ON A CLASS OF DOUBLY TRANSITIVE PERMUTATION GROUPS[1]

BY

WALTER FEIT

1. Introduction

In this paper we will study permutation groups satisfying the following conditions.

HYPOTHESIS I. *G is a doubly transitive permutation group on $m + 1$ letters in which no nontrivial permutation leaves three letters fixed.*

All known examples of permutation groups G satisfying Hypothesis I either contain a normal subgroup of order $m + 1$ or are contained in an exactly[2] triply transitive permutation group G_0, with $[G_0:G] \leqq 2$. In the latter case it is known [10] that $m = p^e$ for some prime p and that the Sylow p-groups of G are abelian. In view of this it seems reasonable to conjecture that the only permutation groups satisfying Hypothesis I are the ones just mentioned. In this paper we prove the following result which is a step in the direction of the conjecture.

THEOREM 1. *Let G be a permutation group of order $qm(m + 1)$ which satisfies Hypothesis I. Then either G contains a normal subgroup of order $m + 1$, or $m = p^e$ for some prime p. In the latter case, $[S_p:S_p'] < 4q^2$, where S_p is the Sylow p-group of G, and if $S_p' = \{1\}$, there exists an exactly triply transitive permutation group G_0 containing G such that $[G_0:G] \leqq 2$.*

Section 2 is devoted to the proof of Theorem 2 which is the main result of this paper. This theorem enables one to compute a large part of the character table for groups G which contain a subgroup M satisfying certain conditions (Hypothesis II in Section 2). The proof of Theorem 2 uses the fundamental result recently proved by J. G. Thompson [9], which together with the results of [5] and [7] show that the regular subgroup of a Frobenius group[3] is nilpotent. The special case of Theorem 2 in which the subgroup M is abelian was proved by R. Brauer and M. Suzuki [8] and has turned out to be a powerful tool in the study of finite linear groups[4] (see for example [3], [8]). Since

Received December 8, 1958.

[1] This research was supported by the United States Army and by the National Science Foundation.

[2] An exactly k-tuply transitive permutation group is a k-tuply transitive permutation group in which only the identity element leaves k or more letters fixed.

[3] By a Frobenius group is meant a group which contains a proper normal subgroup M, called the regular subgroup, with the property that no element in $M - \{1\}$ commutes with any element not in M. Elementary properties of such groups can be found in [5, Section 2].

[4] I am indebted to the authors of [3] for allowing me to see a copy of their manuscript before publication.

it may be of interest independent of its application here, Theorem 2 is proved in a more general form than is actually needed for the proof of Theorem 1.

The methods used in Section 3 to derive Theorem 1 from Theorem 2 are similar to those used in [1] and [3]. It is easily seen from the proof of Theorem 1 that if Theorem 2 could be proved for the case in which M is a non-abelian p-group with $[M:M'] < 4q^2$, then the above-mentioned conjecture would be proved in full.[5]

The object of Section 4 is to classify those groups G which satisfy Hypothesis I, are not exactly doubly transitive, but contain a normal subgroup of order $m + 1$. Furthermore, transitive extensions of such groups are also classified.

For any subset T of a group G, $C(T)$, $N(T)$, $| T |$, will mean respectively the centralizer, normalizer, and number of elements in T. For any complex valued functions ξ_1, ξ_2 on G, the hermitian product $(\xi_1, \xi_2)_G$ is defined by

$$(\xi_1, \xi_2)_G = (1/g) \sum_G \xi_1(x)\overline{\xi_2(x)},$$

and the norm by $\| \xi_1 \|_G^2 = (\xi_1, \xi_1)_G$. The subscript G will be dropped in cases where it is clear from the context which group is involved.

2. A theorem on characters

LEMMA 2.1. *Let P be a p-group, and let ρ be an irreducible character of P with $\rho(1) > 1$. Then*

$$\sum \rho_i(1)^2 \equiv 0 \pmod{\rho(1)^2},$$

where the summation ranges over all irreducible characters ρ_i of P with $\rho_i(1) < \rho(1)$.

Proof. The degree of every irreducible character of P is a power of p; hence $\rho(1) \leqq \rho_i(1)$ is equivalent to $\rho(1) \mid \rho_i(1)$. The relation $\sum \rho_i(1)^2 = | P |$, where ρ_i ranges over all the irreducible characters of P, implies that $\rho_i(1)^2$ is a power of p which is less than $| P |$, hence $\rho_i(1)^2 \mid | P |$ for all i. Consequently

$$\sum_{\rho_i(1)<\rho(1)} \rho_i(1)^2 = | P | - \sum_{\rho_i(1)\geqq\rho(1)} \rho_i(1)^2 \equiv 0 \pmod{\rho(1)^2},$$

as was to be shown.

Before getting to the main result of this section it is necessary to prove some lemmas about characters of groups related to Frobenius groups.

LEMMA 2.2. *Let N be a group of order qmh which contains a normal subgroup of the form $M \times H$, where $| M | = m$, $| H | = h$. Suppose both M and H are normal subgroups of N, and N/H is a Frobenius group whose regular subgroup is $(M \times H)/H$. Let $\zeta_0, \zeta_1, \cdots$ be the irreducible characters of $(M \times H)/H$, and let $\lambda_0, \lambda_1, \cdots$ be the irreducible characters of $(M \times H)/M$, where $\zeta_0 = \lambda_0$ is the trivial character of $M \times H$. Denote $\zeta_i \lambda_s$ by ζ_{is}. The character of N*

[5] I was informed by Professor M. Suzuki that he and H. Zassenhaus had independently proved Theorem 1 under the additional assumption that the subgroup M of G (which is shown to exist in Lemma 3.1) is abelian.

induced by ζ_{is} will be written as $\tilde{\zeta}_{is}$. Then for $i \neq 0$, $\tilde{\zeta}_{is}$ is an irreducible character of N which vanishes outside of $M \times H$. Define ζ_{is}^{x} by

$$\zeta_{is}^{x}(y) = \zeta_{is}(xyx^{-1})$$

for all y in $M \times H$. Then $\tilde{\zeta}_{is}^{x} = \tilde{\zeta}_{is}$ and $\zeta_{is}^{x} \neq \zeta_{is}$ for x in $N - (M \times H), i \neq 0$.

Proof. Assume first that $s = 0$. Then without loss of generality it may be assumed that $H = \{1\}$.

Suppose that M has $k_1 + 1$ classes of conjugate elements and N/M has k_2 classes of conjugate elements. Then it is easily seen that N has $k_1/q + k_2$ irreducible characters, and the representations of k_2 of these contain M in their kernel. Furthermore it is clear that $\tilde{\zeta}_0$ is the character of the regular representation of N/M. Hence no irreducible character of N whose representation has M in its kernel occurs in any $\tilde{\zeta}_i$ for $i \neq 0$.

Let Q be a subgroup of N of order q; then for y in M,

$$\tilde{\zeta}_i(y) = \sum\nolimits_{x \epsilon Q} \zeta_i(xyx^{-1}) = \sum\nolimits_{x \epsilon Q} \zeta_i^{x}(y).$$

This immediately yields that $(\tilde{\zeta}_i, \tilde{\zeta}_j)_N = 0$ unless $\zeta_j^{x} = \zeta_i$ for some $x \epsilon Q$; in that case $\tilde{\zeta}_i = \tilde{\zeta}_j$. Hence there are at least k_1/q distinct $\tilde{\zeta}_i$, and at most k_1/q irreducible characters which can occur as constituents of the $\tilde{\zeta}_i$. As no irreducible character is a constituent of two distinct $\tilde{\zeta}_i$, there must be exactly k_1/q distinct $\tilde{\zeta}_i$, and for each $i = 1, 2, \cdots, k_1/q$, $\tilde{\zeta}_i = d_i \hat{\zeta}_i$, where $\hat{\zeta}_i, \hat{\zeta}_2, \cdots$ are the irreducible characters of N whose representations do not contain M in their kernel. Only the characters ζ_i^{x}, $x \epsilon Q$, induce a given $\tilde{\zeta}_\iota$. Hence for each i, there must be q distinct characters ζ_i^{x}, $x \epsilon Q$, since there are k_1 non-trivial characters of M and only k_1/q distinct $\tilde{\zeta}_i$. The Frobenius reciprocity theorem now implies that each ζ_i^{x}, $x \epsilon Q$, occurs as a constituent of $\hat{\zeta}_i$ when restricted to M. Hence $\hat{\zeta}_i(1) \geqq qz_i = \tilde{\zeta}_i(1)$. Consequently $\tilde{\zeta}_i = \hat{\zeta}_i$ is irreducible.

Assume now that $s \neq 0$. It is clear that $\tilde{\zeta}_{is}^{x} = \tilde{\zeta}_{is}$. Since $\zeta_{is}^{x} = (\zeta_i^{x})(\lambda_s^{x})$, the equation $\zeta_{is}^{x} = \zeta_{is}$ would imply that $\zeta_i^{x} = \zeta_i$, and we have already shown this to be false. To complete the proof it is now only necessary to show that $\tilde{\zeta}_{is}$ is an irreducible character of N. This will be done by showing that it has norm one. Since $\tilde{\zeta}_{is} = \sum_x \zeta_{is}^{x}$, where x ranges over a system of coset representations of $M \times H$ in N, we get

$$\| \tilde{\zeta}_{is} \|_N^2 = (1/qmh) \sum\nolimits_{M \times H} | \tilde{\zeta}_{is}(y) | = (1/qmh) \sum\nolimits_{x_1, x_2} \sum\nolimits_{M \times H} \{\zeta_{is}^{x_1}(y)\}\{\zeta_{is}^{x_2}(y)\}$$
$$= (1/q) \sum\nolimits_{x_1, x_2} \delta(x_1, x_2) = 1,$$

where $\delta(x_1, x_2) = 1$ or 0 according to whether $x_1 = x_2$ or $x_1 \neq x_2$. This completes the proof of the lemma.

LEMMA 2.3. *Let M, N have the same meaning as in Lemma 2.2, and assume that $H = \{1\}$. Suppose that M is not a non-abelian p-group with $[M:M'] < 4q^2$. Then for any irreducible character ζ of M of degree $z > 1$*

$$\sum z_i^2 > 2qz,$$

where the z_i range over the degrees of all characters ζ_i of M, $\zeta_i \neq \zeta_0$, with $z_i < z$.

Proof. For any character ζ of M of degree $z > 1$, let $A(\zeta) = A(z)$ denote $\sum z_i^2$, where z_i ranges over the degrees of all nontrivial characters of M with $z_i < z$.

If M is abelian, the result is trivial, since there are no characters of degree $z > 1$. Hence we may assume that M is not abelian. Therefore by a well known theorem of Burnside [4, p. 172] q is odd. It follows from [5], [7], [9] that M is nilpotent. Two cases will be considered:

$$\text{(I)}\quad A(z) \geqq 4q^2, \qquad \text{(II)}\quad A(z) < 4q^2.$$

Case (I) $A(z) \geqq 4q^2$. Let p be a prime dividing z. Since M is nilpotent, $M = S_p \times M_0$ where S_p is a p-group and the order of M_0 is not divisible by p. The character ζ can be written as $\zeta = \rho\lambda$, where ρ is an irreducible character of M/M_0 of degree $\rho(1) > 1$ and λ is an irreducible character of M/S_p It follows from Lemma 2.1 that

$$\sum \rho_i(1)^2 \geqq \rho(1)^2,$$

where ρ_i ranges over all irreducible characters of M/M_0 with $\rho_i(1) < \rho(1)$. The characters $\rho_i\lambda$ are all distinct and have degree $\rho_i(1)\lambda(1) < \rho(1)\lambda(1) = z$; hence

$$A(z) + 1 \geqq \sum \rho_i(1)^2\lambda(1)^2 \geqq \rho(1)^2\lambda(1)^2 = z^2.$$

Since $A(z) \geqq 4q^2$, this implies that

$$\{A(z) + 1\}^2 > 4q^2z^2;$$

therefore $A(z) + 1 > 2qz$. As $A(z)$ is an integer, this yields that $A(z) \geqq 2qz$.

If $A(z) = 2qz$, then $2qz \geqq 4q^2$; hence $z \geqq 2q$. Since z divides m which is relatively prime to q, this implies that $z \geqq 2q + 1$. Therefore

$$2qz + 1 = A(z) + 1 \geqq z^2 \geqq z(2q + 1).$$

This is clearly impossible as $z > 1$. Therefore $A(z) \neq 2qz$; hence $A(z) > 2qz$.

Case (II) $A(z) < 4q^2$. The number of characters of M of degree 1 is $[M:M']$; hence $[M:M'] \leqq A(z) + 1 \leqq 4q^2$. Since $(m, q) = 1$, this implies that $[M:M'] < 4q^2$. Therefore by assumption M is not a p-group. Let $p_1, p_2, \cdots, p_k$ be the distinct primes dividing m; then

$$M = S_{p_1} \times S_{p_2} \times \cdots \times S_{p_k},$$

where S_{p_i} is a p_i-group, $k > 1$. Furthermore

$$[M:M'] = \textstyle\prod_{i=1}^{k} [S_{p_i}:S'_{p_i}].$$

It follows from [5, Lemma 2.5], that q divides $[S_{p_i}:S'_{p_i}] - 1$. If p_i is odd, this implies that $2q$ divides $[S_{p_i}:S'_{p_i}] - 1$, since q is odd. Hence if at least two odd primes were to divide m, it would follow that $4q^2 < [M:M']$, in contradiction to a previous inequality. Therefore $M = S_2 \times S_p$, where p is an odd prime, and neither S_p nor S_2 has order one. Furthermore

$$A(z) \geqq [M:M'] - 1 > 2q^2.$$

The character ζ of M can be written in the form $\zeta = \rho\lambda$, where ρ is a character of M/S_2, and λ is a character of M/S_p. Either $\rho(1) \neq 1$, or $\lambda(1) \neq 1$. The proof will be broken up into three cases: (i) $\lambda(1) = 1$, (ii) $\rho(1) = 1$, (iii) $\lambda(1) \neq 1 \neq \rho(1)$.

Case (i) $\lambda(1) = 1$; therefore $\rho(1) \neq 1$. Lemma 2.1 implies that

$$\sum \rho_i(1)^2 \geqq \rho(1)^2 - 1 > 2\rho(1) = 2z,$$

where ρ_i ranges over all the nontrivial characters of M/S_2 with $\rho_i(1) < \rho(1)$. The second inequality follows from the fact that $\rho(1) \geqq p \geqq 3$. There are at least q distinct characters μ_j of M/S_p of degree 1, and the characters $\rho_i\,\mu_j$ are all distinct as ρ_i, μ_j range over characters of M/S_2, M/S_p, respectively. Hence

$$A(z) \geqq q\sum \rho_i(1)^2 > 2qz.$$

Case (ii) $\rho(1) = 1$; therefore $\lambda(1) \neq 1$. Lemma 2.1 implies that

$$\sum \lambda_i(1)^2 \geqq \lambda(1)^2 - 1 > \lambda(1) = z,$$

where λ_i ranges over the characters of M/S_p with $\lambda_i(1) < \lambda(1)$. There are at least $2q$ characters of M/S_2 of degree 1. By an argument similar to that used in case (i), this yields that

$$A(z) \geqq 2q\sum \lambda_i(1)^2 > 2qz.$$

Case (iii) $\rho(1) \neq 1 \neq \lambda(1)$. Lemma 2.1 now yields that

$$\sum \lambda_i(1)^2 \geqq \lambda(1)^2, \qquad \sum \rho_j(1)^2 \geqq \rho(1)^2,$$

where λ_i, ρ_j range over the characters of M/S_p, M/S_2 with degree less than $\lambda(1)$, $\rho(1)$ respectively. Therefore

$$\sum_{i,j} \lambda_i(1)^2\rho_j(1)^2 \geqq \lambda(1)^2\rho(1)^2 = z^2,$$
$$\sum_i \lambda_i(1)^2\rho(1)^2 \geqq \lambda(1)^2\rho(1)^2 = z^2,$$
$$\sum_j \lambda(1)^2\rho_j(1)^2 \geqq \lambda(1)^2\rho(1)^2 = z^2.$$

The degree of every character which occurs in any of the three sums is less than z, and no character of M appears twice. Therefore $A(z) + 1 \geqq 3z^2$. Since $A(z) > 2q^2$, it follows that

$$\{A(z) + 1\}^2 > 6z^2q^2;$$

therefore

$$A(z) + 1 > \sqrt{6}\,zq > 2zq + (2/5)zq.$$

Since $zq \geqq 4$, this implies that $A(z) + 1 > 2zq + 1$; hence $A(z) > 2zq$. This completes the proof of Lemma 2.3.

In the remainder of this section, groups satisfying special assumptions will be studied. To prevent repetition, the basic hypothesis will be stated separately with the notation to be used.

HYPOTHESIS II. *The group G contains a subgroup of the form $M \times H$, $M \neq \{1\}$, satisfying the following conditions*:

(i) *If y is in $M \times H - H$, then $C(y) \subset M \times H$.*

(ii) *For every x in G which is not contained in the normalizer of $M \times H$, $(M \times H) \cap x(M \times H)x^{-1} \subset H$.*

(iii) *$N(M \times H) \neq M \times H$, and both H and M are normal subgroups of $N(M \times H)$.*

Let $|M| = m$, $|H| = h$, $|N(M \times H)| = qmh$; hence $q > 1$. Let ζ_0, $\zeta_1, \cdots$ be the irreducible characters of $(M \times H)/H$, and let $\lambda_0, \lambda_1, \cdots$ be the irreducible characters of $(M \times H)/M$, where $\zeta_0 = \lambda_0$ is the trivial character of $M \times H$. Let $z_i = \zeta_i(1)$, and denote $\zeta_i \lambda_s$ by ζ_{is}. The characters of G, $N(M \times H)$ induced by ζ_{is} will be denoted by ζ_{is}^*, $\tilde{\zeta}_{is}$, respectively.

LEMMA 2.4. *If G is a group which satisfies Hypothesis II, then $N(M \times H) = N(M)$, and $N(M \times H)/H$ is a Frobenius group whose regular subgroup is $(M \times H)/H$. Furthermore no element of H is conjugate to any element of $M \times H - H$, and for y in $M \times H - H$, $\tilde{\zeta}_{is}(y) = \zeta_{is}^*(y)$ for all i, s.*

Proof. By assumption $N(M \times H) \subset N(M)$. If $x \in N(M)$, then $xHx^{-1} \subset C(M)$; therefore by (i), $xHx^{-1} \subset M \times H$; hence $x(M \times H)x^{-1} \subset M \times H$. Consequently $N(M) \subset N(M \times H)$.

If $y \in M \times H - H$, then $y = y_1 y_2$, where $y_1 \in M$, $y_2 \in H$, $y_1 \neq 1$. Suppose there is an $x \in N(M \times H) - M \times H$ such that $xyx^{-1} \equiv y \pmod{H}$. Since H is a normal subgroup of $N(M \times H)$, this implies that $xy_1x^{-1} \equiv y_1 \pmod{H}$. As M is normal in $N(M \times H)$, $xy_1x^{-1} \in M$; therefore $xy_1x^{-1} = y_1$ since each coset of H in $M \times H$ contains exactly one element of M. This contradicts condition (i) of Hypothesis II. Consequently $(M \times H)/H$ is a normal subgroup of $N(M \times H)/H$ with the property that no element in $(M \times H)/H$, other than the identity, commutes with an element of $N(M \times H)/H$ not in $(M \times H)/H$. By [5, Lemma 2.1] this proves that $N(M \times H)/H$ is a Frobenius group whose regular subgroup is H.

If $y \in H$, $xyx^{-1} \in M \times H - H$, then x is not in $N(M \times H)$ since H is normal in $N(M \times H)$. Therefore

$$xyx^{-1} \in x(M \times H)x^{-1} \cap (M \times H) \subset H;$$

hence $xyx^{-1} \in H \cap (M \times H - H)$ which is clearly impossible. Therefore no element of H is conjugate to any element of $M \times H - H$.

If $x_1 = 1$, $x_2, \cdots$ form a system of coset representatives of $N(M \times H)$ in G, then

$$\zeta_{is}^*(y) = \textstyle\sum_k \tilde{\zeta}_{is}(x_k y x_k^{-1}).$$

Therefore it is sufficient to show that for $k \neq 1$, $y \in M \times H - H$, $x_k y x_k^{-1}$ is not contained in M $\times H$. If this were not the case, then

$$x_k y x_k^{-1} \in (M \times H) \cap x(M \times H)x^{-1} \subset H,$$

and $y \in M \times H - H$ would be conjugate to an element of H, in contradiction to what has just been proved.

We are now in a position to state and prove the main result of this section. Only the special case $h = 1$ will be needed in the remainder of this paper. The following theorem generalizes a special case of [8, Lemma 5], which is essentially due to R. Brauer.

THEOREM 2. *Let G be a group satisfying Hypothesis II. Suppose that $q \neq m - 1$, and M is not a non-abelian p-group with $[M:M'] < 4q^2$. Then for each λ_s, there exist irreducible characters $\chi_{1s}, \chi_{2s}, \cdots$ of G and a sign $\varepsilon_s = \pm 1$ such that*

$$(1) \qquad z_j \zeta_{is}^* - z_i \zeta_{js}^* = \varepsilon_s(z_j \chi_{is} - z_i \chi_{js})$$

for all $i, j \neq 0$. Furthermore for $i \neq 0$,

$$(2) \qquad \zeta_{is}^* = \varepsilon_s \chi_{is} + a_s z_i \sum\nolimits_j z_j \chi_{js} + z_i \Gamma_s ,$$

where $(\Gamma_s, \chi_{js}) = 0$ for all j.

Remark. In the language of [8, p. 662], the classes of G which contain elements of $M \times H - H$ are called special classes. In analogy with the definition on p. 663 of [8], we will say that $\chi_{1s}, \chi_{2s}, \cdots$ are the *exceptional* characters associated with $\tilde{\zeta}_{1s}, \tilde{\zeta}_{2s}, \cdots$.

Proof. If $\zeta_{is}^* \neq \zeta_{js}^*$, then [8, Lemma 4] implies that

$$(3) \qquad \| z_j \zeta_{is}^* - z_i \zeta_{js}^* \|^2 = z_i^2 + z_j^2$$

for $i, j \neq 0$. Since $z_j \zeta_{is}^* - z_i \zeta_{js}^*$ vanishes on elements of H by Lemma 2.4, and since for any class function ξ of $M \times H$, Lemma 2.4 implies that for y in $M \times H - H$, $\tilde{\xi}(y) = \xi^*(y)$, an easy computation yields that

$$(4) \qquad (z_j \zeta_{is}^* - z_i \zeta_{js}^*, \xi^*)_G = (z_j \tilde{\zeta}_{is} - z_i \tilde{\zeta}_{js}, \tilde{\xi})_{N(M \times H)} .$$

For $i \neq 0$, $\tilde{\zeta}_{is}$ is an irreducible character of $N(M \times H)$ by Lemma 2.2. If M is abelian, all the characters $\tilde{\zeta}_{1s}, \tilde{\zeta}_{2s}, \cdots$ have the same degree; hence the theorem is a special case of [8, Lemma 5]. Therefore it may be assumed that M is not abelian. Since M is isomorphic to the regular subgroup of the Frobenius group $N(M \times H)/H$, this implies that $q \neq 2$ by [4, p. 172]. As M is nilpotent ([5], [7], [9]), the assumptions of the theorem imply that $[M:M'] > q^2 + 1$. Therefore by Lemma 2.2 there are at least $q > 2$ distinct characters $\zeta_{1s}^*, \zeta_{2s}^*, \cdots$ with $z_1 = z_2 = \cdots = 1$. Hence by [8, Lemma 5], there exist irreducible characters $\chi_{1s}, \chi_{2s}, \cdots$ of G such that for $i, j \neq 0$, $z_i = z_j = 1$,

$$(5) \qquad \zeta_{is}^* - \zeta_{js}^* = \varepsilon_s(\chi_{is} - \chi_{js}),$$

where $\varepsilon_s = \pm 1$ is independent of i, j. As there are more than two such characters, ε_s is uniquely determined, and the characters χ_{is} are well defined.

From now on, let ζ_{1s}^* be a fixed character with $z_1 = 1$. Let E_s be the set of all characters ζ_{is}^*, $i \neq 0$, such that there exists an irreducible character χ_{is} of G with

$$(6) \qquad z_i\zeta_{1s}^* - \zeta_{is}^* = \varepsilon_s(z_i\chi_{1s} - \chi_{is}).$$

By (5), E_s contains all ζ_{is}^* with $z_i = 1$. If ζ_{is}^*, ζ_{js}^* are in E_s, then

$$\begin{aligned} z_j\zeta_{is}^* - z_i\zeta_{js}^* &= z_j(\zeta_{is}^* - z_i\zeta_{1s}^*) - z_i(\zeta_{js}^* - z_j\zeta_{1s}^*) \\ (7) \qquad &= \varepsilon_s\{z_j(\chi_{is} - z_i\chi_{1s}) - z_i(\chi_{js} - z_j\chi_{1s})\} \\ &= \varepsilon_s(z_j\chi_{is} - z_i\chi_{js}). \end{aligned}$$

Furthermore, for any $k \neq 0$, relations (4) and (7) imply that

$$\begin{aligned} (8) \qquad (\zeta_{ks}^*, z_j\chi_{is} - z_i\chi_{js})_G &= \varepsilon_s(\tilde{\zeta}_{ks}, z_j\tilde{\zeta}_{is} - z_i\tilde{\zeta}_{js})_{N(M)} \\ &= \varepsilon_s(z_j\delta'_{ik} - z_i\delta'_{jk}), \end{aligned}$$

where $\delta'_{jk} = 1$ if $\zeta_{js}^* = \zeta_{ks}^*$ and $\delta'_{jk} = 0$ otherwise. In particular, (8) implies

$$(9) \qquad \zeta_{1s}^* = \varepsilon_s\chi_{1s} + a_s\sum z_i\chi_{is} + \Gamma_{1s},$$

where χ_{is} ranges over all characters associated with some ζ_{is}^* in E_s, and Γ_{1s} is orthogonal to each of these χ_{is}. The relations (7) and (9) now imply that if ζ_{ks}^* is in E_s, then

$$(10) \qquad \zeta_{ks}^* = \varepsilon_s\chi_{ks} + z_k a_s\sum z_i\chi_{is} + z_k\Gamma_{1s},$$

and if ζ_{ks}^* is not in E_s, then

$$(11) \qquad \zeta_{ks}^* = b_{ks}\sum z_i\chi_{is} + \Gamma_{ks},$$

where the summations in (10), (11) range over all χ_{is} associated with ζ_{is}^* in E_s, and Γ_{1s}, Γ_{ks} are orthogonal to each of these χ_{is}.

The theorem will be proved once it is shown that E_s contains all characters ζ_{is}^*, $i \neq 0$, since in that case (7) is equivalent to (1), and (10) is equivalent to (2).

Suppose that E_s does not contain all characters ζ_{is}^* for $i \neq 0$. Let ζ be a character of this form of minimum degree z such that ζ^* is not in E_s; then $z > 1$ by a previous remark. The relations (9) and (11) imply that

$$(12) \quad z\zeta_{1s}^* - \zeta^* = (z\varepsilon_s + za_s - b)\chi_{1s} + (za_s - b)\textstyle\sum_{i\neq 1} z_i\chi_{is} + \Gamma',$$

where $\Gamma' = z\Gamma_{1s} - \Gamma$. Now (3) and (12) imply

$$\begin{aligned} (13) \qquad z^2 + 1 &= \| z\zeta_{1s}^* - \zeta^* \|^2 \\ &= z^2 + 2\varepsilon_s z(za_s - b) + (za_s - b)^2\textstyle\sum z_i^2 + \| \Gamma' \|^2. \end{aligned}$$

The summation ranges over all values of i such that ζ_{is}^* is in E_s. The set E_s includes all ζ_{is}^* with $z_i < z$, $i \neq 0$. By Lemma 2.2 and Lemma 2.4 there are exactly q distinct characters of $M \times H$ which induce ζ_{is}^*, namely the characters $(\zeta_i\lambda_s)^x$, where x ranges over a system of coset representatives of $M \times H$ in $N(M \times H)$. Each of these has degree $z_i\lambda_s(1)$. Therefore the expression $\sum z_i^2$ in (13) is at least $(1/q)A(z)$, where $A(z) = \sum z_j^2$, and the summation ranges over all ζ_j with $j \neq 0$, $z_j < z$. Lemma 2.3 now implies that the expression $\sum z_i^2$ in (13) satisfies $\sum z_i^2 > 2z$.

Suppose $(za_s - b) \neq 0$. Then (13) yields

$$\begin{aligned} 1 &> 2\varepsilon_s z(za_s - b) + 2z(za_s - b)^2 + \| \Gamma' \|^2 \\ &= 2z\{(za_s - b)^2 + \varepsilon_s(za - b)\} + \| \Gamma' \|^2. \end{aligned} \tag{14}$$

It is easily seen that $(za_s - b)^2 + \varepsilon_s(za_s - b) \geqq 0$; clearly $\| \Gamma' \|^2 \geqq 0$. Hence (14) implies that both these expressions vanish. Therefore $\Gamma' = 0$, $(za_s - b) = -\varepsilon_s$. Substituting these values into (12) leads to

$$z\zeta_{1s}^* - \zeta^* = \varepsilon_s\{(z - 1)\chi_{1s} - \textstyle\sum_{i \neq 1} z_i \chi_{is}\}. \tag{15}$$

Since the left-hand side of (15) has degree zero, so does the right-hand side. It follows from (6) that $\chi_{is}(1) = z_i \chi_{1s}(1)$; hence

$$(z - 1)\chi_{1s}(1) = \textstyle\sum_{i \neq 1} z_i^2 \chi_{1s}(1).$$

Consequently

$$2z < \sum z_i^2 = (z - 1) + 1 = z,$$

which is impossible. Hence $(za_s - b) = 0$.

Now (13) implies that $\| \Gamma' \|^2 = 1$. Hence $\Gamma' = \varepsilon\chi$, where $\varepsilon = \pm 1$ and χ is an irreducible character of G. When these values are substituted in (12), we get

$$z\zeta_{1s}^* - \zeta^* = \varepsilon_s(z\chi_{1s} + \varepsilon\varepsilon_s \chi). \tag{16}$$

As the degree of the left-hand side of (16) is zero, this is also the case for the right-hand side; therefore $\varepsilon\varepsilon_s = -1$. Consequently ζ^* is in E_s, contradicting our assumption. Therefore every character ζ_{is}^* is in E_s, and this suffices to prove the theorem.

COROLLARY 2.1. *Let G satisfy the assumptions of Theorem 2. If χ_{is}, χ_{js} are exceptional characters associated with $\tilde{\zeta}_{is}$, $\tilde{\zeta}_{js}$, then $z_j \chi_{is} - z_i \chi_{js}$ vanishes on elements which are not conjugate to some element of $M \times H - H$.*

Proof. This is an immediate consequence of (1).

COROLLARY 2.2. *Let G satisfy the assumptions of Theorem 2. Suppose λ_1, λ_2 are distinct characters of $(M \times H)/M$; then a character χ of G cannot be an exceptional character that is associated with both $\tilde{\zeta}_{i1}$ and $\tilde{\zeta}_{j2}$, where ζ_i, ζ_j are any two nontrivial characters of $(M \times H)/H$.*

Proof. Suppose the statement is false. Let ζ_1 be a nontrivial character of $(M \times H)/H$ of degree $z_1 = 1$ with $\tilde{\zeta}_i \neq \tilde{\zeta}_1$. Then by (1) we get

$$z_i \zeta_{11}^* - \zeta_{i1}^* = \varepsilon_1(z_i \chi_{11} - \chi),$$

$$z_j \zeta_{k2}^* - z_k \zeta_{j2}^* = \varepsilon_2(z_j \chi_{12} - z_k \chi),$$

where $k = 1$ if $\zeta_j^* \neq \zeta_1^*$, $k = i$ if $\zeta_j^* = \zeta_1^*$. This yields

$$(17) \qquad \varepsilon_1 z_k(z_i \zeta_{11}^* - \zeta_{i1}^*) - \varepsilon_2(z_j \zeta_{k2}^* - z_k \zeta_{j2}^*) = z_i z_k \chi_{11} - z_j \chi_{12}\,.$$

By using (4) and Lemma 2.2 the norm of the left-hand side is easily computed to be $z_i^2 z_k^2 + z_k^2 + z_j^2 + z_k^2$. This is strictly larger than $z_i^2 z_k^2 + z_j^2$ which is larger than, or equal to, the norm of the right-hand side of (17). Hence (17) is impossible, and this proves the corollary.

Corollary 2.3. *Let G satisfy the assumptions of Theorem 2. Then for y in $M \times H - H$*

$$\chi_{is}(y) = \varepsilon_s \tilde{\zeta}_{is}(y) + z_i\{\textstyle\sum_s a_s \sum_{j\neq 0} z_j \zeta_{js}(y) + \sum_s c_s \zeta_{0s}(y)\}.$$

If χ is a character of G distinct from all the χ_{is}, then

$$\chi(y) = \textstyle\sum_s a_s \sum_{j\neq 0} z_j \zeta_{js}(y) + \sum_s c_s \zeta_{0s}(y).$$

Proof. This is an immediate consequence of the Frobenius reciprocity theorem applied to (1), (2), and Corollary 2.2.

Corollary 2.4. *Let G satisfy the assumptions of Theorem 2, and suppose $h = 1$. There exists a rational integer c such that if $\chi_i = \chi_{i0}$ is an exceptional character associated with $\tilde{\zeta}_i$, then for any element y in $M - \{1\}$,*

$$\chi_i(y) = \varepsilon \tilde{\zeta}_i(y) + z_i c.$$

If χ is not an exceptional character, then the restriction of χ to $M - \{1\}$ is a constant.

Proof. Since $h = 1$, Corollary 2.3 yields that if χ_i is the exceptional character associated with $\tilde{\zeta}_i$, then for y in $M - \{1\}$

$$\chi_i(y) = \varepsilon \tilde{\zeta}_i(y) + z_i a_0 \textstyle\sum_j z_j \zeta_j(y) + z_i(c_0 - a_0)\zeta_0(y).$$

Since $\sum z_j \zeta_j$ is the character of the regular representation of M, it vanishes on $M - \{1\}$. This implies the desired result. A similar argument applied to the nonexceptional character χ shows that χ is a constant on $M - \{1\}$.

3. The proof of Theorem 1

Lemma 3.1. *Suppose that G is a group of order g which satisfies Hypothesis I. Then $g = qm(m + 1)$, and q divides $m - 1$. If $q \neq 1$, then G contains a subgroup M of order m which satisfies conditions* (i), (ii), (iii) *of Hypothesis II where $h = 1$, $| N(M) | = qm$. Furthermore for any subgroup Q of $N(M)$ of order q,*

$$yQy^{-1} \cap Q = Q \text{ or } \{1\}$$

for every y in G, and $| N(Q) | \leqq 2q$. Hence for x in $Q - \{1\}$, $C(x) \subset N(Q)$.

Proof. Let N be the subgroup of G consisting of those permutations which leave a given letter fixed. Then by a theorem of Frobenius [4, p. 334], N contains a normal subgroup M of order m which consists of the identity and the permutations in N which leave only the given letter fixed. If $|N| = mq$, then q divides $m - 1$, and $g = qm(m + 1)$. The group M is a normal subgroup of N and has $m + 1$ conjugates in G; therefore $N = N(M)$. Any element x which commutes with y in $M - \{1\}$ must leave the same letter fixed as y does; hence x is in $N(M)$. If x is not in M, then it leaves exactly two letters fixed; hence so does y, which is impossible. Therefore x is in M. This verifies condition (i) of Hypothesis II. Condition (ii) is easily seen to be true, since any element in $M \cap xMx^{-1}$ must leave two letters fixed unless $xMx^{-1} = M$. The only element in M leaving at least two letters fixed is the identity. If $q \neq 1$, $N(M) \neq M$; thus condition (iii) is also verified.

The subgroup Q of $N(M)$ is the set of all permutations fixing two given letters; hence if $yQy^{-1} \neq Q$, the only element in $yQy^{-1} \cap Q$ is the identity by assumption. The group $N(Q)$ is a permutation group on the two letters left fixed by the elements of Q; hence $|N(Q)| \leqq 2q$.

Before proceeding to the proof of Theorem 1 we need some other lemmas. Groups satisfying the following conditions will be considered.

HYPOTHESIS III. *G is a group of order $qm(m + 1)$ which satisfies Hypothesis II with $h = 1$. Furthermore q is odd, G does not contain a normal subgroup of order $m + 1$, and the normal subgroup generated by M is G.*

LEMMA 3.2. *To prove Theorem 3, it suffices to prove the following statement: If G is a group satisfying Hypothesis III, then $q \geqq (m - 1)/2$, or M is a non-abelian p-group with $[M:M'] < 4q^2$.*

Proof. Suppose the statement has been proved. Let G satisfy the assumptions of Theorem 1. By [10, Theorem 19], only the case that q is odd needs to be considered. Let G_1 be the normal subgroup generated by M. Since M has $m + 1$ conjugates in G, G_1 has order $q_1 m(m + 1)$ where q_1 divides q. If $q_1 = 1$, then ([4, p. 181])G_1 contains a normal subgroup of order $m + 1$; this subgroup is characteristic in G_1, and hence normal in G. If $q_1 > 1$, then by Lemma 3.1, G_1 satisfies Hypothesis II with $h = 1$, and therefore also Hypothesis III unless G_1, and therefore G, contains a normal subgroup of order $m + 1$. Consequently $q \geqq q_1 \geqq (m - 1)/2$ or M is a non-abelian p-group with $[M:M'] < 4q_1^2 < 4q^2$. The conclusion of Theorem 1 now follows from [10, pp. 37–38].

Throughout the remainder of this section we will assume that G is a group which satisfies Hypothesis III.

LEMMA 3.3. *$|N(Q)| = 2q$, Q is cyclic, and no element of $Q - \{1\}$ commutes with any element not in Q.*[6]

Proof. Since q is odd, it follows from [4, p. 335] that every Sylow group

[6] I am indebted to Professor M. Suzuki for suggesting this proof. My original method for handling the case in which some element of $Q - \{1\}$ commutes with an element not in Q was more complicated than the method used in the text.

of Q is cyclic. As $|N(Q)| \leqq 2q$, this is also the case for $N(Q)$. Hence by [11, p. 175], $N(Q)'$ and $N(Q)/N(Q)'$ are cyclic groups, and

$$([N(Q):N(Q)'], [N(Q)':1]) = 1.$$

Suppose an odd prime p divides $[N(Q):N(Q)']$, and let S_p be a Sylow p-group of $N(Q)$. It follows from Lemma 3.1 that $N(S_p) \subset N(Q)$. It is easily seen that this implies that S_p is in the center of $N(S_p)$; hence a theorem of Burnside [4, p. 327] implies that G contains a normal subgroup of index p. This normal subgroup must contain M, contradicting Hypothesis III. Therefore $[N(Q):N(Q)']$ is a power of 2. Since q is odd and $Q \neq Q'$, this implies that $N(Q) \neq Q$. Therefore by Lemma 3.1, $|N(Q)| = 2q$; hence $N(Q)' = Q$, and Q is cyclic.

Suppose an element x in $Q - \{1\}$ commutes with some element not in Q. By Lemma 3.1, $C(x) \subset N(Q)$. Therefore there exists an involution[7] t which commutes with x. Hence there is some element x_1 of prime order p which commutes with t. Let x_0 be a generator of the Sylow p-group S_p of $N(Q)$. If $tx_0t = x_0^{-1}$, then $tx_1t = x_1^{-1}$, which is not the case; therefore $tx_0t = x_0$. Consequently S_p is in the center of $N(Q)$; hence by Burnside's theorem [4, p. 327], p divides $[N(Q):N(Q)']$, which contradicts what we have just shown and completes the proof of the lemma.

Lemma 3.4. *G contains only one class of involutions. If m is even, there are $q(m+1)$ involutions in G; if m is odd, there are mq. In both cases the only elements of $M - \{1\}$ which are products of two involutions are involutions.*

Proof. Suppose m is even. Let M_1 be a subgroup of G conjugate to M, but distinct from M. Let u, u_1 be involutions, u in M, u_1 in M_1. It is easily seen that no involution commutes with both u and u_1. Therefore by [2, Lemma 3A], u is conjugate to u_1. Since u was an arbitrary involution in M, every involution in M is conjugate to u_1; hence any two involutions of M are conjugate. Since every involution in G is conjugate to some involution in M, this implies that G contains only one class of involutions. As M is nilpotent, there is an involution u in the center of M; hence $C(u) = M$. The number of involutions in G is $[G:C(u)] = q(m+1)$; furthermore every involution in M is in the center of M. Suppose u_1, u_2 are distinct involutions such that u_1u_2 is in M; then $u_1(u_1u_2)u_1^{-1} = u_2u_1 = (u_1u_2)^{-1}$. Hence u_1u_2 is contained in $u_1Mu_1^{-1} \cap M$; therefore $u_1Mu_1^{-1} = M$. Thus u_1 is in $N(M)$; hence u_1 is in M since M is a normal subgroup of $N(M)$ and $[N(M):M]$ is odd. Consequently u_2 is in M; hence they are both in the center of M. Therefore u_1u_2 is an involution.

Suppose m is odd. If for some y in $M - \{1\}$, there exists an x such that $xyx^{-1} = y^{-1}$, then y is in $M \cap xMx^{-1}$; hence x is in $N(M)$. This is impossible as $N(M)$ has odd order. Therefore $M - \{1\}$ contains no real elements;[8]

[7] An involution is an element of order two; see [2].

[8] An element is said to be real if it is conjugate to its inverse; see [2].

hence [2, Corollary 2B] no element of $M - \{1\}$ is the product of two involutions. If u_1, u_2 are involutions, $u_1 M = u_2 M$ implies $u_1 u_2$ is in M; therefore $u_1 u_2 = 1$; hence $u_1 = u_2$. No coset of M contains more than one involution, and $N(M)$ contains no involutions; hence there are at most $q(m + 1) - q = qm$ involutions in G. If u is an involution, then any element which commutes with u must have order dividing $m + 1$; therefore $| C(u) |$ divides $m + 1$. Consequently the number of elements conjugate to u is $[G:C(u)]$, which is a multiple of qm. Hence $[G:C(u)] = qm$, and every involution in G is conjugate to u.

LEMMA 3.5. *There are at least q nontrivial characters of G which are not exceptional characters associated with M.*

Proof. It is sufficient to show that G has at least q conjugate classes, none of which contain any elements of M. Let k be the number of conjugate classes which contain no elements whose order divides two, but in which every element is a product of two involutions. By Lemma 3.4, it is sufficient to show that $k \geqq q$. Lemma 3.4 implies that G contains at least qm involutions. Hence by [2, Theorem 2J],[9]

$$k \geqq qm(qm + 1)/g = (qm + 1)/(m + 1) = q - (q - 1)/(m + 1);$$

hence $k > q - 1$; therefore $k \geqq q$, as was to be shown.

We are now in a position to prove Theorem 1. Suppose G satisfies Hypothesis III, M is not a non-abelian p-group with $[M:M'] < 4q^2$, and $q < m - 1$. By Lemma 3.2 it is sufficient to show that $q \geqq (m - 1)/2$; we will now do this.

Let $\eta_0, \eta_1, \cdots, \eta_{q-1}$ be the irreducible characters of $N(M)/M$, where η_0 is the trivial character of $N(M)$, and $\eta_{i+(q-1)/2} = \bar{\eta}_i$ for $i = 1, \cdots, (q - 1)/2$. Let η_i^* denote the character of G induced by η_i. With the help of Lemmas 3.1 and 3.3 the values of η_i^* can be computed; the results are given by

$$\eta_i^*(x) = \begin{cases} m + 1 & \text{if } x = 1, \\ 1 & \text{if } x^m = 1, x \neq 1, \\ \eta_i(x) + \overline{\eta_i(x)} & \text{if } x \text{ is in } Q - \{1\}, \\ 0 & \text{if } x^{mq} \neq 1. \end{cases} \tag{18}$$

This implies that for $1 \leqq i, j \leqq (q - 1)/2$

$$\begin{aligned} (\eta_i^*, \eta_j^*) &= \frac{1}{g}\Big[(m + 1)^2 + \frac{g}{mq}(m - 1) \\ &\qquad + \frac{g}{2q}\sum_{Q-\{1\}} \{\eta_i(x) + \overline{\eta_i(x)}\}\{\overline{\eta_j(x)} + \eta_j(x)\}\Big] \\ &= \frac{2}{q} + \frac{1}{2q}\sum_{Q-\{1\}} \{\eta_i(x) + \overline{\eta_i(x)}\}\{\overline{\eta_j(x)} + \eta_j(x)\} \\ &= \tfrac{1}{2}(\eta_i + \bar{\eta}_i, \eta_j + \bar{\eta}_j)_Q = \delta_{ij}. \end{aligned} \tag{19}$$

[9] The statement of the theorem quoted is not quite strong enough. However the same proof can be used to get the inequality needed here.

Equation (19) implies that $\eta_1^*, \cdots, \eta_{(q-1)/2}^*$ are distinct irreducible characters of G.

Since M is nilpotent, there exists a nontrivial irreducible character ζ_1 of M of degree $z_1 = 1$. Lemma 2.2 and Theorem 2 imply that

$$\begin{aligned} \| \zeta_1^* \|^2 &= \frac{1}{g}\left[q^2(m+1)^2 + \frac{g}{qm} \sum_{M-\{1\}} | \tilde{\zeta}_1(y) |^2 \right] \\ &= \frac{1}{g}\left[q^2(m+1)^2 - \frac{q^2 g}{qm} + \frac{g}{qm} \sum_{M} | \tilde{\zeta}_1(y) |^2 \right] \qquad (20) \\ &= q(m+1)/m - q/m + 1 = q + 1. \end{aligned}$$

By Hypothesis III, the representation of no nontrivial character of G contains M in its kernel. By Corollary 2.4, this implies that any nontrivial nonexceptional character, when restricted to M, has ζ_1 as a constituent. Hence by the Frobenius reciprocity theorem, every nontrivial nonexceptional character is a constituent of ζ_1^*. By Lemma 3.5 there are at least q nontrivial nonexceptional characters. At least one exceptional character occurs as a constituent of ζ_1^*. Therefore (20) implies that $\varepsilon = 1$ and

$$\zeta_1^* = \chi_1 + \Gamma, \qquad (21)$$

where $(\chi_i, \Gamma) = 0$ for every exceptional character χ_i. Hence by Theorem 2, for $i \neq 0$,

$$\zeta_i^* = \chi_i + z_i \Gamma. \qquad (22)$$

It is easily seen that $\zeta_0^* = \sum_{i=0}^{q-1} \eta_i^*$. By (19) and Corollary 2.4, χ_1 cannot occur as a constituent of ζ_0^*. In view of this, (21), (22), and the Frobenius reciprocity theorem imply that for all y in M,

$$\chi_1(y) = \tilde{\zeta}_1(y); \qquad (23)$$

in particular

$$\chi_1(1) = q. \qquad (24)$$

Let χ_2 be an exceptional character associated with $\tilde{\zeta}_2$, where $\tilde{\zeta}_1 \neq \tilde{\zeta}_2$. Corollary 2.1 implies that $z_2 \chi_1 - \chi_2$ vanishes on elements not conjugate to an element of $M - \{1\}$. By (18), $\eta_i^* - 1$ vanishes on elements conjugate to an element of $M - \{1\}$; hence

$$(z_2 \chi_1 - \chi_2)(\eta_i^* - 1) = 0 \qquad \text{for } i = 1, \cdots, (q-1)/2. \qquad (25)$$

This leads to

$$z_2 \chi_1 \eta_i^* + \chi_2 = \chi_2 \eta_i^* + z_2 \chi_1. \qquad (26)$$

Hence χ_1 is a constituent of $\chi_1 \eta_i^*$. Therefore

$$\textstyle\sum_G \chi_1(x)\overline{\chi_1(x)}\eta_i^*(x) \neq 0; \qquad (27)$$

hence η_i^* is a constituent[10] of $\chi_1 \overline{\chi_1}$, for $i = 1, \cdots (q-1)/2$. Clearly χ_0 is a constituent of $\chi_1 \overline{\chi_1}$. Since by (18), $\eta_i^*(1) = m + 1$, (24) implies that

$$(28) \qquad q^2 = \chi_1(1)\overline{\chi_1(1)} \geqq 1 + \tfrac{1}{2}(q-1)(m+1).$$

Therefore $2(q + 1) \geqq m + 1$; hence $2q \geqq m - 1$, as was to be shown. This completes the proof of Theorem 1.

4. The case where G contains a normal subgroup of order $m + 1$

Let F be the field containing exactly 2^q elements. Let A_q denote the group of all transformations of F of the form $\omega \rightarrow a\omega^\tau + b$, where a, b are in F, $a \neq 0$, and τ is an automorphism of F. Let P_q denote the group of all transformations of the projective line over F of the form

$$\omega \rightarrow (a\omega^\tau + b)/(c\omega^\tau + d),$$

where a, b, c, d are in F, $ad - bc \neq 0$, τ is an automorphism of F, and $\infty^\tau = \infty$.[11]

LEMMA 4.1. *If q is a prime, then A_q considered as a permutation group on F satisfies Hypothesis I and contains a normal subgroup of order $2^q = m + 1$. Conversely, a permutation group which satisfies Hypothesis I and contains a normal subgroup of order $m + 1$ is either exactly doubly transitive or is isomorphic to A_q for some prime q. In the latter case, $m + 1 = 2^q$.*

Proof. Since A_q contains the affine group, it is certainly doubly transitive as a group of permutations of F. Suppose the mapping $\omega \rightarrow a\omega^\tau + b$ leaves three letters fixed; it may be assumed that 0, 1 are two of the fixed letters. Hence $a = 1$, $b = 0$, but then the fixed field of τ must contain at least three elements. Since q is a prime, this implies that F is the fixed field of τ; hence τ is the trivial automorphism. Therefore the transformation is the identity.

Suppose G satisfies Hypothesis I, is not exactly doubly transitive, and contains a normal subgroup H of order $m + 1$. By Lemma 3.1, G satisfies Hypothesis II. If m is even, a Sylow 2-subgroup of M contains a unique element of order two [4, p. 335] since MH is a Frobenius group. By conditions (i), (ii), (iii) of Hypothesis II, M is nilpotent ([5], [7], [9]); therefore M contains a unique element of order two which must necessarily be in the center of $N(M)$, contradicting condition (i) of Hypothesis II. Therefore m is odd, M is nilpotent, and every Sylow subgroup of M is cyclic [4, p. 335]; hence M is cyclic. Therefore the near field F associated to MH is a field containing $m + 1$ elements (see [11]); hence $m + 1 = 2^\alpha$ since $m + 1$ is even. The group Q acts as a group of automorphisms on MH, none of which can leave more than two elements fixed by Lemma 3.1. This can be interpreted as a group of automorphisms of the field F. Since the fixed field of no nontrivial automorphism can contain more than two elements, it follows that q is a prime,

[10] An argument of this type was first used by R. Brauer in [1, p. 426].

[11] A_q is the automorphism group of the one-dimensional affine group over F; P_q is the automorphism group of $PSL(2, 2^q)$.

and F contains 2^q elements. It is now easily verified that G is isomorphic to A_q.

LEMMA 4.2. *If q is a prime, then P_q considered as a permutation group on the projective line over F is triply transitive, and no nontrivial permutation leaves four letters fixed. Conversely, a triply transitive permutation group G on $m + 2$ letters in which no nontrivial permutation leaves four letters fixed, and in which the subgroup G_1, consisting of those permutations leaving a given letter fixed, contains a normal subgroup of order $m + 1$, is either exactly triply transitive or is isomorphic to P_q for some prime q.*

Proof. Since P_q contains the projective linear group over F, it is triply transitive. The subgroup of P_q, consisting of those permutations leaving ∞ fixed, is A_q. Hence by Lemma 4.1 no nontrivial permutation in P_q leaves four letters fixed.

Conversely, by Lemma 4.1, G_1 is isomorphic to A_q for some prime q. Thus G can be considered as a permutation group on the projective line over F, where A_q is the subgroup consisting of those permutations which leave ∞ fixed. The order of G is $g = q(2^q - 1)2^q(2^q + 1)$, where q is a prime. If $q = 2$, then G and P_2 are both isomorphic to the symmetric group on five letters, and the result is clearly true. Hence it may be assumed that q is odd.

G contains a permutation σ with the property that $\sigma(0) = \infty$, $\sigma(\infty) = 0$, $\sigma(1) = 1$. Since no element of G of even order leaves three letters fixed, σ^2 has odd order. Hence some power of σ has order two and acts the same way as σ on $0, 1, \infty$. Therefore it may be assumed that $\sigma^2 = 1$. By checking the values $\omega = 0, 1, \infty$, it is easily seen that

$$\sigma(a\omega^{\tau} + b) + c = \sigma(a'\omega^{\tau'} + b') + c'$$

only if $a = a'$, $b = b'$, $c = c'$, $\tau = \tau'$. Hence the transformations which send ω into $a\omega^{\tau} + b$ or $\sigma(a\omega^{\tau} + b) + c$ are all distinct. It is easily seen that there are $q(2^q - 1)2^q2^q + q(2^q - 1)2^q = g$ of these. Consequently every permutation in G is of one of these types.

The Sylow 2-group of A_q has order $m + 1 = 2^q$ and is a Sylow 2-group of G. Hence no permutation in G of order two leaves more than one letter fixed. Therefore $\sigma(\omega) \neq \omega$ unles $\omega = 1$.

Let γ be a primitive element of the field F; the mapping which sends ω into $\gamma\sigma(\omega)$ is in G; hence $\gamma\sigma(\omega) = \sigma(a\omega^{\tau} + b) + c$ for some a, b, c, τ. By setting $\omega = 0, \infty$, we get that $b = c = 0$; hence $\gamma\sigma(\omega) = \sigma(a\omega^{\tau})$. Let $\omega = 1$; then $\gamma = \sigma(a)$; hence $a = \sigma(\gamma)$. Repeated application of this relation yields that

$$\sigma(aa^{\tau} \cdots a^{\tau^{q-1}}) = \gamma\sigma(aa^{\tau} \cdots a^{\tau^{q-2}}) = \cdots = \gamma^q.$$

If $\tau \neq 1$, $aa^{\tau} \cdots a^{\tau^{q-1}}$ is a nonzero element of F which is a norm; therefore it must be 1; hence $\gamma^q = \sigma(1) = 1$, which is impossible by the choice of γ. Thus $\tau = 1$, $\gamma\sigma(\omega) = \sigma(a\omega)$. Repeated application of this identity yields that $\sigma(a^k\omega) = \gamma^k\sigma(\omega)$, for all integers k, where ω is any element in F. Consequently σ induces an automorphism of order two on the multiplicative group of the field F which leaves only 1 fixed. Therefore $\sigma(\omega) = \omega^{-1}$ for all ω in F. It is now an easy matter to verify that G contains the projective linear group over F; hence G contains P_q. Since P_q has the same order as G, this implies that $G = P_q$.

THEOREM 3. *Let G be a permutation group of order $g = qm(m + 1)$ which satisfies Hypothesis I. Suppose $q > 1$ and G contains a normal subgroup of order $m + 1$; then q is prime, and G is isomorphic to A_σ. If G is the subgroup of a k-tuply transitive permutation group K on $m + k - 1$ letters, consisting of those permutations which leave a given set of $k - 2$ letters fixed, then either K is the symmetric group, or $k = 2$ or 3 and K is isomorphic to A_q or P_q.*

Proof. By Lemmas 4.1 and 4.2 only the case $k \geqq 4$ needs to be considered. If $q = 2$, then G is the symmetric group on four letters; hence $m = 3$, and K is the symmetric group on $k + 2$ letters. If q is odd, then it follows from a theorem of M. Hall [6] that $k \leqq 3$.

BIBLIOGRAPHY

1. R. BRAUER, *On groups whose order contains a prime number to the first power II*, Amer. J. Math., vol. 64 (1942), pp. 421–440.
2. R. BRAUER AND K. A. FOWLER, *On groups of even order*, Ann. of Math. (2), vol. 62 (1955), pp. 565–583.
3. R. BRAUER, M. SUZUKI, AND G. E. WALL, *A characterization of the one-dimensional unimodular projective groups over finite fields*, Illinois J. Math., vol. 2 (1958), pp. 718–745.
4. W. BURNSIDE, *Theory of groups of finite order*, 2nd ed., Cambridge, 1911.
5. W. FEIT, *On the structure of Frobenius groups*, Canadian J. Math., vol. 9 (1957), pp. 587–596.
6. M. HALL, JR., *On a theorem of Jordan*, Pacific J. Math., vol. 4 (1954), pp. 219–226.
7. G. HIGMAN, *Groups and rings having automorphisms without non-trivial fixed elements*, J. London Math. Soc., vol. 32 (1957), pp. 321–334.
8. M. SUZUKI, *On finite groups with cyclic Sylow subgroups for all odd primes*, Amer. J. Math., vol. 77 (1955), pp. 657–691.
9. JOHN G. THOMPSON, *Finite groups with fixed-point-free automorphisms of prime order*, Proc. Nat. Acad. Sci. U.S.A., vol. 45 (1959), pp. 578–581.
10. H. ZASSENHAUS, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg, vol. 11 (1936), pp. 17–40.
11. ———, *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg, vol. 11 (1936), pp. 187–220.

CORNELL UNIVERSITY
ITHACA, NEW YORK
THE INSTITUTE FOR ADVANCED STUDY
PRINCETON, NEW JERSEY