*Glasgow Math. J.* **54** (2012) 715–720. © Glasgow Mathematical Journal Trust 2012.
doi:10.1017/S0017089512000468.

# AN ALGEBRAIC-METRIC EQUIVALENCE RELATION OVER $p$-ADIC FIELDS

MARIAN VÂJÂITU

*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*

and ALEXANDRU ZAHARESCU

*Department of Mathematics, University of Illinois at Urbana-Champaign,* 1409 *W. Green Street, Urbana, IL* 61801, *USA*
*e-mail: zaharesc@math.uiuc.edu*

(Received 24 November 2011; revised 13 March 2012; accepted 17 April 2012)

**Abstract.** Let $p$ be a prime number, $\mathbf{Q}_p$ the field of $p$-adic numbers, $K$ a finite field extension of $\mathbf{Q}_p$, $\bar{K}$ a fixed algebraic closure of $K$ and $\mathbf{C}_p$ the completion of $\bar{K}$ with respect to the $p$-adic valuation. We introduce and investigate an equivalence relation on $\mathbf{C}_p$, defined in terms of field extensions and metric properties of Galois orbits over $K$.

2000 *Mathematics Subject Classification.* 11S99.

**1. Introduction.** Let $p$ be a prime number, $\mathbf{Q}_p$ the field of $p$-adic numbers, $K$ a fixed finite field extension of $\mathbf{Q}_p$, $\bar{K}$ a fixed algebraic closure of $K$ and $\mathbf{C}_p$ the completion of $\bar{K}$ with respect to the $p$-adic valuation. Here and in what follows we denote by $|.|$ the $p$-adic absolute value on $\mathbf{C}_p$, normalised by $|p| = \frac{1}{p}$. We also denote by $O_{\mathbf{C}_p}$ the ring of integers of $\mathbf{C}_p$ and by $G_K$ the group of continuous automorphisms of $\mathbf{C}_p$ over $K$. The group $G_K$ is canonically isomorphic to the Galois group $Gal(\overline{K}/K)$, see [**1**], [**2**] and [**6**]. By the Galois orbit over $K$ we mean a set of the form $C_K(T) := \{\sigma(T) : \sigma \in G_K\}$, with $T$ in $\mathbf{C}_p$. Associated to each such Galois orbit $C_K(T)$, we have the Haar distribution (in the sense of Mazur and Swinnerton-Dyer [**7**]) on $C_K(T)$, call it $\pi_{K,T}$, which is a unique distribution on $C_K(T)$ with values in $\mathbf{Q}_p$, normalised by $\pi_{K,T}(C_K(T)) = 1$, which is $G_K$-invariant, in the sense that for any ball $B$ in $C_K(T)$ and for any $\sigma \in G_K$ one has $\pi_{K,T}(\sigma(B)) = \pi_{K,T}(B)$.

Our goal in this short paper is to introduce an algebraic-metric equivalence relation on $\mathbf{C}_p$, which appears to have some nice properties. We establish a few of them in the present paper. This equivalence relation is defined in terms of field extensions of $K$ and metric properties of Galois orbits over $K$. Our starting point is to consider the following natural question: Given two elements $T$ and $U$ of $\mathbf{C}_p$, under which circumstances is there a canonical way to define a map from the Galois orbit $C_K(T)$ to the Galois orbit $C_K(U)$? The existence of such a map would have useful implications in questions related to integration along Galois orbits with respect to the Haar distribution, and to the problem of the existence of trace over $K$ of transcendental elements over $K$ (see [**3**], [**5**] and [**11**]). Given two elements $T$ and $U$ of $\mathbf{C}_p$, the obvious choice for the definition of a natural map from $C_K(T)$ to $C_K(U)$ would be to take each element $z$ in $C_K(T)$, write

https://doi.org/10.1017/S0017089512000468 Published online by Cambridge University Press

it in the form $z = \sigma(T)$ with $\sigma \in G_K$ and then send it to the element $\sigma(U)$ of $C_K(U)$. In general, this is not a well-defined map. In order for this map to be well defined, the following condition is necessary and sufficient: For any $\sigma \in G_K$ for which $\sigma(T) = T$, one also has $\sigma(U) = U$. The automorphisms $\sigma \in G_K$ that satisfy the equality $\sigma(T) = T$ form a closed subgroup of $G_K$, call it $H_{K,T}$, and similarly the automorphisms satisfying $\sigma(U) = U$ form a closed subgroup $H_{K,U}$ of $G_K$. The above condition then asks for the inclusion of $H_{K,T} \subseteq H_{K,U}$. If this condition holds, then one has a well-defined map from $C_K(T)$ to $C_K(U)$ given by $\sigma(T) \mapsto \sigma(U)$, $\sigma \in G_K$. We denote this map by $h_{K,T,U}$. If the other inclusion also holds so that we have equality, $H_{K,T} = H_{K,U}$, then we also have a map $h_{K,U,T} : C_K(U) \to \mathbf{C}_K(T)$ given by $\sigma(U) \mapsto \sigma(T)$, and the two maps, $h_{K,T,U}$ and $h_{K,U,T}$, are bijections, inverse to each other. By the Galois theory in $\mathbf{C}_p$, as developed by Tate [**9**], Sen [**8**] and Ax [**4**], we know that the closed subgroups of the Galois group $G_K$ are in one-to-one correspondence with the closed subfields of $\mathbf{C}_p$, which contain $K$. Therefore, if we denote by $E_{K,T}$ and $E_{K,U}$ the topological closure of the fields $K(T)$ and respectively $K(U)$ in $\mathbf{C}_p$, the above condition $H_{K,T} = H_{K,U}$ is equivalent to the equality $E_{K,T} = E_{K,U}$. Let us assume now that the elements $T$ and $U$ of $\mathbf{C}_p$ are such that $E_{K,T} = E_{K,U}$, and consider the maps $h_{K,T,U}$ and $h_{K,U,T}$. These maps then may be used to transfer metric information between the Galois orbits $C_K(T)$ and $C_K(U)$. The best case, in terms of the accuracy of this transfer of metric information, is when the maps $h_{K,T,U}$ and $h_{K,U,T}$ are isometries. We take this as our definition of equivalence. Thus, given two elements $T$ and $U$ of $\mathbf{C}_p$, we say that these are equivalent over $K$, and write $T \sim_K U$ if and only if $E_{K,T} = E_{K,U}$ and the maps $h_{K,T,U}$ and $h_{K,U,T}$ are isometries. It is easy to see that $\sim_K$ is an equivalence relation on $\mathbf{C}_p$. Let us remark that in case $T$ and $U$ are algebraic over $K$, the equality $E_{K,T} = E_{K,U}$ reduces to the equality $K(T) = K(U)$.

In what follows, we establish some properties of the equivalence relation $\sim_K$ defined above. We focus on three basic questions. The first one asks whether there is any connection between this equivalence relation and the metric symbol introduced and studied in [**10**]. The answer is that there is such a connection. This connection provides additional motivation for the study of the equivalence relation $\sim_K$, as this equivalence relation is suitable for addressing phenomena in $\mathbf{C}_p$ that are not expressible in terms of the original metric symbol from [**10**]. The second question is whether there are any simple transformations that behave nicely with respect to the equivalence relation $\sim_K$, in the sense that many elements $T$ of $\mathbf{C}_p$ are sent to elements equivalent to themselves. We will see that fractional linear transformations of $\mathbf{P}^1(\mathbf{C}_p) = \mathbf{C}_p \cup \{\infty\}$, $z \to \frac{az+b}{cz+d}$, with $a, b, c, d \in K$, send large classes of elements $T$ of $\mathbf{C}_p$ to elements equivalent to themselves. The third problem is to investigate the topological properties of the set of elements equivalent to a given element $T$ of $\mathbf{C}_p$. We prove that all the equivalence classes are closed in $\mathbf{C}_p$. The results mentioned above show that this equivalence relation enjoys some nice properties, and deserves further study.

**2. Connection with the metric symbol.** In [**10**] a metric symbol was defined for pairs of polynomials. Precisely, one considers pairs of monic polynomials $f(X), g(X) \in K[X]$ of degree a prime number $q$. For such a pair one defines a metric symbol $\left(\frac{g}{f}\right)$ by the following rule:

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

https://doi.org/10.1017/S0017089512000468 Published online by Cambridge University Press

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. One has the following result.

THEOREM 1. ([**10**]). (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*

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

We also need the following lemma (see for example [**10**]).

LEMMA 1. *Let $f \in K[X]$ be irreducible of prime degree $q$. Then the distance between any two distinct roots of $f$ is the same.*

Let now $q$ be a prime number and let $f(X)$ and $g(X)$ be monic polynomials with coefficients in $K$ of degree $q$, irreducible over $K$, such that $\left(\frac{f}{g}\right) = 1$. Then for any root $\alpha$ of $f(X)$, we claim that there is a unique root $\beta$ of $g(X)$ in $\bar{K}$, which satisfies the equality

$$|\alpha - \beta| = \min\{|\alpha - \theta| : g(\theta) = 0\}. \tag{2}$$

Indeed, let us assume that the above equality holds for two distinct roots $\beta$ and $\beta'$ of $g(X)$. Then from $|\alpha - \beta| = |\alpha - \beta'|$ it follows that $|\beta - \beta'| \leq |\alpha - \beta|$. By the above lemma, the distance between any two roots of $g(X)$ is the same, so all these distances are bounded by $|\alpha - \beta|$. On the other hand, the distance between any root of $f(X)$ and any root of $g(X)$ is at least $|\alpha - \beta|$. Indeed, via a suitable automorphism of the Galois group each such distance coincides with the distance from $\alpha$ to a root of $g(X)$, which in turn is at least $|\alpha - \beta|$. Therefore, the geometric mean of the distances between the roots of $g(X)$ is less than or equal to the geometric mean of the distances between the roots of $f(X)$ and the roots of $g(X)$. By expressing the above two geometric means in terms of the discriminant of $g(X)$ and respectively the resultant of $f(X)$ and $g(X)$, one sees that the above is in contradiction with our assumption that $\left(\frac{f}{g}\right) = 1$. Therefore, the above $\beta$ is unique, as claimed.

We then have $\alpha \sim_K \beta$. Indeed, let $\{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_q\}$ and $\{\beta = \beta_1, \beta_2, \ldots, \beta_q\}$ be all the distinct roots of $f$ and $g$ in $\bar{K}$. We can arrange the set of all distinct roots of $g$ such that

$$|\alpha - \beta| = |\alpha_i - \beta_i| = \min\{|\alpha_i - \theta| : g(\theta) = 0\}. \tag{3}$$

By (1) and Theorem 1 one has

$$v(R(f, g)) > \frac{q}{q-1} \max\{v(\Delta(f)), v(\Delta(g))\}. \tag{4}$$

From (2), (3), (4) and Lemma 1, we have

$$v(\alpha - \beta) > \max_{2 \leq i \leq q} \{v(\alpha - \alpha_i), v(\beta - \beta_i)\}. \tag{5}$$

By using (5) and Krasner's Lemma one obtains $K(\alpha) = K(\beta)$. It is clear that $h_{K,\alpha,\beta}$ and $h_{K,\beta,\alpha}$ are bijections, inverse to each other. To prove that the above functions

https://doi.org/10.1017/S0017089512000468 Published online by Cambridge University Press

preserve the distances, it is enough to show that $|\alpha - \alpha_i| = |\beta - \beta_i|$, for any $2 \le i \le q$. Because $|\alpha - \beta| = |\alpha_i - \beta_i| < \min\{|\alpha - \beta_i|, |\alpha_i - \beta|\}$, one has $|\beta - \beta_i| = |\alpha - \beta_i| = |\alpha - \alpha_i|$, for any $2 \le i \le q$, so $h_{K,\alpha,\beta}$ and $h_{K,\beta,\alpha}$ are isometries.

We state the above result in the following theorem.

THEOREM 2. *Let $q$ be a prime number, and let $f(X)$ and $g(X)$ be monic polynomials with coefficients in $K$ of degree $q$, irreducible over $K$, such that $\left(\frac{f}{g}\right) = 1$. Choose a root $\alpha$ of $f(X)$ in $\bar{K}$ and let $\beta$ be the unique root of $g(X)$ in $\bar{K}$, which satisfies* (2). *Then $\alpha \sim_K \beta$.*

**3. Special transformations.** Here and in what follows, we denote the equivalence class of an element $U \in \mathbf{C}_p$ by $[U]_K$. Thus, $[U]_K = [V]_K$ if and only if $U \sim_K V$. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $GL_2(K)$. Let us consider the fractional linear transformation $z \to \gamma z := \frac{az+b}{cz+d}$ of $\mathbf{P}^1(\mathbf{C}_p) = \mathbf{C}_p \cup \{\infty\}$. We first remark that for any element $z$ of $K$, the equivalence class $[z]_K$ of $z$ coincides with $K$. Here we may extend the equivalence relation $\sim_K$ from $\mathbf{C}_p$ to $\mathbf{C}_p \cup \{\infty\}$ by letting the point at infinity be equivalent with any element of $K$. Then $[z]_K = \mathbf{P}^1(K)$ for any $z \in K$. The above transformation $z \to \gamma z$ maps the equivalence class $\mathbf{P}^1(K)$ to itself. We now fix an element $U$ in $\mathbf{C}_p \setminus K$, and denote $V = \gamma U$. We want to see that under what circumstances $U \sim_K V$? First of all, $U$ and $V$ generate the same field extension of $K$, and hence $E_{K,U} = E_{K,V}$. Therefore, the maps $h_{K,U,V}$ and $h_{K,V,U}$ are bijections inverse to each other, and one has $U \sim_K V$ if and only if these maps are isometries. Choose any two elements $U'$ and $U''$ of $C_K(U)$. We need to see when one has the equality

$$|h_{K,U,V}(U'') - h_{K,U,V}(U')| = |U' - U''|. \tag{6}$$

Let $\sigma, \tau \in G_K$ be such that $U' = \sigma(U)$ and $U'' = \tau(U)$. Then, since

$$h_{K,U,V}(\sigma(U)) = \sigma(V) = \sigma(\gamma U) = \gamma\sigma(U),$$

and similarly

$$h_{K,U,V}(\tau(U)) = \tau(V) = \tau(\gamma U) = \gamma\tau(U),$$

equation (6) reduces to

$$|\gamma\tau(U) - \gamma\sigma(U)| = |\tau(U) - \sigma(U)|. \tag{7}$$

On the other hand, using the equalities $|c\tau(U) + d| = |c\sigma(U) + d| = |cU + d|$, a straightforward calculation gives

$$|\gamma\tau(U) - \gamma\sigma(U)| = \frac{|\det\gamma|}{|cU + d|^2} \cdot |\tau(U) - \sigma(U)|. \tag{8}$$

Combining (7) with (8) we derive $U \sim_K V$ if and only if $|\det\gamma| = |cU + d|^2$. This provides a characterisation for the set of elements $U$, which are equivalent to their image via $\gamma$.

THEOREM 3. *Let $U$ be an element of $\mathbf{C}_p \setminus K$ and let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $GL_2(K)$. Then $\gamma U \sim_K U$ if and only if $|\det\gamma| = |cU + d|^2$.*

https://doi.org/10.1017/S0017089512000468 Published online by Cambridge University Press

Now, let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(K)$ and $T, U \in \mathbf{C}_p$ such that $T \sim_K U$ and $|cT + d| = |cU + d|$. By a simple calculation we have

$$|\sigma(\gamma T) - \gamma T| = |\gamma\sigma(T) - \gamma T| = \frac{|\det \gamma|}{|cT + d|^2} \cdot |\sigma(T) - T| = \frac{|\det \gamma|}{|cU + d|^2} \cdot |\sigma(U) - U| = |\sigma(\gamma U) - \gamma U|. \tag{9}$$

Since $E_{K,\gamma T} = E_{K,\gamma U}$, which follows from $T \sim_K U$, one has $\gamma T \sim_K \gamma U$. We have the following proposition.

PROPOSITION 1. *Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(K)$, and let $T, U \in \mathbf{C}_p \setminus K$ be such that $T \sim_K U$ and $|cT + d| = |cU + d|$. Then $\gamma T \sim_K \gamma U$.*

**4. Topological properties.** Let $T$ be an element of $\mathbf{C}_p$. Let $\{U_n\}_{n\geq 1}$ be a sequence of elements of $\mathbf{C}_p$ such that $U_n \in [T]_K$, for any $n \geq 1$. We assume that the sequence $\{U_n\}_{n\geq 1}$ converges to $U \in \mathbf{C}_p$. We want to show that $U \in [T]_K$. It is enough to prove the following.

*Claim*: The maps $h_{K,U,T}$ and $h_{K,T,U}$ are isometries and $E_{K,T} = E_{K,U}$.

Since $U_n \in [T]_K$, for any $n \geq 1$ the maps $h_{K,U_n,T}$ and $h_{K,T,U_n}$ are isometries. On the one hand we have that $|\sigma(U_n) - U_n| = |\sigma(T) - T|$, for any $\sigma \in G_K$ and any $n \geq 1$. By passing to the limit one obtains $|\sigma(U) - U| = |\sigma(T) - T|$, so the first part of the claim is clear. On the other hand, to prove that $E_{K,T} = E_{K,U}$, by the Galois theory it is enough to prove that $H_{K,T} = H_{K,U}$. Let $\sigma \in H_{K,T}$. One has that $\sigma \in H_{K,U_n}$, for any $n \geq 1$, which means $\sigma(U_n) = U_n$ for any $n \geq 1$, so $\sigma(U) = U$. This implies $H_{K,T} \subseteq H_{K,U}$. For the reverse inclusion, let $\sigma \in H_{K,U}$. Recall that $|\sigma(U_n) - U_n| = |\sigma(T) - T|$ for any $n \geq 1$. Since $U_n \to U$ and $\sigma(U) = U$, we have $\sigma(T) = T$ and the claim is proved. One has the following result.

THEOREM 4. *Let $K$ be a fixed finite field extension of $\mathbf{Q}_p$. Then all equivalence classes with respect to the equivalence relation $\sim_K$ are topologically closed in $\mathbf{C}_p$.*

ACKNOWLEDGEMENTS. This work was supported by Grant PN-II-ID-PCE-2012-4-0376, titled 'p-Adic Analytic Functions and Distributions of Sequences'. The authors are grateful to the referee for useful comments and suggestions.

## REFERENCES

**1.** V. Alexandru, N. Popescu and A. Zaharescu, On the closed subfields of $\mathbf{C}_p$, *J. Number Theory* **68**(2)(1998), 131–150.

**2.** V. Alexandru, N. Popescu and A. Zaharescu, The generating degree of $\mathbf{C}_p$, *Canad. Math. Bull.* **44**(1) (2001), 3–11.

**3.** V. Alexandru, N. Popescu and A. Zaharescu, Trace on $\mathbf{C}_p$, *J. Number Theory* **88**(1) (2001), 13–48.

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

**5.** D. Barsky, Transformation de Cauchy $p$-adique et algèbre d'Iwasawa, *Math. Ann.* **232**(3) (1978), 255–266.

https://doi.org/10.1017/S0017089512000468 Published online by Cambridge University Press

**6.** A. Ioviţă and A. Zaharescu, Completions of r.a.t.-valued fields of rational functions, *J. Number Theory* **50**(2) (1995), 202–205.

**7.** B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math.* **25** (1974), 1–61.

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

**9.** J. T. Tate, *p*-divisible groups, in *Proc. Conf. Local Fields*, Driebergen, 1966 (Springer, Berlin, Germany, 1967) 158–183.

**10.** A. Zaharescu, A metric symbol for pairs of polynomials over local fields, *C.R. Math. Acad. Sci. Soc. R. Can.* **22**(4) (2000), 147–150.

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

https://doi.org/10.1017/S0017089512000468 Published online by Cambridge University Press