MINIMAL SPLITTING FIELDS FOR GROUP REPRESENTATIONS

BURTON I. FEIN
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 $\chi$ be the character afforded by $T$. An algebraic number field $K \supseteq \mathbb{Q}(\chi)$ is a splitting field for $\chi$ if $T$ can be written in $K$. The minimum of $[K: \mathbb{Q}(\chi)]$, taken over all splitting fields $K$ of $\chi$, is the Schur index $m_{\mathbb{Q}}(\chi)$ of $\chi$. In view of the famous theorem of R. Brauer that $\mathbb{Q}(\exp(2\pi i/n))$ is a splitting field for $\chi$, it is natural to ask whether there exists a splitting field $L$ with $\mathbb{Q}(\exp(2\pi i/n)) \supseteq L \supseteq \mathbb{Q}(\chi)$ and $[L: \mathbb{Q}(\chi)] = m_{\mathbb{Q}}(\chi)$. 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 $\mathbb{Q}$ 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 $\mathbb{Q}$, the center of $A$ being $K$, and $\pi_1$ and $\pi_2$ 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 $l.i._p A$ for this common value and refer to $l.i._p A$ as the $p$-local index of $A$. If $L \supseteq K$ and $L$ is an abelian extension of $\mathbb{Q}$, we refer to the ramification degree of a prime $\pi$ of $K$ from $K$ to $L$ as the $q$-ramification degree where $\pi$ extends the rational prime $q$. Clearly, this does not depend on the choice of $\pi$. We use similar notation when referring to residue class degrees.

Throughout this paper $\chi$ will denote an irreducible complex character of a finite group $G$ of order $n$. There is a unique constituent $\mathcal{A}$ of the group algebra of $G$ over $\mathbb{Q}(\chi)$ corresponding to $\chi$ in the sense that the representation of $G$ afforded by a minimal left ideal of $\mathcal{A}$ is equivalent to $m_{\mathbb{Q}}(\chi)T$, where $T$ affords $\chi$. If $D$ is the division algebra component of $\mathcal{A}$ we say that $D$ (and $\mathcal{A}$) is associated with $\chi$. The index of $D$ equals $m_{\mathbb{Q}}(\chi)$ and $\chi$ 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 $m$th root of unity by $\varepsilon_m$. $\text{Gal}(L/K)$ 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]:

427
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 $p^t | q - 1$, $p^{t+1} \nmid q - 1$. Let $E$ be a cyclic extension of $F$ of degree $p^a \cdot p^b$ where $p^a, e > 0$, is the ramification degree of $E$ over $F$. Let $\langle \sigma \rangle = \text{Gal}(E/F)$ and let $\varepsilon_{p^t} \in F$. We have:

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

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

Proof. By Hensel's lemma, $\varepsilon_{p^t} \in F$, $\varepsilon_{p^{t+1}} \in F$. Let $[K : F] = p^e$, $K$ unramified over $F$. All $p$-power roots of unity in $E$ are in $K$. If $p^t \geq 3$, 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 $2^{t+f}$th root of unity but not a primitive $2^{t+f+1}$th root of unity. If $p^t = 2$ and $f = 0$, then $E$ does not contain $\varepsilon_2$. From the theory of cyclic algebras over local fields, $(E, \sigma, \varepsilon_{p^t})$ has index $p^v$ if and only if $\varepsilon_{p^t-v}$ is a norm from $E$ to $F$ but $\varepsilon_{p^{t+1}}$ is not a norm. Suppose $\varepsilon_{p^t-v}$ is a norm from $E$ to $F$. Let $N$ denote the norm map from $E$ to $F$. Since $\varepsilon_{p^t-v}$ is a unit, $\varepsilon_{p^t-v} = N(\gamma)$ where $\gamma$ is a unit of $E$. Let $U_{E_1}, U_{E_1}$ denote, respectively, the units and the units (mod 1) of $E$. We have $U_{E_1}/U_{E_1} \cong E^*$, the multiplicative group of the residue class field of $E$. Since $E$ and $K$ have the same residue class field, there is a root of unity $\delta$ in $K$ with $\gamma U_{E_1} = \delta U_{E_1}$. Since $N(\delta)U_{E_1} = \varepsilon_{p^t-v}U_{E_1} = N(\delta)U_{E_1}$, we may assume that $\delta$ has $p$-power order. Let $N'$ denote the norm from $K$ to $F$. Then $N(\delta) = N'(\delta^{p^v})$ since $\delta \in K$. Since $\text{Gal}(K/F)$ is generated by the Frobenius automorphism, we have $N(\delta) = \delta^{mp^v}$ where

$$m = (q^{e_1} - 1)/(q - 1).$$

Suppose (1) holds so $p^t = 2$, $\varepsilon_{p^t} = -1$. $(E, \sigma, -1)$ 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 $-1U_{E_1} = \delta^{mp^v}U_{E_1}$ where $\delta$ is a 2-power root of unity, $e > 0$, and $m = (q^{e_1} - 1)/(q - 1)$. One verifies easily that $\delta^{mp^v} = 1$, a contradiction.

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

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

**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, \( q \equiv 1 \pmod{r} \), \( q \not\equiv 1 \pmod{p^4} \), and \( q \equiv 1 \pmod{p^5} \). Let \( F \) be the subfield of \( \mathbb{Q}(\varepsilon_q) \) with \([\mathbb{Q}(\varepsilon_q): F] = p^4 \) and let \( E \) be the subfield of \( \mathbb{Q}(\varepsilon_r) \) with \([\mathbb{Q}(\varepsilon_r): E] = p^5 \). Let \( \langle \sigma \rangle = \text{Gal}(\mathbb{Q}(\varepsilon_{p^5q})/\mathbb{Q}(\varepsilon_{p^4})) \) and \( \langle \tau \rangle = \text{Gal}(\mathbb{Q}(\varepsilon_{p^5q})/\mathbb{Q}(\varepsilon_{p^4})) \). Let \( K(\varepsilon_q) = \mathbb{Q}(\varepsilon_{p^5q}) \) and \( [K(\varepsilon_q): K] = p^4 \).

Since \( q \) is totally ramified from \( EF(\varepsilon_{p^5q}) \) to \( F(\varepsilon_{p^5q}) \) and splits completely from \( EF(\varepsilon_{p^5q}) \) to \( E(\varepsilon_{p^5q}) \), we see that \( q \) is totally ramified from \( EF(\varepsilon_{p^5q}) \) 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 \( G = \langle \omega, x, y, z \mid \omega^q = x^q = y^q = z^q = 1, y^{-1}wy = x^5, y^{-1}xw = x^5 \rangle \) where \( \sigma(\varepsilon_q) = (\varepsilon_q)^{p^6} \) and \( \sigma(\varepsilon_r) = (\varepsilon_r)^{p^6} \). The cyclic algebra \( \mathcal{A} = (\mathbb{Q}(\varepsilon_{p^5q}), \sigma(\varepsilon_q), \sigma(\varepsilon_r)) \) is a homomorphic image of the group algebra of \( G \) over \( \mathbb{Q} \) and so there exists a complex irreducible representation \( T \) of \( G \) with character \( \chi \) such that the enveloping algebra of \( T \) is \( \mathcal{A} \) and \( \mathbb{Q}(\chi) = K \). The index of \( \mathcal{A} \) equals \( m_\chi(\chi) \).

By the lemma we see that \( \mathcal{A} \) has \( q \)-local index \( p \). Since \( K(\varepsilon_q) = \mathbb{Q}(\varepsilon_{p^5q}), r \) is unramified from \( K \) to \( \mathbb{Q}(\varepsilon_{p^5q}) \), and so the \( r \)-local index of \( \mathcal{A} \) is \( 1 \). Since the \( 2 \)-local index is at most \( 2 \) [7, Satz 11] and at infinite primes \( \mathcal{A} \) can only have index \( 1 \) or \( 2 \), we conclude that \( m_\chi(\chi) = p \). \(|G| = p^q r \) and \( \text{Gal}(\mathbb{Q}(\varepsilon_{p^5q})/K) \cong C_{p^4} \times C_{p^4} \). Since \( q \equiv 1 \pmod{p^4} \) we see that \( q \) splits completely in the unique extension \( J \) of \( K, J \subset \mathbb{Q}(\varepsilon_{p^5q}) \), \( \text{Gal}(J/K) = C_p \times C_p \). It follows, therefore, that \( q \) splits completely in every subfield of \( \mathbb{Q}(\varepsilon_{p^5q}) \) of degree \( p \) over \( K \) and so \( T \) is not realizable in any subfield \( L \) of the \(|G| \)-th roots of unity with \([L: \mathbb{Q}(\chi)] = p \).

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 \( \chi \) and where \([L: \mathbb{Q}(\chi)] = m_\chi(\chi) \).

**Theorem.** Let \( \chi \) be a complex irreducible character of a finite group \( G \) of exponent \( n \) with \( m_\chi(\chi) \geq 3 \). Assume either (a) or (b) below hold:

(a) \( \mathbb{Q}(\chi) = \mathbb{Q}(\varepsilon_m) \) for some \( m \).

(b) \( n = p^aq^b \) 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 $\chi$.

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 $m_Q(\chi) = p^r$.

Let $K$ be the subfield of $Q(\varepsilon_n)$ such that $K \supseteq Q(\chi)$, $p \nmid [K: Q(\chi)]$, and $[Q(\varepsilon_n): K]$ is a power of $p$. Let $D$ be the $Q(\chi)$-central division algebra associated with $\chi$. By the Brauer-Witt theorem [8, § 2], $D$ is similar to a crossed product $(K(\psi)/K, \beta)$ where $\psi$ is a linear character of a subgroup of $G$, $\beta$ is a factor set whose values are roots of unity, and where $\text{Gal}(K(\psi)/K)$ 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 $m_Q(\chi) \geq 3$, $Q(\chi)$ and $K$ are both totally imaginary. Thus the nonzero invariants of $D$ are at finite primes.

Suppose (a) holds, so $Q(\chi) = Q(\varepsilon_n)$. We may assume $m$ is not twice an odd number. We have $m_Q(\chi) | m$. 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 $q_1, \ldots, q_t$ be the rational primes at which $D$ has nontrivial local index. Let the $q_i$-local index of $D$ be $p^{e_i}$. Then $e_i \leq c$ for all $i$ and $e_i = c$ for some $i$ since $D$ has index $p^c$. Suppose $q_i$ is odd.

By [7, Satz 10] $p^{e_i} | q_i - 1$ and so $Q(\varepsilon_n)$ has a subfield $E_i$ with $[E_i: Q] = p^{c_i}$. Since $q_i \nmid m$, $[E_i Q(\chi): Q(\chi)] = p^{c_i}$. Let $L_i = E_i Q(\chi)$. By [3, Theorem 1], $\varepsilon_{p^{c_i} \varepsilon}$ is in $Q(\chi)$ and so $L_i = Q(\chi)(\alpha_i)$ where $\alpha_i^{p^{c_i}}$ is in $Q(\chi)$. If all of the $q_i$ are odd, let $\alpha = \alpha_1 \alpha_2 \cdots \alpha_t$. If $q_i = 2$, say, let $a = \sqrt{-1} \alpha_1 \cdots \alpha_t$. We note that $q_i$ can equal 2 only if $p^{c_i} = 2$ and $\sqrt{-1} \in Q(\chi)$ [7, Satz 11]. If this happens, then $4 | n$ by [4]. Thus $\alpha \in Q(\varepsilon_n)$. Since $\alpha^{p^c} \in Q(\chi)$, $[Q(\chi)(\alpha): \alpha(\chi)] \leq p^c$. Since $q_i$ is ramified of degree $p^{e_i}$ 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 $p^\tau > 1$, $(K(\psi)/K, \beta)$ has $q$-local index $p^\tau$ and so $q$ is ramified from $K$ to $K(\psi)$. This implies that $K(\psi) \supseteq K(\varepsilon_n)$. Since $m_Q(\chi) = p^t \geq 3$, 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 $\varepsilon_{p^\tau} \in K(\psi)$, $\varepsilon_{p^\tau+1} \in K(\psi)$. We note that $K(\psi) = Q(\varepsilon_{p^\tau+1})$ since $[Q(\varepsilon_{p^\tau+1}): K]$ is a power of $p$. Let $\langle \sigma \rangle = \text{Gal}(Q(\varepsilon_{p^\tau+1})/Q(\varepsilon_{p^\tau}))$, $\langle \tau \rangle = \text{Gal}(Q(\varepsilon_{p^\tau+1})/Q(\varepsilon_{p^\tau}))$. Then $\langle \sigma^i \tau^j \rangle = \text{Gal}(Q(\varepsilon_{p^\tau+1})/K)$ for some $i$ and $j$. Let $F_i$ and $F_j$ be, respectively, the fixed fields of $\langle \sigma^i \rangle$ and $\langle \tau^j \rangle$. Let
\( p^e \) and \( p^f \) 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 \( p^f \) in \( Q(\varepsilon_{p^r}) \) and \( Q(\varepsilon_{p^q}) \). Then \( F_1 = L_1(\varepsilon_{p^r}) \) and \( F_2 = L_2(\varepsilon_{p^q}) \) and \( F_1 \cap F_2 = L_1L_2 \). Since \( q \) is totally ramified from \( L_1L_2 \) to \( F_1 \) 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 \( [K(\varepsilon_{p^r}): K] = p^e \). Then \( (\sigma^i\tau^j)^{p^e} \) fixes \( K(\varepsilon_{p^r}) \). Since \( \sigma \) fixes \( \varepsilon_{p^r} \), \( \tau^{j,p^e} \) fixes \( \varepsilon_{p^r} \) and so \( \tau^{j,p^e} = 1 \). Thus \( s \geq t \). But \( q \) is unramified from \( K \) to \( K(\varepsilon_{p^r}) \) and so the ramification degree of \( q \) from \( K \) to \( K(\psi) \) is at most \( p^{e-t} \). Thus \( e - s \geq e - t \) so \( s = t \). This shows that \( q \) is totally ramified from \( K(\varepsilon_{p^r}) \) to \( K(\psi) \). Since \( q \) is unramified from \( K(\psi) \) to \( K(\varepsilon_{p^r}) = Q(\varepsilon_{p^r}) \), we see that \( K(\varepsilon_{p^r}) \) is the maximal extension of \( K \) inside \( Q(\varepsilon_{p^r}) \) in which \( q \) is unramified.

\( Q(\varepsilon_{p^r}) \) is not a cyclic extension of \( K \) by [5]. Thus \( \text{Gal}(Q(\varepsilon_{p^r})/K) \) is the direct product of two cyclic groups. Let \( M_1 \) and \( M_2 \) be subfields of \( Q(\varepsilon_{p^r}) \) such that \( M_1 \cap M_2 = K \), \( Q(\varepsilon_{p^{r+q}}) = M_1M_2 \) and \( M_1 \) and \( M_2 \) are cyclic extensions of \( K \). Since \( K(\varepsilon_{p^r}) \) 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 \( Q(\varepsilon_{p^r}) \) is cyclic over \( M_1 \), \( M_1 \) is a splitting field for \( \chi \). Thus \( M_1 \) splits \( (K(\psi)/K, \beta) \) and so \( [M_1: K] \geq p^e \). The subfield \( L \) of \( M_1 \) with \( [L: Q(\chi)] = p^e \) is the desired splitting field for \( \chi \). This completes the proof of the theorem.

REFERENCES


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

OREGON STATE UNIVERSITY
Robert F. V. Anderson, Laplace transform methods in multivariate spectral theory .................................................. 339
William George Bade, Two properties of the Sorgenfrey plane ................................................................. 349
John Robert Baxter and Rafael Van Severen Chacon, Functionals on continuous functions ................................................................. 355
Phillip Wayne Bean, Helly and Radon-type theorems in interval convexity spaces .............................................. 363
James Robert Boone, On k-quotient mappings ......................................................................................... 369
Ronald P. Brown, Extended prime spots and quadratic forms ................................................................. 379
William Hugh Cornish, Crawley’s completion of a conditionally upper continuous lattice ................................................. 397
Robert S. Cunningham, On finite left localizations .............................................................................. 407
Robert Jay Daverman, Approximating polyhedra in codimension one spheres embedded in s^n by tame polyhedra ........................................................................................................ 417
Burton I. Fein, Minimal splitting fields for group representations ................................................................. 427
Peter Fletcher and Robert Allen McCoy, Conditions under which a connected representable space is locally connected ........................................................................................................ 433
Jonathan Samuel Golan, Topologies on the torsion-theoretic spectrum of a noncommutative ring ........................................................................................................ 439
Manfred Gordon and Edward Martin Wilkinson, Determinants of Petrie matrices ........................................................................................................ 451
Alfred Peter Hallstrom, A counterexample to a conjecture on an integral condition for determining peak points (counterexample concerning peak points) ........................................................................ 455
E. R. Heal and Michael Windham, Finitely generated F-algebras with applications to Stein manifolds ........................................................................................................ 459
Denton Elwood Hewgill, On the eigenvalues of a second order elliptic operator in an unbounded domain ........................................................................................................ 467
Charles Royal Johnson, The Hadamard product of A and A* ......................................................................... 477
Darrell Conley Kent and Gary Douglas Richardson, Regular completions of Cauchy spaces ........................................................................................................ 483
Alan Greenwell Law and Ann L. McKerracher, Sharpened polynomial approximation ........................................................................................................ 491
Bruce Stephen Lund, Subalgebras of finite codimension in the algebra of analytic functions on a Riemann surface ........................................................................................................ 495
Robert Wilmer Miller, TTF classes and quasi-generators ........................................................................... 499
Roberta Mura and Akbar H. Rhemtulla, Solvable groups in which every maximal partial order is isolated ........................................................................................................ 509
Isaac Namioka, Separate continuity and joint continuity ........................................................................... 515
Edgar Andrews Rutter, A characterization of QF – 3 rings ........................................................................ 533
Alan Saleski, Entropy of self-homeomorphisms of statistical pseudo-metric spaces ........................................................................................................ 537
Ryōtarō Satō, An Abel-maximal ergodic theorem for semi-groups ........................................................................... 543
H. A. Seid, Cyclic multiplication operators on L_p-spaces ........................................................................... 549
H. B. Skerry, On matrix maps of entire sequences ................................................................................. 563
John Brendan Sullivan, A proof of the finite generation of invariants of a normal subgroup ........................................................................................................ 571
John Griggs Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, VI ........................................................................................................ 573
Ronson Joseph Warne, Generalized ω – L-unipotent bisimple semigroups ................................................. 631
Toshihiko Yamada, On a splitting field of representations of a finite group ................................................. 649