

# THE SCHUR SUBGROUP OF THE BRAUER GROUP OF A LOCAL FIELD

Autor(en): **Riehm, C.**

Objektyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **34 (1988)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.04.2024**

Persistenter Link: <https://doi.org/10.5169/seals-56585>

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

# THE SCHUR SUBGROUP OF THE BRAUER GROUP OF A LOCAL FIELD

by C. RIEHM <sup>1)</sup>

For any field  $K$  of characteristic 0, the Schur subgroup  $S(K)$  of the Brauer group  $B(K)$  consists of those Brauer classes  $\beta$  arising as follows: there exists a finite group  $G$  such that one of the simple components of the group algebra  $KG$  lies in  $\beta$ . Now let  $K$  be a local field, i.e. a finite extension of  $\mathbf{Q}_p$ . Let  $\mathbf{Q}_p^c$  be the cyclotomic closure of  $\mathbf{Q}_p$  — the field generated over  $\mathbf{Q}_p$  by adjunction of all roots of unity — and let  $K_c = K \cap \mathbf{Q}_p^c$ .

THEOREM.  $S(K) \cong \text{tor } \mathcal{G}(\mathbf{Q}_p^c/K_c)$ , the torsion subgroup of the Galois group of  $\mathbf{Q}_p^c$  over  $K_c$ .

The determination of  $S(K)$  when  $K$  is local was first carried out by T. Yamada (see [Y]) and, in the non-dyadic case, by J.-M. Fontaine [F], although their formulations differ considerably from the above one — see the remarks at the end of the paper. In the non-dyadic case, our proof uses the cup product pairing and norm residue symbol of local class field theory and is quite different than earlier proofs. In the dyadic case, our proof combines the ideas of T. Yamada, G.J. Janusz, F. Lorenz, and U. Jannsen. It is not the most elementary one known — the proof of Janusz stands out in that regard. But it seems to me that it is somewhat more conceptual and more transparent than the others, in spite of the fact that it uses more sophisticated methods. Some remarks are made at the beginning of the section on the dyadic case concerning the possibility of a unified proof for dyadic and non-dyadic fields.

The work on this problem was carried out while I was on sabbatical leave at l'Université de Lausanne and Universität Münster, and I wish to thank both institutions heartily for their hospitality and financial support.

---

<sup>1)</sup> Support by N.S.E.R.C. grant #A8778 gratefully acknowledged.

## K NON-DYADIC

We begin with a well known lemma, valid for an arbitrary field of characteristic 0.

LEMMA. Let  $K_0$  be a subfield of  $K$  which contains  $\mathbf{Q}^c \cap K$ . Then

$$S(K) = K \otimes S(K_0)$$

where  $K \otimes S(K_0)$  denotes the subgroup of  $B(K)$  obtained from  $S(K_0)$  by extension of scalars.

*Proof.* See Prop. 4.6 in [Y]; a proof of a more general result can be found in [M]. Since the proof is short, we give it here. We can assume  $K_0 = \mathbf{Q}^c \cap K$ . Let  $\beta \in S(K)$  and let  $A$  be a Schur algebra in  $\beta$ , i.e. a simple component of some group algebra  $KG$  with Brauer class  $[A] = \beta$ . Then  $A$  is also a direct summand of  $K \otimes A_0$  for some simple component  $A_0$  of  $K_0G$ . But the center of  $A_0$  is a sub-cyclotomic extension of  $K_0$  (see exercise 9.15, [I], e.g.), so is  $K$  since it is also contained in  $K$ . Thus  $[A_0] \in S(K_0)$  and  $A = K \otimes A_0$ . It follows that  $S(K) \subseteq K \otimes S(K_0)$  and the reverse inclusion is obvious.  $\square$

This lemma allows us to assume, from now on, that  $K$  is a sub-cyclotomic extension of  $\mathbf{Q}_p$ , i.e. a (finite) abelian extension of  $\mathbf{Q}_p$ .

We shall denote the group of roots of unity of a field  $L$  by  $\mu(L)$ . The subgroup of roots of unity of order a power of  $p$ , resp. of order relatively prime to  $p$ , is denoted by  $\mu(L)_p$  resp.  $\mu(L)_{p'}$ . The group of all roots of unity, i.e.  $\mu(\mathbf{Q}_p^c)$ , will be denoted by  $\mu$ , with  $\mu_2$  and  $\mu_{2'}$  having the obvious meanings.

Assume now that  $p$  is odd. Since  $\mu(\mathbf{Q}_p)$  is  $\cong \mathbf{Z}/p-1$ , the root of unity theorem of Benard and Schacher (Th. 6.1, [Y]) and the fact that  $B(\mathbf{Q}_p) \cong \mathbf{Q}/\mathbf{Z}$  (see [S], e.g.) imply that  $S(\mathbf{Q}_p) \hookrightarrow \mathbf{Z}/p-1$ . (In fact this map is an isomorphism). By the theory of central simple algebras over a local field, we can identify  $B(K)$  with  $H^2(\mathcal{G}(\mathbf{Q}_p^c/K), (\mathbf{Q}_p^c)^*)$ , (which we also denote by  $H^2(\mathbf{Q}_p^c/K)$ ). By the Brauer-Witt theorem (Cor. 3.11, [Y]),  $S(K)$  is thereby identified with the image of the canonical map

$$H^2(\mathcal{G}(\mathbf{Q}_p^c/K), \mu) \rightarrow H^2(\mathcal{G}(\mathbf{Q}_p^c/K), (\mathbf{Q}_p^c)^*), \quad (\mu = \mu(\mathbf{Q}_p^c)),$$

which we denote by  $H_c^2(\mathbf{Q}_p^c/K)$ . The (cohomological) corestriction map  $B(K) \rightarrow B(\mathbf{Q}_p)$  carries  $S(K)$  into  $S(\mathbf{Q}_p)$  since, on the cocycle level, it takes a cocycle  $f$  to a cocycle whose values are products of the values of  $f$  (see [W], e.g.). Furthermore the corestriction is injective in this case

(p. 175, [S]) and so  $S(K)$  is finite — in fact it is a subgroup of  $\mathbb{Z}/p-1$ . We may therefore choose a primitive  $m^{\text{th}}$  root of unity  $\varepsilon_m$  so that

$$S(K) = H_c^2(\mathbb{Q}_p(\varepsilon_m)/K).$$

We may also assume that  $p \mid m$ , i.e. that  $\varepsilon_p \in \mathbb{Q}_p(\varepsilon_m)$ .

We now show that  $\mathbb{Q}_p(\varepsilon_m)$  can be replaced by a field  $L$  so that  $L/K$  is cyclic and totally tamely ramified. First of all, by Lemma 4.1, [Y], we can assume that  $\mathbb{Q}_p(\varepsilon_m)$  is the (disjoint) compositum  $UV$  of an unramified extension  $U/K$  and a totally ramified extension  $V/K$ . Since the order of  $S(K)$  is relatively prime to  $p$ ,  $S(K)$  is the image  $H_c^2(\mathbb{Q}_p(\varepsilon_m)/K)'$  of the canonical map

$$H^2(\mathcal{G}(\mathbb{Q}_p(\varepsilon_m)/K), \mu(\mathbb{Q}_p(\varepsilon_m))_{p'}) \rightarrow H^2(\mathbb{Q}_p(\varepsilon_m)/K).$$

Since  $UV/V$  is unramified,  $N_{UV/V}(\mu(UV)_{p'}) = \mu(V)_{p'}$ , and it follows from the inflation-restriction sequence (see Lemme 1, [F]) that the inflation

$$H^2(\mathcal{G}(V/K), \mu(V)_{p'}) \rightarrow H^2(\mathcal{G}(UV/K), \mu(UV)_{p'})$$

is an isomorphism (since  $UV/V$  cyclic implies that  $H^2(\mathcal{G}(UV/V), \mu(UV)_{p'}) \cong H^0(\mathcal{G}(UV/V), \mu(UV)_{p'}) = 1$ ). Thus  $S(K) = H_c^2(V/K)'$ . Let  $L/K$  be the tamely ramified part of  $V/K$ . Since the  $p'$  roots of unity in a local field are the same as the non-zero elements in the residue class field,  $\mu(V)_{p'} = \mu(L)_{p'} = \mu(K)_{p'}$  and so  $N_{V/L}(\mu(V)_{p'}) = \mu(L)_{p'}$  because  $(V:L)$  is a power of  $p$ . Once again the inflation-restriction sequence shows that  $S(K) = H_c^2(L/K)'$ .

Consider now the cup product pairing

$$(1) \quad \cup : \mathcal{G}(L/K) \times H^2(L/K) \rightarrow K^*/N_{L/K}L^*.$$

See for example pp. 139-140, [C-F]. It is known that there is a "canonical class"  $u_{L/K}$  in  $H^2(L/K)$  with the property that the map  $\sigma \mapsto \sigma \cup u_{L/K}$  is an isomorphism  $\mathcal{G}(L/K) \rightarrow K^*/N_{L/K}L^*$ . It follows that if  $\sigma$  is a generator of  $\mathcal{G}(L/K)$ , the map

$$\sigma \cup : H^2(L/K) \rightarrow K^*/N_{L/K}L^*$$

is also an isomorphism. We wish to identify the image of  $H_c^2(L/K)'$  under this map. The cohomology class  $[f]$  of the cocycle  $f$  has image  $\prod_{\tau} f(\tau, \sigma) \bmod N_{L/K}L^*$  (Lemme 4, p. 186, [S]). Since  $\mathcal{G}(L/K)$  is cyclic with generator  $\sigma$ , every cohomology class with coefficients in an arbitrary  $\mathcal{G}(L/K)$ -module  $A$  is represented by a cocycle  $f$  of the form



$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i+j < d, \\ a & \text{if } i+j \geq d. \end{cases}$$

Here  $d = |\mathcal{G}(L/K)|$ ,  $0 \leq i, j < d$ , and  $a$  is an arbitrary element of  $A^{\mathcal{G}(L/K)}$ . If  $A = L^*$ , it follows that a class in  $H^2(L/K)$  is in  $H_c^2(L/K)'$  iff it contains such an  $f$  with  $a \in \mu(K)_{p'}$ . Since it is clear that  $\sigma \cup [f] = a \bmod N_{L/K}L^*$ , we see that the image of  $H_c^2(L/K)'$  is

$$\mu(K)_{p'} N_{L/K} L^* / N_{L/K} L^* \cong \mu(K)_{p'} / \mu(K)_{p'} \cap N_{L/K} L^*.$$

But it is easy to see that  $\mu(K)_{p'} \cap N_{L/K} L^* = N_{L/K} \mu(L)_{p'}$  so we have an isomorphism

$$S(K) = \mu(K)_{p'} / N_{L/K} \mu(L)_{p'}$$

depending only on the choice of  $\sigma$ .

We now show that the norm residue symbol

$$v_K = ( \ , \mathbf{Q}_p^c / K ) : K^* \rightarrow \mathcal{G}(\mathbf{Q}_p^c / K)$$

induces an isomorphism of  $\mu(K)_{p'} / N_{L/K} \mu(L)_{p'}$  onto  $\text{tor } \mathcal{G}(\mathbf{Q}_p^c / K)$ . It is clear that the image of  $\mu(K)_{p'}$  is contained in  $\text{tor } \mathcal{G}(\mathbf{Q}_p^c / K)$ . Let  $v = ( \ , \mathbf{Q}_p^c / \mathbf{Q}_p )$ . The diagram

$$\begin{array}{ccc} K^* & \xrightarrow{v_K} & \mathcal{G}(\mathbf{Q}_p^c / K) \\ N_{K/\mathbf{Q}_p} \downarrow & & \downarrow \text{incl.} \\ \mathbf{Q}_p^* & \xrightarrow{v} & \mathcal{G}(\mathbf{Q}_p^c / \mathbf{Q}_p) \end{array}$$

is commutative (Prop. 10, ch. XIII, [S]). Recall now that  $\varepsilon_p \in \mathbf{Q}_p(\varepsilon_m)$ . It follows that the tame ramification index of  $L/\mathbf{Q}_p$  is  $p-1$ . Therefore if  $L'/\mathbf{Q}_p$  is the maximal unramified subextension of  $L/\mathbf{Q}_p$ , then  $(L:L')$  is a  $p$ -power multiple of  $p-1$ . Since  $\mu(L)_{p'} = \mu(L')_{p'}$  and  $N_{L'/\mathbf{Q}_p} \mu(L')_{p'} = \mu(\mathbf{Q}_p)_{p'} \cong \mathbf{Z}/p-1$ , the kernel  $\kappa$  of the restriction of  $N_{K/\mathbf{Q}_p}$  to  $\mu(K)_{p'}$  is  $\subseteq N_{L/K} \mu(L)_{p'}$ . On the other hand if one factors  $N_{K/\mathbf{Q}_p}$  through the tame and unramified closures of  $\mathbf{Q}_p$  in  $K$ , one sees that  $N_{L/K}$  on  $\mu(K)_{p'}$  is  $\varepsilon \mapsto \varepsilon^{e(p^f-1)/(p-1)}$  where  $e$  and  $f$  are resp. the ramification and inertial indices of  $K/\mathbf{Q}_p$ . It follows that  $\kappa = N_{L/K} \mu(L)_{p'}$  which is equal to  $\ker v_K \mid_{\mu(K)_{p'}}$  since  $v$  is injective.

Now  $v$  maps the torsion subgroup  $\mu(\mathbf{Q}_p) \cong \mathbf{Z}/p-1$  of  $\mathbf{Q}_p^*$  onto the torsion subgroup of  $\mathcal{G}(\mathbf{Q}_p^c / \mathbf{Q}_p)$ . Furthermore an element  $a \in \mathbf{Q}_p^*$  is mapped into  $\mathcal{G}(\mathbf{Q}_p^c / K)$  iff  $a \in N_{K/\mathbf{Q}_p} K^*$ . It follows at once that  $v$  maps  $N_{K/\mathbf{Q}_p} \mu(K)_{p'}$  isomorphically onto  $\text{tor } \mathcal{G}(\mathbf{Q}_p^c / K)$ . This proves our main theorem in the case  $p$  odd.

## K DYADIC

It would be very nice to have a unified proof for the dyadic and non-dyadic cases along the lines of the one above for the non-dyadic case. However that would require a "deflation"  $H_c^2(V/K) \cong H_c^2(L/K)$  to some *cyclic* extension  $L/K$  in order that the cup product pairing (1) be non-degenerate on both sides. U. Jannsen has shown that this is impossible in general. Since  $H^2(L_1/K) = H^2(L_2/K)$  (when inflated to a common extension) if  $(L_1:K) = (L_2:K)$ , one can try to replace the cyclotomic extension  $V/K$  by a some cyclic but possibly non-cyclotomic extension to achieve non-degeneracy. This is done, however, at the expense of losing the identification of  $S(K)$  as the subgroup of cyclotomic cocycles. This is essentially what is done in the second half of the following proof.

Since  $\mu(\mathbf{Q}_2) = \pm 1$ , it follows (as in the non-dyadic case) that  $S(K)$  is 1 or  $\pm 1$ . Thus to prove the theorem it suffices to show that

$$(2) \quad S(K) \neq 1 \Leftrightarrow -1 \in \mathcal{G}(\mathbf{Q}_2^c/K).$$

Before beginning we recall a few facts about Galois groups of  $\mathbf{Q}_2^c$ . Let  $\varepsilon_m$  be a primitive  $m^{\text{th}}$  root of unity and write  $m = 2^n m'$  where  $m'$  is odd. Let  $f$  be the smallest integer such that  $m' \mid 2^f - 1$ . Then if  $n \geq 2$ ,

$$\mathcal{G}(\mathbf{Q}_2(\varepsilon_m)/\mathbf{Q}_2) \cong \mathbf{Z}/f \times (\mathbf{Z}/2^n)^* \cong \mathbf{Z}/f \times \mathbf{Z}/2^{n-2} \times \mathbf{Z}/2.$$

Taking  $\varprojlim$  over  $m$  one gets

$$(3) \quad \mathcal{G}(\mathbf{Q}_2^c/\mathbf{Q}_2) \cong \hat{\mathbf{Z}} \times \hat{\mathbf{Z}}_2 \times \mathbf{Z}/2.$$

The topological generator 1 of  $\hat{\mathbf{Z}}$  is the Frobenius of the maximal unramified extension  $\mathbf{Q}_2(\mu_{2'})$  of  $\mathbf{Q}_2$ . The topological generator 1 of  $\hat{\mathbf{Z}}_2$  and the generator 1 of  $\mathbf{Z}/2$  are the automorphisms of the field  $\mathbf{Q}_2(\mu_2)$  determined by  $\varepsilon \mapsto \varepsilon^5$  and  $\varepsilon \mapsto \varepsilon^{-1}$  resp. for all  $\varepsilon \in \mu_2$  (see e.g. [H], § 4, 5). We shall denote these automorphisms by  $\sigma_5$  and  $\sigma_{-1}$  resp.

From (3) we get a "primary decomposition"

$$(4) \quad \mathcal{G}(\mathbf{Q}_2^c/\mathbf{Q}_2) \cong \prod_{p \neq 2} \hat{\mathbf{Z}}_p \times (\hat{\mathbf{Z}}_2 \times \hat{\mathbf{Z}}_2 \times \mathbf{Z}/2)$$

since  $\hat{\mathbf{Z}} \cong \prod \hat{\mathbf{Z}}_p$ . Since  $\mathcal{G}(\mathbf{Q}_2^c/K)$  is an open subgroup, one can show that the isomorphism implied in (4) restricts to an isomorphism

$$\mathcal{G}(\mathbf{Q}_2^c/K) \cong \prod_{p \neq 2} k_p \hat{\mathbf{Z}}_p \times C_K \cong \hat{\mathbf{Z}} \times \hat{\mathbf{Z}}_2 \times D_K$$

where  $C_K$  is a  $\hat{\mathbf{Z}}_2$ -submodule of finite index in the component  $\hat{\mathbf{Z}}_2 \times \hat{\mathbf{Z}}_2 \times \mathbf{Z}/2$  of (4),  $k_p$  is an integer (or a power of  $p$ ) = to 1 for almost all  $p$ , and  $D_K$  is either the trivial group or  $\langle \sigma_{-1} \rangle$ .

We now begin the proof of (2). Suppose first that  $\sigma_{-1} \notin \mathcal{G}(\mathbf{Q}_2^c/K)$ , i.e. that  $\mathcal{G}(\mathbf{Q}_2^c/K) \cong \hat{\mathbf{Z}} \times \hat{\mathbf{Z}}_2$ . It suffices to show that  $H^2(\mathcal{G}(\mathbf{Q}_2^c/K), \mu_2)$  is trivial. Let  $K_{nr}$  be the unramified closure of  $K$  in  $\mathbf{Q}_2^c$ . Then  $K_{nr} = K(\mu_{2^r})$  and  $\mathcal{G}(K_{nr}/K) \cong \hat{\mathbf{Z}}$ .

Let  $C_n$  denote the cyclic group of order  $n$ .

LEMMA. Suppose  $C_{2^k}$  operates faithfully on  $C_{2^h}$ . Then  $H^n(C_{2^k}, C_{2^h}) = 1$  for all  $n \geq 1$  except in one case:  $k = 1$  and the non-trivial automorphism in  $C_2$  inverts the elements of  $C_{2^h}$  (i.e. " $C_{2^k} = \langle \sigma_{-1} \rangle$ ").

This is a well-documented fact, although perhaps not exactly in this form (see e.g. [N], 4.8, or the proof of Lemma 2, [L]). By the Herbrand theory for the cohomology of cyclic groups (see e.g. [S], ch. VIII, § 4), it suffices to show that  $\hat{H}^0(C_{2^k}, C_{2^h}) = 1$ , i.e. that every fixed element is a norm. There is generator of  $C_{2^k}$  which acts by raising the elements of  $C_{2^h}$  to either the power  $5^{2^{h-k-2}}$ , or possibly the power  $-5$  if  $k = h-2$  (again [H], § 4, 5). Then a straightforward calculation leads to the desired result (one uses the fact that  $2^{r+2} \parallel (5^{2^r} - 1)$  for all  $r \geq 0$ ).  $\square$

Since

$$\mathbf{Q}_2^c = K_{nr}(\mu_2), H^n(\mathcal{G}(\mathbf{Q}_2^c/K_{nr}), \mu_2) = \varinjlim H^n(\mathcal{G}(L/K_{nr}), \mu(L)_2)$$

where  $L$  runs over the fields  $K_{nr}(\varepsilon_{2^h})$ , and so is trivial by the lemma for  $n \geq 1$ . Thus the inflation-restriction sequence (p. 126, [C-F])

$$1 \rightarrow H^2(\mathcal{G}(K_{nr}/K), \mu(K_{nr})_2) \rightarrow H^2(\mathcal{G}(\mathbf{Q}_2^c/K), \mu_2) \rightarrow H^2(\mathcal{G}(\mathbf{Q}_2^c/K_{nr}), \mu_2) = 1$$

is exact whence the inflation is an isomorphism. But  $\mathcal{G}(K_{nr}/K) = \hat{\mathbf{Z}}$  has cohomological dimension 1, so  $H^2(\mathcal{G}(K_{nr}/K), \mu(K_{nr})_2)$  is 1, hence  $H^2(\mathcal{G}(\mathbf{Q}_2^c/K), \mu_2)$  is also 1 as desired. (I am grateful to U. Jannsen for the foregoing proof).

We now assume that  $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/K)$ . This part of the proof is derived from pp. 540-542 in [J] and pp. 467-468, [L]. (F. Lorenz has asked me to point out that the proof on pp. 465-466 of the latter paper is incomplete — one must show that  $\rho$  is the identity on  $k$ .)

LEMMA 1.  $K(\varepsilon_4)/K$  is ramified of degree 2.

*Proof.* It is clear that the extension is of degree 2. Suppose it is unramified. Let  $q$  be the number of elements in the residue class field of

$K(\varepsilon_4)$ . Then  $K(\varepsilon_4) = K(\varepsilon_{q-1})$ . But  $K(\varepsilon_{q-1})$  is left element-wise fixed by  $\sigma_{-1}$ , which contradicts the fact that  $\varepsilon_4$  is *not* left fixed.  $\square$

Let  $h$  be the smallest integer  $\geq 2$  such that there is an odd integer  $m$  with the property that  $L = \mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_m)$  contains  $K$ . By replacing  $m$  by a suitable multiple, we can suppose that the residue class degree of  $L/K$

$$f(L/K) \equiv 0 \pmod{2^h}.$$

Let  $\mathcal{G}$  be the Galois group of this extension. We shall construct a Schur class of  $K$  using  $L/K$ . For this we use the following very useful lemma. Let  $G$  be a finite abelian group, written as the direct sum of cyclic subgroups:

$$G = C_1 \oplus C_2 \oplus \dots \oplus C_r,$$

where each  $C_i$  is of order  $c_i$  with generator  $\sigma_i$ . Let  $A$  be a  $G$ -module, written multiplicatively. Define the operators  $\Delta_{\sigma_i}$  and  $N_{\sigma_i}$  on  $A$  by

$$\Delta_{\sigma_i} a = a^{\sigma_i^{-1}}, N_{\sigma_i} a = a^{1 + \sigma_i + \sigma_i^2 + \dots + \sigma_i^{c_i - 1}}.$$

LEMMA. Let  $\gamma$  be a cohomology class in  $H^2(G, A)$ , and let  $f$  be a normalized cocycle in  $\gamma$ . Then the elements

$$\begin{aligned} a_i &= f(\sigma_i, \sigma_i) f(\sigma_i^2, \sigma_i) \dots f(\sigma_i^{c_i - 1}, \sigma_i), \\ a_{ij} &= f(\sigma_i, \sigma_j) / f(\sigma_j, \sigma_i) \quad (i \neq j) \end{aligned} \tag{5}$$

satisfy the following relations:

$$\Delta_{\sigma_i} a_j = \begin{cases} 1 & \text{if } i = j \\ N_{\sigma_j} a_{ij} & \text{if } i \neq j \end{cases}, \tag{6}$$

$$a_{ij} a_{ji} = 1 \quad (i \neq j), \quad \Delta_{\sigma_i} a_{jk} \cdot \Delta_{\sigma_j} a_{ki} \cdot \Delta_{\sigma_k} a_{ij} = 1 \quad (i, j, k \text{ distinct}).$$

Conversely if we have elements  $a_i$  and  $a_{ij}$  in  $A$  satisfying (6), then there is a uniquely determined cohomology class  $\gamma$  in  $H^2(G, A)$  and a normalized cocycle  $f$  in  $\gamma$  bearing the relationship (5) to the  $a_i$  and  $a_{ij}$ .

*Proof.* This is just a restatement of the abelian case of [Z], III, § 8, Theorem 22, in terms of cocycles. See also [Y], pp. 15-19.  $\square$

We now apply this to the situation at hand:  $G = \mathcal{G}$  and  $A = \mu(L)_2 = \langle \varepsilon_{2^h} \rangle$ . First of all we note that the restriction  $\sigma_1$  of  $\sigma_{-1}$  to  $L$  is a non-trivial element of  $\mathcal{G}$ , and that the minimality of  $h$  implies that

$K(\varepsilon_4, \varepsilon_m) = K(\varepsilon_{2^h}, \varepsilon_m) = L$  (see e.g. Lemma 3.3, [J]). Since  $K(\varepsilon_4)/K$  is ramified and  $K(\varepsilon_m)$  is unramified (because  $m$  is odd),  $\mathcal{G}$  is the direct product of the Galois groups  $\langle \sigma_1 \rangle$  of  $L/K(\varepsilon_m)$  and  $\langle \sigma_2 \rangle$  (say) of  $L/K(\varepsilon_4)$  of orders 2 and  $f$  respectively. We now choose  $a_1 = 1 = a_2$  and  $a_{12} = \varepsilon_{2^h} = a_{21}^{-1}$ . Then  $N_{\sigma_1} a_{21} = \varepsilon_{2^h}^{-1} \varepsilon_{2^h} = 1$  and  $N_{\sigma_2} a_{12} = \varepsilon_{2^h}^s$  where, if  $\sigma_2(\varepsilon_{2^h}) = \varepsilon_{2^h}^r$ ,

$$s = 1 + r + r^2 + \dots + r^{f-1}.$$

Since  $\sigma_2(\varepsilon_4) = \varepsilon_4$ , we have  $r \equiv 1 \pmod{4}$ .

Claim:  $s \equiv 0 \pmod{2^h}$ . If  $\sigma_2(\varepsilon_{2^h}) = \varepsilon_{2^h}$ , we choose  $r = 1$ ; then  $s = f \equiv 0 \pmod{2^h}$ .

Suppose then that  $\sigma_2(\varepsilon_{2^h}) \neq \varepsilon_{2^h}$ , and write  $s = (r^f - 1)/(r - 1)$ . Now  $r = 1 + 2^k a$  where  $h > k \geq 2$  and  $a$  is odd. By induction  $r^{2^i} = 1 + 2^{k+i} a_i$  ( $a_i$  an odd integer) for all  $i \geq 0$ , whence the claim.

It follows of course that  $N_{\sigma_2} a_{12} = 1$ . Therefore the above lemma provides a 2-cocycle  $f$  with coefficients in  $\langle \varepsilon_{2^h} \rangle$ . We now consider it to have coefficients in  $L^*$  and so its cohomology class  $\gamma = [f]$  is a Schur class in  $B(K)$ . We shall show that this class is non-trivial, which will finish the proof of the theorem. This will be effected by showing that  $\gamma$  is the inflation of a non-trivial Brauer class arising from the extension  $K(\varepsilon_m)/K$  — this latter class will not arise from a cyclotomic cocycle but this of course does not matter.

We shall use the crossed-product algebra  $A = (L/K, f)$  in order to carry this out. As a vector space over  $L$  it has a basis  $u_1^i u_2^j$  where  $0 \leq i < 2$  and  $0 \leq j < f$ , with  $u_1^2 = 1 = u_2^f$  and  $u_1 u_2 u_1^{-1} u_2^{-1} = \varepsilon_{2^h}$ . We replace  $u_2$  by  $u'_2 = \pi u_2$  where  $\pi = \varepsilon_4(1 - \varepsilon_{2^h})$ . The new parameters are

$$a'_1 = u_1^2 = 1, \quad a'_{12} = u_1 u'_2 u_1^{-1} u'_2^{-1} = 1, \quad a'_2 = u'^f_2 = N_{\sigma_2} \pi.$$

By (6),  $\Delta_{\sigma_1} a'_2 = N_{\sigma_2} a'_{12} = 1$  and  $\Delta_{\sigma_2} a'_2 = 1$ , so  $N_{\sigma_2} \pi \in K$ . Since  $u_1$  and  $u'_2$  commute with each other, it follows easily that

$$A = (K(\varepsilon_4)/K, 1) \otimes (K(\varepsilon_m)/K, N_{\sigma_2} \pi).$$

The first of these crossed-product algebras is clearly split but the second is *not* split:  $\pi$  is a prime element of  $L$ , so  $N_{\sigma_2} \pi$  has order (valuation)  $f$  in  $K(\varepsilon_4)$  ( $L/K(\varepsilon_4)$  is unramified), hence order  $1/2 f$  in  $K$  ( $K(\varepsilon_4)/K$  is ramified); but the (non-zero) norms in  $K$  from  $K(\varepsilon_m)$  are exactly the elements whose order is a multiple of  $f$  (since the extension is unramified of degree  $f$ ). Thus  $A$  is not split, as desired.  $\square$

## REMARKS

There are several proofs and several formulations of this result ( $S(K)$  when  $K$  is dyadic) in the literature. We shall briefly indicate why these formulations are, with one exception, equivalent to the above one.

1. T. Yamada, [Y], p. 88. One formulation of Yamada's theorem is that  $S(K)$  is non-trivial iff there is a root of unity  $\zeta$  such that the inertia group of the extension  $\mathbf{Q}_2(\zeta)/K$  is non-cyclic. The inertia group of  $\mathbf{Q}_2(\zeta)/K$  is the image of the inertia group of  $\mathcal{G}(\mathbf{Q}_2^c/K)$ , namely  $\mathcal{G}(\mathbf{Q}_2^c/K_{nr})$ . The latter group is of the form  $\hat{\mathbf{Z}}_2 \times (\mathbf{Z}/2)$  or  $\hat{\mathbf{Z}}_2$ , depending on whether or not  $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/K)$ . If  $\sigma_{-1} \notin \mathcal{G}(\mathbf{Q}_2^c/K)$ , then it follows that the inertia group of  $\mathbf{Q}_2(\zeta)/K$  is always cyclic. Suppose  $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/K)$ . Then  $\mathcal{G}(\mathbf{Q}_2^c/K_{nr}) = \hat{\mathbf{Z}}_2 \times \mathbf{Z}/2$  where the first factor is topologically generated by  $\sigma_5^{2^k}$  for some  $k \geq 0$  and  $\mathbf{Z}/2$  is generated by  $\sigma_{-1}$ . If we choose  $\zeta$  to have order divisible by a power of 2 large enough so that  $\sigma_5^{2^k}(\zeta) \neq \zeta$ , then it is clear that the inertia subgroup of  $\mathbf{Q}_2(\zeta)/K$  is not cyclic. Thus the inertia group of  $\mathbf{Q}_2(\zeta)/K$  is non-cyclic iff  $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/K)$ , and so Yamada's criterion is equivalent to mine.

2. U. Fontaine, [F], Cor. 2', p. 138. The result is:  $S(K)$  is non-trivial iff  $\varepsilon_4 \notin K$ . This is easily seen to be inequivalent to the other formulations. As an example, let  $K$  be the subfield of  $\mathbf{Q}_2(\varepsilon_{16})$  fixed by the automorphism  $\sigma_{-1}\sigma_5^2$ . Then  $\varepsilon_4 \notin K$  and  $\sigma_{-1} \notin \mathcal{G}(\mathbf{Q}_2^c/K)$ .

3. G. J. Janusz, [J], p. 543. Let  $h$  be the smallest integer  $\geq 2$  such that there is an odd integer  $c \geq 1$  with the property that  $\mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_c)$  contains  $K$ . Then Janusz' theorem is the following:

$S(K)$  is non-trivial iff there is an odd integer  $n$  with the following properties:

- (i)  $K(\varepsilon_4)/K$  is ramified.
- (ii)  $K(\varepsilon_{4n}) = \mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_n)$ .
- (iii)  $(K(\varepsilon_n):K) = 2^r w$ , where  $w$  is odd and  $r \geq 1$ .
- (iv) The automorphism of order 2 in  $\mathcal{G}(K(\varepsilon_{4n})/K(\varepsilon_n))$  carries  $\varepsilon_{2^h}$  to  $\varepsilon_{2^h}^{-1}$ .
- (v) If  $r \leq h-1$ , then any root of unity in  $K(\varepsilon_{4n})$  whose order divides  $2^{h-r+1}$  already lies in  $K(\varepsilon_4)$ .

It can be shown that the conditions (iii) and (v) can be omitted. Indeed suppose that we are given an odd integer  $n$  such that (i), (ii), and (iv) are

satisfied. Let the residue class field of  $K(\varepsilon_n)$  have  $2^k$  elements. Set  $n' = (2^k)^{2^h} - 1$ . Then  $n \mid n'$ ,  $n'$  is odd, and  $K(\varepsilon_{n'})/K(\varepsilon_n)$  is unramified of degree  $2^h$ . Consider the conditions (i)-(v) with  $n'$  instead of  $n$ . Then (i) is unchanged, (ii) holds because  $n \mid n'$ , (iii) holds trivially and (v) holds vacuously because  $2^h \mid (K(\varepsilon_{n'}) : K)$ . Finally  $K(\varepsilon_{n'}) \cap K(\varepsilon_4) = K$  since one is ramified and the other is not, so the non-trivial automorphism of  $K(\varepsilon_{4n})/K(\varepsilon_n)$  is the restriction of that of  $K(\varepsilon_{4n'})/K(\varepsilon_{n'})$ , so (iv) holds also for  $n'$ .

We can deduce from this abbreviated form of Janusz' theorem that it is equivalent to Yamada's. Suppose that Janusz' conditions are satisfied, and consider the extension  $\mathbf{Q}_2(\varepsilon_{2^{h+1}}, \varepsilon_n)/K$ . The inertia subgroup of its Galois group is  $\mathcal{g} = \mathcal{G}(\mathbf{Q}_2(\varepsilon_{2^{h+1}}, \varepsilon_n)/K(\varepsilon_n))$ , a group of order 4. Suppose that  $\rho$  is an extension of the non-trivial automorphism of  $\mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_n)/K(\varepsilon_n)$  to  $\mathbf{Q}_2(\varepsilon_{2^{h+1}}, \varepsilon_n)$ , so  $\rho \in \mathcal{g}$ . By condition (iv), there is an integer  $a \equiv -1 \pmod{2^h}$  such that  $\rho(\varepsilon_{2^{h+1}}) = \varepsilon_{2^{h+1}}^a$ . It follows that  $\rho^2$  is the identity. Thus  $\mathcal{g}$  is non-cyclic. Conversely suppose that there is an extension  $\mathbf{Q}_2(\zeta)/K$  whose inertia subgroup  $\mathcal{g}$  is non-cyclic. As we saw in 1., this means that  $\sigma_{-1}$  is in the Galois group of  $\mathbf{Q}_2^c/K$  and so its restriction (which we also call  $\sigma_{-1}$ ) is in  $\mathcal{G}(\mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_c)/K)$  and is non-trivial. Its fixed field contains  $K(\varepsilon_c)$ ; by Lemma 3.3 of [J],  $K(\varepsilon_c, \varepsilon_4) = \mathbf{Q}_2(\varepsilon_{2^h}, \varepsilon_c)$  and so the fixed field is *exactly*  $K(\varepsilon_c)$ . Thus both (iv) and (ii) are also fulfilled. (i) holds by Lemma 1.

4. F. Lorenz, [L], p. 463. His condition for *non-triviality of  $S(K)$*  is that  $-1$  is a norm in the extension  $K/\mathbf{Q}_2$ . The norm residue symbol in the extension  $\mathbf{Q}_2^c/\mathbf{Q}_2$  sends  $-1$  to  $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/\mathbf{Q}_2)$ . Thus it follows from [S], pp. 204-205, that  $-1$  is a norm in  $K/\mathbf{Q}_2$  iff  $\sigma_{-1} \in \mathcal{G}(\mathbf{Q}_2^c/K)$ .

## REFERENCES

- [C-F] CASSELS, J. W. S. and A. FROHLICH. *Algebraic Number Theory*. Thompson Book Co. Inc., Washington (1967).
- [F] FONTAINE, J.-M. Sur la décomposition des algèbres de groupes. *Ann. Sc. Ec. Norm. Sup.* 49 (1971), 121-180.
- [H] HASSE, H. *Zahlentheorie*, 2<sup>nd</sup> ed. Akademie-Verlag, Berlin, 1963.
- [I] ISAACS, I. M. *Character Theory of Finite Groups*. Academic Press, New York (1976).

- [J] JANUSZ, G. J. Generators for the Schur group of local and global number fields. *Pac. J. Math.* 56 (1975), 525-546.
- [L] LORENZ, F. Zur Schurgruppe eines lokalen Körpers. *Arch. Math.* 32 (1979), 458-468.
- [M] MOLLIN, R. The Schur group of a field of characteristic zero. *Pac. J. Math.* 76 (1978), 471-478.
- [N] NEUKIRCH, J. Über das Einbettungsproblem der algebraischen Zahlentheorie. *Inv. Math.* 21 (1973), 59-116.
- [S] SERRE, J.-P. *Corps Locaux*. Act. Sci. et Ind. 1296, Hermann, Paris (1962).
- [W] WEISS, E. *Cohomology of Finite Groups*. Pure and Appl. Math. 34, Academic Press, New York (1969).
- [Y] YAMADA, T. *The Schur Subgroup of the Brauer Group*. Lecture Notes in Math. 397, Springer-Verlag, Berlin (1974).
- [Z] ZASSENHAUS, H. J. *The Theory of Groups*. 2<sup>nd</sup> ed. Chelsea, New York, 1949.

(Reçu le 12 décembre 1986)

C. Riehm

Dept. of Mathematics and Statistics  
McMaster University  
Hamilton, Ontario  
Canada L8S 4K1



**vide-leer-empty**