PACIFIC JOURNAL OF MATHEMATICS
Vol. 76, No. 2, 1978

THE SCHUR GROUP OF A FIELD OF CHARACTERISTIC ZERO

R. MOLLIN

We determine when a class in the Schur subgroup $S(K)$ of the Brauer group $B(K)$ of a field K of characteristic zero contains an algebra which is isomorphic to a simple summand A of the group algebra FG for some finite group G, where F is a subfield of K. We then investigate $A \otimes_F K$ which is the direct sum of simple algebras with center K, and determine exactly when these are K-isomorphic. Finally we refine existing examples in the theory of the Schur group, and obtain a decomposition theorem for the related group of algebras with uniformly distributed invariants.

In the introduction to [6] Janusz notes that: For a finite abelian extension K of the rationals Q, $S(K)$ the Schur subgroup of the Brauer group $B(K)$ consists of all classes $[A]$ consisting of an algebra A which is isomorphic to a simple summand of the group algebra QG for some finite group G. Our first result in this paper is that for an arbitrary field K of characteristic zero the above is false.

In Mollin [8-13] we develop the concept of the uniform distribution group $U(K)$ for an algebraic number field K. If ε_{p^a} denotes a primitive p^ath root of unity and ε_{p^a} is the highest p-power root of unity in K we have from Mollin [8] that when p does not divide $|K: Q(\varepsilon_{p^a})|$ then:

$$(*) \qquad U(K)_p = S(K)_p = K \otimes S(Q(\varepsilon_{p^a}))_p$$

where G_p denotes the p-primary part of a group G. In Janusz [7] it is shown that if p does not divide $|Q(\varepsilon_n): K|$ when $Q(\varepsilon_n)$ is the smallest root of unity field containing K then:

$$(**) \qquad S(K)_p = K \otimes S(Q(\varepsilon_{p^a}))_p \,.$$

C. Ford and G. Janusz [5] give for each prime p, examples of fields K for which $(**)$ does not hold. In this paper we present, for each prime p, fields K for which the second equality of $(*)$ does not hold but for which the first equality does hold. Finally, we obtain a decomposition theorem for $U(K)$.

2. Notation and preliminaries.

Let K be 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. By

Yamada [16, Cor. 3.11, p. 33] this is equivalent to $S(K)$ being the subgroup of $B(K)$ consisting of those equivalence classes which contain a cyclotomic algebra; i.e., a crossed product of the form $(K(\varepsilon)/K, \alpha)$ where ε is a root of unity and α is a factor set whose values are roots of unity in $K(\varepsilon)$.

In general we denote a crossed product by $(L/K, \beta)$ which is the central simple K-algebra having L-basis u_τ, $\tau \in G(L/K)$, the Galois group of L/K, subject to:

$$u_\tau u_\gamma = \beta(\tau, \gamma)u_{\tau\gamma}\ , \quad u_\tau x = \tau(x)u_\tau$$

for $x \in L$.

For further information on crossed products the reader is referred to Reiner's book [14].

Now, if G is a finite group and X is an irreducible character of G we shall denote the simple component of KG corresponding to X as $A(X, K)$. By Yamada [16, Prop. 1.1, p. 4], $A(X, K) = KGa(X)$ with $a(X) = \sum e(X^\tau)$ where the sum ranges over $\tau \in G(K(X)/K)$. $a(X)$ is a primitive central idempotent of KG, and $K(X)$ is the center of $A(X, K)$.

$$e(X) = X(1)|G|^{-1}\sum_{g \in G} X(g^{-1})g\ .$$

3. **The Schur group.** We let K be a field of characteristic zero throughout this section.

DEFINITION 3.1. Let K/L be cyclotomic, i.e., there is a root of unity ε such that $L \subseteq K \subseteq L(\varepsilon)$. *The Schur subgroup* $S_L(K)$ *of* K *relative to* L is the subgroup of $S(K)$ consisting of those classes that contain an algebra which is isomorphic to a simple summand of LG for some finite group G.

We note here that, in fact, $S_L(K)$ is nonempty if and only if K/L is cyclotomic. Now we ask whether or not $S_L(K)$ is a proper subgroup of $S(K)$. The answer is the content of the next theorem.

THEOREM 3.2. *If* K/L *is cyclotomic then* $S(K) = S_L(K)$.

Proof. Let $[A] \in S(K)$. By Yamada [16, Cor. 3.11, p. 33] we may assume that $A = (K(\varepsilon)/K, \beta)$. But, by hypothesis $K \subseteq L(\varepsilon')$ for some root of unity ε'. Thus, using the inflation map of cohomology theory we get $[A] = [B]$ where

$$B = (L(\varepsilon\varepsilon')/K, \beta) = \sum L(\varepsilon\varepsilon')u_\sigma$$

where the direct sum ranges over all $\tau \in \mathscr{G} = G(L(\varepsilon\varepsilon')/K)$.

Now, the values of β and $\varepsilon\varepsilon'$ generate a cyclic group $\langle\varepsilon''\rangle$ in $L^*(\varepsilon\varepsilon')$, the multiplicative group of $L(\varepsilon\varepsilon')$. Moreover, $\mathscr{G}$ can be regarded as an automorphism group of $\langle\varepsilon''\rangle$ where the values of β belong to $\langle\varepsilon''\rangle$. Therefore, by the theory of group extensions (e.g., Zassenhaus [17, III, § 6]) we have the exact sequence

$$1 \longrightarrow \langle\varepsilon''\rangle \longrightarrow G \longrightarrow \mathscr{G} \longrightarrow 1$$

where G is the multiplicative subgroup of B^* generated by ε'' and the elements $u_\sigma(\sigma \in \mathscr{G})$. In other words, G is an extension of $\langle\varepsilon''\rangle$ by $\mathscr{G}$. Since G spans B with coefficients in L then there is an L-algebra homomorphism of LG onto B. Hence B is isomorphic to a simple summand of LG.

The following is immediate.

COROLLARY 3.3. *If K/L is cyclotomic and $L \subseteqq T \subseteqq K$ then $S(K) = S_T(K)$.*

THEOREM 3.4. *If K/L is cyclotomic then*

$$S_L(K) = \bigcup_{L_0} S_Q(L_0) \otimes_{L_0} K$$

where L_0 ranges through cyclotomic extensions of Q such that $LL_0 = K$.

Proof. It suffices to prove $S_L(K) \subseteqq \bigcup_{L_0} S_Q(L_0) \otimes_{L_0} K$. Let $[A] \in S_L(K)$ with $A = A(X, L)$, say. Thus $K \cong L(X)$, by Dornhoff [3, Lemma 24.7, p. 124]. Now:

$$QG = A(X_0, Q) \oplus A(X_1, Q) \oplus \cdots \oplus A(X_n, Q) .$$

For simplicity we set $A(X_i, Q) = A_i$, $i = 0, 1, 2, \cdots, n$; $X_0 = X$, $Q(X) = L_0$ and $A(X, Q) = A_0$. Thus:

$$LG \cong QG \otimes_Q L \cong A_0 \otimes_Q L \oplus \cdots \oplus A_n \otimes_Q L$$

and

$$\begin{aligned} A_0 \otimes_Q L &\cong (A_0 \otimes_{L_0} L_0) \otimes_Q L \\ &\cong A_0 \otimes_{L_0} (L_0 \otimes_Q L) \\ &\cong A_0 \otimes_{L_0} L(X) \oplus \cdots \oplus A_0 \otimes_{L_0} L(X) \\ &\cong A_0 \otimes_{L_0} K \oplus \cdots \oplus A_0 \otimes_{L_0} K \end{aligned}$$

where the latter summands correspond to X^σ, $\sigma \in G((Q(X) \cap L)/Q)$. We note that by Yamada [16, Prop. 1.5, p. 8] we have $A_0 \cong A(X, L_0)$. Thus $[A_0] \in S_Q(L_0)$. We have shown that:

$$A = A(X, L) \cong A_0 \otimes_{L_0} K \quad \text{as required .}$$

As mentioned in the introduction we do *not* have in general that $S_Q(K) = S(K)$. The following example illustrates this assertion, and we thereafter determine exactly when $S_Q(K) = S(K)$.

If $K = Q(\sqrt[3]{2}, \varepsilon_3)$ where $\sqrt[3]{2}$ is a real root of $f(x) = x^3 - 2$, $L = Q(\sqrt[3]{2})$ and $[A] \in S(K)$, then by Theorem 3.2 we have $[A] \in S_L(K)$. If K were cyclotomic over Q then $K \subseteq Q(\varepsilon)$ for some root of unity ε. However, this means that K/Q is abelian, which is a contradiction. In fact, by the Kronecker-Weber theorem (e.g., see Ribenboim [15, p. 233]) an algebraic number field K is cyclotomic over Q if and only if K/Q is abelian. In this case we could use the Kronecker-Weber theorem and the method of proof of Theorem 3.2 to show that $S_Q(K) = S(K)$.

Now we let $[A] \in S_L(K)$ and $G(K/L) = \{\sigma_1 = 1, \sigma_2, \cdots, \sigma_n\}$, then $A(X, L) \otimes_L K \cong A(X^{\sigma_1}, K) \oplus \cdots \oplus A(X^{\sigma_n}, K)$. Since $A(X^{\sigma_i}, K) = KGe(X^{\sigma_i})$, $e(X^{\sigma_i}) = X(1)\,|G|^{-1} \sum X^{\sigma_i}(g^{-1})g$ then $A(X, K)$ is L-isomorphic to $A(X^{\sigma_i}, K)$ for $i = 1, 2, \cdots, n$. We ask: Are these algebras K-isomorphic? To illustrate that in general the answer is negative we give the following example.

We let $K = Q(\varepsilon_3)$ then $L = Q$ and $G(K/Q) = \langle\sigma\rangle$ where $\sigma(\varepsilon_3) = \varepsilon_3^{-1}$. If the index of $A(X, K)$ is 3 then $[A(X, K)] \neq [A(X^\sigma, K)]$ in $B(K)$. Hence $A(X, K)$ and $A(X^\sigma, K)$ are not K-isomorphic.

The following tells us exactly when $A(X^\sigma, K)$ and $A = A(X, K)$ are K-isomorphic.

THEOREM 3.5. *Let* $[A(X, K)] \in S_L(K)$ *and let* $\sigma \in G(K/L)$ *then* $[A(X, K)] = [A(X^\sigma, K)]$ *if and only if* σ *fixes* ε_m *where* m *is the exponent of* A.

Proof. By Yamada [16, p. 14] we may assume $[A] = [A(\beta)] = [(K(\varepsilon)/K, \beta)]$ where $(K(\varepsilon)/K, \beta) = \sum K(\varepsilon)u_\tau$ with the direct sum ranging over all $\tau \in G(K(\varepsilon)/K)$.

Now, σ can be extended to $G(K(\varepsilon)/L)$ and we maintain the notation σ for this automorphism.

Put:

$$\beta^\sigma(\tau, \gamma) = (\beta(\tau, \gamma))^\sigma \quad \text{for} \quad \tau, \gamma \in G(K(\varepsilon)/K)\,,$$

then β^σ is a factor set of $K(\varepsilon)/K$ because $G(K(\varepsilon)/K)$ is central in $G(K(\varepsilon)/L)$.

We let:

$$A(\beta^\sigma) = (K(\varepsilon)/K, \beta^\sigma) = \sum K(\varepsilon)v_\sigma$$

where $v_\gamma v_\tau = \beta^\sigma(\gamma, \tau)v_{\tau\tau}$; $\gamma, \tau \in G(K(\varepsilon)/K)$.

Now, if the values of β generate a group $\langle \varepsilon_n \rangle$ of nth roots of unity then:

$$[A(\beta)]^n = [A(\beta^n)] = [A(1)] = 1 .$$

Thus m divides n. If $\sigma(\varepsilon_n) = \varepsilon_n^t$ then $\sigma(\varepsilon_m) = \varepsilon_m^t$. But then we have $[A(\beta^\sigma)] = [A(\beta)]^t$. Hence $[A(\beta^\sigma)] = [A(\beta)]$ if and only if σ fixes ε_m. But $[A(X^\sigma, K)] = [A(\beta^\sigma)]$. Thus $[A(X^\sigma, K)] = [A(X, K)]$ if and only if σ fixes ε_m.

Maintaining the above notation we get:

COROLLARY 3.6. *If* $\sigma \in \mathrm{Aut}(K)$ *then* $[A(X, K)] = [A(X^\sigma, K)]$ *if and only if* σ *extends to* $\mathrm{Aut}(A)$.

Proof. In Mollin [13] we proved that σ extends to $\mathrm{Aut}(A)$ if and only if σ fixes ε_m.

4. **Uniform distribution and $S(K)$.** We let K/L be a finite Galois extension of number fields. A central simple algebra A over K is said to have *uniformly distributed Hasse invariants relative to* L if the following are satisfied:

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

(4.2) If $\mathfrak{P}$ is a K-prime above the L-prime $\mathfrak{p}$ and $\tau \in G(K/L)$ with $\varepsilon_m^\sigma = \varepsilon_m^b$ then the $\mathfrak{P}$-invariant of A satisfies:

$$\mathrm{inv}_{\mathfrak{P}}(A) \equiv b \,\mathrm{inv}_{\mathfrak{P}^\sigma}(A) \pmod 1 .$$

Now let $\mathfrak{P}$ and $\mathfrak{Q}$ be K-primes above some L-prime $\mathfrak{p}$ and let $K_{\mathfrak{P}}$ denote the completion of K at $\mathfrak{P}$. For an algebra A with uniformly distributed invariants we have that $A \otimes K_{\mathfrak{P}}$ and $A \otimes K_{\mathfrak{Q}}$ have the same index (see Mollin [12]). We denote the common value of the indices of $A \otimes K_{\mathfrak{P}}$ for all K-primes $\mathfrak{P}$ above $\mathfrak{p}$ by $\mathrm{ind}_{\mathfrak{p}} A$, called the *$\mathfrak{p}$-local* index of A. The *uniform distribution group for K relative to L* is the subgroup of $B(K)$ consisting of classes having an algebra with uniformly distributed invariants relative to L. If $L = Q$ we let $U_Q(K) = U(K)$ and refer to this group as the *absolute uniform distribution group for K.*

The above is a generalization of Benard and Schacher [1, Th. 1, p. 280], (see also [16, Th. 6.1, p. 89]). In fact $S(K)$ is a subgroup of $U_L(K)$, (see Mollin [12]). In Mollin [8–13] the relationship between $S(K)$ and $U(K)$ for K/Q finite abelian is examined.

For a rational prime p let $S(K)_p$ denote the p-primary part of $S(K)$. We let K/Q be finite abelian and $Q(\varepsilon_{p^a}) \subseteq K \subseteq Q(\varepsilon_n)$ where p^a is the highest power of p dividing n. G. Janusz [7, Cor. 1, p. 350] shows that if p does not divide $|Q(\varepsilon_n) : K|$ then:

$$S(K)_p = K \otimes S(Q(\varepsilon_{p^a}))_p \tag{4.3}$$

where the tensor product is taken over $Q(\varepsilon_{p^a})$.

In Mollin [8] it is shown that if p does not divide $|K: Q(\varepsilon_{p^a})|$ then:

$$U(K)_p = S(K)_p = K \otimes S(Q(\varepsilon_{p^a}))_p \ . \tag{4.4}$$

That is, every element in $U(K)_p$ is in fact an element of $S(K)_p$ and is of the form $[K \otimes A]$ where $[A] \in S(Q(\varepsilon_{p^a}))_p$.

C. Ford and G. Janusz [5] give, for each prime p, examples of fields K for which (4.3) does not hold. Following Ford and Janusz we present, for each prime p, fields K for which the second equality of (4.4) does not hold but for which the first equality does hold.

We let $m = p \cdot s$ where p and s are odd rational primes with $s \equiv 1 \pmod{p}$ and $L = Q(\varepsilon_m)$ with $\langle \tau \rangle = G(L/Q(\varepsilon_p))$. We let K be the fixed field of $\langle \sigma \rangle$ where $\sigma = \tau^{(s-1)/p}$.

THEOREM 4.5. (1) *If* $s \equiv 1 \pmod{p^2}$ *then* A, *where* $[A] \in S(K)_p$, *is not similar to* $K \otimes B$ *for all* $[B] \in S(Q(\varepsilon_p))_p = U(Q(\varepsilon_p))_p$. *In particular*:

$$S(K)_p \neq K \otimes S(Q(\varepsilon_p))_p \ .$$

Moreover: $U(K)_p = S(K)_p$.

(2) *If* $s \not\equiv 1 \pmod{p^2}$ *then*

$$U(K)_p = S(K)_p = K \otimes S(Q(\varepsilon_p))_p \ .$$

Proof. (1) First we show that $U(K)_p = S(K)_p$. By Mollin, [8], if $[A] \in U(K)_p$ with $\mathrm{ind}_q(A) > 1$ for some prime q then $q \equiv 1 \pmod{p}$ and conversely, given a prime $q \equiv 1 \pmod{p}$ there exists $[A] \in U(K)_p$ with $\mathrm{ind}_q(A) = p$ and $\mathrm{ind}_t(A) = 1$ for all primes $t \neq q$. We note that the latter does not necessarily hold for $p = 2$. Now, that $[A]$ is in fact in $S(K)_p$ follows from Janusz [4, Th. 3, p. 267], and since the list of notation needed to state the aforementioned theorem is longer than the proof we do not reproduce it here, but rather leave the reader to verify the technical details.

Thus we have $U(K)_p = S(K)_p$. Now we show $S(K)_p \neq K \otimes S(Q(\varepsilon_p))_p$.

Assume $S(K)_p = K \otimes S(Q(\varepsilon_p))_p$. Since $[A] \in S(K)_p$ then $[A] = [K \otimes B]$ where $[B] \in S(Q(\varepsilon_p))_p$. Now let $\mathfrak{P}$ be a K-prime above the $Q(\varepsilon_p)$-prime $\mathfrak{p}$ which lies over q. Then:

$$\mathrm{inv}_{\mathfrak{P}}(A) \equiv |K_{\mathfrak{P}}: Q_q(\varepsilon_p)| \, \mathrm{inv}_{\mathfrak{P}} B \pmod{1}$$

(see Deuring [3]).

However, $p \mid |K_{\mathfrak{P}}: Q_q(\varepsilon_p)|$ and $\mathrm{ind}_{\mathfrak{P}} B \leqq p$ (see Mollin [7]). Thus

$\text{inv}_{\mathfrak{P}} A = 0$, a contradiction. Hence

$$S(K)_p \neq K \otimes S(Q(\varepsilon_p))_p .$$

(2) $q \equiv 1 \pmod{p^2}$ then p does not divide $|K: Q(\varepsilon_p)|$ then by Mollin [6] $U(K)_p = S(K)_p = S(Q(\varepsilon_p))_p \otimes K$.

To find examples for the case $p = 2$ we invoke Yamada [16, Th. 7.8, p. 107] from which it follows that if $K = Q(\sqrt{d})$ is a real quadratic field with d not divisible by a prime congruent to 3 modulo 4 then $U(K) = S(K) \neq S(Q) \otimes K$. We have $U(K) = U(K)_2$ and $S(K) = S(K)_2$ by (4.1). We now have fields K such that $U(K)_2 = S(K)_2 \neq S(Q) \otimes K$. If d is divisible by a prime congruent to 3 modulo 4 then $U(K)_2 \neq S(K)_2 = S(Q) \otimes K$, thus completing our task.

5. The decomposition theorem.

DEFINITION 5.1. Let $S(K, q)_p$, (respectively $U(K, q)_p$) denote the subgroup of $S(K)_p$ consisting of all elements having t-local index 1 for $t \neq q$.

Janusz [6, p. 254] notes that one would like (for neatness sake) to assert that $S(K)_p$ is the direct sum of groups $S(K, q)_p$ as q ranges over all primes. This, however, he proves is not in general true. We prove that for p odd we get:

THEOREM 5.2. *$U(K)_p$ is the direct sum of groups $U(K, q)_p$ as q ranges over all primes.*

Proof. By Mollin [8] there exists $[A(q)] \in U(K)_p$ with $\text{ind}_q A(q) = p^a$ and $\text{ind}_t A(q) = 1$ for all primes $t \neq q$ where p^a is the highest p-power root of unity in K. Thus, it follows that any $[A] \in U(K)_p$ has the form $A = \pi A(q)^{c_q}$.

REFERENCES

1. M. Benard and M. Schacher, *The Schur subgroup II*, J. Algebra, **22** (1972), 378-385.
2. M. Deuring, *Algebren*, second edition, Springer Verlag, Berlin, 1968.
3. L. Dornhoff, *Group Representation Theory*, Part a., Marcel Dekker Inc., New York, 1971.
4. B. Fein and B. Gordon, *Fields generated by characters of finite groups*, J. London Math. Soc., (2), **4** (1972), 735-740.
5. C. Ford and G. Janusz, *Examples in the theory of the Schur group*, Bull. Amer. Math. Soc., **79** (1973), 1233-1235.
6. G. Janusz, *The Schur group of an algebraic number field*, Annals of Math., **103** (1976), 253-281.
7. ———, *The Schur group of cyclotomic fields*, J. Number Theory, **7** (1975), 345-352.
8. R. Mollin, *Algebras with uniformly distributed invariants*, J. Algebra, **44** (1977), 271-282.
9. ———, *Uniform distribution and the Schur subgroup*, J. Algebra, **42** (1976),

261-277.
10. R. Mollin, *Uniform distribution and real fields*, J. Algebra, **43** (1976), 155-167.
11. ———, *U(K) for a quadratic field K*, Communications in Algebra, **4** (8), (1976), 747-759.
12. ———, *Generalized uniform distribution of Hasse invariants*, Communications in Algebra, **5** (3), (1977), 245-266.
13. ———, *Herstein's conjecture, automorphisms, and the Schur group*, Communications in Algebra, **6** (3), (1978), 237-248.
14. I. Reiner, *Maximal Orders*, Academic Press, New York, 1975.
15. P. Ribenboim, *Algebraic Numbers*, Wiley-Interscience, New York, 1972.
16. T. Yamada, *The Schur Subgroup of the Brauer Group*, Lecture Notes in Mathematics, No. 397, Springer-Verlag, 1974.
17. H. J. Zassenhaus, *The Theory of Groups*, 2nd Ed., Chelsea, New York, 1958.

Received July 15, 1977.

UNIVERSITY OF TORONTO
TORONTO, ONTARIO, M5S 1A1