

INDUCED p -ELEMENTS IN THE SCHUR GROUP

RICHARD ANTHONY MOLLIN

The main result of this paper gives necessary and sufficient conditions for the p -primary part $S(K)_p$ of the Schur group $S(K)$ to be induced from $S(F)_p$ for any subfield F of K where K is contained in $Q(\varepsilon_n)$, under the restriction that ε_{p^2} is not in K if $p > 2$ and n is odd if $p = 2$, where ε_n is a primitive n th root of unity.

Moreover we completely answer the question: "When is $S(Q(\varepsilon_n + \varepsilon_n^{-1}))$ induced from $S(Q)$?" for any n , and also the question: "When are the quaternion division algebras in $S(Q(\varepsilon_n))$ induced from $S(Q(\varepsilon_n + \varepsilon_n^{-1}))$?" for any n . Finally, in the last section we investigate the "generalized group of algebras with uniformly distributed invariants" which we introduced in an earlier paper. We obtain, for the first time, a sufficient condition for the group to be induced from a certain subgroup.

Preliminaries. Let $L = Q(\varepsilon_n)$ and let K be a subfield of L . Although it is not necessary for all results in the paper it is convenient to choose n as small as possible for a given K . The Schur subgroup $S(K)$ of the Brauer group $B(K)$ consists of those equivalence classes $[A]$ which contain an algebra which is isomorphic to a simple summand of the group algebra KG for some finite group G . An elegant proof of the following result was given by Janusz [18, Prop. 6.2, p. 89]:

(1.1) Let $[A] \in S(K)$ where $[A]$ has exponent n then ε_n , a primitive n th root of unity is in K . (In fact (1.1) holds for any field K .)

For K over Q finite abelian, Benard and Schacher [2, Th. 6.1, p. 89] proved the following:

If $[A] \in S(K)$ then:

(1.2) If the index of A is n then ε_n is in K .

(1.3) If q is a K -prime above the rational prime q and $\sigma \in G(K/Q)$, the Galois group of K over Q , with $\sigma(\varepsilon_n) = \varepsilon_n^{h^2}$ then the Hasse q -invariant of A satisfies:

$$\text{inv}_q A \equiv b_\sigma \text{inv}_{q,\sigma} A \pmod{1}.$$

If $[A] \in B(K)$ and A satisfies (1.2)-(1.3) then A is said to have *uniformly distributed invariants*. These algebras form a subgroup $U(K)$ of $B(K)$. For a treatment of this group see Mollin [7, 14, 15, 16]. We note from (1.2)-(1.3) that $S(K)$ is a subgroup of $U(K)$. For

a generalization of $U(K)$ to the algebraic number field case and consequences thereof (including, therefore, results for $S(K)$ see Mollin [8]-[13]).

Now, if $[A] \in U(K)$ and q' and q are K -primes above q then $A \otimes_K K_{q'}$ and $A \otimes_K K_q$ have the same index where K_q denotes the completion of K at q . We call the common value of the indices of $A \otimes_K K_q$ for all $K =$ primes above q the q -local index of A and denote it by $\text{ind}_q(A)$.

We shall have need of the following formula which can be found in Deuring [3]:

(1.4) Let $[A] \in B(K)$. Let K/F be finite and let \hat{q} be a K -prime above the F -prime q . Then:

$$\text{inv}_{\hat{q}}(A \otimes_F K) \equiv |K_{\hat{q}} : F_{\hat{q}}| \text{inv}_q A \pmod{1}.$$

Henceforth, when we write a tensor product it shall be assumed to be taken over the center of the algebra in the left factor. Moreover, by the symbol $S(F) \otimes K$ we mean the image of $S(F)$ under the map which extends the center to K . The symbol \sim denotes equivalence in the Brauer group.

If q is an F -prime above q , then any reference to the decomposition of q in K over F (abelian), shall be referred to as the decomposition of q in K/F since the decomposition essentially depends on q and not on q . For example if q is unramified in K over F we say q is unramified in K over F .

Finally, for groups G and H contained in G , $a \in G - H$ means $a \in G$ but $a \notin H$.

For most basic results concerning $S(K)$ the reader is referred to [18].

2. Induced p -elements. Let $Q(\varepsilon_n)$ be the smallest cyclotomic field containing K . We may assume $n \not\equiv 2 \pmod{4}$ since $Q(\varepsilon_n) = Q(\varepsilon_{2n})$ whenever n is odd. Let p be a prime such that if p is odd then ε_{p^2} is not in K and if $p = 2$ then n is odd. Let F be a subfield of K and set $G_0 = G(Q(\varepsilon_n)/F)$. Now we present for the first time necessary and sufficient conditions for $S(K)_p$ to be induced from $S(F)_p$. In the following theorem we maintain the above notation and assumptions. To avoid the trivial case $S(K)_p = 1$ we assume ε_p is in K .

THEOREM 2.1. $S(K)_p = S(F)_p \otimes K$ if and only if

- (1) ε_p is in F and
- (2) $G_0^p \cap G = G^p$.

Proof. Since $S(K)_p \neq 1$ then equality holds only if ε_p is in F .

We show that the equality of the theorem is equivalent to (2) when (1) holds.

By [6, Th. 2, Th. 3, Th. 5] and [17, Th. 2.2, Th. 2.3], an algebra class in $S(K)_p$ is determined by a skew-pairing ψ^K on G to $\langle \varepsilon_p \rangle$ and by certain elements in $S(Q(\varepsilon_p))_p \otimes K$ (which also lie in $S(F) \otimes K$). A similar statement holds for $S(F)_p$. Therefore $S(K)_p = S(K)_p \otimes K$ if and only if every skew-pairing on G is the restriction of a skew-pairing on G_0 . Since the values lie in $\langle \varepsilon_p \rangle$, this is equivalent to the assertion that the inclusion of G into G_0 induces an inclusion of G/G^p into G_0/G_0^p . This is equivalent to (2).

The following result obtained in Mollin [14, Corollary 2.3, p. 165] is immediate.

COROLLARY 2.2. *If K/Q is real of even degree and K is in $Q(\varepsilon_n)$ where n is odd and no prime congruent to 1 modulo 4 divides n then $S(K) = S(Q) \otimes K$.*

Before presenting a sequence of results anchored to Theorem 2.1 we demonstrate that the theorem does not hold if n is even and ε_4 is not in K . We shall need a result which we isolate as a lemma since it verifies remarks made in Mollin [14, p. 165], (remarks follow Theorem 2.2 therein).

LEMMA 2.3. *Let $n = 2^a h$, $a \geq 2$, $(2, h) = 1$, and let $K = Q(\varepsilon_n + \varepsilon_n^{-1})$.*
 (i) *If $a = 2$ then $S(K) = S(Q) \otimes K$,*
 (ii) *If $a > 2$ then $S(K) \neq S(Q) \otimes K$.*

Proof. (i) If $a = 2$ and $h = 1$ the result is clear. We assume that $h > 1$. We see easily that in order to obtain $S(K) = S(Q) \otimes K$ it suffices to prove $\text{ind}_p A = 1$ for $[A] \in S(K)$ whenever $|K_p:Q_p|$ is even where p is a K -prime above p . If $p|n$ then by Yamada [18, Th. 1, p. 591], $\text{ind}_p A = 1$ for any $[A] \in S(K)$. If p does not divide n and $|K_p:Q_p|$ is even then Yamada's aforementioned result says that if $[A] \in S(K)$ with $\text{ind}_p A = 2$ then $p^{f/2} \equiv -1 \pmod{n}$ where f is the residue class degree of p in $Q(\varepsilon_n)/Q$. This means that p is inert in $Q(\varepsilon_n)/K$ so that $f/2$ must be even in order that $|K_p:Q_p|$ is even. Thus, $p^{f/2} \equiv -1 \pmod{n}$ implies that -1 is a square modulo 4, which is absurd. This establishes (i).

(ii) If $h = 1$ then the result follows from Yamada [18, Th. 2.2, p. 586] and Mollin [7, Th. 2.6, p. 277]. We assume $h > 1$ and let $n = p_1^{a_1} \cdots p_s^{a_s}$ where the p_i 's are distinct primes. Choose a prime p such that $p \equiv -1 \pmod{h}$ and $p \equiv 5 \pmod{2^a}$. Such a choice is allowed by the Chinese Remainder theorem. Now we show that

there exists $[A] \in S(K)$ with $\text{ind}_p A = 2$ and such that $[A] \notin S(Q) \otimes K$.

The smallest positive integer f such that $p^f \equiv 1 \pmod{n}$ is 2^{a-2} ; i.e., the residue class degree of p in K over Q is 2^{a-2} . Thus, by the choice of p we have: p does not divide n , f is even, $p^{f/2} \not\equiv -1 \pmod{n}$ and $p^{f/2} \not\equiv \pm 1 \pmod{2^a}$. By Yamada [18, Th. 1, p. 591] this guarantees the existence of $[A]$ in $S(K)$ with $\text{ind}_p A = 2$. Now, since $p^{f/2} \not\equiv -1 \pmod{n}$ then p splits completely in $Q(\varepsilon_n)$ over K . Hence, $f = 2^{a-2}$ equals the residue class degree of p in K over Q . Since $a > 2$ it follows that $[A] \notin S(Q) \otimes K$ from (1.4).

Now we present the aforementioned example to show that the theorem does not hold if n is even and ε_4 is not in K . We maintain the above notation; i.e., $K = Q(\varepsilon_n + \varepsilon_n^{-1})$ where $n = 2^a h$, $h > 1$, $a > 2$, $(2, h) = 1$, and $G_0 = GQ(\varepsilon_n)/(Q)$. Let:

$$G_0 = \langle \theta \rangle \times \langle \alpha \rangle \times \langle \phi_1 \rangle \times \cdots \times \langle \phi_s \rangle$$

where:

$$\begin{aligned} \varepsilon_{2^a}^{\theta} &= \varepsilon_{2^a}^5, & \varepsilon_h^{\theta} &= \varepsilon_h; \\ \varepsilon_{2^a}^{\alpha} &= \varepsilon_{2^a}^{-1}, & \varepsilon_h^{\alpha} &= \varepsilon_h; \end{aligned}$$

and

$$\theta^{2^{a-2}} = \alpha^2 = \phi_i^{h_i} = 1$$

where:

$$\phi_i(\varepsilon_n) = \varepsilon_n^{s_i}; \quad s_i \equiv r_i \pmod{p_i^{s_i}}; \quad s_i \equiv 1 \pmod{n/p_i^{s_i}}$$

where r_i is a primitive root modulo p_i , and $h_i = p_i^{s_i-1}(p_i - 1)$ for $i = 1, 2, \dots, s$. By Lemma 2.3, $S(K) \neq S(Q) \otimes K$. We have $G_0^2 = \langle \theta^2 \rangle \times \langle \phi_1^{h_1/2} \rangle \times \cdots \times \langle \phi_s^{h_s/2} \rangle$ and $G = \langle \alpha \phi_1^{h_1/2} \cdots \phi_s^{h_s/2} \rangle$. Therefore $G_0^2 \cap G = \langle 1 \rangle = G^2$. This establishes the counterexample.

Now we establish a series of results tied to Theorem 2.1. In the introduction to [19] Yamada remarks that if K is a real subfield of $Q(\varepsilon_n)$ such that $G(Q(\varepsilon_n)/K)$ is cyclic; then the structure of $S(K)$ does not depend on whether or not n is divisible by a prime congruent to 3 modulo 4. Lemma 2.3 indicates that Yamada is correct in general. However, if we restrict our attention to maximal real subfields of $Q(\varepsilon_n)$ for n odd the result goes through. The following theorem therefore is the exact analogue of Yamada's result on real quadratic fields [18].

Moreover, this theorem generalizes and simplifies the proof of the result obtained in Mollin [14, Th. 2.2, p. 164]. Finally it completes the answer to the 'Tensoring question' for the maximal real subfield of $Q(\varepsilon_n)$ for any n .

THEOREM 2.4. *Let $K = Q(\varepsilon_n + \varepsilon_n^{-1})$ where $n > 1$ is odd. Then $S(K) = S(Q) \otimes K$ if and only if there exists a prime q dividing n such that $q \equiv 3 \pmod{4}$.*

Proof. To establish the necessity assume $S(K) = S(Q) \otimes K$. We have: $G = G(Q(\varepsilon_n)/K) = \langle \phi_1^{h_1/2} \cdots \phi_s^{h_s/2} \rangle$ where the ϕ_i and h_i are defined as in the above example. If we assume $p_i \equiv 1 \pmod{4}$ for all $i = 1, 2, \dots, s$ then it is clear that $h_i \equiv 0 \pmod{4}$ for all $i = 1, 2, \dots, s$. Thus: $G_0^2 \cap G = \langle (\phi_1^{h_1/4})^2 \rangle \times \cdots \times \langle (\phi_s^{h_s/4})^2 \rangle = G$. However $G^2 = \langle 1 \rangle$, so $G_0^2 \cap G \neq G^2$ which implies by Theorem 2.1 that $S(K) \neq S(Q) \times K$ contradicting the hypothesis, thereby establishing the necessity.

Conversely if $S(K) \neq S(Q) \otimes K$ then by Theorem 2.1 we have: $G_0^2 \cap G \neq G^2 = \langle 1 \rangle$. Therefore $G_0^2 \cap G = G$. This forces $h_i \equiv 0 \pmod{4}$ for each $i = 1, 2, \dots, s$, which establishes the theorem.

It is reasonable to ask whether or not a similar result holds for an arbitrary real subfield $Q(\varepsilon_n)$ for n odd. If n is a prime-power it does, (see [18]).

However, if n is divisible by at least 2 distinct primes it does not. The following counterexample illustrates this fact.

Let $n = 65$ and let:

$$\begin{aligned} \phi_{13}: \varepsilon_{13} &\longrightarrow \varepsilon_{13}^2; & \phi_{13}: \varepsilon_5 &\longrightarrow \varepsilon_5; \\ \phi_5: \varepsilon_5 &\longrightarrow \varepsilon_5^2; & \phi_5: \varepsilon_{13} &\longrightarrow \varepsilon_{13}. \end{aligned}$$

Let $\phi = \phi_{13}^3 \cdot \phi_5$ and let K equal the fixed field of $\langle \phi \rangle$. We note $G_0^2 \cap G = \langle \phi_{13}^6 \cdot \phi_5^2 \rangle = G^2$ which yields $S(K) = S(Q) \otimes K$ from Theorem 2.1. This completes the counterexample.

Now, let K over Q be finite imaginary and abelian with M as maximal real subfield. From [1, Th. 2.1, p. 161] it follows that $[A] \in S(K)$ with index 2 satisfies $A \sim B \otimes K$ where $[B] \in B(M)$ and B is also quaternion. A natural question to ask is whether or not $[B] \in S(M)$. The following theorem answers this question for certain fields.

THEOREM 2.5. *Let K be contained in $Q(\varepsilon_n)$ with n odd such that K over Q is finite, imaginary and abelian, then*

$$S(K)_2 = S(M) \otimes K.$$

Proof. If $G_0^2 \cap G \neq G^2$ then there is a cyclic subgroup of G_0 of 2 power order such that

- (i) $H \cap G^2 \neq H \cap G$
- (ii) $H \cap G \neq \langle 1 \rangle$ and
- (iii) $H \cap G \neq H$.

Therefore by Pendergrass [17, Th. 2.3, p. 433] there exists $[A] \in S(K)_2$ with $\text{ind}_p A = 2$ where p has Frobenius automorphism corresponding to a generator of H . By [1], op. cit., $A \sim B \otimes K$ where $[B] \in B(M)$ is quaternion. Thus, for a K -prime \mathfrak{p} above an M -prime \mathfrak{p} which in turn sits above the rational prime p ; we have from (1.4) that:

$$\text{inv}_{\mathfrak{p}} A = \text{inv}_{\mathfrak{p}} B \otimes K \equiv |K_{\mathfrak{p}}: M_{\mathfrak{p}}| \text{inv}_{\mathfrak{p}} B \pmod{1}.$$

However, by (iii) above we have $|K_{\mathfrak{p}}: M_{\mathfrak{p}}| = 2$ so it follows that $\text{inv}_{\mathfrak{p}} A = 0$, a contradiction which secures the theorem.

We note that the above theorem includes the case where $M = \mathbb{Q}(\varepsilon_n + \varepsilon_n^{-1})$ for n odd. The following theorem establishes that for n even the result does not hold. Moreover it yields necessary and sufficient conditions for elements of order 2 in $S(\mathbb{Q}(\varepsilon_n))$ to be induced from $S(M)$.

THEOREM 2.6. *Let*

$$K = \mathbb{Q}(\varepsilon_n), \quad M = \mathbb{Q}(\varepsilon_n + \varepsilon_n^{-1}).$$

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.

Proof. First we prove the necessity of the condition. Assume that $n = 2^a m$, where $(2, m) = 1$, $a > 1$, $m > 1$. We now prove that there exists an element of order 2 in $S(K)$ which is not induced from $S(M)$. Choose a prime $p \equiv 1 \pmod{2^a}$ and $p \equiv -1 \pmod{m}$. Thus the residue class degree of p in K over \mathbb{Q} is 2; i.e., the smallest integer f such that $p^f \equiv 1 \pmod{n}$ is $f = 2$. However, $p = p^{f/2} \not\equiv -1 \pmod{n}$ so p has inertial degree 1 in K over M . This fact together with $p = p^{f/2} \equiv 1 \pmod{2^a}$ is enough to ensure that there does not exist an element in $S(M)$ with p -local index 2, by Yamada [18, Th. 1, p. 591]. Now,

$$S(K)_2 = S(\mathbb{Q}(\varepsilon_{2^a})) \otimes K,$$

by Janusz [5, Th. 1, p. 346]. Since $p \equiv 1 \pmod{2^a}$ then there exists $[A] \in S(\mathbb{Q}(\varepsilon_{2^a}))$ with $\text{ind}_p A = 2^a$ by Yamada [18, pp. 135-139]. Let $[A]^{2^{a-2}} = [B]$. Then $\text{ind}_p B = 4$ and if \mathfrak{p} is a K -prime above p then:

$$\text{inv}_{\mathfrak{p}} B \otimes K \equiv |K_{\mathfrak{p}}: \mathbb{Q}_p(\varepsilon_{2^a})| \text{inv}_{\mathfrak{p}} B \pmod{1}.$$

But $|K_{\mathfrak{p}}: \mathbb{Q}_p(\varepsilon_{2^a})| = 2$ so that $\text{ind}_p(B \otimes K) = 2$. We have $[B \otimes K] \in S(K)$ having p -local index 2 but $B \otimes K$ is not induced from $S(M)$. This establishes the necessity.

Conversely, if n is odd then we are done by Theorem 2.1, so we assume n is a power of 2. Given $[A] \in S(K)$ with $\text{ind}_p A = 2$ we have $|K_{\mathfrak{p}}: M_{\mathfrak{p}}| = 1$ which follows from the fact that $A \sim B \otimes K$ with $[B] \in B(M)$ being quaternion. Now it suffices to show that there exists $[C] \in S(M)$ with $\text{ind}_p C = 2$, but this is immediate from Yamada [18, Th. 2.2, p. 586].

3. The tensoring question for $U_x(K)$. Let K/F be finite Galois where F is an algebraic number field. We define $U_x(K)$ to be the subset of $B(K)$ consisting of $[A] \in B(K)$ such that:

(3.1) If the index of A is m then, ε_m is in K , and

(3.2) If \mathfrak{P} is a K -prime lying over the F -prime \mathfrak{p} and

$$\begin{aligned} \tau \in G(K/F) \text{ with } \varepsilon_m^{\tau} = \varepsilon_m^b \text{ then:} \\ \text{inv}_{\mathfrak{P}}(A) \equiv b_{\tau} \text{inv}_{\mathfrak{P}}(A) \pmod{1}. \end{aligned}$$

For a treatment of this subgroup, which we call the ‘group of algebras with uniformly distributed invariant for K relative to F ’, see Mollin [9]. We note here that $S(K)$ is a subgroup of $U_x(K)$.

We need a definition before stating the next result. If K and E are number fields and D is a K -division ring; i.e., D is a division ring with $[D] \in B(K)$ then we say that D is ‘ E -adequate’ if there exists an E -division ring containing D .

THEOREM 3.1. *Let E/F be a Galois extension of number fields and K/F any extension of number fields. If D is a K -adequate division ring with $[D] \in U_x(E)$ where D has exponent n , then ε_n is in K and for all $p|n$ we have:*

$$U_x(KE)_p = U_x(E)_p \otimes KE.$$

Proof. From Mollin [9, Th. 3.2, p. 263] we have ε_n is in K and from Mollin [9, Lemma 31, p. 262] we have that $U_x(E)_p \otimes KE$ is contained in $U_x(KE)_p$. From the proof of [9, Th. 2.10, p. 260] and from [9, Lemma 3.1, p. 262] it is easily seen that it suffices to prove that there are no higher p -power roots of unity in KE than in E and that p does not divide $|KE: E|$.

Now, let D_1 be a K -division ring containing D . Then $D \otimes KE$ is isomorphic to the division ring, of index n in D_1 , generated by D and K . Therefore p does not divide $|KE: E|$. Now, if ε_{p^a} is in KE but not in E then $|E(\varepsilon_{p^a}): E| = p$ and $E(\varepsilon_{p^a}) \subseteq KE$. Thus $p \mid |KE: E|$, a contradiction which establishes the theorem.

ACKNOWLEDGMENT. The author welcomes this opportunity to

thank the referee for several helpful suggestions which improved the paper.

REFERENCES

1. A. A. Albert, *Structure of Algebras*, Amer. Math. Soc., Providence, R.I., 1961.
2. M. Benard and M. Schacher, *The Schur subgroup II*, *J. Algebra*, **22** (1972), 378-385.
3. M. Deuring, *Algebren*, Springer, Berlin, 1935.
4. L. Goldstein, *Analytic Number Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1971.
5. G. L. Janusz, *The Schur group of cyclotomic fields*, *J. Number Theory*, **7** (1975), 345-352.
6. ———, *The Schur group of an algebraic number field*, *Annals of Math.*, **103** (1976), 253-281.
7. R. Mollin, *Algebras with uniformly distributed invariants*, *J. Algebra*, **44** (1977), 271-282.
8. ———, *Cyclotomic division algebras*, (preprint).
9. ———, *Generalized uniform distribution of Hasse invariants*, *Communications in Algebra*, **5** (3), (1977), 245-266.
10. ———, *Herstein's conjecture, automorphisms and the Schur group*, *Communications in Algebra*, **6** (3), (1978), 237-248.
11. ———, *Splitting fields and group characters*, *J. reine angew Math.* **315** (1980), 107-119.
12. ———, *The Schur group of a field of characteristics zero*, *Pacific J. Math.*, **76** (2), (1978), 471-478.
13. ———, *Uniform distribution classified*, *Math. Zeitschrift*, **165** (1979), 199-211.
14. ———, *Uniform distribution and real fields*, *J. Algebra*, **43** (1976), 155-167.
15. ———, *Uniform distribution and the Schur subgroup*, *J. Algebra*, **42** (1976), 261-277.
16. ———, *$U(K)$ for a quadratic field*, *Communications in Algebra*, **4** (8), (1976), 747-759.
17. J. W. Pendergrass, *The 2-part of the Schur group*, *J. Algebra*, **41** (1976), 422-438.
18. T. Yamada, *The Schur Subgroup of the Brauer Group*, *Lecture Notes in Mathematics*, No. 397, Springer-Verlag, 1974.
19. ———, *The Schur subgroup of a real cyclotomic field*, *Math. Zeitschrift*, **139** (1974), 35-40.

Received November 10, 1977 and in revised form August 28, 1979.

UNIVERSITY OF LETHBRIDGE
 4401 UNIVERSITY DRIVE
 LETHBRIDGE, ALBERTA T1K 3M4