PACIFIC JOURNAL OF MATHEMATICS
Vol. 69, No. 1, 1977

CALCULATIONS OF THE SCHUR GROUP

J. WILLIAM PENDERGRASS

Let the field K be an abelian extension of the rational field Q. The Schur group of K, $S(K)$, consists of those classes in the Brauer group of K which contain an algebra isomorphic to a simple component of a rational group algebra QG for some finite group G.

Suppose that K has a cyclic extension of the form $Q(\zeta)$ where ζ is a primitive nth root of unity. In this paper we calculate the 2-part of $S(K)$ where K contains the fourth roots of unity.

An interesting facet of these results is that in some cases certain local indices of classes in $S(K)$ are tied together. That is, a class in $S(K)$ must have a nontrivial local index at an even number of the primes in a certain set. The tying together of local indices in these fields is caused by quadratic reciprocity and is not found in the q-part of $S(K)$ where q is an odd prime number.

Let $[A]$ be the class in the Brauer group of K which contains the K-central simple algebra A. The Hasse invariant of $[A]$ at a prime $\mathfrak{G}$ of K is denoted $\text{inv}_{\mathfrak{G}}[A]$. Benard and Schacher [2] showed that each class $[A]$ in $S(K)$ has uniformly distributed invariants. That is, if the index of $[A]$ is I, and $\sigma(\varepsilon_I) = \varepsilon_I^{\lambda}$ where ε_I is a primitive Ith root of unity and $\sigma \in \text{Gal}(K/Q)$, then $\text{inv}_{\mathfrak{G}}[A] = \lambda \, \text{inv}_{\sigma(\mathfrak{G})}[A]$ for each prime $\mathfrak{G}$ in K. A corollary of this result is that the local index of a class $[A]$ in $S(K)$ is the same at each of the primes of K which divide a single rational prime p. This common index is called the p-local index of $[A]$.

Set $L = Q(\xi)$ where ξ is a primitive $2^s n$th root of unity, $(2, n) = 1$. Let K be a field contained in L such that $\text{Gal}(L/K) = \langle \phi \rangle$ is a cyclic group of order $2^t t'$, $(2, t') = 1$. Let ζ be a primitive 2^sth root of unity and suppose that $\phi(\zeta) = \zeta^h$ where $h = 5^{2^{r-2}}$. Thus the 2^rth roots of unity lie in K. A theorem of Benard and Schacher [2] implies that the exponent of the 2-part of $S(K)$ is at most 2^r.

Observe that there can be at most one rational prime p with even ramification index in L/K. This follows from the fact that the inertia group of a divisor of p is contained in $\text{Gal}(L/K(\varepsilon))$ where ε is a root of unity in L having largest possible order not divisible by p. If p is such a prime, then let:

2^k exactly divide $p - 1$,

2^e exactly divide $e(p, L/K)$,

2^d exactly divide $f(p, K/Q)$,

where $e(p, L/K)$ is the ramification index of p in L/K and $f(p, K/Q)$ is the residue class degree of p in K/Q.

Now suppose that q is a prime which does not divide $2n$. We shall use the following notation:

$2^{\ell(q)}$ exactly divides $q - 1$,

$2^{b(q)}$ exactly divides $f(q, K/Q)$,

$2^{a(q)}$ exactly divides $A(q)$ where $\phi^{A(q)} = [L/K, q]$ is the Frobenius automorphism of q in L/K,

$2^{v(q)}$ exactly divides $V(q)$ where $h^{A(q)} - q^{f(q,K/Q)} = V(q)2^s$.

In addition, for any prime p we denote $p^{f(p,K/Q)} - 1$ by $\Gamma(p)$.

Finally let $\lambda = \max\{s - t, 0\}$.

THEOREM. *The 2-part of $S(K)$ consists of those classes $[A]$ in the Brauer group of K which have uniformly distributed invariants which satisfy the following conditions.*

(I) *If q does not divide n, then the q-invariants of $[A]$ are integral multiples of $1/2^{I(q)}$ where*

$$I(q) = \begin{cases} \max\{r - b(q), \ell(q) - v(q), 0\} & \text{if } \ell(q) \leqq r - \lambda \\ \max\{r - b(q), r - \lambda - v(q), 0\} & \text{if } \ell(q) \geqq r - \lambda . \end{cases}$$

(II) *If p divides n, then the p-invariants of $[A]$ are integral multiples of $1/2^{I(p)}$ where*

$$I(p) = \begin{cases} 0 & \text{if } p = 2 \text{ or if } e(p, L/K) \text{ is odd} \\ \max\{c - d + r - k, c - d + s - t - \lambda, 0\} & \text{otherwise.} \end{cases}$$

(III) *Suppose that p divides n and $I(p) \neq 0$. If* $\cdot k > s$, $k \neq t$, *and $2^{k+s-t-\lambda}$ is greater than the power of 2 which divides $p' - 1$ for all primes $p' \neq p$ which divide n, then the q-invariants of $[A]$ are odd multiples of $1/2^{I(q)}$ for an even number of primes q in the set.*

$$\{p\} \cup \{q\colon (q/p) = -1, (q, 2n) = 1, \text{ and } \ell(q) \geqq r - \lambda\}$$

where (q/p) is the Legendre symbol.

Proof. Let $K' \supset K$ be the field such that $[L\colon K'] = 2^t$. Then Lemma 2 of [5] implies that the set of permissible invariants for elements in the 2-part of $S(K)$ is exactly the set of permissible invariants for elements in the 2-part of $S(K')$. Thus we may assume that $[L\colon K] = 2^t$ without any loss of generality.

Now we must determine the invariants of the crossed product algebras of the form

$$[L(\varepsilon_q)/K, \alpha] = \sum L(\varepsilon_q)u_\sigma\,, \quad \sigma \in \mathrm{Gal}\,(L(\varepsilon_q)/K)$$

where ε_q is a primitive qth root of unity, q is an odd prime which does not divide n, and α is a factor set from $\mathrm{Gal}(L(\varepsilon_q)/K) \times \mathrm{Gal}(L(\varepsilon_q)/K)$ into $\langle\zeta\rangle$. The multiplication in these algebras is given by

$$u_\sigma u_\tau = \alpha(\sigma, \tau)u_{\sigma\tau} ,$$
$$u_\sigma w = \sigma(w)u_\sigma ,$$

for $\sigma, \tau \in \mathrm{Gal}(L(\varepsilon_q)/K)$ and $w \in L(\varepsilon_q)$. We know from Theorem 1 of [5] that the classes in the Brauer group of K which contain these classes generate the 2-part of $S(K)$.

Let $\Delta_q = \Delta_q(x, y, z)$ be the algebra $(L(\varepsilon_q)/K, \alpha)$ where the values of α are in $\langle\zeta\rangle$ and q is an odd prime not dividing n. Set $\mathrm{Gal}(L(\varepsilon_q)/L) = \langle\gamma\rangle$. The factor set α is determined by the integers x, y, and z where

$$u_\gamma u_\phi = \zeta^x u_\phi u_\gamma ,$$
$$(u_\gamma)^{q-1} = \zeta^y ,$$
$$(u_\phi)^{2^t} = \zeta^z .$$

We must have

$$u_\phi(\zeta^z) = \phi(\zeta^z)u_\phi = \zeta^z u_\phi ,$$
$$u_\gamma(\zeta^y) = \gamma(\zeta^y)u_\gamma = \zeta^y u_\gamma ,$$
$$(u_\gamma u_\phi u_\gamma^{-1})^{2^t} = (\zeta^x u_\phi)^{2^t} ,$$
$$(u_\phi u_\gamma u_\phi^{-1})^{q-1} = (\zeta^{-x} u_\gamma)^{q-1} .$$

Thus

(1)
(a) 2^{s-r} divides z,
(b) 2^λ divides x,
(c) $y(h-1) + x(q-1) = Y2^s$ for some integer Y.

The Frobenius automorphism of q in L/K is $\phi^{A(q)}$. Thus

$$\phi^{A(q)}(\zeta) = \zeta^{h^{A(q)}} = \zeta^{q^{f(q,K\ Q)}} .$$

Hence

$$h^{A(q)} - q^{f(q,K/Q)} = V2^s \text{ for some integer } V.$$

Now applying Theorem 3 of [6] we get that the q-local index of $[\Delta_q]$ is given by

$$\frac{q-1}{(\nu(q)(q-1),\, q-1)}$$

where

(2)
(a) $$\nu(q) = \frac{1}{2^s}\left[x\frac{h^{A(q)}-1}{h-1} + y\frac{\Gamma(q)}{q-1}\right]$$
(b) $$= \frac{1}{h-1}\left[Y\frac{\Gamma(q)}{q-1} - xV\right].$$

Thus, since 2^r exactly divides $h-1$, the q-local index of $[\Delta_q]$ is $\max\{2^{r-\mu}, 1\}$ where 2^μ exactly divides $Y\Gamma(q)/(q-1) - xV$.

We know that $2^{b(q)}$ exactly divides $\Gamma(q)/(q-1)$. Moreover, we may make Y either odd or even without changing the power of 2 which divides x. If $\ell(q) \leqq r - \lambda$, then equation (1)(c) implies that $2^{r-l(q)}$ is the smallest power of 2 which can divide x. If $\ell \geqq r - \lambda$, then 2^λ is the least power of 2 which can divide x. Thus, the maximum q-local index of $[\Delta^q]$ is $2^{I(q)}$ where

$$I(q) = \begin{cases} \max\{r - b(q), \ell(q) - v(q), 0\} & \text{if } \ell(q) \leqq r - \lambda \\ \max\{r - b(q), r - \lambda - v(q), 0\} & \text{if } \ell(q) \geqq r - \lambda\,. \end{cases}$$

Now observe that for any prime q' which does not divide $2nq$, q is unramified in $L(\varepsilon_{q'})/K$. Thus the q-invariants of $[\Delta_{q'}]$ must be zero. This means that the only classes amongst the generators of the 2-part of $S(K)$ which have non-zero invariants at the primes of K dividing q are those classes of the form $[\Delta_q(x, y, z)]$. Thus we have proved (I).

If there is no prime which ramifies in L/K, then $[\Delta_q]$ can have nonzero invariants only at the primes of K which divide q. If 2 ramifies in L/K, it must be the only prime which ramifies in L/K. So, since the 2-invariants of any class in $S(K)$ must be zero by the results of Yamada [7], the only nonzero invariants that $[\Delta_q]$ can have are at the primes of K which divide q. In both of these cases we are done and the theorem is proved.

So for the remainder of the proof let p be an odd prime which is ramified in L/K. Set $\phi^{g'}\gamma^{g}$ equal to a Frobenius automorphism for p in $L(\varepsilon_q)/K$. Observe that $\phi^{2^{t-c}}$ generates the inertia group of p in L/K where $2^c = e(p, L/K)$.

Applying Theorem 3 of [6] we get that the p-local index of $[\Delta_q]$ is given by

$$\frac{2^c}{(2^c\nu(p), 2^c)}$$

where

$$\nu(p) = \frac{1}{2^s}\left[-xg\frac{h^{2^{t-c}} - 1}{h-1} + z\frac{\Gamma(p)}{2^c}\right].$$

Thus the p-local index of $[\Delta_q]$ is $\max\{2^{s-\eta}, 1\}$ where 2^η exactly divides

$$-xg\frac{h^{2^{t-c}} - 1}{h-1} + z\frac{\Gamma(p)}{2^c}\,.$$

We know that 2^{t-c} exactly divides $(h^{2^{t-c}} - 1)/(h-1)$, that 2^{k+d-c} exactly divides $\Gamma(p)/2^c$, and that 2^{s-r} is the least power of 2 which divides z. Hence we need to find the smallest power of 2 which divides xg.

We know that g must be an $f(p, K/Q)$th power, so picking q such that $(q/p) = -1$ we get that $\min\{2^d, 2^{\ell(q)}\}$ is the smallest power of 2 which can divide g. If $\ell(q) \geqq r - \lambda$, then 2^λ must divide x, and if $\ell(q) \leqq r - \lambda$, then $2^{r-\ell(q)}$ must divide x. Hence we find that $\min\{2^{\lambda+d}, 2^r\}$ is the smallest power of 2 which can exactly divide xg. Thus the maximum p-local index of a class in the 2-part of $S(K)$ is $2^{I(p)}$ where

$$\begin{aligned} I(p) &= \max\{c - d + s - t - \lambda,\ c - t + s - r,\ c - d + r - k,\ 0\} \\ &= \max\{c - d + s - t - \lambda,\ c - d + r - k,\ 0\} \end{aligned}$$

since $c \leqq t - (s - r)$. This proves (II).

If $I(p) = 0$, then we are finished. So assume for the rest of the proof that $I(p) > 0$.

Now assume that $k > s$, $k \neq t$, and $2^{k+s-t-\lambda}$ is greater than the power of 2 which divides $p' - 1$ for all primes p' which are unequal to p and which divide n.

Suppose that the p-local index of $[\Delta_q(x, y, z)]$ is $2^{I(p)}$. Now $s - t - \lambda > r - k$ so $I(p) = c - d + s - t - \lambda$. Thus $2^{\lambda+d}$ exactly divides xg, indeed 2^λ must exactly divide x and 2^d must exactly divide g. Thus $\ell(q) \geqq r - \lambda$ and $(q/p) = -1$. Further, since $p \equiv 1 \bmod 4$, $(p/q) = -1$ by the law of quadratic reciprocity. This, together with the hypotheses, implies that $b(q) = k - t + a(q)$ where $2^{b(q)}$ exactly divides $f(q, K/Q)$ and $a(q)$ exactly divides $A(q)$. Hence $\ell(q) + b(q) > r + a(q)$. So, since $2^{\ell(q)+b(q)}$ exactly divides $q^{f(q)} - 1$ and $2^{r+a(q)}$ exactly divides $h^{A(q)} - 1$, we get that $r + a(q) = s + v(q)$. Thus

$$r - b(q) = r - k + t - a(q) < r - \lambda - a(q) \leqq r - \lambda - v(q)\,.$$

Hence $I(q) = r - \lambda - v(q)$ and the q-local index of $[\Delta_q(x, y, z)]$ is $2^{I(q)}$. Observe that $I(q) > 0$ since the hypotheses insure that $a(q) < s - \lambda$, so that $v(q) < r - \lambda$.

Now let q be a prime such that $(q/p) = -1$, $(q, 2n) = 1$, and $\ell(q) \geqq r - \lambda$. Suppose that the q-local index of $[\Delta_q(x, y, z)]$ is $2^{I(q)}$. We have seen that $I(q)$ is positive and is equal to $r - \lambda - v(q)$ in this instance. Hence 2^λ must exactly divide x by equation (2)(b). Thus the p-local index of $[\Delta_q(x, y, z)]$ is greater than or equal to $2^{c-d+s-t-\lambda}$. However $I(p) = c - d + s - t - \lambda > 0$, so the p-local index of $[\Delta_q(x, y, z)]$ must be $2^{I(p)}$.

We have now shown that under the hypotheses of (III), the p-local index of $[\Delta_q]$ is $2^{I(p)}$ if and only if $(q/p) = -1$, $\ell(q) \geqq r - \lambda$, and the q-local index of $[\Delta_q]$ is $2^{I(q)}$. This proves (III).

We now need to show that the restrictions on the invariants of elements in the 2-part of $S(K)$ given in the theorem are the only restrictions on the invariants of elements in the 2-part of $S(K)$.

First assume that the hypotheses of (III) hold. Let $F = Q(\varepsilon_p, \varepsilon_{2^s+1}, \sqrt[4]{p})$ and let σ be the element in $\mathrm{Gal}(F/Q)$ such that $\sigma(\varepsilon_p) = \varepsilon_p^{-1}$, $\sigma(\sqrt[4]{p}) = -\sqrt[4]{p}$, and $\sigma(\varepsilon_{2^s+1}) = (\varepsilon_{2^s+1})^\beta$ where $\beta = 5^{2^{s-2}}$. Such a σ exists since p does not have a fourth root in $Q(\varepsilon_p, \varepsilon_{2^s+1})$. Let q be a prime not dividing n whose Frobenius automorphism in F/K is σ. There are infinitely many such primes by the Tchebotarev density theorem. This means that 2^s exactly divides $q-1$, 2 exactly divides $f(q, Q(\varepsilon_p)/Q)$, and 2^{s-1} exactly divides $f(p, Q(\varepsilon_q)/Q)$. Thus the Frobenius automorphism of q in L/K is an odd power of $\phi^{2^{t-1}}$ if $f(q, K/Q)$ is odd, and it is 1 if $f(q, K/Q)$ is even. So we have that $a(q) = t-1$ if $f(q, K/Q)$ is odd, and $a(q) = 0$ if $f(q, K/Q)$ is even. Further $\ell(q) \geqq r - \lambda$.

Now the algebra class $[\Delta_q(2^\lambda, 0, 0)]$ has q-local index 1 if $f(q, K/Q)$ is even and $[\Delta_q(2^\lambda, 2^{s-1}, 0)]$ has q-local index 1 if $f(q, K/Q)$ is odd. This follows from equation (2)(a). Now both of these algebra classes have p-local index $2^{\Gamma(p)-1}$ since $2^{\lambda+d+1}$ divides xg in both cases. Thus the algebra class which has local index $2^{\Gamma(p)-1}$ at p and local index 1 at all other primes is in $S(K)$. This implies that there are no further restrictions on the 2-part of $S(K)$ in the case where the hypotheses of (III) hold.

Now assume that either $k \leqq s$ or $k = t > s$. Let ψ_p be a generator of $\mathrm{Gal}(L/Q(\zeta, \varepsilon_{n^*}))$ where $(n^*, p) = 1$ and n/n^* is a power of p. Also set ψ equal to the automorphism in $\mathrm{Gal}(L/Q(\varepsilon_n))$ which sends ζ to ζ^5. Now let q' be a prime whose Frobenius automorphism in L/Q is $\psi_p\psi^{2^{r+t-k-2}}$. This implies that $(q'/p) = (p/q') = -1$, that 2^{r+t-k} exactly divides $q'-1$, and that 2^{a+k-t} exactly divides $f(q', K/Q)$. Consider the algebra class $[\Delta_{q'}(x_0, y_0, 0]$ where

$$x_0 \equiv 2^{\lambda-b(q')}\left[\frac{\Gamma(q')}{q'-1}\right] \bmod 2^s$$

and

$$y_0 \equiv -2^{\lambda-b(q')}\left[\frac{h^{A(q')}-1}{h-1}\right] \bmod 2^s \,.$$

Observe that $x_0(q'-1) + y_0(h-1) \equiv 0 \bmod 2^s$ so that equation (1)(c) is satisfied. Now we have that

$$x_0\left[\frac{h^{A(q')}-1}{h-1}\right] + y_0\left[\frac{\Gamma(q')}{q'-1}\right] \equiv 0 \bmod 2^s \,.$$

Hence the q'-local index of $[\Delta_{q'}(x_0, y_0, 0)]$ is 1. Further, 2^λ exactly divides x_0, $2^{r-\lambda}$ divides $q'-1$, and $(q'/p) = -1$. Thus the p-local index of $[\Delta_{q'}(x_0, y_0, 0)]$ is $\max\{2^{c-d+s-t-\lambda}, 1\}$.

Now consider the algebra class $[\Delta_{q'}(0, 0, 2^{s-r})]$. Its q'-local index is 1 and its p-local index is $\max\{2^{c-d+r-k}, 1\}$.

Thus $S(K)$ contains the algebra class with local index $2^{I(p)}$ at p and local index 1 at all other primes. This implies that there are no extra restrictions on the 2-part of $S(K)$ when either $k \leqq s$ or $k = t$.

Finally assume that $k > s$, $k \neq t$, and that there is a prime $p' \neq p$ which divides n such that $2^{k+s-t-\lambda}$ divides $p' - 1$. Let $\psi_{p'}$ be a generator of $\mathrm{Gal}(L/Q(\zeta, \varepsilon_{n'}))$ where $(n', p') = 1$ and n/n' is a power of p'. Let ψ_p be as above.

Let q'' be a prime whose Frobenius automorphism in L/Q is $\psi_p\psi_{p'}$. Thus $(q''/p) = -1$ and 2^s divides $q'' - 1$. Further observe that if β is the smallest integer such that $(\psi_p\psi_{p'})^\beta \in \mathrm{Gal}(L/K)$, then $2^{k+s-t-\lambda}$ must divide β. Hence $a(q'') \geqq s - \lambda$. Thus $[\Delta_{q''}(2^\lambda, 0, 0)]$ has q''-local index 1 and p-local index $2^{c-d+s-t-\lambda}$. Since $k > s \geqq r$, we have that $I(p) = c - d + s - t - \lambda$. So $S(K)$ contains an algebra with local index $2^{I(p)}$ at p and local index 1 at all other primes. This implies that there are no further restrictions on the 2-part of $S(K)$ in this case.

This completes the proof to the theorem.

REFERENCES

1. M. Benard, *The Schur subgroup I*, J. of Algebra, **22** No. 2 (1972), 374–377.
2. M. Benard and M. Schacher, *The Schur subgroup II*, J. of Algebra, **22**, No. 2 (1972), 378–385.
3. G. J. Januz, *Generators for the Schur group of local and global number fields*, Pacific J. Math., (to appear).
4. ———, *The Schur group of an algebraic number field*, University of Illinois preprint, Urbana Ill. 1975.
5. J. W. Pendergrass, *The Schur subgroup of the Brauer group.*
6. Y. Yamada, *Characterization of the simple components of the group algebras over the p-adic number field*, J. Math. Soc. Japan, **23** (1971) 295–310.
7. ———, *Cyclotomic algebras over a 2-adic field*, Proc. Japan Acad., **49**, No. 6 (1973) 438–442.
8. ———, *The Schur subgroup of the Brauer group, I*, J. of Algebra, **27**, No. 3 (1973) 579–589.

Received February 14, 1975

NEW MEXICO STATE UNIVERSITY