A NOTE ON A CONJECTURE OF BRAUER

PAUL FONG

To RICHARD BRAUER on the occasion of his 60th Birthday

§ 1. Introduction

In [1] R. Brauer asked the following question: Let $\mathfrak{G}$ be a finite group, p a rational prime number, and B a p-block of $\mathfrak{G}$ with defect d and defect group $\mathfrak{D}$. Is it true that $\mathfrak{D}$ is abelian if and only if every irreducible character in B has height 0? The present results on this problem are quite incomplete. If $d = 0, 1, 2$ the conjecture was proved by Brauer and Feit, [4] Theorem 2. They also showed that if $\mathfrak{D}$ is cyclic, then no characters of positive height appear in B. If $\mathfrak{D}$ is normal in $\mathfrak{G}$, the conjecture was proved by W. Reynolds and M. Suzuki, [12]. In this paper we shall show that for a solvable group $\mathfrak{G}$, the conjecture is true for the largest prime divisor p of the order of $\mathfrak{G}$. Actually, one half of this has already been proved in [7]. There it was shown that if $\mathfrak{G}$ is a p-solvable group, where p is any prime, and if $\mathfrak{D}$ is abelian, then the condition on the irreducible characters in B is satisfied.

The proof of the converse presented here is somewhat difficult. A series of reductions gives rise to the following situation: $\mathfrak{G}$ is a finite solvable group of order pg', where $(p, g') = 1$, such that $\mathfrak{G}$ has no proper normal subgroups of p'-index. Moreover $\mathfrak{G}$ acts faithfully and irreducibly on a vector space $\mathscr{V}$ over a finite field, such that each vector v in $\mathscr{V}$ is fixed by some Sylow p-subgroup of $\mathfrak{G}$. Using methods similar to those used by Huppert in [10], [11], we shall see that $g' = 1$ if p is the largest prime divisor of the order of $\mathfrak{G}$.

The author was a participant in the Special Year Program in the Theory of Groups at the University of Chicago 1960-1961. Many of the ideas in this paper had their origin in the discussions I had with my colleagues there. In particular, I should like to thank G. Higman and J. G. Thompson for their helpful advice.

Received November 12, 1961.
Revised June 6, 1962.

§ 2. Proofs of the Theorems

Notation will be explained when used; for the most part, it will be that of [7]. Let $\mathfrak{G}$ be a finite group of order $|\mathfrak{G}| = p^a g'$, where p is a fixed prime number, a is an integer ≥ 0, and $(p, g') = 1$. Since the only characters of $\mathfrak{G}$ which will concern us are those of complex-valued representations, the word "character" will refer only to such characters. The basic results of modular representation theory can be found in [3]. If B is a block of $\mathfrak{G}$ of defect d, and χ is an irreducible character in B, then the height of χ is the integer $e \geq 0$ such that p^{a-d+e} is the exact power of p dividing the degree of χ.

THEOREM 1. *Let $\mathfrak{G}$ be a finite solvable group, p the largest prime divisor of $|\mathfrak{G}|$. Let B be a p-block of $\mathfrak{G}$ with defect d and defect group $\mathfrak{P}$. If every character in B has height* 0, *then $\mathfrak{P}$ is abelian.*

Proof. The proof is by double induction on a and $g = |\mathfrak{G}|$. We assume that the theorem is true for all solvable groups of order divisible by at most p^{a-1} and for all solvable groups of order $p^a m$, where $(p, m) = 1$ and $p^a m < g$.

a) The reduction in [7] § 3 permits us to assume B has defect a. The defect group $\mathfrak{P}$ is hence a Sylow p-subgroup of $\mathfrak{G}$ and the condition on the heights means that the characters in B all have degree prime to p.

b) Let $\tilde{\mathfrak{G}}$ be a maximal normal subgroup of $\mathfrak{G}$. By [7] (3 J), (1 F), there is a block $\tilde{B}$ of $\tilde{\mathfrak{G}}$ such that $\mathfrak{P} \cap \tilde{\mathfrak{G}}$ is a defect group of $\tilde{B}$, and such that every character in $\tilde{B}$ has height 0. The induction hypothesis implies that $\mathfrak{P} \cap \tilde{\mathfrak{G}}$ is abelian. If $|\mathfrak{G} : \tilde{\mathfrak{G}}| \neq p$, then $\mathfrak{P} \cap \tilde{\mathfrak{G}} = \mathfrak{P}$ and we are done. We may therefore assume that $\mathfrak{G}$ has no nontrivial normal subgroups of p'-index (a number n is p' if $p \nmid n$).

c) Let $\mathfrak{H}$ be the maximal normal p'-subgroup of $\mathfrak{G}$; we may assume that $\mathfrak{H} > 1$; otherwise B contains all the irreducible characters of $\mathfrak{G}$ and the theorem follows from [7] (3 A), (3 D). By [7] (2 D) there is then a group $\mathfrak{M}$ and a block B' of $\mathfrak{M}$ such that (i) B and B' have isomorphic defect groups, (ii) there is a 1-1 height preserving correspondence between the characters of B and B', (iii) there is cyclic normal p'-subgroup $\mathfrak{E}$ in the center of $\mathfrak{M}$ such that $\mathfrak{M}/\mathfrak{E} \simeq \mathfrak{G}/\mathfrak{H}$, (iv) the characters of $\mathfrak{M}$ in B' are all the irreducible characters of $\mathfrak{M}$ which induce a given linear character of $\mathfrak{E}$.

The characters in B' all have height 0, and we therefore need prove

https://doi.org/10.1017/S0027763000010990 Published online by Cambridge University Press

Theorem 1 only for the group $\mathfrak{M}$. We note p^a is the exact power of p dividing $|\mathfrak{M}|$; moreover, p is the largest prime divisor of $|\mathfrak{M}|$ by the construction of $\mathfrak{M}$ in [7]. Let $\tilde{\mathfrak{M}}$ be a maximal normal subgroup of $\mathfrak{M}$ containing $\mathfrak{E}$; by b) and the isomorphism $\mathfrak{M}/\mathfrak{E} \simeq \mathfrak{G}/\mathfrak{H}$, $|\mathfrak{M} : \tilde{\mathfrak{M}}| = p$. Denote by $\mathfrak{P}$ a Sylow p-subgroup of $\mathfrak{M}$ (since the rest of the proof concerns $\mathfrak{M}$, this should cause no confusion). As in b) the subgroup $\mathfrak{D} = \mathfrak{P} \cap \tilde{\mathfrak{M}}$ is abelian. $\mathfrak{D}\mathfrak{E}/\mathfrak{E}$ is the maximal normal p-subgroup in $\mathfrak{M}/\mathfrak{E}$ by [9] Lemma 1.2.3, and since $\mathfrak{D}\mathfrak{E} = \mathfrak{D} \times \mathfrak{E}$, the characteristic subgroup $\mathfrak{D}$ of $\tilde{\mathfrak{M}}$ is therefore normal in $\mathfrak{M}$.

d) Suppose $\phi(\mathfrak{D}) \neq 1$, where $\phi(\mathfrak{D})$ is the Frattini subgroup of $\mathfrak{D}$. Since the p-blocks of $\mathfrak{M}/\phi(\mathfrak{D})$ may be regarded as subsets of the p-blocks of $\mathfrak{M}$ by means of the lifting mapping of characters [3] (9 B), it follows by induction that $\mathfrak{P}/\phi(\mathfrak{D})$ is abelian. But $\mathfrak{M}/\mathfrak{D}\mathfrak{E}$ acts faithfully on $\mathfrak{D}/\phi(\mathfrak{D})$ by [9] Lemma 1.2.5. This is impossible, and hence $\phi(\mathfrak{D}) = 1$. We may assume then $\mathfrak{D}$ is an elementary abelian p-group.

e) Let D be any element in $\mathfrak{D}$. The condition on the heights of the characters in B' implies that D is centralized by a Sylow p-subgroup of $\mathfrak{M}$ (see [7] (1 A), (3 D)). Suppose $\mathfrak{D}_1$ is a normal subgroup of $\mathfrak{M}$ (written $\mathfrak{D}_1 \trianglelefteq \mathfrak{M}$) such that $1 < \mathfrak{D}_1 < \mathfrak{D}$. By d) $\mathfrak{D} = \mathfrak{D}_1 \times \mathfrak{D}_2$, where $\mathfrak{D}_2$ is any complement to $\mathfrak{D}_1$ in $\mathfrak{D}$. However, $\mathfrak{D}_2$ can be selected so that $\mathfrak{D}_2 \trianglelefteq \mathfrak{M}$. For represent $\tilde{\mathfrak{M}}/\mathfrak{D}$ on $\mathfrak{D}$ by transformation. Since $\tilde{\mathfrak{M}}/\mathfrak{D}$ is a p'-group, this representation is completely reducible by Maschke's Theorem. Hence there exists a complement $\mathfrak{D}_2$ such that $\mathfrak{D}_2 \trianglelefteq \tilde{\mathfrak{M}}$. Let A be a fixed element of p-power order, A not in $\mathfrak{D}$. If D is any element in $\mathfrak{D}_2$ then $A^{-1}DA = X^{-1}DX$ for some X in $\tilde{\mathfrak{M}}$, and D^A is in $\mathfrak{D}_2$, that is, $\mathfrak{D}_2 \trianglelefteq \mathfrak{M}$. Induction applies to $\mathfrak{M}/\mathfrak{D}_1$ and to $\mathfrak{M}/\mathfrak{D}_2$; therefore $\mathfrak{M}/\mathfrak{D}_1$ and $\mathfrak{M}/\mathfrak{D}_2$ have abelian Sylow p-subgroups. Since $\mathfrak{M}$ can be embedded in $\mathfrak{M}/\mathfrak{D}_1 \times \mathfrak{M}/\mathfrak{D}_2$, $\mathfrak{P}$ is abelian. We may therefore assume $\mathfrak{D}$ is a minimal normal subgroup of $\mathfrak{M}$.

f) Let $\mathfrak{B}$ be the representation of $\mathfrak{M}$ in the vector space $\mathfrak{D}$ over $GF(p)$. The group $\mathfrak{M}/\mathfrak{D}\mathfrak{E}$ with the representation $\mathfrak{B}$ satisfies the hypothesis of the following theorem. Applying that theorem, we conclude that $\mathfrak{M}/\mathfrak{D}\mathfrak{E}$ is a p-group, and hence $\mathfrak{M} = \mathfrak{P} \times \mathfrak{E}$. From this it follows that $\mathfrak{P}$ must be abelian.

THEOREM 2. *Let $\mathfrak{G}$ be a finite solvable group of order pg', where $(p, g') = 1$. Let $\mathscr{V}$ be a vector space of dimension d over the finite field K on which $\mathfrak{G}$ acts irreducibly and faithfully. Suppose*

https://doi.org/10.1017/S0027763000010990 Published online by Cambridge University Press

(i) $\mathfrak{G}$ *has no proper normal subgroups of* p'*-index.*

(ii) *Each vector* v *in* $\mathscr{V}$ *is fixed by some Sylow* p*-subgroup of* $\mathfrak{G}$.

(iii) p *is the largest prime divisor of* $|\mathfrak{G}|$.

Then $g'=1$, *that is,* $\mathfrak{G}$ *is a group of order* p.

Proof. We proceed by double induction on g' and d. We assume that the theorem is true for all groups of order pm with $m<g'$, and for all groups of order pg' acting on vector spaces of dimension less than d. Groups of order p satisfying the conditions of Theorem 2 trivially have the required structure. On the other hand, if $d=1$, $\mathfrak{G}$ must be a group of order p, and again Theorem 2 is true.

a) Denote the representation of $\mathfrak{G}$ on $\mathscr{V}$ by $\mathfrak{V}$. Suppose $\mathfrak{V}$ is not absolutely irreducible. If $\mathfrak{V}$ decomposes into $s>1$ absolutely irreducible constituents, then there exists an extension field L of K of degree s such that in $L\otimes_K\mathscr{V}$,

$$\mathfrak{V}\approx\begin{pmatrix}\mathfrak{W}_1 & 0 & & 0\\ 0 & \mathfrak{W}_2 & & 0\\ & & \cdot & \\ & & & \cdot \\ 0 & 0 & & \mathfrak{W}_s\end{pmatrix} \tag{1}$$

The $\mathfrak{W}_i$ are distinct absolutely irreducible representations of $\mathfrak{G}$, and they are all algebraically conjugate to a fixed one with respect to the automorphisms $\sigma_1, \sigma_2, \ldots, \sigma_s$ of L/K. Let $L\otimes_K\mathscr{V}=\mathscr{W}_1\oplus\mathscr{W}_2\oplus\cdots\oplus\mathscr{W}_s$ be the decomposition of $L\otimes_K\mathscr{V}$ corresponding to (1). If $e_{i1}, e_{i2}, \ldots, e_{im}$ is a basis for $\mathscr{W}_i$, then the vectors of $\mathscr{V}$ can be identified with the vectors in $L\otimes_K\mathscr{V}$ of the form

$$\sum_{i=1}^{s}\sum_{j=1}^{m}(\alpha_j)^{\sigma_i}e_{ij} \qquad \alpha_j \text{ in } L.$$

It follows that each vector in $\mathscr{W}_1$ is fixed by some Sylow p-subgroup of $\mathfrak{G}$. Hence by induction on the degree of $\mathfrak{W}_1$, $\mathfrak{G}$ has the required structure. We may assume then $\mathfrak{V}$ is absolutely irreducible.

b) Let $\tilde{\mathfrak{G}}$ be a maximal normal subgroup of $\mathfrak{G}$; by condition (i) $\tilde{\mathfrak{G}}$ must have index p in $\mathfrak{G}$, and indeed $\tilde{\mathfrak{G}}=[\mathfrak{G},\mathfrak{G}]$, where $[\mathfrak{G},\mathfrak{G}]$ is the commutator subgroup of $\mathfrak{G}$. Suppose the restriction $\mathfrak{V}|\tilde{\mathfrak{G}}$ of $\mathfrak{V}$ to $\tilde{\mathfrak{G}}$ is reducible. If $\mathscr{W}$ is any $\tilde{\mathfrak{G}}$-invariant subspace of $\mathscr{V}$, and if w is any vector in $\mathscr{W}$, then there exists a Sylow p-subgroup $\mathfrak{P}$ of $\mathfrak{G}$ which fixes w. But $\mathfrak{P}\tilde{\mathfrak{G}}=\mathfrak{G}$, and thus $w\mathfrak{G}\subseteq\mathscr{W}$. In other words, $\mathscr{W}$ is also $\mathfrak{G}$-invariant. Hence we may assume $\mathfrak{V}|\tilde{\mathfrak{G}}$ is irreducible (We shall show later that we may even assume $\mathfrak{B}|\tilde{\mathfrak{G}}$ is absolutely irreducible.).

c) Suppose that $\mathfrak{B}$ is induced by some representation $\mathfrak{U}$ over K from some subgroup $\mathfrak{M}<\mathfrak{G}$. By b) it follows that $\mathfrak{M}$ contains a Sylow p-subgroup of $\mathfrak{G}$, say $\mathfrak{P}=\{A\}$. We may assume $\mathfrak{M}$ is a maximal subgroup of $\mathfrak{G}$ by replacing $\mathfrak{M}$ with a maximal subgroup containing it and by replacing $\mathfrak{U}$ by the corresponding induced representation. Let $\mathfrak{S}$ be the maximal normal subgroup of $\mathfrak{G}$ contained in $\mathfrak{M}$, and let $\mathfrak{T}/\mathfrak{S}$ be a minimal normal subgroup of $\mathfrak{G}/\mathfrak{S}$. It is well-known that $\mathfrak{G}=\mathfrak{M}\mathfrak{T}$ and $\mathfrak{M}\cap\mathfrak{T}=\mathfrak{S}$. We may thus take for coset representatives of $\mathfrak{M}$ in $\mathfrak{G}$, elements $1=T_0,\ T_1,\ \ldots,\ T_r$ of $\mathfrak{T}$ which are coset representatives of $\mathfrak{S}$ in $\mathfrak{T}$.

Let $\mathscr{U}$ be the subspace of $\mathscr{V}$ on which $\mathfrak{U}$ is defined. As a $\mathfrak{G}$-module $\mathscr{V}$ is isomorphic to the $\mathfrak{G}$-module

$$\mathscr{V}'=\mathscr{U}\otimes 1+\mathscr{U}\otimes T_1+\cdots+\mathscr{U}\otimes T_r$$

the action being defined as follows: If G is in $\mathfrak{G}$, let $T_iG=M_iT_{i'}$, where M_i is in $\mathfrak{M}$ and $i\to i'$ is a permutation of $0,1,\ldots,r$. If $v=\sum v_i\otimes T_i$ is a vector in $\mathscr{V}'$, where the v_i are in $\mathscr{U}$, then

$$vG=\sum_i v_iM_i\otimes T_{i'}$$

Let j be a fixed index, $1\le j\le r$, and u a fixed non-zero vector in $\mathscr{U}$. The vector

$$v=u\otimes T_0+u\otimes T_j+\sum_{i\neq 0,\,j}0\otimes T_i$$

by hypothesis is fixed by some conjugate A_j of A. Now we may assume $p\ge 3$; otherwise $\mathfrak{G}$ is a cyclic group of order 2. $p\ge 3$ implies that A_j leaves the subspaces $\mathscr{U}\otimes T_0$, $\mathscr{U}\otimes T_j$ fixed, and since $\mathfrak{M}$ is the subgroup of $\mathfrak{G}$ leaving $\mathscr{U}\otimes T_0$ fixed, the element A_j must be in $\mathfrak{M}$. On the other hand $\mathscr{U}\otimes T_jA_j=\mathscr{U}\otimes T_j$ implies that $T_jA_jT_j^{-1}$ is in $\mathfrak{M}$, and hence $T_jA_jT_j^{-1}A_j^{-1}$ belongs to $\mathfrak{M}$. Since $T_jA_jT_j^{-1}A_j^{-1}$ belongs to $\mathfrak{T}$ as well, $T_jA_jT_j^{-1}A_j^{-1}$ is in $\mathfrak{S}$. In other words, we have shown that given any element of $\mathfrak{T}/\mathfrak{S}$ there exists a p-element in $\mathfrak{M}$ centralizing it.

Let $\mathfrak{X}$ be the representation of $\mathfrak{G}$ induced on $\mathfrak{T}/\mathfrak{S}$ by transformation, and let $\mathfrak{K}$ be the kernel of $\mathfrak{X}$. If $\mathfrak{K}$ contains A, then the permutation representation of $\mathfrak{G}$ on the cosets of $\mathfrak{M}$ would contain A in its kernel, which is impossible.

We may therefore assume $\mathfrak{K} < \mathfrak{G}$. In this case, the induction hypothesis applies to the group $\mathfrak{G}/\mathfrak{K}$ and the representation $\mathfrak{X}$. $\mathfrak{K}$ must then be $\tilde{\mathfrak{G}}$; by the irreducibility of $\mathfrak{X}$, A can fix only the zero vector in the space $\mathfrak{T}/\mathfrak{S}$. This property is shared by the conjugates of A as well. But this is impossible, since we have just seen that given any T in $\mathfrak{T}/\mathfrak{S}$, there is a conjugate of A which transforms T onto itself. We may therefore assume $\mathfrak{V}$ is not an induced representation over K.

d) Let $\mathfrak{H}$ be the maximal abelian normal subgroup of $\mathfrak{G}$. By c) and Clifford's Theorem [5], the restriction $\mathfrak{V}|\mathfrak{H}$ must be a direct sum of equivalent representations

$$\mathfrak{V}|\mathfrak{H} = \mathfrak{W} \oplus \mathfrak{W} \oplus \cdots \oplus \mathfrak{W} \tag{2}$$

where $\mathfrak{W}$ is an irreducible representation of $\mathfrak{H}$ over K. Since $\mathfrak{W}(\mathfrak{H})$ is a cyclic group and $\mathfrak{V}$ represents $\mathfrak{H}$ faithfully by (2), it follows that $\mathfrak{H}$ is cyclic. Let $\mathfrak{C}(\mathfrak{H})$ be the centralizer of $\mathfrak{H}$ in $\mathfrak{G}$. $\mathfrak{G}/\mathfrak{C}(\mathfrak{H})$ is isomorphic to a subgroup of the automorphism group of $\mathfrak{H}$, and hence is abelian. By b) it follows that $\mathfrak{C}(\mathfrak{H}) \supseteq \tilde{\mathfrak{G}}$ (We shall show later that $\mathfrak{H}$ is even in the center of $\mathfrak{G}$).

e) We may assume $\tilde{\mathfrak{G}}$ is non-abelian. For if not, then $\tilde{\mathfrak{G}} = \mathfrak{H}$ would be cyclic, and in particular, A would act trivially on the Frattini factor group $\mathfrak{H}/\phi(\mathfrak{H})$, since p is the largest prime divisor of $|\mathfrak{G}|$. This would contradict condition (i) of the theorem. Let $\mathfrak{N}$ be a minimal non-abelian normal subgroup of $\mathfrak{G}$; $\mathfrak{N}$ is contained in $\tilde{\mathfrak{G}}$ and in particular, $\mathfrak{N}$ is centralized by $\mathfrak{H}$. The results of Huppert [10] §2 therefore apply to this situation. Let r be the characteristic of K. $\mathfrak{N}$ then has the following structure: i) $\mathfrak{N}$ is a q-group for some prime $q \neq r$. ii) The center $\mathfrak{Z}(\mathfrak{N})$ of $\mathfrak{N}$ is cyclic and $\mathfrak{N}/\mathfrak{Z}(\mathfrak{N})$ is a minimal normal subgroup of $\mathfrak{G}/\mathfrak{Z}(\mathfrak{N})$. iii) The order of $\mathfrak{N}/\mathfrak{Z}(\mathfrak{N})$ is of the form q^{2n}, and $|\mathfrak{N}| = q^{2n+1}$ or q^{2n+2}, the latter possibility occurring only in the case $q = 2$. iv) The exponent of $\mathfrak{N}$ is q or q^2, the latter occurring only for $q = 2$. v) Transformation by elements of $\mathfrak{G}$ on $\mathfrak{N}/\mathfrak{Z}(\mathfrak{N})$ induces sympletic linear transformations over $GF(q)$. (For q odd, $\mathfrak{N}$ is an extra-special q-group in the terminology of Hall-Higman [9].)

f) Suppose $\mathfrak{V}|\mathfrak{N}$ is reducible, say

$$\mathfrak{V}|\mathfrak{N} = \mathfrak{U} \oplus \mathfrak{U} \oplus \cdots \oplus \mathfrak{U};$$

the irreducible constituents $\mathfrak{U}$ of $\mathfrak{V}|\mathfrak{N}$ are all equivalent by c). Let $\mathscr{U}$ be an irreducible subspace of $\mathcal{V}$ for $\mathfrak{N}$. If u is any non-zero vector in $\mathcal{U}$, there exists a conjugate B of A which fixes u. Now $\mathcal{U}B$ is also an irreducible subspace of $\mathcal{V}$ for $B^{-1}\mathfrak{N}B = \mathfrak{N}$, and since u is in $\mathcal{U} \cap \mathcal{U}B$, it follows that $\mathcal{U} = \mathcal{U}B$. In other words every vector u in $\mathcal{U}$ is fixed by a conjugate of A belonging to the normalizer $\mathfrak{N}(\mathcal{U})$ of $\mathcal{U}$ in $\mathfrak{G}$. Let $\mathfrak{L}$ be the group $\mathfrak{N}(\mathcal{U})/\mathfrak{C}(\mathcal{U})$, where $\mathfrak{C}(\mathcal{U})$ is the centralizer of $\mathcal{U}$ in $\mathfrak{G}$. Since $\mathfrak{N}$ is faithfully represented on $\mathcal{U}$, $\mathfrak{N} \cap \mathfrak{C}(\mathcal{U}) = 1$. We may assume A is in $\mathfrak{N}(\mathcal{U})$ be replacing $\mathcal{U}$ by a suitable conjugate subspace. If A is in $\mathfrak{C}(\mathcal{U})$, then A centralizes $\mathfrak{N}$, since $\mathfrak{N}$ and $\mathfrak{C}(\mathcal{U})$ are normal subgroups of $\mathfrak{N}(\mathcal{U})$ with trivial intersection. This is impossible, for it would imply that $\mathfrak{C}(\mathfrak{N}) = \mathfrak{G}$ or that $\mathfrak{N} \subseteq \mathfrak{Z}(\mathfrak{G})$. We may therefore assume A is not in $\mathfrak{C}(\mathcal{U})$. Let $\mathfrak{L}_1$ be the normal subgroup of $\mathfrak{L}$ generated by the Sylow p-subgroups of $\mathfrak{L}$. $\mathfrak{L}_1$ has p'-index in $\mathfrak{L}$, and moreover $\mathfrak{L}_1$ contains no proper normal subgroups of p'-index. Let $\tilde{\mathfrak{L}}_1$ be the normal p-complement of $\mathfrak{L}_1$. $\mathfrak{U}|\mathfrak{L}_1$ may no longer be irreducible. Suppose that

$$\mathfrak{U}|\mathfrak{L}_1 \approx \begin{pmatrix} \mathfrak{W}_1 & & & \\ & \mathfrak{W}_2 & & \\ & & \ddots & \\ & & & \mathfrak{W}_t \end{pmatrix}$$

where the $\mathfrak{W}_i$ are irreducible representations of $\mathfrak{L}_1$ conjugate to one another in $\mathfrak{L}$. For $i = 1, 2, \ldots, t$ let $\mathfrak{K}_i$ be the kernel of $\mathfrak{W}_i$. No $\mathfrak{K}_i$ can contain A, for otherwise $\mathfrak{K}_i$ would be $\mathfrak{L}_1$, and the representations $\mathfrak{W}_1, \mathfrak{W}_2, \ldots, \mathfrak{W}_t$ would be trivial. Let $\mathcal{W}_i$ be the subspace of $\mathcal{U}$ corresponding to $\mathfrak{W}_i$. The group $\mathfrak{L}_1/\mathfrak{K}_i$ acting on the subspace $\mathcal{W}_i$ satisfies the conditions of Theorem 2. The induction hypothesis therefore implies that $\tilde{\mathfrak{L}}_1 = \mathfrak{K}_i$. In other words, $\tilde{\mathfrak{L}}_1$ is in the kernel of each $\mathfrak{W}_i$, and hence in the kernel of $\mathfrak{U}|\mathfrak{L}_1$. It follows that $\{A\}\mathfrak{C}(\mathcal{U})$ is normal in $\mathfrak{N}(\mathcal{U})$. But $\{A\}\mathfrak{C}(\mathcal{U}) \cap \mathfrak{N} = 1$, and again we conclude that A centralizes $\mathfrak{N}$, which we have already seen to be impossible. We may therefore assume $\mathfrak{B}|\mathfrak{N}$ is irreducible.

g) Let K have r^b elements, where r is the characteristic of K. Let s be the order of r^b modulo q if q is odd, modulo 4 if $q = 2$. In particular s divides $q-1$ if q is odd, s divides 2 if q is 2. The degree of $\mathfrak{B}$ must be sq^n by [9], 2.4. Since $p > q$, p does not divide sq^n. In particular we conclude that $\mathfrak{B}|\tilde{\mathfrak{G}}$ is absolutely irreducible. Moreover, since $\mathfrak{H} \subseteq \mathfrak{Z}(\tilde{\mathfrak{G}})$, the matrices of $\mathfrak{B}(\mathfrak{H})$ can be represented as scalar multiples of the identity matrix in some extension field of K, and we conclude that $\mathfrak{H}$ is even in $\mathfrak{Z}(\mathfrak{G})$.

h) Let $\mathscr{W}$ be the sympletic space $\mathfrak{N}/\mathfrak{Z}(\mathfrak{N})$, and let $\mathscr{W}_0$ be the subspace of all vectors in $\mathscr{W}$ fixed by A. Since A acts as a sympletic transformation on $\mathscr{W}$, there exists a complement $\mathscr{W}_1$ to $\mathscr{W}_0$ in $\mathscr{W}$ which is invariant under A and on which A acts sympletically. A has no fixed vectors in $\mathscr{W}_1$ besides the zero vector. Let $2m$ be the dimension of $\mathscr{W}_1$ over $GF(q)$. $m \geq 1$, for otherwise A would not only centralize $\mathfrak{N}/\mathfrak{Z}(\mathfrak{N})$, but even $\mathfrak{N}$ by [8] § 1. 3. Let $\mathscr{W}_1 = \mathfrak{M}/\mathfrak{Z}(\mathfrak{N})$, and let the index of $\mathscr{W}_1$ in $\mathscr{W}$ be q^{2t}. Choose a basis in $\mathscr{V}$ over K such that the restriction of $\mathfrak{B}$ to $\{A, \mathfrak{M}\}$ has the form

$$\begin{pmatrix} \mathfrak{A}_1 & 0 & & 0 \\ * & \mathfrak{A}_2 & & 0 \\ & & \cdot & \\ & & & \cdot \\ * & * & & \mathfrak{A}_{q^t} \end{pmatrix}$$

Here each $\mathfrak{A}_i$ is an irreducible representation of $\{A, \mathfrak{M}\}$ of degree sq^m.

i) We now calculate the number of vectors in $\mathscr{V}$ fixed by A. Let L be an extension field of degree s over K such that over L, the representation $\mathfrak{A}_i$ decomposes into s absolutely irreducible representations

$$\mathfrak{A}_i \simeq \mathfrak{B}_1 \oplus \mathfrak{B}_2 \oplus \cdots \oplus \mathfrak{B}_s$$

If the vectors in the subspace corresponding to $\mathfrak{B}_1$ which are fixed by A span a subspace of dimension N over L, then the vectors in the space corresponding to $\mathfrak{A}_i$ which are fixed by A span a subspace of dimension sN over K. Since there are q^t such representations $\mathfrak{A}_i$, the vectors of $\mathscr{V}$ which are fixed by A span at most a subspace of dimension sNq^t over K.

If $r = p$, N can be computed by the theorems of Hall-Higman [9], 2. 5. 1-2. 5. 3. Indeed, $q^m = kp + 1$ or $q^m = kp + (p-1)$, and $N = k + 1$. If $r \neq p$, we must use a different method. Since r does not divide $|\mathfrak{M}|$, N is precisely the number of characteristic values of $\mathfrak{B}_1(A)$ which are 1. Now there exist an algebraic number field Ω, a prime ideal divisor $\mathfrak{r}$ of r in Ω, and an absolutely irreducible representation $\mathfrak{X}$ of $\mathfrak{M}$ written in the ring of $\mathfrak{r}$-local integers of Ω, such that the representation $\mathfrak{X}$ modulo $\mathfrak{r}$ is equivalent to $\mathfrak{B}_1$. In particular, N is also the number of characteristic values of $\mathfrak{X}(A)$ which are 1. Let χ be the character of $\mathfrak{X}$; we then have

$$N = \frac{1}{p}\sum_{i=1}^{p}\chi(A^i)$$

Since $\mathfrak{M}$ is a group whose order contains p only to the first power, N can be computed by the results of Brauer [2] Theorem 4. Indeed, for $i \not\equiv 0 \pmod{p}$,

$$\chi(A^i) = \begin{cases} \pm f & \text{if } \chi \text{ is non-exceptional} \\ \pm \varepsilon^i f & \text{if } \chi \text{ is exceptional} \end{cases}$$

where ε is a primitive p-th root of unity and f is the degree of an irreducible character of the p'-part of the centralizer of A in $\mathfrak{M}$. The structure of $\mathfrak{M}$ implies that f must be 1. As for the case $r = p$, we find that $q^m = kp + 1$ or $q^m = kp + (p-1)$, but now we have only $N \leq k+1$. In any case, we can conclude that the total number of vectors in $\mathscr{V}$ fixed by A is less than or equal to r^{bsNq^t}.

j) Let $\mathfrak{P}$ be a Sylow p-subgroup of $\mathfrak{G}$, and let $\mathfrak{N}(\mathfrak{P})$ be the normalizer of $\mathfrak{P}$ in $\mathfrak{G}$. Since the total number of vectors in $\mathscr{V}$ is r^{bsq^n}, the conditions of Theorem 2 imply that

$$|\mathfrak{G} : \mathfrak{N}(\mathfrak{P})| \geq r^{bs(q^n - Nq^t)} \tag{3}$$

Represent $\mathfrak{G}$ on $\mathfrak{N}/\mathfrak{Z}(\mathfrak{N})$, and let $\mathfrak{K}$ be the kernel of this representation. By [10] Hilfssatz II

$$\mathfrak{G}/\mathfrak{K} \subseteq Sp(2n, q)$$
$$\mathfrak{K}/\mathfrak{H} \subseteq \mathfrak{Z}(\mathfrak{N}) \times \mathfrak{Z}(\mathfrak{N}) \times \cdots \times \mathfrak{Z}(\mathfrak{N}) \qquad (2n \text{ times}),$$

where $Sp(2n, q)$ is the sympletic group of dimension $2n$ over $GF(q)$. Now

$$\begin{aligned} |Sp(2n, q)| &= (q^{2n}-1)(q^{2n-2}-1)\cdots(q^2-1)q^{2n-1}q^{2n-3}\cdots q \\ &\leq q^{2n^2+n} \end{aligned}$$

$$|\mathfrak{K}/\mathfrak{H}| \leq \begin{cases} q^{2n} & \text{if } q \neq 2 \\ q^{4n} & \text{if } q = 2 \end{cases}$$

It then follows that

$$r^{bs(q^n - Nq^t)}|\mathfrak{N}(\mathfrak{P})| \leq \begin{cases} |\mathfrak{H}|q^{2n^2+n}q^{2n} & \text{if } q \neq 2 \\ |\mathfrak{H}|q^{2n^2+n}q^{4n} & \text{if } q = 2. \end{cases}$$

$\mathfrak{H} \subseteq \mathfrak{Z}(\mathfrak{G})$ implies that $\mathfrak{H} \subseteq \mathfrak{N}(\mathfrak{P})$ and thus we have finally

https://doi.org/10.1017/S0027763000010990 Published online by Cambridge University Press

$$(4) \qquad r^{bs(q^n - Nq^t)} \leq \begin{cases} q^{2n^2+3n} & \text{if } q \neq 2 \\ q^{2n^2+5n} & \text{if } q = 2. \end{cases}$$

The inequality (4) holds only for small values of n, r, p, and q. The proof will then be complete once we show no groups $\mathfrak{G}$ correspond to these exceptional values.

k) To obtain an estimate on n, we use the inequality

$$q^n - Nq^t \geq q^n - \frac{2q^n}{p}$$

Putting this in (4) we obtain the inequality

$$\frac{p-2}{p} q^n \log r \leq \begin{cases} (2n^2+3n) \log q & \text{if } q \neq 2 \\ (2n^2+5n) \log q & \text{if } q = 2, \end{cases}$$

and this can hold only for the following values of n and q.

n	q
7	2
6	2
5	2
4	2
3	2, 3
2	2, 3, 5, 7
1	$q \leq 31$

We treat the case $p=3$ separately. For $p=3$, the 3-complement in $\mathfrak{G}$ must be a 2-group. Hence $|\mathfrak{G}:\mathfrak{K}|=3$, $|\mathfrak{N}:\mathfrak{Z}(\mathfrak{N})|=4$, and $|\mathfrak{G}|=48$ or 24. Since the representation $\mathfrak{V}$ of $\mathfrak{G}$ is absolutely irreducible, $\mathfrak{V}$ must have degree 2. Let $\mathfrak{P}$ be a Sylow 3-subgroup of $\mathfrak{G}$; $\mathfrak{N}(\mathfrak{P})$ has index 1, 2, or 4 in $\mathfrak{G}$. $\mathfrak{P}$ can fix at most r^b vectors in $\mathscr{V}$, so that (3) for this case becomes $4r^b \geq r^{2b}$. This is possible only for $r^b=3$. But then s would be 2 and the degree of $\mathfrak{V}$ would be 4, which is a contradiction. We may therefore assume that $p \geq 5$.

If $n=1$, $p \mid q \pm 1$ implies that $p<q$ or $p=3$. Thus no groups $\mathfrak{G}$ can occur for this case. The same argument allows us to assume $m \geq 2$ in the remaining cases. The following argument will be used frequently. For given n, m, q, p we know that $|\mathfrak{G}:\mathfrak{K}|$ divides the order of $Sp(2n, q)$. The conditions (i) and (iii) of the theorem further restrict the possible divisors of $|\mathfrak{G}:\mathfrak{K}|$. Using the bounds for $|\mathfrak{G}:\mathfrak{K}|$ obtained in this way in (3), we can eliminate most of

the remaining cases.

If $n=2$, there are three cases,

m	q	p
2	2	5
2	3	5
2	5	13

The case $m=2$, $q=2$, $p=5$. The group $Sp(4, 2)$ has order $2^4.3.5$, and hence $|\mathfrak{G}:\mathfrak{K}|=5$. If $|\mathfrak{Z}(\mathfrak{N})|=2$, then (3) for this case becomes $2^4.r^{bs}\geq r^{4bs}$ or $r^{3bs}\leq 2^4$. This cannot hold for any possible value of r. If $|\mathfrak{Z}(\mathfrak{N})|=4$, then $|\mathfrak{G}:\mathfrak{N}(\mathfrak{P})|\leq 2^4$. (3) for this case becomes $r^{3bs}\leq 2^4$ and again this is impossible.

The case $m=2$, $q=3$, $p=5$. The group $Sp(4, 3)$ has order $2^7.3^4.5$. The subgroups of $Sp(4, 3)$ have been studied by Dickson in [6]; in particular $\mathfrak{G}/\mathfrak{K}$ must have order dividing $2^7.5$, and thus $|\mathfrak{G}:\mathfrak{N}(\mathfrak{P})|$ divides $2^7.3^4$. Since $|\mathfrak{G}:\mathfrak{N}(\mathfrak{P})|\equiv 1 \pmod 5$, we can even assert that $|\mathfrak{G}:\mathfrak{N}(\mathfrak{P})|$ divides $2^4.3^4=6^4$. (3) for this case becomes $r^{7bs}\leq 6^4$. If $r=2$, then $bs\geq 2$ and the inequality is false. No other values for r are possible.

The case $m=2$, $q=5$, $p=13$. The group $Sp(4, 5)$ has order $2^7.3^2.5^4.13$, and hence $|\mathfrak{G}:\mathfrak{K}|=13$. (3) for this case becomes $r^{23bs}\leq 5^4$, which is impossible.

If $n=3$, there are five cases,

m	q	p
2	2	5
2	3	5
3	2	7
3	3	13
3	3	7

The case $m=2$, $q=2$, $p=5$. The group $Sp(6, 2)$ has order $2^9.3^4.5.7$, and hence $|\mathfrak{G}:\mathfrak{K}|$ divides $2^9.3^4.5$. The representation $\mathfrak{X}$ of $\mathfrak{G}/\mathfrak{K}$ on $\mathfrak{N}/\mathfrak{Z}(\mathfrak{N})$ is irreducible, and has dimension 6 over $GF(2)$. A degree consideration shows that $\mathfrak{X}|\tilde{\mathfrak{G}}$ is still irreducible. Now if 3^4 does not divide $|\mathfrak{G}:\mathfrak{K}|$, then $|\mathfrak{G}:\mathfrak{K}|=5$, and (3) for this case becomes $r^{6bs}\leq 2^{12}$. If $r=3$, then $bs\geq 2$ and the inequality is impossible. No other values for r are possible. If 3^4 divides $|\mathfrak{G}:\mathfrak{K}|$, then $\tilde{\mathfrak{G}}/\mathfrak{K}$ must have a normal Sylow 3-subgroup of type (3, 3, 3, 3). But such a

https://doi.org/10.1017/S0027763000010990 Published online by Cambridge University Press

group cannot have an irreducible representation of degree 6 over $GF(2)$.

The case $m=2$, $q=3$, $p=5$. The group $Sp(6, 3)$ has order $2^{10}.3^{9}.5.7.13$, and hence $|\mathfrak{G}:\mathfrak{K}|$ divides $2^{10}.3^{9}.5$. (3) for this case becomes $r^{21bs}\leq 2^{10}.3^{15}$. If $r=2$, then $bs\geq 2$ and the inequality is impossible. The inequality cannot hold for $r\geq 5$. The last three cases are very similar to this one. Indeed (3) for these cases becomes $r^{6bs}\leq 2^{12}$, $r^{25bs}\leq 3^{6}$, $r^{23bs}\leq 2^{10}.3^{15}$ respectively, and these are impossible.

If $n=4$, there are four cases,

m	q	p
2	2	5
3	2	7
4	2	5
4	2	17

The group $Sp(8, 2)$ has order $2^{16}.3^{5}.5^{2}.7.17$. (3) for the cases $p=7, 17$ becomes $r^{12bs}\leq 2^{16}$, $r^{14bs}\leq 2^{16}$, respectively, and both are impossible. Suppose then that $p=5$, so that $|\mathfrak{G}:\mathfrak{K}|$ divides $2^{16}.3^{5}.5$. If $\mathfrak{G}/\mathfrak{K}$ has no principal factor of type $(3, 3, 3, 3)$, then $|\mathfrak{G}:\mathfrak{K}|=5$, and (3) becomes $r^{12bs}\leq 2^{16}$, which is impossible. Let $\mathfrak{L}/\mathfrak{K}$ be the maximal normal 3-subgroup of $\mathfrak{G}/\mathfrak{K}$; the order of $\mathfrak{L}/\mathfrak{K}$ is either 3^{4} or 3^{5}. If $\mathfrak{X}$ is the representation of $\mathfrak{G}/\mathfrak{K}$ on $\mathfrak{N}/\mathfrak{Z}(\mathfrak{N})$, then the restriction $\mathfrak{X}|\mathfrak{L}/\mathfrak{K}$ must decompose into four distinct irreducible representations; otherwise $\mathfrak{X}$ would not represent $\mathfrak{L}/\mathfrak{K}$ faithfully. But this would imply that $\mathfrak{G}$ has a subgroup of index 4, and hence a homomorphic image in the symmetric group on 4 letters This is a contradiction, since 5 does not divide 4 !

If $n=5$, there are six cases,

m	q	p
2	2	5
3	2	7
4	2	5
4	2	17
5	2	31
5	2	11

The group $Sp(10, 2)$ has order $2^{25}.3^{6}.5^{2}.7.11.17.31$. All six cases can be eliminated by the same sort of argument. For $p=5, 7$, (3) becomes $r^{24bs}\leq$

$2^{45}.3^6$; for $p=17$, 31, (3) becomes $r^{30bs}\leq 2^{20}$; and for $p=11$, (3) becomes $r^{29bs}\leq 2^{45}.3^6$. In all six cases, these inequalities cannot hold for the possible values of r and bs.

Finally, for $n=6$, 7 the inequality (4) cannot hold for $p\geq 5$. Indeed, for $n=6$, we find that $r^{bs(q^n-Nq^t)}\geq r^{48bs}$, and for $n=7$, $r^{bs(q^n-Nq^t)}\geq r^{96bs}$. Then (4) becomes $r^{48bs}\leq 2^{102}$, $r^{96bs}\leq 2^{133}$ respectively, both of which cannot hold for the possible values of r and bs.

References

[1] R. Brauer, Number theoretical investigations on groups of finite order, Proceedings of the International Symposium on Algebraic Number Theory, Tokyo, 1956, pp. 55–62.

[2] R. Brauer, On groups whose order contains a prime number to the first power, I, Amer. J. Math. vol **64** (1942), pp. 401–420.

[3] R. Brauer, Zur Darstellungstheorie der Gruppen endlicher Ordnung I, Math. Z. vol. **63** (1956), pp. 409–444.

[4] R. Brauer and W. Feit, On the number of irreducible characters of finite groups in a given block, Proc. Nat. Acad. Sci. vol. **45** (1959), pp. 361–365.

[5] A. H. Clifford, Representations induced in an invariant subgroup, Ann. of Math. vol. **38** (1937), pp. 533 550.

[6] L. E. Dickson, Determination of all the subgroups of the known simple group of order 25920, Trans. A.M.S. vol. **5** (1904), pp. 126–166.

[7] P. Fong, On the characters of p-solvable groups, Trans. A.M.S. vol. **98** (1961), pp. 263–284.

[8] P. Hall, A contribution to the theory of groups of prime-power order, Proc. London Math. Soc. vol. **36** (1934), pp. 29–95.

[9] P. Hall and G. Higman, On the p-length of p-soluble groups, Proc. London Math. Soc. vol **6** (1956), pp. 1–42.

[10] B. Huppert, Lineare auflösbare Gruppen, Math. Z. vol. **67** (1957), pp. 479–518.

[11] B. Huppert, Zweifach transitive, auflösbare Permutations-gruppen, Math. Z. vol. **68** (1957), pp. 126–150.

[12] W. Reynolds, Blocks with normal defect group, Seminar on Finite Groups at Harvard University, 1960-1961 (mimeographed notes).

University of California
Berkeley 4, California