Pacific Journal of Mathematics

MINIMAL SPLITTING FIELDS FOR GROUP REPRESENTATIONS

BURTON I. FEIN

Vol. 51, No. 2 December 1974

PACIFIC JOURNAL OF MATHEMATICS
Vol. 51, No. 2, 1974

MINIMAL SPLITTING FIELDS FOR GROUP REPRESENTATIONS

BURTON FEIN

Let T be a complex irreducible representation of a finite group G of order n and let χ be the character afforded by T. An algebraic number field $K \supset Q(\chi)$ is a splitting field for χ if T can be written in K. The minimum of $[K: Q(\chi)]$, taken over all splitting fields K of χ, is the Schur index $m_Q(\chi)$ of χ. In view of the famous theorem of R. Brauer that $Q(e^{2\pi i}/n)$ is a splitting field for χ, it is natural to ask whether there exists a splitting field L with $Q(e^{2\pi i}/n) \supset L \supset Q(\chi)$ and $[L: Q(\chi)] = m_Q(\chi)$. In this paper examples are constructed which show that such a splitting field L does not always exist. Sufficient conditions are also obtained which guarantee the existence of a splitting field L as above.

Throughout this paper Q will denote the field of rational numbers. If K is an algebraic number field and p is a prime of K, we denote the completion of K at p by K_p. 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 [2, Theorem 1]. We write $l.i._pA$ for this common value and refer to $l.i._pA$ as the p-local index of A. If $L \supset K$ and L is an abelian extension of Q, we refer to the ramification degree of a prime π of K from K to L as the q-ramification degree where π extends the rational prime q. Clearly, this does not depend on the choice of π. We use similar notation when referring to residue class degrees.

Throughout this paper χ will denote an irreducible complex character of a finite group G of order n. There is a unique constituent $\mathscr{A}$ of the group algebra of G over $Q(\chi)$ corresponding to χ in the sense that the representation of G afforded by a minimal left ideal of $\mathscr{A}$ is equivalent to $m_Q(\chi)T$, where T affords χ. If D is the division algebra component of $\mathscr{A}$ we say that D (and $\mathscr{A}$) is associated with χ. The index of D equals $m_Q(\chi)$ and χ is realizable in K if and only if K is a splitting field for D. We refer the reader to [1] for the relevant theory of algebras assumed.

We denote a primitive mth root of unity by ε_m. Gal (L/K) denotes the Galois group of L over K, and $[L: K]$ the degree of L over K. If A and B are two central simple K-algebras we write $A \sim B$ to denote that A and B are similar in the Brauer group of K.

A special case of the following lemma is proved in [6, page 631]:

LEMMA. *Let F be the completion of an algebraic number field at a finite prime and suppose the residue class field of F has q elements. Let p be a prime, $p \nmid q$, and suppose $p^t \mid q-1$, $p^{t+1} \nmid q-1$. Let E be a cyclic extension of F of degree $p^e \cdot p^f$ where p^e, $e > 0$, is the ramification degree of E over F. Let $\langle\sigma\rangle = \mathrm{Gal}(E/F)$ and let $\varepsilon_{p^s} \in F$. We have:*

(1) *Let $p^t = 2$ so $\varepsilon_{p^s} = -1$. Then the cyclic algebra $(E, \sigma, -1)$ has index 2.*

(2) *Suppose $p^t \geqq 3$ and $s \geqq v > 0$. Then $(E, \sigma, \varepsilon_{p^s})$ has index p^v if and only if $t = e + s - v$.*

Proof. By Hensel's lemma, $\varepsilon_{p^t} \in F$, $\varepsilon_{p^{t+1}} \notin F$. Let $[K: F] = p^f$, K unramified over F. All p-power roots of unity in E are in K. If $p^t \geqq 3$, an easy induction shows that E contains a primitive p^{t+f}th root of unity but does not contain a primitive p^{t+f+1}th root of unity. If $p^t = 2$ and $f > 0$, then E contains a primitive 2^{2+f}th root of unity but not a primitive 2^{3+f}th root of unity. If $p^t = 2$ and $f = 0$, then E does not contain ε_4. From the theory of cyclic algebras over local fields, $(E, \sigma, \varepsilon_{p^s})$ has index p^v if and only if $\varepsilon_{p^{s-v}}$ is a norm from E to F but $\varepsilon_{p^{s-v+1}}$ is not a norm. Suppose $\varepsilon_{p^{s-v}}$ is a norm from E to F. Let N denote the norm map from E to F. Since $\varepsilon_{p^{s-v}}$ is a unit, $\varepsilon_{p^{s-v}} = N(\gamma)$ where γ is a unit of E. Let U_E, U_{E^1} denote, respectively, the units and the units (mod 1) of E. We have $U_{E/U_{E}^1} \cong \bar{E}^*$, the multiplicative group of the residue claas field of E. Since E and K have the same residue class field, there is a root of unity δ in K with $\gamma U_{E^1} = \delta U_{E^1}$. Since $N(\delta) U_{F^1} = \varepsilon_{p^{s-v}} U_{F^1} = N(\delta) U_{F^1}$, we may assume that δ has p-power order. Let N' denote the norm from K to F. Then $N(\delta) = N'(\delta^{p^e})$ since $\delta \in K$. Since Gal (K/F) is generated by the Frobenius automorphism, we have $N(\delta) = \delta^{mp^e}$ where

$$m = (q^{p^f} - 1) / (q - 1) .$$

Suppose (1) holds so $p^t = 2$, $\varepsilon_{p^s} = -1$. $(E, \sigma, -1)$ has index 1 or 2 and we have index 1 if and only if -1 is a norm from E. By the argument above, if -1 is a norm, then $-1 U_{F^1} = \delta^{m2^e} U_{F^1}$ where δ is a 2-power root of unity, $e > 0$, and $m = (q^{2^f} - 1)/(q - 1)$. One verifies easily that $\delta^{m2^e} = 1$, a contradiction.

Now suppose (2) holds. Assuming $\varepsilon_{p^{s-v}}$ is a norm from E we obtain, as above, that $N(\delta)$ is a power of a primitive p^{t-e}th root of unity. Thus $t - e \geqq s - v$ so $t \geqq s + e - v$. Conversely, if $t = s + e - v$, then E contains a primitive $p^{s+e+f-v}$th root of unity ζ. An easy calculation using the Frobenius automorphism shows that $N(\zeta^u) = \varepsilon_{p^{s-v}}$ for some u. Let $\mathscr{A} = (E, \sigma, \varepsilon_{p^s})$ so $\mathscr{A}^{p^v} \sim (E, \sigma, \varepsilon_{p^{s-v}})$. If $t = s + e - v$, then we have shown that $\mathscr{A}^{p^v} \sim F$. If $\mathscr{A}^{p^{v-1}} \sim F$, then we would have $t \geqq s + e - v + 1$ which is not the case. Thus $t = s + e - v$ implies $\mathscr{A}$ has index p^v. Conversely, if $\mathscr{A}$ has index p^v, then $t \geqq s + e - v$. If $t \geqq s + e - v + 1$ we would have $\mathscr{A}^{p^{v-1}} \sim F$. Thus $t = s + e - v$, proving the lemma.

We can now construct an example (actually one for each prime p) of an irreducible character χ of a finite group G of order n such that $m_Q(\chi) = p$ but no subfield L of $Q(\varepsilon_n)$ with $[L: Q(\chi)] = p$ is a splitting field for χ.

EXAMPLE. Let p be an arbitrary prime. Let r be prime, $r \equiv 1 \pmod{p^2}$, $r \not\equiv 1 \pmod{p^3}$. Let q be a prime, $q \equiv 1 \pmod{r}$, $q \equiv 1 \pmod{p^4}$, and $q \not\equiv 1 \pmod{p^5}$. Let F be the subfield of $Q(\varepsilon_q)$ with $[Q(\varepsilon_q): F] = p^4$ and let E be the subfield of $Q(\varepsilon_r)$ with $[Q(\varepsilon_r): E] = p^2$. Let $\langle \sigma \rangle = \mathrm{Gal}\,(Q(\varepsilon_{p^3qr})/F(\varepsilon_{p^3r}))$ and $\langle \tau \rangle = \mathrm{Gal}\,(Q(\varepsilon_{p^3qr})/E(\varepsilon_{p^3q}))$. Let K be the fixed field of $\langle \sigma\tau \rangle$. Then $K(\varepsilon_q) = Q(\varepsilon_{p^3qr})$ and $[K(\varepsilon_q): K] = p^4$. Since q is totally ramified from $EF(\varepsilon_{p^3})$ to $F(\varepsilon_{p^3q})$ and splits completely from $EF(\varepsilon_{p^3})$ to $E(\varepsilon_{p^3r})$, we see that q is totally ramified from $EF(\varepsilon_{p^3})$ to K. Thus the ramification degree of q from K to $K(\varepsilon_q)$ is p^2 and the residue class degree is 1.

Let $G = \langle w, x, y, z \mid w^q = x^r = z^{p^3} = 1,\ y^{p^4} = z,\ z \text{ central},\ (w, x) = 1,\ y^{-1}wy = w^a,\ y^{-1}xy = x^b \rangle$ where $\sigma\tau(\varepsilon_q) = (\varepsilon_q)^a$ and $\sigma\tau(\varepsilon_r) = (\varepsilon_r)^b$. The cyclic algebra $\mathscr{A} = (Q(\varepsilon_{p^3qr}), \sigma\tau, \varepsilon_{p^3})$ 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 $m_Q(\chi)$.

By the lemma we see that $\mathscr{A}$ has q-local index p. Since $K(\varepsilon_q) = Q(\varepsilon_{p^3qr})$, r is unramified from K to $Q(\varepsilon_{p^3qr})$ and so the r-local index of $\mathscr{A}$ is 1. Since the 2-local index is at most 2 [7, Satz 11] and at infinite primes $\mathscr{A}$ can only have index 1 or 2, we conclude that $m_Q(\chi) = p$. $|G| = p^7qr$ and $\mathrm{Gal}\,(Q(\varepsilon_{p^7qr})/K) \cong C_{p^4} \times C_{p^4}$. Since $q \equiv 1 \pmod{p^4}$ we see that q splits completely in the unique extension J of K, $J \subset Q(\varepsilon_{p^7qr})$, $\mathrm{Gal}\,(J/K) = C_p \times C_p$. It follows, therefore, that q splits completely in every subfield of $Q(\varepsilon_{p^7qr})$ of degree p over K and so T is not realizable in any subfield L of the $|G|$th roots of unity with $[L: Q(\chi)] = p$.

We next prove that under certain conditions there always exists a subfield L of the order of $|G|$th roots of unity which is a splitting field for χ and where $[L: Q(\chi)] = m_Q(\chi)$.

THEOREM. *Let χ be a complex irreducible character of a finite group G of exponent n with $m_Q(\chi) \geqq 3$. Assume either* (a) *or* (b) *below hold*:

(a) $Q(\chi) = Q(\varepsilon_m)$ *for some* m.

(b) $n = p^a q^b$ *where* p *and* q *are primes*, $p < q$.

Then there exists a subfield L of $Q(\varepsilon_n)$ with $[L: Q(\chi)] = m_Q(\chi)$ and such that L is a splitting field for χ.

Proof. By a standard reduction using the Brauer-Witt theorem [8, § 2], we may assume that $m_Q(\chi)$ is a prime power. Since if (b) holds, $m_Q(\chi)$ is a power of p by [7, Satz 10], we will assume that $m_Q(\chi) = p^c$.

Let K be the subfield of $Q(\varepsilon_n)$ such that $K \supset Q(\chi)$, $p \nmid [K: Q(\chi)]$, and $[Q(\varepsilon_n): K]$ is a power of p. Let D be the $Q(\chi)$-central division algebra associated with χ. By the Brauer-Witt theorem [8, § 2], $D \otimes_{Q(\chi)} K$ is similar to a crossed product $(K(\psi)/K, \beta)$ where ψ is a linear character of a subgroup of G, β is a factor set whose values are roots of unity, and where $\mathrm{Gal}(K(\psi)/K)$ is isomorphic to a factor group of a Sylow p-subgroup of G.

$Q(\chi)$ contains a primitive $m_Q(\chi)$th root of unity [3, Theorem 1]. Since $m_Q(\chi) \geqq 3$, $Q(\chi)$ and K are both totally imaginary. Thus the nonzero invariants of D are at finite primes.

Suppose (a) holds, so $Q(\chi) = Q(\varepsilon_m)$. We may assume m is not twice an odd number. We have $m_Q(\chi) \mid m$. If r is a prime divisor of m, $r \neq p$, then since, for some d, $[Q(\varepsilon_n): K] = p^d$, r is unramified from K to $K(\psi)$. This implies that the r-local index of D equals 1. Now let $q_1, \cdots, q_t$ be the rational primes at which D has nontrivial local index. Let the q_i-local index of D be p^{c_i}. Then $c_i \leqq c$ for all i and $c_i = c$ for some i since D has index p^c. Suppose q_i is odd. By [7, Satz 10] $p^{c_i} \mid q_i - 1$ and so $Q(\varepsilon_{q_i})$ has a subfield E_i with $[E_i: Q] = p^{c_i}$. Since $q_i \nmid m$, $[E_iQ(\chi): Q(\chi)] = p^{c_i}$ and q_i is totally ramified from $Q(\chi)$ to $E_iQ(\chi)$. Let $L_i = E_iQ(\chi)$. By [3, Theorem 1], $\varepsilon_{p^{c_i}} \in Q(\chi)$ and so $L_i = Q(\chi)(\alpha_i)$ where $\alpha_i^{p^{c_i}} \in Q(\chi)$. If all of the q_i are odd, let $\alpha = \alpha_1\alpha_2 \cdots \alpha_t$. If $q_1 = 2$, say, let $\alpha = \sqrt{-1}\alpha_2 \cdots \alpha_t$. We note that q_1 can equal 2 only if $p^{c_1} = 2$ and $\sqrt{-1} \notin Q(\chi)$ [7, Satz 11]. If this happens, then $4 \mid n$ by [4]. Thus $\alpha \in Q(\varepsilon_n)$. Since $\alpha^{p^c} \in Q(\chi)$, $[Q(\chi)(\alpha): Q(\chi)] \leqq p^c$. Since q_i is ramified of degree p^{c_i} from $Q(\chi)$ to $Q(\chi)(\alpha)$, $[Q(\chi)(\alpha): Q(\chi)] = p^c$ and $Q(\chi)(\alpha)$ splits D. Thus $Q(\chi)(\alpha)$ is our desired field.

Assume (b) holds. $K(\psi)$ is an abelian extension of K generated by roots of unity. Since $(K(\psi)/K, \beta)$ has index $p^c > 1$, $(K(\psi)/K, \beta)$ has q-local index p^c and so q is ramified from K to $K(\psi)$. This implies that $K(\psi) \supset K(\varepsilon_q) = K(\varepsilon_{q^b})$. Since $m_Q(\chi) = p^c \geqq 3$, if $p = 2$ we see that $\sqrt{-1} \in K$. In view of [7, Satz 12] this implies that q is the only prime of Q with the q-local index of $(K(\psi)/K, \beta)$ different from 1.

Let $\varepsilon_{p^v} \in K(\psi)$, $\varepsilon_{p^{v+1}} \notin K(\psi)$. We note that $K(\psi) = Q(\varepsilon_{p^v q^b})$ since $[Q(\varepsilon_{p^a q^b}): K]$ is a power of p. Let $\langle\sigma\rangle = \mathrm{Gal}(Q(\varepsilon_{p^v q^b})/Q(\varepsilon_{p^v}))$, $\langle\tau\rangle = \mathrm{Gal}(Q(\varepsilon_{p^v q^b})/Q(\varepsilon_{q^b}))$. Then $\langle\sigma^i\tau^j\rangle = \mathrm{Gal}(Q(\varepsilon_{p^v q^b})/K)$ for some i and j. Let F_1 and F_2 be, respectively, the fixed fields of $\langle\sigma^i\rangle$ and $\langle\tau^j\rangle$. Let

p^e and p^t be, respectively, the order, of $\langle\sigma^i\rangle$ and $\langle\tau^j\rangle$. Let L_1 and L_2 be, respectively, the subfields of index p^e and p^t in $Q(\varepsilon_{q^b})$ and $Q(\varepsilon_{p^v})$. Then $F_1 = L_1(\varepsilon_{p^v})$ and $F_2 = L_2(\varepsilon_{q^b})$ and $F_1 \cap F_2 = L_1L_2$. Since q is totally ramified from L_1L_2 to F_2 and is unramified from L_1L_2 to F_1, q is totally ramified from L_1L_2 to K. Thus $e > t$ and q has ramification degree p^{e-t} from K to $K(\psi)$.

Suppose $[K(\varepsilon_{p^v}): K] = p^s$. Then $(\sigma^i\tau^j)^{p^s}$ fixes $K(\varepsilon_{p^v})$. Since σ fixes ε_{p^v}, τ^{jp^s} fixes ε_{p^v} and so $\tau^{jp^s} = 1$. Thus $s \geqq t$. But q is unramified from K to $K(\varepsilon_{p^v})$ and so the ramification degree of q from K to $K(\psi)$ is at most p^{e-s}. Thus $e - s \geqq e - t$ so $s = t$. This shows that q is totally ramified from $K(\varepsilon_{p^v})$ to $K(\psi)$. Since q is unramified from $K(\psi)$ to $K(\varepsilon_{p^aq^b}) = Q(\varepsilon_{p^aq^b})$, we see that $K(\varepsilon_{p^a})$ is the maximal extension of K inside $Q(\varepsilon_{p^aq^b})$ in which q is unramified.

$Q(\varepsilon_{p^aq^b})$ is not a cyclic extension of K by [5]. Thus Gal $(Q(\varepsilon_{p^aq^b})/K)$ is the direct product of two cyclic groups. Let M_1 and M_2 be subfields of $Q(\varepsilon_{p^aq^b})$ such that $M_1 \cap M_2 = K$, $Q(\varepsilon_{p^aq^b}) = M_1M_2$, and M_1 and M_2 are cyclic extensions of K. Since $K(\varepsilon_{p^a})$ is cyclic over K, q must be totally ramified in either M_1 or M_2. Suppose q is totally ramified in M_1. By [5], since $Q(\varepsilon_{p^aq^b})$ is cyclic over M_1, M_1 is a splitting field for χ. Thus M_1 splits $(K(\psi)/K, \beta)$ and so $[M_1: K] \geqq p^c$. The subfield L of M_1 with $[L: Q(\chi)] = p^c$ is the desired splitting field for χ. This completes the proof of the theorem.

References

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., **24**, Providence, R. I., 1939.

2. M. Benard, *The Schur subgroup, I*, J. Algebra, **22** (1972), 374-377.

3. M. Benard and M. Schacher, *The Schur subgroup II*, J. Algebra, **22** (1972), 378-385.

4. B. Fein and T. Yamada, *The Schur index and the order and exponent of a finite group*, J. Algebra, **28** (1974), 496-498.

5. D. Goldschmidt and I. M. Isaacs, to appear, in J. Algebra.

6. M. Schacher, *Cyclotomic splitting field*, Proc. Amer. Math. Soc., **25** (1970), 630-633.

7. E. Witt, *Die algebraische Struktur des Grupperringes einer endlicher Gruppe über einem Zahlkörper*, J. Reine Angew, Math., **190** (1952), 231-245.

8. T. Yamada, *Characterization of the simple components of the group algebras over the p-adic number field*, J. Math. Soc. Japan, **23** (1971), 295-310.

Received October 15, 1973. This work was done under the sponsorships of NSF Grant GP-29068. AMS classification: 20C15

OREGON STATE UNIVERSITY

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. **39**. All other communications to the editors should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

100 reprints are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The *Pacific of Journal Mathematics* is issued monthly as of January 1966. Regular subscription rate: $72.00 a year (6 Vols., 12 issues). Special rate: $36.00 a year to individual members of supporting institutions.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 270, 3-chome Totsuka-cho, Shinjuku-ku, Tokyo 160, Japan.

* C. R. DePrima California Institute of Technology, Pasadena, CA 91109, will replace J. Dugundji until August 1974.

Pacific Journal of Mathematics

Vol. 51, No. 2 December, 1974