Bull. Math. Soc. Sci. Math. Roumanie
Tome 59 (107) No. 4, 2016, 295–301

Isometric Galois actions over p-adic fields

by
[(1)]V. Alexandru, [(2)]M. Vâjâitu and [(3)]A. Zaharescu

Abstract

Let p be a prime number, $\mathbb{Q}_p$ the field of p-adic numbers, $\overline{\mathbb{Q}}_p$ a fixed algebraic closure of $\mathbb{Q}_p$ and $\mathbb{C}_p$ the completion of $\overline{\mathbb{Q}}_p$ with respect to the p-adic valuation. Let $G_p = Gal_{cont}(\mathbb{C}_p/\mathbb{Q}_p)$ be the group of continuous automorphisms of $\mathbb{C}_p$ over $\mathbb{Q}_p$. We investigate isometric Galois actions of the Galois group G_p on subsets of $\mathbb{C}_p$.

Key Words and phrases: Galois actions, p-adic fields, isometries
2010 Mathematics Subject Classification: 11S99

1 Introduction

Let p be a prime number, $\mathbb{Q}_p$ the field of p-adic numbers, $\overline{\mathbb{Q}}_p$ a fixed algebraic closure of $\mathbb{Q}_p$, and $\mathbb{C}_p$ the completion of $\overline{\mathbb{Q}}_p$ with respect to the unique extension to $\overline{\mathbb{Q}}_p$ of the p-adic valuation on $\mathbb{Q}_p$. We denote by $|\cdot|$ the absolute value on $\mathbb{C}_p$, normalized by $|p| = \frac{1}{p}$. Let $G_p = Gal_{cont}(\mathbb{C}_p/\mathbb{Q}_p)$ be the group of continuous automorphisms of $\mathbb{C}_p$ over $\mathbb{Q}_p$. By restricting each automorphism to $\overline{\mathbb{Q}}_p$, one obtains an isomorphism between $Gal_{cont}(\mathbb{C}_p/\mathbb{Q}_p)$ and the Galois group $Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Let K be a fixed finite field extension of $\mathbb{Q}_p$ and $\overline{K}$ a fixed algebraic closure of K with respect to the p-adic valuation. Denote by I_K the ring of integers of K. Let $G_K = Gal_{cont}(\mathbb{C}_p/K)$ be the group of continuous automorphisms of $\mathbb{C}_p$ over K, which is canonically isomorphic to the Galois group $Gal(\overline{K}/K)$, see [1], [2] and [7]. Here and in what follows by a Galois orbit in $\mathbb{C}_p$ we mean a set of the form $O_K(T) = \{\sigma(T) : \sigma \in G_K\}$, with $T \in \mathbb{C}_p$. Some metric aspects of the natural action of the Galois group G_p on $\mathbb{C}_p$ have been investigated in [14], [12], [11]. A metric symbol for pairs of polynomials $f(x), g(x) \in K[x]$ of the same (prime) degree was introduced and studied in [13]. Roughly speaking, the symbol is 1 or -1 according as to whether the roots of $f(x)$ are, or are not, close enough to the roots of $g(x)$, in a certain averaged way. In the present paper we investigate what we call isometric actions of the Galois group G_K on subsets of $\mathbb{C}_p$. As a matter of notation, if M is a subset of $\mathbb{C}_p$, we denote by $G_K M$ the union of Galois orbits of elements from M, that is, $G_K M = \{\sigma(x) : \sigma \in G_K \text{ and } x \in M\}$. Given two subsets M_1 and M_2 of $\mathbb{C}_p$, we say that the natural actions of the Galois group G_K on M_1 and M_2 are isometric provided that there exists a bijection $\Psi : M_1 \to M_2$ such that

$$|\sigma(\Psi(x)) - \tau(\Psi(y))| = |\sigma(x) - \tau(y)|, \tag{1.1}$$

for all $x, y \in M_1$ and all $\sigma, \tau \in G_K$. If such a map Ψ exists, we write $M_1 \simeq_{G_K} M_2$. Note that by taking both σ and τ in (1.1) to be the identity, it follows that

$$|\Psi(x) - \Psi(y)| = |x - y|, \tag{1.2}$$

for all $x, y \in M_1$. Thus in order for a bijection $\Psi : M_1 \to M_2$ to establish an isometry between the actions of the group G_K on M_1 and M_2 it is necessary for Ψ to provide an isometry between M_1 and M_2. Evidently this condition is not also sufficient in order to have $M_1 \simeq_{G_K} M_2$. Let us consider the case when the sets M_1 and M_2 consist of one element each. Say $M_1 = \{T\}$ and $M_2 = \{U\}$. In this case there is only one map $\Psi : M_1 \to M_2$, which is given by $\Psi(T) = U$, and this map automatically satisfies (1.2). Now, the condition (1.1) reduces to

$$|\sigma(U) - \tau(U)| = |\sigma(T) - \tau(T)|, \tag{1.3}$$

for all $\sigma, \tau \in G_K$. Therefore, in order to have $\{T\} \simeq_{G_K} \{U\}$ it is necessary for the Galois orbits $O_K(T)$ and $O_K(U)$ to be isometric. We remark that this condition is not also sufficient. That is, relation (1.3) is stronger than the condition on the orbits $O_K(T)$ and $O_K(U)$ to be isometric. Besides this metric condition, relation (1.3) also forces another condition, which is more algebraic in nature. To be specific, by (1.3) it follows that an automorphism $\sigma \in G_K$ satisfies the equality $\sigma(U) = U$ if and only if it satisfies the equality $\sigma(T) = T$. Now the elements $\sigma \in G_K$ which satisfy $\sigma(T) = T$ form a closed subgroup of G_K, call it $H_{K,T}$, and similarly the elements $\sigma \in G_K$ which satisfy $\sigma(U) = U$ form a closed subgroup $H_{K,U}$ of G_K. Relation (1.3) thus forces the equality $H_{K,T} = H_{K,U}$. On the other hand, by Galois theory in $\mathbb{C}_p$, as developed by Tate [10], Sen [9] and Ax [5], we know that the closed subgroups of the Galois group G_K are in one-to-one correspondence with the closed subfields of $\mathbb{C}_p$ which contain K. The equality $H_{K,T} = H_{K,U}$ then implies the equality $\widetilde{K(T)} = \widetilde{K(U)}$, where $\widetilde{K(T)}$ and $\widetilde{K(U)}$ denote the topological closure of $K(T)$ and respectively of $K(U)$ in $\mathbb{C}_p$. In the particular case when the elements T and U are algebraic over K, the equality $\widetilde{K(T)} = \widetilde{K(U)}$ reduces to the equality $K(T) = K(U)$. Therefore, in order for two elements $T, U \in \overline{K}$ to satisfy the relation $\{T\} \simeq_{G_K} \{U\}$, besides having isometric Galois orbits the elements T and U also need to generate the same field extension over K.

Taking into account all the above restrictions, the reader may naturally wonder whether there are any nontrivial examples of elements T, U for which $\{T\} \simeq_{G_K} \{U\}$, or other examples of nontrivial isometric Galois actions. After some background material is presented in Section 2, we provide some classes of isometric Galois actions in Section 3 below. It would be interesting, and we leave this as a general question for the reader, to find other natural classes of isometric Galois actions and investigate their properties.

2 Background material

In [13] a metric symbol $\left(\frac{g}{f}\right)$ is defined for pairs of polynomials $f(x)$, $g(x) \in K[x]$ of prime degree q by the following rule:

$$\left(\frac{g}{f}\right) = \begin{cases} 1 & \text{if } v(R(f,g)) > \frac{q}{q-1} v(\Delta(f)) \\ -1 & \text{else} \end{cases} \tag{2.1}$$

where $\Delta(f)$ denotes the discriminant of f, $R(f,g)$ denotes the resultant of f and g, and v denotes the p-adic valuation. Although the above definition is not symmetric in f and g this metric symbol has some nice properties that we mention below.

Theorem 1. *([13]) (i) (Irreducibility criterion): If f is irreducible and $\left(\frac{g}{f}\right) = 1$ then g is also irreducible.*

(ii) (Transitivity): If f is irreducible and $\left(\frac{g}{f}\right) = \left(\frac{h}{g}\right) = 1$ then $\left(\frac{h}{f}\right) = 1$.

(iii) (Reciprocity Law): If f and g are irreducible then

$$\left(\frac{g}{f}\right) = \left(\frac{f}{g}\right).$$

A subset $D \subseteq \mathbb{C}_p$ is said to be G_K-equivariant provided that $\sigma(x) \in D$ for any $x \in D$ and any $\sigma \in G_K$. An example is $D = O_K(x)$, where $x \in \mathbb{C}_p$.

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

Proposition 1. *([4]) Let T be a transcendental element of $\mathbb{C}_p$ such that $|T| < |p|$. Then*

$$\widetilde{I_K[T]} = \left\{ \sum_{n \geq 0} a_n T^n : a_n \in I_K \right\}.$$

3 Main results

Proposition 2. *Let $f \in K[x]$ be a monic irreducible polynomial of degree d and $T \in \overline{K}$ a root of f. Then for any monic polynomial $g \in K[x]$ of degree d whose coefficients are close enough to those of f in the $p-$adic distance, there is a root U of g such that $\{T\} \simeq_{G_K} \{U\}$.*

Proof. Choose a polynomial $f(x) \in K[x]$, irreducible over K, say

$$f(x) = x^d + a_1 x^{d-1} + \cdots + a_d,$$

and fix a root T of $f(x)$. Next, choose a small real number $\varepsilon > 0$, select elements $b_1, b_2, \ldots, b_d \in K$ such that $|b_j - a_j| < \varepsilon$ for $1 \leq j \leq d$, and consider the polynomial $g(x) = x^d + b_1 x^{d-1} + \cdots + b_d$. Now, if ε is small enough, then there will be a root of $g(x)$, call it U, which is closer to T than any conjugate of T over K. By Krasner's lemma it follows that $K(T) \subseteq K(U)$. Since $K(T)$ has degree d over K, this shows that the polynomial $g(x)$ is irreducible over K, and that $K(T) = K(U)$. Also, for any two distinct conjugates of T, say $\sigma(T)$ and $\tau(T)$, we have

$$\begin{aligned} |\sigma(T) - \sigma(U)| = |\tau(T) - \tau(U)| &= |T - U| \\ &< |T - (\sigma^{-1}\tau)(T)| = |\sigma(T) - \tau(T)|. \end{aligned}$$

Since we work in an ultrametric space, it follows that

$$|\sigma(U) - \tau(U)| = |\sigma(T) - \tau(T)|.$$

Therefore the Galois orbits $O_K(T)$ and $O_K(U)$ are isometric. Moreover, one sees that $\{T\} \simeq_{G_K} \{U\}$. $\square$

Proposition 3. *Let T be an element of $\mathbb{C}_p$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ an element of $GL_2(K)$ such that $|det(\gamma)| = |cT+d|^2$. Then $O_K(T) \simeq_{G_K} O_K(\gamma(T))$.*

Proof. Let us define $\Psi : O_K(T) \to O_K(\gamma(T))$ by

$$\Psi(\sigma(T)) = \gamma(\sigma(T)) = \frac{a\sigma(T)+b}{c\sigma(T)+d} = \sigma(\gamma(T)),$$

for any $\sigma \in G_K$. Clearly, Ψ is a bijection between $O_K(T)$ and $O_K(\gamma(T))$. In order to establish (1.1), let $x = \sigma_1(T)$ and $y = \sigma_2(T)$ be arbitrary elements of $O_K(T)$, $\sigma_1, \sigma_2 \in G_K$. Also, let σ, τ be arbitrary elements of G_K. One has

$$\begin{aligned} |\sigma(\Psi(x)) - \tau(\Psi(y))| &= |\sigma(\gamma(\sigma_1(T))) - \tau(\gamma(\sigma_2(T)))| \\ &= |\gamma(\sigma\sigma_1(T)) - \gamma(\tau\sigma_2(T))|. \end{aligned}$$

Using the fact that $|c\sigma\sigma_1(T)+d| = |cT+d| = |c\tau\sigma_2(T)+d|$ one finds after a straightforward computation that

$$\begin{aligned} |\gamma(\sigma\sigma_1(T)) - \gamma(\tau\sigma_2(T))| &= \frac{|det(\gamma)|}{|cT+d|^2} \cdot |\sigma\sigma_1(T) - \tau\sigma_2(T)| \\ &= |\sigma\sigma_1(T) - \tau\sigma_2(T)| = |\sigma(x) - \tau(y)|. \end{aligned}$$

This completes the proof of the proposition. □

Proposition 4. *Let $\mathcal{X}$ be a compact subset of $\mathbb{C}_p$ without isolated points and let $\psi : \mathcal{X} \to \mathbb{C}_p$ be differentiable. Then ψ is locally an isometry if and only if $|\psi'(z)| = 1$ for all $z \in \mathcal{X}$.*

Proof. All the points of $\mathcal{X}$ are accumulation points. Let us assume that ψ is locally an isometry and let z be an arbitrary element of $\mathcal{X}$. One has

$$\psi'(z) = \lim_{\substack{u \to z \\ u \in \mathcal{X}}} \frac{\psi(u) - \psi(z)}{u - z} \tag{3.1}$$

and, by hypothesis, $|\psi(u) - \psi(z)| = |u - z|$ locally so $|\psi'(z)| = 1$.

For the reverse implication, it is enough to see that for an arbitrary $z \in \mathcal{X}$ we have

$$\left| \psi'(z) - \frac{\psi(u) - \psi(z)}{u - z} \right| < 1$$

for all u in a certain neighborhood of z. We deduce that for such u one has $|\psi(u) - \psi(z)| = |u - z|$, so ψ is locally an isometry and the proof of the proposition is complete. □

Remark 1. *Proposition 3 shows that in some cases, $\mathcal{X} = O_K(x)$, $x \in \mathbb{C}_p$, the condition $|\psi'(x)| = 1$ is sufficient for ψ to be an isometry. In that case $\psi(x) = \frac{ax+b}{cx+d}$ so $\psi'(x) = \frac{ad-bc}{(cx+d)^2}$ and $|\psi'(x)| = 1$.*

Theorem 2. *Let $f(x)$ and $g(x)$ be monic polynomials of prime degree q with coefficients in a finite extension K of $\mathbb{Q}_p$. If f is irreducible over K and $\left(\frac{g}{f}\right) = 1$ then $Z(f) \simeq_{G_K} Z(g)$, where $Z(f)$, respectively $Z(g)$, denote the set of zeros of f, respectively g.*

Proof. From Theorem 1 g too is irreducible over K. Let $Z(f) = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$ and $Z(g) = \{\beta_1, \beta_2, \ldots, \beta_q\}$ be all the distinct roots of f and respectively g. As in the proof of Theorem 2 from [11] we can arange the sets $Z(f)$ and $Z(g)$ such that

$$|\alpha_i - \beta_i| = |\alpha_j - \beta_j| = \min\{|\alpha_j - \theta| : g(\theta) = 0\} \tag{3.2}$$

where the minimum on the far right side of (3.2) is achieved for a unique root θ of g. Moreover,

$$|\alpha_i - \alpha_j| = |\beta_i - \beta_j| = |\alpha_i - \beta_j|, \tag{3.3}$$

for any $1 \leq i \neq j \leq q$. Let us define $\Psi : Z(f) \to \mathbb{Z}(g)$, $\Psi(\alpha_i) = \beta_i$, for any $1 \leq i \leq q$. In order to establish (1.1) it is enough to show that

$$|\sigma(\Psi(\alpha_i)) - \tau(\Psi(\alpha_j))| = |\sigma(\alpha_i) - \tau(\alpha_j)| \tag{3.4}$$

for any $\sigma, \tau \in G_K$ and any $1 \leq i, j \leq q$. If $\sigma(\alpha_i) = \alpha_k$ and $\tau(\alpha_j) = \alpha_l$ then by the construction from [11] $\sigma(\beta_i) = \beta_k$ and $\tau(\beta_j) = \beta_l$. Indeed, if $\sigma(\alpha_i) = \alpha_k$ one has

$$|\sigma(\alpha_i) - \sigma(\beta_i)| = |\alpha_i - \beta_i| = |\alpha_k - \beta_k| = |\alpha_k - \sigma(\beta_i)|,$$

and by this we have $\sigma(\beta_i) = \beta_k$. Similarly if $\tau(\alpha_j) = \alpha_l$ then $\tau(\beta_j) = \beta_l$. Since $|\alpha_k - \alpha_l| = |\beta_k - \beta_l|$, by (3.3), one obtains (3.4), which completes the proof of the theorem. □

Theorem 3. *Let x be a transcendental element of $\mathbb{C}_p$ such that $|x| < r_p|p|$, where $r_p = |p|^{\frac{1}{p-1}}$, and $y \in \widetilde{I_K[x]}$, $y = \sum_{n\geq 0} a_n x^n$, $a_n \in I_K$ for any $n \geq 0$, that satisfies $|a_1| = 1$. Let $\psi : O_K(x) \to O_K(y)$ be defined by $\sigma(x) \rightsquigarrow \sigma(y)$, $\sigma \in G_K$. Then ψ is an isometry and, moreover, $O_K(x) \simeq_{G_K} O_K(y)$.*

Proof. First of all let us see that under our hypotheses, by Proposition 1 all the elements $y \in \widetilde{I_K[x]}$ are of the form $y = \sum_{n\geq 0} a_n x^n$, where $a_n \in I_K$ for any $n \geq 0$. It is clear that $H_x \subseteq H_y$, so ψ is well defined and, moreover, ψ is surjective. Since x is transcendental all the points of $O_K(x)$ are accumulation points. So, by the identity principle, ψ has a unique G_K-equivariant analytic continuation to $B(0,1)$, given by $\psi(z) = \sum_{n\geq 0} a_n z^n$. By hypothesis $|x| < r_p|p|$, where $r_p = |p|^{\frac{1}{p-1}}$, so $O_K(x) \subset B(0, r_p|p|)$. Because $|a_1| = 1$ it is clear that $|\psi'(z)| = 1$ for any $z \in B(0,1)$. Now, using the p-adic Rolle Theorem for series [8] one finds that ψ is an isometry between $O_K(x)$ and $O_K(y)$. In order to establish (1.1) it is enough to show that

$$|\sigma(\psi(x_1)) - \tau(\psi(x_2))| = |\sigma(x_1) - \tau(x_2)| \tag{3.5}$$

for any $\sigma, \tau \in G_K$ and any $x_1, x_2 \in O_K(x)$. Let $x_1 = \sigma_1(x)$ and $x_2 = \sigma_2(x)$, where $\sigma_1, \sigma_2 \in G_K$. Since ψ is G_K-equivariant one has

$$\begin{aligned} |\sigma(\psi(x_1)) - \tau(\psi(x_2))| &= |\sigma(\psi(\sigma_1(x))) - \tau(\psi(\sigma_2(x)))| \\ &= |\psi(\sigma\sigma_1(x)) - \psi(\tau\sigma_2(x))| \\ &= |\psi'(c)| \cdot |\sigma\sigma_1(x) - \tau\sigma_2(x)| \\ &= |\sigma\sigma_1(x) - \tau\sigma_2(x)| \\ &= |\sigma(x_1) - \tau(x_2)|, \end{aligned} \tag{3.6}$$

via the p-adic Rolle Theorem for series [8], where $c \in B(0, |p|)$. So (3.5) holds true, which means that $O_K(x) \simeq_{G_K} O_K(y)$, and the proof of the theorem is complete. $\square$

Theorem 4. *Let x be a transcendental element of $\mathbb{C}_p$ and $\Psi \in K(X)$, $\Psi(X) = \frac{A(X)}{B(X)}$ where $A, B \in K[X]$ with $\deg \Psi = d \geq 1$. Denote $y = \Psi(x)$ and let $\psi : O_K(x) \to O_K(y)$ be defined by $\psi(z) = \Psi(z)$, for any $z \in O_K(x)$. If there exists an $r > 0$ such that $O_K(x) \subset B(x, r)$ and ψ has an analytic continuation to $B(x, rr_p^{-1})$ with $|\psi'(z)| = 1$ for any $z \in B(x, rr_p^{-1})$, then ψ is an isometry between $O_K(x)$ and $O_K(y)$ and, moreover, $O_K(x) \simeq_{G_K} O_K(y)$.*

Proof. By hypothesis $[\mathbb{Q}_p(x) : \mathbb{Q}_p(y)] = d \geq 1$ so y is transcendental. Because $\Psi \in K(X)$, $\psi(\sigma(x)) = \sigma(\psi(x))$ and $H_x \subseteq H_y$ one sees that ψ is well defined. Moreover, ψ is surjective and G_K-equivariant. Let u, v be arbitrary elements of $O_K(x)$. By the p-adic Rolle Theorem for rational fractions [6] it follows that there exists $c \in B(x, rr_p^{-1})$ such that $\psi(u) - \psi(v) = \psi'(c)(u-v)$. It is then clear that ψ is an isometry between $O_K(x)$ and $O_K(y)$. The remaining part of the proof that $O_K(x) \simeq_{G_K} O_K(y)$ follows along the same lines as in the proof of Theorem 3. $\square$

References

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

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

[3] V. Alexandru, N. Popescu, A. Zaharescu, *Trace on* $\mathbb{C}_p$, J. Number Theory **88** (2001), no. 1, 13–48.

[4] V. Alexandru, M. Vâjâitu, A. Zaharescu, *On p-adic analytic continuation with applications to generating elements*, P. Edinburgh Math. Soc., **59** (2016), 1-10.

[5] J. Ax, *Zeros of polynomials over local fields—The Galois action*, J. Algebra **15** (1970), 417–428.

[6] X. Faber, *Topology and geometry of the Berkovich ramification locus for rational functions, II*, Math. Ann. **356**(2013), no. 3, 819–844.

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

[8] A.M. Robert, *A course in p-adic analysis*, volume 198 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2000.

[9] S. Sen, *On automorphisms of local fields*, Ann. of Math. (2) **90** (1969), 33–46.

[10] J. T. Tate, *p-divisible groups*, 1967 Proc. Conf. Local Fields (Driebergen, 1966) pp. 158–183 Springer, Berlin.

[11] M. Vâjâitu, A. Zaharescu, *An algebraic-metric equivalence relation over p-adic fields*, Glasgow Math. J. **54**(2012), 715-720.

[12] M. Vâjâitu, A. Zaharescu, *Non-Archimedean Integration and Applications*, The publishing house of the Romanian Academy, 2007.

[13] A. Zaharescu, *A metric symbol for pairs of polynomials over local fields*, C.R. Math. Acad. Sci. Soc. R. Can. **22** (2000), no. 4, 147–150.

[14] A. Zaharescu, *Lipschitzian elements over p-adic fields*, Glasgow Math. J. **47** (2005), 363–372.

Received: 27.10.2015
Accepted: 02.02.2016

(1) Department of Mathematics, University of Bucharest
Romania
E-mail: vralexandru@yahoo.com

(2) Simion Stoilow Institute of Mathematics of the Romanian Academy
Research Unit 5
P.O.Box 1-764, RO-014700 Bucharest
Romania
E-mail: Marian.Vajaitu@imar.ro

(3) Simion Stoilow Institute of Mathematics of the Romanian Academy
Research Unit 5
P.O.Box 1-764, RO-014700 Bucharest
Romania
and
Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, IL, 61801, USA
E-mail:zaharesc@illinois.edu