

## Invariants of Group Rings

F. R. DEMEYER

*Department of Mathematics, Colorado State University,  
Fort Collins, Colorado 80526*

AND

R. A. MOLLIN\*

*Department of Mathematics and Statistics, University of Calgary,  
Calgary, Alberta, Canada T2N 1N4*

*Communicated by Walter Feit*

Received February 26, 1987

DEDICATED TO THE MEMORY OF IRVING REINER

The Schur group, uniform (distribution) group, Schur index, and Schur exponent are examined in the context of separable group rings of finite groups over commutative rings. © 1988 Academic Press, Inc.

Since the foundation paper of M. Auslander and O. Goldman [1], several authors have generalized constructions for studying group algebras over fields to separable algebras over commutative rings. Specifically, we have in mind the Schur index [20], the Schur exponent [18], the Schur group [8], and the uniform group [11]. This paper gives additional properties of these constructions and studies the relationship between them. First we reproduce the definitions of the Schur index  $M_\chi(R)$  and Schur exponent  $m_\chi(R)$  of a character  $\chi$  on a finite group  $G$  with respect to a commutative ring  $R$  in which  $[G:1]$  is a unit. If  $R$  is a field then  $m_\chi(R) = M_\chi(R)$  and more generally if  $R$  is a commutative ring then  $m_\chi(R) | M_\chi(R)$ . We conjecture  $m_\chi(R) = M_\chi(R)$  for every commutative ring  $R$ . If  $\mathcal{S}(R)$  denotes the Schur group of  $R$ ,  $\mathcal{U}(R)$  the uniform group of  $R$ , and  $B(R)$  the Brauer group of  $R$  then when  $R$  is a field  $\mathcal{S}(R) \subset \mathcal{U}(R) \subset B(R)$ . Each of these inclusions may be proper. Here we are mostly interested in  $\mathcal{U}(R)$  and

\* Research supported by an I. W. Killam Fellowship at the University of Calgary and by NSERC Canada Grant A8484.

the connections between  $\mathcal{S}(R)$  and  $\mathcal{U}(R)$ . For each positive integer  $n$  there is a local field  $K_\rho$  such that  $\mathcal{U}(K_\rho)/\mathcal{S}(K_\rho) \cong C_n$ , where  $C_n$  is the cyclic group of order  $n$ . Let  $\varepsilon_n$  be a primitive  $n$ th root of unity ( $n \not\equiv 2 \pmod 4$ ) and let  $M = \mathbf{Q}(\varepsilon_n + \varepsilon_n^{-1})$ . If  $[A]$  has order 2 in  $\mathcal{S}(\mathbf{Q}(\varepsilon_n))$  then  $[A] = [B \otimes_M \mathbf{Q}(\varepsilon_n)]$ , where  $[B] \in \mathcal{U}(M)$  and the order of  $[B]$  is 2. There may not be such a  $[B]$  in  $\mathcal{S}(M)$ . If  $k$  is a perfect field we determine  $\mathcal{U}(k[t, t^{-1}])$  and give some other examples. In particular, there are commutative rings  $R$  for which  $\mathcal{S}(R) \not\subseteq \mathcal{U}(R)$  but we have not been able to find an integral domain  $R$  with  $\mathcal{S}(R) \not\subseteq \mathcal{U}(R)$ .

Let  $R$  denote a commutative ring with no idempotents other than 0 and 1. Let  $G$  be a finite group of order  $n$  and assume the group ring  $RG$  is a separable  $R$ -algebra. Note  $RG$  is separable over  $R$  if and only if  $n \cdot 1 \in \text{Units}(R)$ . Let  $M$  be a finitely generated projective left  $RG$ -module and let  $\{f_1, \dots, f_m\} \subseteq \text{Hom}_R(M, R)$ ,  $\{x_1, \dots, x_m\} \subseteq M$  be an  $R$  dual basis for  $M$ . Following [21] the character  $\chi$  on  $G$  determined by  $M$  is given by

$$\chi_M(g) = \sum_{j=1}^m f_j(gx_j), \quad g \in G. \tag{1}$$

In [21] it is shown that  $\chi_M$  is independent of the choice of dual basis for  $M$  and other properties of  $\chi_M$  are given. Summarizing [21], let  $\Omega$  denote the separable closure of  $R$ . A separable  $R$ -subalgebra  $S$  of  $\Omega$  is called a splitting ring for  $RG$  in case

$$SG \cong \bigoplus_{i=1}^s \text{End}_S(P_i) \tag{2}$$

for finitely generated projective  $S$ -modules  $P_i$  ( $1 \leq i \leq s$ ), where  $s$  is the number of conjugacy classes of  $G$ . If  $\varepsilon_n$  is a root of  $x^n - 1$  in  $\Omega$  of order  $n$  (a primitive  $n$ th root of 1) then  $R(\varepsilon_n)$  is a splitting ring for  $RG$  so splitting rings exist. Moreover, if we write

$$\Omega G = \bigoplus_{i=1}^s \text{End}_\Omega(M_i) \tag{3}$$

and let  $\chi_i$  be the character determined by  $M_i$ , then after a reordering  $\chi_i$  will also be the character determined by  $P_i$  so  $\chi_i$  is independent of the choice of splitting ring. Moreover, if we let  $R[\chi_i]$  be the  $R$ -subalgebra of  $\Omega$  generated by the  $\chi_i(g)$  then  $R[\chi_i]$  is a finitely generated projective separable  $R$ -subalgebra of  $\Omega$  and for each  $g \in G$ ,  $\chi_i(g)$  is a sum of powers of  $\varepsilon_n$  (Theorem 2.1 of [21]).

A separable extension  $T$  of  $R$  in  $\Omega$  is called a splitting ring for  $\chi_i$  in case there is a finitely generated projective  $TG$  module  $N_i$  such that  $\Omega \otimes_T N_i \cong M_i$  as  $\Omega G$  modules [20]. It is clear that if  $T$  is a splitting ring for  $\chi_i$  then  $R[\chi_i] \subseteq T$ .

DEFINITION [20]. The Schur index  $M_R(\chi_i)$  is  $\min\{\text{Rank}_{R[\chi_i]}(T)\}$ , where  $T$  runs over all splitting rings for  $\chi_i$  in  $\Omega$ .

Since  $R(\varepsilon_n)$  is a splitting ring for  $RG$ ,  $R(\varepsilon_n)$  splits  $\chi_i$  for every  $i$  (Theorem 1.2 of [21]) so  $M_R(\chi_i)$  is finite.

Additional properties of  $M_R(\chi_i)$  and some computations are given in [20].

As above, let  $M_i$  be a finitely generated projective  $\Omega G$  module determining the character  $\chi_i$ . The restriction of the natural epimorphism  $\bar{\psi}_i: \Omega G \rightarrow \text{End}_\Omega(M_i)$  gives an epimorphism  $\psi_i: R[\chi_i]G \rightarrow A$ . Since  $R[\chi_i]G$  is a separable  $R[\chi_i]$ -algebra,  $A$  is a separable  $R[\chi_i]$ -algebra. Let  $C$  denote the center of  $A$  and let  $c \in C$ ,

$$c = \sum_{g \in G} r_g \psi(g), \quad r_g \in R[\chi_i]. \tag{4}$$

Viewing both sides of this equation as lying in  $\text{End}_\Omega(M_i)$  and taking the trace to  $\Omega$  of both sides we get (since  $c \in \Omega$ )

$$z_i c = \sum_{g \in G} r_g \chi_i(g), \tag{5}$$

where  $z_i = \text{Rank}_\Omega(M_i)$ . If we let  $R_0 = P(1/n, \varepsilon_n)$ , where  $P$  is the prime subring of  $R$ , then  $R_0 G \cong \bigoplus_{i=1}^t \text{End}_{R_0}(Q_i)$  for finitely generated projective  $R_0$ -modules  $Q_i$ . Then  $\Omega G \cong \bigoplus_{i=1}^t \text{End}_{\Omega \otimes R_0}(\Omega \otimes Q_i)$  so we can assume  $t = s$  and  $\Omega \otimes Q_i \cong M_i$ . In particular, letting  $K_0$  be the quotient field of  $R_0$  if characteristic  $R = 0$  or  $K_0 = R_0$  otherwise we get  $z_i = \text{Rank}_\Omega(M_i) = \text{Rank}_{R_0}(Q_i) = \text{Rank}_{K_0}(K_0 \otimes Q_i)$  divides  $n$  so we can solve (5) for  $c$  and conclude  $c \in R[\chi_i]$ . Therefore,  $A$  is an Azumaya algebra over  $R[\chi_i]$ . By Corollary 3.2.6 of [6],  $R[\chi_i]G \cong A \oplus B$  for some separable  $R[\chi_i]$ -algebra  $B$  and  $\Omega \otimes_{R[\chi_i]} A \cong \text{End}_\Omega(M_i)$ .

DEFINITION. The Schur exponent  $m_R(\chi_i)$  is the exponent of  $A$  in  $B(R[\chi_i])$ .

This definition was prompted by the discussion at the end of [18].

PROPOSITION 1. *The Schur exponent  $m_R(\chi_i)$  divides the Schur index  $M_R(\chi_i)$ .*

*Proof.* Let  $S$  be a splitting ring for  $\chi_i$  in  $\Omega$  with  $M_R(\chi_i) = \text{Rank}_{R[\chi_i]}(S)$ . Write  $M_i = \Omega \otimes_S P_i$  for some finitely generated projective  $SG$ -module  $P_i$ . Let  $\phi: SG \rightarrow \text{End}_S(P_i)$  be the homomorphism given by the  $SG$ -module structure of  $P_i$ . If  $B = \phi(SG)$  then  $\Omega \otimes_S B = \text{End}_\Omega(\Omega \otimes P_i) = \text{End}_\Omega(M_i)$ . This implies  $B = \text{End}_S(P_i)$  so  $\phi$  is an epimorphism. Keeping the notation preceding Proposition 1, the restriction of  $\phi$  to  $S \otimes_{R[\chi_i]} A$  gives an epimorphism of  $S$ -Azumaya algebras which is a monomorphism on  $S$  and

therefore a monomorphism. Thus,  $S \otimes_{R[\chi_i]} A \cong \text{End}_S(P_i)$  and  $S$  is a splitting ring for  $A$ . By Theorem 2.5.5 of [6] there is an  $R[\chi_i]$ -algebra  $D$  equivalent to  $A$  in  $B(R[\chi_i])$  and containing  $S$  as a maximal commutative subalgebra. Thus,  $\text{Rank}_{R[\chi_i]}(D) = M_R(\chi_i)^2$ . By Theorem 3 of [19], the exponent of  $D$  in  $B(R[\chi_i])$  divides  $M_R(\chi_i)$ . Q.E.D.

We have not been able to find an example where  $m_R(\chi_i) \neq M_R(\chi_i)$ . The following remark may be of interest. Assume  $R$  is an integral domain whose quotient field  $K$  is an algebraic number field. With notation as above, let  $J = \{p \mid p \text{ is a finite rational prime and } \text{ind}_p(A) \neq 1\}$ , where  $\text{ind}_p(A)$  is the  $p$ -local index of  $A$  (see [14]). If  $k = m_R(\chi_i)$  then  $m_R(\chi_i) = M_R(\chi_i)$  whenever  $R(\sqrt[k]{\pm m})$  is a splitting ring for  $A$  (where the minus sign is chosen when  $\text{ind}_\infty(A_i) > 1$ ). As B. Fein pointed out to us, in the example presented in [10],  $R(\sqrt[k]{\pm m})$  may not always split  $A$ .

A class in  $B(R)$  is contained in the Schur subgroup  $\mathcal{S}(R)$  in case there is a representing Azumaya algebra  $A$  which is a homomorphic image of  $RG$  for some finite group  $G$ . Note that  $RG$  is not required to be separable over  $R$ . Information about  $\mathcal{S}(R)$  for commutative rings  $R$  is contained in [7, 8].

The group  $\text{Aut}(R)$  of automorphisms of  $R$  acts on  $B(R)$ . If  $\sigma \in \text{Aut}(R)$  and  $|A| \in B(R)$  then  $\sigma(|A|) = |A_\sigma|$ , where  $A_\sigma = A$  as a ring and the action of  $R$  on  $A_\sigma$  is given by  $r \cdot a = \sigma^{-1}(r)a$  for all  $r \in R, a \in A_\sigma$ . The formal properties of this action in the context of commutative rings can be found in [3]. A class  $[A] \in B(R)$  is contained in the uniform subgroup  $\mathcal{U}(R)$  in case: (see [11])

1. If the order of  $[A]$  in  $B(R)$  is  $n$  then the group of  $n$ th roots of unity in  $R$  is cyclic of order  $n$ .

2. If  $\varepsilon_n$  is a primitive  $n$ th root of unity in  $R$  and  $\sigma \in \text{Aut}(R)$  then  $\sigma(\varepsilon_n) = \varepsilon_n^t$  implies  $[A_\sigma] = [A]^t$ .

If  $S$  is a commutative  $R$ -algebra let  $B(R) \otimes S$  denote the natural image of  $B(R)$  in  $B(S)$ . The corresponding images of the subgroups  $\mathcal{S}(R)$  and  $\mathcal{U}(R)$  are denoted  $\mathcal{S}(R) \otimes S$  and  $\mathcal{U}(R) \otimes S$ , respectively.

LEMMA 2. *Let  $K$  be an algebraic number field and let  $q$  be a  $K$  prime above the rational prime  $q$ .*

(1)  $\mathcal{U}(K) \otimes K_q \subseteq \mathcal{U}(K_q)$ , where the inclusion may be proper when  $q > 3$ .

(2)  $\mathcal{U}(K_q)$  is the subgroup of  $B(K_q)$  of order  $q - 1$  if  $q > 2$  and of order 2 if  $q = 2$ .

(3)  $\mathcal{U}(K(\varepsilon_{q-1})) \otimes K_q = \mathcal{U}(K_q)$ .

*Proof.* (1) If  $|A| \in \mathcal{U}(K)$  with  $\exp |A| = m$  then  $\varepsilon_m \in K$ . If  $\exp |A \otimes K_q| = t$ , then  $t \mid m$  so  $\varepsilon_t \in K_q$ . It follows from [14, Theorem 1.1] that if  $q > 2$  then  $q \equiv 1 \pmod{t}$  and if  $q = 2$  then  $m = 1, 2$ . Therefore, if

$\sigma \in \text{Aut}(K_\rho)$  then  $\sigma(\varepsilon_i) = \varepsilon_i$ . The lemma on page 385 of [13] gives  $[A \otimes K_\rho] = [(A \otimes K_\rho)_\sigma]$  so  $[A \otimes K_\rho] \in \mathcal{U}(K_\rho)$ , proving the first part of (1). To see that the inclusion may be proper, observe that  $\mathcal{U}(\mathbf{Q})$  has exponent = 2, but if  $q$  is odd then  $\mathcal{U}(\mathbf{Q}_q)$  contains an element of order  $q - 1$  [23, Theorem 4.4, p. 45; 11, Lemma 3.1].

(2) If  $|A| \in \mathcal{U}(K_\rho)$  with  $\exp |A| = n$  and  $\sigma \in \text{Aut}(K_\rho)$  then  $\sigma(\varepsilon_n) = \varepsilon_n^b$  implies  $|A_\sigma| = |A|^b$ . As in (1),  $|A_\sigma| = |A|$  so  $b \equiv 1 \pmod{n}$  for all  $\sigma \in \text{Aut}(K_\rho)$ . Therefore,  $\varepsilon_n \in \mathbf{Q}_q$  and thus  $q \equiv 1 \pmod{n}$  or  $q = n = 2$ . It remains to check that  $\mathcal{U}(K_\rho)$  has an element of order  $q - 1$  when  $q$  is odd. From Theorem 1.5 of [14], there exists an element  $|A| \in \mathcal{U}(K(\varepsilon_{q-1}))$  with  $\text{ind}_q(A) = q - 1$ . Since  $\varepsilon_{q-1} \in K_\rho$ ,  $|A \otimes K_\rho(\varepsilon_{q-1})| = |A \otimes K_\rho|$ . From (1),  $|A \otimes K_\rho| \in \mathcal{U}(K_\rho)$  so  $\mathcal{U}(K_\rho)$  contains an element of order  $q - 1$ .

(3) We saw in (2) that  $\mathcal{U}(K(\varepsilon_{q-1})) \otimes K_\rho \subset \mathcal{U}(K_\rho)$ . If  $|A| \in \mathcal{U}(K_\rho)$  with  $\exp |A| = \rho$  then as in (2),  $q \equiv 1 \pmod{\rho}$  or  $q = \rho = 2$ . From [14] there is an element  $|D| \in \mathcal{U}(K(\varepsilon_{q-1}))$  with  $\text{ind}_q(D) = \rho$ . Replace  $|D|$  by an appropriate power if necessary, and get  $|D \otimes K_\rho(\varepsilon_{q-1})| = |D \otimes K_\rho| = |A|$ . Q.E.D.

The exponent of  $\mathcal{U}(K)$  for any algebraic number field  $K$  is the order of the group of roots of unity in  $K$ . Lemma 2(2) implies that this statement fails in local fields, for example, for  $\mathbf{Q}_q(\varepsilon_q)$  with  $q > 2$ .

For a positive integer  $n$  let  $C_n$  denote the cyclic group of order  $n$ .

**THEOREM 3.** *For each positive integer  $n$  there is a local field  $K_\rho$  such that  $\mathcal{U}(K_\rho)/\mathcal{S}(K_\rho) \cong C_n$ .*

*Proof.* Let  $n > 1$  and let  $q > 2$  be a prime with  $q \equiv 1 \pmod{n}$ . Let  $K$  be the subfield of  $\mathbf{Q}(\varepsilon_q, \varepsilon_{q-1})$  with  $|K: \mathbf{Q}(\varepsilon_{q-1})| = n$ . If  $\rho$  is a  $K$ -prime above  $q$  then Theorem 4.4 of [23] implies  $\mathcal{S}(K_\rho)$  is the subgroup of  $B(K_\rho)$  of order  $(q - 1)/n$ . By (2) of Lemma 2,  $\mathcal{U}(K_\rho)$  is the subgroup of  $B(K_\rho)$  of order  $q - 1$ . Since  $\mathcal{S}(K_\rho) \subset \mathcal{U}(K_\rho)$  [11], we have  $\mathcal{U}(K_\rho)/\mathcal{S}(K_\rho) \cong C_n$ . Q.E.D.

In [15, 16] algebraic number fields  $K$  were given with  $|\mathcal{U}(K): \mathcal{S}(K)| = \infty$ .

If  $R = \mathbf{Z}(\sqrt{2})$  then  $\mathcal{S}(R) = C_2 = \mathcal{U}(R)$  [7, 11]. Moreover,  $\mathcal{S}(R \oplus R) \cong C_2 \times C_2$ . However,  $\mathcal{U}(R \oplus R) = \{e\}$  since the group of square roots of unity in  $R \oplus R$  is not cyclic. Here  $\mathcal{S}(R \oplus R) \not\subset \mathcal{U}(R \oplus R)$ .

Observe that Lemma 2(1) holds when  $\mathcal{U}(-)$  is replaced by  $\mathcal{S}(-)$ . However, Lemma 2(2) holds for  $\mathcal{S}(-)$  if and only if the tame ramification index of  $q$  in  $K$  is 1 [23, Theorem 4.4, p. 45]. Lemma 2(3) also fails when  $\mathcal{U}(-)$  is replaced by  $\mathcal{S}(-)$ . To illustrate the latter let  $K = \mathbf{Q}(\sqrt[3]{3})$  and  $q = 5$ . Then  $K(\varepsilon_{q-1}) = \mathbf{Q}(\varepsilon_{12})$  and  $\mathbf{Q}_5(\varepsilon_{12}) = \mathbf{Q}_5(\sqrt[3]{3})$ . If  $\mathcal{S}(\mathbf{Q}_5(\sqrt[3]{3})) = \mathcal{S}(\mathbf{Q}(\varepsilon_{12})) \otimes \mathbf{Q}_5(\sqrt[3]{3})$  then  $\mathcal{S}(\mathbf{Q}(\varepsilon_{12}))$  would contain an element  $[A]$  with  $\text{ind}_5 A = 4$  [23, Theorem 4.4, p. 45]. We now show that this is not the case.

By Theorem 8.12 of [23],  $\mathcal{S}(\mathbf{Q}(\varepsilon_4)) \otimes \mathbf{Q}(\varepsilon_{12}) = \mathcal{S}(\mathbf{Q}(\varepsilon_{12}))$ . Thus,  $[A] = [B \otimes \mathbf{Q}(\varepsilon_{12})]$  with  $[B] \in \mathcal{S}(\mathbf{Q}(\varepsilon_4))$ , so  $\text{ind}_5 B \leq 4$ . Suppose that  $\varphi$  is a  $\mathbf{Q}(\varepsilon_4)$  prime above 5 and that  $\hat{\varphi}$  is a  $\mathbf{Q}(\varepsilon_{12})$  prime over  $\varphi$ . From [9] we have  $\text{inv}_{\hat{\varphi}} A = \text{inv}_{\hat{\varphi}} B \otimes \mathbf{Q}(\varepsilon_{12}) \equiv |\mathbf{Q}_5(\varepsilon_{12}) : \mathbf{Q}_5(\varepsilon_4)| \text{inv}_{\varphi} B = 2 \text{inv}_{\varphi} B \pmod{1}$ . Since  $\text{ind}_5 B \leq 4$  then  $\text{ind}_5 A \leq 2$ .

**PROPOSITION 4.** *If  $q$  has residue class degree 1 in  $K$ ,  $q \equiv 3 \pmod{4}$ , and  $q$  is a prime in the algebraic number field  $K$  lying over  $q$ , then  $\mathcal{S}(K(\varepsilon_{q-1})) \otimes K_{\mathcal{q}} = \mathcal{S}(K_{\mathcal{q}})$ .*

*Proof.* The hypothesis implies  $|K_{\mathcal{q}}(\varepsilon_{q-1})| = |K_{\mathcal{q}} : \mathbf{Q}_q| = c$ , the tame ramification index of  $q$  in  $K$ . From [23, Theorem 4.4],  $\mathcal{S}(K_{\mathcal{q}})$  is the subgroup of  $B(K_{\mathcal{q}})$  of order  $(q-1)/c$ . From Lemma 2(3) it is sufficient to show  $\mathcal{S}(\mathbf{Q}(\varepsilon_{(q-1)/2})) = \mathcal{U}(\mathbf{U}(\varepsilon_{(q-1)/2}))$ . Let  $(q-1)/2 = p_1^{a_1} \cdots p_r^{a_r}$  be the canonical prime factorization. From [14, Corollary 2.8],  $\mathcal{S}_{p_i}(\mathbf{Q}(\varepsilon_{p_i^{a_i}})) \otimes \mathbf{Q}(\varepsilon_{(q-1)/2}) = \mathcal{S}_{p_i}(\mathbf{Q}(\varepsilon_{(q-1)/2})) = \mathcal{U}_{p_i}(\mathbf{Q}(\varepsilon_{(q-1)/2}))$  for  $i = 1, \dots, r$ . Q.E.D.

The following examples show each of the hypotheses of Proposition 4 is necessary and that the converse of Proposition 4 may fail.

To show the necessity of the hypothesis  $q \equiv 3 \pmod{4}$  we consider  $\mathcal{S}(\mathbf{Q}(\sqrt{15})) = \mathcal{S}(\mathbf{Q}) \otimes \mathbf{Q}(\sqrt{15})$ . Thus,  $\mathcal{S}(\mathbf{Q}(\sqrt{15})) \otimes \mathbf{Q}_5(\sqrt{15})$  is trivial but  $\mathcal{S}(\mathbf{Q}_3(\sqrt{15}))$  has order 2. Also observe that  $|\mathcal{U}(\mathbf{Q}(\sqrt{15})) : \mathcal{S}(\mathbf{Q}(\sqrt{15}))| = \infty$ , (see [16]).

To see that the hypothesis  $q$  has residue class degree 1 in  $K$  it is necessary we consider  $\mathcal{S}(\mathbf{Q}(\sqrt{11})) = \mathcal{S}(\mathbf{Q}) \otimes \mathbf{Q}(\sqrt{11})$ . Thus  $\mathcal{S}(\mathbf{Q}(\sqrt{11})) \otimes \mathbf{Q}_3(\sqrt{11})$  is trivial, but  $\mathcal{S}(\mathbf{Q}_3(\sqrt{11}))$  has order 2.

Finally, we show that the converse of Proposition 4 may fail.  $\mathcal{U}(\mathbf{Q}(\sqrt{5})) = \mathcal{S}(\mathbf{Q}(\sqrt{5}))$  so Lemma 2(3) implies  $\mathcal{S}(\mathbf{Q}(\sqrt{5})) \otimes \mathbf{Q}_3(\sqrt{5}) = \mathcal{S}(\mathbf{Q}_3(\sqrt{5})) = \mathcal{U}(\mathbf{Q}_3(\sqrt{5}))$ . However, the residue class degree of 3 in  $\mathbf{Q}(\sqrt{5})$  is 2.

Suppose  $K$  is an imaginary abelian number field with maximal real subfield  $M$ . The elements of order 2 in  $\mathcal{S}(K)$  are of the form  $[C \otimes_M K]$ , where  $[C]$  has order 2 in  $B(M)$  [23, p. 132]. We can make a little more precise statement. First note that  $\mathbf{Q}(\varepsilon_n) = \mathbf{Q}(\varepsilon_{n/2})$  whenever  $n \equiv 2 \pmod{4}$ .

**THEOREM 5.** *Assume  $n \not\equiv 2 \pmod{4}$ . Let  $K = \mathbf{Q}(\varepsilon_n)$  and  $M = \mathbf{Q}(\varepsilon_n + \varepsilon_n^{-1})$ . If  $[D]$  has order 2 in  $\mathcal{S}(K)$  then  $[D] = [C \otimes_M K]$ , where  $[C]$  has order 2 in  $\mathcal{U}(M)$ .*

*Proof.* When  $n$  is odd or a power of 2 all elements in  $\mathcal{S}(K)$  of order 2 are of the form  $[C \otimes_M K]$ , where  $[C]$  has order 2 in  $\mathcal{S}(M) \subseteq \mathcal{U}(M)$  [17, Theorem 2.6]. Assume  $n = 2^a h$ , where  $a > 1$  and  $h > 1$ ,  $h$  odd. Let  $[D]$  have order 2 in  $\mathcal{S}(K)$  and let  $T = \{q | q \text{ is a rational prime and } \text{ind}_q(D) > 1\}$ . Let

$q$  be a rational prime. Check first that if  $q|n$  then  $q \notin T$ . We have  $[D] = [A \otimes K]$ , where  $[A] \in \mathcal{S}(\mathbf{Q}(\varepsilon_{2^a}))$  [23, Theorem 8.12]. If  $q \neq 2$  and  $|q-1|_2 = 2^c$  then  $\text{ind}_q(A) \leq \min\{2^a, 2^c\}$  [23, Lemma 8.5 and Theorem 8.6]. Since  $q|n$ ,  $|K_\varphi : \mathbf{Q}_q(\varepsilon_{2^a})|_2 \geq 2^c$ , where  $\varphi$  is a  $K$  prime above  $q$ . But  $\text{inv}_\varphi(A \otimes K) \equiv |K_\varphi : \mathbf{Q}_q(\varepsilon_{2^a})| \text{inv}_{\bar{\varphi}}(A) \pmod{1}$  (where  $\bar{\varphi}$  is a  $\mathbf{Q}((\varepsilon_{2^a}))$  prime below  $\varphi$ ) (see [9]). Hence  $\text{ind}_q(D) = 1$  and  $q \notin T$ . If  $q = 2$  then  $\text{ind}_q(A) = 1$  [23, Theorem 8.6].

Now let  $S$  be the set of primes in  $T$  which have an odd number of  $M$  primes above them. Check next that if  $S \neq \emptyset$  then  $n = 4p^c$ , where  $p$  is a prime,  $p \equiv 3 \pmod{4}$ . Let  $n = 2^a p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ , where the  $p_i$  are distinct odd primes and  $a_i > 0$  ( $1 \leq i \leq r$ ) and arrange the  $p_i$ 's such that  $|p_i - 1|_2 = 2^{b_i}$  with  $b_i \geq b_{i+1}$  ( $1 \leq i \leq r-1$ ). If  $q \in S$  then  $q \nmid n$  so  $|f_q|_2 = |M : \mathbf{Q}|_2$ , where  $f_q$  is the inertial degree of  $q$  in  $M$  over  $\mathbf{Q}$ . Therefore  $|f_q|_2 = 2^{a-2} 2^{b_1 + \cdots + b_r}$ . Since the Frobenius automorphism generates a cyclic group,  $|f_q|_2 \leq \max\{2^{a-2}, 2^{b_1} \cdots 2^{b_r}\} = \max\{2^{a-2}, 2^{b_1}\}$ . Thus  $n = 4p^{a_1}$ . Now  $[D] = [A \otimes K]$  with  $[A] \in \mathcal{S}(\mathbf{Q}(\varepsilon_4))$  [23, Theorem 8.12] so  $\text{ind}_q(A) \leq 4$ . If  $|M : \mathbf{Q}|_2 \geq 4$  then  $\text{ind}_q(A \otimes K) = 1$ . Since  $q \in T$ ,  $|M : \mathbf{Q}|_2 = 2$ . Thus  $b_1 = 1$  so  $p \equiv 3 \pmod{4}$ .

To complete the proof of the theorem first assume  $|S|$  is odd. Define  $[C] \in B(M)$  by  $\text{inv}_\varphi(C) = \frac{1}{2}$  at all  $M$  primes  $\varphi$  above the primes in  $T$ , and  $\text{inv}_{\not\varphi}(C) = \frac{1}{2}$  at the unique  $M$  prime  $\not\varphi$  above  $p$  ( $p$  cannot split in  $K$  since  $n = 4p^c$  with  $p \equiv 3 \pmod{4}$ ). The class  $[C]$  with these invariants is a well-defined element of  $B(M)$  and since  $\mathcal{U}(M)$  corresponds to the group of algebras with uniformly distributed invariants,  $[C] \in \mathcal{U}(M)$ . Since  $n = 4p^c$  with  $p \equiv 3 \pmod{4}$ ,  $|\mathbf{Q}_p(\varepsilon_n) : \mathbf{Q}_p|_2 = |\mathbf{Q}(\varepsilon_n) : \mathbf{Q}|_2 = 4$ . Thus,  $\text{ind}_p(C \otimes K) = 1$ . If  $q \in T$  then  $|\mathbf{Q}_q(\varepsilon_n) : M_q| = 1$ , where  $q$  is an  $M$  prime above  $q$  [23, p. 132]. Hence,  $\text{ind}_q(C \otimes K) = 2$  at precisely the  $q \in T$ . Thus, the Hasse invariants of  $[D]$  and  $[C \otimes K]$  are the same so  $[D] = [C \otimes K]$ . If  $S = \emptyset$  or  $|S|$  is even define  $[C] \in B(M)$  by  $\text{inv}_\varphi(C) = \frac{1}{2}$  at all the  $M$  primes  $\varphi$  above the primes  $q \in T$ . As above,  $[D] = [C \otimes K]$ , completing the proof of the theorem.

Q.E.D.

*Remark 1.* With the hypothesis of Theorem 5, if  $[C]$  has order 2 in  $\mathcal{U}(M)$  it may not be the case that  $[K \otimes C] \in \mathcal{S}(K)$ . Let  $K = \mathbf{Q}(\varepsilon_{12})$ , then  $M = \mathbf{Q}(\sqrt{3})$ . Define  $[C] \in B(M)$  by  $\text{inv}_{\not\varphi}(C) = \frac{1}{2} = \text{inv}_\varphi(C)$ , where  $\not\varphi$  is the  $M$  prime above 7 and  $\varphi$  is the  $M$  prime above 2, and  $\text{inv}_R(C) = 0$  for all  $R \neq \not\varphi, \varphi$ . Then  $[C] \in \mathcal{U}(M)$ . If  $[D] = [C \otimes K] \in \mathcal{S}(K)$  then  $[D] = [A \otimes K]$  with  $[A] \in \mathcal{S}(\mathbf{Q}(\varepsilon_4))$  [23, Theorem 8.12, p. 140]. Since  $\text{ind}_7(D) = 2$  and  $\text{ind}_p(D) = 1$  for all  $p \neq 7$  then  $\text{ind}_7(A) = 2$ . This is impossible by [23, Theorem 8.6, p. 136].

*Remark 2.* With the hypothesis of Theorem 5, if  $n > 1$  it is never the case that all elements of order 2 in  $\mathcal{U}(K)$  are induced from elements of  $\mathcal{U}(M)$  [14, Theorem 2.6].

EXAMPLE. Let  $k$  be a perfect field and  $t$  an indeterminate. In [4] it was shown that  $B(k[t, t^{-1}]) = B(k) \oplus \hat{G}$ , where  $G$  is the Galois group of  $k$  and  $\hat{G} = \text{Hom}(G, Q/Z)$  is its dual. In the last paragraph on page 334 of [3] the action of  $\text{Aut}(k[t, t^{-1}])$  on  $B(k[t, t^{-1}]) = H^2_{\text{Gal}}(k[t, t^{-1}], U)$  is given explicitly on the cocycle level. If  $\sigma \in \text{Aut}(k[t, t^{-1}])$  it is easy to check that  $\sigma|_k \in \text{Aut}(k)$  and  $\sigma(t) = \beta t^\varepsilon$ , where  $\beta \in \text{Units}(k)$  and  $\varepsilon = \pm 1$ . For a 2 cocycle corresponding to an element in  $B(k)$  the action of  $\sigma$  corresponds to the action of  $\sigma|_k$  on  $B(k)$ . Let  $\bar{\sigma}$  be an extension of  $\sigma|_k$  to the separable closure  $\Omega$  of  $k$ . For a cocycle corresponding to an element  $f \in \hat{G}$  one can check that the action of  $\sigma$  on  $f$  is  $\sigma \cdot f(x) = \varepsilon f(\bar{\sigma}^{-1}x\bar{\sigma})$ . By choosing  $\sigma|_k = \text{id}_k$  and  $\sigma(t) = t^{-1}$  it follows that any element of odd order in  $\mathcal{U}(k[t, t^{-1}])$  is in  $\mathcal{U}(k)$ . If  $\text{char } k = 2$  then  $-1 = 1$  so every element in  $\mathcal{U}(k[t, t^{-1}])$  has odd order and  $\mathcal{U}(k[t, t^{-1}]) = \mathcal{U}(k)$ . If  $\text{char } k \neq 2$  then  $-1 \neq 1$  and  $\sigma(-1) = -1$  for all  $\sigma \in \text{Aut}(k[t, t^{-1}])$  so in this case  $\mathcal{U}(k[t, t^{-1}]) = \mathcal{U}(k) \oplus H$ , where if  $\hat{G}_2 = \{f \in \hat{G} \mid 2f = 0\}$  and  $\mathcal{G} = \text{Aut}(k[t, t^{-1}])$  then  $H = \hat{G}_2^{\mathcal{G}}$ . If  $k$  is the field with  $p^m$  elements ( $p$  an odd prime) or a  $p$ -adic field then  $\hat{G}_2 = Z/2$  so  $\hat{G}^{\mathcal{G}} = \hat{G}_2 = Z/2$  and  $\mathcal{U}(k[t, t^{-1}]) \cong \mathcal{U}(k) \oplus Z/2$ . Summarizing

$$\begin{aligned} \mathcal{U}(k[t, t^{-1}]) &= \mathcal{U}(k) && \text{if char } k = 2, \\ \mathcal{U}(k[t, t^{-1}]) &= Z/2 && \text{if } k \text{ is finite of odd characteristic,} \\ \mathcal{U}(k[t, t^{-1}]) &= Z/2 && k = \mathbb{R} \text{ (see also the next example),} \\ \mathcal{U}(k[t, t^{-1}]) &= Z_{p-1} \oplus Z/2 && k \text{ a } p\text{-adic field, } p \text{ odd,} \\ \mathcal{U}(k[t, t^{-1}]) &= Z/2 \oplus Z/2 && k \text{ a 2-adic field.} \end{aligned}$$

We conjecture that if  $\mathcal{U}(R) \neq 0$  then  $\mathcal{U}(R)$  contains an element of order 2.

EXAMPLE. Let  $p(x) \in \mathbb{R}[x]$  with  $p(x)$  square free of degree  $2n + 1$  and with  $2n + 1$  real roots. Let  $R = \mathbb{R}[x, y]/(y^2 - p(x))$ . Then  $R$  is the coordinate ring of a nonsingular real curve with  $n + 1$  real components (in the Euclidean topology). Let  $\sigma \in \text{Aut}(R)$  be given by  $\sigma(x) = x$ ,  $\sigma(y) = -y$ , and let  $N: R \rightarrow R$  by  $N(\alpha) = \alpha\sigma(\alpha)$ . If  $u \in \text{Units}(R)$  then  $N(u)$  is a unit. After checking that  $N(u) \in \mathbb{R}[x]$  for any  $u \in \mathbb{R}$  one can check  $\text{Units}(R) = \text{Units}(\mathbb{R})$ . Thus,  $\text{Aut}(R) = \text{Aut}_{\mathbb{R}}(R)$ . Following the exposition on page 276 of [12], by choosing the roots of  $f(x)$  in general position,  $\text{Aut}_{\mathbb{R}}(R) = C_2$ . It follows that the  $n + 1$  real components of  $\text{Spec}(R)$  are not permuted by any element in  $\text{Aut}(R)$ . The description of Azumaya algebras  $A$  over real curves given in [4] or [5] makes it clear that for any  $\tau \in \text{Aut}(R)$ ,  $[A] = [A_\tau]$  so  $\mathcal{U}(R) = B(R) = (C_2)^{(n+1)}$ . On the other hand,  $\mathcal{S}(R) = C_2$  in this case.

We conclude with an example where both  $\mathcal{S}(R) \not\subseteq \mathcal{U}(R)$  and  $\mathcal{U}(R) \not\subseteq \mathcal{S}(R)$ . This example arose in a conversation with G. Greenfield.

EXAMPLE 3. Let  $q_i = 1 + 2p_i$  for  $i = 1, 2$ , where  $p_1, p_2, q_1$ , and  $q_2$  are distinct odd primes. Let  $K^{(i)} = \mathbf{Q}(\varepsilon_{q_i} + \varepsilon_{q_i}^{-1}, \varepsilon_{p_i})$ , and let  $\varphi_i$  be a  $K^{(i)}$  prime above  $q_i$ . Set  $R = K_{\varphi_1}^{(1)} \oplus K_{\varphi_2}^{(2)}$ . By (2) of Lemma 2,  $\mathcal{U}(K_{\varphi_i}^{(i)})$  has order  $2p_i$ , whence  $\mathcal{U}(R)$  has an element of order  $p_i$  for  $i = 1, 2$ . (However,  $\mathcal{U}(R)$  does not have an element of order 2.) On the other hand,  $\mathcal{S}(R) \cong \mathcal{S}(K_{\varphi_1}^{(1)}) \oplus \mathcal{S}(K_{\varphi_2}^{(2)})$ , where  $\mathcal{S}(K_{\varphi_i}^{(i)})$  has order 2 for  $i = 1, 2$  [23, Theorem 4.4].

## REFERENCES

1. M. AUSLANDER AND O. GOLDMAN, The Brauer group of a commutative ring, *Trans. Amer. Math. Soc.* **97** (1960), 367–409.
2. C. W. CURTIS AND I. REINER, “Representation Theory of Finite Groups and Associative Algebras,” Interscience, London/New York, 1962.
3. F. R. DEMEYER, An action of the automorphism group of a commutative ring on its Brauer group, *Pacific J. Math.* **97** (1981), 327–338.
4. F. R. DEMEYER, The Brauer group of affine curves, in “Brauer Groups (Evanston 1975),” Lecture Notes in Mathematics, Vol. 549, pp. 16–24, Springer-Verlag, New York/Berlin, 1975.
5. F. R. DEMEYER AND M. A. KNUS, The Brauer group of a real curve, *Proc. Amer. Math. Soc.* **57** (1976), 227–323.
6. F. R. DEMEYER AND E. INGRAHAM, Separable algebras over commutative rings, in “Lecture Notes in Mathematics, Vol. 181,” Springer-Verlag, Berlin/New York, 171.
7. F. R. DEMEYER AND R. A. MOLLIN, The Schur group, in “Lecture Notes in Mathematics, Vol. 1142,” pp. 205–210, Springer-Verlag, Berlin/New York, 1985.
8. F. R. DEMEYER AND R. A. MOLLIN, The Schur group of a commutative ring, *J. Pure Appl. Algebra* **35** (1985), 117–122.
9. M. DEURING, “Algebren,” Springer-Verlag, Berlin, 1935.
10. B. FEIN, Minimal splitting fields for group representations, *Pacific J. Math.* **51** (1974), 427–431.
11. G. R. GREENFIELD AND R. A. MOLLIN, The uniform distribution group of a commutative ring, *J. Algebra* **108** (1987), 179–187.
12. P. GRIFFITHS AND J. HARRIS, “Principles of Algebraic Geometry,” Wiley-Interscience, New York, 1978.
13. G. J. JANUSZ, Automorphism groups of simple algebras and group algebras, in “Proceedings, Philadelphia Conference on Ring Theory,” Lecture Notes in Pure and Applied Mathematics, Vol. 37, pp. 381–388, Dekker, New York, 1978.
14. R. A. MOLLIN, Algebras with uniformly distributed Hasse invariants, *J. Algebra* **44** (1977), 271–282.
15. R. A. MOLLIN, Uniform distribution and the Schur subgroup, *J. Algebra* **42** (1976), 261–277.
16. R. A. MOLIN, Uniform distribution and real fields, *J. Algebra* **43** (1976), 155–167.
17. R. A. MOLLIN, Induced  $p$ -elements in the Schur group, *Pacific J. Math.* **90** (1980), 169–176.
18. R. A. MOLLIN, More on the Schur group of a commutative ring, *Int. J. Math. Math. Sci.* **8** (1985), 275–282.
19. D. SALTMAN, The Brauer group is torsion, *Proc. Amer. Math. Soc.*, (1981), 385–387.

20. G. SZETO, "On the Brauer Splitting Theorem," Ph.D. dissertation, Purdue University, 1968.
21. G. SZETO, The group character and split group algebras, *Pacific J. Math.* **34** (1970), 183–191.
22. G. SZETO, On the Brauer splitting theorem, *Pacific J. Math.*, (1969), 505–512.
23. T. YAMADA, The Schur subgroup of the Brauer group, in "Lecture Notes in Mathematics, Vol. 397," Springer-Verlag, Berlin/New York, 1974.