PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 87, Number 1, January 1983

MINIMAL SPLITTING FIELDS IN CYCLOTOMIC EXTENSIONS

EUGENE SPIEGEL AND ALLAN TROJAN

ABSTRACT. Suppose G is a finite group of exponent n and X an irreducible character of G. In this note we give sufficient conditions for the existence of a minimal degree splitting field L with $Q(X) \subseteq L \subseteq Q(\zeta_n)$.

1. Introduction. Let G be a finite group of exponent n, X an irreducible complex character of G, $m_Q(X)$ the Schur index of X and $A(X; Q)$ the simple component of the group algebra QG corresponding to X. In this note we investigate the existence of a splitting field L of X such that $Q(X) \subseteq L \subseteq Q(\zeta_n)$ and $[L : Q(X)] = m_Q(X)$, where ζ_n denotes a primitive nth root of unity. Fein [3, 4] and more recently Mollin [9] have investigated this question showing that such L does not always exist, and giving sufficient conditions when this minimal splitting field does exist. An improved sufficient condition for the existence of L is given, as an application of Abhyankar's Lemma. The authors would like to thank Dr. Gary Cornell for both pointing out Abhyankar's Lemma and useful discussions about its applicability.

If K is the algebraic number field $Q(X)$, q a rational prime and q_1 and q_2 primes in K lying above q, then $A(X; Q) \otimes_K K_{q_1}$ and $A(X, Q) \otimes_K K_{q_2}$ have the same index which we denote as $\operatorname{ind}_q A(X; Q)$. K_{q_i} denotes the q_i-adic completion of K.

For n an integer and p a prime we use n_p to denote the p-part of n.

2. For completeness, we begin with Abhyankar's Lemma.

THEOREM. *Let F be a local field and E_1 and E_2 finite extensions of F with ramification indices e_1 and e_2 respectively. Suppose E_2 is tamely ramified and $e_2 \mid e_1$. Then E_1E_2 is an unramified extension of E_1.*

PROOF. We follow Cornell [2, Theorem 1, p. 83]. Let L be the maximal unramified extension of F in E_2, so that E_2 is totally unramified over L. Then E_1L is unramified over E_1, and $e(E_1L \mid F) = e(E_1 \mid F)$. Similarly $e(E_1L \mid L) = e(E_1 \mid F)$. As the composite of an unramified extension with an unramified extension, remains unramified, we may assume that $E_2 \mid F$ is a totally and tamely ramified extension. From [8, p. 249], there is a prime element $\pi \in F$ with $E_2 = F(\pi^{1/e_2})$. Let Π be a prime element in E_1, so $u\Pi^{e_1} = \pi$ for u a unit in E_1. Then $E_1E_2 = E_1(u^{1/e_2}\Pi^{e_1/e_2}) = E_1(u^{1/e_2})$ as $e_2 \mid e_1$, and E_1E_2 is unramified over $E_1(u^{1/e_2})$ which is unramified over E_1. The result now follows.

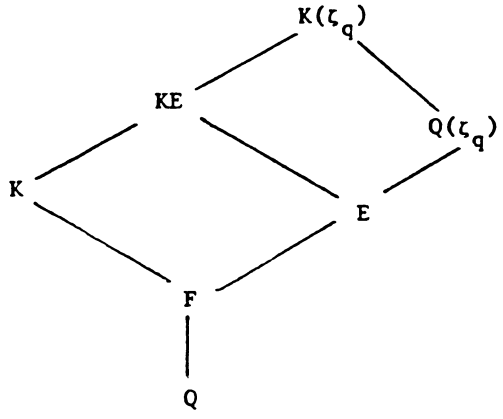
Received by the editors December 4, 1981 and, in revised form, February 2, 1982.
1980 *Mathematics Subject Classification.* Primary 20C05.

© 1983 American Mathematical Society
0002-9939/82/0000-0572/$02.00

Let K be a finite abelian extension of Q and q a rational prime. If $F = K \cap Q(\zeta_q)$ and $t = \text{g.c.d.}\ (q-1, e_q(K|Q))$, where $e_q(K|Q)$ denotes the index of ramification of q in $K|Q$, then we denote by E the unique subfield of $Q(\zeta_q)$ of degree t over Q. $Q(\zeta_q)$ is a cyclic extension of Q of degree $q-1$. $E \supseteq F$ as $Q(\zeta_q)$ is totally ramified at q.

We then have the following diagram of fields

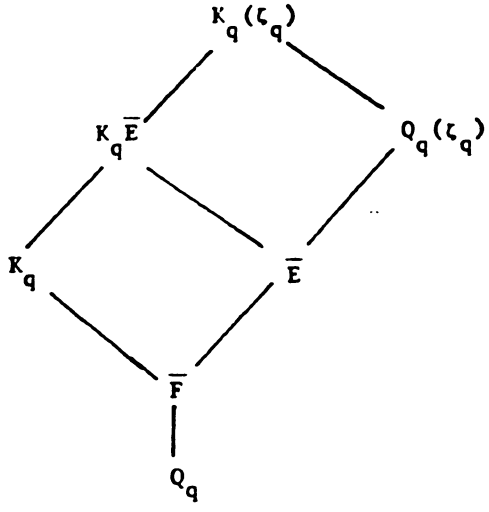
(*)



with $[KE:K] = [E:F]$ and $[K(\zeta_q):KE] = [Q(\zeta_q):E]$. By Abhyankar's Lemma, KE is a totally unramified extension of K with respect to q. If L_1 is an unramified extension at q of KE in $K(\zeta_q)$ and L_2 is the subfield of $Q(\zeta_q)$ containing E with $[L_2:E] = [L_1:KE]$, then $KL_2 = L_1$. Also $e_q(L|Q) = e_q(K|Q)$, and $e_q(K|Q) = [L_2:Q]e_q(L_1|L_2)$. This implies $[L_2:Q] \mid e_q(K|Q)$ and as $t \mid [L_2:Q]$, we must have $[L_2:Q] = t$. Thus $L_2 = E$ and $L_1 = KE$ and $K(\zeta_q)$ is a totally ramified extension at q of KE.

Let, now, $\bar{F} = K_q \cap Q_q(\zeta_q)$ and $\bar{t} = \text{g.c.d.}\ (q-1, e(K_q|Q_q))$, where $e(K_q|Q_q)$ denotes the ramification index of the local field K_q over Q_q. Since $e(K_q|Q_q) = e_q(K|Q)$, $t = \bar{t}$. Let $\bar{E}$ denote the unique subfield of $Q_q(\zeta_q)$ of degree t over Q_q. $\bar{E} \supseteq \bar{F}$ and $[Q_q(\zeta_q):E] = [Q(\zeta_q):E]$. This gives the following diagram of fields

(**)



with $[K_q\bar{E}: K_q] = [\bar{E}: \bar{F}]$ and $[K_q(\zeta_q): K_q\bar{E}] = [Q(\zeta_q): E]$. Again by Abhyankar's Lemma, $K_q\bar{E}$ is an unramified extension of K_q and $K_q(\zeta_q)$ is a totally ramified extension of $K_q\bar{E}$.

With the above notation, we have shown

PROPOSITION 1. *Let p be a rational prime. The following are equivalent:*
(a) $[K(\zeta_q): K]_p = [K_q(\zeta_q): K_q]_p$,
(b) $[E: F]_p = [\bar{E}: \bar{F}]_p$,
(c) $[F: Q]_p = [\bar{F}: Q_q]_p$.

COROLLARY 2. *If $p \nmid [E: F]$, then $e(K_q(\zeta_q)K_q)_p = [K_q(\zeta_q): K_q]_p = [K(\zeta_q)K]_p = e_q(K(\zeta_q)K)_p$.*

PROOF. $p \nmid [E: F]$ implies $[E: F]_p = [\bar{E}: \bar{F}]_p = 0$. The result then follows from the proposition, as $F \supseteq F_q$ and KE/K and $K_q\bar{E}/K_q$ are totally unramified while $K(\zeta_q)/KE$ and $K_q(\zeta_q)/K_q\bar{E}$ are totally ramified at q.

THEOREM 3. *Let X be an irreducible character of a finite group G of exponent n. Suppose $m_Q(X) \geqslant 3$ and p is a prime with $p^c \| m_Q(X)$, $c > 0$. Let r be the smallest positive integer such that $Q(\zeta_r) \supset Q(X)$ and $q_1, q_2, \ldots, q_t$ the distinct rational primes with $[\mathrm{ind}_{q_i} A(X; Q)]_p = p^{a_i}$, $a_i \geqslant 1$. Suppose that for each q_i, $i = 1, \ldots, t$, we have $e_{q_i}(K(\zeta_{q_i})/K)_p = [K(\zeta_{q_i}): K]_p$. Then there exists an extension field L of K contained in $Q(\zeta_n)$ with $[L: K] = p^c$ and $p \nmid \mathrm{ind}(L \otimes_K A(X, Q))$.*

PROOF. Since $p^c = \text{l.c.m.}\ \{p^{a_1}, p^{a_2}, \ldots, p^{a_t}\}$ we have $a_i \leqslant c$ and $a_i = c$ for some i. We can suppose that $a_1 = c$. By the theorem of Benard and Shacher [**1**], $\zeta_{p^c} \in K$. Pick α_i in $K(\zeta_{q_i})$ with $\alpha_i^{p^{a_i}} \in K$ and $[K(\alpha_i): K] = p^{a_i}$. By the assumption, q_i is totally ramified in $K(\alpha_i)/K$ and q_j is unramified in $K(\alpha_i)/K$ for $i \neq j$. Let $\alpha = \alpha_1\alpha_2 \cdots \alpha_t$. $K(\alpha, \alpha/\alpha_i) = K(\alpha_i, \alpha/\alpha_i)$ implying $e_{q_i}(K(\alpha)/K) = p^{a_i}$ and thus $[K(\alpha): K] = p^c$. If $p^c \geqslant 3$ or all q_i are odd, then $L = K(\alpha)$ is the desired splitting field since $A(X; Q)$ has trivial index at any infinite prime. Similarly, if $p^c = 2$ and all q_i are odd. If $p = 2$ and $q_i = 2$ we find L as in Mollin [**9**, p. 109].

In the following, $h(K)$ denotes the class number of K and $Q(\zeta_r)$ denotes the smallest root of unity field containing K.

COROLLARY 4 (MOLLIN). *Let G be a finite group of exponent n, X an irreducible character of G and $m_Q(X) \geqslant 3$. Suppose that $p^c \| m(X)$ with $c > 0$ and $p \nmid [Q(\zeta_r): K]$. Then there exists a field L with $K \subset L \subset Q(\zeta_n)$, $[L: K] = p^c$ and $p \nmid \mathrm{ind}(L \otimes_K A(X; Q))$.*

PROOF. Let $q_1, q_2, \ldots, q_t$ be the rational primes for which $p \mid \mathrm{ind}_{q_i} A(X; Q)$. If $1 \leqslant i \leqslant t$, by the linear disjointness of full cyclotomic fields over Q, $Q(\zeta_r) \cap Q(\zeta_{q_i})$ is either $Q(\zeta_{q_i})$ or Q. If $Q(\zeta_r) \cap Q(\zeta_{q_i}) = Q(\zeta_{q_i})$, then $A(X, Q) \otimes_K A(\zeta_r) = B$ is a central simple algebra with index still divisible by p^c, since $p \nmid [Q(\zeta_r): K]$. Similarly $p \mid \mathrm{ind}_{q_i} B$. But then $B \otimes K_{q_i}$, has a nontrivial index and contains a q_ith root of unity in its center contradicting [**10**, Theorem 4.4]. Hence we must have $Q(\zeta_r) \cap Q(\zeta_{q_i}) = Q$

and q_i is unramified in K/Q. Looking at (*), we see that $E = F = Q$. From Corollary 2, $e_{q_i}(K(\zeta_{q_i})/K)_p = [K(\zeta_{q_i}) : K]_p$ and the result follows via Theorem 3. □

COROLLARY 5. *Let G be a finite group of exponent n, X an irreducible character of G and $m_Q(X) \geq 3$. Suppose that $p^c \| m(X)$, $c > 0$ and $p \nmid h(K)$. Then there exists a field L with $K \subset L \subset Q(\zeta_n)$, $[L : K] = p^c$ and $p \nmid \operatorname{ind}(L \otimes_K A(X : Q))$.*

PROOF. From class field theory, $p \nmid h(K)$ implies there are no unramified abelian extensions of K of degree p. By (*), $p \nmid [KE : K]$ and so $e_{q_i}(K(\zeta_{q_i})/K)_p = [K(\zeta_{q_i}) : K]_p$ for any prime q_i. By Theorem 3, the result follows. □

These corollaries can be combined to give a generalization of Mollin's result [**9**, Corollary 1].

COROLLARY 6. *Let G be a finite group of exponent n, X an irreducible character of G and $m(X) \geq 3$. Suppose that $1 = (m(X), [Q(\zeta_r) : K], h(K))$. Then there exists a splitting field L of X with $[L : K] = m(X)$ and $K \subset L \subset Q(\zeta_n)$.*

PROOF. Write $m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$. If $p_i \mid m(X)$ and $p \nmid h(K)$, find a field L_i as in Corollary 5. If $p_j \mid (m(X), h(K))$, then $p_j \nmid [Q(\zeta_r) : K]$ and find a field L_j as in Corollary 4. Then $L = L_1 L_2 \cdots L_s$ is the desired splitting field. □

The following extends Corollary 4.

COROLLARY 7. *Let G be a finite group of exponent n, X an irreducible character of G, $m(X) \geq 3$, and p a prime with $p^c \| m(X)$, $c > 0$. Let $q_1, q_2, \ldots, q_t$ be the distinct rational primes such that $p \mid \operatorname{ind}_{q_i}(A(X; Q))$ and suppose that $p \nmid e_{q_i}(Q(\zeta_r) \mid K)$. Then there exists a field L with $K \subset L \subset Q(\zeta_n)$, $[L : K] = p^c$ and $p \nmid \operatorname{ind}(L \otimes_K A(X; Q))$.*

PROOF. We claim that $Q(\zeta_r) \cap Q(\zeta_{q_i}) = Q$. Otherwise, we can assume that q_i is odd and $Q(\zeta_r) \cap Q(\zeta_{q_i}) = Q(\zeta_{q_i})$ and $q_i \mid r$. Write $n = q^s u$ with $(u, q) = 1$. $(e(K_q \mid \zeta_u)K_q) = 1$. As q_i has ramification index relatively prime to p in $Q(\zeta_n) \mid K$, also $(e(K_q(\zeta_{q^s}) \mid K_q), p) = 1$. Let I be the inertia subfield (maximal unramified extension) of K_q in $K_q(\zeta_n)$.

Then $([K_q(\zeta_n) : I], p) = 1$. Because $\operatorname{Gal}(I \mid K_q)$ is isomorphic to a factor group of the finite abelian group $\operatorname{Gal}(K_q(\zeta_n) \mid K_q)$, then $\operatorname{Gal}(I \mid K_q)$ is isomorphic to a subgroup of $\operatorname{Gal}(K_q(\zeta_n) \mid K_q)$ and in particular the p-Sylow subgroup of $\operatorname{Gal}(I \mid K_q)$ is isomorphic to the p-Sylow subgroup of $\operatorname{Gal}(K_q(\zeta_n) \mid K_q)$. But $I \mid K_q$ is an unramified extension and thus the p-Sylow subgroup of $\operatorname{Gal}(I \mid K_q)$ is cyclic. If $p \neq 2$, by the theorem of Goldschmidt and Isaacs [**7**], we have that $p \nmid m_Q(X)$, a contradiction, while if $p = 2$ and q is odd, we have that -1 is a sum of two squares in K_q ([**10**, Lemma 2.2]) as $K_q \supset Q_q$. By Fein's theorem [**5**], again $2 \nmid m_Q(X)$. In either case we have a contradiction and have established the claim.

Thus q_i is unramified in $K \mid Q$. By (*) we see that $E = F = Q$, and from Corollary 2, $e_{q_i}(K(\zeta_{q_i}) \mid K)_p = [K(\zeta_q) : K]_p$. By Theorem 3 the result follows.

We observe that, it is sufficient to assume in Theorem 3 through Corollary 7, that $K(X)$ is a nonreal field, rather than $m(X) \geq 3$, since that will guarantee that all infinite prime completions of the number field will be complex. Also the "splitting field", L, constructed in each case is a cyclic extension of K.

REFERENCES

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

2. G. Cornell, *Abhyankar's lemma and the class group* (Proc. Illinois Number Theory Conf.), Lecture Notes in Math., vol. 751, Springer-Verlag, Berlin and New York, 1979, pp. 82–88.

3. B. Fein, *Minimal splitting fields for group representations*, Pacific J. Math. **51** (1974), 427–431.

4. _____, *Minimal splitting fields for group representations*. II, Pacific J. Math. **77** (1978), 445–449.

5. _____, *Schur indices and sums of squares*, Proc. Amer. Math. Soc. **51** (1975), 31–34.

6. C. Ford, *Groups which determine the Schur index of a representation*, J. Algebra **57** (1979), 339–354.

7. D. Goldschmidt and I. Isaacs, *Schur indices in finite groups*, J. Algebra **33** (1975), 191–199.

8. H. Hasse, *Number theory*, Springer-Verlag, Berlin and New York, 1980.

9. R. Mollin, *Splitting fields and group characters*, J. Reine Angew. Math. **315** (1980), 107–114.

10. E. Spiegel and A. Trojan, *On semi-simple group algebras*. II, Pacific J. Math. **66** (1976), 553–559.

11. T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Math., vol. 397, Springer-Verlag, Berlin and New York, 1974.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CONNECTICUT, STORRS, CONNECTICUT 06268

DEPARTMENT OF MATHEMATICS, ATKINSON COLLEGE, YORK UNIVERSITY, DOWNSVIEW, ONTARIO M3J 1P3, CANADA