MINIMAL CYCLOTOMIC SPLITTING FIELDS FOR GROUP CHARACTERS

R. A. MOLLIN

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 $\chi$. 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 $\varepsilon_n$ 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 $n$, $\chi$ a complex irreducible character of $G$, and let $A(\chi, F)$ denote the simple component of $FG$ corresponding to $\chi$. A finite extension $L$ of $F(\chi)$ is a splitting field for $\chi$ 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 $\chi$ is the Schur index $m_F(\chi)$ of $\chi$ over $F$. It is the purpose of this paper to provide sufficient conditions for the existence of a splitting field $L$ of $\chi$ 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 $p$ is a $K$-prime above the $F$-prime $p$ then any reference to the decomposition of $p$ in $K$ over $F$ shall be made instead to the decomposition of $p$ in $K/F$. Moreover, in this case we write $K_\hat{p}$ for $K_{p\hat{}}$, the completion of $K$ at $\hat{p}$.

Now let $A(\chi, F)$ be as in §1; then if $\hat{q}$ and $\hat{q}'$ are $F(\chi)$-primes above the same rational prime $q$ then $A(\chi, F) \otimes_{F(\chi)} F(\chi)_{\hat{q}}$ and $A(\chi, F) \otimes_{F(\chi)} F(\chi)_{\hat{q}'}$ 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.

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

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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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 $F^{(n)} = \tilde{F} \cap F(\varepsilon_n)$. We call $|F^{(n)} : F| = g_n(F)$ 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 $\varepsilon$ 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 $n = q^at$ 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 $g_n(F) = |Z^{(q)} : F|$. □

Now we set the stage for the main result. Let $\chi$ 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 $\chi$ 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 $\chi$ 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 $|M^{(q)} : K_{\hat{q}}| = \text{ind}_q(A)$ where $\hat{q}$ is any $K$-prime above $q$. However $|M^{(q)} : K| = |M^{(q)} : T^{(q')}| |T^{(q')} : K| = p^b |T^{(q')} : K| = p^b |g_q(K)|_p$ 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 \( \chi \) at \( q \) and \(|M^{(q)} : K| \leq p^a \). By [Ya, Theorem 6.2, p. 89] we have that \( \varepsilon_{p^a} \) 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 \( \alpha \) as in [Mo 5]. Therefore \(|K_q^{(\alpha)} : K_q| = \text{ind}_q(A) \) for all \( q \in S(A) \) where \( q \) 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 \( \alpha \) 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 \( 2 \not\in S(A) \). 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 \( A(\chi,F) = A(\chi,Q) \otimes_Q K \). 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 \(|g(K)|_p = 1 \) 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 \( q \equiv 1 \) (mod \( p^4 \)) but \( q \not\equiv 1 \) (mod \( p^5 \)). Let

\[
\langle \sigma \rangle = G(Q(\varepsilon_{p^4q}))/Q(\varepsilon_{p^3}) \quad \text{and} \quad \langle \tau \rangle = G(Q(\varepsilon_{p^3q}))/Q(\varepsilon_q).
\]

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

Let \( G = \langle x, y, z : x^4 = z^{p^3} = 1, y^{p^4} = z^p, z^p \text{ central}, yzy^{-1} = z^a \text{ and } yxy^{-1} = x^b \rangle \) where \( \varepsilon_{p^3} \rightarrow \varepsilon_{p^3}^a \) and \( \varepsilon_q \rightarrow \varepsilon_q^b \). Set \( A = (Q(\varepsilon_{p^4q})/K, \varepsilon_{p^4}) \), a crossed product algebra (see [Mo 1]) which is a homomorphic image of \( QG \). Therefore there is a complex irreducible character \( \chi \) 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 $|G| = p^6 q = n$ then by [Fe 1, Theorem 6, p. 429] there is a field with $(n, Q)$-splitting property. However $\bar{K} = Q(\epsilon_{p^3}, \theta)$ where $Q(\theta)$ is the unique subfield of $Q(\epsilon_q)$ 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 $F(\epsilon_r)$ be the smallest root of unity field with $K \subseteq F(\epsilon_r)$. Suppose $p$ does not divide the ramification index of any $\hat{q}$ above $q \in S(A)$ in $F(\epsilon_r)$ 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 $|K_{\hat{q}}(\epsilon_q) : K_{\hat{q}}| = |K(\epsilon_q) : K|$. 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 $|K(\epsilon_q) : K|_p = |K(\epsilon_q) : K_d|_p$ 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]. $\epsilon_r$ is as defined in Corollary 3.

**COROLLARY 5.** Suppose that $1 = (m_F(\chi), |F(\epsilon_r) : K|, g(K))$. 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 $p \nmid |F(\epsilon_r) : K|$ 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 $|T^{(q)} : K|_p = 1$ where $T^{(q)}$ is the inertia subfield of $K(\epsilon_q)$ over $K$ at $q$ 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 $K(\epsilon_q) = Q(\epsilon_{3^{34} 163})$ and $|K(\epsilon_q) : K| = 3^4$ which is greater than $|K_q(\epsilon_q) : K_q| = 3^3$ since $163$ splits in $\bar{K} = Q(\epsilon, \epsilon_{p^3})$ as defined in Example 1. Now as in Example 1 we get $K = Q(\chi)$ for a complex irreducible character $\chi$ 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 $G_p = G(K(\epsilon_n)/K)_p$ 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 \( |L : K| = |m_F(\chi)|_p \). □

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 \( K(\varepsilon_n) \) 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 \( q \). □

**References**


