PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 103, Number 1, May 1988

THE SCHUR SUBGROUP OF THE BRAUER GROUP OF CYCLOTOMIC RINGS OF INTEGERS

C. RIEHM

(Communicated by Bhama Srinivasan)

ABSTRACT. Let K be a finite abelian extension of the rational numbers $\mathbf{Q}$. Let $\mathbf{S}$ be a finite set of primes of K including the infinite ones, and let $\mathfrak{o}$ be the ring of $\mathbf{S}$-integers in K. Then the Schur subgroup $S(\mathfrak{o})$ of the Brauer group $B(\mathfrak{o})$ is defined, in analogy with $S(K)$, via representations of finite groups on finitely generated projective $\mathfrak{o}$-modules. It is easy to see that $S(\mathfrak{o}) \subseteq S(K) \cap B(\mathfrak{o})$. We shall show that there is equality in the case of K a purely cyclotomic extension $\mathbf{Q}(\varepsilon_m)$ of $\mathbf{Q}$ (where ε_m is an mth root of 1).

Introduction. For any commutative ring $\mathfrak{o}$, one can define the Schur subgroup $S(\mathfrak{o})$ of the Brauer group $B(\mathfrak{o})$ as follows: Let G be a finite group, and $\rho: G \to \mathbf{GL}(M)$ a homomorphism of G to the automorphism group of a projective module M over $\mathfrak{o}$ with the property that the $\mathfrak{o}$-span $\mathfrak{o}\rho G$ of ρG is an Azumaya algebra over $\mathfrak{o}$. In this case we denote the Brauer class $[\mathfrak{o}\rho(G)]$ by $\beta(\rho)$. Then $S(\mathfrak{o})$ consists of the Brauer classes $\beta(\rho)$ as ρ runs over all such homomorphisms of all finite groups G. Alternatively, one can define $S(\mathfrak{o})$ to be the set of all Brauer classes $[\Lambda]$ where Λ runs over all Azumaya algebras which are homomorphic images of some group algebra $\mathfrak{o}G$ (G finite). It is easy to see, as in the case $\mathfrak{o} =$ a field, that $S(\mathfrak{o})$ is indeed a subgroup of $B(\mathfrak{o})$ (see [**D-M 1**]).

Suppose now that the canonical map $B(\mathfrak{o}) \to B(K)$ is injective (this is the case if $\mathfrak{o}$ is a Dedekind domain, e.g., see [**O-S**]). Then it is clear that

$$S(\mathfrak{o}) \subseteq S(K) \cap B(\mathfrak{o}) \tag{1}$$

and E. B. Williams has asked for conditions under which there is equality in the following situation: K is a finite abelian extension of $\mathbf{Q}$, and $\mathfrak{o}$ is the ring of $\mathbf{S}$-integers in K for a finite set of places $\mathbf{S}$ of K. We shall prove the following theorem.

THEOREM. *Let K be a cyclotomic field $\mathbf{Q}(\varepsilon_m)$ where m is a positive integer, and let $\mathbf{S}$ be any finite set of primes (containing the infinite primes). Then if $\mathfrak{o}$ is the ring of S-integers,*

$$S(\mathfrak{o}) = S(K) \cap B(\mathfrak{o}).$$

For other results on $S(\mathfrak{o})$, see [**D-M 1** and **D-M 2**].

Received by the editors March 19, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20C10, 16A26; Secondary 12A60, 16A16, 16A18, 12A35.

Key words and phrases. Schur subgroup, Brauer group, Azumaya algebras, integral representations, representations of finite groups.

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

The proof. For any abelian group A and any positive integer q, let A_q denote the q-primary subgroup of A—that is, the subgroup of A of those elements whose order divides some power of q.

Let $K = \mathbb{Q}(\varepsilon_m)$. We may assume that $m \not\equiv 2 \pmod 4$. We must show that an arbitrary element $\alpha \in S(K) \cap B(\mathfrak{o})$ is in $S(\mathfrak{o})$. Since $B(K)$ is a torsion group, we may write $\alpha = \sum \alpha_q$ where q runs over the rational primes and α_q is the q-primary component of α. This allows us to assume that $\alpha = \alpha_q$, i.e. that α is q-primary. By the "root of unity theorem" of Benard (see Theorem 6.1, [**Y**]), we can also assume that $q|2m$.

If p is any rational prime, possibly ∞, and L is an algebraic number field, then the p-local invariants of a Brauer class $\gamma \in B(L)$ are, by definition, the Hasse invariants (with values in $\mathbb{Q}/\mathbb{Z}$) of γ at the primes of L which lie above p—see Definition 6.4, [**Y**]. The Benard-Schacher theorem says that the Hasse invariants of each γ in $S(K)$ are "uniformly distributed", i.e. for each p, the p-local invariants of γ are determined (in a very explicit way) by any one of them (Theorem 6.1, [**Y**]). The p-local component of γ is defined to be the Brauer class $\gamma(p)$ whose p-invariants coincide with those of γ and whose other Hasse invariants are 0. Thus $\gamma = \sum_p \gamma(p)$.

Let M/L be a Galois extension with Galois group $\mathcal{G}(M/L)$. We shall denote the cohomology group $H^2(\mathcal{G}(M/L), M^*)$ by $H^2(M/L)$ and identify it with a subgroup of $B(L)$ in the usual way. Let $\mu(M)$ denote the group of roots of unity in M. There is a canonical map of $H^2(\mathcal{G}(M/L), \mu(M))$ into $H^2(\mathcal{G}(M/L), M^*)$ whose image will be denoted by $H^2_c(M/L)$. The Brauer-Witt theorem (Chapter 3, [**Y**]) says that $S(L)$ is the union of all $H^2_c(M/L)$ as M runs over all cyclotomic extensions $M = L(\varepsilon_n)$ of L.

Suppose that $q^r \| m$.

LEMMA 1. *The p-components $\alpha(p)$ of α are also in $S(K) \cap B(\mathfrak{o})$. Moreover $\alpha(p) = K \otimes \beta$ where $\beta \in H^2_c(\mathbb{Q}(\varepsilon_{pq^r})/\mathbb{Q}(\varepsilon_{q^r}))$ is a p-local ($\beta = \beta(p)$) Brauer class of $\mathbb{Q}(\varepsilon_{q^r})$.*

Here $K \otimes \beta$ stands for the Brauer class of K obtained from β by "restriction" (extension of scalars).

PROOF. By a theorem of Janusz [**J**], there is a $\beta \in S(\mathbb{Q}(\varepsilon_{q^r}))_q$ such that $\alpha = K \otimes \beta$. Benard, Schacher, and Yamada have characterized $S(\mathbb{Q}(\varepsilon_{q^r}))_q$ in terms of Hasse invariants (pp. 135–139, [**Y**]). Namely $S(\mathbb{Q}(\varepsilon_{q^r}))_q$ consists of all uniformly distributed Brauer classes in $B(\mathbb{Q}(\varepsilon_{q^r}))$ whose p-local invariants have order dividing $(p-1, q^r)$ for each (rational) prime p; there is one exception: if $q = 2$ and $p \equiv -1 \bmod 2^r$, then the p-local invariant is 0. It follows that $S(\mathbb{Q}(\varepsilon_{q^r}))_q$ is the direct sum of its p-local components—the latter are the (cyclic) subgroups of $S(\mathbb{Q}(\varepsilon_{q^r}))_q$ which are 0 locally at all primes of $\mathbb{Q}(\varepsilon_{q^r})$ not above p. Therefore if we express β as the sum $\sum \beta(p)$ of its p-local components, each component lies in $S(\mathbb{Q}(\varepsilon_{q^r}))_q$ and furthermore we can assume it is 0 if the corresponding p-component $\alpha(p)$ of α is 0. It is also clear that $\alpha(p) = K \otimes \beta(p)$ and, in particular that $\alpha(p) \in S(K)$. Since $B(\mathfrak{o})$ consists of the classes in $B(K)$ whose Hasse invariants are 0 outside of $\mathbf{S}$ (cf. Theorem 6.33 and Proposition 6.34, [**O-S**]), it follows at once that $\alpha(p) \in S(K) \cap B(\mathfrak{o})$. It follows from Lemma 8.5 and Theorem 8.6, [**Y**], that $\beta(p) \in H^2_c(\mathbb{Q}(\varepsilon_{pq^r})/\mathbb{Q}(\varepsilon_{q^r}))$. This finishes the proof of Lemma 1.

By Lemma 1, we can now assume that α is p-local as well being q-primary.

LEMMA 2. *The cohomology class α contains a cocycle $f \in Z^2(K(\varepsilon_p)/K)$ all of whose values are in $\langle \varepsilon_{q^r} \rangle$.*

PROOF. Because of our identifications,

$$H_c^2(\mathbf{Q}(\varepsilon_{pq^r})/\mathbf{Q}(\varepsilon_{q^r})) \subseteq H_c^2(\mathbf{Q}(\varepsilon_{p^m})/\mathbf{Q}(\varepsilon_{q^r})).$$

Therefore since $\alpha = K \otimes \beta$ where β is as in Lemma 1, we get $\alpha \in H_c^2(K(\varepsilon_p)/K)$ and so Lemma 2 follows at once since α is q-primary.

LEMMA 3. *If $\alpha \neq 0$, then p lies below a prime of $\mathbf{S}$ and does not divide m.*

PROOF. If p were a divisor of m, then K would contain ε_p resp. ε_4 if $p = 2$; by Proposition 4.8 and Corollary 5.4 of [**Y**], the Schur subgroup of a completion $K_\mathfrak{p}$ of K, at any prime $\mathfrak{p}$ lying over p, would then be trivial, so α also would be trivial. On the other hand, the fact that $\alpha \in B(\mathfrak{o})$ means exactly that its local components are 0 at all $\mathfrak{p}$ not in $\mathbf{S}$. □

We now define A be the the crossed-product algebra

$$A = (K(\varepsilon_p)/K, f) = \sum_{\sigma \in \mathscr{G}} K(\varepsilon_p) u_\sigma$$

where $\mathscr{G} = \mathscr{G}(K(\varepsilon_p)/K)$. Of course $A \in \alpha$. Similarly we define the order

$$\Lambda = (\mathfrak{o}[\varepsilon_p]/\mathfrak{o}, f) = \sum_{\sigma \in \mathscr{G}} \mathfrak{o}[\varepsilon_p] u_\sigma.$$

Thus $A = K \otimes \Lambda$.

LEMMA 4. *Λ is an Azumaya algebra over $\mathfrak{o}$ with Brauer class $[\Lambda] = \alpha$.*

PROOF. Let $\mathfrak{p}$ be any prime not in $\mathbf{S}$. Then

$$\hat{\mathfrak{o}}_\mathfrak{p} \otimes \Lambda = \sum_{\sigma \in \mathscr{G}} \hat{\mathfrak{o}}_\mathfrak{p} \otimes \mathfrak{o}[\varepsilon_p] u_\sigma$$

is an $\hat{\mathfrak{o}}_\mathfrak{p}$-order in the $K_\mathfrak{p}$-algebra

$$K_\mathfrak{p} \otimes A = \sum_{\sigma \in \mathscr{G}} K_\mathfrak{p} \otimes K(\varepsilon_p) u_\sigma.$$

Let $L_1, \ldots, L_g$ be the completions of $L = K(\varepsilon_p)$ at the primes lying above $\mathfrak{p}$. Then the $K_\mathfrak{p}$-algebra $K_\mathfrak{p} \otimes K(\varepsilon_p)$ is (isomorphic to) the direct sum $L_1 \oplus \cdots \oplus L_g$. We shall now show that $\hat{\mathfrak{o}}_\mathfrak{p} \otimes \mathfrak{o}[\varepsilon_p]$ is likewise the direct sum of the rings of integers $\mathfrak{O}_i$ of the L_i, after identifying by means of this isomorphism.

Since $\hat{\mathfrak{o}}_\mathfrak{p} \otimes \mathfrak{o}[\varepsilon_p] \subseteq \bigoplus \mathfrak{O}_i$ and both are $\hat{\mathfrak{o}}_\mathfrak{p}$-orders on a separable algebra, it suffices to show that they have the same discriminant (cf. [**MO**]). Now the discriminant of $\hat{\mathfrak{o}}_\mathfrak{p} \otimes \mathfrak{o}[\varepsilon_p]$ is $d(\mathfrak{o}[\varepsilon_p]/\mathfrak{o})\hat{\mathfrak{o}}_\mathfrak{p}$ where $d(\mathfrak{o}[\varepsilon_p]/\mathfrak{o})$ is the discriminant of $\mathfrak{o}[\varepsilon_p]/\mathfrak{o}$. The discriminant of $\bigoplus \mathfrak{O}_i$ is the product of the $d(\mathfrak{O}_i/\hat{\mathfrak{o}}_\mathfrak{p})$ and thus is equal to $d(\mathfrak{o}[\varepsilon_p]/\mathfrak{o})\hat{\mathfrak{o}}_\mathfrak{p}$ by Proposition 5, Chapter I, [**C-F**].

Let $\mathscr{G}_1 \subseteq \mathscr{G}$ be the stabilizer of the summand L_1—it is the decomposition group of the prime belonging to L_1. Consider the crossed-product order $\Lambda_1 = (\mathfrak{O}_1/\hat{\mathfrak{o}}_\mathfrak{p}, f_1)$ where f_1 is the restriction of f to $\mathscr{G}_1$. Now f_1 is split since f splits at $\mathfrak{p}$. Since $\mathfrak{p}$ does not ramify in $\mathfrak{O}_1$, Λ_1 is a maximal order by a theorem of Auslander and Goldman—see Theorem 28.5, [**C-RI**]. Since $\hat{\mathfrak{o}}_\mathfrak{p} \otimes \mathfrak{o}[\varepsilon_p]$ is the direct sum of the $\mathfrak{O}_i$, it follows that Λ is also maximal by a theorem of Merklen (Proposition 1, (iv), [**M**]). Since $K \otimes \Lambda = A$ and the local Hasse invariants of A are all 0 at the primes of $\mathfrak{o}$ (i.e. the primes $\mathfrak{p} \notin \mathbf{S}$), it follows that Λ is an Azumaya algebra over $\mathfrak{o}$ and $\Lambda \in \alpha$ (cf. [**D-I**]). □

Thus to prove our theorem, it suffices to prove that $\Lambda \in S(\mathfrak{o})$.

Let G be the extension of $\mathscr{G}$ by $\mu(L)$, corresponding to the cocycle f. Then we can view G as the group generated by $\mu(L)$ and the u_σ in Λ. Moreover it is clear that G spans Λ over $\mathfrak{o}$, and so $\Lambda \in S(\mathfrak{o})$ as desired. □

REFERENCES

[**C-F**] J. W. S. Cassels and A. Frohlich, *Algebraic number theory*, Thompson Book, Washington, D. C., 1967.

[**C-RI**] C. W. Curtis and I. Reiner, *Methods of representation theory with applications to groups and orders*, vol. I, Pure and Appl. Math., Wiley, New York, 1981.

[**D-I**] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Math., vol. 181, Springer-Verlag, Berlin and New York, 1971.

[**D-M 1**] F. R. DeMeyer and R. A. Mollin, *The Schur group of a commutative ring*, J. Pure Appl. Math. **35** (1985), 117–122.

[**D-M 2**] ____, *The Schur group*, Lecture Notes in Math., vol. 1142, Springer-Verlag, Berlin and New York, pp. 205–210.

[**J**] G. J. Janusz, *The Schur group of cyclotomic fields*, J. Number Theory **7** (1975), 345–352.

[**M**] H. Merklen, *Hereditary crossed product orders*, Pacific J. Math. **74** (1978), 391–406.

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

[**O-S**] M. Orzech and C. Small, *The Brauer group of commutative rings*, Lecture Notes in Pure and Appl. Math., vol. 11, Marcel Dekker, New York, 1975.

[**Y**] T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Math., vol. 397, Springer-Verlag, Berlin and New York, 1974.

DEPARTMENT OF MATHEMATICS AND STATISTICS, MCMASTER UNIVERSITY, HAMILTON, ONTARIO L8S 4K1, CANADA