Z}_p$ and G/H. The above Galois action on $\mathbb{Z}_p$ is exactly $\sigma * \alpha = \beta \in \mathbb{Z}_p$, where β corresponds to the embedding $\sigma\mu_{(\alpha)}$ of K into $\overline{\mathbb{Q}}$. This $\beta = b_0 + b_1 p + \cdots$ is the p-adic limit of the integers $k_n = b_0 + b_1 p + \cdots + b_{n-1}p^{n-1}$, where k_n is the index which appears in σ_{nk_n}, the restriction of $\sigma\mu_{(\alpha)}$ to K_n, which in addition has the following property: $|\sigma_{nk_n}(x_n) - k_n|_v \le 1/p^n$ (see the above construction of $\{\sigma_{nj}\}_{n,j}$, $j = 0, 1, \ldots, p^{n-1}$). This Galois action can also be described by using the above homeomorphism between $\mathbb{Z}_p$ and G/H. Let $\theta : \mathbb{Z}_p \to G/H$ be this homeomorphism. Then

$$\sigma * \alpha = \theta^{-1}(\widehat{\sigma\theta(\alpha)}).$$

This Galois action depends on the p-tower of fields

$$K_1 \subset K_2 \subset \cdots \subset K = \bigcup_n K_n$$

and on $x \overset{\|\cdot\|_p}{=} \lim_{n\to\infty} x_n$.

REMARK 4.1. The completion $\widetilde{K}$ of the above infinite algebraic number field $K = \operatorname{Inv} H_x$, with $\mathbb{Z}_p = C(x)$, is $\mathbb{Q}_p$-homeomorphic to $C_{G_p}(\mathbb{Z}_p, \mathbb{C}_p)$ (Theorem 3.1). But this last $\mathbb{Q}_p$-Banach algebra is in fact $C(\mathbb{Z}_p, \mathbb{Q}_p)$, the $\mathbb{Q}_p$-Banach algebra of all continuous functions from $\mathbb{Z}_p$ to $\mathbb{Q}_p$. The p-adic algebra and analysis of $C(\mathbb{Z}_p, \mathbb{Q}_p)$ can be sometimes more deeply understood if one uses the identification $C(\mathbb{Z}_p, \mathbb{Q}_p) = \widetilde{K}$. For instance, instead of the well known orthogonal basis of Mahler for $C(\mathbb{Z}_p, \mathbb{Q}_p)$ (see [M]), we can use the image of the orthogonal basis $\{M_n(x)\}$, $n = 0, 1, \ldots$, constructed in [A]. This last basis has deep arithmetical roots (see also [APZ1], [APZ2], [P2]) and it will be studied in another paper.

Acknowledgements. We are grateful to the staff of the School of Mathematical Sciences, Government College University, Lahore, Pakistan, for their warm hospitality during the preparation of this paper.

References

[APZ1] V. Alexandru, N. Popescu and A. Zaharescu, *On the closed subfields of* $\mathbb{C}_p$, J. Number Theory 68 (1998), 131–150.

[APZ2] —, —, —, *Trace on* $\mathbb{C}_p$, ibid. 88 (2001), 13–48.

[A] C. S. Andronescu, Doctoral thesis, Mathematical Institute of the Romanian Academy, Bucureşti, 2002.

[M] K. Mahler, *An interpolation series for continuous functions of a p-adic variable*, J. Reine Angew. Math. 199 (1958), 23–34.

[Neu] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.

[P1] A. Popescu, *On some topological representations of the absolute Galois group*, JP J. Algebra Number Theory Appl. 4 (2004), 103–112.

[P2] —, *Galois ultrametric spaces*, Math. Rep. (Bucur.) 4 (54) (2002), 269–288.

[PPZ1] A. Popescu, N. Popescu and A. Zaharescu, *On the spectral norm of algebraic numbers*, Math. Nachr. 260 (2003), 78–83.

[PPZ2] —, —, —, *Galois structures on plane compacts*, J. Algebra 270 (2003), 238–248.

[PPZ3] —, —, —, *Transcendental divisors and their critical functions*, Manuscripta Math. 110 (2003), 527–541.

[PPZ4] —, —, —, *Trace series on* $\overline{\mathbb{Q}}_K$, Results Math. 43 (2003), 331–342.

[PPZ5] —, —, —, *A Galois theory for the Banach algebra of continuous symmetric functions on absolute Galois groups*, ibid. 45 (2004), 349–358.

[PL] E. L. Popescu, *Spectral extensions*, Anal. Univ. Bucureşti Mat. 51 (2002), 159–168.

[PPV] E. L. Popescu, N. Popescu and C. Vraciu, *Completion of the spectral extension of p-adic valuation*, Rev. Roumaine Math. Pures Appl. 46 (2001), 805–817.

[PN] N. Popescu, *Galois action on plane compacts*, in: Proc. 35th Sympos. on Ring Theory and Representation Theory (Okayama, 2002), Okayama, 2003, 113–120.

[R] P. Ribenboim, *On the existence of fields with few discrete valuations*, J. Reine Agnew. Math. 216 (1964), 43–49.

[Sch] W. H. Schikhof, *Ultrametric Calculus. An Introduction to p-Adic Analysis*, Cambridge Univ. Press, 1984.

A. D. R. Choudary
School of Mathematical Sciences
GC University
Lahore, Pakistan
and
Mathematics Department CWU
Ellensburg, WA, U.S.A.

Angel Popescu
Department of Mathematics
Technical University of Civil Engineering
of Bucharest
B-dul Lacul Tei 124
72302 Bucureşti 38, Romania
E-mail: popescuangel@yahoo.co.uk

Nicolae Popescu
Mathematical Institute of the Romanian Academy
P.O. Box 1-764
70700 Bucureşti, Romania
E-mail: Nicolae.Popescu@imar.ro

Received on 1.8.2005
and in revised form on 11.2.2006 (5041)