Can. J. Math., Vol. XXII, No. 3, 1970, pp. 626–640

SOME RESULTS ON THE SCHUR INDEX OF A REPRESENTATION OF A FINITE GROUP

CHARLES FORD

Let $\mathfrak{G}$ be a finite group with a representation as an irreducible group of linear transformations on a finite-dimensional complex vector space. Every choice of a basis for the space gives the representing transformations the form of a particular group of matrices. If for some choice of a basis the resulting group of matrices has entries which all lie in a subfield K of the complex field, we say that the representation can be *realized* in K. It is well known that every representation of $\mathfrak{G}$ can be realized in some algebraic number field, a finite-dimensional extension of the rational field Q.

Let χ be the character of an irreducible complex representation $\mathbf{T}$ of $\mathfrak{G}$. We shall denote by $Q(\chi)$ the field extension of Q obtained by adjoining all the values $\chi(G)$ for $G \in \mathfrak{G}$. Then $Q(\chi)$ is contained in any field extension K of Q in which $\mathbf{T}$ can be realized. The *Schur index* $m(\chi)$ of χ over the rational field is the minimum possible dimension $(K:Q(\chi))$ taken over all algebraic number fields K in which $\mathbf{T}$ can be realized. This number $m(\chi)$ has two additional properties. First, $m(\chi)$ divides the dimension $(K:Q(\chi))$ for any algebraic number field K in which $\mathbf{T}$ can be realized. For the second, suppose that K is a field containing $Q(\chi)$ and that $\mathbf{T}$ appears as a component with multiplicity one in some representation which can be realized in K. Then $\mathbf{T}$ can be realized in K. See [**3**, § 70, theorem 70.12; **4**, theorem (11.4)] for these results. The number we have called $m(\chi)$ is there called $m_Q(\chi)$.

The problem of determining $m(\chi)$ has been greatly simplified by a theorem of R. Brauer, which we state after the following definition. For a prime number p, a group is said to be *elementary* with respect to p if it is the semi-direct product of a normal cyclic p'-group with a p-group.

THEOREM (Brauer). *Let χ be an irreducible complex character of a finite group $\mathfrak{G}$. Let $m(\chi)$ be the Schur index of χ over the rational field. For each prime divisor p of $m(\chi)$ there is an elementary subgroup of $\mathfrak{G}$ with respect to p, and an irreducible complex character of that subgroup whose Schur index is the p-part of $m(\chi)$.*

See [**5** or **3**, § 42 and § 70, pp. 475–479]. Elementary subgroups are called Q-elementary and, as with $m(\chi)$ and $m_Q(\chi)$, the definitions given here are easily seen to be special cases of the definitions given in [**3**; **4**; **5**].

Received April 7, 1969 and in revised form, February 5, 1970. The research for this paper was done while the author was a post-doctoral fellow at the University of Toronto and was supported by the National Research Council under grant number A-3022.

Let n be the exponent of $\mathfrak{G}$ and let ϵ be a primitive nth root of unity. Then the field $Q(\epsilon)$ is a Galois extension of Q with an Abelian Galois group over Q. Thus if K_1 and K_2 are subfields of $Q(\epsilon)$ with $K_1 \subset K_2$, then K_2 is a Galois extension of K_1, and the Galois group, which will be denoted by $\mathrm{Gal}(K_2/K_1)$, is Abelian. The field $Q(\epsilon)$ contains the field $Q(\psi)$ for any character ψ of a subgroup of $\mathfrak{G}$.

Suppose that $\{q_i\}$ is the set of prime divisors of the order of $\mathfrak{G}$. Let $k = 2\Pi q_i$ and let η be a primitive kth root of unity. Solomon [**5**] has shown that any irreducible complex representation of $\mathfrak{G}$ can be realized in the field $Q(\eta, \chi)$, where χ is the character of the representation. The first property of the Schur index then implies that $m(\chi)$ divides the dimension $(Q(\eta, \chi):Q(\chi))$. This equals the dimension $(Q(\eta):Q(\eta) \cap Q(\chi))$ which is a divisor of $(Q(\eta):Q)$. Using the Euler Φ-function, this last dimension is either $2\Pi(q_i - 1)$ or $\Pi(q_i - 1)$. Hence $m(\chi)$ divides $2\Pi(q_i - 1)$. The first theorem of the present paper is the following, which strengthens this result. This theorem may also be deduced from Witt's paper [**6**, *Satz* 12, p. 245].

THEOREM. *Let χ be an irreducible complex character of a finite group $\mathfrak{G}$. Let $m(\chi)$ be the Schur index of χ over the rational field. Then for each prime divisor p of $m(\chi)$, there is a prime q dividing the order of $\mathfrak{G}$ such that the p-part of $m(\chi)$ divides $(q - 1)$. An exception can occur if $\mathfrak{G}$ is a 2-group. We may have $m(\chi) = 2$ in this case.*

The second main result of the paper appears as the corollary to Theorem 2. It is a new result which relates the Schur index to the field of characters.

THEOREM. *Let χ be an irreducible complex character of a finite group $\mathfrak{G}$. Let $m = m(\chi)$ be the Schur index of χ over the rational field. For each odd prime divisor p of m, let p^e be the p-part of m. Then p^{e-1} divides the dimension $(Q(\chi):Q)$.*

Similar techniques are used in the proofs of the two theorems, and we begin by considering the first one. In view of Brauer's theorem, it is sufficient to prove this theorem for elementary groups, and we assume at the outset that $\mathfrak{G} = \mathfrak{A}\mathfrak{P}$, where $\mathfrak{A}$ is a cyclic normal p'-group and $\mathfrak{P}$ is a p-group. We shall use standard notation and basic properties of representation theory which can be found in either [**3**] or [**4**]. We begin with a result found in [**6**] with a proof adapted from [**5**]. See [**4**, theorem (14.3)].

LEMMA 1. *Let $\mathfrak{G} = \mathfrak{A}\mathfrak{P}$ be an elementary group with respect to the prime p. Let χ be an irreducible complex character of $\mathfrak{G}$. Then there exist subgroups $\mathfrak{H}$ and $\mathfrak{F}$ in $\mathfrak{G}$ and a linear character λ of $\mathfrak{H}$ such that:*

(1) $\mathfrak{A} \subseteq \mathfrak{H} \subseteq \mathfrak{F}$ *and* $\mathfrak{F}$ *normalizes* $\mathfrak{H}$,

(2) $Q(\xi) = Q(\chi)$, *where* ξ *is the character of* $\mathfrak{F}$ *induced by* λ,

(3) $\mathfrak{F}/\mathfrak{H} \approx \mathrm{Gal}(Q(\lambda)/Q(\xi))$,

(4) $m(\xi) = m(\chi)$.

Proof. There exist subgroups $\mathfrak{H}$ and $\mathfrak{F}$ in $\mathfrak{G}$ and a character λ (not necessarily linear) of $\mathfrak{H}$ which satisfy conditions (1) and (2) above, for example

take $\mathfrak{H} = \mathfrak{F} = \mathfrak{G}$ and $\lambda = \chi$. Among all such triples $(\mathfrak{H}, \mathfrak{F}, \lambda)$, choose one for which $|\mathfrak{F}| + \lambda(1)$ is minimal. Letting ξ be the character of $\mathfrak{F}$ induced by λ, we have assumed that $Q(\xi) = Q(\chi)$. We will show that $\mathscr{G} = \mathrm{Gal}(Q(\lambda)/Q(\chi))$ is isomorphic to a subgroup of $\mathfrak{F}/\mathfrak{H}$. Using the definitions of induction and irreducibility, it is not difficult to justify the following line of argument. Since λ induces an irreducible character, it must itself be irreducible. By the transitivity of induction, ξ induces χ, and hence ξ is also irreducible. Let $\sigma \in \mathscr{G}$. Since λ is irreducible, λ^σ is irreducible and λ^σ induces ξ^σ. But we assumed that $Q(\xi) = Q(\chi)$ which is the field fixed by $\mathscr{G}$. Thus λ^σ induces ξ. By the Frobenius Reciprocity Theorem, λ^σ appears once as a component in $\xi|_{\mathfrak{H}}$. Clifford's theorem shows that $\xi|_{\mathfrak{H}}$ is the sum of the group-theoretic conjugates of λ given by the factor group $\mathfrak{F}/\mathfrak{H}$. Thus $\lambda^\sigma = \lambda^G$ for a uniquely determined coset $G\mathfrak{H}$ of $\mathfrak{F}/\mathfrak{H}$. Since the processes of algebraic conjugation and group conjugation of a character commute, and since $\mathscr{G}$ is Abelian, the corresponding mapping $\sigma \to G\mathfrak{H}$ of $\mathscr{G}$ into $\mathfrak{F}/\mathfrak{H}$ is multiplicative.

Let $\mathfrak{F}_1/\mathfrak{H}$ be the image of $\mathscr{G}$ in $\mathfrak{F}/\mathfrak{H}$, and let ξ_1 be the character of $\mathfrak{F}_1$ induced by λ. Then the restriction $\xi_1|_{\mathfrak{H}}$ is, by the choice of $\mathfrak{F}_1$, the sum of the conjugates of λ under $\mathscr{G}$, and is therefore invariant under $\mathscr{G}$. Since $\mathfrak{F}_1$ normalizes $\mathfrak{H}$, and ξ_1 is induced from $\mathfrak{H}$, ξ_1 must vanish off $\mathfrak{H}$. Together, these statements show that ξ_1 is invariant under $\mathscr{G}$. Since $Q(\chi)$ is the subfield of $Q(\lambda)$ fixed by $\mathscr{G}$, $Q(\chi)$ must contain $Q(\xi_1)$. But ξ_1 induces χ, and thus the reverse containment must also hold. Therefore ξ_1 and χ generate the same field. Thus by our minimality assumption, $\mathfrak{F}_1 = \mathfrak{F}$, $\xi_1 = \xi$, and condition (3) holds.

Now suppose that λ is not linear. Since $\mathfrak{H}$ is a subgroup of an elementary group, it is also elementary. As is the case for p-groups, our character λ is induced from a character λ_0 of a normal subgroup $\mathfrak{H}_0$ of index p in $\mathfrak{H}$. (See [**4**, the proof of theorem (10.2)].) Since $\mathfrak{A}$ is a p'-group contained in $\mathfrak{H}$, $\mathfrak{A}$ is contained in $\mathfrak{H}_0$. Since λ is induced from a normal subgroup $\mathfrak{H}_0$, it must vanish off $\mathfrak{H}_0$. Then, for $G \in \mathfrak{F}$, λ^G vanishes off $\mathfrak{H}_0{}^{G^{-1}}$. But $\lambda^G = \lambda^\sigma$ for some $\sigma \in \mathscr{G}$; thus λ^σ and therefore λ vanish off $\mathfrak{H}_0{}^{G^{-1}}$. Let $\mathfrak{J}$ be the intersection of the conjugates of $\mathfrak{H}_0$ in $\mathfrak{F}$. Then λ vanishes off $\mathfrak{J}$, and $\mathfrak{J}$ is normal in $\mathfrak{F}$. Since $\mathfrak{A}$ is normal in $\mathfrak{G}$, $\mathfrak{A} \subseteq \mathfrak{J}$. By choosing a chief series for $\mathfrak{F}/\mathfrak{J}$ which includes $\mathfrak{H}/\mathfrak{J}$, we can find a subgroup $\mathfrak{H}_1$ normal in $\mathfrak{F}$ with $\mathfrak{J} \subseteq \mathfrak{H}_1 \subset \mathfrak{H}$ and $\mathfrak{H}_1$ of index p in $\mathfrak{H}$. The inner product formula involves division by the group order, and so since λ vanishes off $\mathfrak{H}_1$, the inner product of $\lambda|_{\mathfrak{H}_1}$ with itself equals the index p of $\mathfrak{H}_1$ in $\mathfrak{H}$. This means that $\lambda|_{\mathfrak{H}_1}$ is reducible. If λ_1 is an irreducible component of $\lambda|_{\mathfrak{H}_1}$, then λ is an irreducible component of $\lambda_1{}^{\mathfrak{H}}$. But the degree of λ_1 is strictly less than that of λ while the degree of λ is at most the degree of $\lambda_1{}^{\mathfrak{H}}$ which is p times the degree of λ_1. Since these degrees are all p-powers, λ and $\lambda_1{}^{\mathfrak{H}}$ have the same degree, which makes them equal. Since the use of λ_1 in place of λ would contradict our minimality assumption, λ must be linear.

We now prove (4). We have $\mathbf{T}$ as the representation affording χ, and we let $\mathbf{U}$ afford ξ. Suppose that $\mathbf{T}$ can be realized in some field K. By reciprocity,

ξ is a component with multiplicity one in $\chi|_{\mathfrak{F}}$. Thus by the second property of the Schur index, $\mathbf{U}$ can be realized in K. On the other hand, since ξ induces χ, $\mathbf{T}$ can be realized in any field in which $\mathbf{U}$ can be realized. Thus both representations can be realized in the same fields, and so ξ and χ must have the same Schur index. This proves the lemma.

In view of this lemma, the first main theorem will be proved if we can show the following: $m(\xi)$ divides $q - 1$ for some prime q dividing the order of $\mathfrak{F}$. Given the nature of the result we are trying to prove, we may as well assume that ξ is faithful. Thus we shall identify $\mathfrak{A}$, $\mathfrak{H}$, and $\mathfrak{F}$ with their images under the representation $\mathbf{U}$ affording ξ. We know from Lemma 1 that $\xi|_{\mathfrak{H}}$ is the sum of the algebraic conjugates of λ by the group $\mathcal{G} = \mathrm{Gal}(Q(\lambda)/Q(\xi))$. Therefore any element in the kernel of λ would also be in the kernel of ξ. Hence λ is also faithful, and $\mathfrak{H}$ must be cyclic. Since the correspondence between $\mathfrak{F}/\mathfrak{H}$ and $\mathcal{G}$ is one-to-one, $\mathfrak{H}$ must be its own centralizer in $\mathfrak{F}$.

It is not difficult to turn this argument around. Assume that $\mathfrak{H}$ is a cyclic, normal self-centralizing subgroup of a group $\mathfrak{F}$ and that λ is a faithful linear character of $\mathfrak{H}$. Then the character ξ of $\mathfrak{F}$ induced from λ is irreducible, and the correspondence between the coset $G\mathfrak{H}$ and $\sigma \in \mathcal{G}$ determined by $\lambda^G = \lambda^\sigma$ is an isomorphism between $\mathfrak{F}/\mathfrak{H}$ and $\mathcal{G}$. Notice that since the prime q we are trying to produce will be different from p, it will have to be a divisor of the order of $\mathfrak{A}$. In view of these remarks, the theorem we are trying to prove may be stated as follows.

THEOREM 1. *Let p be a prime and let $\mathfrak{F} = \mathfrak{A}\mathfrak{B}$ be an elementary group with respect to p. Let $\mathfrak{H}$ be a cyclic, normal self-centralizing subgroup of $\mathfrak{F}$ with a faithful linear character λ and let ξ be the character of $\mathfrak{F}$ induced by λ. Then ξ is an irreducible character of $\mathfrak{F}$, and there is a prime divisor q of the order of $\mathfrak{A}$ such that the Schur index $m(\xi)$ divides $q - 1$. An exception can occur when $p = 2$ and $\mathfrak{F} = \mathfrak{B}$ is a 2-group. We may have $m(\xi) = 2$ in this case.*

Proof. Let $\mathbf{U}$ be the representation affording ξ. As in [**6**], we shall use $\mathbf{U}$ to produce a simple algebra. The index of this algebra, or of the associated division algebra, will be our Schur index $m(\xi)$. (See [**1**, p. 58].) This algebra will have a natural representation as a crossed product, and using the corresponding factor set we shall prove that the exponent of this algebra in the class group divides $q - 1$ (see [**1**, Chapter V]). By a famous theorem [**1**, p. 149, Theorem 32] the exponent of our algebra is its index, which will complete the proof.

Let $F = Q(\xi)$ be the field of characters of ξ, and let

$$\Gamma = \sum_{G \in \mathfrak{F}} F\mathbf{U}(G)$$

be the algebra of F linear combinations of the linear transformations $\mathbf{U}(G)$ for $G \in \mathfrak{F}$. If n is the degree of $\mathbf{U}$ and C is the complex field, we know from Burnside's Theorem [**3**, theorem (27.4)] that ΓC, the complex linear combinations of the $\mathbf{U}(G)$, $G \in \mathfrak{F}$, is the full algebra of linear transformations on the

underlying n-dimensional vector space. Since this is a simple algebra, it is not difficult to show that Γ is also simple. Therefore Γ is isomorphic to the $k \times k$ matrix algebra over a division algebra Δ, for some integer k. In [3, pp. 468, 469], the following results are proved. The field F is the centre of Γ and therefore of Δ. The dimension of Δ over F is m^2, where $m = m(\xi)$, and $n = mk$. It follows that the dimension of Γ over F is n^2. The number m is the index of Γ.

Let h be the order of $\mathfrak{H}$. Since λ is a faithful linear character of $\mathfrak{H}$, $Q(\lambda)$ is just the field of hth roots of unity over Q. We know that the character $\xi|_{\mathfrak{H}}$ is the sum of conjugates of λ by the group $\mathfrak{G} = \mathrm{Gal}(Q(\lambda)/Q(\xi))$. Thus a basis of the space may be found for which the corresponding matrices $\mathbf{U}(H)$, $H \in \mathfrak{H}$, are diagonal, with the elements $\lambda^\sigma(H)$, $\sigma \in \mathfrak{G}$, as the diagonal entries. But this representation is similar to the regular representation of the field $Q(\lambda)$ over $Q(\xi)$. Recall that $Q(\xi)$, which we call F, is the field fixed by $\mathfrak{G}$.

The argument just given shows that the algebra

$$K = \sum_{H \in \mathfrak{H}} F\mathbf{U}(H)$$

generated by the elements $\mathbf{U}(H)$ over F is a field isomorphic to $Q(\lambda)$. With this isomorphism we shall identify the group $\mathfrak{G}$ with $\mathrm{Gal}(K/F)$. For each $\sigma \in \mathfrak{G}$, let G_σ be chosen as a representative of the coset of $\mathfrak{F}/\mathfrak{H}$ corresponding to σ. Conjugation of K by the element $\mathbf{U}(G_\sigma)$, which we shall call U_σ, is easily seen to induce the automorphism on K corresponding to σ. Our hypotheses clearly imply that $\mathfrak{H}$ contains $\mathfrak{A}$, and therefore $\mathfrak{H} = \mathfrak{A}\mathfrak{Z}$, where $\mathfrak{Z}$ is a cyclic p-group. Then since $\mathfrak{F} = \mathfrak{A}\mathfrak{B}$ and $\mathfrak{H} = \mathfrak{A}\mathfrak{Z}$, the G_σ can be chosen as coset representatives of $\mathfrak{B}/\mathfrak{Z}$. Therefore, for all $\sigma, \tau \in \mathfrak{G}$, the elements $G_\sigma G_\tau G_{\sigma\tau}^{-1}$ will lie in $\mathfrak{Z}$. Let $\gamma_{\sigma,\tau}$ be the image of this element under $\mathbf{U}$, and let ζ be the image of a generator of $\mathfrak{Z}$. Then the $\gamma_{\sigma,\tau}$ are all powers of ζ and we have, for all $\sigma, \tau \in \mathfrak{G}$,

$$U_\sigma U_\tau = U_{\sigma\tau}\gamma_{\sigma,\tau}.$$

Thus we have a particular expression of the algebra Γ as a crossed product of the field K by the group $\mathfrak{G} = \mathrm{Gal}(K/F)$. The elements $\{\gamma_{\sigma,\tau}\}$ of K form the factor set for the representatives $\{U_\sigma\}$ of $\mathfrak{G}$. For a positive integer d, let Γ^d denote of d-fold tensor product of Γ. Then the algebra Γ^d is similar to a crossed product of K by $\mathfrak{G}$ with representatives $\{V_\sigma\}$ of $\mathfrak{G}$ for which the elements $\{\gamma_{\sigma,\tau}^d\}$ form a factor set. (See [1, p. 71, Theorem 6].) This algebra has K as a maximal subfield, and for all $\sigma, \tau \in \mathfrak{G}$, $\rho \in K$, we have

$$V_\sigma V_\tau = V_{\sigma\tau}\gamma_{\sigma,\tau}^d, \qquad V_\sigma^{-1}\rho V_\sigma = \rho^\sigma.$$

If the representatives V_σ are replaced with multiples $V_\sigma' = V_\sigma\rho_\sigma$ by elements ρ_σ of K, the $\{V_\sigma'\}$ are a new set of representatives of $\mathfrak{G}$ and a new factor set is obtained from them. If this new factor set is trivial, with all members equal to 1, then the algebra Γ^d must be trivial in the class group. Thus the exponent of Γ, and therefore its index, will divide d.

Let $\mathfrak{C}$ be the centralizer of $\mathfrak{A}$ in $\mathfrak{F}$. Then $\mathfrak{C}$ contains $\mathfrak{H}$, and $\mathfrak{F}/\mathfrak{C}$ acts faithfully as a p-group of automorphisms on $\mathfrak{A}$. We shall apply the remarks of the last paragraph with d as the exponent of $\mathfrak{F}/\mathfrak{C}$.

Let $\{q_i\}$ be the prime divisors of the order of $\mathfrak{A}$. The automorphism group Aut $\mathfrak{A}$ of $\mathfrak{A}$ is the direct product of the groups Aut $\mathfrak{A}_i$, where $\mathfrak{A}_i$ is the q_i-Sylow subgroup of $\mathfrak{A}$. Since $\mathfrak{A}$ is a p'-group, each q_i is different from p. Thus, since $\mathfrak{A}_i$ is cyclic, the p-Sylow subgroup of Aut $\mathfrak{A}_i$ is cyclic with order equal to the p-part of $q_i - 1$. Choose the q_i for which $q_i - 1$ has maximal p-part and call it q. Then d, the exponent of $\mathfrak{F}/\mathfrak{C}$, divides $q - 1$.

Thus our proof will be complete if we show that Γ^d is trivial in the class group. This will be accomplished by producing a particular set of new representatives $\{V_\sigma'\}$ which have trivial factor set.

Let $\mathscr{G}_1$ be the subgroup of $\mathscr{G}$ fixing $F(\zeta)$, where ζ is the image in K of a generator of $\mathfrak{Z}$. The corresponding subgroup of $\mathfrak{F}/\mathfrak{H}$ is $\mathfrak{K}/\mathfrak{H}$, where $\mathfrak{K}$ is the centralizer of $\mathfrak{Z}$. Since $\mathfrak{H}$ is self-centralizing, $\mathfrak{H} = \mathfrak{K} \cap \mathfrak{C}$. Thus for $\tau \in \mathscr{G}_1$, the corresponding G_τ lies in $\mathfrak{K}$. The order t of τ in $\mathscr{G}$ is the smallest power of G_τ which lies in $\mathfrak{H}$. The remarks above show that this is also the smallest power of G_τ to lie in $\mathfrak{C}$. Thus t divides d, the exponent of $\mathfrak{F}/\mathfrak{C}$.

Let $\tau \in \mathscr{G}_1$, $\sigma \in \mathscr{G}$. Recall that with $\mathbf{U}(G_\tau) = U_\tau$, $\mathbf{U}(G_\sigma) = U_\sigma$, we have

$$U_\sigma U_\tau = U_{\sigma\tau}\gamma_{\sigma,\tau}, \qquad U_\tau U_\sigma = U_{\tau\sigma}\gamma_{\tau,\sigma}.$$

Inverting the first equation and multiplying, we obtain

$$U_\tau^{-1}U_\sigma^{-1}U_\tau U_\sigma = \gamma_{\sigma,\tau}^{-1}U_{\sigma\tau}^{-1}U_{\tau\sigma}\gamma_{\tau,\sigma}.$$

Since $\sigma\tau = \tau\sigma$, the right-hand side becomes $\gamma_{\sigma,\tau}^{-1}\gamma_{\tau,\sigma}$, which we will call $\zeta_{\sigma,\tau}$. Thus $U_\tau^{-1}U_\sigma^{-1}U_\tau U_\sigma = \zeta_{\sigma,\tau}$. Since $V_\sigma V_\tau = V_{\sigma\tau}\gamma_{\sigma,\tau}^{\,d}$ for all $\sigma, \tau \in G$, a similar argument will show that

$$V_\tau^{-1}V_\sigma^{-1}V_\tau V_\sigma = \zeta_{\sigma,\tau}^{\,d}. \tag{1}$$

Rewriting the equation for the Us yields

$$U_\sigma^{-1}U_\tau U_\sigma = U_\tau\zeta_{\sigma,\tau}.$$

Since the order of τ is t, there is a power ζ_τ of ζ for which $U_\tau^{\,t} = \zeta_\tau$. Since τ belongs to $\mathscr{G}_1$, U_τ centralizes ζ. Taking powers, we obtain:

$$U_\sigma^{-1}U_\tau^{\,t}U_\sigma = (U_\tau\zeta_{\sigma,\tau})^t = U_\tau^{\,t}\zeta_{\sigma,\tau}^{\,t},$$

which yields

$$\zeta_\tau^{\,\sigma} = \zeta_\tau\zeta_{\sigma,\tau}^{\,t}. \tag{2}$$

If σ also belongs to $\mathscr{G}_1$, then $\zeta_\tau^{\,\sigma} = \zeta_\tau$ and $\zeta_{\sigma,\tau}^{\,t} = 1$. Since t divides d, equation (1) shows that, for all $\sigma, \tau \in \mathscr{G}_1$, V_σ and V_τ commute.

We could have chosen $U_1 = 1$ when we began and it is not difficult to show now that V_1 may be chosen equal to 1. Let $\sigma \in \mathscr{G}$ have order s. Then for some power ζ_σ of ζ, $U_\sigma^{\,s} = \zeta_\sigma$. Using an induction argument, one shows that

$$U_\sigma^{\,s} = U_{\sigma^s}\cdot\gamma_{\sigma,\sigma^{s-1}}\cdot\gamma_{\sigma,\sigma^{s-2}}\cdot\ldots\cdot\gamma_{\sigma,\sigma}.$$

https://doi.org/10.4153/CJM-1970-069-3 Published online by Cambridge University Press

A similar argument shows that

$$V_\sigma{}^s = V_{\sigma^s}(\gamma_{\sigma,\sigma^{s-1}})^d(\gamma_{\sigma,\sigma^{s-2}})^d \cdots (\gamma_{\sigma,\sigma})^d.$$

Since $U_\sigma{}^s = \zeta_\sigma$, and since $U_{\sigma^s} = V_{\sigma^s} = 1$, we have

$$V_\sigma{}^s = \zeta_\sigma{}^d. \tag{3}$$

Let us make the following notational convention. We have used exponential notation for automorphisms, and since automorphisms obey all the rules of exponentiation, there will be no confusion if we use such expressions as $\zeta^{\sigma-1}$ for $\zeta^\sigma\zeta^{-1}$, $\zeta^{w\alpha}$ for $(\zeta^w)^\alpha$ or $\zeta^{\sigma+\tau}$ for $\zeta^\sigma\zeta^\tau$. Thus we shall use as exponents any member of the integral group ring of the automorphism group.

Our element $\tau \in \mathcal{G}_1$ has order $t = p^c$ for some integer c, and $d = p^e$ for some integer $e \geqq c$. Equation (2) becomes

$$1 = \zeta_\tau{}^{1-\sigma}(\zeta_{\sigma,\tau})^{p^c}. \tag{2'}$$

Equation (1) becomes

$$V_\tau{}^{-1}V_\sigma{}^{-1}V_\tau V_\sigma = (\zeta_{\sigma,\tau})^{p^e} \tag{1'}$$

and equation (3), with τ in place of σ, becomes

$$V_\tau{}^{p^c} = \zeta_\tau{}^{p^e}. \tag{3'}$$

Define

$$V_\tau' = V_\tau\zeta_\tau{}^{-p^{e-c}}. \tag{4}$$

Then substitute into the commutator formula for V_τ' and V_σ. Recall that V_τ commutes with any power of ζ and that $V_\sigma{}^{-1}\zeta = \zeta^\sigma V_\sigma{}^{-1}$. We obtain

$$\begin{aligned}(V_\tau')^{-1}V_\sigma{}^{-1}V_\tau' V_\sigma &= V_\tau{}^{-1}\zeta_\tau{}^{p^{e-c}}V_\sigma{}^{-1}V_\tau\zeta_\tau{}^{-p^{e-c}}V_\sigma \\ &= \zeta_\tau{}^{p^{e-c}}(\zeta_\tau{}^{-p^{e-c}})^\sigma V_\tau{}^{-1}V_\sigma{}^{-1}V_\tau V_\sigma \\ &= \zeta_\tau{}^{p^{e-c}(1-\sigma)}(\zeta_{\sigma,\tau})^{p^e}\end{aligned}$$

which equals 1 as can be seen by raising equation (2') to the power p^{e-c}. Therefore the V_τ', $\tau \in \mathcal{G}_1$, commute with all V_σ, $\sigma \in \mathcal{G}$. In addition,

$$(V_\tau')^{p^c} = (V_\tau\zeta_\tau{}^{-p^{e-c}})^{p^c} = V_\tau{}^{p^c}\zeta_\tau{}^{-p^e},$$

which equals 1 by equation (3'). Since the $\{V_\tau\}$ commute with each other for all $\tau \in \mathcal{G}_1$, the $\{V_\tau'\}$ will also commute with each other.

We now turn our attention to V_σ for $\sigma \notin \mathcal{G}_1$. At this point, the proof must be divided into two parts in order to treat the cases where p is odd and $p = 2$ separately. We shall first consider the case p odd and begin with some necessary results in the form of a lemma. Suppose that $\mathfrak{Z}$ has order p^r. Essentially, the lemma investigates how the p-group $\mathfrak{F}/\mathfrak{H}$ can act on $\mathfrak{Z}$. This lemma is related to work in [**5**].

https://doi.org/10.4153/CJM-1970-069-3 Published online by Cambridge University Press

LEMMA 2. *Let p be an odd prime, r a positive integer, and let ζ be a primitive p^rth root of unity. Let $[\zeta]$ be the cyclic subgroup generated by ζ. Then the p-Sylow subgroup of the automorphism group of $[\zeta]$ is cyclic of order p^{r-1}. For each positive integer $a \leqq r-1$, any automorphism α of order p^a leaves fixed exactly those powers of ζ which are powers of ζ^{p^a}. We also have the identity*

$$\zeta^{1+\alpha+\ldots+\alpha^{p^a-1}} = \zeta\,\zeta^{\alpha}\ldots\zeta^{\alpha^{p^a-1}} = \zeta^{p^a}.$$

Proof. The automorphism group of $[\zeta]$ is isomorphic to $\mathrm{Gal}(Q(\zeta)/Q)$. The order of this group is the dimension $(Q(\zeta):Q)$ which is, using the Euler Φ-function, $p^{r-1}(p-1)$. The dimension $(Q(\zeta^{p^{r-1}}):Q)$ is $p-1$. Therefore $\mathrm{Gal}(Q(\zeta)/Q(\zeta^{p^{r-1}}))$ has order p^{r-1} and is the p-Sylow subgroup of $\mathrm{Gal}(Q(\zeta)/Q)$. The automorphism defined by $\zeta \to \zeta^{1+p}$ fixes only the field $Q(\zeta^{p^{r-1}})$, and so the group $\mathrm{Gal}(Q(\zeta)/Q(\zeta^{p^{r-1}}))$ is cyclic.

For a positive integer $a \leqq r-1$, the subfield $Q(\zeta^{p^a})$ has index p^a in $Q(\zeta)$. Any automorphism α of order p^a generates the unique subgroup of $\mathrm{Gal}(Q(\zeta)/Q)$ of order p^a, and so by the Galois correspondence, α must generate the group $\mathrm{Gal}(Q(\zeta)/Q(\zeta^{p^a}))$. For an indeterminate x, the polynomial $x^{p^a} - \zeta^{p^a}$ is satisfied by ζ and has coefficients in the field $Q(\zeta^{p^a})$. Since the dimension $(Q(\zeta):Q(\zeta^{p^a}))$ is also the degree of this polynomial, it must be the minimum polynomial of ζ over the field $Q(\zeta^{p^a})$. Since α generates $\mathrm{Gal}(Q(\zeta)/Q(\zeta^{p^a}))$, this polynomial must equal the product $\Pi(x - \zeta^{\alpha^i})$ over all powers $i = 0, \ldots, p^a - 1$. Comparing the constant term in the two expressions for the polynomial, we obtain

$$-\zeta^{p^a} = \Pi(-\zeta^{\alpha^i}),$$

the product taken over $i = 0, \ldots, p^a - 1$. Since p is odd, the minus signs can all be removed, and this proves the lemma.

We chose $\mathscr{G}_1$ as the subgroup of $\mathscr{G}$ fixing $F(\zeta)$; hence $\mathscr{G}/\mathscr{G}_1$ is isomorphic to $\mathrm{Gal}(F(\zeta)/F) \simeq \mathrm{Gal}(Q(\zeta)/Q(\zeta) \cap F)$. Since $\mathscr{G}$ is a p-group, we see from Lemma 2 that $\mathscr{G}/\mathscr{G}_1$ is cyclic of order p^a for some integer $a \leqq r-1$. Let α be a generator of $\mathscr{G}$ modulo $\mathscr{G}_1$.

Let p^b be the order of α in $\mathscr{G}$. Then $b \geqq a$. Equation (3′) with α in place of σ becomes

$$V_\alpha{}^{p^b} = \zeta_\alpha{}^{p^e}. \tag{3''}$$

If $e \geqq b$, define

$$V_\alpha{}' = V_\alpha \zeta_\alpha{}^{-p^{e-b}}. \tag{5}$$

Using the identity in Lemma 2, we shall show that $(V_\alpha{}')^{p^b} = 1$.

$$\begin{aligned}(V_\alpha{}')^{p^b} = (V_\alpha\zeta_\alpha{}^{-p^{e-b}})^{p^b} &= V_\alpha{}^{p^b}\zeta_\alpha{}^{-p^{e-b}(1+\alpha+\ldots+\alpha^{p^b-1})} \\ &= V_\alpha{}^{p^b}\zeta_\alpha{}^{-p^{e-b}(1+\alpha+\ldots+\alpha^{p^a-1})p^{b-a}} \\ &= V_\alpha{}^{p^b}\zeta_\alpha{}^{-p^{e-b}p^ap^{b-a}} \\ &= V_\alpha{}^{p^b}\zeta_\alpha{}^{-p^e},\end{aligned}$$

which equals 1 by (3″).

Suppose that $e < b$. Recall our correspondence between $G_\alpha\mathfrak{H}$ in $\mathfrak{G}/\mathfrak{H}$ and $\alpha \in \mathscr{G}$. Since p^e is the exponent of $\mathfrak{F}/\mathfrak{C}$ and $\mathfrak{C}$ is the centralizer of $\mathfrak{A}$, $e < b$ simply means that $G_\alpha{}^{p^b}$ is not the smallest power of G_α to centralize $\mathfrak{A}$. Since $\alpha \in \mathscr{G}$ has order p^b, $G_\alpha{}^{p^b}$ is the smallest power of G_α to lie in $\mathfrak{H}$. Therefore since $\mathfrak{H} = \mathfrak{A}\mathfrak{Z}$ is self-centralizing, $G_\alpha{}^{p^b}$ must be the smallest power of G_α to centralize $\mathfrak{Z}$. This means that $\alpha \in \mathscr{G}$ acts faithfully on $[\zeta]$. Since $\mathscr{G}_1$ is the subgroup of $\mathscr{G}$ fixing $F(\zeta)$ and α^{p^a} is the smallest power of α contained in $\mathscr{G}_1$, we must have $a = b$. Since $\zeta_\alpha{}^{p^e} = V_\alpha{}^{p^b}$ must be centralized by V_α, Lemma 2 shows that it must be a power of ζ^{p^a}. Let us say that $V_\alpha{}^{p^b} = \zeta^{wp^a}$. Define

$$V_\alpha' = V_\alpha\zeta^{-w}. \tag{6}$$

Then

$$(V_\alpha')^{p^a} = (V_\alpha\zeta^{-w})^{p^a} = V_\alpha{}^{p^a}\zeta^{-w(1+\alpha+\alpha^2+\cdots+\alpha^{p^a-1})} = V_\alpha{}^{p^a}\zeta^{-wp^a} = 1.$$

Since $a = b$, we have shown that $(V_\alpha')^{p^b} = 1$.

We know that V_α commutes with all V_τ' for $\tau \in \mathscr{G}_1$, and it follows easily that V_α' also commutes with the V_τ'. We have proved that V_τ' has order at most the order of τ and since $(V_\tau')^{-1}\gamma V_\tau' = \gamma^\tau$ for all $\gamma \in K$, V_τ' must have the same order as τ. Similarly, V_α' has the same order as α.

The set $\{\alpha, \mathscr{G}_1\}$ generates $\mathscr{G}$, and thus by the Burnside Basis Theorem, this set contains a basis of $\mathscr{G}$. Suppose that $\{\alpha, \tau_1, \ldots, \tau_x\}$ is such a basis. The element α actually appears in the basis unless $\mathscr{G} = \mathscr{G}_1$. Since each $\sigma \in \mathscr{G}$ has a unique expression as a product of members of $\{\alpha, \tau_1, \ldots, \tau_x\}$, we define V_σ'' to be the corresponding product of the $\{V_\alpha', V_{\tau_1}', \ldots, V_{\tau_x}'\}$. It follows that the set $\{V_\sigma''\}$ is actually a group isomorphic to $\mathscr{G}$. Thus we have expressed the algebra as a crossed product by the $\{V_\sigma''\}$ with trivial factor set, and Theorem 1 is proved for odd primes p.

To complete the proof for $p = 2$, we begin with a lemma, analogous to Lemma 2, concerning the automorphism group of a cyclic 2-group.

LEMMA 3. *Let ζ be a primitive 2^rth root of unity, $r \geqq 3$, and $[\zeta]$ the cyclic group generated by ζ. Let* $\mathrm{Aut}_0[\zeta]$ *be the subgroup of* $\mathrm{Aut}[\zeta]$, *the automorphism group of $[\zeta]$, consisting of those automorphisms which fix $\zeta^{2^{r-2}} = (-1)^{1/2}$. Let β be the conjugation automorphism defined by $\zeta^\beta = \zeta^{-1}$. Then* $\mathrm{Aut}_0[\zeta]$ *is a cyclic group of order 2^{r-2} and* $\mathrm{Aut}[\zeta]$ *is the direct product of* $\mathrm{Aut}_0[\zeta]$ *with the group of order 2 generated by β. If $\alpha \in \mathrm{Aut}_0[\zeta]$ has order 2^a, $a \leqq r-2$, then the subgroup of $[\zeta]$ fixed by α is exactly $[\zeta^{2^a}]$. We also have the following identities*

$$\zeta^{1+\alpha+\cdots+\alpha^{2^a-1}} = -\zeta^{2^a} = \zeta^{2^a y}, \qquad y \text{ an odd integer},$$

and

$$\zeta^{1+\alpha\beta+\cdots+(\alpha\beta)^{2^a-1}} = \zeta^{2^{r-1}} = -1.$$

Proof. We will use the isomorphism between $\mathrm{Aut}[\zeta]$ and $\mathrm{Gal}(Q(\zeta)/Q)$ under which $\mathrm{Aut}_0[\zeta]$ corresponds to $\mathrm{Gal}(Q(\zeta)/Q(\zeta^{r-2}))$. The dimension $(Q(\zeta):Q(\zeta^{2^{r-2}}))$, and hence the order of $\mathrm{Aut}_0[\zeta]$, is 2^{r-2}. Since the automorphism α_0 defined by $\zeta^{\alpha_0} = \zeta^{1+2^2}$ fixes only the powers of $\zeta^{2^{r-2}}$, α_0 is a generator

of $\mathrm{Aut}_0[\zeta]$. Conjugation does not fix $\zeta^{2^{r-2}} = (-1)^{1/2}$, and so, since $\mathrm{Aut}[\zeta]$ has order 2^{r-1}, α_0 and β are generators for $\mathrm{Aut}[\zeta]$.

To prove the first identity, we proceed exactly as in the proof of Lemma 2, except in the last step, where a negative sign occurs since p is even. This yields $\zeta^{1+\alpha+\cdots+\alpha^{2^a-1}} = -\zeta^{2^a}$. Now since ζ^{2^a} is a root of unity of order at least 4, $-\zeta^{2^a}$ has the same order as ζ^{2^a}. Thus $-\zeta^{2^a}$ is a power $\zeta^{2^a y}$ for some odd integer y. This proves the first identity. To prove the second identity, we use the fact that $\beta^2 = 1$, and collect alternate terms.

$$\begin{aligned}\zeta^{1+\alpha\beta+(\alpha\beta)^2+\cdots+(\alpha\beta)^{(2^a-1)}} &= \zeta^{1+\alpha^2+\cdots+\alpha^{(2^a-2)}} \cdot \zeta^{\alpha\beta(1+\alpha^2+\cdots+\alpha^{(2^a-2)})} \\ &= \zeta^{1+(\alpha^2)+\cdots+(\alpha^2)^{(2^{a-1}-1)}} \cdot \zeta^{\alpha\beta(1+(\alpha^2)+\cdots+(\alpha^2)^{(2^{a-1}-1)})} \\ &= \zeta^{2^{a-1}}\zeta^{\alpha\beta(2^{a-1})},\end{aligned}$$

where the last equality comes from applying the first identity for α^2, which has order 2^{a-1}. The automorphism $\alpha\beta$ does not fix $\zeta^{2^{r-2}} = (-1)^{1/2}$. Our expression $\zeta^{1+\alpha\beta+\cdots+(\alpha\beta)^{(2^a-1)}}$ is obviously left fixed by $\alpha\beta$, and hence it must equal either $\zeta^{2^{r-1}} = -1$ or $\zeta^{2^r} = 1$. Suppose that we had the latter case. Then from the computation above, since $\zeta^\beta = \zeta^{-1}$, we have $\zeta^{2^{a-1}} = \zeta^{\alpha(2^{a-1})}$. But we know that α fixes only powers of ζ^{2^a}; hence this cannot happen. Thus the second identity is proved.

We now return to the proof of Theorem 1 for $p = 2$. We chose $\mathcal{G}_1$ as the subgroup of $\mathcal{G}$ fixing $F(\zeta)$, and so $\mathcal{G}/\mathcal{G}_1$ corresponds to a subgroup of $\mathrm{Aut}[\zeta]$.

Suppose first that $\mathcal{G}/\mathcal{G}_1$ corresponds to a subgroup of $\mathrm{Aut}_0[\zeta]$. Then $\mathcal{G}/\mathcal{G}_1$ is cyclic of order 2^a, $a \leqq r-2$. The proof in this case is almost identical with the proof given for odd p. The only difference comes from the integer y appearing in Lemma 3, for which we make a slight adjustment. Since y is odd, we may choose an integer y' such that $yy' \equiv 1 \pmod{2^r}$.

Let 2^b be the order of α in $\mathcal{G}$. Proceeding as we did for odd p in formulas (5) and (6), we define V_α' for the two cases

$$(5') \qquad V_\alpha' = V_\alpha \zeta_\alpha^{-2^{e-b}y'} \quad \text{if } e \geqq b,$$

$$(6') \qquad V_\alpha' = V_\alpha \zeta_\alpha^{-wy'} \quad \text{if } e < b.$$

Then following the earlier proof, one can show that $(V_\alpha')^{2^b} = 1$.

Now suppose that, in addition to α, $\mathcal{G}$ contains an automorphism β corresponding to conjugation. We first define V_α' exactly as it was defined in the case just discussed in formulas (5′) and (6′). Then we need to define V_β' in such a way that V_β' commutes with V_α'.

Suppose first that $e \geqq b$. Raise the equation $U_\beta^{-1}U_\alpha U_\beta = U_\alpha \zeta_{\beta,\alpha}$ to the power 2^b and use the first identity of Lemma 3 to obtain

$$\begin{aligned}(U_\alpha^{2^b})^{U_\beta} = (U_\alpha\zeta_{\beta,\alpha})^{2^b} &= U_\alpha^{2^b}\zeta_{\beta,\alpha}^{(1+\alpha+\cdots+\alpha^{(2^b-1)})} \\ &= U_\alpha^{2^b}\zeta_{\beta,\alpha}^{(1+\alpha+\cdots+\alpha^{(2^{a-1})2^{b-a}})} = U_\alpha^{2^b}(\zeta_{\beta,\alpha})^{2^a y(2^{b-a})}.\end{aligned}$$

Since $U_\alpha^{2^b} = \zeta_\alpha$ this becomes

$$(2'') \qquad 1 = (\zeta_\alpha)^{(1-\beta)}(\zeta_{\beta,\alpha})^{2^b y}.$$

We now define $V_\beta' = V_\beta$ and we will use identity (2'') to prove that V_α' and V_β' commute. This proof is very similar to the proof that V_τ' and V_σ commute given just after definition (4). The commutator formula for V_α' and V_β is

$$V_\alpha^{-1} V_\beta^{-1} V_\alpha V_\beta = (\zeta_{\beta,\alpha})^{2^e}.$$

Into this we substitute equation (5') and we obtain

$$(V_\alpha')^{-1} V_\beta^{-1} (V_\alpha') V_\beta = (\zeta_\alpha)^{2^{e-b} y' (1-\beta)} (\zeta_{\beta,\alpha})^{2^e}$$

which equals 1, as can be seen by raising equation (2'') to the power $2^{e-b}y'$

For the case $e < b$, let the commutator of V_α' and V_β equal ζ_1. Then

$$V_\beta^{-1} V_\alpha' V_\beta = V_\alpha' \zeta_1.$$

Then raise this to the power 2^b and use the first identity of Lemma 3 as we did above to see that

$$V_\beta^{-1} (V_\alpha')^{2^b} V_\beta = (V_\alpha')^{2^b} \zeta_1^{2^b y}$$

However, since $(V_\alpha')^{2^b} = 1$, this shows that $\zeta_1^{2^b y} = 1$. Assuming that $e < b$, we showed just before definition (6) that $a = b$. Thus, since y is odd, we have now shown that $\zeta_1^{2^a} = 1$. Since ζ has order 2^r, ζ_1 must be a power of $\zeta^{2^{r-a}}$, say

$$\zeta_1 = \zeta^{2^{r-a} z}. \tag{7}$$

Define $V_\beta' = V_\beta \zeta^z$ and compute the commutator

$$\begin{aligned}(V_\alpha')^{-1} (V_\beta')^{-1} V_\alpha' V_\beta' &= (V_\alpha')^{-1} V_\beta^{-1} V_\alpha' V_\beta \zeta^{-z(\alpha-1)} \\ &= \zeta_1 \zeta^{-z(\alpha-1)}.\end{aligned}$$

This equals 1 from equation (7), provided we can choose α in such a way that

$$\zeta^{\alpha-1} = \zeta^{2^{r-a}} \quad \text{or} \quad \zeta^\alpha = \zeta^{1+2^{r-a}}. \tag{8}$$

But the automorphism α defined by this equation clearly fixes only the powers of ζ^{2^a} and must have order 2^a by Lemma 3. Thus we can assume that α satisfies this equation and we have proved that V_α' and V_β' commute.

We know that β has order 2 modulo $\mathscr{G}_1$. Suppose that β has order 2^f in $\mathscr{G}$. Now since ζ_β is fixed by β it must be either 1 or -1. By equation (3),

$$V_\beta^{2^f} = \zeta_\beta^{2^e}$$

and therefore $V_\beta^{2^f} = 1$ unless $e = 0$. Recall that p^e is the exponent of $\mathfrak{F}/\mathfrak{C}$, where $\mathfrak{C}$ is the centralizer of $\mathfrak{A}$. Thus $e = 0$ means that $\mathfrak{F} = \mathfrak{C}$ and $\mathfrak{F} = \mathfrak{AB}$ is a direct product.

The group corresponding to $\mathscr{G}_1$ in $\mathfrak{F}/\mathfrak{H}$ is $\mathfrak{K}/\mathfrak{H}$, where $\mathfrak{K}$ is the centralizer of $\mathfrak{Z}$ and satisfies $\mathfrak{K} \cap \mathfrak{C} = \mathfrak{H}$. Since $\mathfrak{C} = \mathfrak{F}$, we must have $\mathfrak{K} = \mathfrak{H}$ or $\mathscr{G}_1 = 1$. Therefore β has order 2 in $\mathscr{G}$ and $f = 1$. Let Z be a generator of $\mathfrak{Z}$ corre-

https://doi.org/10.4153/CJM-1970-069-3 Published online by Cambridge University Press

sponding to ζ under the representation $\mathbf{U}$. Then we have shown that $\mathfrak{B}$ has generators A, B, and Z satisfying the following relations:

$$Z^{2^r} = E, \qquad AB = BA, \qquad Z^A = Z^{1+2^{r-a}}, \qquad Z^B = Z^{-1},$$
$$A^{2^a} = E, \qquad B^2 = Z^{2^{r-1}} \text{ or } E.$$

It is in this case, with $e = 0$ and $d = 1$ that the exception can occur, for Γ need not have exponent 1. If $B^2 = E$, then V_α' and V_β' have trivial factor set and Γ has exponent 1. If $B^2 = Z^{2^{r-1}}$, then the exponent of Γ is 2, since for any choice of $\gamma_\beta \in K$, any new representative $V_\beta' = V_\beta\gamma_\beta$ would still satisfy

$$(V_\beta')^2 = V_\beta\gamma_\beta V_\beta\gamma_\beta = V_\beta^2\gamma_\beta^{-1}\gamma_\beta = \zeta^{2^{r-1}}$$

and we could never produce a set of representatives $\{V_\sigma''\}$ which has a trivial factor set. If $\mathfrak{A} = 1$, then the exceptional case occurs since there are no qs to choose. Although we assumed that $r \geqq 3$ in Lemma 3, the cases where $r < 3$ follow very easily from our considerations thus far.

The final possibility is that $\mathcal{G}/\mathcal{G}_1$ is cyclic but does not correspond either to conjugation or to a subgroup of $\mathrm{Aut}_0[\zeta]$. Then we can pick a generator σ of $\mathcal{G}$ modulo $\mathcal{G}_1$ corresponding to a product $\alpha\beta$ for some $\alpha \in \mathrm{Aut}_0[\zeta]$. Let σ have order 2^c in $\mathcal{G}$. Then $c \geqq a$, where α has order 2^a in $\mathrm{Aut}_0[\zeta]$. Now ζ_σ is left invariant by $\alpha\beta$, and so is either $+1$ or -1. If $\zeta_\sigma = 1$, then by equation (3) our proof is complete. Thus we may assume that $\zeta_\sigma = -1$. Let $V_\sigma' = V_\sigma\zeta$. Then we use the second identity of Lemma 3 to see that

$$(V_\sigma\zeta)^{2^c} = V_\sigma^{2^c}(-1) = 1.$$

The remainder of the proof of Theorem 1 proceeds exactly as in the case for odd p. First we expand generators of $\mathcal{G}$ modulo $\mathcal{G}_1$ to a basis for $\mathcal{G}$, using the Burnside Basis Theorem. Then we pick new representatives $\{V_\sigma''\}$ which have trivial factor set. This completes the proof of Theorem 1.

Another theorem of this general nature can be proved with the techniques presented here.

Suppose that $\mathcal{G}/\mathcal{G}_1$ has order p^a for an odd prime p. Recall that Z is the generator of $\mathfrak{Z}$ corresponding to ζ. A power of Z is central in $\mathfrak{A}$ if and only if the corresponding power of ζ is fixed by a generator α of $\mathcal{G}$ modulo $\mathcal{G}_1$. Therefore by the third sentence in Lemma 2, $[Z^{p^a}]$ is the largest subgroup of $\mathfrak{Z}$ central in $\mathfrak{F}$. In fact, since $\mathfrak{H}$ is self-centralizing, $[Z^{p^a}]$ is the p-Sylow subgroup of the centre of $\mathfrak{F}$. We may state our second theorem as follows.

THEOREM 2. *Let $\mathfrak{F} = \mathfrak{A}\mathfrak{B}$ be an elementary group at the odd prime p. Let λ be a faithful linear character of a cyclic, normal, self-centralizing subgroup $\mathfrak{H}$. Let ξ be the (irreducible) character of $\mathfrak{F}$ induced by λ and let $m(\xi)$ be the Schur index of ξ over the rational field. Then $m(\xi)$ divides the order of the centre of $\mathfrak{F}$.*

Proof. We use the notation and the method of proof of the last theorem, except this time d is the order of the p-Sylow subgroup of the centre of $\mathfrak{F}$.

For σ and τ in $\mathscr{G}_1$, the commutator

$$U_\sigma^{-1}U_\tau^{-1}U_\sigma U_\tau = \zeta_{\tau,\sigma}$$

is left invariant under conjugation by U_μ for any μ in $\mathscr{G}$. Therefore $\zeta_{\tau,\sigma}$ is central in $\mathbf{U}(\mathfrak{F})$ and $\zeta_{\tau,\sigma}^{\,d} = 1$. In view of equation (1), V_σ and V_τ commute.

Suppose that $\mathscr{G}/\mathscr{G}_1$ has order p^a. We may argue as we did earlier for $p = 2$ that a generator α for $\mathscr{G}$ modulo $\mathscr{G}_1$ may be chosen in such a way that

$$(8') \qquad \zeta^{\alpha-1} = \zeta^{p^{r-a}} \quad \text{or} \quad \zeta^{\alpha} = \zeta^{1+p^{r-a}},$$

for since the automorphism α defined by this equation fixes only the powers of ζ^{p^a}, it must have order p^a by Lemma 2. For τ in $\mathscr{G}$ we define $V_\tau' = V_\tau\zeta_{\alpha,\tau}^{-1}$. We compute the commutator to obtain

$$(V_\tau')^{-1}V_\alpha^{-1}V_\tau'V_\alpha = \zeta_{\alpha,\tau}^{\,1-\alpha}\zeta_{\alpha,\tau}^{\,d}.$$

In view of the remarks preceding the theorem, d is the order of $[\zeta^{p^a}]$ which is $d = p^{r-a}$. This fact together with (8') show that the commutator that we just computed equals 1, and V_α commutes with all V_τ', $\tau \in \mathscr{G}_1$. Next we compute $(V_\tau')^t$, where t is the order of τ.

$$(V_\tau\zeta_{\alpha,\tau}^{-1})^t = V_\tau^{\,t}\zeta_{\alpha,\tau}^{-t} = \zeta_\tau^{\,d}\zeta_{\alpha,\tau}^{-t}.$$

The second equality follows from (3). But from (2) we know that $\zeta_\tau^{\alpha-1} = \zeta_{\alpha,\tau}^{\,t}$. Putting this together with the two facts used above yields $(V_\tau')^t = 1$. Only V_α remains. But obviously $\zeta_\alpha \in [\zeta^{p^a}]$ and so $V_\alpha^{p^b} = \zeta_\alpha^{\,d} = 1$. This proves Theorem 2. Notice that this theorem and its proof hold equally well if $p = 2$ and $\mathscr{G}/\mathscr{G}_1$ corresponds to a subgroup of $\mathrm{Aut}_0[\zeta]$.

The following corollary can be deduced from Theorem 2.

COROLLARY. *Let $\mathfrak{G}$ be a finite group. Let ψ be an irreducible character of $\mathfrak{G}$ with Schur index $m(\psi)$ over the rational field. If, for an odd prime p, p^e is the p-part of $m(\psi)$, then p^{e-1} divides the dimension $(Q(\psi):Q)$.*

Proof. For our proof we must use Brauer's theorem together with part of its proof [3, pp. 477–478]. Our field $Q(\psi)$ corresponds to the field K in [3]. We conclude that the existence of a field L containing $Q(\psi)$ and a character χ of an L-elementary subgroup $\mathfrak{AP}$ such that the dimension of L over $Q(\psi)$ is a p'-number and the p-part of $m(\psi)$ is $m_{Q(\psi)}(\chi)$. The Schur index with respect to Q is divisible by the Schur index with respect to an extension field. Therefore, letting $m(\chi) = p^f$, we have $f \geqq e$. Also a group which is elementary with respect to any extension field of Q must be elementary with respect to Q. Thus $\mathfrak{AP}$ is elementary in the sense of the present paper. We can now complete the proof by showing that p^{f-1} divides the dimension of $Q(\psi)$ over Q.

Choose ξ and $\mathfrak{F}$ as given in Lemma 1 to satisfy $Q(\xi) = Q(\chi)$ and $m(\xi) = m(\chi) = p^f$. We have just shown in Theorem 2 that there is a central element Z_0 of order p^f in $\mathfrak{F}$. The trace $\xi(Z_0)$ is an integral multiple of a primitive p^fth root of unity which means $Q(\xi)$ contains a primitive p^fth root of

unity. Therefore L contains a primitive p^fth root of unity and the dimension of L over Q must be divisible by $p^{f-1}(p-1)$. Since the dimension of L over $Q(\psi)$ is a p'-number, the dimension of $Q(\psi)$ over Q must be divisible by p^{f-1}.

In view of Theorem 1, it might be plausible to suppose that for some prime divisor q of the order of $\mathfrak{A}$ the representation $\mathbf{U}$ could be realized in the field $Q(\eta, \chi)$, where η is a primitive qth root of unity. We conclude this paper with an example to show that this is not the case.

Let $\mathfrak{G}$ be the group defined by the following relations:

$$A_1^7 = 1, \quad A_2^{13} = 1, \quad A_1A_2 = A_2A_1,$$
$$X_1^3 = Z, \quad X_2^3 = Z, \quad Z^9 = 1, \quad Z \text{ central in } \mathfrak{G}.$$
$$X_1^{-1}A_1X_1 = A_1^2, \quad X_2^{-1}A_2X_2 = A_2^3,$$
$$A_1X_2 = X_2A_1, \quad A_2X_1 = X_1A_2.$$

Let λ be a faithful linear character on $\mathfrak{A} = \{A_1, A_2, Z\}$. For $i = 1, 2$ define

$$\mathfrak{G}_i = \langle A_1, A_2, X_i, Z \rangle$$

and let χ_i be the character of $\mathfrak{G}_i$ induced by λ. Let χ be the character of $\mathfrak{G}$ induced by λ. Then one easily sees that

$$Q(\chi) \subset Q(\chi_i) \subset Q(\lambda), \quad Q(\chi) \neq Q(\chi_i) \neq Q(\lambda), \quad i = 1, 2,$$

where the relative dimension at each step is 3. Also, $Q(\chi_1) = Q(\chi, \eta_2)$ and $Q(\chi_2) = Q(\chi, \eta_1)$, where η_1 and η_2 are, respectively, primitive 7th and 13th roots of unity. Now it follows from the work of Amitsur [**2**, Theorem 5 (2a)] that $m(\chi_1) = m(\chi_2) = 3$. Suppose that the representation $\mathbf{T}$ affording χ could be realized in $Q(\chi_1)$. Since χ_1 appears once in $\chi|_{\mathfrak{G}_1}$, the second property of the Schur index shows that then the representation affording χ_1 could be realized in $Q(\chi_1)$. This is impossible since $m(\chi_1) = 3$. A similar argument works for χ_2.

This also shows that $m(\chi) \neq 1$. We will show that $m(\chi) = 3$. There are four fields lying strictly between $Q(\chi)$ and $Q(\lambda)$ and except for $Q(\chi_1)$ and $Q(\chi_2)$ we will show that $\mathbf{T}$ can be realized in each of the remaining two fields. Let $\mathfrak{F}_j = \langle A_1, A_2, X_1X_2^j, Z \rangle$ for $j = 1$ or 2 and let ξ_j be the character of $\mathfrak{F}_j$ induced by λ. The fields $Q(\xi_j)$, $j = 1$ or 2, are the remaining two fields and it follows from [**2**, Theorem 5] that $m(\xi_j) = 1$. Therefore the representation affording each ξ_j can be realized in $Q(\xi_j)$ and, since ξ_j induces χ, $\mathbf{T}$ can be realized in $Q(\xi_j)$, $j = 1$ or 2.

References

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., Vol. 24 (Amer. Math. Soc., (New York) Providence, R.I., 1939).
2. S. A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. *18* (1955), 361–386.
3. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (Interscience, New York, 1962).

4. W. Feit, *Characters of finite groups* (Benjamin, New York, 1967).
5. L. Solomon, *The representation of finite groups in algebraic number fields*, J. Math. Soc. Japan *13* (1961), 144–164.
6. E. Witt, *Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper*, J. Reine Angew. Math. *190* (1952), 231–245.

University of Toronto,
Toronto, Ontario;
Washington University,
St. Louis, Missouri