PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

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>

ON A FUNCTORIAL PROPERTY OF POWER RESIDUE SYMBOLS

Erratum to: *Solution of the congruence subgroup problem for* SL_n $(n \geqslant 3)$ *and* $\mathrm{S}p_{2n}$ $(n \geqslant 2)$, 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

$$\mathrm{N}_{k_1/k}(\mu_{k_1}) \subset \mu_k \subset \mu_{k_1}$$

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

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

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*

$$_{k_1}\!\left(\frac{a}{\mathfrak{b}}\right)_{m_1} = \left(_{k}\!\left(\frac{a}{\mathfrak{b}}\right)_{m}\right)^{e},$$

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*:

$$(*)\qquad \mathrm{N}_{k_1/k}(\mu_1)\subset\mu\subset\mu_1.$$

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

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

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

$$\mathrm{G}_1=\mathrm{Gal}(\bar{k}/k_1)\quad\text{and}\quad \mathrm{G}=\mathrm{Gal}(\bar{k}/k),$$

so that G_1 is an open subgroup of index d of G. Denote by G^{ab} (resp. $\mathrm{G}_1^{\mathrm{ab}}$) 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

$$\mathrm{Ver}:\mathrm{G}^{\mathrm{ab}}\to\mathrm{G}_1^{\mathrm{ab}}.$$

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

$$\chi^a_{k,m}:\mathrm{G}^{\mathrm{ab}}\to\mu$$

defined by:

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

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

$$\chi^b_{k_1,m_1}:\mathrm{G}_1^{\mathrm{ab}}\to\mu_1,$$

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

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

$$\chi^a_{k_1,m_1}\circ\mathrm{Ver}:\mathrm{G}^{\mathrm{ab}}\to\mathrm{G}_1^{\mathrm{ab}}\to\mu_1$$

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

Proof. — [In what follows, we write χ_a (resp. ψ_a) instead of $\chi^a_{k,m}$ (resp. $\chi^a_{k_1,m_1}$); 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 mod. G_1; we have $G=\coprod_{i\in I} s_iG_1$. If $s\in G$ and $i\in I$, we write ss_i as $ss_i=s_jt_i$, with $j\in I$, $t_i\in G_1$, and $\mathrm{Ver}(s)$ 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

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

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

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

hence

$$\psi_a(\mathrm{Ver}(s))=h_1h_2h_3,$$

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 $s_j^{-1}s(z)=t_is_i^{-1}(z)=s_i^{-1}(z)$ 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 $h_1h_3=1$, hence

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

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

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

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

$$\chi^b_{k_1,m}\circ\mathrm{Ver}=\chi^a_{k,m},$$

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 $\boldsymbol{b}$ is an *idèle* of k, we denote by $s_k^{\boldsymbol{b}}$ the element of G^{ab} attached to $\boldsymbol{b}$ by class field theory; for every $a\in k^*$, we define an element ${}_k\left(\frac{a}{\boldsymbol{b}}\right)_m$ of μ by:

$${}_k\left(\frac{a}{\boldsymbol{b}}\right)_m=\chi^a_{k,m}(s_k^{\boldsymbol{b}}).$$

Similar definitions apply to k_1 and m_1.

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

$${}_{k_1}\!\left(\frac{a}{\boldsymbol{b}}\right)_{m_1} = \left({}_{k}\!\left(\frac{a}{\boldsymbol{b}}\right)_{m}\right)^{e}.$$

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

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

(i) the v-th component of $\boldsymbol{b}$ is 1 if the place v is archimedean, or is ultrametric and divides $m_1 a$;

(ii) the ideal associated to $\boldsymbol{b}$ is $\mathfrak{b}$.

It is then easy to check that

$${}_{k}\!\left(\frac{a}{\mathfrak{b}}\right)_{m} = {}_{k}\!\left(\frac{a}{\boldsymbol{b}}\right)_{m} \quad \text{and} \quad {}_{k_1}\!\left(\frac{a}{\mathfrak{b}}\right)_{m_1} = {}_{k_1}\!\left(\frac{a}{\boldsymbol{b}}\right)_{m_1}.$$

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

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

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 $s_{k_1}^b = \mathrm{Ver}(s_k^b)$.

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.