

JEAN-PIERRE SERRE

On a functorial property of power residue symbols. Erratum : Solution of the congruence subgroup problem for $SL_n(n \geq 3)$ and $Sp_{2n}(n \geq 2)$

Publications mathématiques de l'I.H.É.S., tome 44 (1974), p. 241-244

http://www.numdam.org/item?id=PMIHES_1974__44__241_0

© Publications mathématiques de l'I.H.É.S., 1974, tous droits réservés.

L'accès aux archives de la revue « Publications mathématiques de l'I.H.É.S. » (<http://www.ihes.fr/IHES/Publications/Publications.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

ON A FUNCTORIAL PROPERTY OF POWER RESIDUE SYMBOLS

Erratum to: *Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)*,
by Hyman BASS, John MILNOR and Jean-Pierre SERRE (*Publ. Math. I.H.E.S.*, **33**, 1967,
p. 59-137).

1. Statement of results

This concerns part (A.23) of the Appendix of the above paper (p. 90-92).

Let $k_1 \supset k$ be a finite extension of number fields, of degree $d = [k_1 : k]$. Denote by μ_k (resp. μ_{k_1}) the group of all roots of unity in k (resp. k_1), and by m (resp. m_1) the order of μ_k (resp. μ_{k_1}). We have

$$N_{k_1/k}(\mu_{k_1}) \subset \mu_k \subset \mu_{k_1}$$

and m divides m_1 .

It is easy to see (cf. (A.23, a)) that there is a unique endomorphism φ of μ_k such that

$$\varphi(z^{m_1/m}) = N_{k_1/k}(z) \quad \text{for all } z \in \mu_{k_1}.$$

Since μ_k is cyclic of order m , there is a well-defined element e of $\mathbf{Z}/m\mathbf{Z}$ such that $\varphi(z) = z^e$ for all $z \in \mu_k$. Two assertions about e are made in (A.23):

(A.23), b) *We have $e = (1 + m/2 + m_1/2) dm/m_1$; this makes sense because dm/m_1 has denominator prime to m .*

(A.23), c) *Let a be an algebraic integer of k , and let $\mathfrak{b}$ be an ideal of k prime to $m_1 a$; identify $\mathfrak{b}$ with the corresponding ideal of k_1 . Then*

$$\left(\frac{a}{\mathfrak{b}}\right)_{m_1} = \left(\left(\frac{a}{\mathfrak{b}}\right)_m\right)^e,$$

where the left subscript denotes the field in which the symbol is defined.

Both assertions are proved in (A.23) by a “dévissage” argument which is incorrect (the mistake occurs on p. 91 where it is wrongly claimed that one can break up the extension $k(\mu_{k_1})/k$ into layers such that the order of μ_k increases by a prime factor in each one).

The actual situation is:

Theorem 1. — Assertion (A.23), b) is false and assertion (A.23), c) is true.

To get a counter-example to (A.23), b), take for k_1 the field $\mathbf{Q}(\sqrt{2}, \sqrt{-1})$ of 8th-roots of unity, and for k either $\mathbf{Q}(\sqrt{2})$ or $\mathbf{Q}(\sqrt{-2})$. In both cases, we have

$m=2$, $m_1=8$, $d=2$; this shows that the denominator of dm/m_1 need not be prime to m . Moreover, a simple calculation shows that $e \in \mathbf{Z}/2\mathbf{Z}$ is equal to 0 in the first case and to 1 in the second case; hence, *there is no formula for e involving only d , m and m_1 .*

The truth of (A.23), c) will be proved in § 3 below.

Remark. — The reader can check that (A.23), b) was not used at any place in the original paper, except for a harmless quotation on p. 81.

2. A transfer property of Kummer theory

We generalize the notations of § 1 as follows:

k_1/k is a finite separable extension of commutative fields, $d=[k_1:k]$,
 μ (resp. μ_1) is a finite subgroup of k^* (resp. k_1^*), $m=[\mu:1]$ and $m_1=[\mu_1:1]$.

We make the following *assumption*:

$$(*) \quad N_{k_1/k}(\mu_1) \subset \mu \subset \mu_1.$$

As in § 1, this implies that m divides m_1 and that there is a well-defined element $e \in \mathbf{Z}/m\mathbf{Z}$ such that

$$N_{k_1/k}(z) = z^{em_1/m} \quad \text{for all } z \in \mu_1.$$

Let now $\bar{k}$ be a separable closure of k_1 , and put

$$G_1 = \text{Gal}(\bar{k}/k_1) \quad \text{and} \quad G = \text{Gal}(\bar{k}/k),$$

so that G_1 is an open subgroup of index d of G . Denote by G^{ab} (resp. G_1^{ab}) the quotient of G (resp. G_1) by the closure of its commutator group; this group is the Galois group of the maximal abelian extension k^{ab} (resp. k_1^{ab}) of k (resp. k_1) in $\bar{k}$. The transfer map (*Verlagerung*) is a continuous homomorphism

$$\text{Ver} : G^{\text{ab}} \rightarrow G_1^{\text{ab}}.$$

Let $a \in k^*$. Kummer theory attaches to a the continuous character

$$\chi_{k,m}^a : G^{\text{ab}} \rightarrow \mu$$

defined by:

$$\chi_{a,m}^k(s) = s(\alpha)\alpha^{-1} \quad \text{for } s \in G^{\text{ab}} \text{ and } \alpha \in k^{\text{ab}} \text{ with } \alpha^m = a.$$

Similarly, every element b of k_1^* defines a character

$$\chi_{k_1,m_1}^b : G_1^{\text{ab}} \rightarrow \mu_1,$$

and this applies in particular when $b = a$.

Theorem 2. — *If a belongs to k^* , the map*

$$\chi_{k_1,m_1}^a \circ \text{Ver} : G^{\text{ab}} \rightarrow G_1^{\text{ab}} \rightarrow \mu_1$$

takes values in μ , and is equal to the e -th-power of $\chi_{k,m}^a$.

Proof. — [In what follows, we write χ_a (resp. ψ_a) instead of $\chi_{k,m}^a$ (resp. χ_{k_1,m_1}^a); we view it indifferently as a character of G or G^{ab} (resp. of G_1 or G_1^{ab}).]

Let $(s_i)_{i \in I}$ be a system of representatives of the left cosets of $G \bmod G_1$; we have $G = \prod_{i \in I} s_i G_1$. If $s \in G$ and $i \in I$, we write ss_i as $ss_i = s_j t_i$, with $j \in I$, $t_i \in G_1$, and $\text{Ver}(s)$ is the image of $\prod_{i \in I} t_i$ in G_1^{ab} .

Let now $w : G \rightarrow \mu_1$ be the 1-cocycle defined by

$$w(s) = s(\lambda)\lambda^{-1}, \quad \text{where} \quad \lambda^{m_1} = a.$$

The restriction of w to G_1 is ψ_a . Hence we have

$$\psi_a(\text{Ver}(s)) = \prod_{i \in I} \psi_a(t_i) = \prod_{i \in I} w(t_i).$$

Since $t_i = s_j^{-1} s s_i$ and w is a cocycle, we get:

$$w(t_i) = w(s_j^{-1}) \cdot s_j^{-1}(w(s)) \cdot s_j^{-1}s(w(s_i)),$$

hence

$$\psi_a(\text{Ver}(s)) = h_1 h_2 h_3,$$

with $h_1 = \prod_{i \in I} w(s_j^{-1})$, $h_2 = \prod_{i \in I} s_j^{-1}(w(s))$ and $h_3 = \prod_{i \in I} s_j^{-1}s(w(s_i))$.

When i runs through I , the same is true for j , hence h_1 can be rewritten as $\prod w(s_i^{-1})$; on the other hand, since t_i acts trivially on μ_1 , we have $s_j^{-1}s(z) = t_i s_i^{-1}(z) = s_i^{-1}(z)$ for all $z \in \mu_1$, hence $h_3 = \prod s_i^{-1}(w(s_i)) = \prod w(s_i)^{-1}$ since w is a cocycle. This shows that $h_1 h_3 = 1$, hence

$$\psi_a(\text{Ver}(s)) = h_2 = N_{k_1/k}(w(s)) = w(s)^{em_1/m}.$$

Put now $\alpha = \lambda^{m_1/m}$. We have $\alpha^m = a$, hence

$$\chi_a(s) = s(\alpha)\alpha^{-1} = w(s)^{m_1/m} \quad \text{for all } s \in G.$$

This shows that

$$\psi_a(\text{Ver}(s)) = \chi_a(s)^e, \quad \text{q.e.d.}$$

Remark. — When $m = m_1$, we have $e = d$ and th. 2 reduces to a special case of the well-known formula

$$\chi_{k_1,m}^b \circ \text{Ver} = \chi_{k,m}^a,$$

valid for $b \in k_1^*$ and $a = N_{k_1/k}(b) \in k^*$.

3. The number field case

We keep the notations of § 2, and assume that k is a *number field*. If $\mathfrak{b}$ is an *idèle* of k , we denote by $s_k^{\mathfrak{b}}$ the element of G^{ab} attached to $\mathfrak{b}$ by class field theory; for every

$a \in k^*$, we define an element $\left(\frac{a}{\mathfrak{b}}\right)_m$ of μ by:

$$\left(\frac{a}{\mathfrak{b}}\right)_m = \chi_{k,m}^a(s_k^{\mathfrak{b}}).$$

Similar definitions apply to k_1 and m_1 .

Theorem 3. — If a (resp. $\mathbf{b}$) is an element of k^* (resp. an idèle of k), we have

$$\left(\frac{a}{\mathbf{b}}\right)_{k_1, m_1} = \left(\left(\frac{a}{\mathbf{b}}\right)_m\right)^e.$$

This follows from th. 2 and the known fact that $s_{k_1}^{\mathbf{b}} = \text{Ver}(s_k^{\mathbf{b}})$.

Proof of (A.23), c). — Assume now a to be an integer of k , and let $\mathbf{b}$ be an ideal of k prime to $m_1 a$. Choose for $\mathbf{b}$ an idèle with the following properties:

- (i) the v -th component of $\mathbf{b}$ is 1 if the place v is archimedean, or is ultrametric and divides $m_1 a$;
- (ii) the ideal associated to $\mathbf{b}$ is $\mathbf{b}$.

It is then easy to check that

$$\left(\frac{a}{\mathbf{b}}\right)_m = \left(\frac{a}{\mathbf{b}}\right)_m \quad \text{and} \quad \left(\frac{a}{\mathbf{b}}\right)_{k_1, m_1} = \left(\frac{a}{\mathbf{b}}\right)_{m_1}.$$

Hence (A.23), c) follows from th. 3.

4. The local case

We keep the notations of § 2, and assume that k is a *local field*, i.e. is complete with respect to a discrete valuation with finite residue field. If $b \in k^*$, we denote by s_k^b the element of G^{ab} attached to b by local class field theory; if $a \in k^*$, the Hilbert symbol $\left(\frac{a, b}{k}\right)_m \in \mu$ is defined by

$$\left(\frac{a, b}{k}\right)_m = \chi_{k, m}^a(s_k^b).$$

Theorem 4. — If a, b are elements of k^* , we have:

$$\left(\frac{a, b}{k_1}\right)_{m_1} = \left(\left(\frac{a, b}{k}\right)_m\right)^e.$$

This follows from th. 2 and the known fact that $s_{k_1}^b = \text{Ver}(s_k^b)$.

Remark. — It would have been possible to prove th. 4 first, and deduce th. 3 and (A.23), c) from it.

Manuscrit reçu le 7 mai 1974.