



Minimal Cyclotomic Splitting Fields for Group Characters

R. A. Mollin

Proceedings of the American Mathematical Society, Vol. 91, No. 3 (Jul., 1984), 359-363.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9939%28198407%2991%3A3%3C359%3AMCSFFG%3E2.0.CO%3B2-I>

Proceedings of the American Mathematical Society is currently published by American Mathematical Society.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/ams.html>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is an independent not-for-profit organization dedicated to creating and preserving a digital archive of scholarly journals. For more information regarding JSTOR, please contact support@jstor.org.

MINIMAL CYCLOTOMIC SPLITTING FIELDS FOR GROUP CHARACTERS

R. A. MOLLIN¹

ABSTRACT. Let F be a finite Galois extension of the rational number field Q , and let G be a finite group of exponent n with absolutely irreducible character χ . This paper provides sufficient conditions for the existence of a minimal degree splitting field L with $F(\chi) \subseteq L \subseteq F(\varepsilon_n)$, where ε_n is a primitive n th root of unity. We obtain as immediate corollaries known results pertaining to this question in the literature. Moreover we obtain necessary *and* sufficient conditions for the existence of a minimal splitting field L as above which is *cyclic* over $F(\chi)$. The machinery we use to achieve the above results are certain genus numbers of $F(\chi)$.

1. Introduction. Let F be a finite Galois extension of Q , G a finite group of exponent n , χ a complex irreducible character of G , and let $A(\chi, F)$ denote the simple component of FG corresponding to χ . A finite extension L of $F(\chi)$ is a *splitting field* for χ over F if the class of $A(\chi, F) \otimes_{F(\chi)} L$ is equivalent to L in the Brauer group $B(L)$ of L . The minimum of the degrees $|L : F(\chi)|$ of L over $F(\chi)$ taken over all splitting fields L of χ is the *Schur index* $m_F(\chi)$ of χ over F . It is the purpose of this paper to provide sufficient conditions for the existence of a splitting field L of χ such that $F(\chi) \subseteq L \subseteq F(\varepsilon_n)$ and $|L : F(\chi)| = m_F(\chi)$. Under a suitable restriction we generalize this to a field F of characteristic zero. Moreover, we are able to provide necessary *and* sufficient conditions for such an L to exist, where L is *cyclic* over $F(\chi)$.

The above results continue work begun in [Mo 1] and advances [Fe 1], [Fe 2] and the more recent [Sp-T].

2. Notation and preliminaries. Relevant notation or concepts not discussed may be found in [Mo 1]. Let K be a finite Galois extension of an algebraic number field F with Galois group $G(K/F)$. When $G(K/F)$ is abelian we adopt the convention of [Mo 1] with respect to decomposition of primes; i.e. if \hat{p} is a K -prime above the F -prime p then any reference to the decomposition of \hat{p} in K over F shall be made instead to the decomposition of p in K/F . Moreover, in this case we write K_p for $K_{\hat{p}}$, the completion of K at \hat{p} .

Now let $A(\chi, F)$ be as in §1; then if \hat{q} and q' are $F(\chi)$ -primes above the same rational prime q then $A(\chi, F) \otimes_{F(\chi)} F(\chi)_{\hat{q}}$ and $A(\chi, F) \otimes_{F(\chi)} F(\chi)_{q'}$ have the same index (we proved this in [Mo 2]–[Mo 3] as a generalization of [Be]). Denote the common value of all indices of $A(\chi, F) \otimes_{F(\chi)} F(\chi)_{\hat{q}}$ for all $F(\chi)$ -primes \hat{q} above a given rational prime q by $\text{ind}_q(A(\chi, F))$ called the q *local index* of $A(\chi, F)$.

Received by the editors April 25, 1983.

1980 *Mathematics Subject Classification.* Primary 20C05.

¹The author's research is supported by N.S.E.R.C. Canada.

©1984 American Mathematical Society
0002-9939/84 \$1.00 + \$.25 per page

For an algebraic number field F we denote the *genus field* of F by \tilde{F} which is defined as the maximal abelian extension of F , such that \tilde{F} is the composite of an abelian extension of Q with F and is unramified at all finite primes (see [Ish] for details). $|\tilde{F} : F| = g(F)$ is called the *genus number* of F . We define the n th *genus field* for a given positive integer n as $\tilde{F}^{(n)} = \tilde{F} \cap F(\varepsilon_n)$. We call $|\tilde{F}^{(n)} : F| = g_n(F)$ the n th *genus number* of F . It is this number which will provide the machinery for the major result of this paper.

3. Splitting fields.

LEMMA 1. *Let F be a finite Galois extension of Q , and let n be a positive integer. Suppose that $G = G(F(\varepsilon_n)/F)$ is cyclic of prime power order. Then we have that $g_n(F) = |T^{(q)} : F|$ where $T^{(q)}$ is the inertia field of an F -prime q having nontrivial ramification in $F(\varepsilon_n)$. Furthermore if n is divisible by at least two distinct primes then $g_n(F) = |Z^{(q)} : F|$ where $Z^{(q)}$ is the decomposition subfield of $F(\varepsilon_n)$ over F at q .*

PROOF. The inertia subgroup $I^{(q)}$ of G at q is contained in $G(F(\varepsilon_n)/F(\varepsilon))$ where ε is a root of unity in $F(\varepsilon_n)$ having largest possible order relatively prime to $p = q \cap Q$ (see [Nark, Theorem 5.9, p. 210]). Since G is cyclic of prime power order it follows that only F -primes above p may ramify in $F(\varepsilon_n)$. Since F is Galois over Q then $I^{(q)} = I^{(q')}$ for any F -primes q and q' above p . Hence $g_n(F) = |T^{(q)} : F|$.

Now suppose $n = q^a t$ where q and t are relatively prime, $t > 1$, and q lies above p . Then $F_q(\varepsilon_t)$ is nontrivial cyclic unramified over F_q if $Z^{(q)} \neq T^{(q)}$. Moreover by hypothesis $G(F_q(\varepsilon_{q^a})/F_q)$ is nontrivial. Hence $G(F_q(\varepsilon_n)/F_q)$ is generated by at least 2 elements. Since $G(F_q(\varepsilon_n)/F_q) \cong G(F(\varepsilon_n)/Z^{(q)})$, the decomposition subgroup of G at q , then G is not cyclic, a contradiction. Hence $g_n(F) = |Z^{(q)} : F|$. \square

Now we set the stage for the main result. Let χ be a complex irreducible character of a finite group of exponent n , and set $A = A(\chi, F)$ where F is finite Galois over Q . Let $S(A)$ be defined as the set of all rational primes q such that $\text{ind}_q(A) > 1$. We now define, for convenience sake, a field L to have (n, F) -*splitting property* provided that L is a splitting field of χ such that $F(\chi) \subseteq L \subseteq F(\varepsilon_n)$ and $|L : F(\chi)| = m_F(\chi)$. Moreover let $K = F(\chi)$ henceforth.

THEOREM 1. *Let χ be a complex irreducible character of a finite group of exponent n , and set $A = A(\chi, F)$ where F is a finite Galois extension of Q such that if K is real then $2 \notin S(A)$. If for all finite odd $q \in S(A)$ we have that $|g_q(K)|_p \leq |m_F(\chi)/\text{ind}_q(A)|_p$ for each $p|m_F(\chi)$ then there exists an L with (n, F) -splitting property.*

PROOF. By the same reasoning as in the proof of [Mo 1] we may assume that $m_F(\chi) = p^a$ where p is prime.

Let $q \in S(A)$ where q is finite odd. Suppose furthermore that $\text{ind}_q(A) = p^b$. From [Ya, Theorem 4.7, p. 46] we may deduce that there exists a subfield $M^{(q)} \subseteq K(\varepsilon_q)$ such that $|M_{\hat{q}}^{(q)} : K_{\hat{q}}| = \text{ind}_q(A)$ where \hat{q} is any K -prime above q . However

$$|M^{(q)} : K| = |M^{(q)} : T^{(\hat{q})}| |T^{(\hat{q})} : K| = p^b |T^{(\hat{q})} : K| = p^b |g_q(K)|_p$$

by Lemma 1, where $T^{(\hat{q})}$ is the inertia subfield of $K(\varepsilon_q)$ over K at \hat{q} . Thus by hypothesis we have $|M^{(q)} : K| \leq p^a$.

Therefore, for each finite odd $q \in S(A)$ we have a field $M^{(q)}$ such that $M^{(q)}$ splits χ at q and $|M^{(q)} : K| \leq p^a$. By [Ya, Theorem 6.2, p. 89] we have that ε_{p^a} is in K ; so $M^{(q)} = K(\theta(q))$ where $\theta(q)^{p^a} \in K$.

Now we construct L according to the contents of $S(A)$.

Case (1). If all $q \in S(A)$ are finite odd then choose α as in [Mo 5]. Therefore $|K_{\hat{q}}(\alpha) : K_{\hat{q}}| = \text{ind}_q(A)$ for all $q \in S(A)$ where \hat{q} is any K -prime above q . However there exists a $q \in S(A)$ with $\text{ind}_q(A) = p^a$ so $L = K(\alpha)$ is the required field.

Case 2. If $2 \in S(A)$ then by hypothesis K is nonreal and thus only finite primes are contained in $S(A)$. By [Ya], $p^a = 2$ and $\sqrt{-1}$ is not in K . Now we choose α as in the proof of [Mo 1, Theorem 1, p. 108]. Then $L = K(\alpha)$ is the required field.

Case 3. If $q \in S(A)$ is infinite then K must be real so that by hypothesis $2 \notin S(A)$. Let $\alpha' = \prod \theta(q)$ where the product ranges over all finite primes q in $S(A)$. If $K(\alpha')$ is nonreal then choose $\alpha = \alpha'$ and choose $\alpha = \sqrt{-1} \cdot \alpha'$ otherwise. Hence $L = K(\alpha)$ is the required field. \square

Now we give a sequence of applications of Theorem 1. We anchor them to the theorem as corollaries thereof and for each corollary we maintain the first statement of Theorem 1 as being in force.

Under a suitable restriction we may generalize Theorem 1 to a field F of characteristic zero.

COROLLARY 1. *Let F be a field of characteristic zero such that $m_F(\chi) = m_{F'}(\chi)$ where $F' = F \cap Q(\varepsilon_n)$. Then there exists a field with (n, F) splitting property if and only if there exists a field with (n, F') splitting property.*

PROOF. By [Mo 4, Theorem 3.4, p. 473] we have $A(\chi, F) \cong A(\chi, Q) \otimes_{Q(\chi)} K$. When $m_F(\chi) = m_{F'}(\chi)$ the result clearly follows. (Note that in general we always have $m_F(\chi) | m_{F'}(\chi)$.) \square

The following generalizes [Sp-T, Corollary 5, p. 36] (see also [Mo 1, Corollary 1, p. 110]).

COROLLARY 2. *If $g(K)$ and $m_F(\chi)$ are relatively prime then there is a field with (n, F) -splitting property.*

PROOF. For each prime p dividing $m_F(\chi)$ we have $|g(K)|_p = 1$. Hence $|g_q(K)|_p = 1$ for each $q \in S(A)$. \square

We note that the converse of the above fails. We provide the following counterexample (which corrects [Mo 1, Example 2, p. 111] which was missed in [Mo 5]).

EXAMPLE 1. Let p be an arbitrary odd prime and q a prime with $q \equiv 1 \pmod{p^4}$ but $q \not\equiv 1 \pmod{p^5}$. Let

$$\langle \sigma \rangle = G(Q(\varepsilon_{p^3q})/Q(\varepsilon_{p^3})) \quad \text{and} \quad \langle \tau \rangle = G(Q(\varepsilon_{p^3q})/Q(\varepsilon_q)).$$

Set $\gamma = \sigma^{((q-1)/p^4)} \tau^{p(p-1)}$ and let K be the fixed field of $\langle \gamma \rangle$.

Let $G = \langle x, y, z : x^q = z^{p^3} = 1, y^{p^4} = z^p, z^p \text{ central, } yzy^{-1} = z^a \text{ and } yxy^{-1} = x^b \rangle$ where $\gamma : \varepsilon_{p^3} \rightarrow \varepsilon_{p^3}^a$ and $\gamma : \varepsilon_q \rightarrow \varepsilon_q^b$. Set $A = (Q(\varepsilon_{p^3q})/K, \varepsilon_{p^2})$, a crossed product algebra (see [Mo 1]) which is a homomorphic image of QG . Therefore there is a complex irreducible character χ of G with $A = A(\chi, Q)$, and $K = Q(\chi)$. As in [Mo 1], $\text{ind}_q(A) = p = m_Q(\chi)$ and in fact $S(A) = \{q\}$.

Also since $|G| = p^6q = n$ then by [Fe 1, Theorem 6, p. 429] there is a field with (n, Q) -splitting property. However $\tilde{K} = Q(\varepsilon_{p^3}, \theta)$ where $Q(\theta)$ is the unique subfield of $Q(\varepsilon_q)$ of degree $(q - 1)/p^3$ over Q ; i.e. $p|g(K)$. This completes the example.

The following generalizes [Sp-T, Corollary 7, p. 36].

COROLLARY 3. *Let $F(\varepsilon_r)$ be the smallest root of unity field with $K \subseteq F(\varepsilon_r)$. Suppose p does not divide the ramification index of any \hat{q} above $q \in S(A)$ in $F(\varepsilon_r)$ over K , for each $p|m_F(X)$. Then there is a field with (n, F) -splitting property.*

PROOF. As in the proof of [Sp-T, Corollary 7, p. 36] we get $|K_{\hat{q}}(\varepsilon_q) : K_{\hat{q}}| = |K(\varepsilon_q) : K|$. Hence $g_q(K) = 1$. \square

The following corollary which is immediate from the theorem generalizes the main result of [Mo 1, Theorem 1, p. 108].

COROLLARY 4. *If K is totally nonreal over Q and if for each prime $p|m_F(\chi)$ we have $|K(\varepsilon_q) : K|_p = |K_{\hat{q}}(\varepsilon_q) : K_{\hat{q}}|_p$ whenever \hat{q} is K -prime above an odd prime $q \in S(A)$ then there is a field with (n, F) -splitting property.*

The following uses Corollaries 3 and 4 to give a result which generalizes [Sp-T, Corollary 6, p. 36] which in turn generalized [Mo 1, Corollary 1, p. 110]. ε_r is as defined in Corollary 3.

COROLLARY 5. *Suppose that $1 = (m_F(\chi), |F(\varepsilon_r) : K|, g(K))$. Then there is a field with (n, F) -splitting property.*

PROOF. If

$$(m_F(\chi), g(K)) = 1$$

then we proceed as in Corollary 2. If $p|(m_F(\chi), g(K))$ then $p \nmid |F(\varepsilon_r) : K|$ and we proceed as in Corollary 3. \square

The next corollary generalizes the main result of [Sp-T, Theorem 3, p. 35].

COROLLARY 6. *Suppose that whenever $q \in S(A)$ and $p|\text{ind}_q(A)$ we have $|T^{(\hat{q})} : K|_p = 1$ where $T^{(\hat{q})}$ is the inertia subfield of $K(\varepsilon_q)$ over K at \hat{q} which lies over q . Then there is a field with (n, F) -splitting property.*

PROOF. The hypothesis forces $|g_q(K)|_p = 1$. \square

The converse of Corollary 6 fails as shown in

EXAMPLE 2. Take $p = 3$ and $q = 163$ in Example 1. Then $K(\varepsilon_q) = Q(\varepsilon_{3^3 \cdot 163})$ and $|K(\varepsilon_q) : K| = 3^4$ which is greater than $|K_q(\varepsilon_q) : K_q| = 3^3$ since 163 splits in $\tilde{K} = Q(\theta, \varepsilon_{p^3})$ as defined in Example 1. Now as in Example 1 we get $K = Q(\chi)$ for a complex irreducible character χ of G and an $A = A(\chi, Q)$ with $\text{ind}_q(A) = p = m_Q(\chi)$. Moreover there is a field with (n, F) -splitting property where n is the exponent of G . This secures the example.

Now we are able to achieve necessary and sufficient conditions for the existence of a field with (n, F) -splitting property which is cyclic over $F(\chi)$.

THEOREM 2. *Let $\chi, A, S(A), G, n, F$ and K be as above. Then there is a field L with (n, F) -splitting property such that L is cyclic over K if and only if for each p dividing $m_F(\chi)$ there is a decomposition $G_p = G(K(\varepsilon_n)/K)_p$ as a direct product of cyclic groups C_i with fixed field K_i such that for some i , say $i = 1$, we have that*

for all $q \in S(A)$, $|Z_1^{(q)} : K_1| \leq |m_F(\chi)/\text{ind}_q(A)|_p$ and $|K(\varepsilon_n) : K_1| \geq |m_F(\chi)|_p$ where $Z_1^{(q)}$ is the decomposition subfield of $K(\varepsilon_n)$ over K_1 at q .

PROOF. If such an L exists then, since L is cyclic over K , there is a decomposition such that $L \subseteq \bigcap_{i>1} K_i$ after possibly renumbering the K_i . Now since $Z_1^{(q)} \cap L$ is the p -part of the decomposition subfield of L over K at q for each $q \in S(A)$ then it follows that $|Z_1^{(q)} : K_1| \leq |m_F(\chi)/\text{ind}_q(A)|_p$. Moreover since $|K(\varepsilon_n) : K_1| \geq |L : K|_p$ then $|K(\varepsilon_n) : K_1| \geq |m_F(\chi)|_p$.

Conversely, suppose that we have such a decomposition. Then we may choose $L \subseteq \bigcap_{i>1} K_i$ such that $|L_q : K_q| = |\text{ind}_q(A)|_p$ for each $q \in S(A)$. Now for some $q \in S(A)$ we have that $|\text{ind}_q(A)|_p = |m_F(\chi)|_p$ and for this q we have $Z_1^{(q)} = K_1$. Since $Z_1^{(q)} \cap L = K$ is the decomposition subfield of L at q then $|L : K| = |m_F(\chi)|_p$. \square

Now as a consequence of Theorem 2 we easily generalize [Fe 1, Theorem (b), p. 429] which we could not accomplish in [Mo 1]. The above notation remains in force.

COROLLARY 7. Suppose $m_F(\chi) \geq 3$ and $n = p^a q^b$ for primes $p < q$ then there exists a cyclic field with (n, F) -splitting property.

PROOF. By [Gold-Is] (see also [Mo 6]) $G_p = G(K(\varepsilon_n)/K)_p$ is not cyclic. Now since $K(\varepsilon_{p^a})$ is cyclic over K then there is a decomposition of G_p as a product of cyclic groups $C_1 \times C_2$ with $K(\varepsilon_n)$ totally ramified over K_1 at q . \square

REFERENCES

[Be] M. Benard, *The Schur subgroup*. I, J. Algebra **22** (1972), 374–377.
 [Cor] 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.
 [Fe 1] B. Fein, *Minimal splitting fields for group representations*, Pacific J. Math. **51** (1974), 427–431.
 [Fe 2] —, *Minimal splitting fields for group representations*. II, Pacific J. Math. **77** (1978), 445–449.
 [Gold-Is] D. Goldschmidt and I. Isaacs, *Schur indices in finite groups*, J. Algebra **33** (2) (1975), 191–199.
 [Ish] M. Ishida, *The genus fields of algebraic number fields*, Lecture Notes in Math., Vol. 555, Springer-Verlag, Berlin and New York, 1976.
 [Mo 1] R. Mollin, *Splitting fields and group characters*, J. Reine Angew. Math. **315** (1980), 107–114.
 [Mo 2] —, *Generalized uniform distribution of Hasse invariants*, Comm. Algebra **5** (1977), 245–266.
 [Mo 3] —, *Uniformly distributed Hasse invariant*, preprint.
 [Mo 4] —, *The Schur group of a field of characteristic zero*, Pacific J. Math. **76** (1978), 471–478.
 [Mo 5] —, *Correction to the paper: Splitting fields and group characters*, J. Reine Angew. Math. **327** (1981), 219–220.
 [Mo 6] *Schur indices, sums of squares and splitting fields*, C. R. Math. Rep. Acad. Sci. Canada **3** (1981), 301–306.
 [Nark] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Scientific Publishers, Warsaw, 1974.
 [Rib] P. Ribenboim, *Algebraic numbers*, Wiley Interscience, New York, 1972.
 [Sp-T] E. Spiegel and A. Trojan, *Minimal splitting fields in cyclotomic extensions*, Proc. Amer. Math. Soc. **87** (1983), 33–37.
 [Ya] T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Math., Vol. 397, Springer-Verlag, Berlin and New York, 1974.