PACIFIC JOURNAL OF MATHEMATICS
Vol. 77, No. 2, 1978

MINIMAL SPLITTING FIELDS FOR GROUP REPRESENTATIONS, II

BURTON FEIN

Let p be an arbitrary prime and m an arbitrary positive integer. A finite group G is constructed which has an irreducible complex representation T with character χ such that the Schur index of χ over Q is p but the minimum of $[K: Q(\chi)]$, taken over all abelian extensions K of Q in which T is realizable, is p^m.

Let Q denote the rationals and, for n a pasitive integer, let ε_n denote a primitive nth root of unity over Q. Let χ be the character afforded by a complex irreducible representation T of a finite group G of order n and let $m_Q(\chi)$ denote the Schur index of χ over Q. In view of the famous theorem of R. Brauer that T is realizable in $Q(\varepsilon_n)$, it is natural to ask how close to $m_Q(\chi)$ is $\min[L: Q(\chi)]$, where the minimum is taken over all subfields L of cyclotomic extensions of Q in which T is realizable. Our main result shows that the above minimum is not, in general, very close to $m_Q(\chi)$.

THEOREM 1. *Let p be an arbitrary prime and m an arbitrary positive integer. Then there exists a finite group G of exponent n and an irreducible complex representation T of G affording the character χ such that $m_Q(\chi) = p$ and $p^m = \min[L: Q(\chi)]$ where the minimum is taken over all abelian extensions L of Q in which T is realizable. The minimum is attained at a subfield of $Q(\varepsilon_n)$.*

There are several results in the recent literature that are similar in spirit to the above theorem. In [5], Schacher produces an example of a finite dimensional division algebra D with center an abelian extension of Q with the property that no maximal subfield of D is an abelian extension of Q. It can be shown, however, that his example does not arise from a group algebra of a finite group. Given an arbitrary prime p and an arbitrary integer $m \geqq 2$, Ford and Janusz in [3] produce an example of a complex irreducible representation T with character χ of a finite group G such that $m_Q(\chi) = p$, $\varepsilon_{p^2} \notin Q(\chi)$, and for some $r > m$, T is realizable in $Q(\chi)(\varepsilon_{p^r})$ but not in any proper subfield. It can be shown, however, that T is also realizable in a subfield L of $Q(\varepsilon_n)$, n the exponent of G, where $[L: Q(\chi)] = p$. In [2] an example is found of an irreducible complex representation T with character χ of a finite group G of order n with the property that T is not realizable in any subfield L of $Q(\varepsilon_n)$

with $[L: Q(\chi)] = m_Q(\chi)$. It turns out, however, that there exists a prime q and a subfield L of $Q(\varepsilon_{nq})$ with $[L: Q(\chi)] = m_Q(\chi)$ in which T is realizable. The example in this paper is obtained by suitably modifying the construction we gave in [2]; both the details of the construction and the verification of the properties asserted are much more complicated than in that paper.

Notation and Terminology. We denote the completion of an algebraic number field K at a prime π by K_π. If A is a simple component of a group algebra over Q, the center of A being K, and π_1 and π_2 are primes of K extending the rational prime p, then the indices of $A \otimes_K K_{\pi_1}$ and $A \otimes_K K_{\pi_2}$ are equal [6, Corollary 6.3]. We refer to this common value as the p-local index of A. If $L \supset K$ and L is an abelian extension of K, we refer to the local degree (respectively, residue class degree and ramification degree) of a prime π of K from K to L as the p-local degree (respectively, p-residue class degree and p-ramification degree) where π extends the rational prime p. We denote the Galois group of L over K by $\mathrm{Gal}(L/K)$. Let G be a finite group, T a complex irreducible representation of G, and χ the character afforded by T. We say that the simple component A of the group algebra of G over $Q(\chi)$ is associated with χ if the representation of G afforded by a minimal left ideal of A is equivalent to $m_Q(\chi)T$. The index of A equals $m_Q(\chi)$ and T is realizable in a field L if and only if L splits A. In this case, we say that L is a splitting field for χ.

Proof of Theorem 1. Let p be an arbitrary prime and m an arbitrary positive integer. Let r and s be primes with $r \equiv 1 + p^m \pmod{p^{m+1}}$ and $s \equiv 1 + p^{m-1} \pmod{p^m}$. Let $\gamma \in \mathrm{Gal}(Q(\varepsilon_s)/Q)$ have order p^{m-1}. By the Frobenius density theorem [4, Theorem 5.2], there is a prime q_0 whose Frobenius automorphism $[Q(\varepsilon_s)/Q/q_0]$ is γ. Let q be a prime with $q \equiv q_0 \pmod{s}$, $q \equiv 1 + p^{3m-1} \pmod{p^{3m}}$, and $q \equiv 1 \pmod{r}$.

Let F_0 be the subfield of $Q(\varepsilon_s)$ with $[Q(\varepsilon_s): F_0] = p^{m-1}$ and let F_1 be the subfield of $Q(\varepsilon_r)$ with $[Q(\varepsilon_r): F_1] = p^m$. Let $\langle\alpha\rangle = \mathrm{Gal}(Q(\varepsilon_{rs})/F_0(\varepsilon_r))$ and $\langle\beta\rangle = \mathrm{Gal}(Q(\varepsilon_{rs})/F_1(\varepsilon_s))$. Let K_0 be the fixed field of $Q(\varepsilon_{rs})$ under $\langle\alpha\beta\rangle$. Then $K_0 \cap F_0(\varepsilon_r) = K_0 \cap F_1(\varepsilon_s) = F_0(\varepsilon_r) \cap F_1(\varepsilon_s) = F_0F_1$ since an element in the first intersection, for example, will be invariant under both $\langle\alpha\rangle$ and $\langle\alpha\beta\rangle$ and so under $\langle\alpha, \beta\rangle$. $[K_0: F_0F_1] = p^{m-1}$ and $[Q(\varepsilon_{rs}): K_0] = p^m$.

Since $\equiv qq_0 \pmod{s}$, q splits completely in F_0. Since $q \equiv 1 \pmod{r}$, q also splits completely in $Q(\varepsilon_r)$ and so q splits completely from Q to $F_0(\varepsilon_r)$. Because of our choice of q_0, q is inertial from F_0F_1 to $F_1(\varepsilon_s)$. Thus q is unramified from F_0F_1 to $Q(\varepsilon_{rs})$ with residue class degree p^{m-1}. Since $K_0 \cap F_0(\varepsilon_r) = F_0F_1$ and $K_0(\varepsilon_r) = Q(\varepsilon_{rs})$, we see that q must be inertial from F_0F_1 to K_0. Thus q splits completely from K_0 to $Q(\varepsilon_{rs})$ and has residue class degree p^{m-1} from Q to K_0.

Let ζ denote a primitive $qrsp^{2m}$-th root of unity. Let E be the subfield of $Q(\varepsilon_q)$ with $[Q(\varepsilon_q): E] = p^{3m-1}$ and let $\langle\tau\rangle = \mathrm{Gal}(Q(\zeta)/E(\varepsilon_{rsp^{2m}}))$. Let $\langle\sigma\rangle = \mathrm{Gal}(Q(\zeta)/K_0(\varepsilon_{qp^{2m}}))$ and let K be the fixed field of $Q(\zeta)$ under $\langle\sigma\tau\rangle$. As before, $K \cap K_0(\varepsilon_{qp^{2m}}) = K \cap E(_{rsp^{2m}}) = K_0(\varepsilon_{qp^{2m}}) \cap E(\varepsilon_{rsp^{2m}}) = K_0E(\varepsilon_{p^{2m}})$. $[Q(\zeta): K] = p^{3m-1}$ and $[K: K_0E(\varepsilon_{p^{2m}})] = p^m$.

Since q splits completely from K_0 to $Q(\varepsilon_{rs})$, q splits completely from $K_0E(\varepsilon_{p^{2m}})$ to $E(_{rsp^{2m}})$. Since q is totally ramified from $K_0E(\varepsilon_{p^{2m}})$ to $K_0(\varepsilon_{qp^{2m}})$, we conclude that q must be totally ramified from $K_0E(\varepsilon_{p^{2m}})$ to K. Since $q \equiv 1 \pmod{p^{2m}}$ we have determined completely the behavior of q from Q to K and from K to $Q(\zeta)$: the q-ramification degree is p^m from Q to K and p^{2m-1} from K to $Q(\zeta)$ while the q-residue class degree is p^{m-1} from Q to K and 1 from K to $Q(\zeta)$. We also note that since $Q(\zeta) = K(\varepsilon_q)$, all primes except q are unramified from K to $Q(\zeta)$. Since $p^{2m} \geqq 4$, K is totally imaginary.

Let G by the finite group generated by w, x, y, and z subject to the following relations: $w^{p^{5m-1}} = x^q = y^r = z^s = (x, y) = (x, z) = (y, z) = 1$, $w^{p^{3m-1}}$ central in G, $w^{-1}xw = x^a$, $w^{-1}yw = y^b$, and $w^{-1}zw = z^c$ where $\tau(\varepsilon_q) = (\varepsilon_q)^a$, $\sigma(\varepsilon_r) = (\varepsilon_r)^b$, and $\sigma(\varepsilon_s) = (\varepsilon_s)^c$. The cyclic algebra $\mathscr{A} = (Q(\zeta), \sigma\tau, \varepsilon_{p^{2m}})$ is a homomorphic image of the group algebra of G over Q and so there exists a complex irreducible representation T of G with character χ such that the enveloping algebra of T is $\mathscr{A}$ and $Q(\chi) = K$. The index of $\mathscr{A}$ equals $m_Q(\chi)$.

Since $\mathscr{A}$ is a cyclotomic algebra over a totally imaginary field and only primes over q are ramified from K to $Q(\zeta)$, $\mathscr{A}$ can have nonzero Hasse invariant only at primes of K over q [6, Lemma 4.2]. Since the index of $\mathscr{A}$ is the least common multiple of the indices of $\mathscr{A} \otimes_K K_\pi$ over all primes π of K [1, VII, §5], we conclude that $m_Q(\chi)$ equals the q-local index of $\mathscr{A}$.

The q-local index of $\mathscr{A}$ can be computed from [2, Lemma, page 428]. Since p^{3m-1} is the exact power of p dividing $q - 1$ and the q-residue class degree from Q to K is p^{m-1}, we conclude that p^{4m-2} is the exact power of p dividing the order of the multiplicative group of the residue class field of K at q. Since the q-ramification degree from K to $Q(\zeta)$ is p^{2m-1}, we conclude that the q-local index of $\mathscr{A}$ is p. Thus $m_Q(\chi) = p$.

Let L be an abelian extension of Q which is a splitting field for $\mathscr{A}$ and suppose $[L: K] < p^m$. If $K \subset L_0 \subset L$ with $[L_0: K]$ being the full p-part of $[L: K]$, then L_0 must split $\mathscr{A}$ since $\mathscr{A} \otimes_K L_0$ must have index prime to p. Thus we may assume that $[L: K]$ is a power of p. Since L is abelian over Q, $L \subset Q(\varepsilon_b)$ for some b. We clearly may assume that p is the only prime whose square divides b. Since $L \supset K$, b is divisible by $p^{2m}qrs$ so we may write $b = qrsv$

where $(qrs, v) = 1$. Let W be the subfield of $K(\varepsilon_v)$, $W \supset K$, such that $[W: K]$ equals the full p-part of $[K(\varepsilon_v): K]$. Since $\varepsilon_{rs} \in K(\varepsilon_q) = Q(\zeta)$, we have $W(\varepsilon_q) \supset L$ and $W \cap K(\varepsilon_q) = K$. Thus $[W(\varepsilon_q): W] = [K(\varepsilon_q): K] = p^{3m-1}$. Since $\mathrm{Gal}(W(\varepsilon_q)/W)$ is cyclic of order p^{3m-1}, the subfields of $W(\varepsilon_q)$ containing W are linearly ordered and there is one such field for each p^i, $1 \leqq p^i \leqq p^{3m-1}$. Since $[K(\varepsilon_{rs}): K] = p^m$, $[W(\varepsilon_{rs}): W] = p^m$. Since we have assumed that $[L: K] < p^m$, $[WL: W] < p^m$ and so $WL \subset W(\varepsilon_{rs})$. Since $(q, vrs) = 1$, q is unramified from K to L and $L \subset W(\varepsilon_{rs})$.

Let the prime factorization of v be $p^i p_2 \cdots p_d$. Let $W_1, \cdots, W_d$ be subfields of W such that $K \subset W_1 \subset K(\varepsilon_{p^i})$, $K \subset W_j \subset K(\varepsilon_{p_j})$ for $j \geqq 2$, $L \subset W_1 W_2 \cdots W_d(\varepsilon_{rs})$, but L is not contained in any subfield $V_1 V_2 \cdots V_d(\varepsilon_{rs})$ where $V_j \subset W_j$, $j \geqq 1$, and V_j is a proper subfield of W_j for some j. Assume $|W_j| \geqq p^m$ for some j. Let V be the subfield of $W(\varepsilon_{rs})$ generated by the W_k with $k \neq j$ and by ε_{rs}. Let $Y = W_j$ and let $Y_0 \subset Y$ with $[Y_0: K] = p^{m-1}$. By the minimality assumption on the $\{W_j\}$, L is not a subfield of VY_0. Since $\mathrm{Gal}(YV/V)$ is a cyclic p-group, the fields intermediate between YV and V are linearly ordered. Since $Y \cap V = K$, $[Y_0 V: V] = [Y_0: K] = p^{m-1}$. $[LV: V] \leqq [L: K] \leqq p^{m-1}$ so $LV \subset Y_0 V$. But then $L \subset Y_0 V$, contradicting our minimality assumption.

We have shown that $[W_j: K] \leqq p^{m-1}$ for $j \geqq 1$. Since L splits $\mathscr{A}$, the q-local degree from K to L is divisible by p [1, VII, § 5]. Since q splits completely from K to $K(\varepsilon_{rs})$, the q-local degree from K to W_j must be divisible by p for some $j \geqq 1$. Since $W_1 \subset K(\varepsilon_{p^i})$ and $[W_1: K] \leqq p^{m-1}$, $W_1 \subset K(\varepsilon_{p^{3m-1}})$. But $q \equiv 1 \pmod{p^{3m-1}}$ and so the q-local degree from K to W_1 must be one.

We have now shown the existence of a prime t, $(t, pqrs) = 1$, such that there is a subfield S of $K(\varepsilon_t)$, $S \supset K$, with $[S: K] = p^g \leqq p^{m-1}$ and such that the q-local degree from K to S is divisible by p. Since $Q(\varepsilon_t) \cap K = Q$, $S = KS_0$ where $S_0 \subset Q(\varepsilon_t)$, $[S_0: Q] \leqq p^{m-1}$. But the q-residue class degree from Q to K is p^{m-1} and so the completion of S_0 at a prime extending q is contained in the completion of K at a prime extending q. This proves that the q-local degree from K to $KS_0 = S$ is 1 and so we conclude that $[L: K] \geqq p^m$. Finally, we note that since $q \equiv 1 \pmod{p^{3m-1}}$, $q \not\equiv 1 \pmod{p^{3m}}$, $K(\varepsilon_{p^{3m}})$ splits $\mathscr{A}$ and $[K(\varepsilon_{p^{3m}}): K] = p^m$. This completes the proof of Theorem 1.

Our final result shows that examples as in Theorem 1 do not exist if we require $Q(\chi)$ to be a cyclotomic field.

THEOREM 2. *Let χ be an irreducible complex character of a finite group G of order n and suppose $Q(\chi) = Q(\varepsilon_r)$ for some r. Then there is a splitting field L for χ with $Q(\varepsilon_n) \supset L \supset Q(\chi)$ and $[L: Q(\chi)] = m_Q(\chi)$.*

Proof. This result was proved in [2] provided $m_Q(\chi) \geqq 3$. If $r \geqq 3$, the argument of that paper is still valid even if $m_Q(\chi) = 2$. Thus we may assume that $m_Q(\chi) = 2$ and $Q(\chi) = Q$. Let $\mathscr{A}$ be the simple component of QG which is associated with χ. If $8|n$, set $t = -2p_1 \cdots p_u$, where $p_1, \cdots, p_u$ are the distinct odd primes dividing n. Then $Q(\sqrt{t}) \subset Q(\varepsilon_n)$ and the p-local degree from Q to $Q(\sqrt{t})$ is 2 for all primes p of Q at which $\mathscr{A}$ could have nonzero Hasse invariant. It follows that $Q(\sqrt{t})$ splits $\mathscr{A}$ and so we may assume that $8 \nmid n$. By [6, Theorem 9.1], $4|n$. Let $Q(\varepsilon_n) \supset K \supset Q$ be such that $[K: Q]$ is odd and $[Q(\varepsilon_n): K]$ is a power of 2. By the Brauer-Witt theorem [6, page 31], there is a hyperelementary subgroup F of G, a normal subgroup N of F, and a linear character ψ of N such that $\mathscr{A} \otimes_Q K$ is similar to a cyclotomic algebra $(K(\psi)/K, \beta)$ where the values of β are values of ψ on N and where $\mathrm{Gal}(K(\psi)/K) \cong F/N$. If $|N|$ is odd, then $(K(\psi)/K, \beta)^{|N|} \sim (K(\psi)/K, 1)$ is split, contradicting $m_Q(\chi) = 2$. Thus $2 \| N|$ and so $|F/N| = 2$. It follows that the quadratic subfield of $Q(\psi)$ is our desired splitting field for χ. This completes the proof of Theorem 2.

It would be interesting to replace the n in the statement of Theorem 2 by the exponent of G. If $Q(\chi) \neq Q$, this result is already in [2]. If 8 divides the exponent of G, the argument of Theorem 2 applies. There is only difficulty if $Q(\chi) = Q$, $m_Q(\chi) = 2$, and, in the notation of Theorem 2, $\mathscr{A}$ has nonzero invariants at 2, ∞, and some other primes of Q. The problem, of course, is that the natural candidate for a splitting field, $Q(\sqrt{v})$ with $v = -p_1 \cdots p_u$, need not split $\mathscr{A}$ at the prime 2. We have not been able to resolve this difficulty.

References

1. M. Deuring, *Algebren*, Springer, Berlin, 1935.
2. B. Fein, *Minimal splitting fields for group representations*, Pacific J. Math. **51** (1974), 427-431.
3. C. Ford and G. Janusz, *Examples in the theory of the Schur group*, Bull. Amer. Math. Soc., **79** (1973), 1233-1235.
4. G. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
5. M. Schacher, *Cyclotomic splitting fields*, Proc. Amer. Math. Soc., **25** (1970), 630-633.
6. T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Math., Vol. 397, Springer, Berlin-Heidelberg-New York, 1974.

Received September 23, 1975. This work was supported in part by NSF Grant GP-29068.

OREGON STATE UNIVERSITY
CORVALLIS, OR 97331