Math. Ann. 283, 479–489 (1989)

Mathematische Annalen

The Quadratic Schur Subgroup Over Local and Global Fields

C. Riehm*

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

Let K be a field of characteristic 0 and let A be a central simple K-algebra with an involution I. The restriction ω of I to K is an involution of K, and we call I an ω-involution. If ω is the identity, I is said to be an involution of the first kind, otherwise an involution of the second kind.

Suppose now that the dimension of A is n^2. If I is of the first kind, the dimension of the subspace of elements fixed by I is one of $\frac{1}{2}n(n\pm 1)$ – see [Sch, 7.5, Chap. 8]. In this case we define the *type* of I to be $+1$ if the $+$sign prevails, otherwise -1. An involution of type 1 is sometimes called an *orthogonal* involution, and one of type -1 a *symplectic* involution. The *quadratic Brauer class* $[A, I]$ is then defined to be ($[A]$, type I) where $[A]\in \mathrm{Br}(K)$ is the Brauer class of A. If (B, J) is another central simple algebra B with involution J of the first kind, then $I\otimes J$ is an involution of the first kind on the central simple algebra $A\otimes B$, and it is easy to check that type $I\otimes J$ = (type I) (type J). It follows that the set of quadratic Brauer classes is a multiplicatively closed subset of $B(K)\times\{\pm 1\}$, and therefore also a subgroup since $B(K)$ is a torsion group; we call it the *quadratic Brauer group* $B(K, \mathrm{id})$. It follows from a theorem of A.A. Albert that

$$B(K,\mathrm{id}) = {}_2B(K)\times\{\pm 1\}\,,$$

where ${}_2B(K)$ denotes the subgroup of $B(K)$ of exponent 2 – see Sect. 1.

Suppose now that $\omega \neq \mathrm{id}$. In this case one defines $[A, I]$ to be simply the Brauer class $[A]$, and the quadratic Brauer group $B(K, \omega)$ is the set of Brauer classes that arise in this way – it is again a group. It is sometimes convenient in this case to say that I is of type 0, and formally write $[A, I] = ([A], 0)$ instead; one also sometimes refers to such an I as a *unitary* involution. Let K_0 be the subfield of K fixed by ω. Another theorem of Albert says that

$$B(K,\omega) = \ker \mathrm{cor}_{K/K_0}\,,$$

where cor_{K/K_0}: $B(K)\to B(K_0)$ is the corestriction map (Theorem 8).

The quadratic Brauer group is defined more generally for a commutative ring K in [HTW]. This definition is related to the one used here in Sect. 1.

* Support by N.S.E.R.C. grant #A8778 gratefully acknowledged

Recall that the Schur subgroup $S(K)$ of $B(K)$ consists of the Brauer classes which are represented by a central simple direct summand of the group algebra KG for some finite group G. The quadratic Schur subgroup $S(K,\omega)$ is defined in an analogous manner: an element c in $B(K,\omega)$ is in $S(K,\omega)$ if and only if there is a finite group G and a central simple direct summand A of KG with the following property: A is stable under the canonical ω-involution Ω of KG (which inverts the elements of G and is ω-linear) and $[A,I]=c$ where I is the restriction of Ω to A.

Our principal goal is the determination of $S(K,\omega)$ in the case of K a local or global field.

Let K_c be the largest subcyclotomic extension of $\mathbb{Q}$ contained in K, and let $\tilde{K}$ be the subfield of K_c fixed by the composition of ω and complex conjugation ($\tilde{K}$ is the maximal real subfield of K_c in the case $\omega=\mathrm{id}$). If L/k is any extension of fields, denote by $L\otimes S(k)$ the subgroup of $B(L)$ of classes obtained from those in $S(k)$ by extension of scalars; it is easy to see that $L\otimes S(k)\subseteqq S(L)$.

Lemma 1. *If K is any field of characteristic 0, the image of the forgetful map $S(K,\omega)\to S(K)$ is $K\otimes S(\tilde{K})$, and $S(K,\omega)=K\otimes S(\tilde{K},\omega)$.*

Theorem 2. *Let K be an algebraic number field.*

(i) *If $\omega\neq\mathrm{id}$, $S(K,\omega)=K\otimes S(\tilde{K})$.*

(ii) *If $\omega=\mathrm{id}$ and K is totally imaginary, then*

$$S(K,\mathrm{id})=(K\otimes S(\tilde{K}))\times\{\pm 1\}.$$

(iii) *If $\omega=\mathrm{id}$ and K is not totally imaginary, then $S(K,\mathrm{id})$ consists of the quadratic Brauer classes*

$$(\beta,\varepsilon)\in(K\otimes S(\tilde{K}))\times\{\pm 1\} \tag{1}$$

with $\varepsilon=1$ resp. -1 iff β is split resp. non-split at all real primes.

Remarks. 1. Obviously $K\otimes S(\tilde{K})$ depends on a knowledge of $S(\tilde{K})$, and on the local degrees in $K/\tilde{K}$. In Chap. 7 of Yamada's book [Y], $S(\tilde{K})$ is determined in many cases.

2. We note that (i) actually holds for K an arbitrary field of characteristic 0.

3. (iii) can be given more generally: if $\omega=\mathrm{id}$ and K is any formally real field, then $S(K,\mathrm{id})$ consists of the classes (1) with $\varepsilon=1$ iff β splits in all real closures of K (see Theorem 9). This theorem also contains a simple variant of the Benard-Schacher theorem on the "uniform distribution of invariants" [Y, Theorem 6.1] for formally real fields.

Theorem 3. *Let K be a local field, i.e. a finite extension of $\mathbb{Q}_p$.*

(i) *If $\omega\neq\mathrm{id}$, $S(K,\omega)=1$.*

(ii) *$S(K,\mathrm{id})={}_2S(K)\times\{\pm 1\}$ if K is an odd degree extension of an abelian extension of $\mathbb{Q}_p$, otherwise $S(K,\mathrm{id})=\{\pm 1\}$.*

The proofs are given in Sects. 2 and 3.

1. The Quadratic Brauer Group

We first recall the definition of $B(K,\omega)$ as formulated in [HTW] and, in the case of a field K of characteristic 0, indicate its relationship to the definition given in the introduction.

An *anti-structure* over a commutative ring K is a triple $\mathbf{A}=(A,I,\lambda)$ where A is an algebra (associative with 1) over K, I is an antiautomorphism of A, and λ is a unit of A satisfying $\lambda\lambda^I=1$ and

$$a^{I^2}=\lambda a\lambda^{-1} \quad \text{for all } a\in A .$$

$\mathbf{A}$ is called an ω-antistructure if the restriction of I to K is ω.

We recall that a Morita equivalence between two rings A and B is a quadruple consisting of two bimodules $M={}_BM_A$ and $N={}_AN_B$, and two bimodule isomorphisms $M\otimes_A N\to B$ and $N\otimes_B M\to A$ whose associated pairings $M\times N\to B$ and $N\times M\to A$ (both denoted by $\langle\ ,\ \rangle$), satisfy

$$\langle m,n\rangle m'=m\langle n,m'\rangle \quad \text{and} \quad \langle n,m\rangle n'=n\langle m,n'\rangle$$

for all m,m' in M and n,n' in N. A particular Morita equivalence, called a *derived* Morita equivalence, is obtained as follows: let M be a progenerator for A (i.e. a finitely generated projective module such that A is a direct summand of some direct product $M\times M\times\ldots\times M$), set $N=\mathrm{Hom}_A(M,A)$ and $B=\mathrm{End}_AM$; then the bimodule isomorphisms are given by the canonical maps

$$M\otimes_A\mathrm{Hom}_A(M,A)\to\mathrm{End}_AM, \quad \text{and} \quad \mathrm{Hom}_A(M,A)\otimes_BM\to A .$$

Suppose now that $\mathbf{A}=(A,I,\lambda)$ and $\mathbf{B}=(B,J,\mu)$ are antistructures and that we have a Morita equivalence between the rings A and B, effected by the modules M and N. Make N into a $B-A$ bimodule by twisting by I and J: $bna:=a^Inb^J$. Suppose that $h:M\to N$ is a bimodule isomorphism satisfying

$$\langle h(m\lambda),m'\rangle^I=\langle h(m'),\mu m\rangle \tag{2}$$

for all m,m' in M. Then we say that the two antistructures are *quadratic Morita equivalent* (cf. [HTW, FM, H]). The quadratic Brauer group as defined in [HTW] is the set of quadratic Morita classes of ω-antistructures on Azumaya algebras, and is a group under tensor product. We shall denote it by $B(K,\omega)'$ in order to distinguish it from the group $B(K,\omega)$ defined in the introduction. We note that there is also a forgetful homomorphism of $B(K,\omega)'$ into $B(K)$ given by $[A,I,\lambda]\mapsto[A]$.

There is also a notion of *derived* quadratic Morita equivalence: Suppose that we have a Morita equivalence between the rings A and B, effected by M and N, and let $\mathbf{A}=(A,I,\lambda)$ be an antistructure. Make N into a right A-module via I, and suppose that $h:M\to N$ is an isomorphism of A-modules. Then

(i) *there is a unique antiautomorphism J on B such that h is also a B-isomorphism when N is made into a left B-module via J,*
and

(ii) *there is a unique unit μ in B such that (B,J,μ) is an antistructure and such that h effects a quadratic Morita equivalence between it and* $\mathbf{A}$.

The *scaling* ${}^u\mathbf{A}$ of an antistructure $\mathbf{A}$ by a unit u of A is the antistructure (A,I',λ') where

$$a^{I'}=u^{-1}a^Iu \quad \text{and} \quad \lambda'=u^{-1}u^I\lambda .$$

Lemma 4. *Let* **A** *be an antistructure, let $M = A$ as right A-module, and identify both $B = \mathrm{End}_A M$ and $N = \mathrm{Hom}_A(M, A)$ with A via left multiplication. Let $h: M \to N$ be any isomorphism where N is a right A-module via I. Then h is of the form $h(m) = um$ for some unit u in A, and the derived antistructure is* ${}^u\mathbf{A}$.

This is an easy calculation. We note that it follows from this that scaling an antistructure does not change the quadratic Morita equivalence class – one need only define the map h as above using the scaling unit u.

We assume from now on that K is a field of characteristic 0.

Theorem 5. *Two antistructures on the same simple algebra are quadratic Morita equivalent if and only if they are mutual scalings.*

Proof. Let **A** and **B** be the antistructures. As mentioned above, the sufficiency follows from the lemma. So assume that they are quadratic Morita equivalent, say via the bimodules M and N and the isomorphism $h: M \to N$. Since **A** and **B** have the same underlying ring A, $A \cong \mathrm{End}_A M$ and so $M \cong A$; we shall therefore identify M with A. Thus we can also identify N with A, acting via left multiplication. Then

$$h(a) = h(1)a^J = a^I h(1)$$

and so $a^J = u^{-1} a^I u$ with $u = h(1)$ (which is a unit since h is an isomorphism). Similarly (2) with $m = m' = 1$ is $h(\lambda)^I = h(1)\mu$, which implies that $\mu = u^{-1} u^I \lambda$. □

Theorem 6. *There is an isomorphism $\pi: B(K, \omega) \to B(K, \omega)'$ which takes $[A, I] \mapsto [A, I, 1]$.*

Proof. Let $[A, I] \in B(K, \omega)$. If k is a positive integer, there is a canonical "extension" $\tilde{I}$ of I to the $k \times k$ matrices $\tilde{A} = A(k \times k)$, given by "conjugate transpose", $(a_{ij})^{\tilde{I}} = {}^t(a_{ij}^I)$. It is easy to check that $\tilde{I}$ has the same type as I, so $[\tilde{A}, \tilde{I}] = [A, I]$. Now suppose that $[B, J] = [A, I]$. Since $[A] = [B]$, we can choose k and another integer ℓ so that $\tilde{A} \cong \tilde{B} = B(\ell \times \ell)$; we shall assume that $\tilde{A}$ and $\tilde{B}$ are equal. By the Skolem-Noether theorem, there is a unit u of $\tilde{A}$ such that $\tilde{J} = (\mathrm{inn}\, u) \circ \tilde{I}$ where $\mathrm{inn}\, u$ is the inner automorphism $a \mapsto u^{-1} a u$. Then (see [Sch, Sect. 7, Chap. 8]) $u^{\tilde{I}} = u$ if $\tilde{I}$ is of the first kind (since then $\tilde{J}$ is also of the first kind and has the same type as $\tilde{I}$), and this can also be assumed if $\tilde{I}$ is of the second kind. Thus $(\tilde{B}, \tilde{J}, 1)$ is the scaling ${}^u(\tilde{A}, \tilde{I}, 1)$ and so $[\tilde{B}, \tilde{J}, 1] = [\tilde{A}, \tilde{I}, 1]$ by Lemma 4. The fact that π is well-defined now follows from:

Lemma 7. $[\tilde{A}, \tilde{I}, \tilde{\lambda}] = [A, I, \lambda]$ *for any antiautomorphism I, where $\tilde{\lambda} = \lambda E_k$ (E_k the identity matrix of degree k).*

Proof. Take $M = A(k \times 1)$. In the corresponding derived Morita equivalence, we may take $B = \tilde{A}$ operating by left multiplication on M, and $N = A(1 \times k)$ operating on M by both left and right multiplication. We let $h: M_A \to N_A$ be the map $h(m_i) = {}^t(m_i^I)$. It is straightforward to check that the resulting derived Morita equivalence yields the desired result. □

We now return to the proof of Theorem 6. It is clear that π is a homomorphism.

If $\omega \neq \mathrm{id}$, it is injective since

$$\begin{tikzcd} B(K,\omega) \arrow[rr, "\pi"] \arrow[dr, "?"'] & & B(K,\omega)' \arrow[dl, "?"] \\ & B(K) & \end{tikzcd}$$

is commutative and the forgetful map on $B(K,\omega)$ is simply the identity map. If $\omega = \mathrm{id}$, the kernel of π is certainly contained in the subgroup $([K], \pm 1)$ of order 2. Suppose $[M(m,K), I, 1] = [M(n,K), J, 1]$; By Lemma 7 we can assume that $m=n$, and so $(M(n,K), J, 1) = {}^{u}(M(n,K), I, 1)$ for some unit $u \in M(n,K)$ by Theorem 5. Then $u^{-1}u^{I}1 = 1$ so $u^{I} = u$. It is easy to see that a is fixed by I iff $u^{-1}a$ is fixed by $J = (\mathrm{inn}\, u) \circ I$. Thus type $I =$ type J, which implies that π is injective.

To show that π is surjective, suppose that $[A, I, \lambda] \in B(K,\omega)'$. Since $\lambda\lambda^{I} = 1$, A supports an ω-involution J by [Sch, 8.2, Chap. 8], and so by Theorem 5 and the Skolem-Noether theorem, we may assume that I itself is an involution. Then $\lambda \in K^{*}$. If $\omega \neq \mathrm{id}$, another scaling (using Hilbert's Theorem 90) shows that we can take $\lambda = 1$, so $[A, I, \lambda] = \pi[A, I]$. Suppose $\omega = \mathrm{id}$. Then $\lambda = \pm 1$; we are finished if $\lambda = 1$ so suppose $\lambda = -1$. By Wedderburn's theorem we can assume $A = M(n, D)$ for some division algebra D. One can show, using the results in ibid, that there is an ω-involution J on D and that I differs by an inner automorphism from $(d_{ij}) \mapsto {}^{t}(d_{ij}^{J})$. Thus there is a unit u in A such that $u^{I} = -u$, and scaling by it yields $[A, I, -1] = [A, (\mathrm{inn}\, u) \circ I, 1]$ which is obviously in the image of π. $\square$

Theorem 8.

$$B(K,\omega) = \begin{cases} {}_{2}B(K) \oplus \{\pm 1\} & \text{if} \quad \omega = \mathrm{id}, \\ \ker \mathrm{cor}_{K/K_0} & \text{if} \quad \omega \neq \mathrm{id}. \end{cases}$$

Proof. By a theorem of Albert, [Sch, 8.4, Chap. 8], a central simple algebra has a K-involution iff its Brauer class has order 1 or 2. The expression for $B(K, \mathrm{id})$ follows from this and the fact that $M(2,K)$, for example, has involutions of both types, namely transpose, and transpose followed by the inner automorphism with respect to $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Similarly the expression when $\omega \neq \mathrm{id}$ is another theorem of Albert – see 9.5, ibid.

2. The Schur Subgroup Over a Number Field

We begin by proving Lemma 1.

Suppose that $[A, I] \in S(K,\omega)$, say that A is the direct summand of the group algebra KG with I induced on A by the canonical ω-involution Ω of KG. There is a unique absolutely irreducible character χ of G which corresponds to A. The center of A is $K = K(\chi)$, so the values of χ lie in K. Since $\mathbb{Q}(\chi)$ is a cyclotomic extension of $\mathbb{Q}$, this means that the values of χ lie in K_c. Now consider the formula for the idempotent

$$e_{\chi} = \frac{n}{g} \sum_{s \in G} \chi(s^{-1})s,$$

where $n=\chi(1)$ and g is the order of G. Now Ω permutes the primitive central idempotents of KG, and since A is stable under it, it fixes e_χ. Therefore

$$e_\chi = \frac{n}{g} \sum_{s\in G} \chi(s^{-1})^\omega s^{-1} = \frac{n}{g} \sum_{s\in G} \chi(s^{-1})^{*\omega} s,$$

where * is complex conjugation. On comparing the expressions for e_χ, we see that the values of χ are fixed by $*\omega$, and so $\tilde{K}(\chi)=\tilde{K}$. This means that the direct summand $\tilde{A}$ of $\tilde{K}G$ which belongs to χ has center $\tilde{K}$, and so since $K\otimes\tilde{K}G=KG$, it follows at once that $K\otimes\tilde{A}=A$ since $K\otimes\tilde{A}$ is simple. Therefore im $S(K,\omega) \subseteqq K\otimes S(\tilde{K})$.

We now show the reverse inclusion. Let $\tilde{\Omega}$ be the canonical ω-involution of the group algebra $\tilde{K}G$. Because $*\omega=\mathrm{id}$ on $\tilde{K}$, ω acts on $\tilde{K}$ via complex conjugation. This implies that $\tilde{\Omega}$ leaves invariant all simple factors of $\tilde{K}G$. (Indeed the proof is almost identical to Theorem 13.3, Chap. 8, [Sch]: If T is the algebra trace of $\tilde{K}G$, then it is easy to see that $T(xy^{\tilde{\Omega}})$ is a positive definite hermitian form on $\tilde{K}G$ (with G as an orthogonal basis). Thus $T(xx^{\tilde{\Omega}})>0$, which implies that every simple factor is $\tilde{\Omega}$-invariant.) Thus if $\tilde{A}$ is a central simple factor of $\tilde{K}G$, it is clear that $K\otimes\tilde{A}$ is a central simple factor of KG and is invariant under the canonical ω-involution of KG, and so Lemma 1 is proved. □

Theorem 9. *Let K be a formally real field. If $\beta\in S(K)$ is split in at least one real closure of K, then it is split in all real closures of K. $S(K,\mathrm{id})$ consists of all*

$$(\beta,\varepsilon)\in S(K)\times\{\pm1\}$$

with $\varepsilon=1$ iff β is split at all real closures.

Proof. As in the previous proof, any simple component of a group algebra KG is stable under the canonical K-involution (of KG). Suppose for the moment that K is real closed. It is easy to check that Frobenius' theorem on simple algebras over $\mathbb{R}$ [Sch, Theorem 6.4, Chap. 8] and the Frobenius-Schur theory of representations over $\mathbb{R}$ [S, 13.2] hold more generally for real closed fields. Therefore if $(\beta,\varepsilon)\in S(K,\mathrm{id})$, ε must be 1 if β is split and must be -1 if β is non-split (in which case β is the class of the unique non-commutative central division algebra over K, the quaternion algebra $(-1,-1)$). Now suppose again that K is merely formally real, and that $(\beta,\varepsilon)\in S(K,\mathrm{id})$. If $\hat{K}$ is a real closure of K, then $(\hat{K}\otimes\beta,\varepsilon)\in S(\hat{K},\mathrm{id})$ and so ε is 1 if β splits in $\hat{K}$ and is -1 otherwise. Since this holds for any real closure, the first statement of the theorem follows, and the second is a consequence of this and Lemma 1 and the fact that $K\otimes S(\tilde{K})=S(K)$. □

Lemma 10. *Let k be a finite extension of $\mathbb{Q}$, and let K/k be a finite extension of even degree. Then there exists a finite prime $\mathfrak{p}$ of k and a prime $\mathfrak{P}$ of K lying over $\mathfrak{p}$ with the property that the local extension $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ also has even degree.*

Proof. Let L be the normal closure of K/k, let $\mathscr{G}$ be the Galois group of L/k and $\mathscr{H}$ that of L/K. Choose $\tau\in\mathscr{G}-\mathscr{H}$ such that $\tau^2\in\mathscr{H}$, for example by considering a 2-Sylow subgroup of $\mathscr{H}$ contained in a 2-Sylow subgroup of $\mathscr{G}$. By the Tchebotarev density theorem [CF, p. 227], there is a prime $\mathfrak{P}'$ of L which is unramified over k and whose Frobenius automorphism is τ. Let $\mathfrak{P}$ and $\mathfrak{p}$ be resp. the primes of K and k lying below $\mathfrak{P}'$. Then the decomposition group of $\mathfrak{P}'/\mathfrak{p}$ is

$$\mathscr{Z}(\mathfrak{P}'/\mathfrak{p})=\langle\tau\rangle=\mathrm{Gal}(L_{\mathfrak{P}'}/k_{\mathfrak{p}}).$$

Now $\tau \notin \mathrm{Gal}(L_{\mathfrak{P}'}/K_{\mathfrak{P}})$ since the latter group is a subgroup of $\mathscr{H}$ but

$$\tau^2 \in \mathscr{G}(L/K) \cap \mathscr{Z}(\mathfrak{P}'/\mathfrak{p}) = \mathscr{Z}(\mathfrak{P}'/\mathfrak{P}) = \mathrm{Gal}(L_{\mathfrak{P}'}/K_{\mathfrak{P}}).$$

It follows at once that $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ has even degree. □

We can now prove Theorem 2. Parts (i) and (iii) follow from Lemma 1 and Theorem 9 respectively. Therefore we assume that K is totally imaginary and that $\omega = \mathrm{id}$. We must show that ([K], -1) is in $S(K, \mathrm{id})$.

Since $K/\mathbb{Q}$ has even degree, there is a finite prime $\mathfrak{P}$ in K such that $K_{\mathfrak{P}}/\mathbb{Q}_p$ also has even degree by Lemma 10. Let Q be the quaternion algebra over $\mathbb{Q}$ with non-trivial Hasse invariants at p and ∞, and invariant 0 at the other primes. By a theorem of M. Benard and K.L. Fields [Y, Theorem 7.2], $S(\mathbb{Q})$ consists of the quaternion algebras and so $[Q] \in S(\mathbb{Q})$. Since $\mathbb{Q}$ is formally real, every simple component of a rational group algebra $\mathbb{Q}G$ is invariant under the canonical involution, so $([Q], \varepsilon) \in S(\mathbb{Q}, \mathrm{id})$ for a suitable choice of $\varepsilon = \pm 1$. By Theorem 9, $\varepsilon = -1$ since $\mathbb{R} \otimes Q$ is non-split. Thus $([K \otimes Q], -1) \in S(K, \mathrm{id})$. But $K \otimes Q$ is split at $\mathfrak{P}$, and hence at all other primes lying over p by the "uniform distribution theorem" of Benard and Schacher [Y, Theorem 6.1]. Since K is totally imaginary, this means that $K \otimes Q$ is split, so $([K], -1) \in S(K, \mathrm{id})$ as desired. □

3. The Schur Subgroup Over a $\mathfrak{p}$-Adic Field

We now assume that K is a finite extension of $\mathbb{Q}_p$ for some p, and we shall prove Theorem 3 in several stages.

Case 1: $\omega \neq \mathrm{id}$. For *any* finite extension K/K_0 of local fields, the corestriction map cor_{K/K_0} is injective [CL, Proposition 1, Chap. XI, and Theorem 1, Chap. XIII], and so $S(K, \omega) = B(K, \omega) = 1$ by Theorem 8.

From now on we assume that $\omega = \mathrm{id}$. We first show that the kernel of the forgetful map on $S(K, \mathrm{id})$ is ± 1. Let Q be a rational quaternion algebra which is split at p but not split at ∞. Then because $S(\mathbb{Q}) = {}_2B(\mathbb{Q})$ and every direct summand of a rational group algebra $\mathbb{Q}G$ is stable under the canonical $\mathbb{Q}$-involution, $([Q], \varepsilon) \in S(\mathbb{Q}, \mathrm{id})$ for some choice of $\varepsilon = \pm 1$. By the usual argument of extending to $\mathbb{R}$, we see that $\varepsilon = -1$. Now extend to K to show that $([K], -1) \in S(K, \mathrm{id})$, as desired.

We can assume for the rest of the proof that ${}_2S(K) = \pm 1$ since ${}_2S(K)$ is either trivial or ± 1 (recall that $B(K) = \mathbb{Q}/\mathbb{Z}$ – cf. [CL, Proposition 6, Chap. XIII]). We shall have to construct "quadratic Schur algebras", that is central simple algebras which are direct summands of group algebras (over K) and which are stable under the canonical K-involution of the group algebra – or what is the same, which are the images of KG under an irreducible K-representation of the finite group G and which admit an involution of the first kind which inverts the images of the elements of G. This is done by the use of a crossed-product algebra $A = (K(\zeta)/K, z)$ (see [MO, Sect. 29]) using a cocycle $z \in Z^2(\mathrm{Gal}(K(\zeta)/K), \mu(K(\zeta))$, where ζ is a suitable root of unity and $\mu(K(\zeta))$ is the group of roots of unity of $K(\zeta)$. Thus A has a distinguished basis $\{u_\sigma : \sigma \in \mathrm{Gal}(K(\zeta)/K)\}$ over $K(\zeta)$ with multiplication defined by

$$(a_\sigma u_\sigma)(b_\tau u_\tau) = a_\sigma b_\tau^\sigma z(\sigma, \tau) u_{\sigma\tau}$$

for any a_σ and b_τ in $K(\zeta)$.

Lemma 11. *Suppose that the values of z are actually ± 1 and that there is $\iota \in \mathrm{Gal}(K(\zeta)/K)$ such that $\zeta^\iota = \zeta^{-1}$. Then $A = (K(\zeta)/K, z)$ is a quadratic Schur algebra.*

Proof. We can assume that z is normalized, i.e. $z(\sigma,\tau)=1$ if either σ or τ is the identity. A is easily seen to be a "Schur algebra" for the group $G = \bigcup_\sigma \langle \pm\zeta\rangle u_\sigma$ since G spans A over K (the representation space is of course any simple A-module). We must show that there is a K-involution on A which inverts the elements of G. Consider the K-linear map I on A which, for each σ, takes $a_\sigma u_\sigma$ to $a_\sigma^{\iota\sigma^{-1}} u_\sigma^{-1}$ ($a_\sigma \in K(\zeta)$). A straightforward calculation shows that I has the desired properties. □

Lemma 12. *If p_1 is an odd prime such that $K(\zeta_{p_1})/K$ is a Galois extension of even degree, then there is an automorphism ι of $K(\zeta_{p_1})/K$ which inverts ζ_{p_1}.*

Proof. Note that $\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}$ has even degree and is cyclic, so the unique element of order 2 in its Galois group is complex conjugation, which inverts ζ_{p_1}. The restriction of the Galois group of $K(\zeta_{p_1})/K$ to $\mathbb{Q}(\zeta_{p_1})$ is injective and so the image contains complex conjugation, whence the lemma. □

A standard technique for constructing crossed-product algebras is to use a *cyclic* extension $K(\zeta)/K$; in this case one can assume that the algebra has the form

$$A = \sum K(\zeta) u_\sigma^i, \quad 0 \leqq i < (K(\zeta):K) = n,$$

where $u_\sigma^n = a \in K^*$; in particular the u_σ^i form a distinguished basis. A is often denoted by $(K(\zeta)/K, \sigma, a)$ or simply $(K(\zeta)/K, a)$. Furthermore A is split iff a is a norm in the extension $K(\zeta)/K$. See [MO, 30.4], for example. Less well known is the fact that there is a similar construction, due to Yamada, for any finite cyclotomic extension – see [Y, Chap. 2]. We shall use his construction in the bicyclic case only:

Yamada's Lemma. *Suppose that ζ is a root of unity and that $K(\zeta)/K$ has Galois group the direct product of two cyclic groups $\langle\varrho\rangle$ and $\langle\sigma\rangle$ of finite orders r and s resp. Let a, b, and c be roots of unity in $K(\zeta)$ satisfying*

$$a^{\varrho-1} = b^{\sigma-1} = 1, \quad a^{\sigma-1} = N_\varrho c, \quad b^{\varrho-1} = N_\sigma c^{-1},$$

where, for example, $N_\varrho c = c^{1+\varrho+\varrho^2+\dots+\varrho^{r-1}}$. Then there is a crossed-product algebra ("bicyclic algebra") $A = (K(\zeta)/K, a, b, c)$ which has a distinguished basis $u_\varrho^i u_\sigma^j$, $0 \leqq i < r$, $0 \leqq j < s$, with the property that

$$u_\varrho^r = a, \quad u_\sigma^s = b, \quad u_\sigma u_\varrho = c u_\varrho u_\sigma.$$

If λ and μ are roots of unity in $K(\zeta)^*$, and if $v_\varrho := \lambda u_\varrho$ and $v_\sigma := \mu u_\sigma$, then the elements $v_\varrho^i v_\sigma^j$ form a distinguished basis for the bicyclic algebra $A = (K(\zeta)/K, a', b', c')$ where

$$a' = (N_\varrho \lambda) a, \quad b' = (N_\sigma \mu) b, \quad c' = \lambda^{\sigma-1}(\mu^{\varrho-1})^{-1} c. \quad \square$$

We now return to the proof of Theorem 3.

Case 2: $\omega = \mathrm{id}$, $K/\mathbb{Q}_p$ abelian, p odd, and $\mu(K)_2 = \pm 1$. By a theorem of Janusz, [J], $S(K)$ is generated by the class of a cyclic algebra $(K(\zeta_p)/K, \zeta)$ where ζ generates the group of roots of unity in K with order prime to p. Since the Brauer class of a cyclic algebra $(L/K, a)$ is multiplicative in a, it is easy to see that the class of $(K(\zeta_p)/K, -1)$

is the non-trivial element of ${}_2S(K)$. By the Yamada-Fontaine theorem [Y, 4.4′, 4.5], $S(K)$ is a cyclic group of order $(p-1)/e_0$ where e_0 is the tame ramification index of $K/\mathbb{Q}_p$. Since $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ has tame index $p-1$, $S(K(\zeta_p))$ must be trivial. Thus $K(\zeta_p)/K$ has even degree since the scalar extension map $B(K)\to B(K(\zeta_p))$ is multiplication by $(K(\zeta_p):K)$ when viewed as a map $\mathbb{Q}/\mathbb{Z}\to\mathbb{Q}/\mathbb{Z}$. This case then follows from Lemmas 11 and 12.

Case 3: $\omega=\mathrm{id}$, $K/\mathbb{Q}_p$ abelian, p odd, $|\mu(K)_2|>2$, and $K(\zeta_p)/K$ a ramified quadratic extension. Suppose $\mu(K)_2$ has order 2^h $(h\geqq 2)$. Let ζ be a primitive 2^{h+1}-root of unity; then $K(\zeta)$ is an unramified quadratic extension of K and so is disjoint from $K(\zeta_p)$. Thus $K(\zeta,\zeta_p)=K(\zeta\zeta_p)$ has Galois group over K generated by elements ϱ and σ of order 2 where the fixed field of ϱ is $K(\zeta)$ and that of σ is $K(\zeta_p)$. By Yamada's lemma, there is a bicyclic algebra $A=(K(\zeta\zeta_p)/K,1,1,-1)$. Suppose that the residue class field of K has q elements (so q is a power of p). The gcd of $q+1$ and $q-1$ is 2, so $q+1$ is not a power of 2 since the fact that K contains the fourth roots of unity implies that $q-1$ is divisible by 4. It follows that there is an odd prime p_1 which divides q^2-1 but not $q-1$. It is easy to see then that $K(\zeta)=K(\zeta_{p_1})$ and $K(\zeta,\zeta_p)=K(\zeta_{p_1p})$.

It follows from Lemma 12 that $\varrho\sigma$ inverts ζ_{p_1p} and so A is a quadratic Schur algebra by Lemma 11. The proof for case 3 will be finished by showing that A is non-split.

We define a new distinguished basis of A by taking $v_\varrho:=\zeta u_\varrho$ (with ζ a 2^{h+1}-root of unity as before) and $v_\sigma=u_\sigma$. Since $N_\varrho\zeta=\zeta^2$ and $\zeta^{\sigma-1}=-1$, $A=(K(\zeta_{p_1p})/K,\zeta^2,1,1)$ by Yamada's Lemma. In particular v_ϱ and v_σ commute and one sees easily that

$$A\cong(K(\zeta_p)/K,\zeta^2)\otimes(K(\zeta_{p_1})/K,1).$$

The second factor is of course split, and so this case will follow if we show that ζ^2 is not a norm in $K(\zeta_p)/K$. Suppose that ζ^2 *is* a norm, say $\zeta^2=N\alpha$ with $\alpha\in K(\zeta_p)$. Certainly α must be a unit; we can write $\alpha=\zeta'\beta$ where ζ' is a $(q-1)^{st}$ root of unity and β is a 1-unit, i.e. is $\equiv 1 \bmod \mathfrak{P}$ where $\mathfrak{P}$ is the maximal ideal of the ring of integers of $K(\zeta_p)$. Now $N\beta$ is also a 1-unit, and is also a root of unity since both of $N\alpha$ and $N\zeta'$ are, and so must be a p-power root of unity. Since ζ^2 is a 2-power root of unity, we can therefore assume that $\beta=1$, and that ζ' is also a 2-power root of unity. Since $K(\zeta_p)/K$ is totally ramified, $\mu(K(\zeta_p))_2=\mu(K)_2$ and so ζ' is a power of ζ^2. This is impossible since $N\zeta'=\zeta'^2=\zeta^2$. This finishes the proof of case 3.

Case 4: $\omega=\mathrm{id}$, $K/\mathbb{Q}_p$ abelian, p odd, and $|\mu(K)_2|>2$. Let $K(\zeta_p)_u$ be the maximal unramified subextension of $K(\zeta_p)/K$. Since $S(K)_2\neq 1$, $K(\zeta_p)/K(\zeta_p)_u$ must be tamely ramified of even degree; let L be the unique intermediate field of which $K(\zeta_p)$ is a quadratic extension. We can therefore apply Case 3 (and its proof) to find an odd prime $p_1\neq p$ and a cocycle $z\in Z^2(\mathrm{Gal}(K(\zeta_{p_1p})/L),\pm 1)$ such that the corresponding crossed-product algebra is non-split and such that there is an $\iota\in\mathrm{Gal}(K(\zeta_{p_1p})/L)$ which inverts ζ_{p_1p}. Let $z'\in Z^2(\mathrm{Gal}(K(\zeta_{p_1p})/K,\pm 1)$ be the corestriction of z. As mentioned earlier, cor is injective on the Brauer group over a local field, and so the crossed-product algebra corresponding to z' is non-split. Therefore this case follows from Lemma 11.

Case 5: $\omega=\mathrm{id}$, $K/\mathbb{Q}_p$ abelian, and $p=2$. It is known in this case that the non-trivial Brauer class in $S(K)$ $(={}_2S(K))$ is represented by a bicyclic algebra of the following form (see [R], for example): Let h be the smallest integer $\geqq 2$ with the property that there is an odd integer m such that $L := \mathbb{Q}_2(\zeta_{2^h}, \zeta_m)$ contains K; we can assume that the residue class degree f of L/K is $\equiv 0 \bmod 2^h$. The Galois group $\mathcal{G}$ of L/K is the bicyclic group $\langle\sigma_1\rangle \times \langle\sigma_2\rangle$ where

(i) σ_1 is of order 2, inverts $\zeta = \zeta_{2^h}$, and has fixed field $K(\zeta_m)$.

(ii) σ_2 is of order f and has fixed field $K(\zeta_4)$.

Then the bicyclic algebra is $A := (L/K, 1, 1, \zeta)$.

As was indicated in [R], one can replace m by any odd multiple m' of m. We shall choose m' in such a way that $\mathbb{Q}_2(\zeta_{2^h}, \zeta_{m'}) = \mathbb{Q}_2(\zeta_{2^h}, \zeta_n)$ for some odd positive integer n which is relatively prime to the order of $\mu(K)$. The following lemma is useful in this regard:

Lemma. *If q is a power of 2, $\mathbb{F}_{q^2}$ is generated over $\mathbb{F}_2$ by a primitive $(q+1)^{st}$ root of 1.*

Proof. Let $\mathbb{F}$ be a proper subfield of $\mathbb{F}_{q^2}$, say with q' elements. Then $q^2 = q'^r$ for some $r \geqq 2$, so $q' \leqq q$. Therefore $q'-1$ is not divisible by $q+1$, whence the lemma. □

Now let q be the number of elements in the residue class field of $\mathbb{Q}_2(\zeta_{2^h}, \zeta_m)$; we can assume $m = q+1$. Clearly $q+1$ is relatively prime to $q-1$, hence a fortiori to $|\mu(K)|$ as well. By the lemma we can choose $m' = q^2 - 1$ and $n = q+1$. Suppose that m has been replaced by m'. Let $f' = \frac{1}{2}f$ and $K' =$ the fixed field of $\sigma_2^{f'}$. If p_1 is any prime divisor of $q+1$, $K'(\zeta_{p_1}) = \mathbb{Q}_2(\zeta_{2^h}, \zeta_m)$ since p_1 does not divide $q-1$. Therefore it follows from Lemma 12 that $\sigma_2^{f'}$ inverts a $(q+1)^{st}$ root of unity ζ'; moreover $2^h | f$ implies that $\sigma_2^{f'}\zeta = \zeta$.

We shall now show that A is a quadratic Schur algebra. Let $\{u_1^i u_2^j\}$ be the distinguished basis of A over L. Let $v_1 = u_1^{-1}$ and $v_2 = u_2^{-1}$. Under the multiplication $\cdot$ of the opposite algebra A^0, $v_1 \cdot v_2 \cdot v_1^{-1} \cdot v_2^{-1} = \zeta^{-1}$, $v_1^2 = 1 = v_2^f$, and $v_i \cdot \lambda \cdot v_i^{-1} = \sigma_i(\lambda)$ for $i = 1, 2$. Thus $A^0 = (L/K, 1, 1, \zeta^{-1})$. Let $J: A \to A^0$ be the additive map defined by $J(\lambda u_1^i u_2^j) = \sigma_1 \sigma_2^{f'}(\lambda) \cdot v_1^i \cdot v_2^j$. Then J is an isomorphism of K-algebras, i.e. J is a K-involution, and it inverts the elements of the group $\langle\zeta, \zeta', u_1, u_2\rangle$. This finishes the proof of Case 5.

Case 6. $K/\mathbb{Q}_p$ an arbitrary finite extension.

Lemma. *Let K_1 be the maximal abelian extension of $\mathbb{Q}_p$ contained in K. Then*

$$\operatorname{im}(S(K, \mathrm{id}) \to S(K)) = K \otimes \operatorname{im}(S(K_1, \mathrm{id}) \to S(K_1)).$$

Proof. The product of the restriction maps

$$\mathrm{Gal}(K_c K_1/\mathbb{Q}_p) \to \mathrm{Gal}(K_c/\mathbb{Q}) \times \mathrm{Gal}(K_1/\mathbb{Q}_p)$$

is clearly injective, so the subextension $K_c K_1/\mathbb{Q}_p$ of $K/\mathbb{Q}_p$ is abelian. Therefore $K_c K_1 = K_1$, i.e. $K_c \subseteqq K_1$, and so $K_{1c} = K_c$ and $\tilde{K}_1 = \tilde{K}$. It follows from Lemma 1 that

$$\operatorname{im}(S(K, \mathrm{id}) \to S(K)) = K \otimes S(\tilde{K}) = K \otimes (\operatorname{im}(S(K_1, \mathrm{id}) \to S(K_1)). \quad \square$$

By the earlier cases we know that $\operatorname{im}(S(K_1, \mathrm{id}) \to S(K_1)) = {}_2S(K_1)$ and so we get

$$\operatorname{im}(S(K, \mathrm{id}) \to S(K)) = K \otimes {}_2S(K_1).$$

Moreover $S(K) = K \otimes S(K_1)$ by [Y, Proposition 4.6], so that ${}_2S(K) \neq 1$ implies that ${}_2S(K_1) \neq 1$ since $S(K_1)$ is a finite group. Theorem 3 follows from this and the fact that the scalar extension map $B(K_1) \to B(K)$, when these two groups are identified with $\mathbb{Q}/\mathbb{Z}$, is multiplication by the degree of K/K_1. $\square$

Acknowledgement. I am grateful to H. Kisilevsky and J. Labute for providing the proof of Lemma 10.

References

[CF] Cassels, J.W.S., Frohlich, A.: Algebraic number theory. Washington: Thompson 1967

[CL] Serre, J.-P.: Corps locaux. Act. Sci. et Ind. 1296. Paris: Hermann 1962

[FM] Frohlich, A., McEvett, A.M.: Forms over rings with involution. J. Algebra **12**, 79–104 (1969)

[H] Hahn, A.: A hermitian Morita theorem for algebras with anti-structure. J. Algebra **93**, 215–235 (1985)

[HTW] Hambleton, I., Taylor, L., Williams, E.B.: An introduction to the maps between surgery obstruction groups. In: Algebraic topology, Aarhus 1982 (Lecture Notes in Math., Vol. 1051, pp. 49–127) Berlin Heidelberg New York: Springer 1984

[MO] Reiner, I.: Maximal Orders, L.M.S. Monographs 5. London: Academic Press 1975

[R] Riehm, C.: The Schur subgroup of the Brauer group of a local field. L'Enseignement Mathématique (to appear)

[Sch] Scharlau, W.: Quadratic and hermitian forms. Grundl. Math. Wiss. 270. Berlin Heidelberg New York: Springer 1985

[S] Serre, J.-P.: Linear representations of finite groups, Graduate Texts in Mathematics 42. Berlin Heidelberg New York: Springer 1977

[Y] Yamada, T.: The Schur subgroup of the Brauer group. Lecture Notes in Math. 397. Berlin Heidelberg New York: Springer 1974

Received June 1, 1988