A NOTE ON SPLITTING FIELDS OF REPRESENTATIONS OF FINITE GROUPS

BY

PAUL FONG

Let $\mathfrak{G}$ be a finite group, and let χ be the character of an absolutely irreducible representation $\mathfrak{X}$ of $\mathfrak{G}$. An algebraic number field K is defined to be a splitting field of χ if $\mathfrak{X}$ can be written in the field $K(\chi)$, where $K(\chi)$ is the field generated by K and the values of χ. The existence of splitting fields with suitable properties has been of fundamental importance in the study of group characters. In [1, Lemma 1], Brauer proved the following result.

(A) Let $\mathfrak{G}$ be a finite group of order $g = p^a m$, where p is a rational prime and $(p, m) = 1$. Then there exists an algebraic number field K with the following properties:

(i) K contains the m^{th} roots of unity ε_m.
(ii) The prime p does not ramify in K.
(iii) K is a splitting field of every irreducible character χ of $\mathfrak{G}$.

Fields K which satisfy the conditions of (A) are called splitting fields of least possible ramification. A recent result by Solomon [9, Corollary, p. 163] is related to (A).

(B) Let $\mathfrak{G}$ be a finite group of order $g = p^a m$, where p is a rational prime and $(p, m) = 1$. Let Q be the rational field, and let $K = Q(\varepsilon_m)$ if p is odd, $K = Q(\varepsilon_m, \sqrt{-1})$ if $p = 2$. If χ is an irreducible character of $\mathfrak{G}$, then the Schur index $m_K(\chi)$ of χ with respect to K divides $p - 1$.

In this paper an improvement of Solomon's result will be given. Namely, the conclusion of (B) can be strengthened to the following: The Schur index $m_K(\chi) = 1$. In particular, for p odd, the field $Q(\varepsilon_m)$ is a splitting field of least possible ramification. A modification of the proof will show that for $p = 2$, the field $Q(\varepsilon_m, \sqrt[3]{1})$ is a splitting field of least possible ramification. The proofs are based on a theorem of Solomon together with some results from modular representation theory. The use of the Hasse Theorem of class field theory, which up to now has been necessary in the proof of (A), can thus be avoided.

Notation. $\mathfrak{G}$ will always be a fixed finite group of order $g = p^a m$, where p is a rational prime and $(p, m) = 1$. A subgroup $\mathfrak{H}$ of $\mathfrak{G}$ is elementary if $\mathfrak{H}$ is a direct product $\mathfrak{H} = \mathfrak{A} \times \mathfrak{Q}$, where $\mathfrak{A}$ is a cyclic group, and where $\mathfrak{Q}$ is a q-group for some prime q not dividing the order $(\mathfrak{A}:1)$ of $\mathfrak{A}$. A subgroup $\mathfrak{H}$ of $\mathfrak{G}$ is a p'-subgroup if p does not divide $(\mathfrak{H}:1)$. Absolutely irreducible char-

Received April 9, 1962.

acters or representations will simply be referred to as the irreducible characters or representations of $\mathfrak{G}$.

1. Results from modular representation theory

In this section, the prime p will be fixed. All reference to modular representation theory will then be with respect to this prime p. The following lemma is due to Brauer [2, Theorem 5]. The proof below is a modified version of the original proof.

LEMMA 1. *Let Φ_ρ be a modular principal indecomposable character of the finite group $\mathfrak{G}$. Then Φ_ρ is a linear combination with integer coefficients of characters of $\mathfrak{G}$ induced by characters of elementary subgroups of p'-order.*

Proof. By a theorem of Brauer [4, Theorem A], the 1-character of $\mathfrak{G}$ can be expressed as

$$1 = \sum a_i \psi_i^* ,$$

where a_i are rational integers, and where ψ_i^* is the character of $\mathfrak{G}$ induced by an irreducible character ψ_i of an elementary subgroup $\mathfrak{H}_i$ of $\mathfrak{G}$. In particular,

$$\Phi_\rho = \sum a_i(\psi_i^* \Phi_\rho) = \sum a_i(\psi_i \Phi_\rho \mid \mathfrak{H}_i)^*.$$

The character $\psi_i \cdot \Phi_\rho \mid \mathfrak{H}_i$ vanishes on p-singular elements of $\mathfrak{H}_i$, and hence must be a linear combination of the principal indecomposable characters of $\mathfrak{H}_i$. The coefficients in such a linear combination are moreover integers by [3, Theorem 17]. But since $\mathfrak{H}_i$ is an elementary subgroup, $\mathfrak{H}_i$ can be factored into a direct product $\mathfrak{H}_i = \mathfrak{P}_i \times \mathfrak{R}_i$, where $\mathfrak{P}_i$ is a p-group and $\mathfrak{R}_i$ is a p'-group. Each principal indecomposable character of $\mathfrak{H}_i$ is thus the product of the character of the regular representation of $\mathfrak{P}_i$ with a suitable irreducible character of $\mathfrak{R}_i$. The principal indecomposable characters of $\mathfrak{H}_i$ are therefore induced by the irreducible characters of $\mathfrak{R}_i$. This proves the lemma.

LEMMA 2. *Let $\mathfrak{G}$ be a finite group of order $g = p^a m$, where p is a rational prime and $(p, m) = 1$. Let Φ_ρ be a principal indecomposable character of $\mathfrak{G}$. If $\mathfrak{U}_\rho$ is a representation of $\mathfrak{G}$ with character Φ_ρ, then $\mathfrak{U}_\rho$ can be written in the field $Q(\varepsilon_m)$.*

Proof. By Lemma 1

$$(1) \qquad \Phi_\rho = \sum a_i \psi_i^* ,$$

where the a_i are rational integers, and where ψ_i is an irreducible character of a p'-subgroup $\mathfrak{H}_i$ of $\mathfrak{G}$. Rearrange the sum (1) so that

$$(2) \qquad \Phi_\rho + \sum b_i \psi_i^* = \sum c_j \psi_j^* ,$$

where the integers b_i and c_j are positive. Each ψ_i is the character of a representation $\mathfrak{F}_i$ which can be written in $Q(\varepsilon_m)$, since the order of $\mathfrak{H}_i$ divides m.

We may assume that the $\mathfrak{F}_i$ are actually representations written in $Q(\varepsilon_m)$. If $\mathfrak{F}_i^*$ is the representation of $\mathfrak{G}$ induced by $\mathfrak{F}_i$, then (2) implies that

$$\mathfrak{U}_\rho + \sum b_i \mathfrak{F}_i^* \simeq \sum c_j \mathfrak{F}_j^* , \tag{3}$$

where the sum of representations denotes the direct sum. The representations $\sum b_i \mathfrak{F}_i^*$, $\sum c_j \mathfrak{F}_j^*$ are written in $Q(\varepsilon_m)$. If these have common components over $Q(\varepsilon_m)$, remove the component from both representations. Repeat this until (3) reduces to

$$\mathfrak{U}_\rho \oplus \mathfrak{V} \simeq \mathfrak{W},$$

where $\mathfrak{V}$ and $\mathfrak{W}$ are representations of $\mathfrak{G}$ written in $Q(\varepsilon_m)$, such that $\mathfrak{V}$ and $\mathfrak{W}$ have no common components over $Q(\varepsilon_m)$. If $\mathfrak{V}$ is not the zero representation, then $\mathfrak{V}$ and $\mathfrak{W}$ would have a common absolutely irreducible component, which is impossible. Therefore $\mathfrak{U}_\rho \simeq \mathfrak{W}$, and the lemma is proved.

LEMMA 3. *Let $\mathfrak{H}$ be a finite group with a normal cyclic Sylow p-subgroup $\mathfrak{P}$. If $\mathfrak{H}/\mathfrak{P}$ is abelian, then the decomposition numbers $d_{\mu\rho}$ are* 0 *or* 1.

Proof. We proceed by induction on $(\mathfrak{H}:1)$. Let $\tilde{\mathfrak{H}}$ be a maximal normal subgroup of $\mathfrak{H}$, $\mathfrak{P} \leqq \tilde{\mathfrak{H}} < \mathfrak{H}$. The index $(\mathfrak{H}:\tilde{\mathfrak{H}})$ is then a prime $q \neq p$. The irreducible modular representations of $\mathfrak{H}$ contain $\mathfrak{P}$ in their kernel, and can therefore be identified with the ordinary irreducible representations of $\mathfrak{H}/\mathfrak{P}$. In particular, if $(\mathfrak{H}:\mathfrak{P}) = r$, then $\mathfrak{H}$ has r irreducible modular characters, and these are all linear. Let χ_μ be an irreducible character of $\mathfrak{H}$, and let

$$\chi_\mu = \sum d_{\mu\rho} \phi_\rho$$

be the decomposition of χ_μ into a sum of irreducible modular characters ϕ_ρ.

Case 1. If $\chi_\mu \mid \tilde{\mathfrak{H}}$ is irreducible, then $(\chi_\mu \mid \tilde{\mathfrak{H}}) = \sum d_{\mu\rho}(\phi_\rho \mid \tilde{\mathfrak{H}})$ is the modular decomposition of $(\chi_\mu \mid \tilde{\mathfrak{H}})$. The numbers $d_{\mu\rho}$ are therefore summands of the decomposition numbers of $(\chi_\mu \mid \tilde{\mathfrak{H}})$; by induction the $d_{\mu\rho}$ can only be 0 or 1.

Case 2. If $\chi_\mu \mid \tilde{\mathfrak{H}}$ is reducible, let $\tilde{\chi}_\mu$ be an irreducible constituent of the restriction. Let $\tilde{\chi}_\mu = \sum \tilde{d}_{\mu\rho} \tilde{\phi}_\rho$ be the modular decomposition of $\tilde{\chi}_\mu$; by induction the $\tilde{d}_{\mu\rho}$ are 0 or 1. Since $\mathfrak{H}/\mathfrak{P}$ is abelian, each irreducible modular character $\tilde{\phi}_\rho$ of $\tilde{\mathfrak{H}}$ has q distinct extensions to $\mathfrak{H}$, and indeed, the character of $\mathfrak{H}$ induced by $\tilde{\phi}_\rho$ is the sum of these q extensions. For $\tilde{\phi}_\rho \neq \tilde{\phi}_\sigma$, the characters of $\mathfrak{H}$ induced by $\tilde{\phi}_\rho$, $\tilde{\phi}_\sigma$ respectively have no common modular constituent. Now $\tilde{\chi}_\mu$ induces χ_μ, and for p-regular elements, this is the character of $\mathfrak{H}$ induced by $\sum \tilde{d}_{\mu\rho} \tilde{\phi}_\rho$. Therefore the $d_{\mu\rho}$ are 0 or 1. This proves the lemma.

LEMMA 4. *Let $\mathfrak{H}$ be a finite group with a normal cyclic Sylow p-subgroup $\mathfrak{P}$. Then the decomposition numbers $d_{\mu\rho}$ are* 0 *or* 1.

Proof. If $p = 2$, then by a theorem of Burnside [5, p. 327], $\mathfrak{H} = \mathfrak{P} \times \mathfrak{V}$, where $\mathfrak{V}$ is a group of odd order. The lemma then follows immediately. We may therefore assume p is odd; the proof for this case is by induction on

$(\mathfrak{H}:1)$. If $\mathfrak{C}(\mathfrak{P})$ is the centralizer of $\mathfrak{P}$ in $\mathfrak{H}$, then $\mathfrak{C}(\mathfrak{P}) = \mathfrak{P} \times \mathfrak{V}$, where $\mathfrak{V}$ is a p'-subgroup. In fact, $\mathfrak{V}$ must be the maximal normal p'-subgroup of $\mathfrak{H}$. Since $\mathfrak{H}/\mathfrak{C}(\mathfrak{P})$ is isomorphic to a subgroup of the automorphism group of $\mathfrak{P}$, $\mathfrak{H}/\mathfrak{C}(\mathfrak{P})$ must be cyclic. Let χ_μ be an irreducible character of $\mathfrak{H}$, and let $\chi_\mu = \sum d_{\mu\rho}\,\phi_\rho$ be the modular decomposition of χ_μ. If $\chi_\mu \mid \mathfrak{V}$ involves two distinct irreducible characters of $\mathfrak{V}$ as constituents, then by [6, Theorem 2B], χ_μ is induced by an irreducible character χ'_μ of a proper subgroup of $\mathfrak{H}$. Moreover, the decomposition numbers of χ_μ and χ'_μ are the same, so that the $d_{\mu\rho}$ are 0 or 1 by induction. We may therefore assume $\chi_\mu \mid \mathfrak{V}$ is the multiple of one irreducible character of $\mathfrak{V}$. By [6, Theorem 2D], there is a group $\mathfrak{M}$, having a cyclic p'-subgroup $\mathfrak{E}$ in its center, such that $\mathfrak{M}/\mathfrak{E} \simeq \mathfrak{H}/\mathfrak{V}$. Moreover, there is an irreducible character χ''_μ of $\mathfrak{M}$ such that the decomposition numbers of χ_μ and χ''_μ are the same. Let $\mathfrak{Q}$ be a Sylow p-complement of $\mathfrak{M}$. Then $\mathfrak{E} \leqq \mathfrak{Q}$ and $\mathfrak{Q}/\mathfrak{E} \simeq \mathfrak{H}/\mathfrak{C}(\mathfrak{P})$. $\mathfrak{Q}$ is then a cyclic extension of a central subgroup, and consequently $\mathfrak{Q}$ is abelian. The decomposition numbers of χ''_μ are therefore 0 or 1 by Lemma 3, and thus the $d_{\mu\rho}$ are 0 or 1.

LEMMA 5. *Let $\mathfrak{H}$ be a finite group of order $h = p^a m$, where p is a rational prime and $(p, m) = 1$. If the Sylow p-subgroup of $\mathfrak{H}$ is cyclic and normal, then the field $Q(\varepsilon_m)$ is a splitting field for every irreducible character of $\mathfrak{H}$.*

Proof. Let χ_μ be an irreducible character of $\mathfrak{H}$. By Lemma 4 there exists a principal indecomposable character Φ_ρ of $\mathfrak{H}$ which contains χ_μ as a constituent with multiplicity 1. Since the representation with character Φ_ρ can be written in $Q(\varepsilon_m)$ and hence a fortiori in $Q(\varepsilon_m, \chi_\mu)$, it follows by the work of Schur [8], that $Q(\varepsilon_m)$ is a splitting field of χ_μ.

2. The main theorem

Let ε be a primitive g^{th} root of unity, and $Q(\varepsilon)$ the cyclotomic field $Q(\varepsilon_g)$. The Galois group of $Q(\varepsilon)/Q$ is isomorphic to the multiplicative group of residue classes of integers modulo g. If σ is an automorphism of $Q(\varepsilon)/Q$ and $\sigma : \varepsilon \to \varepsilon^i$, σ can be identified with the integer i, i being uniquely determined modulo g. Let L be an algebraic number field; the subgroup in the Galois group of $Q(\varepsilon)/Q$ corresponding to $Q(\varepsilon) \cap L$ can therefore be identified with a certain multiplicative group $\mathfrak{g}(L)$ of integers modulo g. An integer i is in $\mathfrak{g}(L)$ if and only if the automorphism of $Q(\varepsilon)/Q$ defined by $\varepsilon \to \varepsilon^i$ leaves $Q(\varepsilon) \cap L$ fixed. It is clear $\mathfrak{g}(L)$ can also be regarded as the Galois group of $L(\varepsilon)/L$.

Let $\mathfrak{G}$ be a finite group of order g. If A is an element of $\mathfrak{G}$, define the L-normalizer of A in $\mathfrak{G}$ to be the subgroup of all elements X in $\mathfrak{G}$ such that $X^{-1}AX = A^i$ for some integer i in $\mathfrak{g}(L)$. A subgroup $\mathfrak{H}$ of $\mathfrak{G}$ is L-elementary if $\mathfrak{H}$ is a product $\mathfrak{H} = \mathfrak{A}\mathfrak{Q}$, where $\mathfrak{A}$ is a normal cyclic subgroup $\{A\}$ of $\mathfrak{H}$, where $\mathfrak{Q}$ is a q-group for some prime q not dividing $(\mathfrak{A}:1)$, and where the L-normalizer of A in $\mathfrak{H}$ is $\mathfrak{H}$.

THEOREM 1. *Let $\mathfrak{G}$ be a finite group of order $g = p^a m$, where p is a rational prime and $(p, m) = 1$. Let Q be the rational field, and let $K = Q(\varepsilon_m)$ if p is odd, let $K = Q(\varepsilon_m, \sqrt{-1})$ or $K = Q(\varepsilon_m, \sqrt[3]{1})$ if $p = 2$. Then K is a splitting field of every irreducible character of $\mathfrak{G}$.*

Proof. Let χ be an irreducible character of $\mathfrak{G}$. Let L be the field $K(\chi)$. Define a character of any subgroup of $\mathfrak{G}$ to be a character in L if its values lie in L; in particular, χ is a character in L. By [9, Theorem 2], it follows that

$$\chi = \sum a_i \psi_i^* ,$$

where the a_i are rational integers, and where the ψ_i^* are characters of $\mathfrak{G}$ induced by characters ψ_i in L of L-elementary subgroups.

Suppose we can show each ψ_i is the character of a representation $\mathfrak{F}_i$ written in L. Then by an argument exactly like that used in the proof of Lemma 2, it follows that the representation $\mathfrak{X}$ with character χ can be written in L, and this proves the theorem. We have thus reduced the theorem to the following case. Let $\mathfrak{H} = \mathfrak{A}\mathfrak{Q}$ be an L-elementary subgroup of $\mathfrak{G}$. If ψ is a character in L of $\mathfrak{H}$, then the representation with character ψ can be written in L. We may assume ψ is an irreducible character in L, that is, ψ is not the sum of two characters in L of $\mathfrak{H}$. This implies that

$$\psi = \zeta_1 + \zeta_2 + \cdots + \zeta_s ,$$

where the ζ_i are s distinct irreducible characters of $\mathfrak{H}$ which form a complete set of algebraic conjugates over the field L. We show each ζ_i is the character of a representation $\mathfrak{Z}_i$ of $\mathfrak{H}$ which can be written in $L(\zeta_i)$.

Consider the case p odd first. If p does not divide $(\mathfrak{H}:1)$, then L contains the $(\mathfrak{H}:1)^{\text{th}}$ roots of unity, and $\mathfrak{Z}_i$ can be written in $L(\zeta_i)$. If p divides $(\mathfrak{Q}:1)$, then L contains the $(\mathfrak{A}:1)^{\text{th}}$ roots of unity, and hence $\mathfrak{Z}_i$ can be written in $L(\zeta_i)$ by [9, Theorem 5]. If p divides $(\mathfrak{A}:1)$, then $\mathfrak{H}$ has a normal cyclic Sylow p-subgroup. $\mathfrak{Z}_i$ can therefore be written in $L(\zeta_i)$ by Lemma 5. Now the case $p = 2$. If $K = Q(\varepsilon_m, \sqrt{-1})$ the argument used for the case p odd applies, since the result of Solomon can still be used. If $K = Q(\varepsilon_m, \sqrt[3]{1})$, this result cannot be used for the subcase where $\mathfrak{Q}$ is a 2-group. But now we use the fact $\mathfrak{H}$ is an L-elementary subgroup (so far we have really used only the fact $\mathfrak{H}$ is a semidirect product of a cyclic group $\mathfrak{A}$ by a q-group $\mathfrak{Q}$, q a prime not dividing the order of $\mathfrak{A}$). Since $\mathfrak{H}$ is the L-normalizer of A in $\mathfrak{H}$, and since L contains the $(\mathfrak{A}:1)^{\text{th}}$ roots of unity, it follows from the definitions that $\mathfrak{A}$ is in the center of $\mathfrak{H}$. Therefore $\mathfrak{H} = \mathfrak{A} \times \mathfrak{Q}$. It is then sufficient to show that K is a splitting field of the irreducible characters of $\mathfrak{Q}$. Roquette has shown in [7] that Q is in fact a splitting field for $\mathfrak{Q}$ unless $\mathfrak{Q}$ is a (generalized) quaternion group. Moreover, for the irreducible characters of a (generalized) quaternion group which are not split by Q, the corresponding skew field is the ordinary quaternion algebra over Q [7, Bemerkung, p. 249]. The skew field in question contains $Q(\sqrt[3]{1})$

as a maximal subfield, and hence K is a splitting field of the characters of $\mathfrak{Q}$ [10, Chapter VII, §9].

To complete the proof, let $\mathfrak{Z}_1$ be written over $L(\zeta_1)$. If $\sigma_1, \sigma_2, \cdots, \sigma_s$ are the s automorphisms of $L(\zeta_1)/L$, we may take $\mathfrak{Z}_i$ to be $\mathfrak{Z}_1^{\sigma_i}$, where σ_i is applied to the coefficients in each of the matrices of $\mathfrak{Z}_1$. The representation

$$\mathfrak{F} = \begin{pmatrix} \mathfrak{Z}_1 & 0 & \cdots & 0 \\ 0 & \mathfrak{Z}_2 & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & \mathfrak{Z}_s \end{pmatrix}$$

is therefore equivalent to a representation in L, and its character is ψ.

As a corollary we have

THEOREM 2. *Let $\mathfrak{G}$ be a finite group of order $g = p^a m$, where p is a rational prime and $(p, m) = 1$. Let $K = Q(\varepsilon_m)$ if p is odd, let $K = Q(\varepsilon_m, \sqrt[3]{1})$ if $p = 2$. Then K is a splitting field of least possible ramification.*

Proof. K is a splitting field by Theorem 1; furthermore, the prime p does not ramify in K by the well-known behavior of the decomposition of primes in cyclotomic extensions [11, Chapter III, §12].

REFERENCES

1. R. BRAUER, *Investigations on group characters*, Ann. of Math. (2), vol. 42 (1941), pp. 936–958.
2. ———, *Applications of induced characters*, Amer. J. Math., vol. 69 (1947), pp. 709–716.
3. ———, *A characterization of the characters of groups of finite order*, Ann. of Math. (2), vol. 57 (1953), pp. 357–377.
4. R. BRAUER AND J. TATE, *On the characters of finite groups*, Ann. of Math. (2), vol. 62 (1955), pp. 1–7.
5. W. BURNSIDE, *Theory of groups of finite order*, 2nd ed., Cambridge, University Press, 1911.
6. P. FONG, *On the characters of p-solvable groups*, Trans. Amer. Math. Soc., vol. 98 (1961), pp. 263–284.
7. P. ROQUETTE, *Realisierung von Darstellungen endlicher nilpotenter Gruppen*, Arch. Math., vol. 9 (1958), pp. 241–250.
8. I. SCHUR, *Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen*, Sitzungsber. Preuss. Akad. Wiss. (Berlin), 1906, pp. 164–184.
9. L. SOLOMON, *The representation of finite groups in algebraic number fields*, J. Math. Soc. Japan, vol. 13 (1961), pp. 144–164.
10. M. DEURING, *Algebren*, Berlin, J. Springer, 1935.
11. H. WEYL, *Algebraic theory of numbers*, Princeton, Princeton University Press, 1940.

UNIVERSITY OF CALIFORNIA
BERKELEY, CALIFORNIA