BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 6, November 1973

EXAMPLES IN THE THEORY OF THE SCHUR GROUP

BY CHARLES FORD AND GERALD JANUSZ

Communicated by Joseph J. Rotman, April 23, 1973

Let K be a subfield of a cyclotomic extension of the rational field Q. The Schur group of K is the subgroup $S(K)$ of the Brauer group of K consisting of those classes of central simple K algebras represented by an algebra which appears as a direct summand of a group algebra $Q[G]$ for some finite group G. For a prime p let $S(K)_p$ denote the subgroup consisting of elements having p-power order. It is known by [1] that $S(K)_p$ can have an element of order p^a only when a primitive p^a root of unity, ε_{p^a}, is in K.

Suppose K is a field which satisfies $Q(\varepsilon_{p^a}) \subseteq K \subseteq Q(\varepsilon_n)$ and p^a is the highest power of p dividing n. It is known that

$$S(K)_p = K \otimes S(Q(\varepsilon_{p^a}))_p \tag{1}$$

in the case $K = Q(\varepsilon_n)$. That is every element in $S(K)_p$ is represented by an algebra $K \otimes B$ with B central simple over $Q(\varepsilon_{p^a})$ [2].

The assertion (1) also holds for K if p does not divide $(Q(\varepsilon_n): K)$. In this paper we present, for each prime p, fields K for which (1) does not hold.

Let p be a prime and r and s distinct primes such that $r \equiv s \equiv 1 \bmod p$. Then the field $L = Q(\varepsilon_p, \varepsilon_r, \varepsilon_s)$ has two nontrivial automorphisms σ, τ which satisfy

(i) $\sigma^p = \tau^p = 1$

(ii) σ fixes ε_p and ε_r; τ fixes ε_p and ε_s.

Let K be the subfield of L fixed by $\langle \sigma, \tau \rangle$. Let A be the algebra defined by

$$A = \sum L u_\sigma^i u_\tau^j;$$

$$u_\sigma^p = u_\tau^p = 1, \qquad u_\sigma u_\tau = \varepsilon_p u_\tau u_\sigma;$$

$$u_\sigma x = \sigma(x) u_\sigma, \qquad u_\tau x = \tau(x) u_\tau \quad \text{for } x \text{ in } L.$$

Then A is central simple over K and is a simple component of the group algebra $Q[G]$ where G is the group of order $p^3 rs$ generated by u_σ, u_τ, ε_{prs}. We use this algebra for several examples.

Let f_r be the exponent of r mod s; that is, f_r is the least positive integer f such that $r^f \equiv 1 \bmod s$. Similarly let f_s be the exponent of s mod r.

THEOREM. (1) *If $p \mid f_r$ then the r-local index of A is p. In particular A has index p if either $p \mid f_r$ or $p \mid f_s$.*

(2) *If A has r-local index p and p^2 divides either $r - 1$ or f_r then A is not*

AMS (MOS) subject classifications (1970). Primary 16A26; Secondary16A40, 20C05.

similar to $K \otimes B$ for any $Q(\varepsilon_p)$-central simple algebra B in $S(Q(\varepsilon_p))$. In particular, $S(K)_p \neq K \otimes S(Q(\varepsilon_p))_p$.

We remark that when p^2 does not divide either $r - 1$ or $s - 1$ then A is similar to $K \otimes B$ with B representing a class in $S(Q(\varepsilon_p))$. In fact B can be explicitly described as follows. Let the Galois group of $Q(\varepsilon_p, \varepsilon_r, \varepsilon_s) = L$ over $Q(\varepsilon_p)$ be $\langle \alpha, \beta \rangle$ where α has order $r - 1$ and fixes ε_s while β has order $s - 1$ and fixes ε_r. Then

$$B = \sum L u_\alpha^i u_\beta^j;$$
$$u_\alpha^{r-1} = u_\beta^{s-1} = 1, \qquad u_\alpha u_\beta = \varepsilon u_\beta u_\alpha;$$
$$u_\alpha x = \alpha(x) u_\alpha, \qquad u_\beta x = \beta(x) u_\beta \quad \text{for } x \in L.$$

Here ε is a suitable power of ε_p.

It should be observed also that for any prime p, there exist primes r, s which satisfy the conditions in (2) of the theorem. In fact a little more can be said. Let p be any prime and m a positive integer. By Dirichlet's theorem there exist infinitely many primes r which satisfy $r \equiv 1 \bmod p^m$. Now for any such r there exist infinitely many primes s such that $s \equiv 1 \bmod p^m$ and the exponent of s mod r equals p^m. In fact the Dirichlet density of the set of such s is $1/(r - 1)$.

One specific case where condition (2) holds occurs with $p = 3$, $r = 7$, $s = 37$. Then $f_r = 9$ and $f_s = 3$.

Suppose we construct the algebra A as above using p, r, s and $m \geqq 2$ which satisfy the divisibility conditions just above. Let p^b and p^c be the highest power of p dividing $r - 1$ and $s - 1$ respectively. Suppose p^d is the highest power of p dividing f_r and $p^m = f_s$. Notice $b, c \geqq m$. Then p^{b+d} and p^{c+m} are the exact powers of p dividing $r^{f_r} - 1$ and $s^{f_s} - 1$ respectively. The algebra A has index p and we ask for which values of n will $K(\varepsilon_{p^n})$ be a splitting field for A? In case $d = 0$ the least n for which $K(\varepsilon_{p^n})$ splits A is $n = c + m$. In case $d \neq 0$ then the least n is the larger of the numbers $b + d$ and $c + m$. In any case the least n is larger than m.

We formulate this more abstractly as follows.

THEOREM. *Given a prime p and an integer $m \geqq 2$ there exists a finite group G and a simple direct summand A of $Q[G]$ having center K and index p such that*

(i) $\varepsilon_p \in K$, $\varepsilon_{p^2} \notin K$,

(ii) *for some integer $n > m$, $K(\varepsilon_{p^n})$ is a splitting field for A but no proper subfield is a splitting field.*

By the general theory of algebras we know A has a splitting field E such that $(E:K) = p$. Here $(K(\varepsilon_{p^n}):K) = p^{n-1}$ can be made as large as desired by selecting suitable G and yet $K(\varepsilon_{p^n})$ is a "minimal splitting field" in the sense that no proper subfield splits the algebra.

References

1. M. Benard and M. Schacher, *The Schur subgroup*. II, J. Algebra **22** (1972), 378–385.
2. G. J. Janusz, *The Schur group of cyclotomic fields*, J. Number Theory (to appear).

Department of Mathematics, Washington University, St. Louis, Missouri 63130

Department of Mathematics, University of Illinois, Urbana, Illinois 61801