Can. J. Math., Vol. XXXIII, No. 6, 1981, pp. 1370–1379

INDUCED QUATERNION ALGEBRAS IN THE SCHUR GROUP

RICHARD A. MOLLIN

Let K be a finite, imaginary and abelian extension of the rational number field $\mathbf{Q}$, and let M be the maximal real subfield of K. It is well known that each element of order 2 in $S(K)$, the Schur group of K, is induced from an element of order 2 in $B(M)$, the Brauer group of M; i.e., if D is a quaternion division algebra central over K such that its class $[D]$ in $B(K)$ is in fact in $S(K)$ then $[D] = [B \otimes_M K]$ where B is a quaternion division algebra with $[B] \in B(M)$. A natural question to ask is: "When is every element of $S(K)$ of order 2 induced from $S(M)$?" The main result of this paper is to provide necessary and sufficient conditions for this to occur when $G(L/K)$, the Galois group of L over K, is cyclic where L is the smallest root of unity field containing K. Moreover we provide necessary conditions, as well as a conjecture, for the general case.

1. Notation and preliminaries. For a field of characteristic zero the Schur group $S(K)$ may be described as consisting of those equivalence classes in $B(K)$ which contain a simple component of the group algebra KG for some finite group G. If $[A] \in S(K)$ and $\mathscr{P}$ and $\mathscr{Q}$ are K-primes above the rational prime p, then $A \otimes_K K_{\mathscr{P}}$ and $A \otimes_K K_{\mathscr{Q}}$ have the same index where $K_{\mathscr{P}}$ denotes the completion of K at $\mathscr{P}$ (see [**2**] or [**10**]). We call the common value of the indices of $A \otimes_K K_{\mathscr{P}}$ for all K-primes $\mathscr{P}$ above p, the *p-local index* of A and denote it by $\mathrm{ind}_p A$. Henceforth when we write a tensor product it shall be assumed to be taken over the center of the algebra in the left factor. For basic results pertaining to $S(K)$ the reader is referred to [**10**]. The symbol $\sim$ denotes equivalence in the Brauer group. If $\mathscr{Q}$ is an F-prime above q then any reference to the decomposition of $\mathscr{Q}$ in K/F (abelian) shall be described as the decomposition of q in K/F since the decomposition essentially depends on q and not on $\mathscr{Q}$. For example if $\mathscr{Q}$ is unramified in K/F we say q is unramified in K/F. Also for each rational prime q, we select a fixed prime $\mathscr{Q}$ of F over q. We shall write F_q to mean the completion of F at $\mathscr{Q}$. Similarly we fix a prime $\hat{\mathscr{Q}}$ of K above $\mathscr{Q}$ and simply write K_q for $K_{\hat{\mathscr{Q}}}$. The Frobenius automorphism of q in K/F shall be denoted $\mathscr{F}(q, K/F)$, and a generator of the inertia group of q in K/F, if it exists,

Received June 3, 1980.

shall be denoted $\theta(q, K/F)$. The order of $\mathscr{F}(q, K/F)$ will be denoted $f(q, K/F)$ and the order of $\theta(q, K/F)$ will be denoted $e(q, K/F)$.

If m is an integer and $m = p^a t$ where p and t are relatively prime then we shall use the symbol $|m|_p = p^a$ to denote the highest power of p dividing m. Finally ϵ_n will denote a primitive nth root of unity.

The results of this paper continue work begun in [**3**]–[**6**]. The author welcomes this opportunity to thank N.S.E.R.C. Canada for their support of this research, via University Research Fellowship U 0077.

2. Preliminary results: A correction. We shall need a determination of the maximum q-local index of elements in $S(K)_2$. The case where ϵ_4 is in K has been covered by Janusz [**1**]. The case where ϵ_4 is not in K for the general case has been treated by Pendergrass [**7**]. However there are certain errors in the latter work which have been corrected by Pendergrass in a correspondence with the author. With his permission we present corrected versions of the results. Since the list of notation is enormous we do not provide it here, but rather refer the reader to [**7**]. We list the corrections by page and line number in reference to [**7**].

The following corrects [**7**, Lemma 1.1, p. 424].

LEMMA 2.1. *There are two possible forms for* G/C:

(1) $G/C = \langle \sigma' \rangle$ *where* $\sigma'(\zeta) = \zeta^{2^r-1}$ *for* r *where* $0 < r < s$.

(2) $G/C = \langle \rho' \rangle \times \langle \sigma' \rangle$ *where* $\rho'(\zeta) = \zeta^{-1}$ *and* $\sigma'(\zeta) = \zeta^{2^r+1}$ *for some* r *where* $0 < r \leqq s$.

Proof.

Page 424, line 1: We shall treat these two cases separately. First suppose that G/C is of form (1). Page 427, line 8: Now assume that G/C is of form (2).

Page 430, line 1: If G/C is of form (1) then ....
line 3: $\sigma(\zeta) = \zeta^{2^r-1}$ for some integer r, with $0 < r < s$;
line 6: $\phi = \sigma^{a(p)}\xi_p$, where ξ_p is in C and $0 \leqq a(p) < 2^t$;
line 12: If G/C is of form (2) then
line 15: $\sigma(\zeta) = \zeta^{2^r+1}$ for some integer r where $0 < r \leqq s$.
line 18: $\phi = \rho^{a'(p)}\sigma^{a(p)}\xi_p$, where ξ_p is in C, $0 \leqq a'(p) < 2$, and $0 \leqq a(p) < 2^t$.
line 19: $V(x) = ((2^r+1)^x - 1)/2^r$ for any integer x.

The following result is a correction of [**7**, Theorem 2.2, p. 430]. Although we do not directly use this theorem we present it with corrected proof because the subsequent theorem which we do use depends on it.

THEOREM 2.2. *Let* α *be a factor set on* G *with values in* W, *and let* ψ *be the skew pairing from* $C \times C$ *into* $\{-1, 1\}$ *determined by* α. *Then*

$$\Phi_p(\alpha) = \psi(\Theta(p), \eta(p))\mu_p(\alpha),$$

where $\mu_p(\alpha)$ *is a root of unity of order dividing* $2^{\nu(p)}$ *unless:*

(i) *G/C is of form* (2)
(ii) $p^{f(p)} \not\equiv (-1)^{a'(p)} \bmod 2^{r+1}$
(iii) *Θ is not a square in C.*
In this special case, $\mu_p(\alpha) \in \{-1, 1\}$. As α runs through all factor sets with values in W which determine ψ, the element $\mu_p(\alpha)$ runs through all of its possible values.

Proof.
Page 431, line 13: Step 1. When G/C is of form (1),

$$\Phi_p(\alpha) = \psi(\Theta, \eta)\mu_p(\alpha).$$

Page 432, line 9: Step 2. When G/C is of form (2),

$$\Phi_p(\alpha) = \psi(\Theta, \eta)\mu_p(\alpha).$$

line 23: Hence $(\Gamma + a'(p)) \equiv 0 \bmod 2^{r-1}$.

Page 433, line 1: Where $\mu \in \{-1, 1\}$ and $\mu = 1$ whenever $t_i(\Gamma + a'(p)) \equiv 0 \bmod 2^r$ for each i. Thus $\mu_p(\alpha) = \mu * \mu$ is a $2^{\nu(p)}$th root of unity unless

$$p^{f(p)} \not\equiv (-1)^{a'p} \bmod 2^{r+1}$$

and Θ is not a square in C, in which case $\mu_p(\alpha) \in \{-1, 1\}$.

line 5: Step 3. Each of the possible values of $\mu_p(\alpha)$ occurs for some factor set α which determines ψ.

Page 433, line 7: First suppose that we are in the special case. Let j be such that $|\tau_j|$ is even and t_j is odd. If $t = 0$ pick $Y = 1$ and replace γ_j by $\zeta\gamma_j$ and ϵ_j by $\zeta^{-|\tau_j|/2}\epsilon_j$. Then $N7$, $N8$ and $N9$ are satisfied, equation (2) is changed merely by multiplying both sides by $\zeta^{((p^{f(p)}-1)/2)(-t_j)}$, and $(\pi\gamma_i^{-t_i})^{\Gamma+a'(p)}$ has been changed to $-(\pi\gamma_i^{-t_i})^{\Gamma(3)+a'(p)}$. Hence ψ, μ_0, and μ_1 are unchanged while μ has been changed to $-\mu$. If $t \neq 0$, then replace β_j by $-\beta_j$, thus changing μ to $-\mu$ without altering ψ, μ_0 or μ_1.

Now suppose that we are not in the special case. If $h \neq g$, then $\nu(p) = 0$ so $\mu_p(\alpha)$ can only have the value 1. So assume that $h \neq g$. Let j be such that $|\tau_j| = e(p)t_j$. Then $T_j = (p^{f(p)} - 1)/e(p)$ is odd. Switch ϵ_j to $-\epsilon_j$ and observe that this leaves ψ unaltered. However, from equations (1) and (2) and the fact that $\mu = 1$, we find that μ_p has been changed to $-\mu_p$.

This completes the proof of the theorem.

In view of the above changes we get the following correction of [**7**, Theorem 2.3, p. 433].

THEOREM 2.3. (A) *If G/C is of form* (2) *and p is a prime such that* $p^{f(p)} \not\equiv (-1)^{a'(p)} \pmod{2^{r+1}}$ *and θ is not a square in C, then there exists an element in $S(K)_2$ with p-local index* 2.

The crossed product algebra $B(p, \alpha) = (L(\epsilon_p)/K, \alpha)$ where α determines the trivial skew pairing but makes $\mu_p(\alpha) = -1$ has p-local index 2.

(B) *If p is not covered under* (A) *and p does not divide n then the maximum p-local index of an element is $S(K)_2$ is* $\max \{2^{\nu(p)}, N(p)\}$.

The cyclic algebra $D(p) = (K(\epsilon_p), \tau, -1)$ where $\langle \tau \rangle = G(K(\epsilon_p)/K)$ has p-local index $2^{\nu(p)}$ and l-local index 1 *for all primes $l \neq p$.*

The crossed product algebra $B(p, \alpha) = (L(\epsilon_p)/K, \alpha)$ has p-local index $N(p)$ if the skew pairing ψ associated with α is such that $\psi(\theta(p), \eta(p))$ has order $N(p)$ and $\mu_p(a)$ has order less than $N(p)$.

(C) *If p is not covered by* (A) *and p does divide n, then the maximum p-local index of an element in $S(K)_2$ is*

$$\max \{2^{\nu(p)}, N_1(p), N_2(P)\}.$$

The cyclic algebra $D(p) = (K(\epsilon_p), \theta, -1)$ has p-local index $2^{\nu(p)}$ and l-local index 1 *for all primes $l \neq p$.*

The crossed product algebra $A(\alpha) = (L/K, \alpha)$ made with a factor set α on $G(L/K)$ having values in W, has p-local index $N_1(p)$ if the pairing ψ associated with α has the property that $\psi(\theta, \sigma^{-2^t x(p)} \xi_p)$ has order $N_1(p)$ and $\mu_p(\alpha)$ has order less than $N_1(p)$.

The crossed product $B(p, q, \alpha) = (L(\epsilon_q)/K, \alpha)$ has p-local index $N_2(p)$ if

(1) *α is a factor set on G with values in W and the pairing ψ associated with α satisfies the conditions:*

(a) *$\psi(\tau, \gamma) = 1$ for $\tau, \gamma \in C \cap G(L/K)$;*

(b) *$\psi(\theta, \tau^{f(p)})$ has order $N_2(p)$ where $\langle \tau \rangle = G(L(\epsilon_q)/L)$;*

(c) *$\mu_p(\alpha)$ has order less than $N_2(p)$;*

and:

(2) *q is an odd prime such that p is not a square modulo q.*

The major change of [**7**, Theorem 2.3, p. 433] is Theorem 2.3 (A) above, which is the only part of the theorem that we will use in this paper. Relevant comments pertaining to Theorem 2.3 (C) will be made at the end of the paper.

3. Maximal real subfields. Let K/Q be finite imaginary and abelian and let M denote the maximal real subfield of K. Furthermore, let $L = \mathbf{Q}(\epsilon_n)$ be the smallest root of unity field containing K. We may assume without loss of generality that $n \not\equiv 2 \pmod 4$ since $\mathbf{Q}(\epsilon_{2m}) = \mathbf{Q}(\epsilon_m)$ when m is odd. We let $\mathbf{Q}(\epsilon_{2^r})$ be the largest 2-power root of unity field in K with $r \neq 1$, and set

$$n = 2^s h = 2^{r+b} h = 2^{r+b} p_1^{a_1} \dots . p_t^{a_t}$$

https://doi.org/10.4153/CJM-1981-106-5 Published online by Cambridge University Press

where the p_i are distinct odd primes. Finally let:

$$G(L/\mathbf{Q}) = \langle \rho^u \rangle \times \langle \psi^v \rangle \times \langle \phi_1 \rangle \times \ldots \times \langle \phi_t \rangle$$

where $u, v \in \{0, 1\}$ and;

$$\rho: \epsilon_{2^s} \to \epsilon_{2^s}^{-1};\ \psi: \epsilon_{2^s} \to \epsilon_{2^s}^{5};$$

$$\rho: \epsilon_h \to \epsilon_h;\ \psi: \epsilon_h \to \epsilon_h;$$

$$\phi_i: \epsilon_{p_i^{a_i}} \to \epsilon_{p_i^{a_i}}^{r_i} \text{ and } \phi_i: \epsilon_{n/p_i^{a_i}} \to \epsilon_{n/p_i^{a_i}}$$

where r_i is a primitive root modulo p_i and $\phi_i^{h_i} \equiv 1$ where

$$h_i = p_i^{a_i - 1}(p_i - 1) \text{ for } 1 \leqq i \leqq t.$$

The above notation will be maintained for the rest of the paper.

Now we present for the first time necessary conditions for each element of order 2 in $S(K)$ to be induced from $S(M)$.

THEOREM 3.1. *If each element of order* 2 *in* $S(K)$ *is induced from* $S(M)$ *then either*

(a) ϵ_4 *is not in* K, *or*

(b) ϵ_4 *is in* K *and either*

(i) $|K : \mathbf{Q}(\epsilon_{2^r})|_2 = 1$ *or*

(ii) *when* $h > 1$ *then* $\phi_i^{h_i/2} \in G(L/K)$ *for all* $i = 1, 2, \ldots, t$.

Proof. We prove the contrapositive. Assume ϵ_4 is in K, $|K: \mathbf{Q}(\epsilon_{2^r})|_2 > 1$ and when $h > 1$ then $\phi_i^{h_i/2} \notin G(L/K)$ for some i. If $h = 1$ then $K = \mathbf{Q}(\epsilon_{2^r})$ is forced. This contradicts the assumption $|K: Q(\epsilon_{2^r})|_2 > 1$. Therefore $h > 1$, and we let $\gamma = \phi_i^{h_i/2} \notin G(L/K)$. Since γ corresponds to the Frobenius automorphism of infinitely many primes in $L/\mathbf{Q}$, we shall let q be such a prime. By the choice of q we have $q \equiv 1 \pmod{2^s}$. Therefore, by [**10**, Theorem 8.6, p. 136] there exists $[A] \in S(\mathbf{Q}(\epsilon_{2^r}))$ with $\text{ind}_q A = 2^r$. Set $[B] = [A]^{2^{r-2}}$. By the choice of q we have $[B \otimes K] \in S(K)$ with $\text{ind}_q B \otimes K = 2$. Assume there exists $[C] \in S(M)$ with $\text{ind}_q C = 2$. Therefore $[C \otimes Q(\epsilon_n + \epsilon_n^{-1})]$ is in $S(\mathbf{Q}(\epsilon_n + \epsilon_n^{-1}))$ and has q-local index 2. By [**10**, Theorem 7.16, p. 131] such an element cannot exist. This contradiction yields the theorem.

Now we show that restricting $G = G(L/K)$ to being cyclic forces the conditions of Theorem 3.1 to become necessary and sufficient.

THEOREM 3.2. *Assume* G *is cyclic. Each element of order* 2 *in* $S(K)$ *is induced from* $S(M)$ *if and only if either:*

(a) ϵ_4 *is not in* K *or*

(b) ϵ_4 *is in* K *and either*

(i) $|K: \mathbf{Q}(\epsilon_{2^r})|_2 = 1$ *or*

(ii) $t = 1$ *and* $\phi_1^{h_1/2} \in G$.

Proof. Necessity is a special case of Theorem 3.1. Now we prove sufficiency. First we assume (a), i.e., ϵ_4 is not in K. Let $[A] \in S(K)$ with $\mathscr{S} = \{q: \text{ind}_q A = 2\}$. If $b = 0$ then the result follows from [**5**, Theorem 2.5, p. 173]. Therefore we may assume $b > 0$. First consider those $q \in \mathscr{S}$ for which

$$|f(q, K/Q)|_2 = 1 = |e(q, K/Q)|_2.$$

By [**10**, Theorem 7.2, p. 96] there exists $[B] \in S(Q)$ with $\text{ind}_q B = 2 = \text{ind}_\infty B$ and $\text{ind}_p B = 1$ for all $p \neq q, \infty$. Therefore $[B \otimes M] \in S(M)$ with

$$\text{ind}_q B \otimes M = 2 = \text{ind}\, B \otimes M$$

since

$$|f(q, K/Q)|_2 = 1 = |e(q, K/Q)|_2,$$

and

$$\text{ind}_p B \otimes M = 1 \text{ for all } p \neq q, \infty.$$

Hence by [**10**, Theorem 8.1, p. 132] we have $[(B \otimes M) \otimes K] \in S(M) \otimes K$ with q-local index equal to 2 and p-local index equal to 1 for all $p \neq q$. We note that the ∞-local index is 1 since K is non-real. We may now assume without loss of generality that $\mathscr{S}$ contains only primes q with

$$|f(q, K/Q)|_2 > 1 \text{ or } |e(q, K/Q)|_2 > 1.$$

First consider the case $|f(q, K/Q)|_2 > 1$. By [**8**, Theorem 3 (I)] we necessarily have $e(q, L/Q) = 1$; i.e., q is unramified in L. Set

$$M^{(i)} = \mathbf{Q}(\epsilon_{p_i^{a_i}}) \cap M \text{ for } i = 0, 1, 2, \ldots, t$$

where $p_0 = 2$ and $a_0 = s$. We claim that $|M_q: M_q^{(i)}|_2 = 1$ for some $i = 0, 1, 2, \ldots, t$. Suppose

$$|M_q: M_q^{(i)}|_2 > 1 \text{ for all } i = 0, 1, \ldots, t.$$

Since $\mathscr{F}(q, M/Q)$ generates a cyclic group in M/Q then we must have

$$|M_q: \pi M_q^{(i)}|_2 > 1$$

where $\pi M_q^{(i)}$ is the compositum of $M_q^{(i)}$ for all $i = 0, 1, 2, \ldots, t$. Now we show that this contradicts the hypothesis $q \in \mathscr{S}$.

Set $G = \langle \phi \rangle$. Then we may assume that $\phi = \rho \psi^{2^{d-2}} \tau$ where the order of $\langle \psi^{2^{d-2}} \rangle = 2^{s-d}$ divides the order of $\tau \in G(L/\mathbf{Q}(\epsilon_{2^s}))$. Thus

$$\phi(\epsilon_{2^s}) = \epsilon_{2^s}{}^{-h} \text{ where } h = 5^{2^{d-2}}.$$

Set $\mathscr{F} = \mathscr{F}(q, L/\mathbf{Q})$ and $f = f(q, K/\mathbf{Q})$. Since $\mathscr{F}(q, L/\pi M^{(i)})$ has the form

$$\phi^x \rho^y \phi_1^{h_1 x_1/2} \ldots \phi_t^{h_t x_t/2}$$

and $\mathscr{F}^f = \mathscr{F}(L/K)$ then $|M_q: \pi M_q^{(i)}|_2 > 1$ implies that $\mathscr{F}(L/K) =$

https://doi.org/10.4153/CJM-1981-106-5 Published online by Cambridge University Press

φ^{2t}. By [**8**, Theorem 3 (II) (b)] this implies $q \notin \mathcal{S}$, a contradiction. (We note that t should be c in [**8**, Theorem 3 (II)]).

We have demonstrated that $|M_q: M_q^{(i)}|_2 = 1$ for some i. By [**10**, Theorem 7.4, p. 97] there exists $[B_q] \in S(M^{(i)})$ with $\text{ind}_q B_q = 2$. Furthermore, if q splits into an even number of primes in $M^{(i)}$ we may assume $\text{ind}_p B_q = 1$ for all $p \neq q$. If q splits into an odd number of primes in $M^{(i)}$ we may assume

> $\text{ind}_{t_i} B_q = 2 = \text{ind}_q B_q$ and $\text{ind}_p B_q = 1$ for all $p \neq q, t_i$ where t_i is a prime with $|K_{t_i}: M^{(i)}|_2 > 1$, and t_i splits into an odd number of primes in $M^{(i)}$.

Now $\pi_q[B_q \otimes M] \in S(M)$ with $\text{ind}_q B_q \otimes M$ for each $q \in \mathcal{S}$ such that q is unramified in L. Thus from [**10**, Theorem 8.1, p. 132] we have

$$\pi_q[(B_q \otimes M) \otimes K] \in S(M) \otimes K$$

with q-local index equal to 2 for all $q \in \mathcal{S}$ such that q is unramified in L. Now, since G is cyclic then at most one prime ramifies in L/K. Thus by [**8**, Theorem 3 (I)] there can be at most one ramified prime in $\mathcal{S}$. Suppose

$$|e(p_j, L/K)|_2 > 1 = |f(p_j, K/Q)|_2.$$

Then by [**8**, Theorem 3 (III)], $p_j \in \mathcal{S}$ if and only if there are an odd number of unramified $q \in \mathcal{S}$ with $(p_j/q) = -1$ where $(/)$ is the Legendre symbol. However, $\pi_q[(B_q \otimes M) \otimes K]$ has q-local index equal to 2 for all unramified $q \in \mathcal{S}$. So by [**8**, Theorem 3 (III)],

$$\text{ind}_{p_j} \pi_q{}^{\rho}(B_q \otimes M) \otimes K = 2$$

if and only if there are an odd number of unramified $q \in \mathcal{S}$ with $(p_j/q) = -1$. We conclude:

$$\text{ind}_{p_j} A = \text{ind}_{p_j}(\pi_q(B_q \otimes M) \otimes K).$$

Hence: $[A] \in S(M) \otimes K$. This completes the proof of the sufficiency of (a).

Now we assume (b); i.e., that ϵ_4 is in K. First we assume (i), i.e.,

$$|K: \mathbf{Q}(\epsilon_{2^r})|_2 = 1.$$

Let $[A] \in S(K)$ and $q \in \mathcal{S}$ where $\mathcal{S}$ is as defined in (a). By [**10**, Theorem 7.4, p. 97] there exists $[D] \in S(Q(\epsilon_{2^r} + \epsilon_{2^r}{}^{-1}))$ with $\text{ind}_q D = 2$ and if $r > 2$, then $\text{ind}_p D = 1$ for all $p \neq q$. If $r \leqq 2$ then C may be chosen such that $\text{ind}_q D = \text{ind}_\infty D = 2$ and $\text{ind}_p D = 1$ for all $p \neq q, \infty$. Now we have

$$|K: \mathbf{Q}(\epsilon_{2^r})|_2 = 1 = |M: \mathbf{Q}(\epsilon_{2^r} + \epsilon_{2^r}{}^{-1})|_2.$$

Therefore $[D \otimes M] \in S(M)$ with $\mathrm{ind}_q D \otimes M = 2$. By [**9**, Theorem 8.1, p. 132] we have $|K_q : M_q|_2 = 1$ which implies

$$[(D \otimes M) \otimes K] \in S(M) \otimes K$$

with

$$\mathrm{ind}_q(D \otimes M) \otimes K = 2 \text{ and } \mathrm{ind}_r(D \otimes M) \otimes K = 1$$

for all $r \neq q$. We note that $\mathrm{ind}_\infty(D \otimes M) \otimes K = 1$ since K is non-real. This completes the proof of the sufficiency of (b) (i).

Now we assume (ii), i.e., $t = 1$ and $\phi_i^{h_i/2} \in G$. Since ϵ_4 is in K then $b = 0$ is forced and so $r = s$. Suppose first that

$$|f(q, K/\mathbf{Q})|_2 > 1 \text{ and } |e(q, K/\mathbf{Q})|_2 > 1.$$

Then by [**10**, Corollary 5.4] we have $q > 2$. Moreover $|M_q^{(i)} : \mathbf{Q}_q|_2 > 1$ for $i = 0, 1$ where $M^{(i)}$ is defined as in (a). Also $q = p_1$ is forced since $|e(q, K/Q)|_2 > 1$ and $q > 2$. Thus L is the smallest cyclotomic field in which M is contained. Now we demonstrate the existence of $[B] \in S(M)$ with $\mathrm{ind}_q B = 2$. Since $|M_q^{(0)} : Q_q|_2 > 1$ then $|q^f - 1|_2 = 2^r$ where $f = f(q, K/\mathbf{Q})$. Also $\mathscr{F}(q, L/K) \notin G^2$ since

$$\mathbf{Q}(\epsilon_{2^r}) \subseteq K \subseteq \mathbf{Q}(\epsilon_{2^r}, \epsilon_{p_1}{}^{a_1} + \epsilon_{p_1}^{-1}{}^{b_1}).$$

Since $|K_q : M_q|_2 = 1$ by virtue of $q \in S$, then

$$\Theta(q, L/K) = \Theta(q, L/M) \text{ and } C_M = G(L/M(\epsilon_{2^s})) = G(L/K) = G.$$

Therefore $\Theta(q, L/M) \notin C_M^2$. Thus the hypothesis of Theorem 2.3 (A) is satisfied so there exists $[B] \in S(M)$ with $\mathrm{ind}_q B = 2$. By Theorem 2.3 (A) we may choose

$$B = B(q, \alpha) = (L(\epsilon_q)/M, \alpha)$$

and since only q and 2 ramify in $L(\epsilon_q)/M$ then the only other possibility for non-trivial index of B is at 2. Now we have: $[B \otimes K] \in S(M) \otimes K$ with $\mathrm{ind}_q B \otimes K = 2$ and $\mathrm{ind}_p B \otimes K = 1$ for all $p \neq q$. We note that $\mathrm{ind}_2 B \otimes K = 1$ by [**10**, Corollary 5.4]. Now we may assume without loss of generality that all $q \in \mathscr{S}$ satisfy either

$$|e(q, K/\mathbf{Q})|_2 = 1 \text{ or } |f(q, K/\mathbf{Q})|_2 = 1.$$

Thus $|M_q : M_q^{(i)}|_2 = 1$ for some $i = 0, 1$. Now, by exactly the same argument as in the proof of (a) we get

$$\pi_q[C_q \otimes K] \in S(M) \otimes K$$

with q-local index equal to 2 for all $q \in \mathscr{S}$ such that q is unramified in L. Now the only other prime at which $\pi_q[C_q \otimes K]$ can have non-trivial index is at p_1. If $p_1 \not\equiv 1 \pmod{2^{s+1}}$ then, since $\Theta(p_1, L/M) \notin C_M^2$ by the same argument as above, we have the existence of $[B_{p_1} \otimes K] \in S(M) \otimes K$

https://doi.org/10.4153/CJM-1981-106-5 Published online by Cambridge University Press

with non-trivial index 2 exactly at p_1, by Theorem 2.3 (A). Thus either

$$A \sim (B_{p_1} \otimes K)(\pi_q(C_q \otimes K))$$

or

$$A \sim \pi_q C_q \otimes K.$$

Now we may assume $p_1 \equiv 1 \pmod{s^{s+1}}$. By [**8**, Theorem III, p. 170], $p_1 \in \mathscr{S}$ if and only if there are an odd number of unramified $q \in \mathscr{S}$ with $(p_1/q) = -1$ and $l(q) \geqq r - \lambda$, (see [**9**] for the definition of $l(q)$ and λ). However $\pi_q[C_q \otimes K]$ has q-local index equal to 2 for all unramified $q \in \mathscr{S}$. So by [**9**, Theorem (III), p. 170] $\text{ind}_{p_1}\pi_q(C_q \otimes K) = 2$ if and only if there are an odd number of unramified $q \in \mathscr{S}$ with $(p_j/q) = -1$ and $l(q) \geqq r - \lambda$. We conclude

$$\text{ind}_{p^1}A = \text{ind}_{p^1}(\pi_q C_q \otimes K).$$

Hence $[A] \in S(M) \otimes K$. This proves the theorem.

The following was obtained in [**5**, Theorem 2.6]. We isolate it since it may be of independent interest. We remind the reader that $n \not\equiv 2 \pmod 4$.

Corollary 3.3. *If $K = \mathbf{Q}(\epsilon_n)$ then all elements of order 2 in $S(K)$ are induced from $S(M)$ if and only if n is odd or a power of 2.*

We conclude with the conjecture that the conditions of Theorem 3.1 are necessary and sufficient in general.

We were unable to make more progress in the general case because of new problems with [**7**] which is the only paper in the literature dealing with the case where ϵ_4 is not in K. We have verified that Theorem 2.3 (A) is correct and this is the only portion of Theorem 2.3 which we have used in this paper. However we maintain that Theorem 2.3 (C) is false, which is the reason for referring to [**8**] for the ramified case.

The following is a counterexample.

Let $K = \mathbf{Q}(\sqrt{5}, \sqrt{-13})$; then $L = \mathbf{Q}(\epsilon_{4.5.13})$. Let

$$G(L/\mathbf{Q}(\epsilon_{5.13})) = \langle \rho \rangle$$
$$G(L/\mathbf{Q}(\epsilon_{4.13})) = \langle \phi_5 \rangle; \text{ and}$$
$$G(L/\mathbf{Q}(\epsilon_{4.5})) = \langle \phi_{13} \rangle.$$

Set $C = \langle \phi_5^2 \rangle \times \langle \phi_{13}^2 \rangle$. A generator of the inertia group of 5 in $G = G(L/K)$ is $\Theta(5) = \phi_5^2$, and the Frobenius automorphism of 5 in G is ϕ_{13}^6. On the other hand $f(5, K/Q) = 2$ and $5^2 \equiv 1 \pmod 8$ so Theorem 2.3 (A) does not apply. Now $\eta(5) = \phi_{13}^6$, (see [**7**, p. 430] for the definition of η). Thus the order, $N_1(5)$, of $\Theta(5)\eta(5)$ in C/C^2 is 2. By Theorem 2.3 (C) there exists $[A] \in S(K)$ with $\text{ind}_5 A = 2$. However by [**10**, Theorem

8.1, p. 132] we have $A \sim B \otimes K$ where $[B] \in B(\mathbf{Q}(\sqrt{5}))$ with $\text{ind}_5 B = 2$, and so

$$|K_5 : \mathbf{Q}_5(\sqrt{5})|_2 = 1,$$

a contradiction since $f(5, K/\mathbf{Q}) = 2$. This completes the counterexample.

References

1. G. J. Janusz, *The Schur group of an algebraic number field*, Annals of Math. *103* (1976), 253–281.
2. R. Mollin, *Algebras with uniformly distributed invariants*, J. Algebra *44* (1977), 271–282.
3. ——— *The Schur group of a field of characteristic zero*, Pacific J. Math. *76* (1978), 471–478.
4. ——— *Uniform distribution classified*, Math. Z. *165* (1979), 199–211.
5. ——— *Induced p-elements in the Schur group*, Pacific J. Math. *90* (1980), 169–176.
6. ——— *Splitting fields and group characters*, J. Reine Angew. Math. *315* (1980), 107–114.
7. J. W. Pendergrass, *The 2-part of the Schur group*, J. Algebra *41* (1976), 422–438.
8. ——— *The Schur subgroup of the Brauer group*, (preprint).
9. ——— *Calculations in the Schur group*, J. Algebra *41* (1976), 422–438.
10. T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Mathematics *397* (Springer-Verlag, 1974).

Queen's University,
Kingston, Ontario