J. Aust. Math. Soc. **79** (2005), 361–368

COHOMOLOGICAL CHARACTERIZATION OF THE HILBERT SYMBOL OVER $\mathbb{Q}_p^*$

FERNANDO PABLOS ROMO

(Received 11 February 2004; revised 15 November 2004)

Communicated by K. F. Lai

Abstract

The aim of this work is to offer a new characterization of the Hilbert symbol over $\mathbb{Q}_p^*$ from the commutator of a certain central extension of groups. We obtain a characterization for $\mathbb{Q}_p^*$ $(p \neq 2)$ and a different one for $\mathbb{Q}_2^*$.

2000 *Mathematics subject classification*: primary 19F15, 20F12.

1. Introduction

In recent years, characterizations of algebraic symbols have been obtained from the properties of infinite-dimensional vector spaces in order to provide new interpretations for these symbols and to deduce standard theorems from the new definitions in an easy way.

Thus, in 1968 Tate [7] gave a definition of the residues of differentials on curves in terms of traces of certain linear operators on infinite-dimensional vector spaces.

A few years later, in 1989, Arbarello, de Concini and Kac [1] obtained a definition of the tame symbol of an algebraic curve from the commutator of a certain central extension of group. More recently, the author has given an interpretation of this central extension in terms of determinants associated with infinite-dimensional vector subspaces [3], and has defined the Parshin symbol on a surface as iterated tame symbols [4].

This work is partially supported by the DGESYC research contract no. BFM2003-00078 and Castilla y León Regional Government contract SA071/04.

In all articles referred to above, the respective reciprocity laws (in particular, the residue theorem) are deduced directly from the finiteness of the cohomology groups $H^0(C, \mathcal{O}_C)$ and $H^1(C, \mathcal{O}_C)$.

The purpose of the present work is to give a new characterization of the Hilbert symbol over $\mathbb{Q}_p^*$ by using the method described in [1] and [3]. This definition, which involves topics of Steinberg symbols, allows us to use the results of [1, 2, 3] to study the properties of this symbol. A remaining problem is to obtain a new proof of the Gauss Reciprocity Law from the statements of this characterization.

Similarly to the computation of the symbol ([6, page 20]), we obtain a characterization for $\mathbb{Q}_p^*$ with $p \neq 2$ and a different one for $\mathbb{Q}_2^*$.

For a detailed study of p-adic fields and the Hilbert symbol, the reader is referred to [6].

2. Preliminaries

This section is added for the sake of completeness.

2.1. Definition of the Hilbert symbol If k denotes either the field $\mathbb{R}$ of real numbers or the field $\mathbb{Q}_p$ of p-adic numbers (p being a prime number), Serre [6] defines the Hilbert symbol $(\cdot, \cdot)_k : k^* \times k^* \to \mu_2$ as:

$$(a, b)_k = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a non-trivial solution in } k^3; \\ -1 & \text{otherwise,} \end{cases}$$

where $a, b \in k^*$ and $\mu_2 = \{1, -1\}$.

The Hilbert symbol is a Steinberg symbol ([2, page 94]) because it is bimultiplicative and satisfies $(a, 1-a)_k = 1$. Moreover, $(a, -a)_k = 1$ and $(a, b)_k = (b, a)_k$.

If $k = \mathbb{Q}_p$, we shall write $(a, b)_p = (a, b)_k$.

It is known that $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathcal{U}^p$, where $\mathcal{U}^p$ is the group of p-adic units. Hence, if v_p denotes the p-adic valuation, each element $a \in \mathbb{Q}_p^*$ can be written uniquely in the form $a = p^\alpha u$, with $\alpha = v_p(a)$ and $u \in \mathcal{U}^p$.

Moreover, if we denote by $\mathcal{U}^2$ the group of units of $\mathbb{Z}_2$, we can define the morphisms of groups $\epsilon, \omega : \mathcal{U}^2 \to \mathbb{Z}/2$ as follows:

$$\epsilon(u) = \frac{u-1}{2} \pmod 2 = \begin{cases} 0 & \text{if } u \equiv 1 \pmod 4; \\ 1 & \text{if } u \equiv -1 \pmod 4, \end{cases}$$

$$\omega(u) = \frac{u^2-1}{8} \pmod 2 = \begin{cases} 0 & \text{if } u \equiv \pm 1 \pmod 8; \\ 1 & \text{if } u \equiv \pm 5 \pmod 8. \end{cases}$$

Setting $\mathscr{U}_n^p = 1 + p^n\mathbb{Z}_p$, ϵ and ω determine isomorphisms of groups

$$\epsilon : \mathscr{U}^2/\mathscr{U}_2^2 \xrightarrow{\sim} \mathbb{Z}/2 \quad \text{and} \quad \omega : \mathscr{U}_2^2/\mathscr{U}_3^2 \xrightarrow{\sim} \mathbb{Z}/2.$$

Furthermore, $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ and each element $a = 2^\alpha u \in \mathbb{Q}_2^*$ can be written in the form $(-1)^{\epsilon(u)} 2^\alpha 5^{\omega(u)} \bar{u}$, where $\bar{u} \in (\mathbb{Q}_2^*)^2$.

There exist also isomorphisms of groups $\phi : \mathscr{U}^p/\mathscr{U}_1^p \xrightarrow{\sim} (\mathbb{Z}/p)^*$, and if $f \in \mathscr{U}^p$, we shall write $f(p) = \phi(\bar{f}) \in (\mathbb{Z}/p)^*$.

Thus, given $a, b \in \mathbb{Q}_p^*$, $a = p^\alpha u$ and $b = p^\beta v$, the value of the Hilbert symbol is:

$$(a, b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u^\beta}{v^\alpha}(p)\right)^{(p-1)/2} \qquad \text{if } p \neq 2,$$
$$(a, b)_2 = (-1)^{\epsilon(u)\epsilon(v) + \alpha\omega(v) + \beta\omega(u)}.$$

2.2. The group Gl(V, A) and its canonical central extension Let V be a vector space over a field k (in general infinite-dimensional) and let A be a vector subspace of V. With the same notation as in [1] we set

$$\mathrm{Gl}(V, A) = \{f \in \mathrm{Aut}(V) \text{ such that } fA \sim A\},$$

where $f \sim fA$ when $\dim_k(A + fA/A \cap fA) < \infty$, which is the definition of commensurable subspaces of Tate [7].

If $f \in \mathrm{Gl}(V, A)$, we set $(A|fA) = \Lambda(A/A \cap fA)^* \bigotimes_k \Lambda(fA/A \cap fA)$, Λ being the maximal exterior power. Canonically, Arbarello, de Concini and Kac [1] defined a group $\widetilde{\mathrm{Gl}}(V, A) = \{(f, s) \text{ with } f \in \mathrm{Gl}(V, A) \text{ and } s \in (A|fA), s \neq 0\}$, which induces a central extension:

$$1 \to k^* \to \widetilde{\mathrm{Gl}}(V, A) \to \mathrm{Gl}(V, A) \to 1.$$

Let us set $A = k[[t]]$ and $V = k((t))$. Since $k((t))^* \subseteq \mathrm{Gl}(V, A)$, if we denote by $\{\cdot, \cdot\}_A$ the commutator of the above extension and we consider two elements, $f, g \in k((t))^*$ with $f = \lambda t^\alpha\big(1 + \sum_{i\geq 1} a_i t^i\big)$, and $g = \mu t^\beta\big(1 + \sum_{j\geq 1} b_j t^j\big)$, where $\lambda, \beta \in k^*$ and $\alpha, \beta \in \mathbb{Z}$, we have that

$$\{f, g\}_A = \frac{\lambda^\beta}{\mu^\alpha} \in k^*.$$

This computation of the commutator can also be found in [3].

2.3. Steinberg symbols For any field F, a bimultiplicative mapping $c : F^* \times F^* \to A$ to an abelian group, satisfying $c(x, 1 - x) = 1$ for $x \neq 1$, is called a 'Steinberg symbol' on the field F.

If F_v is a discrete valuation field, $\mathcal{O}_v$ is the valuation ring, $\mathfrak{m}_v$ is the unique maximal ideal and $k(v) = \mathcal{O}_v/\mathfrak{m}_v$ is the residue class field, the tame symbol

$$\begin{aligned} d_v : F_v^* \times F_v^* &\to k(v)^* \\ (x, y) &\mapsto (-1)^{v(x)v(y)} \frac{x^{v(y)}}{y^{v(x)}} \pmod{\mathfrak{m}_v} \end{aligned}$$

is an easy example of a Steinberg symbol on F_v^*.

For a detailed study of Steinberg symbols, we refer the reader to [2].

3. Characterization of the Hilbert symbol

Let us now consider $k = \mathbb{Q}_p$, $A_p = \mathbb{Q}_p[[t]]$ and $V_p = \mathbb{Q}_p((t))$.

Since each element $f \in \mathbb{Q}_p^*$ can be written uniquely in the form $a = p^{v_p(f)}u$ with $u \in \mathcal{U}^p$, we can consider the injective group morphism

$$\begin{aligned} \varphi : \mathbb{Q}_p^* &\hookrightarrow \mathbb{Q}_p((t))^*, \\ p^\alpha u &\mapsto u t^\alpha, \end{aligned}$$

and we deduce that $\mathbb{Q}_p^*$ is a commutative subgroup of $\mathrm{Gl}(V_p, A_p)$ by considering the homotheties $h_{\varphi(f)}$. Thus the commutator of the following central extension of groups

$$1 \to \mathbb{Q}_p^* \to \widetilde{\mathrm{Gl}}(V_p, A_p) \to \mathrm{Gl}(V_p, A_p) \to 1$$

determines a 2-cocycle $\{\cdot,\cdot\}_p : \mathbb{Q}_p^* \times \mathbb{Q}_p^* \to \mathcal{U}^p$ whose value is $\{f, g\}_p = u^\beta/v^\alpha$, where $f = p^\alpha u$ and $g = p^\beta v$.

3.1. Hilbert symbol over $\mathbb{Q}_p^*$ ($p \neq 2$) From the morphism of groups $\psi_p : \mathcal{U}^p \to \mu_2$ defined as $\psi_p(u) = (u(p))^{(p-1)/2}$ we have a 2-cocycle $\widetilde{\{\cdot,\cdot\}}_p : \mathbb{Q}_p^* \times \mathbb{Q}_p^* \to \mu_2$, whose value is

$$\widetilde{\{f, g\}}_p = \psi_p(\{f, g\}_p) = \left(\frac{u^\beta}{v^\alpha}(p)\right)^{(p-1)/2}.$$

In general , one has that $\widetilde{\{\cdot,\cdot\}}_p$ is not a Steinberg symbol because

$$\widetilde{\{p^{-1}, 1 - p^{-1}\}}_p = -1$$

when $p \equiv 3 \pmod 4$.

We shall now give a cohomological definition of the Hilbert symbol as a distinguished element in the cohomology class $[\widetilde{\{\cdot,\cdot\}}_p] \in H^2(\mathbb{Q}_p^*, \mu_2)$, where $H^2(A, B)$ is the group of classes of 2-cocycles $f : A \times A \to B$ (mod 2-coboundaries) [5].

Lemma 3.1. *For each $a \in \mathbb{Z}$, there exists a unique 2-coboundary $c_a : \mathbb{Z} \times \mathbb{Z} \to \mu_2$ satisfying the conditions*:

- $c_a(\alpha, \beta + \gamma) = c_a(\alpha, \beta)c_a(\alpha, \gamma)$;
- $c_a(\alpha, \alpha) = (-1)^{\alpha a}$

for $\alpha, \beta, \gamma \in \mathbb{Z}$.

Proof. Recall that a 2-cocycle $c_a : \mathbb{Z}\times\mathbb{Z} \to \mu_2$ is a 2-coboundary when there exists a map $\phi: \mathbb{Z} \to \mu_2$ such that $c_a(\alpha, \beta) = \phi(\alpha+\beta)\phi(\alpha)^{-1}\phi(\beta)^{-1}$. Let $\phi(\alpha) = \lambda_\alpha \in \mu_2$. It follows from the conditions of the lemma that

$$\lambda_\alpha = (-1)^{\alpha(\alpha-1)a/2}\lambda_1^\alpha \quad \text{for each } \alpha \in \mathbb{Z}.$$

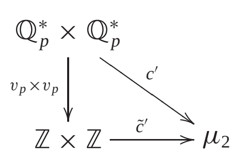
Hence $c_a(\alpha, \beta) = (-1)^{\alpha\beta a}$ is the unique 2-coboundary that satisfies the statement of the lemma. □

Theorem 3.2. *There exists a unique Steinberg symbol $(\cdot, \cdot)_p$ in the cohomology class $[\widetilde{\{\cdot, \cdot\}}_p] \in H^2(\mathbb{Q}_p^*, \mu_2)$ satisfying the condition*

$$(f, g)_p = \widetilde{\{f, g\}}_p \quad \textit{if } v_p(f) = 0.$$

This Steinberg symbol is the Hilbert symbol over $\mathbb{Q}_p^*$.

Proof. Let $\nu(f, g) = c'(f, g)\widetilde{\{f, g\}}_p$ be a Steinberg symbol in the cohomology class $[\widetilde{\{\cdot, \cdot\}}_p] \in H^2(\mathbb{Q}_p^*, \mu_2)$ such that $c'(f, g) = 1$ for $v_p(f) = 0$. Since c' is a 2-coboundary, one has that $c'(f, g) = 1$ when $v_p(g) = 0$ and, therefore, there exists a commutative diagram



where $\tilde{c}'$ is a 2-coboundary satisfying $\tilde{c}'(\alpha, \beta + \gamma) = \tilde{c}'(\alpha, \beta)\tilde{c}'(\alpha, \gamma)$.

Furthermore, since $\nu(f, -f) = 1$ for all $f \in \mathbb{Q}_p^*$, one has that $\tilde{c}'(\alpha, \alpha) = (-1)^{\alpha(p-1)/2} = (-1)^{\alpha\epsilon(p)}$. It then follows from Lemma 3.1 that $\tilde{c}'(\alpha, \beta) = (-1)^{\alpha\beta\epsilon(p)}$ and $c'(f, g) = (-1)^{v_p(f)v_p(g)\epsilon(p)}$.

Thus, the unique Steinberg symbol in $[\widetilde{\{\cdot, \cdot\}}_p] \in H^2(\mathbb{Q}_p^*, \mu_2)$ is

$$\nu(f, g) = (-1)^{v_p(f)v_p(g)\epsilon(p)}\widetilde{\{f, g\}}_p,$$

which is the Hilbert symbol. □

REMARK 3.3. The above property, which characterizes the Hilbert symbol in $\mathbb{Q}_p^*$ is equivalent to one of the conditions that Serre gave to define local symbols on algebraic curves ([5]) which are also Steinberg symbols.

Let us now consider in $\mathbb{Q}_p^*$ the structure of the topological group induced by the p-adic valuation and let us consider μ_2 as a topological group with the discrete topology.

CONJECTURE 3.4. *$(\cdot,\cdot)_p$ is the unique continuous Steinberg symbol in the cohomology class $[\widetilde{\{\cdot,\cdot\}}_p] \in H^2(\mathbb{Q}_p^*,\mu_2)$.*

3.2. Hilbert symbol over $\mathbb{Q}_2^*$ Let us consider the morphism of groups $\psi_2 : \mathscr{U}^2 \to \mu_2$ defined as $\psi_2(u) = (-1)^{\omega(u)}$. This map induces a 2-cocycle $\widetilde{\{\cdot,\cdot\}}_2 : \mathbb{Q}_2^* \times \mathbb{Q}_2^* \to \mu_2$ whose value is

$$\widetilde{\{f,g\}}_2 = \psi_2(\{f,g\}_2) = (-1)^{\beta\omega(u)+\alpha\omega(v)},$$

where $f = 2^\alpha u$ and $g = 2^\beta v$.

Again, $\widetilde{\{\cdot,\cdot\}}_2$ is not a Steinberg symbol because $\widetilde{\{6,-5\}}_2 = -1$. We shall now determine the relation between the commutator $\widetilde{\{\cdot,\cdot\}}_2$ and the Steinberg symbol $(\cdot,\cdot)_2$ in the group of 2-cocycles $Z^2(\mathbb{Q}_2^*,\mu_2)$.

THEOREM 3.5. *There exists a unique 2-cocycle $c_2 \in Z^2(\mathbb{Q}_2^*,\mu_2)$ such that $c_2\widetilde{\{\cdot,\cdot\}}_2$ is a non-trivial Steinberg symbol. This symbol is the Hilbert symbol $(\cdot,\cdot)_2$. Moreover, c_2 is not a 2-coboundary and hence $(\cdot,\cdot)_2 \notin [\widetilde{\{\cdot,\cdot\}}_2] \in H^2(\mathbb{Q}_2^*,\mu_2)$.*

PROOF. Let $c_2 \in Z^2(\mathbb{Q}_2^*,\mu_2)$ such that $\nu = c_2\widetilde{\{\cdot,\cdot\}}_2$ is a Steinberg symbol. Since $\widetilde{\{\cdot,\cdot\}}_2$ is a bimultiplicative map, c_2 must be bimultiplicative and one has that

$$c_2(f,1-f) = \widetilde{\{f,1-f\}}_2 \quad \text{for} \quad f \neq 1.$$

Moreover, since $\widetilde{\{f,-f\}}_2 = 1$, the condition $c_2(f,-f) = 1$ must be satisfied and it follows from the equality

$$\widetilde{\{f,g\}}_2 = \widetilde{\{g,f\}}_2$$

that c_2 must be a symmetric 2-cocycle.

Furthermore, since $c_2(f^2,g) = c_2(f,g^2) = 1$, we have that c_2 is characterized by its values in -1, 2 and 5, which are the generators of the group $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$.

Bearing in mind the previous considerations, we have that

$$c_2(2,-1) = \widetilde{\{2,-1\}}_2 = 1, \quad c_2(2,2) = c_2(2,-2)c_2(2,-1) = 1.$$

From the equalities

$$c_2(5,-4) = \widetilde{\{5,-4\}}_2 = 1 \quad \text{and} \quad c_2(5,2^2) = 1,$$

we deduce that $c_2(5,-1) = 1$. It is now clear that $c_2(5,5) = 1$.

To conclude, let us first assume that $c_2(-1,-1) = 1$. Then, since $\epsilon(3) = 1$ and $\omega(3) = 1$ we have that $3 = -5u^2$. Moreover, $c_2(6,-5) = \widetilde{\{6,-5\}}_2 = -1$, and thus

$$\begin{aligned} c_2(2,5) &= c_2(2,-5) = -c_2(12,-5) = -c_2(3,-5) \\ &= -c_2(-5,-5) = -c_2(-1,-1) = -1. \end{aligned}$$

Hence if we write $f = (-1)^{\epsilon(u)} 2^{\alpha} 5^{\omega(u)} \bar{u}^2$ and $g = (-1)^{\epsilon(v)} 2^{\beta} 5^{\omega(v)} \bar{v}^2$, we have in this case that

$$c_2(f,g) = c_2(2^{\alpha}, 5^{\omega(v)}) c_2(5^{\omega(u)}, 2^{\beta}) = (-1)^{\alpha\omega(v)+\beta\omega(u)} = \widetilde{\{f,g\}}_2$$

and $\nu = c_2 \widetilde{\{\cdot,\cdot\}}_2 = 1$ is the trivial Steinberg symbol.

Finally, when $c_2(-1,-1) = -1$ we deduce, using a similar argument, that $c_2(2,5) = 1$. Hence, $c_2(f,g) = (-1)^{\epsilon(u)\epsilon(v)}$, and

$$\nu(f,g) = (-1)^{\epsilon(u)\epsilon(v)} \widetilde{\{f,g\}}_2 = (f,g)_2.$$

Furthermore, since $c_2(-1,-1) \neq 1$ we have that c_2 is not a 2-coboundary and we conclude the proof. □

Acknowledgements

The author wishes to thank Professors José Mourao, Joao Nunes and Carlos Florentino at the Instituto Superior Técnico of Lisbon (Portugal) for their hospitality during a three-month period in 2001 when much of the work of this paper was done.

References

[1] E. Arbarello, C. de Concini and V. G. Kac, 'The infinite wedge representation and the reciprocity law for algebraic curves', in: *Theta functions – Bowdoin 1987 (Brunswick, ME, 1987)*, Proc. Sympos. Pure Math. 49, Part I (Amer. Math. Soc., Providence, RI, 1989) pp. 171–190.

[2] J. Milnor, *Introduction to algebraic K-theory*, Ann. of Math. Stud. 72 (Princeton University Press, Princeton, 1971).

[3] F. Pablos Romo, 'On the tame symbol of an algebraic curve', *Comm. Algebra* **30** (2002), 4349–4368.

[4] ———, 'Algebraic construction of the tame symbol and the Parshin symbol on a surface', *J. Algebra* **274** (2004), 335–346.

[5] J. P. Serre, *Groupes algébriques et corps de classes* (Hermann, Paris, 1959).
[6] ———, *A course in arithmetic* (Springer, New York, 1973).
[7] J. Tate, 'Residues of differentials on curves', *Ann. Sci. École Norm. Sup.* **4** (1968), 149–159.

Departamento de Matemáticas
Universidad de Salamanca
Plaza de la Merced 1-4
37008 Salamanca
Spain
e-mail: fpablos@usal.es