J. Math. Soc. Japan
Vol. 13, No. 2, 1961

The representation of finite groups in algebraic number fields

By Louis SOLOMON

(Received Jan. 7, 1960)
(Revised Oct. 29, 1960)

1. Introduction

Let $\mathfrak{G}$ be a finite group. We may state our problem naively as follows. Suppose given an absolutely irreducible representation of $\mathfrak{G}$. It has been known since the time of Frobenius that the given representation may be replaced by an equivalent representation in which all the coefficients lie in a field of algebraic numbers of finite degree over the rational field. The problem is to decide which number fields may be used and in particular to determine how small a field will suffice. The full answer to the question is not yet known. If $\mathfrak{G}$ has exponent n, then it is plausible that the field of n-th roots of unity will suffice for all the absolutely irreducible representations of $\mathfrak{G}$. This quite plausible conjecture was made by Maschke around 1900, but the first proof was given by R. Brauer just a few years ago.

In order to study the problem, Schur introduced a numerical invariant which has come to be known as the Schur index of the representation. This is, roughly speaking, a measure of the size of the smallest field that will do. Since the time of Schur, his invariant has been given a more natural significance in a more general setting as part of the theory of algebras. However, even though there exist several characterizations of the index, none of them will serve to determine it in terms of the table of characters and the multiplication table for the group.

The present paper is a small contribution toward this problem. Section 2 contains some preliminary definitions and remarks. In Section 3 we prove a lemma which is used in Section 4 to prove two theorems on the structure of certain rings of characters associated with a finite group $\mathfrak{G}$ and an algebraic number field K. The first of these is a new proof of a theorem of Witt, using a method due to Brauer and Tate. The second is an easy corollary. The same techniques will prove a theorem of Brauer which reduces the problem of determination of the indices for the representations of $\mathfrak{G}$, to the problem of determination of the indices for the representations of certain solvable sub-

groups of $\mathfrak{G}$. In Section 5 we construct splitting fields for the representations of these solvable subgroups. We shall see in particular that all the representations of a p-group, p an odd prime, are split by the rational field. Finally, in Section 6, we use the preceding results to derive an upper bound for the Schur indices of an arbitrary finite group.

This work is the content of a doctoral thesis submitted to Harvard University in May 1958. I am happy to express a deep felt thank you to my teacher, Professor Brauer, for his kind and gentle manner with a wayward student, and for his good mathematical advice over a period of years.

2. The Schur Index

Let $\mathfrak{G}$ be a finite group of exponent n and let $\varepsilon = \varepsilon_n$ be a primitive n-th root of unity. Let $\mathbf{Q}$ be the field of rational numbers. If χ is an absolutely irreducible character of $\mathfrak{G}$, then the algebraic numbers $\chi(G)$, $G \in \mathfrak{G}$, are sums of n-th roots of unity and lie in the cyclotomic field $\mathbf{Q}(\varepsilon)$. Thus if σ is an automorphism of $\mathbf{Q}(\varepsilon)$ we may define a function χ^σ on $\mathfrak{G}$ by $\chi^\sigma(G) = \chi(G)^\sigma$ for $G \in \mathfrak{G}$. The function χ^σ is also an absolutely irreducible character of $\mathfrak{G}$ and we say that the characters χ and χ^σ are *algebraically conjugate.*

Let $\mathbf{K}$ be an algebraic number field. If $\mathbf{L}$ is a subfield of $\mathbf{K}$, and $\mathbf{K}/\mathbf{L}$ is a Galois extension, we let $\mathrm{Gal}(\mathbf{K}/\mathbf{L})$ denote the Galois group of $\mathbf{K}$ over $\mathbf{L}$. It may happen that two absolutely irreducible characters χ_1, χ_2 of $\mathfrak{G}$ are not only algebraically conjugate, but are algebraically conjugate under an automorphism σ of $\mathbf{Q}(\varepsilon)$ that leaves $\mathbf{Q}(\varepsilon)\cap\mathbf{K}$ fixed. Thus $\chi_2 = \chi_1^\sigma$ for some $\sigma \in \mathrm{Gal}(\mathbf{Q}(\varepsilon)/\mathbf{Q}(\varepsilon)\cap\mathbf{K})$. In this case we say that χ_1 and χ_2 are $\mathbf{K}$-*conjugate characters*, or that they are *algebraically conjugate over* $\mathbf{K}$. Without danger of confusion we may identify $\mathrm{Gal}(\mathbf{Q}(\varepsilon)/\mathbf{Q}(\varepsilon)\cap\mathbf{K})$ with the isomorphic group $\mathrm{Gal}(\mathbf{K}(\varepsilon)/\mathbf{K})$ and sometimes we shall consider σ as an automorphism of $\mathbf{K}(\varepsilon)/\mathbf{K}$.

If χ is an absolutely irreducible character of $\mathfrak{G}$, we let $\mathbf{K}(\chi)$ denote the field generated over $\mathbf{K}$ by the algebraic numbers $\chi(G)$, $G \in \mathfrak{G}$. For $\sigma \in \mathrm{Gal}(\mathbf{K}(\varepsilon)/\mathbf{K})$ we have $\chi^\sigma = \chi$ if and only if σ leaves $\mathbf{K}(\chi)$ fixed. Thus the degree $[\mathbf{K}(\chi):\mathbf{K}]$ is equal to the number of distinct $\mathbf{K}$-conjugates of χ. We let $\mathrm{Sp}_\mathbf{K}(\chi)$ denote the sum of the distinct $\mathbf{K}$-conjugates of χ. The function $\mathrm{Sp}_\mathbf{K}(\chi)$ is a character of $\mathfrak{G}$ and its values lie in $\mathbf{K}$, but it need not be the character of a representation with coefficients in $\mathbf{K}$. However, Schur [**10**] has shown the existence of a least positive integer $m = m_\mathbf{K}(\chi)$ such that $m_\mathbf{K}(\chi)\,\mathrm{Sp}_\mathbf{K}(\chi)$ is the character of a representation of $\mathfrak{G}$ with coefficients in $\mathbf{K}$. This integer $m_\mathbf{K}(\chi)$ has come to be known as the *Schur index* of the absolutely irreducible character χ over the field $\mathbf{K}$.

We say that a field $\mathbf{L}$ is a splitting field of χ if the representation with character χ may be written with coefficients in $\mathbf{L}(\chi)$. If $\mathbf{L}$ is a splitting field

of χ then Schur has shown that the degree $[\mathsf{L}(\chi):\mathsf{K}(\chi)]$ is a multiple of the index $m_{\mathsf{K}}(\chi)$ and that there exist minimal splitting fields L for which $[\mathsf{L}(\chi):\mathsf{K}(\chi)]=m_{\mathsf{K}}(\chi)$. A sketch of the connection between this notion of splitting field and the splitting fields which occur in the theory of simple algebras has been given by Brauer in [4].

3. A Preliminary Lemma

Let a be a positive rational integer and let $\varepsilon=\varepsilon_a$ be a primitive a-th root of unity. All the automorphisms of the cyclotomic field $\mathsf{Q}(\varepsilon)$ are defined by $\varepsilon\to\varepsilon^i$ where i is an integer prime to a. The Galois group $\mathrm{Gal}(\mathsf{Q}(\varepsilon)/\mathsf{Q})$ is thus isomorphic to the multiplicative group of integers modulo a. Let K be an algebraic number field. We let $\mathsf{I}_{\mathsf{K}}(a)$ denote the multiplicative group of integers i modulo a such that $\varepsilon\to\varepsilon^i$ defines an automorphism of $\mathsf{Q}(\varepsilon)$ which leaves $\mathsf{Q}(\varepsilon)\cap\mathsf{K}$ fixed. We thus have a natural isomorphism

$$\mathsf{I}_{\mathsf{K}}(a)\cong\mathrm{Gal}(\mathsf{Q}(\varepsilon)/\mathsf{Q}(\varepsilon)\cap\mathsf{K})\cong\mathrm{Gal}(\mathsf{K}(\varepsilon)/\mathsf{K})\,.$$

Sometimes it will be convenient to consider the elements of $\mathsf{I}_{\mathsf{K}}(a)$ as rational integers.

Let $\mathfrak{H}$ be a finite group and let $A\in\mathfrak{H}$ be an element of order a. We define the K-*normalizer* $\mathfrak{N}_{\mathsf{K}}(A)$ of A in $\mathfrak{H}$ to be the set of all $H\in\mathfrak{H}$ such that $HAH^{-1}=A^i$ for some $i\in\mathsf{I}_{\mathsf{K}}(a)$. The K-normalizer is a subgroup of $\mathfrak{H}$. If $\varepsilon\in\mathsf{K}$ then the only admissible integers i are $\equiv 1 \bmod a$ and the K-normalizer of A is its normalizer in the usual sense. There is a natural homomorphism of $\mathfrak{N}_{\mathsf{K}}(A)$ into the Galois group $\mathrm{Gal}(\mathsf{K}(\varepsilon)/\mathsf{K})$.

We say that a group $\mathfrak{H}$ is K-*elementary* with respect to the prime p, if it may be factored as a product $\mathfrak{H}=\mathfrak{A}\mathfrak{P}$, where $\mathfrak{A}=\{A\}$ is a cyclic group, where $\mathfrak{P}$ is a p-group of order prime to the order of A, and where the K-normalizer of A in $\mathfrak{H}$ is the full group $\mathfrak{H}$. Usually we shall say merely that $\mathfrak{H}$ is K-elementary. If $\mathsf{K}=\mathsf{Q}$ is the rational field, then the Q-elementary groups are precisely the *groups of type* $\mathfrak{E}$ defined by Brauer in [4]. At the opposite extreme, if K contains the root of unity ε, then the K-elementary groups are just the *elementary groups* of [5].

We begin with some simple remarks about the irreducible representations of the cyclic group $\mathfrak{A}$ in K. The absolutely irreducible representations of $\mathfrak{A}$ are of degree one and are defined by $\omega_t(A)=\varepsilon^t$, $t=0,1,\cdots,a-1$, where a is the order of $\mathfrak{A}$. Then $\phi_t(A)=\mathrm{Sp}_{\mathsf{K}}(\omega_t)$ defines a character of $\mathfrak{A}$ with values in K. The degree of ϕ_t is equal to the number of algebraic conjugates of ω_t over K, which is $[\mathsf{K}(\omega_t):\mathsf{K}]=[\mathsf{K}(\varepsilon^t):\mathsf{K}]$. Since ω_t is a representation of degree one, it follows from the work of Schur that the index $m_{\mathsf{K}}(\omega_t)$ is one, and ϕ_t is actually the character of an irreducible representation $\mathfrak{R}_t$ of $\mathfrak{A}$ in K. We may construct

$\mathfrak{R}_t$ as follows. Consider the field $\mathsf{K}(\varepsilon^t)$ as an algebra over K. Let $\mathfrak{R}$ be the regular representation of $\mathsf{K}(\varepsilon^t)/\mathsf{K}$. For any $x \in \mathsf{K}(\varepsilon^t)$ we have *Trace* $\mathfrak{R}(x) = \sum_i x^{(i)}$, where the sum is over all the $[\mathsf{K}(\varepsilon^t):\mathsf{K}]$ conjugates $x^{(i)}$ of x in $\mathsf{K}(\varepsilon^t)$. In particular then, *Trace* $\mathfrak{R}(\varepsilon^{jt}) = \phi_t(A^j)$. Thus the equation $\mathfrak{R}_t(A^j) = \mathfrak{R}(\varepsilon^{jt})$ defines a representation $\mathfrak{R}_t$ of $\mathfrak{A}$ by linear transformations of $\mathsf{K}(\varepsilon^t)/\mathsf{K}$ and the character of this representation is ϕ_t. The distinct characters ϕ_t furnish all the irreducible representations of $\mathfrak{A}$ in K.

The following lemma is fundamental for all our work. It is closely related to results of Witt [**11**] and Berman [**1**].

LEMMA 1. *Let $\mathfrak{H} = \mathfrak{A}\mathfrak{P}$ be a K-elementary group and let $\phi_t = \mathrm{Sp}_{\mathsf{K}}(\omega_t)$ be the character of an irreducible representation of $\mathfrak{A}$ in K. Let $\mathfrak{P}_t$ be the subgroup of $\mathfrak{P}$ which consists of all elements of $\mathfrak{P}$ that commute with A^t. Then the function ψ_t on $\mathfrak{H}$, defined by*

$$\psi_t(A^jP) = \begin{cases} \phi_t(A^j) & P \in \mathfrak{P}_t \\ 0 & P \notin \mathfrak{P}_t \end{cases}$$

is the character of an irreducible representation of $\mathfrak{H}$ in K.

PROOF. Since $\mathfrak{H}$ is K-elementary there is a natural homomorphism of $\mathfrak{H}$ into $\mathrm{Gal}(\mathsf{K}(\varepsilon)/\mathsf{K})$, hence a homomorphism of $\mathfrak{P}$ into $\mathrm{Gal}(\mathsf{K}(\varepsilon)/\mathsf{K})$, and hence a homomorphism of $\mathfrak{P}$ into $\mathrm{Gal}(\mathsf{K}(\varepsilon^t)/\mathsf{K})$. Let us determine the kernel of this last homomorphism. Let $P \in \mathfrak{P}$ and suppose $PAP^{-1} = A^i$. Then P lies in the kernel if and only if $\varepsilon^t \to \varepsilon^{ti}$ defines the identity automorphism of $\mathsf{K}(\varepsilon^t)/\mathsf{K}$. This will be the case if and only if $t \equiv ti \bmod a$. But $A^{-t}PA^t = A^{t(i-1)}P$ so that P lies in the kernel if and only if P commutes with A^t. Thus the kernel is $\mathfrak{P}_t$.

We consider $\mathsf{K}(\varepsilon^t)$ as left vector space over K and remark that $\mathrm{Gal}(\mathsf{K}(\varepsilon^t)/\mathsf{K})$ acts naturally as a group of linear transformations of $\mathsf{K}(\varepsilon^t)/\mathsf{K}$. Thus to each $P \in \mathfrak{P}$ we may associate a linear transformation $\mathfrak{S}_t(P)$ of the space $\mathsf{K}(\varepsilon^t)/\mathsf{K}$ and the map $P \to \mathfrak{S}_t(P)$ is a representation of $\mathfrak{P}$ with kernel $\mathfrak{P}_t$. Let $[\mathsf{K}(\varepsilon^t):\mathsf{K}] = r$. Then the elements $1, \varepsilon^t, \cdots, \varepsilon^{t(r-1)}$ are a basis for $\mathsf{K}(\varepsilon^t)/\mathsf{K}$. If $PAP^{-1} = A^i$ then

$$\mathfrak{S}_t(P)\varepsilon^{tk} = \varepsilon^{tki}.$$

On the other hand we have already defined a representation $\mathfrak{R}_t$ of $\mathfrak{A}$ by linear transformations of $\mathsf{K}(\varepsilon^t)/\mathsf{K}$ which has ϕ_t for its character. Clearly

$$\mathfrak{R}_t(A^j)\varepsilon^{tk} = \varepsilon^{t(j+k)}.$$

Thus

$$\mathfrak{S}_t(P)\mathfrak{R}_t(A^j) = \mathfrak{R}_t(A^{ij})\mathfrak{S}_t(P)$$

and it follows that

$$\mathfrak{T}_t(A^jP) = \mathfrak{R}_t(A^j)\mathfrak{S}_t(P)$$

defines a representation $\mathfrak{T}_t$ of $\mathfrak{H}$ by linear transformations of $\mathsf{K}(\varepsilon^t)/\mathsf{K}$. Since $\mathfrak{T}_t$ agrees with $\mathfrak{R}_t$ on $\mathfrak{A}$, and $\mathfrak{R}_t$ is irreducible in K, it follows that $\mathfrak{T}_t$ is irreducible

in K. We shall see that the character of $\mathfrak{T}_t$ is ψ_t.

Let L be a field over K, isomorphic over K to $\mathsf{K}(\varepsilon^t)$. Let $\mathsf{W}=\mathsf{L}\otimes\mathsf{K}(\varepsilon^t)$ where the tensor product is formed over K. For the moment we consider W as left vector space over L. The elements $1\otimes 1, 1\otimes\varepsilon^t, \cdots, 1\otimes\varepsilon^{t(r-1)}$ are a basis for W over L. The linear transformations $\mathfrak{R}_t(A^j)$ and $\mathfrak{S}_t(P)$ may be considered as linear transformations of W over L provided we agree to leave L fixed. Thus

$$\mathfrak{R}_t(A^j)(1\otimes\varepsilon^{tk})=1\otimes\varepsilon^{t(j+k)}=(1\otimes\varepsilon^{tj})(1\otimes\varepsilon^{tk}),$$
$$\mathfrak{S}_t(P)(1\otimes\varepsilon^{tk})=1\otimes\varepsilon^{tki}.$$

Now let us consider W as a commutative semisimple algebra over L. The structure theory for such a tensor product of fields is given in [7]. The algebra W has a Wedderburn decomposition

$$\mathsf{W}=\mathsf{L}e_1\dotplus\cdots\dotplus\mathsf{L}e_r$$

where the e_i are pairwise orthogonal primitive idempotents. For $x\in\mathsf{K}(\varepsilon^t)$ we have $(1\otimes x)e_i=x^{(i)}e_i$ where $x^{(1)},\cdots,x^{(r)}$ are the conjugates of x in the normal field L of degree r over K. Thus in the basis $e_1,\cdots,e_r$ for W/L the matrices $\mathfrak{R}_t(A^j)$ are diagonal, and the diagonal elements are the conjugates of ε^{jt} in L. On the other hand, the Galois group $\mathrm{Gal}(\mathsf{K}(\varepsilon^t)/\mathsf{K})$ may be considered as a group of automorphisms of W/L if we agree to leave L fixed. It is known [7] that the automorphisms of $\mathrm{Gal}(\mathsf{K}(\varepsilon^t)/\mathsf{K})$ permute the primitive idempotents e_i and that this permutation representation is the regular representation of the Galois group. Thus, in the basis $e_1,\cdots,e_r$ for W/L, the matrices $\mathfrak{S}_t(P)$ have zeros along the main diagonal unless $P\in\mathfrak{P}_t$, and if $P\in\mathfrak{P}_t$ then $\mathfrak{S}_t(P)$ is the identity. Now choose $\mathsf{L}=\mathsf{K}(\varepsilon^t)$ and it is clear that the character of $\mathfrak{T}_t$ is ψ_t. This proves the lemma.

4. The Ring of K-characters

Let $\mathfrak{G}$ be a finite group of exponent n, and let K be an algebraic number field. We say that a character of $\mathfrak{G}$ is a K-*character* if it is the character of a representation which may be written with coefficients in K. We say that two elements $A, B\in\mathfrak{G}$ are K-*conjugate* if there exists an element $T\in\mathfrak{G}$ and an integer $i\in\mathsf{I}_\mathsf{K}(n)$ such that $TAT^{-1}=B^i$. Recall that $\mathsf{I}_\mathsf{K}(n)$ is the multiplicative group of integers i modulo n such that $\varepsilon_n\to\varepsilon_n^{\,i}$ defines an automorphism of $\mathsf{K}(\varepsilon_n)/\mathsf{K}$. The relation of K-*conjugacy* is an equivalence relation on $\mathfrak{G}$, and $\mathfrak{G}$ is partitioned into classes of K-conjugate elements. Each of these classes is a union of ordinary conjugate classes of $\mathfrak{G}$. We assert that the K-characters are constant on the classes of K-conjugate elements. For let χ be a K-character and suppose $TAT^{-1}=B^i$. If $\sigma:\varepsilon_n\to\varepsilon_n^{\,i}$ is the corresponding automorphism of $\mathsf{K}(\varepsilon_n)/\mathsf{K}$, then $\chi(B)=\chi(B)^\sigma$. On the other hand $\chi(B)$ is a sum of powers of ε_n

and thus $\chi(B)^\sigma = \chi(B)^i = \chi(A)$ which proves the assertion. If K contains the primitive n-th root of unity ε_n, this just amounts to the fact that the characters of $\mathfrak{G}$ are constant on the conjugate classes.

Let p be a rational prime. We say that an element of $\mathfrak{G}$ is *p-regular* if its order is prime to p. Every $G \in \mathfrak{G}$ may be written uniquely in the form $G = G'G''$ where G' is p-regular, where the order of G'' is a power of p, and where G' and G'' commute. Both G' and G'' are powers of G. Let R be the domain of integers of the field $\mathsf{K}(\varepsilon_n)$ and let $\mathfrak{p}$ be a fixed prime ideal divisor of p in R. If χ is any character of $\mathfrak{G}$, then the values of χ lie in R and $\chi(G) \equiv \chi(G') \bmod \mathfrak{p}$ for all $G \in \mathfrak{G}$. Thus, modulo the prime ideal $\mathfrak{p}$ it is only the p-regular elements that are significant for a study of the characters. These facts are fairly well known.

We introduce an equivalence relation [**1**], [**11**] on $\mathfrak{G}$ relative to the field K and the prime $\mathfrak{p}$. If $A, B \in \mathfrak{G}$ we write $A \approx B$ if A' and B' are K-conjugate. The equivalence classes under the relation $\approx$ will be called *sections* of $\mathfrak{G}$. If A and B lie in the same section and χ is a K-character then

$$\chi(A) \equiv \chi(A') = \chi(B') \equiv \chi(B) \mod \mathfrak{p}.$$

Thus the K-characters are constant mod $\mathfrak{p}$ on the sections.

Let S be an integral domain included in the field of complex numbers. We let $\mathsf{X}_\mathsf{S} = \mathsf{X}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$ denote the ring of all linear combinations of K-characters of $\mathfrak{G}$ with coefficients in S, and call X_S the *ring of* K*-characters* of the group $\mathfrak{G}$ over the domain S. The ring X_S has a basis over S consisting of the distinct K-characters $m_\mathsf{K}(\chi)\mathrm{Sp}_\mathsf{K}(\chi)$, where χ runs over the set of absolutely irreducible characters of $\mathfrak{G}$. Two distinct K-characters of the form $m_\mathsf{K}(\chi)\mathrm{Sp}_\mathsf{K}(\chi)$ have no absolutely irreducible constituents in common, and it follows from the orthogonality relations that they are independent functions over S. Since the principal character lies in X_S we may identify S with a subring of X_S.

If χ is a character of $\mathfrak{G}$ and $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$, then the restriction $\chi|\mathfrak{H}$ of the function χ to the subgroup $\mathfrak{H}$ is a character of $\mathfrak{H}$. If χ is a K-character of $\mathfrak{G}$, then clearly $\chi|\mathfrak{H}$ is a K-character of $\mathfrak{H}$. The restriction map $\chi \to \chi|\mathfrak{H}$ thus defines a natural S-linear ring homomorphism of $\mathsf{X}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$ into $\mathsf{X}_\mathsf{S}(\mathfrak{H}, \mathsf{K})$. In the opposite direction given a character ψ of the subgroup $\mathfrak{H}$, we may let correspond to ψ the so called induced character ψ^* of $\mathfrak{G}$. The definition of ψ^* is

$$\psi^*(G) = \frac{1}{(\mathfrak{H}:1)} \sum_{T \in \mathfrak{G}} \psi(TGT^{-1}) \qquad G \in \mathfrak{G}$$

where we agree to write $\psi(S) = 0$ whenever $S \notin \mathfrak{H}$. It follows at once from inspection of the matrices for the corresponding representations [8] that K-characters of $\mathfrak{H}$ induce K-characters of $\mathfrak{G}$. Thus the induction map $\psi \to \psi^*$ defines an S-linear mapping, not a ring homomorphism, of $\mathsf{X}_\mathsf{S}(\mathfrak{H}, \mathsf{K})$ into $\mathsf{X}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$.

We shall make frequent use of the Frobenius Reciprocity Theorem: If χ is an absolutely irreducible character of $\mathfrak{G}$ and ψ is an absolutely irreducible character of $\mathfrak{H}$, then the multiplicity of ψ in $\chi|\mathfrak{H}$ is equal to the multiplicity of χ in ψ^*. This statement is an immediate consequence of the orthogonality relations and the defining formula for the induced character.

With these definitions and elementary facts we are able to prove the following theorem on induced characters.

THEOREM 1. *If χ is a* K*-character of $\mathfrak{G}$, then χ may be written as a sum*

$$\chi = \sum_j z_j \psi_j^*$$

where the z_j are rational integers and the ψ_j^* are induced by K*-characters ψ_j of* K*-elementary subgroups of $\mathfrak{G}$.*

This amounts to a structure theorem for the ring X_Z of K-characters of $\mathfrak{G}$ over the domain Z of rational integers. It says, in a sense, that all the K-characters of a finite group $\mathfrak{G}$ may be constructed provided we know the K-characters of its K-elementary subgroup. If $\mathsf{K} \subseteqq \mathsf{L}$, then every L-elementary group is K-elementary. Hence, the smaller the field K, the larger the class of subgroups one must admit in order to be able to express every K-character of $\mathfrak{G}$ as a linear combination of induced K-characters with rational integer coefficients. However, one need never go outside the class of Q-elementary subgroups. A result similar to Theorem 1, but with p-adic coefficients, was proved by Berman [**1**] who used an argument of Roquette [**9**]. Our proof of Theorem 1 is a natural extension of the argument used by Brauer and Tate [**6**] in the case $\mathsf{K} = \mathsf{Q}(\varepsilon_n)$. The only major new difficulty arises in the construction of a certain function on a given K-elementary group $\mathfrak{H}$. For the case $\mathsf{K} = \mathsf{Q}(\varepsilon_n)$ this construction is immediate. For the case of a general number field K we use Lemma 1.

Theorem 1 will be a consequence of several lemmas. We define S-modules $\mathsf{U}_\mathsf{S} = \mathsf{U}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$ and $\mathsf{V}_\mathsf{S} = \mathsf{V}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$ as follows. Let U_S be the set of all complex valued class functions χ on $\mathfrak{G}$ such that the restriction $\chi|\mathfrak{H}$ lies in the ring $\mathsf{X}_\mathsf{S}(\mathfrak{H}, \mathsf{K})$ for all K-elementary subgroups $\mathfrak{H}$ of $\mathfrak{G}$. Let V_S be the set of all linear combinations with coefficients in S of characters ψ^* induced by K-characters ψ of K-elementary subgroups of $\mathfrak{G}$. Now one can use the fact that the restriction map $\chi \to \chi|\mathfrak{H}$ maps $\mathsf{X}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$ into $\mathsf{X}_\mathsf{S}(\mathfrak{H}, \mathsf{K})$, and the fact that the induction map $\psi \to \chi^*$ maps $\mathsf{X}_\mathsf{S}(\mathfrak{H}, \mathsf{K})$ into $\mathsf{X}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$, to show as in [**6**] that U_S is a ring, that V_S is an ideal of U_S, and that $\mathsf{V}_\mathsf{S} \subseteqq \mathsf{X}_\mathsf{S}(\mathfrak{G}, \mathsf{K}) \subseteqq \mathsf{U}_\mathsf{S}$. If we choose $\mathsf{S} = \mathsf{Z}$ we see that in order to prove Theorem 1 it is enough to show $1 \in \mathsf{V}_\mathsf{Z}$. For then $\mathsf{X}_\mathsf{Z} = \mathsf{V}_\mathsf{Z}$ and this is the statement of Theorem 1. As a by product we get the interesting result $\mathsf{X}_\mathsf{Z} = \mathsf{U}_\mathsf{Z}$. Note also that $1 \in \mathsf{V}_\mathsf{Z}$ implies $1 \in \mathsf{V}_\mathsf{S}$ for all domains S and hence $\mathsf{U}_\mathsf{S} = \mathsf{X}_\mathsf{S} = \mathsf{V}_\mathsf{S}$ for all domains S.

LEMMA 2. *Let* $\mathfrak{H}=\mathfrak{A}\mathfrak{P}$ *be a* K*-elementary group. Let* $\varepsilon=\varepsilon_a$ *be a primitive* a*-th root of unity, where* a *is the order of* $\mathfrak{A}=\{A\}$. *Let* S *be the domain of integers of the field* $\mathsf{Q}(\varepsilon)$. *Then there exists a function* $\eta\in \mathsf{X}_{\mathsf{S}}(\mathfrak{H},\mathsf{K})$ *such that*

$$\eta(A^i)=\begin{cases} a & i\in \mathsf{I}_{\mathsf{K}}(a) \\ 0 & i\notin \mathsf{I}_{\mathsf{K}}(a)\,. \end{cases}$$

PROOF. Let ξ be the function defined on $\mathfrak{A}$ by

$$\xi(A^i)=\begin{cases} a & i\in \mathsf{I}_{\mathsf{K}}(a) \\ 0 & i\notin \mathsf{I}_{\mathsf{K}}(a)\,. \end{cases}$$

Then we may write $\xi=\sum_{t=0}^{a-1} c_t\omega_t$ where the ω_t are the absolutely irreducible characters of $\mathfrak{A}$ and the c_t are uniquely determined complex numbers. It follows from the orthogonality relations for the ω_t that

$$c_t=\frac{1}{a}\sum_{i=0}^{a-1}\xi(A^i)\overline{\omega_t(A^i)}=\sum_{i\in \mathsf{I}_{\mathsf{K}}(a)}\overline{\omega_t(A^i)}\,.$$

Thus the c_t lie in S. If ω_t and ω_s are algebraically conjugate over K, then there exists an automorphism of $\mathsf{K}(\varepsilon)/\mathsf{K}$ which maps ε^t into ε^s. Thus $t\equiv sj \bmod a$ for some $j\in \mathsf{I}_{\mathsf{K}}(a)$. Then $\omega_t(A^i)=\varepsilon^{it}=\varepsilon^{ijs}=\omega_s(A^{ij})$. Since ij runs through $\mathsf{I}_{\mathsf{K}}(a)$ with i mod a, it follows that $c_s=c_t$. Thus ξ is a linear combination of K-characters $\mathrm{Sp}_{\mathsf{K}}(\omega_t)$ with coefficients in S. Each of the $\mathrm{Sp}_{\mathsf{K}}(\omega_t)$ may, by Lemma 1, be extended to a K-character of $\mathfrak{H}$ and so ξ may be extended to a function $\eta\in \mathsf{X}_{\mathsf{S}}(\mathfrak{H},\mathsf{K})$ with the required properties.

LEMMA 3. *Let* A *be a* p*-regular element of* $\mathfrak{G}$ *of order* a. *There exists a function* $\theta\in \mathsf{V}_{\mathsf{R}}(\mathfrak{G},\mathsf{K})$ *such that*

$$\theta(A)\equiv 1 \mod \mathfrak{p}\,,$$

$$\theta(G)=0 \text{ if } G \text{ is } p\text{-regular and } G\not\approx A\,.$$

PROOF. Let $\mathfrak{A}=\{A\}$ be the cyclic subgroup generated by A and let $\mathfrak{P}$ be a p-Sylow subgroup of the K-normalizer of A in $\mathfrak{G}$. Then $\mathfrak{H}=\mathfrak{A}\mathfrak{P}$ is a K-elementary group. Let S be the domain of integers of the field $\mathsf{Q}(\varepsilon_a)$. Let $\eta\in \mathsf{X}_{\mathsf{S}}(\mathfrak{H},\mathsf{K})$ be the function furnished by Lemma 2. Since a divides n, it follows that $\mathsf{S}\subseteq\mathsf{R}$ and hence $\eta\in \mathsf{X}_{\mathsf{R}}(\mathfrak{H},\mathsf{K})$. The induction map $\mathsf{X}_{\mathsf{R}}(\mathfrak{H},\mathsf{K})\to \mathsf{X}_{\mathsf{R}}(\mathfrak{G},\mathsf{K})$ defines an element $\eta^*\in \mathsf{V}_{\mathsf{R}}(\mathfrak{G},\mathsf{K})$. By definition of the induced character we have

$$\eta^*(A)=\frac{1}{(\mathfrak{H}:1)}\sum_T \eta(TAT^{-1})$$

where we sum over those $T\in\mathfrak{G}$ for which $TAT^{-1}\in\mathfrak{H}$. If $TAT^{-1}\in\mathfrak{H}$ then TAT^{-1} is a p-regular element of $\mathfrak{H}$. Since the p-regular elements of $\mathfrak{H}$ are just the powers of A, it follows that TAT^{-1} is a power of A. Say $TAT^{-1}=A^i$.

Since $\eta(A^i)=0$ unless $i\in \mathsf{I}_{\mathsf{K}}(a)$ it follows that $i\in \mathsf{I}_{\mathsf{K}}(a)$ and hence that T lies in the K-normalizer $\mathfrak{N}_{\mathsf{K}}(A)$. Thus we need sum over only those T which lie in $\mathfrak{N}_{\mathsf{K}}(A)$, and for those T we have $\eta(TAT^{-1})=(\mathfrak{A}:1)$. Thus

$$\eta^*(A)=\frac{(\mathfrak{A}:1)}{(\mathfrak{H}:1)}(\mathfrak{N}_{\mathsf{K}}(A):1)=(\mathfrak{N}_{\mathsf{K}}(A):\mathfrak{P}).$$

Since we have chosen $\mathfrak{P}$ as a p-Sylow subgroup of $\mathfrak{N}_{\mathsf{K}}(A)$, the index $(\mathfrak{N}_{\mathsf{K}}(A):\mathfrak{P})$ is prime to p and thus there exists a rational integer z with $z(\mathfrak{N}_{\mathsf{K}}(A):\mathfrak{P})\equiv 1 \mod p$. The function $\theta=z\eta^*$ is the function we seek. For $\theta(A)=z\eta^*(A)\equiv 1 \mod p$ and a fortiori $\theta(A)\equiv 1 \mod \mathfrak{p}$. On the other hand $\theta(G)=0$ if G is p-regular and $G\not\approx A$. To see this, suppose the contrary. If $\theta(G)\neq 0$, then $\eta^*(G)\neq 0$ and hence $\eta(TGT^{-1})\neq 0$ for some $T\in\mathfrak{G}$. This means $TGT^{-1}\in\mathfrak{H}$ and since G is p-regular we have $TGT^{-1}=A^i$ for some integer i. But $\eta(A^i)=\eta(TGT^{-1})\neq 0$ and so $i\in \mathsf{I}_{\mathsf{K}}(a)$. Thus $\varepsilon_a\to\varepsilon_a{}^i$ defines an automorphism of $\mathsf{K}(\varepsilon_a)/\mathsf{K}$. Extend this automorphism to an automorphism of $\mathsf{K}(\varepsilon_n)/\mathsf{K}$. The extension must map ε_n into a power of ε_n, say $\varepsilon_n\to\varepsilon_n{}^j$ where $j\in \mathsf{I}_{\mathsf{K}}(n)$ by definition of $\mathsf{I}_{\mathsf{K}}(n)$. Since ε_a is a power of ε_n, the extended automorphism maps ε_a into $\varepsilon_a{}^j$, and it follows that $i\equiv j \mod a$. Thus we have $TGT^{-1}=A^j$ where $j\in \mathsf{I}_{\mathsf{K}}(n)$ and it follows that G and A are K-conjugate. Since G and A are p-regular, this implies $G\approx A$ which is a contradiction. The lemma is proved.

LEMMA 4. *There exists a function* $\zeta\in \mathsf{V}_{\mathsf{R}}(\mathfrak{G},\mathsf{K})$ *such that*

$$\zeta(G)\equiv 1 \mod \mathfrak{p}$$

for all $G\in\mathfrak{G}$.

PROOF. If $G\in\mathfrak{G}$ then certainly G and its p-regular factor G' lie in the same section. Thus every section contains p-regular elements. Choose p-regular elements $A_1,\cdots,A_t$ one element from each of the sections of $\mathfrak{G}$. Let $\mathfrak{A}_j=\{A_j\}$ be the cyclic subgroup generated by A_j, let $\mathfrak{P}_j$ be a p-Sylow subgroup of the K-normalizer $\mathfrak{N}_{\mathsf{K}}(A_j)$ and let $\mathfrak{H}_j$ be the K-elementary group $\mathfrak{A}_j\mathfrak{P}_j$. Let θ_j be the function on $\mathfrak{G}$ which arises from $\mathfrak{H}_j$ by the construction of Lemma 3 and set $\zeta=\theta_1+\cdots+\theta_t$. Then $\zeta(A_j)\equiv 1 \mod p$ for all the p-regular representatives A_j. Each of the functions θ_j, and hence the function ζ is a linear combination of K-characters of $\mathfrak{G}$ with coefficients in R. Since the K-characters are constant $\mod \mathfrak{p}$ on the sections, it follows that ζ is also constant $\mod \mathfrak{p}$ on the sections. Thus given $G\in\mathfrak{G}$, we may choose one of the representatives A_j with $G\approx A_j$ and then $\zeta(G)\equiv\zeta(A_j)\equiv 1 \mod \mathfrak{p}$. This completes the proof of the lemma.

Let the order of $\mathfrak{G}$ be $g=p^cg_0$ where $(g_0,p)=1$. We prove

LEMMA 5. $g_0\in \mathsf{V}_{\mathsf{Z}}$.

PROOF. Let us show first that $g_0\in \mathsf{V}_{\mathsf{R}}$. Let ζ be the function constructed in Lemma 4. Since $\zeta(G)\equiv 1 \mod \mathfrak{p}$, it follows by induction on r that $\zeta(G)^{p^r}\equiv 1 \mod \mathfrak{p}^r$ for all positive rational integers r. Write $g_0=g_0(1-\zeta^{p^r})+g_0\zeta^{p^r}$. Since V_{R} is an ideal in the ring U_{R} and $\zeta\in \mathsf{V}_{\mathsf{R}}$, it follows that $g_0\zeta^{p^r}\in \mathsf{V}^{\mathsf{R}}$. We must

show $g_0(1-\zeta^{p^r}) \in \mathsf{V}_\mathsf{R}$. Note first that the construction of ζ is independent of the particular prime ideal divisor $\mathfrak{p}$ of p that we have chosen. Thus the congruence $1-\zeta(G)^{p^r} \equiv 0 \bmod \mathfrak{p}^r$ is valid for every prime ideal divisor $\mathfrak{p}$ of p in R. This means that for sufficiently large r we have a congruence $1-\zeta(G)^{p^r} \equiv 0 \bmod \mathfrak{p}^c\mathsf{R}$ for all $G \in \mathfrak{G}$.

Let A be any, not necessarily p-regular, element of $\mathfrak{G}$. In the course of the proof of Lemma 2 we have shown the existence of a function $\xi \in \mathsf{X}_\mathsf{R}(\mathfrak{N}, \mathsf{K})$ such that $\xi(A^i) = a$ for $i \in \mathsf{I}_\mathsf{K}(a)$ while $\xi(A^i) = 0$ for $i \notin \mathsf{I}_\mathsf{K}(a)$. Let $\rho = \xi^*$ be the induced function on $\mathfrak{G}$. Then $\rho \in \mathsf{V}_\mathsf{R}(\mathfrak{G}, \mathsf{K})$ and $\rho(A) = (\mathfrak{N}_\mathsf{K}(A) : 1)$ while $\rho(G) = 0$ unless $TGT^{-1} = A^i$ for some $T \in \mathfrak{G}$ and $i \in \mathsf{I}_\mathsf{K}(a)$. But $TGT^{-1} = A^i$ for some $i \in \mathsf{I}_\mathsf{K}(a)$ implies, as in the proof of Lemma 3, that $TGT^{-1} = A^i$ for some $j \in \mathsf{I}_\mathsf{K}(n)$ and then G is K-conjugate to A. Thus $\rho(G) = 0$ unless G is K-conjugate to A.

Now let $A_1, \cdots, A_s$ be representatives for the classes of K-conjugate elements, and let $\rho_1, \cdots, \rho_s$ be the corresponding functions on $\mathfrak{G}$. Since ζ is a linear combination of K-characters, it is constant on the classes of K-conjugate elements, and the same is true for $g_0(1-\zeta^{p^r})$. Thus we may write

$$g_0(1-\zeta^{p^r}) = \sum_{j=1}^{s} \frac{g_0(1-\zeta(A_j)^{p^r})}{(\mathfrak{N}_\mathsf{K}(A_j) : 1)} \rho_j .$$

The ρ_j lie in V_R, and since $1-\zeta(A_j)^{p^r} \equiv 0 \bmod p^c\mathsf{R}$ it follows that the coefficients of the ρ_j in the above expression for $g_0(1-\zeta^{p^r})$ lie in R. Thus $g_0(1-\zeta^{p^r}) \in \mathsf{V}_\mathsf{R}$ and hence $g_0 \in \mathsf{V}_\mathsf{R}$. Now choose an integral basis for R over the domain Z of rational integers, and use the fact that the irreducible K-characters are independent over the complex numbers to conclude as in [**6**] that $g_0 \in \mathsf{V}_\mathsf{Z}$. This proves the lemma.

Thus, for each rational prime p we have $g_0 \in \mathsf{V}_\mathsf{Z}$. If follows that $1 \in \mathsf{V}_\mathsf{Z}$ and this completes the proof of Theorem 1.

Given the finite group $\mathfrak{G}$ and the algebraic number field K, we have defined the ring of K-characters $\mathsf{X}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$ of the group $\mathfrak{G}$ over the domain S. There is a second ring of characters $\mathsf{Y}_\mathsf{S} = \mathsf{Y}_\mathsf{S}(\mathfrak{G}, \mathsf{K})$ associated with the pair $(\mathfrak{G}, \mathsf{K})$ that demands attention. We say that a character χ of $\mathfrak{G}$ is a *character in* K (or a *character with values in* K) if $\chi(G) \in \mathsf{K}$ for all $G \in \mathfrak{G}$. Every K-character is a character in K. The ring Y_S consists of all linear combinations of characters of $\mathfrak{G}$ in K, with coefficients in S. We call Y_S the *ring of characters in* K of the group $\mathfrak{G}$ over the domain S. The ring Y_S has a basis over S consisting of the distinct characters $\mathrm{Sp}_\mathsf{K}(\chi)$, where χ runs through the set of absolutely irreducible characters of $\mathfrak{G}$. Clearly Y_S contains X_S as a subring. For the ring Y_S there is a theorem analogous to Theorem 1, in which "K-character" is replaced by "character in K".

THEOREM 2. *If χ is a character of $\mathfrak{G}$ in K, then χ may be written as a sum*

$$\chi = \sum_{f} z_j \psi_j^*$$

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

PROOF. The result follows easily from Theorem 1. Let us redefine the S-modules U_S and V_S of Theorem 1 as follows. Let U_S' be the set of all complex valued class functions θ on $\mathfrak{G}$ such that the restriction $\theta|\mathfrak{H}$ of θ to $\mathfrak{H}$ lies in the character ring $\mathsf{Y}_S(\mathfrak{H}, \mathsf{K})$ for every K-elementary subgroup $\mathfrak{H}$ of $\mathfrak{G}$. Let V_S' be the set of all linear combinations with coefficients in S of characters ψ^* induced by characters ψ in K of K-elementary subgroups of $\mathfrak{G}$. The restriction map takes $\mathsf{Y}_S(\mathfrak{G}, \mathsf{K})$ into $\mathsf{Y}_S(\mathfrak{H}, \mathsf{K})$ and the induction map takes $\mathsf{Y}_S(\mathfrak{H}, \mathsf{K})$ into $\mathsf{Y}_S(\mathfrak{G}, \mathsf{K})$ for any subgroup $\mathfrak{H}$ of $\mathfrak{G}$. Again here, U_S' is a ring, V_S' is an ideal of U_S' and $\mathsf{V}_S' \subseteq \mathsf{Y}_S(\mathfrak{G}, \mathsf{K}) \subseteq \mathsf{U}_S'$. But clearly $\mathsf{V}_Z \subseteq \mathsf{V}_Z'$. Hence Theorem 1 shows $1 \in \mathsf{V}_Z'$ and this proves Theorem 2.

Now let us use Theorem 1 to prove an important theorem of Brauer [4] on the Schur index. This theorem says, roughly, that in order to find the Schur indices for representations of arbitrary finite groups, it is enough to find the Schur indices for representations of Q-elementary groups. If p is a rational prime and z is a rational integer, then the highest power of p which divides z will be called the p-part of z. Here is Brauer's theorem.

THEOREM 3. *Let $\mathfrak{G}$ be a finite group and let K be an algebraic number field. Let χ be an absolutely irreducible character of $\mathfrak{G}$ with values in K. For each rational prime p there exists an algebraic number field L over K, a subgroup $\mathfrak{H}$ of $\mathfrak{G}$ which is L-elementary with respect to p, and an absolutely irreducible character ξ of $\mathfrak{H}$ with values in L, such that the p-part of $m_{\mathsf{K}}(\chi)$ is $m_{\mathsf{K}}(\xi)$.*

Actually the theorem as stated above is slightly stronger than Brauer's result. But since an L-elementary group is Q-elementary for any number field L, the whole question of the indices is reduced, as in [4], to the determination of the indices for Q-elementary groups. The assumption that χ has values in K is no essential restriction, for Schur has shown that we may replace K by $\mathsf{K}(\chi)$ and the index remains unchanged. The crucial point in Brauer's argument is a lemma which he proves using certain complicated congruences for the minors of a determinant whose entries are the values of characters. The theorem then follows neatly using results of Schur. We shall use Theorem 1 to give a quick proof of the lemma and refer the reader to [4] for the final deduction of Theorem 3. Witt [11] has given a proof of a similar result using the theory of central division algebras over a $\mathfrak{p}$-adic field.

LEMMA 6. *Let χ be an absolutely irreducible character of $\mathfrak{G}$ and let L be a subfield of $\mathsf{K}(\varepsilon_n)$ over $\mathsf{K}(\chi)$ such that $[\mathsf{K}(\varepsilon_n) : \mathsf{L}]$ is a power of p. Then there exists a subgroup $\mathfrak{H}$ of $\mathfrak{G}$ which is L-elementary with respect to p, and an absolutely*

irreducible character ξ of $\mathfrak{H}$ with values in L, *such that ξ appears in the restriction of χ to $\mathfrak{H}$ with multiplicity prime to p.*

PROOF. Let $g=p^e g_0$ be the order of $\mathfrak{G}$, where $(g_0, p)=1$. We apply Lemma 5 with the field L in place of K. This states that g_0 is a linear combination with ratonal integer coefficients of L-characters of $\mathfrak{G}$ induced by L-characters of L-elementary subgroups of $\mathfrak{G}$. The subgroups are actually L-elementary with respect to p. This is the case because our function ζ of Lemma 4 is constructed from characters of subgroups that are K-elementary with respect to p, and the new subgroups we introduce in the proof of Lemma 5 are all cyclic. A cyclic group is L-elementary with respect to p for any field L and any prime p. Thus we have a formula

$$g_0 = \sum_j z_j \psi_j^*$$

where the z_j are rational integers and the ψ_j^* are induced by L-characters ψ_j of L-elementary subgroups of $\mathfrak{G}$. It follows from the Frobenius Reciprocity Theorem as in [**6**] that

$$\chi\psi_j^* = ((\chi \mid \mathfrak{H}_j)\psi_j)^*$$

and hence that

$$g_0\chi = \sum_j z_j \chi\psi_j^* = \sum_j z_j((\chi \mid \mathfrak{H}_j)\psi_j)^*$$

where $\mathfrak{H}_j$ is the L-elementary subgroup corresponding to ψ_j. Since L includes K(χ), it follows that χ is a character in L and hence the characters $(\chi \mid \mathfrak{H}_j)\psi_j$ are characters in L. Thus the characters $(\chi \mid \mathfrak{H}_j)\psi_j$ may be written as linear combinations with rational integer coefficients of characters $\mathrm{Sp}_L(\xi_i)$ where the ξ_i are absolutely irreducible characters of subgroups of $\mathfrak{G}$ which are L-elementary with respect to p. Thus we have a formula

$$g_0\chi = \sum_i w_i(\mathrm{Sp}_L(\xi_i))^*$$

where the w_i are rational integers. Let (χ, ξ_i^*) be the multiplicity of χ in ξ_i^*. Since χ is a character in L, this multiplicity remains the same when we replace ξ_i by any one of its algebraic conjugates over L. Thus the multiplicity of χ in $(\mathrm{Sp}_L(\xi_i))^*$ is $[L(\xi_i) : L](\chi, \xi_i^*)$. If we count the multiplicity of χ on both sides of our equation for $g_0\chi$ we see that

$$g_0 = \sum_i w_i[L(\xi_i) : L](\chi, \xi_i^*),$$

Now g_0 is prime to p. It follows that there must exist some character $\xi=\xi_i$ such that

$$[L(\xi) : L](\chi, \xi^*) \not\equiv 0 \mod p.$$

Our assumption on L implies that $[L(\xi) : L]$ is either one or a power of p, hence $[L(\xi) : L]=1$, $L(\xi)=L$ and ξ is a character in L. Let $\mathfrak{H}$ be the L-elementary

subgroup of which ξ is an absolutely irreducible character. Since (χ, ξ^*) is prime to p, it follows from the Frobenius Reciprocity Theorem that the multiplicity $(\xi, \chi|\mathfrak{H})$ is prime to p, and this completes the proof of the lemma.

Now for the proof of Theorem 3, one chooses L to be that subfield of $\mathsf{K}(\varepsilon_n)/\mathsf{K}$ for which $[\mathsf{K}(\varepsilon_n):\mathsf{L}]$ is a power of p and $[\mathsf{L}:\mathsf{K}]$ is prime to p. The character and subgroup furnished by Lemma 6 are the character and subgroup whose existence is asserted by the theorem. Note that the field L is independent of the character χ and depends only on the exponent of the group.

5. Elementary groups; the construction of splitting fields

In this section all irreducible characters are absolutely irreducible. We recall some general facts about induced characters. Let $\mathfrak{G}$ be a finite group and let $\mathfrak{H}$ be a normal subgroup of $\mathfrak{G}$. If ψ is an irreducible character of $\mathfrak{H}$ and $G \in \mathfrak{G}$, then the function ψ^G defined on $\mathfrak{H}$ by $\psi^G(H) = \psi(G^{-1}HG)$, $H \in \mathfrak{H}$, is also an irreducible character of $\mathfrak{H}$. We say that the characters ψ and ψ^G are *associated* in $\mathfrak{G}$. Those elements $G \in \mathfrak{G}$ for which $\psi^G = \psi$ form a subgroup $\mathfrak{T}$ of $\mathfrak{G}$ which includes $\mathfrak{H}$ and is called the *inertial group* of ψ. If χ is an irreducible character of $\mathfrak{G}$ then a theorem of Clifford states that there exists an irreducible character ψ of $\mathfrak{H}$ such that

$$\chi|\mathfrak{H} = e \sum_{G \bmod \mathfrak{T}} \psi^G$$

where e is a positive rational integer called the *ramification* of χ in $\mathfrak{H}$. If $e=1$ we say that χ is *unramified* in $\mathfrak{H}$. If χ vanishes outside $\mathfrak{H}$, then it follows from the orthogonality relations that $\chi|\mathfrak{H}$ is reducible. A further consequence of the orthogonality relations is the fact that ψ induces χ if and only if χ vanishes outside $\mathfrak{H}$ and χ is unramified in $\mathfrak{H}$. If $(\mathfrak{G}:\mathfrak{H})$ is a prime p, then $e=1$.

Let $\mathfrak{G} = \mathfrak{N}\mathfrak{P}$ be a Q-elementary group with respect to the prime p. In the following Theorem 5 we show that the field generated over Q by the characters of $\mathfrak{N}$ is a splitting field for the representations of $\mathfrak{G}$. This statement is not quite correct in case $p=2$. The heart of the argument is contained in

THEOREM 4. *Let $\mathfrak{G} = \mathfrak{N}\mathfrak{P}$ be a Q-elementary group with respect to the prime p. Let ε_a be a primitive a-th root of unity, where a is the order of $\mathfrak{N}$. If p is odd, let $\mathsf{K} = \mathsf{Q}(\varepsilon_a)$. If $p=2$, let $\mathsf{K} = \mathsf{Q}(\varepsilon_a, \sqrt{-1})$. If χ is an irreducible nonlinear character of $\mathfrak{G}$, then there exists a normal subgroup $\mathfrak{N}$ of index p in $\mathfrak{G}$ and an irreducible character ζ of $\mathfrak{N}$, such that ζ induces χ and $\mathsf{K}(\zeta) = \mathsf{K}(\chi)$.*

PROOF. Let $\mathfrak{H}$ be a normal subgroup of $\mathfrak{G}$ such that

(1) χ vanishes outside $\mathfrak{H}$.

(2) χ is unramified in $\mathfrak{H}$.

(3) the irreducible constituents of $\chi|\mathfrak{H}$ are algebraically conjugate over K.

Thus if ψ is an irreducible constituent of $\chi|\mathfrak{H}$, there exists for each $G \in \mathfrak{G}$ a

uniquely determined automorphism $\sigma(G)$ of $\mathsf{K}(\psi)/\mathsf{K}$ such that $\psi^G = \psi^{\sigma(G)}$.

Let us choose the normal subgroup $\mathfrak{H}$ so that it has minimal order with respect to properties (1), (2) and (3). It may happen that $\mathfrak{H} = \mathfrak{G}$. We consider two cases.

Case I: ψ is a nonlinear character. Since $\mathfrak{H}$ is a subgroup of the Q-elementary group $\mathfrak{G}$, $\mathfrak{H}$ is itself Q-elementary. It is shown in [4] that all irreducible characters of Q-elementary groups have degrees which are powers of p, and are induced by linear characters of suitable subgroups. A subgroup of index p in a Q-elementary group is a normal subgroup; this follows at once from the corresponding fact for p-groups. Thus there exists a normal subgroup $\mathfrak{J}$ of $\mathfrak{H}$ of index p in $\mathfrak{H}$ such that ψ is induced by an irreducible character of $\mathfrak{J}$. Since $\mathfrak{J}$ is normal in $\mathfrak{H}$, it follows that ψ vanishes outside $\mathfrak{J}$. Let $\mathfrak{D}$ be the intersection of the subgroups conjugate to $\mathfrak{J}$ in $\mathfrak{G}$. Then $\mathfrak{D}$ is a normal subgroup of $\mathfrak{G}$. Since ψ induces χ, it follows that ψ is a constituent of $\chi|\mathfrak{H}$ and then ψ^G is a constituent of $\chi|\mathfrak{H}$ for all $G \in \mathfrak{G}$. By assumption, all ψ^G are algebraic conjugates of ψ and hence all ψ^G vanish outside $\mathfrak{J}$. Thus ψ vanishes outside all conjugates of $\mathfrak{J}$ and so ψ vanishes outside $\mathfrak{D}$. Since $\mathfrak{J}$ is properly included in $\mathfrak{H}$, so is $\mathfrak{D}$. It follows at once from the corresponding fact for p-groups, that every Q-elementary group has a principal series in which the factor groups are cyclic of prime order. Since any two principal series for $\mathfrak{G}$ have isomorphic factors, and since both $\mathfrak{D}$ and $\mathfrak{H}$ are normal in $\mathfrak{G}$, it follows that there exists a normal subgroup $\mathfrak{K}$ of $\mathfrak{G}$ such that $\mathfrak{D} \subseteqq \mathfrak{K} \subset \mathfrak{H}$ and $(\mathfrak{H}:\mathfrak{K}) = q$, where q is prime. Since ψ vanishes outside $\mathfrak{K}$, and $(\mathfrak{H}:\mathfrak{K})$ is prime, it follows that ψ is unramified in $\mathfrak{K}$. Thus there exists an irreducible character ϕ of $\mathfrak{K}$ such that

$$\psi|\mathfrak{K} = \sum_{j=0}^{q-1} \phi^{H^j}$$

where $1, H, \cdots, H^{q-1}$ is a set of representatives for $\mathfrak{H} \bmod \mathfrak{K}$. Then ϕ induces ψ and hence ϕ induces χ. Since the degree of χ is a power of p, this implies $q = p$. Moreover the normal subgroup $\mathfrak{K}$ satisfies conditions (1) and (2).

Let $\mathfrak{N}$ be the subgroup of all $G \in \mathfrak{G}$ such that ϕ^G is algebraically conjugate to ϕ over K. By minimality of $\mathfrak{H}$, it follows that $\mathfrak{N} \subset \mathfrak{G}$. Clearly $\mathsf{K}(\psi) \subseteqq \mathsf{K}(\phi)$. Extend each of the automorphisms $\sigma(G)$ to an automorphism of $\mathsf{K}(\phi)/\mathsf{K}$ which we denote again $\sigma(G)$. For $G \in \mathfrak{G}$ we have $\psi^G = \psi^{\sigma(G)}$ and hence

$$\sum_{j=0}^{p-1} \phi^{H^j G} = \sum_{j=0}^{p-1} (\phi^{H^j})^{\sigma(G)}.$$

Thus we must have $\phi^{\sigma(G)} = \phi^{H^j G}$ for some $j = 0, 1, \cdots, p-1$ and this means $H^j G \in \mathfrak{N}$. Since $G \in \mathfrak{G}$ was arbitrary, it follows that $(\mathfrak{G}:\mathfrak{N}) \leqq p$ and hence $(\mathfrak{G}:\mathfrak{N}) = p$.

The restriction of an irreducible character of a group $\mathfrak{G}$ to a normal sub-

group $\mathfrak{M}$ can split into at most $(\mathfrak{G}:\mathfrak{M})$ irreducible constituents. Since $\mathfrak{K}$ has properties (1) and (2), it follows from the orthogonality relations that the number of irreducible constituents of $\chi|\mathfrak{K}$ is

$$\frac{1}{(\mathfrak{K}:1)}\sum_{K\in\mathfrak{K}}|\chi(K)|^2=\frac{1}{(\mathfrak{K}:1)}\sum_{G\in\mathfrak{G}}|\chi(G)|^2=(\mathfrak{G}:\mathfrak{K}).$$

Since $\mathfrak{K}\subseteq\mathfrak{N}\subset\mathfrak{G}$ we see that $\chi|\mathfrak{N}$ splits into $(\mathfrak{G}:\mathfrak{N})$ distinct irreducible constituents. Thus there exists an irreducible character ζ of $\mathfrak{N}$ such that $\chi|\mathfrak{N}=\sum_{G \bmod N}\zeta^G$ and ζ induces χ. One of the characters $\zeta^G|\mathsf{K}$ has ϕ as a constituent and we may suppose without any loss of generality that $\zeta|\mathfrak{K}$ has ϕ as a constituent.

Clearly $\mathsf{K}(\chi)\subseteq\mathsf{K}(\zeta)$. If $\mathsf{K}(\chi)\subset\mathsf{K}(\zeta)$ then there exists an automorphism τ of $\mathsf{K}(\zeta)/\mathsf{K}$ such that $\chi^\tau=\chi$ but $\zeta^\tau\neq\zeta$. Since $\chi^\tau=\chi$ we have $(\zeta^\tau,\chi|\mathfrak{N})=(\zeta,\chi|\mathfrak{N})$ and so ζ^τ is a constituent of $\chi|\mathfrak{N}$. Thus $\zeta^\tau=\zeta^G$ for some $G\in\mathfrak{G}$, $G\notin\mathfrak{N}$. Since $\mathfrak{G}/\mathfrak{N}$ is cyclic of order p it follows that all ζ^G, $G\in\mathfrak{G}$, are algebraically conjugate over K. But $\zeta|\mathfrak{K}$ splits into $(\mathfrak{N}:\mathfrak{K})$ distinct constituents and ϕ is one of them, so that we have $\zeta|\mathfrak{K}=\sum_{N \bmod \mathfrak{K}}\phi^N$. All the characters ϕ^N are algebraically conjugate over K by definition of $\mathfrak{N}$. Hence all constituents of $\chi|\mathfrak{K}$ are algebraically conjugate over K and this contradicts the minimality of $\mathfrak{H}$. Thus we rule out the possibility $\mathsf{K}(\chi)\subset\mathsf{K}(\zeta)$ and must have $\mathsf{K}(\chi)=\mathsf{K}(\zeta)$, which completes the proof in Case I.

Case II: ψ is a linear character. It is no restriction to assume, from the beginning, that χ is the character of a faithful representation of $\mathfrak{G}$. Since all the associates of ψ are algebraically conjugate over K, their corresponding representations have the same kernel, and the formula $\chi|\mathfrak{H}=\sum_{G \bmod \mathfrak{H}}\psi^G$ shows that this kernel must be the identity subgroup. Thus ψ is a faithful linear character of $\mathfrak{H}$ and it follows that $\mathfrak{H}$ is a cyclic group.

We shall have occasion to use, more than once, the following general remark about group characters. Let $\mathfrak{G}$ be a finite group and let $\mathfrak{H}$ be an abelian subgroup of $\mathfrak{G}$. Then any irreducible character of $\mathfrak{G}$ has degree at most $(\mathfrak{G}:\mathfrak{H})$. This is the case because every irreducible character of $\mathfrak{G}$ is a constituent of a character induced by a character of $\mathfrak{H}$ and all the characters of $\mathfrak{H}$ are linear. Let us apply this remark to the case at hand. Since χ is an irreducible character of degree $(\mathfrak{G}:\mathfrak{H})$ it follows that $\mathfrak{H}$ is its own centralizer in $\mathfrak{G}$. Thus the group $\mathfrak{G}/\mathfrak{H}$ may be represented faithfully as a group of automorphisms of the cyclic group $\mathfrak{H}$, and in particular it follows that $\mathfrak{G}/\mathfrak{H}$ is abelian. However, in view of the fact that K contains the a-th roots of unity we can say much more. The map $G\to\sigma(G)$ is a homomorphism of $\mathfrak{G}$ into the Galois group $\mathrm{Gal}(\mathsf{K}(\psi)/\mathsf{K})$. If G lies in the kernel, then $\psi^G=\psi^{\sigma(G)}=\psi$, so that $\psi(G^{-1}HG)=\psi(H)$ for all $H\in\mathfrak{H}$. Since ψ is the character of a faithful repre-

sentation, this means that G lies in the centralizer of $\mathfrak{H}$ and hence $G \in \mathfrak{H}$. Thus the kernel of the homomorphism is $\mathfrak{H}$ and we have an isomorphism of $\mathfrak{G}/\mathfrak{H}$ into $\mathrm{Gal}(\mathsf{K}(\psi)/\mathsf{K})$. Since the index of $\mathfrak{H}$ in $\mathfrak{G}$ is a power of p, the order of $\mathfrak{H}$ may be written as $p^b a$. For p odd we have $\mathsf{K} = \mathsf{Q}(\varepsilon_a)$ and $\mathsf{K}(\psi) = \mathsf{Q}(\varepsilon_{p^b}, \varepsilon_a)$ and since $(a, p) = 1$ we have an isomorphism $\mathrm{Gal}(\mathsf{K}(\psi)/\mathsf{K}) \cong \mathrm{Gal}(\mathsf{Q}(\varepsilon_{p^b})/\mathsf{Q})$. This last group is cyclic of order $p^{b-1}(p-1)$. Thus $\mathfrak{G}/\mathfrak{H}$ is a cyclic group. The case $b = 0$ is impossible, for if $b = 0$ then the Galois groups reduce to the identity, hence $\mathfrak{G} = \mathfrak{H}$ is a cyclic group and cannot have a nonlinear irreducible character χ. For $p = 2$ we have $\mathrm{Gal}(\mathsf{K}(\psi)/\mathsf{K}) \cong \mathrm{Gal}(\mathsf{Q}(\varepsilon_{2^b})/\mathsf{Q}(\sqrt{-1}))$ which is cyclic of order 2^{b-2}. Here too $\mathfrak{G}/\mathfrak{H}$ is a cyclic group. The cases $b = 0, 1, 2$ are impossible.

We introduce generators and relations for $\mathfrak{G}$. Let $A \in \mathfrak{H}$ be an element of order a and let $B \in \mathfrak{H}$ be an element of order p^b. Let the order of $\mathfrak{G}/\mathfrak{H}$ be p^c and choose an element $C \in \mathfrak{G}$ such that C generates $\mathfrak{G} \bmod \mathfrak{H}$. Thus $C^{p^c} = A^r B^s$ for some integers r, s. Since the order of $\mathfrak{G}/\mathfrak{H}$ is p^c and $(a, p) = 1$ it follows that C^a generates $\mathfrak{G} \bmod \mathfrak{H}$ and we have $C^{ap^c} = B^{as}$. Thus we may replace C by C^a and it is no restriction to assume that $C^{p^c} \in \{B\}$. Since $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$ and since the orders of A and B are coprime, it follows that both the cyclic subgroups $\{A\}$ and $\{B\}$ are normal in $\mathfrak{G}$. Thus we may define $\mathfrak{G}$ by generators A, B, C and relations

$$A^a = 1, \qquad B^{p^b} = 1, \qquad C^{p^c} = B^s,$$
$$C^{-1}AC = A^t, \qquad C^{-1}BC = B^u, \qquad AB = BA$$

where s, t, u are rational integers.

Now $\psi(C^{-k}A^iC^k) = \psi(A^i)^{\sigma(C^k)} = \psi(A^i)$ since the automorphisms σ leave K fixed. Thus

$$\chi(A^iB^j) = \sum_{k=0}^{p^c-1} \psi(C^{-k}A^iB^jC^k) = \psi(A^i) \sum_{k=0}^{p^c-1} \psi(C^{-k}B^jC^k)$$

and χ vanishes outside $\{A, B\}$. Let ψ_0 be the restriction of ψ to $\{B\}$ and let χ_0 be the induced character of $\{B, C\}$. Then

$$\chi(A^iB^j) = \psi(A^i)\chi_0(B^j).$$

Since χ is an irreducible character of $\mathfrak{G}$ and vanishes outside $\{A, B\}$, it follows from the orthogonality relations that χ_0 is an irreducible character of $\{B, C\}$. Thus $\{B\}$ is its own centralizer in $\{B, C\}$.

We shall prove the existence of an integer z such that $(CB^z)^{p^c} = 1$. First note $c > 0$, else $\mathfrak{G}$ is cyclic. Since $B = C^{-p^c}BC^{p^c} = B^{up^c}$ it follows that $u^{p^c} \equiv 1 \bmod p^b$. On the other hand $u^{p^{c-1}} \not\equiv 1 \bmod p^b$. For $u^{p^{c-1}} \equiv 1 \bmod p^b$ would imply that $C^{p^{c-1}}$ commutes with B and this contradicts the fact that $\{B\}$ is its own centralizer in $\{B, C\}$. Write $u = 1 + xp^d$ where $(x, p) = 1$. Since $b > 0$ and $c > 0$ we have $u \equiv u^{p^c} \equiv 1 \bmod p$ so that $d \geqq 1$. If $p = 2$, then our assumption that $\sqrt{-1} \in \mathsf{K}$

implies $u \equiv 1 \bmod 4$ and hence $d \geqq 2$. To see this note that $\psi(B)^u = \psi(B^u) = \psi(C^{-1}BC) = \psi(B)^{\sigma(C)}$ where $\sigma(C)$ is an automorphism of $\mathsf{K}(\psi)$ leaving $\sqrt{-1}$ fixed. Since $b > 2$, $\sqrt{-1}$ is a power of the primitive 2^b-th root of unity $\psi(B)$. Thus $(\sqrt{-1})^u = (\sqrt{-1})^{\sigma(C)} = \sqrt{-1}$ and hence $u \equiv 1 \bmod 4$ as asserted. Now

$$u \equiv 1 \mod p^d \qquad u \not\equiv 1 \mod p^{d+1}$$

and we may conclude from this, by successive applications of the binomial theorem, that

$$u^{p^{c-1}} \equiv 1 \mod p^{c+d+1} \qquad u^{p^{c-1}} \not\equiv 1 \mod p^{c+d}$$

$$u^{p^c} \equiv 1 \mod p^{c+d} \qquad u^{p^c} \not\equiv 1 \mod p^{c+d+1}.$$

Thus $c+d=b$ and we have

$$u = 1+xp^{b-c} \qquad \text{where } (x,p)=1.$$

Also

$$u^{p^c} = 1+yp^b \qquad \text{where } (y,p)=1.$$

If z is any rational integer, it is easy to verify by induction the formula

$$(CB^z)^j = C^j B^{z(1+u+\cdots+u^{j-1})}.$$

For $j = p^c$ we have

$$1+u+\cdots+u^{p^c-1} = \frac{u^{p^c}-1}{u-1} = \frac{y}{x}p^c.$$

Since x and y are rational integers prime to p it follows that x divides y. On the other hand we have

$$B^s = C^{-1}B^sC = (C^{-1}BC)^s = B^{s(1+xp^{b-c})}$$

so that $s \equiv s(1+xp^{b-c}) \bmod p^b$ and then $s \equiv 0 \bmod p^c$. If z is a solution of the congruence

$$\frac{s}{p^c} + z\frac{y}{x} \equiv 0 \mod p^{b-c}$$

then

$$s + zp^c\frac{y}{x} \equiv 0 \mod p^b$$

and then

$$(CB^z)^{p^c} = C^{p^c}B^{zp^cy/x} = B^{s+zp^cy/x} = 1.$$

This proves the existence of our rational integer z. If we replace C by CB^z we see that our group $\mathfrak{G}$ may be defined by generators A, B, C and relations

$$A^a = 1, \qquad B^{p^b} = 1, \qquad C^{p^c} = 1,$$

$$C^{-1}AC = A^t, \qquad C^{-1}BC = B^{1+xp^{b-c}}, \qquad AB = BA.$$

Let us consider the subgroup $\mathfrak{N} = \{A, B^p, C\}$ of $\mathfrak{G}$. Clearly $ACA^{-1} \in \mathfrak{N}$ and since $b-c \geqq 1$ we have $BCB^{-1} \in \mathfrak{N}$. Thus $\mathfrak{N}$ is a normal subgroup of index p in $\mathfrak{G}$. The relation $C^{-1}BC = B^{1+xp^{b-c}}$ shows that B^{p^c} commutes with C and

hence $\{B^{p^c}, C\}$ is an abelian subgroup of $\{B^p, C\}$ of order $p^{b-c}p^c = p^b$, and hence of index p^{c-1} in $\{B^p, C\}$. Now the irreducible character χ_0 of $\{B, C\}$ has degree p^c and hence the restriction of χ_0 to $\{B^p, C\}$ must be reducible. Since $|\chi(A^iB^j)| = |\chi_0(B^j)|$ and χ vanishes outside $\{A, B\}$ it follows from the orthogonality relations that the restriction of χ to $\mathfrak{N}$ is reducible. Say $\chi|\mathfrak{N} = \sum_{G \bmod \mathfrak{N}} \zeta^G$ where ζ is an irreducible character of $\mathfrak{N}$.

Since χ vanishes outside $\{A, B\}$ we have

$$\chi(C^k) = \begin{cases} 0 & k = 1, 2, \cdots, p^c - 1 \\ p^c & k = 0. \end{cases}$$

Thus the restriction of χ to $\{C\}$ is the regular representation of $\{C\}$ and in particular this restriction contains the principal character of $\{C\}$ just once. On the other hand $\{C\} \subseteqq \mathfrak{N}$ so that some $\zeta^G|\{C\}$ contains the principal character of $\{C\}$. Thus no two constituents of $\chi|\{C\}$ are algebraically conjugate over K. Now the argument given in the last paragraph of the proof of Case I shows that $\mathsf{K}(\zeta) = \mathsf{K}(\chi)$. This completes the proof of Theorem 4.

With Theorem 4 it is easy to construct a splitting field for the representations of a Q-elementary group.

THEOREM 5. *Let $\mathfrak{G} = \mathfrak{A}\mathfrak{P}$ be a Q-elementary group with respect to the prime p. If p is odd, let $\mathsf{K} = \mathsf{Q}(\varepsilon_a)$ be the field of a-th roots of unity, where a is the order of $\mathfrak{A}$. If $p = 2$, let $\mathsf{K} = \mathsf{Q}(\varepsilon_a, \sqrt{-1})$. If χ is an absolutely irreducible character of $\mathfrak{G}$ then $m_{\mathsf{K}}(\chi) = 1$. Thus the representation corresponding to the character χ may be written with coefficients in the field $\mathsf{K}(\chi)$.*

PROOF. The proof will be by induction on the degree of the character. If χ is a linear character there is nothing to prove. If χ is a nonlinear character, let ζ be the character furnished by Theorem 4. By the induction hypothesis $m_{\mathsf{K}}(\zeta) = 1$ so that ζ is the character of a representation which may be written with coefficients in $\mathsf{K}(\zeta)$. The induced character χ is then the character of a representation which may be written with coefficients in $\mathsf{K}(\zeta) = \mathsf{K}(\chi)$. Hence $m_{\mathsf{K}}(\chi) = 1$ and this completes the proof.

For p-groups we have the following interesting corollary.

COROLLARY. *Let $\mathfrak{G}$ be a p-group and let $\mathfrak{F}$ be an absolutely irreducible representation of $\mathfrak{G}$ with character χ. If p is odd, then $\mathfrak{F}$ may be written with coefficients in the field $\mathsf{Q}(\chi)$. If $p = 2$ then $\mathfrak{F}$ may be written with coefficients in the field $\mathsf{Q}(\chi, \sqrt{-1})$.*

6. A bound for the Schur index

Let $\mathfrak{G}$ be a finite group of order g. Brauer has shown [2] that the field of g-th roots of unity splits all the absolutely irreducible representations of $\mathfrak{G}$. This fact may be deduced [3] from our Theorem 1 for the field $\mathsf{K} = \mathsf{Q}(\varepsilon_g)$.

If χ is an absolutely irreducible character of $\mathfrak{G}$, it follows from the work of Schur that the index $m_{\mathbf{Q}}(\chi)$ divides the degree $[\mathbf{Q}(\varepsilon_g):\mathbf{Q}]=\Phi(g)$ where Φ is the Euler function. If $g=\prod_{i=1}^{r} q_i^{b_i}$ is the decomposition of g into prime factors, then $\Phi(g)=\prod_{i=1}^{r} q_i^{b_i-1}(q_i-1)$, so that $m_{\mathbf{Q}}(\chi)$ divides $\prod_{i=1}^{r} q_i^{b_i-1}(q_i-1)$. With the results of the preceding section we can prove the stronger

THEOREM 6. *Let $\mathfrak{G}$ be a finite group of order $g=\prod_{i=1}^{r} q_i^{b_i}$ and let χ be an absolutely irreducible character of $\mathfrak{G}$. Then $m_{\mathbf{Q}}(\chi)$ divides $2\prod_{i=1}^{r}(q_i-1)$.*

PROOF. Let p be a prime which divides g and write $g=p^c g_0$ where g_0 is prime to p. From Schur's work we know that $m_{\mathbf{Q}}(\chi)=m_{\mathbf{Q}(\chi)}(\chi)$. Theorem 3 for the field $\mathsf{K}=\mathbf{Q}(\chi)$ tells us that there exists a $\mathbf{Q}$-elementary subgroup $\mathfrak{H}$ and an absolutely irreducible character ξ of $\mathfrak{H}$ such that the p-part of $m_{\mathbf{Q}(\chi)}(\chi)$ is $m_{\mathbf{Q}(\chi)}(\xi)$. Since $\mathbf{Q}(\chi)$ is a field over $\mathbf{Q}$ it follows from Schur's work that $m_{\mathbf{Q}(\chi)}(\xi)$ divides $m_{\mathbf{Q}}(\xi)$ and hence the p-part of $m_{\mathbf{Q}}(\chi)$ divides $m_{\mathbf{Q}}(\xi)$. Let ε_0 be a primitive g_0-th root of unity. Set $\mathsf{L}_0=\mathbf{Q}(\varepsilon_0)$ if p is odd, and set $\mathsf{L}_0=\mathbf{Q}(\varepsilon_0,\sqrt{-1})$ if $p=2$. Then Theorem 5 shows that the representation corresponding to ξ may be written with coefficients in the field $\mathsf{L}_0(\xi)$. It follows again from Schur's work that $m_{\mathbf{Q}}(\xi)$ divides $[\mathsf{L}_0(\xi):\mathbf{Q}(\xi)]$ and so $m_{\mathbf{Q}}(\xi)$ divides $[\mathsf{L}_0:\mathbf{Q}]$. Now $[\mathsf{L}_0:\mathbf{Q}]=\Phi(g_0)$ if p is odd and $[\mathsf{L}_0:\mathbf{Q}]=2\Phi(g_0)$ if $p=2$. Since g_0 is prime to p and $m_{\mathbf{Q}}(\xi)$ is a power of p, it follows that $m_{\mathbf{Q}}(\xi)$ divides $\prod(q-1)$ when p is odd, and that it divides $2\prod(q-1)$ when $p=2$, where the products are over all distinct primes q which divide g_0. Now let p range over all the prime divisors of g and the theorem is proved.

References

[1] S. D. Berman, The p-adic ring of characters, Doklady Akad. Nauk SSSR, **106** (1956), 583-586 (Russian).

[2] R. Brauer, On the representation of a group of order g in the field of the g-th roots of unity, Amer. J. Math., **67** (1945), 461-471 (full references are given here to work before 1945).

[3] R. Brauer, Applications of induced characters, Amer. J. Math., **69** (1947), 709-716.

[4] R. Brauer, On the algebraic structure of group rings, J. Math. Soc. Japan, **3** (1951), 237-251.

[5] R. Brauer, A characterization of the characters of groups of finite order, Ann. of Math., **57** (1953), 357-377.

[6] R. Brauer and J. Tate, On the characters of finite groups, Ann. of Math., **62** (1955), 1-7.

[7] M. Deuring, Algebren, Berlin, 1935.

[8] M. Hall, The Theory of Groups, New York, 1959.

[9] P. Roquette, Arithmetische Untersuchung des Charakterringes einer endlichen Gruppe, J. Reine. Angew. Math., **190** (1952), 148-168.

[10] I. Schur, Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen, S.-B. Preuss. Akad. Wiss., (1906) 164-184.

[11] E. Witt, Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper, J. Reine Angew. Math., 190 (1952), 231-245.

Addendum, October 15, 1960: Theorem 5 has an easy corollary which seems worth a short remark.

COROLLARY. *Let $\mathfrak{G}$ be a finite group of order $g=p^{\alpha}g_0$ where $(p,g_0)=1$. Let ε be a primitive g_0-th root of unity. If p is odd let $\mathsf{K}=\mathsf{Q}(\varepsilon)$. If $p=2$ let $\mathsf{K}=\mathsf{Q}(\varepsilon,\sqrt{-1})$. If χ is an absolutely irreducible character of $\mathfrak{G}$ then $m_{\mathsf{K}}(\chi)$ is prime to p.*

This is quite clear in view of Theorems 3 and 5. It would be nice to have some improvement on Theorem 6. For the moment let us suppose that $\mathfrak{G}$ has odd order g. Let χ be an absolutely irreducible character of $\mathfrak{G}$ and let $q_1, q_2, \cdots, q_r$ be the distinct prime divisors of g. If we could construct a splitting field K of χ with $[\mathsf{K}:\mathsf{Q}]=\prod(q_i-1)$ then Theorem 6 would be an immediate corollary. For Schur's results would imply $m_{\mathsf{Q}}(\chi)\,|\,[\mathsf{K}(\chi):\mathsf{Q}(\chi)]$ and hence $m_{\mathsf{Q}}(\chi)\,|\,[\mathsf{K}:\mathsf{Q}]=\prod(q_i-1)$. Now there is at hand an obvious choice for a field of the desired degree, namely the cyclotomic field $\mathsf{Q}(\varepsilon_{q_1},\cdots,\varepsilon_{q_r})$ and this suggests the interesting possibility that the field $\mathsf{Q}(\varepsilon_{q_1},\cdots,\varepsilon_{q_r})$ is a splitting field for all the absolutely irreducible representations of $\mathfrak{G}$. This natural conjecture does turn out to be correct and there is a modified statement for groups of even order. The method of proof is that of Theorem 4 with only minor modifications and we give a brief sketch of the argument.

THEOREM 7. *Let $\mathfrak{G}$ be a finite group and let $q_1,\cdots,q_r$ be the distinct primes dividing the order g of $\mathfrak{G}$. If g is odd let $\mathsf{K}=\mathsf{Q}(\varepsilon_{q_1},\cdots,\varepsilon_{q_r})$. If g is even let $\mathsf{K}=\mathsf{Q}(\varepsilon_{q_1},\cdots,\varepsilon_{q_r},\sqrt{-1})$. If χ is an absolutely irreducible character of $\mathfrak{G}$ then $m_{\mathsf{K}}(\chi)=1$.*

PROOF. Suppose the theorem has been proved for all Q-elementary subgroups of $\mathfrak{G}$. If $p\,|\,g$, Theorem 3 shows the existence of a subgroup $\mathfrak{E}$ of $\mathfrak{G}$, Q-elementary for the prime p, and an absolutely irreducible character ξ of $\mathfrak{E}$ such that the p-part of $m_{\mathsf{K}}(\chi)$ is $m_{\mathsf{K}}(\xi)$. Suppose the primes q_i numbered so that $q_1,\cdots,q_s$ $s\leqq r$, are the primes dividing the order of $\mathfrak{E}$. Let $\mathsf{L}=\mathsf{Q}(\varepsilon_{q_1},\cdots,\varepsilon_{q_s})$ if $\mathfrak{E}$ has odd order and let $\mathsf{L}=\mathsf{Q}(\varepsilon_{q_1},\cdots,\varepsilon_{q_s},\sqrt{-1})$ if $\mathfrak{E}$ has even order. Then by truth of the theorem for Q-elementary groups we have $m_{\mathsf{L}}(\xi)=1$ and a fortiori $m_{\mathsf{K}}(\xi)=1$. Thus the p-part of $m_{\mathsf{K}}(\chi)$ is 1. Since this is true for all $p\,|\,g$ it follows that $m_{\mathsf{K}}(\chi)=1$.

Thus we may assume from the start that $\mathfrak{G}$ is Q-elementary for some prime p and we let $p=q_1,q_2,\cdots,q_r$ denote the prime divisors of g. Proceed by induction on the degree of χ. If χ is a linear character there is nothing to

prove. If χ is nonlinear note that the argument given in Case I of Theorem 4 is independent of the field K and hence applies equally well to our situation here. Thus we may assume that χ is induced by a linear character ψ of a cyclic subgroup $\mathfrak{H}$ of $\mathfrak{G}$ and that all the irreducible constituents of $\chi|\mathfrak{H}$ are algebraically conjugate over K. The crucial point here is that the field $\mathsf{Q}(\varepsilon_{q^\nu})$ is cyclic of degree $q^{\nu-1}$ over $\mathsf{Q}(\varepsilon_q)$ if q is an odd prime and $\nu \geqq 1$ while the field $\mathsf{Q}(\varepsilon_{2^\nu})$ is cyclic of degree $2^{\nu-2}$ over $\mathsf{Q}(\sqrt{-1})$ if $\nu \geqq 2$. Thus with our choice of the field K, the Galois group $\mathrm{Gal}(\mathsf{K}(\psi)/\mathsf{K})$ is a direct product of cyclic groups of relatively prime orders and is itself cyclic. Thus $\mathfrak{G}/\mathfrak{H}$ is a cyclic group. Now most of the argument in Case II of Theorem 4 may be applied. We keep the notation of Theorem 4 and remark that $q_2, \cdots, q_r$ are the prime divisors of a. If $p = q_1$ is odd then $b > 0$. For $b = 0$ would imply that $[\mathsf{K}(\chi) : \mathsf{K}]$ is prime to p, hence $\mathfrak{G} = \mathfrak{H}$ is a cyclic group, a contradiction. Actually the same argument shows that $b = 1$ is also impossible but we do not make use of this fact. Similarly the cases $b = 0, 1, 2$ are impossible for $p = 2$. Now the rest of the argument of Theorem 4, Case II, is independent of the field K. One proves the existence of a normal subgroup $\mathfrak{N}$ of index p in $\mathfrak{G}$ and an absolutely irreducible character ζ of $\mathfrak{N}$ such that ζ induces χ and $\mathsf{K}(\zeta) = \mathsf{K}(\chi)$. Then $m_{\mathsf{K}}(\chi) = m_{\mathsf{K}}(\zeta) = 1$ and the induction is complete.

I would like to thank the referee for his careful reading of the manuscript and in particular for his reference to the work of P. Roquette: Realisierung von Darstellungen endlicher nilpotenter Gruppen, Arch. Math., **9** (1958), 241-250. Roquette's paper appeared at about the same time the present work was submitted as a doctoral dissertation and the two pieces of work were done independently. Roquette proves Theorem 5 for nilpotent groups. His reduction to the case of primitive representations corresponds roughly to the initial reduction given by Case I of Theorem 4. The rest of his argument hinges on a lemma concerning p-groups: If $\mathfrak{G}$ is a p-group in which every abelian normal subgroup is cyclic, then $\mathfrak{G}$ is itself cyclic, unless $p = 2$ in which case $\mathfrak{G}$ has a cyclic subgroup of index 2 and the possibilities for $\mathfrak{G}$ may be enumerated. Roquette's computations in the proof of this lemma have their counterpart here in the computations in Case II of Theorem 4.

Haverford College,
Harvard University