Journal of Pure and Applied Algebra 35 (1985) 117–122
North-Holland

THE SCHUR GROUP OF A COMMUTATIVE RING

F. DeMEYER
Department of Mathematics, Colorado State University, Ft. Collins, CO 80523, USA

R. MOLLIN
Department of Mathematics, University of Calgary, Calgary, Alberta, Canada T2N 1N4

Communicated by H. Bass
Received 29 August 1983
Revised 10 January 1984

Let R denote a commutative ring and $B(R)$ the Brauer group of classes of Azumaya R-algebras as developed in [1]. An Azumaya R-algebra A represents a class in $S(R) \subset B(R)$ if there is a finite group G and an R-algebra epimorphism $f: RG \to A$. Let B be another Azumaya R-algebra and H a finite group with an R-algebra epimorphism $g: RH \to B$. If $\tilde{H}$ is the group whose elements are the same as the elements of H with multiplication given by $x \times y = yx$ (where multiplication on the right is in H), then the correspondence $(x, y) \to f(x) \otimes g(y)$ induces an R-algebra epimorphism $R(G \times \tilde{H}) \to A \otimes B^0$. Thus, $S(R)$ is a subgroup of $B(R)$ called the Schur group of R. This note is concerned with computations of the Schur group of a commutative ring and with properties of cyclotomic algebras which represent certain classes in the Schur group.

If R is a commutative ring of non-zero characteristic, then $S(R) = (0)$. On the other hand, any finite Abelian group is the Schur group of a commutative ring which is finitely generated as an algebra over the rational integers. We generalize several standard facts about the Schur group of a field to commutative rings with finitely many idempotents. If R is a field, a consequence of the Brauer–Witt Theorem (pg. 31 of [14]) is that every element of $S(R)$ is represented by a cyclotomic R-algebra. For a commutative ring R with finitely many idempotents, the classes in $B(R)$ represented by cyclotomic algebras form a subgroup $S'(R)$ of $S(R)$ and the inclusion $S'(R) \subset S(R)$ may be proper. The functorial properties of the Brauer functor give an action of $\mathrm{Aut}(R)$ as a group of automorphisms of $B(R)$, and $S(R)$ (and $S'(R)$ when R contains only finitely many idempotents) are left invariant under this action. If R is an integral domain and $S'(R)$ contains an element of order m, then $\mathrm{Units}(R)$ contains an element of order m, and a cyclotomic R-algebra is fixed by an automorphism of R if and only if the automorphisms fixes the element of order m in $\mathrm{Units}(R)$.

Proposition 1. *Let R be a commutative ring of characteristic $n>0$. Then $S(R)=(0)$.*

Proof. Begin by assuming R is connected (the only idempotents in R are 0 and 1). let G be a finite group and A an Azumaya R-algebra. Assume there is an R-algebra epimorphism $f: RG \to A$. Let P be the prime subring of G and let $B=f(PG)$. Thus, B is the P-subalgebra of A generated by $\{f(g): g \text{ in } G\}$. Any element in the center C of B is in the center of A, so $C \subset R$. Let N be the radical of B. Since B is a finite ring, N is nilpotent. It is easy to check that AN is a nilpotent two-sided ideal in A. Since A is an Azumaya R-algebra, $AN=Am$ for a nilpotent ideal m of R (Corollary 2.3.7 of [4]). Replace R by R/m and A by A/mA. A is still an Azumaya R-algebra, and since m is nilpotent, R is connected. There is still an epimorphism $f: RG \to A$. The prime ring of our new R is a field k, and $B=f(kG)$ has no non-trivial nilpotent two-sided ideals. Thus, the center C of B is a finite connected ring with no nilpotent ideals so C is a field and B is an Azumaya C-algebra. The natural epimorphism $R \otimes B \to A$ is one-to-one since it is one-to-one on $R=R \otimes C$. Since C is finite, B is in the zero class of $B(C)$, so A is in the zero class of $B(R)$. The Brauer group is unchanged modulo a nilpotent ideal [6]. This shows $S(R)=(0)$ whenever R is connected. If R contains idempotents, then for each p in the Pierce Sheaf of R, A_p is in the zero class of $B(R_p)$. It follows from Corollary 1.11 of [10] that A is in the zero class of $B(R)$ and the result follows.

As a result of Proposition 1, we will assume from now on that R has characteristic $=0$.

Theorem 1. *Let $\mathscr{A}$ be any finite abelian group, then there is a commutative, finitely generated Z-algebra R with $S(R) \cong \mathscr{A}$.*

Proof. It is easy to show that $S(R \oplus T)=S(R) \times S(T)$, so it suffices to assume $\mathscr{A}$ is the cyclic group C_{q^n} of order q^n for a prime q and positive integer n.

Case 1: q is an odd prime.

Let p be an odd prime chosen so that $p \equiv 1 \pmod{q^n}$ and $p \equiv 3 \pmod 4$. Such a prime exists by the Chinese Remainder Theorem and Dirichlet's Theorem which says that an arithmetic progression contains an infinite number of primes. Let $K=Q(e_{4q^n}, \sqrt{p})$, where e_{4q^n} is a primitive $4q^n$ root of 1. Let $S(p,q;K)$ be the subgroup of $S(K)$ consisting of those classes (A) such that $\text{ind}_r(A)=1$ for all rational primes $r \neq p,q$ ($\text{ind}_r(A)$ is the index of A tensored with the completion of K at any prime of K lying over r). We want to see first that $S(p,q;K)=C_{q^n}$. By Theorem 1 of [3], the order of any element in $S(K)$ divides $4q^n$. Let (B) be in $S(p,q;K)$ and assume $\text{ind}_p(B)$ divides 4. By Corollary 1 of [7], $(B)=(K \otimes C)$ where (C) is in $S_2(Q(e_4))$. By Theorem 4.4, pg. 43 of [14], b divides $(p-1)$. Since $p \equiv 3 \pmod 4$, then $b=\text{ind}_p(C)<3$. Let P be a prime in $Q(e_4)$ lying over p and let $\hat{P}$ be a prime in K lying over P. Letting inv_p be the Hasse invariant at P, we have by II, pg. 374 of [2],

$$\text{inv}_{\tilde{p}}(K \otimes C) \equiv d \times \text{inv}_p(C) \pmod 1 \quad \text{where } d = (Q_p K : Q_p(e_4)).$$

Since $d=2$, $\text{inv}_{\tilde{p}}(K \otimes C) = 0$. Thus, if (B) is in $S(p, q; K)$, then $\text{ind}_p(B)$ is a power of q. Now assume (B) is in $S(p, q; K)$, and consider $\text{ind}_q(B)$. Applying Theorem 4.3 of [14] again (with $c = (p-1)$ in 4.3 of [14]) we get $\text{ind}_q(B) = 1$. To this point we have seen that if (B) is in $S(p, q; K)$, then $\text{ind}_q(B) = 1$ and $\text{ind}_p(B) = q^s$ with $s \leq n$. In the proof of Lemma 3 of [3], a finite group H of order $p^a q^b$ is constructed so that a central component (B) of $Q(e_{q^n})H$ has $\text{ind}_p(B) = q^n$ and $\text{ind}_r(B) = 1$ for all rational primes $r \neq p$. Let P be a prime in $Q(e_{q^n})$ lying over p and let $\tilde{P}$ be a prime in K lying over P. Then as above,

$$\text{inv}_{\tilde{P}}(K \otimes B) \equiv d \times \text{inv}_P(B) \pmod 1 \quad \text{where } d = (Q_p K : Q_p(e_{q^n})) = 4.$$

Thus, $\text{ind}_p(K \otimes B) = q^n$ and $\text{ind}_r(K \otimes B) = 1$ whenever $r \neq p$. Thus $S(p, q; K)$ contains an element of order q^n. It now follows that $S(p, q; K)$ is cyclic of order q^n with generator $(K \otimes B)$. Let $R = Z(e_{4q^n}, \sqrt{p}, 1/p, 1/q)$, and let A be the natural image of RH in $K \otimes B$. Then A is a separable R-algebra since $[H : 1] \in \text{Units}(R)$. It follows that A is a maximal R order in $K \otimes B$, so A is an Azumaya R-algebra. Thus (A) is in $S(R)$. Since R is a Dedekind domain, the order of (A) in $S(R)$ is equal to the order of $(K \otimes B)$ in $S(K)$ (7.2 of [1]), so $S(R)$ contains a cyclic subgroup of order q^n. Let (C) be in $S(R)$, then $(K \otimes C)$ is in $S(K)$. If $\text{ind}_r(K \otimes C) \neq 1$, then $K \otimes C$ is ramified at r (Theorem 1, pg. 145 of [13]), so in this case $r = p, q$ since C is separable and thus unramified at all (non-invertible) primes of R. Thus, $(K \otimes C)$ is in $S(p, q; K)$ which implies $S(R) = C_{q^n}$.

Case 2: $q = 2$ *and* $n > 1$.

Let p be an odd prime so that $p \equiv 1 \pmod{2^n}$ and let $K = Q(e_{q^n})$. As in Case 1, by employing the construction of Lemma 3 of [3], there is a finite group H of order $2^a p^b$ and a central component B of KH which represents an element of order 2^n in $S(p, 2; K)$. Theorems 3 and 4 of [3] assert that $S(p, 2; K)$ is cyclic of order 2^n. If $R = Z(e_{2^n}, 1/2, 1/p)$, then as in Case 1, $S(R) = C_{2^n}$.

Case 3: $q = 2$ *and* $n = 1$.

Let $R = Z(\sqrt{2})$, and let D be the usual quaternions over $Q(\sqrt{2})$ with basis $(1, \mathrm{i}, \mathrm{j}, \mathrm{k})$. Let $a = (1+\mathrm{i})/\sqrt{\ }$, $b = (1+\mathrm{j})/\sqrt{2}$, and let $A = R + RA + Rb + Rab$. Then it is well known (Exercise 2, pg. 147 of [4]) that $B(R) = C_2$ is generated by the class represented by A. But $a^8 = b^8 = 1$ and $ab = b^4 a$, so A is a homomorphic image of RH where H is a group of order 64. Thus $S(R) = B(R) = C_2$ in this case. This proves the theorem.

Remark. Using the same techniques as in the proof of Theorem 1, one can show that

I. If $p_1, \ldots, p_t$ are distinct primes, then $S(Z(1/p_1 \cdots p_t)) = (C_2)^t$. (The generating classes for $S(Z(1/p_1 \cdots p_t))$ have a representative with index $= 2$ at $1/p_i$ and the infinite real prime of Q.) In particular, $S(Z(1/2)) = C_2$, and the nontrivial class in $S(Z(1/2))$ has a representative which is a homomorphic image of the group ring of the quaternion group of order 8.

II. If q is a prime and n is a positive integer, then $S(Z(e_{q^n}, 1/q) = (0)$.

III. If R is the ring of integers in the algebraic number field K, then $S(R)=(0)$ if there are zero or an odd number of real imbeddings of K. If there are an even number of real imbeddings of K, then $S(R)\subset C_2$. The ring $Z(\sqrt{2})$ in Theorem 1 is the ring of integers in $Q(\sqrt{2})$. This field has two real imbeddings and in this case, $S(R)=C_2$.

IV. Let q be any prime and n a positive integer. Let p be a prime chosen so that $p\equiv 1 \pmod{q^n}$. Let K be a subfield of $Q(e_p)$ with $[K:Q]=(p-1)/q^n$. Let K_p be the local field obtained by completing K at a prime P lying over p. By Theorem 4.4 of [14], $S(K_p)$ is a cyclic group of order $(p-1)/c$ where c is the tame ramification index of K_p over Q_p. Since p is totally ramified in K_p, $c=(p-1)/q^n$ so $(p-1)/c=q^n$ and $S(K_p)=C_{q^n}$. Thus, any cyclic group of prime power order is the Schur group of a local field, and any finite Abelian group is the Schur group of a finite direct sum of local fields.

Let $S''(R)$ be the subset of $S(R)$ consisting of those classes which have a representative which is a homomorphic image of a separable group algebra over R. The group ring of $R(G)$ is separable if and only if $[G:1]$ is a unit in R. Thus $S''(Z(\sqrt{2}))\neq S(Z(\sqrt{2}))$. It follows from the proof of Theorem 1 and Remark I above that for any finite Abelian group $\mathscr{A}$ there is a commutative ring with $S''(R)=\mathscr{A}$.

Let R be a connected commutative ring and let n be a positive integer. Assume the separable closure of R contains a primitive nth root of unity e_n and that $R(e_n)$ is a Galois extension of R in the separable closure with Galois group H. Let b be a 2-cocycle on H with values in the cyclic group generated by e_n. The crossed product algebra $[R(e_n)/R, H, b]$ is called a cyclotomic R-algebra. If $R=R_1\oplus\cdots\oplus R_m$ with R_i connected, then a cyclotomic R-algebra is the direct sum of cyclotomic R_i-algebras, $i=1,\ldots,m$. If R is not connected, questions about cyclotomic R-algebras reduce to questions about cyclotomic algebras over the connected components of R. We will not always explicitly make this reduction. Cyclotomic R-algebras are Azumaya R-algebras (3.2.12 of [4]). There is a central extension G of (e_n) by H determined by the cocycle b, and a natural homomorphism from RG onto $[R(e_n)/R, H, b]$. If $[R(e_m)/R, \hat{H}, \hat{b}]$ is another cyclotomic crossed product determining the central extension K, then $[R(e_n)/R, H, b]\times[R(e_m)/R, H, b]^0$ is a homomorphic image of $R(G\times K)$, so the classes in $S(R)$ with a representative which is a cyclotomic R-algebra form a subgroup of $S(R)$ which we denote $S'(R)$. Let p and q be odd primes and let e_{pq} be a primitive pqth root of 1. Let $R=Z(e_{pq}+\bar{e}_{pq})$ and let $S=Z(e_{pq})$. Then S/R is a Galois extension of rank $=2$ (since S/R is unramified at all the finite primes of R). The algebra $[S/R, C_2, -1]$ is an Azumaya crossed product representing a nontrivial element in $B(R)$ (since -1 is not a norm from the quotient field of S to the quotient field of R). Since no integer bigger than 1 is invertible in R, $S'(R)\neq S''(R)$.

Remark. We have already observed that the inclusion $S''(R)\subset S(R)$ is proper when $R=Z(\sqrt{2})$. Since $Z(\sqrt{2})$ is separably closed, $S'(Z\sqrt{2})=0$ so the inclusion $S'(R)\subset S(R)$ may also be proper.

Proposition 2. *Let R be an integrally closed noetherian domain. Then $S''(R) \subset S'(R)$.*

Proof. Let $(A) \in S''(R)$ with $f: RG \to A$ an epimorphism of R-algebras and $n = [G:1] \in \text{Units}(R)$. Let K be the quotient field of R. By 3.11 of [14] we have $(K \otimes A) = [K(e_m)/K, H, b]$ for some primitive mth root of unity e_m and some 2-cocycle $b: H \times H \to D$ where D is a cyclic group of roots of unity in $K(e_m)$. It follows from the proof of 3.11 of [14] that m may be chosen so that if p is a prime with $(p, n) = 1$, then $(p, m) = 1$. If $(p, m) = 1$, then there are arbitrarily large integers s with $p^s \equiv 1 \pmod{n}$. The order of b in $H^2(H, K(e_m))$ divides n, so $b^{p^s} = b$. Thus we can assume the values of b lie in (e_m). By restriction, H is a group of automorphisms of $R(e_m)$ and since R is integrally closed, H fixes exactly R. Since $m \in \text{Units}(R)$, $R(e_m)$ is a separable extension of R. By (3.1.2 of [4]), $R(e_m)$ is a Galois extension of R with group H. The crossed product $[R(e_m)/R, H, b]$ is a cyclotomic R-algebra and $K \otimes [R(e_m)/R, H, b] \cong [K(e_m)/K, H, b]$. By 7.2 of [1] it follows that A is equivalent to $[R(e_m)/R, H, b]$ in $B(R)$ which proves the proposition.

The functorial properties of the Brauer functor give an action of $\text{Aut}(R)$ on $B(R)$. This action can be given on the algebra level in the following way. If $(A) \in B(R)$ and $\sigma \in \text{Aut}(R)$, let A_σ be the R-algebra equal to R as a ring but with R-algebra action given by the rule $r \times a = \sigma^{-1}(r)a$ for $r \in R$ and $a \in A$. Consequences of this observation have been worked out in [9] and [5].

Proposition 3. *The groups $S(R)$ (and $S'(R)$ when R has finitely many idempotents) are invariant subgroups of $B(R)$ under the natural action of* $\text{Aut}(R)$ *on $B(R)$.*

Proof. Let A be an Azumaya R-algebra and G a finite group. Let $f: RG \to A$ be an algebra epimorphism, and let $\sigma \in \text{Aut}(R)$. Then $f: R_\sigma G \to A_\sigma$ is an R-algebra epimorphism. On the other hand, $RG \cong R_\sigma G$ as R-algebras by the map $r_g \times g \to \sigma(r_g) \times g$. Thus $S(R)$ is invariant under $\text{Aut}(R)$. Assume R is connected, and let $[R(e_m)/R, H, b]$ be a cyclotomic algebra representing an element in $S'(R)$, and let $\sigma \in \text{Aut}(R)$. Then $[R(e_m)/R, H, b]_\sigma = [R(e_m)/R, H, b^\sigma]$. This last algebra is also a cyclotomic algebra. The result for rings with finitely many idempotents follows easily.

Proposition 4 (6.2 of [14]). *Let R be an integral domain. If $S'(R)$ contains an element $[R(e_n), H, b]$ of order m, then R contains a primitive mth root of* 1.

Proof. Since H is abelian, for each σ in H, b is a well-defined factor set where $b(\tau, \gamma) = \sigma(b(\tau, \gamma))$ for all $\tau, \gamma \in H$. Map $[R(e_n)/R, H, b]$ to $[R(e_n)/R, H, b^\sigma]$ by $x_\sigma u_\sigma \to \sigma(x_\sigma)y$. This induces an R-algebra isomorphism, so $[R(e_n)/R, H, b]$ is equivalent to $[R(e_n)/R, H, b^\sigma]$ in $B(R)$. There is a positive integer r such that $\sigma(e_n) = e_n^r$ so $b = b^r$. Since $[R(e_n)/R, H, b]$ has order m, it follows that m divides $r - 1$, or $r = 1 + ms$, $s \in Z$. Now $\sigma(e_m) = e_m^r = e_m^{1+ms} = e_m$, so $\sigma(e_m) = e_m$ for all $\sigma \in H$ so r_m is in R.

Proposition 5 (Corollary 2 of [9]). *Let R be an integral domain. Then an element of order m in $S'(R)$ is fixed by an element σ in* Aut(R) *if and only if R contains a primitive mth root of* 1 *fixed by σ.*

Proof. In the proof of Proposition 4 we saw $e_m \in R$. As in the proof of Proposition 4, for any $\sigma \in \mathrm{Aut}(R)$, if $\sigma(e_m) = e_m^s$ then $[R(e_n)/R, H, b]_\sigma = [R(e_n)/R, H, b]$ if and only if m divides s if and only if $\sigma(e_m) = e_m$.

References

[1] M. Auslander and O. Goldman, The Brauer group of a commutative ring, Trans. Amer. Math. Soc. 97 (1960) 367–409.

[2] M. Bernard, The Schur subgroup 1, J. Algebra 22 (1972) 374–377.

[3] M. Bernard and M. Schacher, The Schur subgroup 2, J. Algebra 22 (1972) 378–385.

[4] F. DeMeyer and E. Ingraham, Separable Algebras over Commutative Rings, Lecture Notes in Math. 181 (Springer, Berlin, 1971).

[5] F. DeMeyer, An action of the automorphism group of a commutative ring on its Brauer group, Pacific J. Math. 97 (1981) 327–338.

[6] F. DeMeyer, The Brauer group of a ring modulo an ideal, Rocky Mtn. J. Math. 6 (1976) 191–198.

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

[8] G.J. Janusz, Separable algebras over commutative rings, Trans. Amer. Math. Soc. 122 (1966) 461–479.

[9] G.J. Janusz, Automorphism groups of simple algebras and group algebras, Proceedings of the Philadelphia Conference on Ring Theory, Lecture Notes in Pure and Applied Math. 37 (M. Dekker, New York, 1978) 381–388.

[10] A. Magid, Pierce's representation and separable algebras, Illinois J. Math. 15 (1971) 114–121.

[11] R. Mollin, Herstein's conjecture, automorphisms and the Schur group, Comm. in Algebra 6 (1978) 237–248.

[12] R. Mollin, The Schur group of a field of characteristic zero, Pacific J. Math. 76 (1978) 471–478.

[13] I. Reiner, Maximal Orders (Academic Press, New York, 1975).

[14] T. Yamada, The Schur subgroup of the Brauer group, Lecture Notes in Math. 397 (Springer, Berlin, 1974).