GROUPS WITH ONLY THE IDENTITY FIXING THREE LETTERS

Thesis by

Gordon Ernest Keller

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1965

(Submitted April 5, 1965)

ACKNOWLEDGEMENTS

I would like to thank Professor Marshall Hall Jr. for the instruction and guidance he has given me, especially in the preparation of this thesis.

I am also indebted to Professor E. C. Dade for many helpful discussions.

Finally I wish to acknowledge the financial assistance made available to me by the National Defense Education Act and the California Institute of Technology.

ABSTRACT

In this paper, we study finite transitive permutation groups in which only the identity fixes as many as three letters, and in which the subgroup fixing a letter is self normalizing. If G is such a group, the principal results concern the case when G is simple.

In this case, H, the subgroup fixing a letter, is a Frobenius group, MQ, with kernel M and complement Q. If $|H|$ is even we show that either G is doubly transitive or permutation isomorphic to the representation of A_5 on ten letters.

If $|H|$ is odd we prove that Q is cyclic, M is a p-group, and G has a single class of involutions. Furthermore, the number of groups for which H has a given positive number of regular orbits is finite.

I. INTRODUCTION

In recent years modern techniques have made it possible to determine all finite simple groups which satisfy some elementary set of conditions. One example of such a result is the determination of all simple permutation groups G satisfying:

(1) G is doubly transitive;

(2) Only the identity element of G fixes as many as three letters.

It is well known that the linear fractional groups $LF(2, q)$, where q is a prime power, have doubly transitive permutation representations such that only the identity fixes as many as three letters. It was felt for some time that these were the only simple groups satisfying (1) and (2). Indeed, the work of Zassenhaus [17], and Feit [4], demonstrated that under fairly general assumptions this is true.

However, Suzuki [11] found another class of simple groups satisfying (1) and (2), and his work [13], together with that of Ito [8], completed the study, showing that other than the linear fractional groups the only simple groups satisfying (1) and (2) are the Suzuki groups.

Since solution of this problem produced a new class of simple groups there has been considerable interest in finding all simple groups satisfying a weaker set of hypotheses. Suzuki [14], and Ree [9], have pursued such a course, retaining (1) and weakening (2) appropriately.

It is the purpose of this thesis to study permutation groups G satisfying:

(1') G is transitive and the subgroup fixing a letter is self normalizing;

(2) Only the identity element of G fixes as many as three letters.

If a group G satisfying (1') and (2) has a regular normal subgroup, it is easily demonstrated that G is either Frobenius or at least solvable with a quite elementary structure. If G has no regular normal subgroup the problem is quickly reduced to the study of a simple group satisfying (1') and (2).

In this case the subgroup of G fixing a letter is a Frobenius group MQ of order mq, with kernel M and complement Q. If mq is even it is easily shown that G is either doubly transitive, or G is permutation isomorphic to the representation of A_5 on ten letters.

Thus the major portion of our effort is spent in analyzing the case when G is simple and mq is odd. In this case we prove that Q is cyclic and M is a p-group. Furthermore, G has a single class of involutions.

Finally, for any fixed positive integer β, there are only finitely many groups G, satisfying (1') and (2) for which MQ has β regular orbits.

We shall now give a more detailed account of our approach to the problem. Section II will be devoted to indicating the notation which we will use throughout the paper.

In section III we derive some general properties of groups satisfying (1') and (2), and we show what happens when such groups have a regular normal subgroup. We show that in this case G is either Frobenius or has a regular normal 2-subgroup and the subgroup of G fixing a letter is a meta-cyclic Frobenius group.

In section IV we count involutions, as Suzuki does in [12], to show that if G has no regular normal subgroups, and mq is even, then G is either doubly transitive or is permutation isomorphic with the representation of A_5 on ten letters.

The purpose of section V is to reduce our work, in the case when mq is odd, to the study of a simple group. We accomplish this by showing that G is either simple or has a Hall normal subgroup N which is simple. N satisfies (1') and (2), and G/N is cyclic or meta-cyclic.

If G is a simple group satisfying (1') and (2) with mq odd, we show in section V that Q is cyclic and has a dihedral normalizer of order 2q.

This structure is used in section VI to ascertain some information about the characters of G. The information obtained in this section is then used to find certain coefficients of the class algebra in section VII. Using these coefficients we prove that G has a single class of involutions.

In section VIII, employing the work of Feit [5] on exceptional characters, we prove that M must be a p-group. Hence, to a large extent, any group satisfying (1') and (2) has very similar properties to a group satisfying (1) and (2).

If a simple group G satisfying (1') and (2), with mq odd, is not doubly transitive, it has $\beta > 0$ regular orbits. In section IX we use the results we have obtained about characters of G to prove that there are only finitely many such groups for a fixed integer $\beta > 0$.

II. NOTATION

Throughout the course of this paper the notation used will be standard in most cases, and can be found in Hall [7] or Curtis and Reiner [3].

A few notations which we will use that are not quite so standard are: $S^{\#}$ for the set of group elements S with the identity deleted; $H^x = x^{-1}Hx$; $|S|$ for the number of elements in S; and $<S>$ for the subgroup generated by S, a subset of a group.

If G is a group and H a subgroup of G we write $\chi|^G$ for the character of G induced by a character χ of H. If G is the group under investigation we write $\chi^* = \chi|^G$. If N is the normalizer of H we write $\tilde{\chi} = \chi|^N$.

If χ is any character of the group G we write χ_H for the restriction of χ to H. All characters and representations of G are assumed to be over the complex numbers.

If χ_1, χ_2 are characters of G,

$$(\chi_1, \chi_2) = \frac{1}{|G|} \sum_{x \in G} \chi_1(x)\overline{\chi_2(x)}$$

denotes the scalar product of χ_1 and χ_2.

Finally, if G is a permutation group and x is an element of G, then we use the functional notation $x(i)$ to indicate the image of the point i under x.

Any other notation which is not standard will be defined in the text itself.

III. GENERAL PROPERTIES

In this section we derive a few elementary properties of groups satisfying (1') and (2). These properties include results on the structure of the subgroup fixing a letter and the distribution of involutions in the cosets of certain subgroups. We also give a brief analysis of groups which satisfy (1') and (2) and have a regular normal subgroup. The results obtained here are not exhaustive but include only observations both simply obtained and necessary in the sequel.

We establish some notation which will be used throughout the thesis by formulating an assumption.

Definition 3.1. A finite group G is said to satisfy (A1) if

(i) G is a permutation group on the set $\{1, 2, \ldots, n\}$, where $n > 1$;

(ii) H is the subgroup fixing 1;

(iii) G satisfies (1') and (2).

Our first theorem is a general theorem on permutation groups in which only the identity fixes as many as two letters. We will apply the results to H.

Theorem 3.2. If X is any permutation group in which only the identity fixes as many as two letters, then there is at most one orbit on which X is not regular. If such an orbit exists, it either consists of a single letter, or X is faithfully represented on it as a Frobenius group.

Proof. Suppose O is an orbit of X containing more than one letter, on which X is not regular. Certainly 1 is the only permutation of X fixing as many as two letters in O. Since X is not regular on O it must therefore be represented as a Frobenius group on O. Since O contains more than one letter, and only 1 fixes as many as two letters, X is represented faithfully on O.

Suppose O and O' are two orbits of X on which X is not regular. If either one contains just one letter any element of $X^{\#}$ fixing a letter of the other orbit fixes two letters. This is impossible. Therefore X is represented faithfully as a Frobenius group on both O and O'. The Frobenius kernel K of X is uniquely determined by any faithful Frobenius representation of X. If x is any element in X but not in K, x fixes a letter in O and O'. This is again a contradiction and the theorem is proved.

Corollary 3.3. If G is a group satisfying (A1) then either G is Frobenius or H has exactly one orbit $O \neq \{1\}$ on which it is represented faithfully as a Frobenius group. On any other orbit different from $\{1\}$, H is regular.

Proof. As a permutation group on $\{2, 3, \ldots, n\}$, H satisfies the hypothesis of the theorem. Hence there is at most one orbit of H in $\{2, 3, \ldots, n\}$ on which H is not regular. If H is regular on every orbit then either $H = 1$ or G is Frobenius. Since $N(H) = H$, $H = 1$ implies $G = 1$ which we ruled out by assuming G was a transitive group on $n > 1$ letters. Thus H has exactly one orbit different from $\{1\}$ on which it is not regular. If this orbit consisted of a single letter, say i, then any element x with $x(1) = i$ normalizes H. This contradicts the fact that $N(H) = H$. Therefore H has exactly one orbit $O \neq \{1\}$ on which H is not regular, and on this orbit H is represented faithfully as a Frobenius group. This completes the proof.

We now give a brief analysis of groups satisfying (A1) which have regular normal subgroups.

Theorem 3.4. If G is a group satisfying (A1) and G has a regular normal subgroup R, either G is Frobenius or R is a 2-group and H is a meta-cyclic Frobenius group.

Proof. Suppose G is not Frobenius. Then by Corollary 3.3, H has exactly one orbit on which it is represented faithfully as a Frobenius group. Let M be the Frobenius kernel of H and Q its complement. Obviously the elements of $M^{\#}$ fix only the letter 1. Hence MR is a Frobenius group with kernel R. By a theorem of Thompson [16], the kernel of a Frobenius group is nilpotent. Hence both M and R are nilpotent groups.

Now suppose p is a prime dividing the order of R, and P is a Sylow p-subgroup of R. P is characteristic in R and hence normal in G. Q normalizes MP. If Q centralizes no element of $P^{\#}$ then Q clearly acts as a fixed point free automorphism group on MP under conjugation. Thus MP is nilpotent, contradicting the fact that MP is Frobenius. Hence some element in $P^{\#}$ centralizes Q.

Any element of $Q^{\#}$ fixes 1 and a letter in the Frobenius orbit of H. Any element in $P^{\#}$ centralizing Q must interchange these two letters and thus have order divisible by 2. Hence $p = 2$ and R is a 2-group.

It is well known that in a Frobenius group the complement has cyclic Sylow p-subgroups for odd primes p and either a cyclic, quaternion or generalized quaternion 2-subgroup. A proof can be constructed using [2], section 248, where it is proved that every subgroup of order p^2 is cyclic for any prime p, and [7], Theorem 12.5.2.

Since M is nilpotent and the complement in the Frobenius group MR, M is cyclic. This follows since $|M|$ must be odd and so M is the direct product of cyclic Sylow subgroups. Since M is cyclic Q is abelian. Therefore the Sylow subgroups of Q are cyclic since it is the complement of M in H. Therefore Q is cyclic and the theorem is proved.

We note that groups satisfying these conditions do exist. Consider all semi-linear transformations $ax^{\sigma} + b$ on the field with 2^{11} elements, where $a \neq 0$ and σ is any automorphism of the field. As a permutation group on the elements of the field it is easily seen that this group satisfies (A1). If we restrict a to the multiplicative subgroup of order 23, we get a group satisfying (A1) which is not doubly transitive.

In the remainder of this paper we assume that G has no regular normal subgroup. In this case Corollary 3.3 implies that

H has exactly one orbit on which it is represented faithfully as a Frobenius group.

Definition 3.5. A group G is said to satisfy (A2) if

(i) G satisfies (A1);

(ii) G has no regular normal subgroup;

(iii) H is represented faithfully as a Frobenius group on $\{2, 3, \ldots, m+1\}$;

(iv) M is the Frobenius kernel of H and has order m;

(v) Q is the subgroup of H fixing 2 and has order q;

(vi) There are β orbits of H on which H is regular, where $\beta \neq 0$.

We have assumed $\beta \neq 0$ since the case in which G is doubly transitive was completely characterized previously. We mentioned the results in the introduction.

We gather some results on M, the Frobenius kernel of H, in the form of a lemma.

Lemma 3.6. If G satisfies (A2) then

(i) The elements of $M^{\#}$ fix only the letter 1;

(ii) $N(M) = H$;

(iii) $M \cap M^{x} = 1$ if x is in G but not in H;

(iv) M is a Hall subgroup of G.

Proof. (i) is clear, since M is regular on every orbit different from $\{1\}$. By (i), any element of G normalizing M must fix 1, and therefore must belong to H. Since M is normal in H we have (ii). Suppose x is in G but not in H. Any element of $M \cap M^x$ fixes 1 and $x(1)$. By (i) the only such element is 1. Hence (iii) is established. Now $|G| = nmq$. Since M is regular on every orbit different from $\{1\}$, $n \equiv 1 \pmod{m}$. Since H is Frobenius with kernel M and complement Q, $m \equiv 1 \pmod{q}$. Therefore $(m, nq) = 1$, and M is a Hall subgroup of G. This proves (iv) and completes the lemma.

In [1], Brauer and Fowler showed that much could be learned about groups of even order by careful consideration of the elements of order two. Suzuki also demonstrated the significance of such elements in his work on ZT-groups and CN-groups in [12]. Here we prove two lemmas which are much the same as lemmas used by Suzuki.

Definition 3.7. If $x \neq 1$ is a group element such that $x^2 = 1$ we call x an involution. If S is a subset of a finite group G, then by $\nu(S)$ we mean the number of involutions in S.

Lemma 3.8. Let G be a finite group satisfying (A2). Then

$$\nu(G) \leq \nu(H) + (n-1)q .$$

Proof. Let Mx be a coset of M in G such that $Mx \not\subseteq H$. Suppose s and t are involutions in Mx. $x(1) \neq 1$, since x is not in H. Since s and t are in the same coset of M they are in the same coset of H. Therefore s and t both interchange 1 and $x(1)$.

Therefore st fixes two letters and is in M. Thus $st = 1$ by Lemma 3.6 (i). So $s = t$. Therefore we have $\nu(Mx) \leq 1$ for $Mx \not\subseteq H$. There are $(n-1)q$ such cosets of M in G. Hence $\nu(G) \leq \nu(H) + (n-1)q$, as was asserted.

Lemma 3.9. Let G be a finite group satisfying (A2). Then if $x(1) > m+1$, $\nu(Hx) \leq 1$. Furthermore

$$\nu(G) \leq \nu(M) + (\beta+1)mq \ .$$

Proof. Let x be any element such that $x(1) > m+1$. By Corollary 3.3 the subgroup of H fixing $x(1)$ is trivial. If s and t are involutions in Hx, their product fixes x and $x(1)$ and hence must be 1. Therefore $s = t$ and $\nu(Hx) \leq 1$ as asserted.

Since Hx is the union of q cosets of M in G, and since these cosets are not in H for $Hx \neq H$, we have for such cosets $\nu(Hx) \leq q$ by Lemma 3.8.

There are m cosets of H corresponding to the Frobenius orbit of H. There are βmq whose coset representatives satisfy $x(1) > m+1$. Hence

$$\nu(G) \leq \nu(M) + mq + \beta mq = \nu(M) + (\beta+1)mq \ .$$

This completes the proof.

IV. ON GROUPS SATISFYING (A2) FOR WHICH $|H|$ IS EVEN

In this section we prove the following theorem:

Theorem 4.1. If G is a group satisfying (A2) and mq is even then $G = A_5$. The representation of A_5 obtained is of degree 10 over a Frobenius subgroup of order 6.

Proof. The proof will be divided into two parts. We first will suppose that m is even and arrive at a contradiction. Then under the hypothesis that q is even we show that G is A_5. The case where m is even could be eliminated by applying Theorem 1 of [15]. However we give a proof here as the details simplify in our situation.

Case 1. Suppose m is even.

By Lemma 3.6, M is a Hall subgroup of G and thus contains a Sylow 2-subgroup of G. Hence every involution occurs in some conjugate of M. By Lemma 3.6 (iii), no involution occurs in two distinct conjugates of M, and since M has n conjugates we get $\nu(G) = n\nu(M)$. Since H is Frobenius with kernel M, every involution in H is in M and so $\nu(H) = \nu(M)$. Therefore, by Lemma 3.8

$$n\nu(H) \leq \nu(H) + (n-1)q$$

from which we get immediately $\nu(H) \leq q$. Since the action of Q on M under conjugation is fixed point free, M must have at least q involutions and so $\nu(H) = q$. Thus $\nu(G) = nq$. By Lemma 3.9 we have

$$nq \leq q + (\beta + 1)mq$$

from which we get immediately

$$n \leq 1 + (\beta + 1)m = 1 + m + \beta m.$$

But

$$n = 1 + m + \beta mq$$

which is contradictory since $\beta \neq 0$ and $q \neq 1$.

Case 2. Suppose q is even.

Then Q contains an involution y. Since y fixes only 1 and 2, any element centralizing y must fix or interchange 1 and 2. Since the product of any two elements interchanging 1 and 2 fixes them there are just two cosets of $C(y) \cap Q$ in $C(y)$ and so $|C(y)| \leq 2q$. Thus we have

$$\nu(G) \geq \frac{mnq}{|C(y)|} \geq \frac{mn}{2} . \tag{4.2}$$

Since H is a Frobenius group any involution in Q has a fixed point free action on M under conjugation. It is well known that any involution in Q must take every element of M into its inverse under conjugation. Hence y is the only involution in Q. It is then obvious that the involutions of H are precisely the elements of the coset My in H and therefore $\nu(H) = m$.

Applying Lemma 3.5 we get

$$\nu(G) \leq m + (n-1)q .$$

Thus by (4.2) we have

$$\frac{mn}{2} \leq m + (n-1)q \, .$$

Therefore

$$m - \frac{m}{n-1} \leq 2q \, .$$

Since $\beta \neq 0$, $m < n - 1$. Therefore $2q > m - 1$, and hence $2q > m$ since m is odd. But since Q has a fixed point free action on M under conjugation, $m \equiv 1 \pmod{q}$. Therefore $q = m - 1$.

Substituting $m - 1$ for q and m for $\nu(H)$ in Lemma 3.9 we get

$$\nu(G) \leq m + (\beta+1)m(m-1) \, .$$

Now $n = 1 + m + \beta mq = 1 + m + \beta m(m-1)$, and $\nu(G) \geq \frac{mn}{2}$. Thus we have

$$\frac{m}{2}\left[1 + m + \beta m(m-1)\right] \leq m + (\beta+1)m(m-1) \, .$$

Multiplying on both sides by $\frac{2}{m}$ and subtracting 2 we get

$$m - 1 + \beta m(m-1) \leq 2(\beta+1)(m-1) \, .$$

Dividing both sides by $(m-1)\beta$ we get

$$\frac{1}{\beta} + m \leq 2 + \frac{1}{\beta} \, ,$$

or

$$m \leq 2 + \frac{1}{\beta} \, .$$

Now m is odd and not 1 so $m = 3$ and $\beta = 1$. This gives $q = m - 1 = 2$, and $n = 1 + m + \beta mq = 10$. Therefore $|G|$ is 60. H is the normalizer of M, the Sylow 3-subgroup of G. If K is a subgroup of G containing H, $[K:H] \equiv 1 \pmod 3$. Hence G is the only subgroup properly containing H and therefore H is maximal. Thus G is a primitive group. Since the degree is not a prime power, G is not solvable. Since $|G| = 60$, this implies $G = A_5$.

To complete the proof we need only show that A_5 has a representation of the desired type on 10 letters.

Consider the set $S = \{1, 2, 3, 4, 5\}$. Let K be the set of all subsets of S with two elements. A_5 is represented as a permutation group on K by $x(\{a, b\}) = \{x(a), x(b)\}$, where x is any element of A_5 and $\{a, b\}$ is any element in K. This representation is certainly transitive since A_5 is doubly transitive on five letters. The subgroup fixing $\{1, 2\}$ is 1, (345), (354), (12) (34), (12) (35), and (12) (45). It is easily seen that only 1 fixes three elements of K. The representation is on 10 letters and is not doubly transitive since $9 \nmid 60$. It is easily seen that the subgroup fixing $\{1, 2\}$ is self-normalizing.

Thus we have shown that precisely one group exists satisfying (A2) when mq is even.

V. GROUPS SATISFYING (A2) WHEN $|H|$ IS ODD

In the last section we proved that if G is a group satisfying (A2), and $|H|$ is even, then G is A_5. In this section we begin to study the case when $|H|$ is odd. We will show that although G may not be simple, G has a Hall normal subgroup N which is simple and G/N is either cyclic or meta-cyclic. Furthermore we show that N satisfies (A2). On the basis of this result we then restrict our attention to simple groups satisfying (A2).

Lemma 5.1. There exists an involution ω normalizing Q and $|N(Q)| = 2q$.

Proof. Let P be a Sylow p-subgroup of Q for some prime p dividing q. Since $(m, q) = 1$, P is a Sylow p-subgroup of H. Each element of $P^{\#}$ fixes precisely the letters 1 and 2. By [7], Theorem 5.7.1, $N(P)$ must be transitive on $\{1, 2\}$. Therefore, there exists an element interchanging 1 and 2, and normalizing P. This element is obviously of even order, and therefore some power of it must be an involution. Let this involution be called ω. ω must interchange 1 and 2 since q is odd.

Now ω normalizes Q since Q consists of all permutations fixing 1 and 2. Furthermore, any permutation normalizing Q must fix or interchange 1 and 2, and therefore must belong to Q or $Q\omega$. This completes the lemma.

Since Q acts as a fixed point free automorphism group on

M, and q is odd, Q has cyclic Sylow p-subgroups for every prime p dividing q.

Thus N(Q) has cyclic Sylow p-subgroups for every prime p dividing its order. By Theorem 11, p. 175 of [18], N(Q) = AB, where A and B are cyclic, $(|A|, |B|) = 1$, $A \cap B = 1$, and A is the derived group of N(Q). Now since N(Q)/Q is abelian, $2 \mid |B|$.

We can now prove the results promised at the beginning of this section.

Theorem 5.2. If G is a group satisfying (A2), G has a normal subgroup N satisfying (A2) such that N is a Hall subgroup of G, G/N is cyclic or meta-cyclic, and $C_{N \cap Q}(\omega) = 1$.

Proof. Let $P_1, P_2, \ldots, P_j$ be the Sylow subgroups of B for all odd primes dividing the order of B.

Since every element of $Q^{\#}$ fixes just the letters 1 and 2, $n \equiv 2 \pmod q$. Since Q is odd $(n, q) = 1$. Hence m, n, and q are pair-wise relatively prime. Since $(|A|, |B|) = 1$, P_i is a Sylow p_i-subgroup of G for $i = 1, 2, \ldots, j$. Any element of G which normalizes P_i is in N(Q). Any element in N(Q) which normalizes P_i must centralize it. Hence by Burnside's Theorem, Theorem 14.3.1 of [7], P_i has a normal complement T_i for $i = 1, 2, \ldots, j$.

Let $T = \bigcap_{i=1}^{j} T_i$. Then $T \cap N(Q) = A \cdot \langle \omega \rangle$.

Now let $P_{j+1}, P_{j+2}, \ldots, P_{j+k}$ be the Sylow subgroups of A centralized by ω. By applying Burnside's Theorem again, we get

P_{j+i} has a normal complement T_{j+i} in T for $i = 1, 2, \ldots, k$. Since T_i is a Hall subgroup for every i, $T_{j+1}, T_{j+2}, \ldots, T_{j+k}$ are characteristic in T and hence normal in G.

Let $N = \bigcap_{i=1}^{j+k} T_i$. N is clearly a normal Hall subgroup of G such that G/N is cyclic or meta-cyclic.

Clearly $[G:N] = [Q:N \cap Q]$ so that a system of coset representatives for $N \cap Q$ in Q is a system of coset representatives for N in G. Such a system of coset representatives must permute the orbits of N transitively. But since each representative is in Q it fixes 1 and therefore the orbit of N containing 1. Hence N is transitive. Certainly 1 is the only element of N fixing as many as three letters. If N had a regular normal subgroup it would be a Hall subgroup and hence characteristic. Therefore it would be a regular normal subgroup of G which is impossible. Since N must contain M, $N \cap H$ is self-normalizing. Therefore N satisfies (A2). Since N has no regular normal subgroup, $N \cap Q \neq 1$. Also, $C_{N \cap Q}(\omega) = 1$.

Corollary 5.3. $N \cap Q$ is cyclic and ω carries every element of $N \cap Q$ into its inverse under conjugation.

Proof. This follows immediately from the fact that $C_{N \cap Q}(\omega) = 1$.

Theorem 5.4. If G is a group satisfying (A2), and if there exists an involution ω in $N(Q)$ carrying every element of Q into its inverse under conjugation, then G is simple.

Proof. Let $S \neq 1$ be a maximal normal subgroup of G. We assert that $S \cap H \neq 1$. If $S \cap H = 1$, MS is represented as a Frobenius group on the orbit of S containing 1. Every element of MS is in S or some conjugate of M. Q normalizes SM and if Q centralizes no element of $S^{\#}$ it clearly acts fixed point free on SM under conjugation. This would imply SM is nilpotent by Thompson [16], which is impossible since SM is Frobenius. Hence Q centralizes a non-identity element of S. Such an element must interchange 1 and 2 since it normalizes Q. By Lemma 5.1 and the hypothesis that an involution ω exists carrying every element of Q into its inverse, $N(Q)$ is dihedral and no involution in $N(Q)$ centralizes an element of $Q^{\#}$. The contradiction implies that $S \cap H \neq 1$.

We now assert that $S \cap M \neq 1$. If $S \cap Q = 1$ then $S \cap Q^{x} = 1$ for every x in G because S is normal in G. Since $S \cap H \neq 1$, this implies $S \cap M \neq 1$. If $S \cap Q \neq 1$ let y be an element of $S \cap Q^{\#}$ and x be an element of $M^{\#}$. Clearly $y^{-1}y^{x}$ is in $M^{\#}$ and in S. Hence, $S \cap M \neq 1$.

Let $S \cap M = D$. Since S is normal in G, and $H = N(M)$, $H \subseteq N(D)$. Since $M \cap M^{x} = 1$ if x is not in H, $H = N(D)$. Hence D has n conjugates in G, all of which are in S since S is normal. The number of subgroups conjugate to D in S is $[S:N_S(D)] = [S:S \cap H]$. This number is a divisor of n and hence prime to mq. If D^{x} is any conjugate of D in G, it permutes the conjugates of D in S. Since $|D^{x}|$ does not divide $[S:S \cap H]$, some element $\mu \neq 1$

in D^x normalizes a conjugate of D in S. Since the only conjugate of D in G which is normalized by μ is D^x, D^x is conjugate to D in S. Hence all n conjugates of D in G are conjugate in S. If D^x is the conjugate of D in G which fixes i, then there must be an element of G in S taking 1 to i. Hence we have shown that S is transitive.

Since S is transitive $G = HS$. Therefore,

$$G/S = (HS)/S \cong H/H \cap S .$$

Since G/S is simple $H/H \cap S$ is simple. Hence $M \subseteq H \cap S$, and $H/H \cap S$ must be cyclic of prime order p, where p divides q. Let v be a generator of Q, which is cyclic since $N(Q)$ is dihedral. Clearly $Sv \neq S$. Since p is odd $S\omega S\omega = S$ implies ω is in S. Since $SvS = Sv$, $\omega v \omega = v^{-1}$ is in Sv. Hence $SvSv = SvSv^{-1} = S$, contradicting the fact that G/S is of odd order.

Hence, G has no maximal normal subgroup different from 1, and is therefore simple.

Corollary 5.5. If G is a group satisfying (A2) then G has a Hall normal subgroup N, such that N is simple and G/N is cyclic or meta-cyclic.

Proof. Let N be the subgroup of G constructed in Theorem 5.2. By Theorem 5.2 and Corollary 5.3 N satisfies the hypothesis of Theorem 5.4. Hence N is simple. The other conclusions of the corollary follow from Theorem 5.2.

In the remainder of this paper we consider groups satisfying a new assumption based on the work of this section.

Definition 5.5. A group G is said to satisfy (A3) provided

(i) G satisfies (A2);

(ii) mq is odd;

(iii) G is simple;

(iv) ω is an involution normalizing Q and mapping every element of Q onto its inverse under conjugation;

(v) $L = N(Q)$ is a dihedral group of order $2q$.

VI. ON EXCEPTIONAL CHARACTERS OF G ASSOCIATED WITH Q

In this section we begin a study of the characters of G. The work in the remainder of this paper will make considerable use of a theorem due to Feit [5].

Theorem 6.1 (Feit) Let G be a finite group and let X be a subgroup of G satisfying the following hypotheses

(i) If $x \in X^{\#}$, $C(x) \subseteq X$;

(ii) $X \cap X^y = 1$ if y is in G but not in $N(X)$;

(iii) $X \neq N(X) \neq G$;

(iv) $[N(X):X] \neq |X| - 1$;

(v) X is not a non-abelian p-group with $[X:X'] < 4[N(X):X]^2$.

Let $\zeta_o = 1, \zeta_1, \dots, \zeta_k$ be all the irreducible characters of X, and let $\zeta_i(1) = z_i$. Let the character of $N(X)$, G induced by ζ_i be denoted by $\tilde{\zeta}_i, \zeta_i^*$ respectively. Let $[N(X):X] = w$.

Then the notation can be chosen so that $\tilde{\zeta}_1, \tilde{\zeta}_2, \dots, \tilde{\zeta}_{k/w}$ are distinct irreducible characters of $N(X)$ and $\zeta_1^*, \zeta_2^*, \dots, \zeta_{k/w}^*$ are distinct characters of G.

Also, $\frac{k}{w} > 1$ and there exist irreducible characters $\chi_1, \chi_2, \dots, \chi_{k/w}$ of G and a sign $\epsilon = \pm 1$ such that

$$z_j \zeta_i^* - z_i \zeta_j^* = \epsilon (z_j \chi_i - z_i \chi_j)$$

for $0 < i, j \leq \frac{k}{w}$.

Finally there exists a rational integer c, such that

$$\chi_i(x) = \epsilon\tilde{\zeta}_i(x) + z_i c$$

for any x in $X^{\#}$, $0 < i \leq \frac{k}{w}$. If χ is an irreducible character of G distinct from $\chi_1, \chi_2, \ldots, \chi_{k/w}$, then the restriction of χ to $X^{\#}$ is a constant.

Definition 6.2. The characters $\chi_1, \chi_2, \ldots, \chi_{k/w}$ constructed in Theorem 6.1 are called the exceptional characters of G associated with X.

As the title indicates, in this section we construct the collection of exceptional characters of G associated with Q. In addition we find another character of G which is closely related to these exceptional characters. Other than this family of characters and the trivial character, every other irreducible character of G will be shown to vanish on $Q^{\#}$ and have degree divisible by q. This will allow us to calculate certain coefficients of the class algebra in the next section.

Throughout this section we assume G satisfies (A3).

Lemma 6.3. Q satisfies the hypotheses of Theorem 6.1.

Any element of G centralizing an element of $Q^{\#}$ must either fix or interchange 1 and 2. Any such element normalizes Q and is in L. Since L is dihedral of order $2q$, $C_L(x) = Q$ if x is in $Q^{\#}$. Hence Q satisfies (i).

If $x \notin L$ the set $\{1, 2, x(1), x(2)\}$ contains at least three distinct elements. Every element of Q fixes 1 and 2. Every element of Q^x fixes $x(1)$ and $x(2)$. Since only the identity fixes as many as three letters, $Q \cap Q^x = 1$. Therefore Q satisfies (ii).

Q obviously satisfies (iii).

If $[L:Q] = q - 1$, then $q = 3$, since $[L:Q] = 2$. If $q = 3$ G is a simple group with a self-centralizing element of order three. A theorem of Feit and Thompson, [6] states:

If G is a non-cyclic simple group which contains a self-centralizing subgroup of order three, then G is either $LF(2,5)$ or $LF(2,7)$.

Since $|LF(2,5)|$ is $3 \cdot 4 \cdot 5$, if $LF(2,5)$ were to satisfy (A3) we would have $mq = 15$ and $n = 4$. This is impossible since $n > mq$. The order of $LF(2,7)$ is $3 \cdot 7 \cdot 8$. If $LF(2,7)$ were to satisfy (A3) we would have $mq = 21$ and $n = 8$, which is again a contradiction to the fact that $n > mq$. Hence $q \neq 3$ and Q satisfies (iv).

Since Q is abelian, Q satisfies (v). This completes the lemma.

Let $\gamma_0 = 1, \gamma_1, \ldots, \gamma_{(q-1)/2}, \overline{\gamma}_1, \overline{\gamma}_2, \ldots, \overline{\gamma}_{(q-1)/2}$ be the irreducible characters of Q. Note that these are linear characters since Q is abelian, and are distinct since q is odd. Furthermore it is easily seen from the fact that L is dihedral, that $\tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_{(q-1)/2}$ are distinct irreducible characters of L and that

$$\tilde{\gamma}_i(x) = \gamma_i(x) + \overline{\gamma_i(x)}$$

for $x \in Q^{\#}$, and $i = 1, 2, \ldots, \frac{q-1}{2}$.

By Theorem 6.1, there exist irreducible characters $\varphi_1, \varphi_2, \ldots, \varphi_{(q-1)/2}$ of G, and a sign $\epsilon = \pm 1$ such that

$$\gamma_i^* - \gamma_j^* = \epsilon(\varphi_i - \varphi_j) \tag{6.3}$$

for $0 < i, j \leq \frac{q-1}{2}$. Furthermore, there exists a rational integer c, such that

$$\varphi_i(x) = \epsilon \tilde{\gamma}_i(x) + \epsilon c$$

for any $x \in Q^{\#}$, $i = 1, 2, \ldots, \frac{q-1}{2}$.

Finally, every other irreducible character of G is constant on $Q^{\#}$.

Lemma 6.4. There is exactly one non-trivial character φ_o, such that $\varphi_o \neq \varphi_i$, $i = 1, 2, \ldots, \frac{q-1}{2}$, and such that φ_o does not vanish on $Q^{\#}$. Furthermore $c = 0$, so that $\varphi_i(x) = \epsilon \tilde{\gamma}_i(x)$ if $x \in Q^{\#}$.

First we show that there is at least one such character. Let $\gamma_1^* = \epsilon \varphi_1 + \Delta$. By Frobenius reciprocity $(1, \gamma_1^*)_G = (\gamma_0, \gamma_1)_Q = 0$. Therefore $(1, \Delta)_G = 0$. Let $\gamma_0^* = 1 + \psi + \Delta$. By Frobenius reciprocity $(1, \gamma_0^*)_G = (\gamma_0, \gamma_0)_Q = 1$. Since $(1, \Delta)_G = 0$ we have $(1, \psi)_G = 0$.

Now $\gamma_0^*(1) = \gamma_1^*(1)$. Therefore $1 + \psi(1) = \epsilon \varphi_1(1)$. By (6.3), $\varphi_i(1) = \varphi_1(1)$ for $i = 1, 2, \ldots, \frac{q-1}{2}$. $\psi(1) \equiv -1 \pmod{\varphi_1(1)}$. Therefore some character of G different from φ_i for any i must have a non-zero scalar product with ψ. Let φ_0 be such a character. Since $(1, \psi)_G = 0$, $\varphi_0 \neq 1$. Now we have $(\varphi_0, \gamma_0^*) = (\varphi_0, \psi) + (\varphi_0, \Delta)$ while $(\varphi_0, \gamma_1^*) = (\varphi_0, \Delta)$. Hence $(\varphi_0, \gamma_0^*) \neq (\varphi_0, \gamma_1^*)$, or

$(\varphi_0|_Q, \gamma_0-\gamma_1) \neq 0$. But φ_0 is constant on $Q^{\#}$, say μ. $(\varphi_0|_Q, \gamma_0-\gamma_1) = \mu \sum_{x\in Q} (\gamma_0-\gamma_1)(x) \neq 0$. Therefore $\mu \neq 0$.

Since φ_0 is constant on $Q^{\#}$ it must be integral valued there since $(\varphi_0|_Q, \gamma_i)$ is the same for $i = 1, 2, \ldots, \frac{q-1}{2}$. Since for any character χ of G and for any $x\in G$, $\chi(x)\overline{\chi(x)} \geq 0$. We have by the orthogonality relations for $x \in Q^{\#}$

$$|C_G(x)| = q \geq 1 + \varphi_0(x)\overline{\varphi_0(x)} + \sum_{i=1}^{\frac{q-1}{2}} \varphi_i(x)\overline{\varphi_i(x)}$$

Now since $\varphi_i(x) = \epsilon\tilde{\gamma}_i(x) + \epsilon c$ for $x \in Q^{\#}$, we have

$$\sum_{i=1}^{\frac{q-1}{2}} \varphi_i(x)\overline{\varphi_i(x)} = \sum_{i=1}^{\frac{q-1}{2}} \tilde{\gamma}_i(x)\overline{\tilde{\gamma}_i(x)} + \sum_{i=1}^{\frac{q-1}{2}} c(\gamma_i(x) + \overline{\gamma_i(x)}) + \frac{q-1}{2} c^2$$

But the irreducible characters of L are $\tilde{\gamma}_i$, $i = 1, 2, \ldots, \frac{q-1}{2}$, 1, and a character which is 1 on Q and -1 outside Q in L. So by the orthogonality relations on L

$$|C_L(x)| = q = 1 + 1 + \sum_{i=1}^{\frac{q-1}{2}} \tilde{\gamma}_i(x)\overline{\tilde{\gamma}_i(x)} .$$

Clearly, $\sum_{i=1}^{\frac{q-1}{2}} c(\gamma_i(x) + \overline{\gamma_i(x)}) = -c$. Hence we have

$$\sum_{i=1}^{\frac{q-1}{2}} \varphi_i(x)\overline{\varphi_i(x)} = q - 2 - c + \frac{q-1}{2} c^2 .$$

Since $\varphi_0(x)$ is a non-zero integer, $\varphi_0(x)\overline{\varphi_0(x)} \geq 1$. Hence

$$q \geq 1 + 1 + q - 2 - c + \frac{q-1}{2} c^2$$

or

$$0 \geq \frac{q-1}{2} c^2 - c \,.$$

Certainly $c \geq 0$. Suppose $c \neq 0$.

$$\frac{q-1}{2} c^2 \leq c$$

or

$$\frac{q-1}{2} c \leq 1 \,.$$

This implies $c = 1$ and $q = 3$. But as we have noted already $q \neq 3$ by a theorem of Feit and Thompson [6]. Hence $c = 0$. From this it now follows that

$$q = 1 + \varphi_0(x)\overline{\varphi_0(x)} + q - 2 + \sum_{\chi} \chi(x)\overline{\chi(x)}$$

where χ ranges over the remaining irreducible characters of G.

Since $\varphi_0(x)\overline{\varphi_0(x)} \geq 1$ and $\chi(x)\overline{\chi(x)} \geq 0$, we have $\varphi_0(x) = \pm 1$, and $\chi(x) = 0$ for all other χ, establishing the lemma.

We now wish to relate the values of φ_0 to those of φ_i, $i = 1, 2, \ldots, \frac{q-1}{2}$. Let $\gamma_1^* = \epsilon\varphi_1 + \Delta$. By (6.3) we get

$$\gamma_i^* = \epsilon\varphi_i + \Delta$$

for $i = 1, 2, \ldots, \frac{q-1}{2}$. Let $\gamma_0^* = 1 + \psi + \Delta$ as in the lemma. We wish to show that $\psi = \epsilon\varphi_0$. If χ is any character of G which vanishes on $Q^{\#}$, $(\chi, \gamma_0^* - \gamma_1^*) = 0$. Hence $(\chi, \psi) = 0$. We have already noted that $(1, \psi) = 0$. If we consider φ_i for $1 \leq i \leq \frac{q-1}{2}$,

$$(\varphi_i, \gamma_0^* - \gamma_j^*) = (\varphi_i|_Q, \gamma_0 - \gamma_j) = \frac{1}{q} \sum_{x\in Q} (\gamma_i(x) + \overline{\gamma_i(x)})(\gamma_0(x) - \overline{\gamma_j(x)}) = 0$$

if $i \neq j$. Hence $(\varphi_i, \psi) = 0$, $i = 1, 2, \ldots, \frac{q-1}{2}$. Hence ψ is a multiple of φ_0.

$$(\varphi_0, \gamma_0^* - \gamma_1^*) = (\varphi_0|_Q, \gamma_0 - \overline{\gamma_1}) = \frac{1}{q} \sum_{x\in Q^\#} \varphi_0(x)(1 - \overline{\gamma_1(x)}) \ .$$

Since φ_0 is constant on $Q^\#$ we get for some fixed x in $Q^\#$ $(\varphi_0, \gamma_0^* - \gamma_1^*) = \varphi_0(x)\frac{1}{q}(q-1+1) = \varphi_0(x)$. Now we noted in proving the last lemma that $\varphi_0(x) = \pm 1$. Since $\gamma_0^*(1) = \gamma_1^*(1)$, $\varphi_0(x)\varphi_0(1) + 1 = \epsilon\varphi_1(x)$. So $\varphi_0(x) = \epsilon$ and

$$\gamma_0^* = 1 + \epsilon\varphi_0 + \Delta \ .$$

Thus we know the values of φ_i, $i = 0, 1, \ldots, \frac{q-1}{2}$ on $Q^\#$. Furthermore we know by (6.3) that $\varphi_1(x) = \varphi_i(x)$, $i \geq 1$, if x is in no conjugate of $Q^\#$. We now relate $\varphi_1(x)$ to $\varphi_0(x)$ in this case.

Lemma 6.5. If x is not conjugate to an element of $Q^\#$,

$$\varphi_1(x) = \varphi_0(x) + \epsilon$$

Proof. If x is not conjugate to an element of $Q^\#$

$$\gamma_0^*(x) = 0 = 1 + \epsilon\varphi_0(x) + \Delta(x)$$

and

$$\gamma_1^*(x) = 0 = \epsilon\varphi_1(x) + \Delta(x) \ .$$

Comparing the two equations gives the result immediately.

We summarize the results of this section as a theorem.

Theorem 6.6. Let G be a group satisfying (A3). Then there exist characters $\varphi_0, \varphi_1, \ldots, \varphi_{(q-1)/2}$ of G with the following properties:

(i) If x is not in any conjugate of $Q^\#$

$$\varphi_1(x) = \varphi_i(x) \qquad \text{for } i = 1, 2, \ldots, \frac{q-1}{2}$$

$$\varphi_1(x) = \varphi_0(x) + \epsilon \qquad \text{where } \epsilon = \pm 1 .$$

(ii) For $i = 1, 2, \ldots, \frac{q-1}{2}$, φ_i is an exceptional character of G associated with Q and if x is in some conjugate of $Q^\#$

$$\varphi_i(x) = \epsilon \tilde{\gamma}_i(x)$$

where $\tilde{\gamma}_i$ is an irreducible character of L induced from Q.

(iii) If x is in some conjugate of $Q^\#$,

$$\varphi_0(x) = \epsilon .$$

(iv) If $\chi \neq 1$ is any irreducible character of G besides the φ_i, $i = 0, 1, \ldots, \frac{q-1}{2}$, then if x is in some conjugate of $Q^\#$, $\chi(x) = 0$.

Corollary 6.7. If χ is any character of G besides $1, \varphi_0, \varphi_1, \ldots, \varphi_{(q-1)/2}$, $q \mid \chi(1)$.

Proof. This is true since $(\gamma_0^*, \chi)_G = (\gamma_0, \chi\mid_Q)_Q = \frac{1}{q}\chi(1)$ is an integer.

Corollary 6.8. φ_0 is integer valued.

We know that $\varphi_0(1) \neq 1$ since G is simple and $\varphi_0 \neq 1$. $\varphi_0(1) \neq \varphi_i(1)$, $i = 1, 2, \ldots, \frac{q-1}{2}$, by the theorem. $(\varphi_0, \gamma_0^*) = (\varphi_0 |_Q, \gamma_0) = \dfrac{\varphi_0(1) + \epsilon(q-1)}{q}$ is an integer and hence $\varphi_0(1) \equiv \epsilon \pmod{q}$. By Corollary 6.7, we see now that every other character of G has degree different from φ_0. Hence φ_0 is identical with all of its algebraic conjugates and hence must be rational. Its values are rational algebraic integers and hence, integers.

We remark that φ_0 is analogous to the irreducible character associated with the doubly transitive representation in the problem which was previously considered.

VII. CERTAIN COEFFICIENTS IN THE CLASS ALGEBRA AND THEIR IMPLICATIONS

In the last section we showed that we can evaluate any character of G on $Q^{\#}$. Now we would like to apply these results to the calculation of certain coefficients in the class algebra.

If x is any element of G let K_x be the class of G containing x. Let $\overline{K}_x = \sum_{y \in K_x} y$ be the class sum, an element of the group algebra. Let $z_1 = 1, z_2, \ldots, z_v$ be class representatives for G. There exist integer constants $a_{\lambda,\mu,\nu}$ such that

$$(7.1) \qquad \overline{K}_{z_\lambda} \cdot \overline{K}_{z_\mu} = \sum_{\nu=1}^{v} a_{\lambda\mu\nu} \overline{K}_{z_\nu}.$$

There is a well known formula for $a_{\lambda\mu\nu}$ (cf. [1], p. 580)

$$(7.2) \qquad a_{\lambda\mu\nu} = \frac{mnq}{|C(z_\lambda)|\,|C(z_\mu)|} \sum_{\chi} \frac{\chi(z_\lambda)\chi(z_\mu)\chi(z_\nu)}{\chi(1)}$$

where χ ranges over all irreducible characters of G.

It is easily seen that if z_λ, z_μ, or z_ν is in some conjugate of $Q^{\#}$ the calculation of $a_{\lambda\mu\nu}$ is not only possible, but fairly simple since most of the terms in the sum vanish.

In this section we will calculate $a_{\lambda\mu\nu}$ when z_λ and z_μ do not belong to conjugates of $Q^{\#}$ and z_ν does. We use this calculation to show that G has a single class of involutions, and to derive information about the degrees of φ_0 and φ_1.

Throughout this section G is assumed to satisfy (A3).

Theorem 7.3. If z_λ and z_μ do not belong to conjugates of $Q^\#$ and z_ν does, then

$$(7.4) \qquad a_{\lambda\mu\nu} = \frac{mnq[\varphi_0(1) - \varphi_0(z_\lambda)][\varphi_0(1) - \varphi_0(z_\mu)]}{|C(z_\lambda)||C(z_\mu)|\varphi_0(1)\varphi_1(1)}$$

Proof. By Theorem 6.6 and (7.2)

$$a_{\lambda\mu\nu} = \frac{mnq}{|C(z_\lambda)||C(z_\mu)|}\left[1 + \frac{\varphi_0(z_\lambda)\varphi_0(z_\mu)\epsilon}{\varphi_0(1)} + \sum_{i=1}^{\frac{q-1}{2}} \frac{\varphi_1(z_\lambda)\varphi_1(z_\mu)\varphi_i(z_\nu)}{\varphi_1(1)}\right]$$

$$= \frac{mnq}{|C(z_\lambda)||C(z_\mu)|}\left[1 + \frac{\varphi_0(z_\lambda)\varphi_0(z_\mu)\epsilon}{\varphi_0(1)} - \frac{\varphi_1(z_\lambda)\varphi_1(z_\mu)\epsilon}{\varphi_1(1)}\right].$$

If we take $\varphi_0(1)[\varphi_0(1) + \epsilon]$ as a common denominator and express φ_1 in terms of φ_0 when possible, we get

$$a_{\lambda\mu\nu} = \frac{mnq[\varphi_0(1) - \varphi_0(z_\lambda)][\varphi_0(1) - \varphi_0(z_\mu)]}{|C(z_\lambda)||C(z_\mu)|\varphi_0(1)\varphi_1(1)}.$$

This completes the proof.

Lemma 7.5. If ρ and σ are distinct involutions such that $\rho\sigma$ fixes two letters, then ρ and σ are in K_ω.

Proof. Suppose $\rho\sigma$ fixes a and b. There exists y such that $(\rho\sigma)^y$ is in $Q^\#$. $\rho^y(\rho\sigma)^y\rho^y = (\sigma\rho)^y$, the inverse of $(\rho\sigma)^y$. Since $Q \cap Q^x = 1$ if $x \notin L$, $\rho^y \in L$. Obviously the same is true for σ. Since every involution in L is conjugate to ω the lemma is proved.

Theorem 7.6. If G satisfies (A3), G has a single class of involutions.

Proof. Suppose K_{z_i} is a class of involutions different from K_ω. Let K_{z_j} be the class of an element of $Q^\#$. By (7.1) a_{iij} is the number of ways z_j can be written as a product of involutions in K_{z_i}. Since $K_{z_i} \neq K_\omega$ by assumption, Lemma 7.5 implies $a_{iij} = 0$. By (7.4) this can happen only if $\varphi_0(1) - \varphi_0(z_i) = 0$. This is contradictory because G is simple and $\varphi_0 \neq 1$. Hence G has a single class of involutions.

Theorem 7.7. $\dfrac{mn[\varphi_0(1) - \varphi_0(\omega)]^2}{|C(\omega)|^2 \varphi_0(1)\varphi_1(1)} = 1$.

Proof. We calculate a_{iij} in two ways, where $K_\omega = K_{z_i}$ and z_j has a conjugate in $Q^\#$.

Let y be an element of $Q^\#$ in K_{z_j}. The proof of Lemma 7.5 indicates that if y is the product of two involutions, these involutions are in L. If ρ is any involution in L, there is a unique element σ in L such that $\rho\sigma = y$. Since L is dihedral of order $2q$, σ must be an involution. Therefore there are q ways in which y can be written as the product of involutions. Hence $a_{iij} = q$. Applying Theorem 7.3 we now get our result immediately.

Corollary 7.8. $m \,|\, \varphi_0(1)\varphi_1(1)$.

Proof. By the theorem $m \,\Big|\, |C(\omega)|^2 \varphi_0(1)\varphi_1(1)$. Any element, not 1, centralizing ω moves all letters. Hence $C(\omega)$ is semi-regular on n letters and $|C(\omega)| \Big| n$. Since $(m, n) = 1$, $m | \varphi_0(1)\varphi_1(1)$, as asserted.

Theorem 7.9. $m | \varphi_0(1)$ or $m | \varphi_1(1)$.

Proof. Since $\varphi_1(1) = \varphi_0(1) + \epsilon$, $(\varphi_1(1), \varphi_0(1)) = 1$. Hence if m is a prime power we are done since $m | \varphi_0(1)\varphi_1(1)$ by Corollary 7.8. If m is not a prime power, we assert that M satisfies the hypotheses of Theorem 6.1.

If x is in $M^{\#}$, x fixes exactly one letter by Lemma 3.6, and $C(x) \subseteq M$ since M contains all elements fixing just the letter 1. That M satisfies hypotheses (ii) and (iii) of Theorem 6.1, follows from Lemma 3.6. Hypotheses (iv) and (v) are obvious since mq is odd, and m is not a prime power. Thus M satisfies the hypotheses of Theorem 6.1, as asserted.

In Theorem 6.1, suppose $\varphi_0 = \chi_j$ for some j. Then for $x \epsilon M^{\#}$

$$\varphi_0(x) = \epsilon' \tilde{\zeta}_j(x) + z_i c$$

where c is a rational integer, $\epsilon' = \pm 1$, and $\tilde{\zeta}_j$ is a non-trivial irreducible character of H. Since H is of odd order, $\tilde{\zeta}_j$ is not real and hence φ_0 is not real. This contradicts Corollary 6.8. Hence φ_0 is not an exceptional character of G associated with M and is therefore constant on $M^{\#}$.

If p^{α} is the highest power of p dividing m for some prime $p | m$, then $p^{\alpha} | \varphi_0(1)$ or $p^{\alpha} | \varphi_1(1)$ since $(\varphi_0(1), \varphi_1(1)) = 1$, and $m | \varphi_0(1)\varphi_1(1)$. Since $(m, nq) = 1$, p^{α} is the highest power of p dividing the order of the group. Hence φ_0 or φ_1 has defect 0 for p and therefore vanishes on $P^{\#}$, where P is the Sylow p-subgroup of G in M (cf. [10], p. 206). Hence φ_0 or φ_1 vanishes on $M^{\#}$ since they are constant there.

If φ_0 vanishes on $M^{\#}$, $(\varphi_0|_M, 1)_M = \dfrac{\varphi_0(1)}{m}$ and hence $m|\varphi_0(1)$. If φ_0 does not vanish on $M^{\#}$, φ_1 does, and $(\varphi_1|_M, 1)_M = \dfrac{\varphi_1(1)}{m}$. Hence $m|\varphi_1(1)$.

This completes the proof of the theorem.

Corollary 7.10. Either φ_0 is 0 on $M^{\#}$, or φ_0 is $-\epsilon$ on $M^{\#}$.

Proof. If $m = p^a$ the result follows from the fact that either φ_0 or φ_1 is of defect 0 for p. Otherwise it is obvious from the proof of the theorem.

VIII. THE STRUCTURE OF M

By a theorem of Thompson, [16], the Frobenius kernel of a Frobenius group is nilpotent, and hence the direct product of its Sylow p-subgroups. In this section we will show that M is not the direct product of non-trivial Q-invariant subgroups, and thereby conclude that M must be a p-group.

Throughout this section we assume that G satisfies (A3).

Lemma 8.1. If $M = B_1 \times B_2$, where B_1 and B_2 are non-trivial Q-invariant subgroups of M, then G satisfies the hypotheses of Theorem 6.1.

Since B_τ is Q-invariant $[B_\tau : B_\tau'] > 2q$ for $\tau = 1, 2$. Therefore $[M:M'] > 4q^2$. Hence it is clear that M satisfies the hypotheses of Theorem 6.1, since we showed it satisfied the other hypotheses in proving Theorem 7.9.

Let $\alpha_1, \alpha_2, \ldots, \alpha_q$ be the elements of Q. $\alpha_1 = 1$. Let $\zeta_0, \zeta_j^{\alpha_i}$, be the irreducible characters of M, where $i = 1, 2, \ldots, q$; and $j = 1, 2, \ldots, r$. Let $z_j = \zeta_j(1)$.

By Theorem 6.1 there exist irreducible characters of G, $\chi_1, \chi_2, \ldots, \chi_r$ and $\epsilon' = \pm 1$ such that

$$\chi_j(x) = \epsilon' \tilde{\zeta}_j(x) + \epsilon' z_j c \tag{8.2}$$

for some rational integer c and every x in $M^{\#}$.

Lemma 8.3. $|C(x)| = q + \sum_{j=1}^{r} \tilde{\zeta}_j(x)\overline{\tilde{\zeta}_j(x)}$ if x is in $M^{\#}$.

Proof. If x is in $M^{\#}$ we know $C(x) = C_H(x)$. The irreducible characters of H consist of $\tilde{\zeta}_1, \tilde{\zeta}_2, \ldots, \tilde{\zeta}_r$ and q linear characters of H/M. By the orthogonality relations we therefore have

$$|C(x)| = |C_H(x)| = q + \sum_{j=1}^{r} \tilde{\zeta}_j(x)\overline{\tilde{\zeta}_j(x)} .$$

Lemma 8.4. If $M = B_1 \times B_2$ where B_1 and B_2 are non-trivial Q-invariant subgroups of M, then in (8.2) $c = 0$.

Proof. By the orthogonality relations we have for x in $M^{\#}$,

$$\begin{aligned} |C(x)| &\geq 1 + \sum_{j=1}^{r} (\tilde{\zeta}_j(x) + z_j c)(\overline{\tilde{\zeta}_j(x)} + z_j c) \\ &= 1 + \sum_{j=1}^{r} \tilde{\zeta}_j(x)\overline{\tilde{\zeta}_j(x)} + c\sum_{j=1}^{r} z_j(\tilde{\zeta}_j(x) + \overline{\tilde{\zeta}_j(x)}) + c^2\sum_{j=1}^{r} z_j^2 \\ &= 1 + |C(x)| - q - 2c + c^2\left(\frac{m-1}{q}\right). \end{aligned}$$

Thus

$$c^2(m-1) \leq (q - 1 + 2c)q .$$

Suppose $c \neq 0$. Then we have

$$m - 1 \leq \frac{(q-1+2c)q}{c^2} \leq \frac{(q-1+2|c|)q}{c^2} \leq q^2 + q .$$

Since B_τ is Q-invariant $|B_\tau| = y_\tau q + 1$, $\tau = 1, 2$.

$$m - 1 = (y_1 y_2 q + y_1 + y_2)q \leq (q + 1)q$$

This is contradictory since B_1 and B_2 are non-trivial. Hence $c = 0$ as asserted.

Theorem 8.5. If G satisfies (A3) then $M \neq B_1 \times B_2$ where B_1 and B_2 are non-trivial Q-invariant subgroups of M.

Proof. By Lemma 8.1, G satisfies the hypothesis of Theorem 6.1. We now designate the characters of G distinct from 1, $\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_{(q-1)/2}; \chi_1, \chi_2, \ldots, \chi_r$.

Let $\xi_1, \xi_2, \ldots, \xi_s$ be the characters of G such that ξ_k is $e_k \neq 0$ on $M^{\#}$, $k = 1, 2, \ldots, s$. Let $\theta_1, \theta_2, \ldots, \theta_t$ be the characters of G which vanish on $H^{\#}$.

Lemma 8.6. If φ_0 is 0 on $M^{\#}$, $\sum_{k=1}^{s} e_k^2 = \frac{q-1}{2}$. If φ_0 is $-\epsilon$ on $Q^{\#}$, $\sum_{k=1}^{s} \ell_k^2 = q - 2$.

Proof. By Lemma 8.4 and Lemma 8.3 $\sum_{j=1}^{r} \chi_j(x)\overline{\chi_j(x)} = |C(x)| - q$ for x in $M^{\#}$.

Case 1. φ_0 is 0 on $M^{\#}$.

By the orthogonality relations

$$|C(x)| = 1 + \sum_{i=1}^{\frac{q-1}{2}} \varphi_i(x)\overline{\varphi_i(x)} + \sum_{j=1}^{r} \chi_j(x)\overline{\chi_j(x)} + \sum_{k=1}^{s} \xi_k(x)\overline{\xi_k(x)}$$

for x in $M^{\#}$. Hence

$$|C(x)| = 1 + \frac{q-1}{2} + |C(x)| - q + \sum_{k=1}^{s} e_k^2$$

or

$$\sum_{k=1}^{s} e_k^2 = \frac{q-1}{2} .$$

Case 2. φ_0 is $-\epsilon$ on $M^{\#}$.

By the orthogonality relations

$$|C(x)| = 1 + 1 + |C(x)| - q + \sum_{k=1}^{s} e_k^2$$

or

$$\sum_{k=1}^{s} e_k^2 = q - 2 .$$

Let ψ_1, ψ_2 be non-trivial linear characters of B_1, B_2 respectively. Let $\hat{\psi}_\tau$ be the character of $B_\tau Q$ induced by ψ_τ for $\tau = 1, 2$. It is clear that $\hat{\psi}_\tau$ is an irreducible character of $B_\tau Q$ which has degree q and vanishes outside B_τ.

Let $\mu_\tau = (q \cdot 1_{B_\tau Q} - \hat{\psi}_\tau)$ for $\tau = 1, 2$. Let $\psi = \mu_1^* \mu_2^*$. μ_τ^* vanishes outside conjugates of $(B_\tau Q)^{\#}$ for $\tau = 1, 2$. If some conjugate of an element in $B_1^{\#}$ were in $B_2^{\#}$ it would have to be a conjugate under Q since $M \cap M^x = 1$ if $x \notin H$. This is impossible since B_τ is Q-invariant. Hence ψ vanishes outside conjugates of $Q^{\#}$.

If x is in $Q^{\#}$,

$$\mu_\tau^*(x) = \frac{1}{b_\tau q} \sum_{y\in G} q \cdot 1_{B_\tau Q}(x^y) = \frac{1}{b_\tau q} \; (q \cdot 2b_\tau q) = 2q \; .$$

Thus

$$(8.7) \qquad (\psi, 1) = \frac{1}{mnq} \; (4q^2)(mn \; \tfrac{q-1}{2}) = 2q^2 - 2q$$

Now $(\psi, 1) = (\mu_1^* \mu_2^*, 1) = \frac{1}{|G|} \sum_{x\in G} \mu_1^*(x)\mu_2^*(x) = \frac{1}{|G|} \sum_{x\in G} \mu_1^*(x)\overline{(\overline{\mu_2^*(x)})} =$
$= (\mu_1^*, \overline{\mu_2^*})$

$$\mu_1^* = \sum_{\chi} (\chi, \mu_1^*)\chi \; , \quad \overline{\mu_2^*} = \sum_{\chi} (\chi, \overline{\mu_2^*})\chi$$

where χ ranges over all irreducible characters of G.

Hence

$$(8.8) \qquad (\psi, 1) = (\mu_1^*, \overline{\mu_2^*}) = \sum_{\chi} \; (\chi, \mu_1^*)(\chi, \overline{\mu_2^*})$$

The remainder of the proof consists of calculating (χ, μ_1^*) and $(\chi, \overline{\mu_2^*})$ for every irreducible character of G and obtaining a contradiction to (8.7) by means of (8.8).

$$(8.9) \qquad (\theta_j, \mu_1^*) = 0 \quad \text{for} \quad j = 1, 2, \ldots, t$$

Proof. $(\theta_j, \mu_1^*) = (\theta_j|_{B_1 Q}, \mu_1)$. The result is now obvious since θ_j vanishes on $H^\#$ and μ_1 vanishes on the identity.

$$(8.10) \qquad \sum_{k=1}^{s} (\xi_k, \mu_1^*)(\xi_k, \overline{\mu_2^*}) + \sum_{i=0}^{\frac{q-1}{2}} (\varphi_i, \mu_1^*)(\varphi_i, \overline{\mu_2^*}) = q^2 - q$$

Proof. $(\xi_k, \overline{\mu_2^*}) = (\xi_k|_{B_2Q}, \overline{\mu}_2) = (\xi_k|_{B_2Q}, \mu_2)$ since ξ_k is rational on H.

$$(\xi_k, \mu_\tau) = \frac{1}{b_\tau q} \sum_{x\epsilon(B_\tau Q)^\#} \xi_k(x)[\, q - \overline{\hat{\psi}_1(x)}\,]$$

$$= \frac{e_k}{b_1 q} \sum_{x\epsilon B_\tau^\#} [\, q - \overline{\hat{\psi}_1(x)}\,] = \frac{e_k}{b_1 q}\, [\,(b_1-1)q + q] = e_k$$

Therefore

$$\sum_{k=1}^{s} (\xi_k, \mu_1^*)(\xi_k, \overline{\mu_2^*}) = \sum_{k=1}^{s} e_k^2 .$$

$(\varphi_i, \overline{\mu_2^*}) = (\varphi_i|_{B_2Q}, \overline{\mu_2}) = (\varphi_i|_{B_2Q}, \mu_2)$ for $i = 0, 1, \ldots, \frac{q-1}{2}$, since φ_i is real on $(B_2Q)^\#$ for $i = 0, 1, \ldots, \frac{q-1}{2}$.

Case 1. φ_0 is 0 on $M^\#$.

$$(\varphi_0, \mu_\tau^*) = (\varphi_0|_{B_\tau Q}, \mu_\tau) = \frac{1}{b_\tau q} \sum_{x\epsilon B_\tau Q} \varphi_0(x)[\, q - \overline{\hat{\psi}_\tau(x)}]$$

$$= \frac{1}{b_\tau q} [\, \epsilon b_\tau (q-1) q] = (q-1)\epsilon$$

$$(\varphi_i, \mu_\tau^*) = (\varphi_i|_{B_\tau Q}, \mu_\tau) = \frac{1}{b_\tau q}\left(\sum_{x\epsilon B_\tau^\#} \epsilon (q - \overline{\hat{\psi}_\tau(x)}) + b_\tau \sum_{x\epsilon Q^\#} \varphi_i(x) q \right)$$

$$= \frac{1}{b_\tau q} (q(b_\tau - 1)\epsilon + \epsilon q + b_1 q(-2\epsilon)) = -\epsilon .$$

By Lemma 8.6, $\sum_{k=1}^{s} e_k^2 = \frac{q-1}{2}$. Thus

$$\sum_{k=1}^{s} (\xi_k, \mu_1^*)(\xi_k, \overline{\mu_2^*}) + \sum_{i=0}^{\frac{q-1}{2}} (\varphi_i, \mu_1^*)(\varphi_i, \overline{\mu_2^*}) = \frac{q-1}{2} + (q-1)^2 + \frac{q-1}{2} = q^2 - q$$

as asserted.

Case 2. φ_0 is $-\epsilon$ on $M^{\#}$.

$$(\varphi_0, \mu_\tau^*) = (\varphi_0 |_{B_\tau Q}, \mu_\tau) = \frac{1}{b_\tau q}\left(\sum_{x \epsilon B_\tau^{\#}} (-\epsilon)(q - \overline{\hat{\psi}_\tau(x)}) + b_\tau \sum_{x \epsilon Q^{\#}} \epsilon q\right)$$

$$= \frac{1}{b_\tau q}\left((-\epsilon)([b_\tau - 1] q + q) + (q-1) b_\tau q \epsilon\right)$$

$$= (q - 2)\epsilon$$

$$(\varphi_i, \mu_\tau^*) = (\varphi_i |_{B_\tau Q}, \mu_\tau) = \frac{1}{b_\tau q} \sum_{x \epsilon Q^{\#}} b_\tau q \varphi_i(x) = -2\epsilon$$

for $i = 1, 2, \ldots, \frac{q-1}{2}$.

By Lemma 8.6 $\sum_{k=1}^{s} e_k^2 = q - 2$.

$$\sum_{k=1}^{s} (\xi_k, \mu_1^*)(\xi_k, \overline{\mu_2^*}) + \sum_{i=0}^{\frac{q-1}{2}} (\varphi_i, \mu_1^*)(\varphi_i, \overline{\mu_2^*}) = q - 2 + (q-2)^2 + 2(q-1) = q^2 - q .$$

This completes the proof of (8.10).

(8.11) $(1, \mu_\tau^*) = (1, \overline{\mu_\tau^*}) = q$

Proof. Since 1 is real $(1, \mu_\tau^*) = (1, \overline{\mu_\tau^*})$

$(1, \mu_\tau^*) = (1_{B_\tau Q}, \mu_\tau) = q$.

We have now reduced our problem to calculating (χ_j, μ_1^*) and $(\chi_j, \overline{\mu_2^*})$ for $j = 1, 2, \ldots, r$. By Lemma 8.4

$$\chi_j(x) = \epsilon' \tilde{\zeta}_j(x) \text{ on } M^\# .$$

Lemma 8.12. $\chi_j = \epsilon' \zeta_j \left|_{B_\tau}\right|^{B_\tau Q}$ on $(B_\tau Q)^\#$.

Proof. χ_j vanishes on every element of $(B_\tau Q)^\#$ outside $B_\tau^\#$ since χ_j vanishes on $Q^\#$. $\epsilon' \zeta_{j,\tau} |^{B_\tau Q}$ obviously vanishes there. Hence we need only consider x in $B_\tau^\#$. For such an x

$$\chi_j(x) = \epsilon' \tilde{\zeta}_j(x) = \epsilon' \sum_{i=1}^{q} \zeta_j^{a_i}(x) = \epsilon' \sum_{i=1}^{q} \zeta_{j,\tau}^{a_i}(x) = \epsilon' \zeta_{j,\tau} |^{B_\tau Q}(x)$$

(8.13) If $\zeta_j|_{B_1}$ is not $y_1\psi_1^{a_i}$ for some i, or 1, then $(\chi_j, \mu_1^*) = 0$.

Proof. Since $M = B_1 \times B_2$, $\zeta_j|_{B_1}$ is a multiple of an irreducible character $y_1\zeta$. By Lemma 8.12 $\chi_j = \epsilon' y_1 \zeta |^{B_\tau Q}$ on $(B_\tau Q)^\#$. $(\chi_j, \mu_1^*) = (\chi_j|_{B_1 Q}, \mu_1) = (\epsilon' y_1 \zeta|^{B_1 Q}, \mu_1)$ since μ_1 vanishes on the identity. The conclusion of (8.13) is now clear.

(8.14) If $\zeta_j|_{B_2}$ is not $y_2\overline{\psi}_2^{a_i}$ for some i, or 1, then $(\chi_j, \overline{\mu_2^*}) = 0$.

Proof. The proof is obviously carried out in the same way as (8.13).

Now since $M = B_1 \times B_2$, ζ_j is the product of an irreducible character of B_1 and an irreducible character of B_2. We have just shown that if $(\chi_j, \mu_1^*) \neq 0$, and $(\chi_j, \overline{\mu_2^*}) \neq 0$ then ζ_j is either $1_{B_1} \cdot \overline{\psi_2}$, $\psi_1 \cdot 1_{B_2}$, or $\psi_1 \cdot \overline{\psi_2}$. $1_{B_1} \cdot 1_{B_2}$ is not possible since ζ_j is not the identity of M for $j = 1, 2, \ldots, r$. Clearly, for each of these choices $y_1 = y_2 = 1$ since ψ_1 and ψ_2 are linear.

(8.15) If $\zeta_j = 1_{B_1} \cdot \overline{\psi_2}$ $\quad (\chi_j, \mu_1^*) = \epsilon' q$, $\quad (\chi_j, \overline{\mu_2^*}) = -\epsilon'$.

If $\zeta_j = \psi_1 \cdot 1_{B_2}$ $\quad (\chi_j, \mu_1^*) = -\epsilon'$, $\quad (\chi_j, \overline{\mu_2^*}) = \epsilon' q$.

If $\zeta_j = \psi_1 \cdot \overline{\psi_2}$ $\quad (\chi_j, \mu_1^*) = -\epsilon'$, $\quad (\chi_j, \overline{\mu_2^*}) = -\epsilon'$.

Proof. $(\chi_j, \mu_1^*) = (\chi_j|_{B_1Q}, \mu_1) = (\epsilon'\zeta|^{B_1Q}, q1_{B_1Q} - \psi_1)$ which gives the results for scalar products with μ_1^*.
$(\chi_j, \overline{\mu_2^*}) = (\chi_j|_{B_2Q}, \overline{\mu_2}) = (\epsilon'\zeta|^{B_2Q}, q1_{B_2Q} - \overline{\psi_2})$ which gives the results for scalar products with $\overline{\mu_2^*}$.

Combining the results of (8.9) through (8.15) and substituting in (8.8) we get

(8.16) $$(\psi, 1) = q^2 - q + q^2 - q - q + 1 = 2q^2 - 3q + 1$$

Together with (8.7) this implies $2q^2 - 2q = 2q^2 - 3q + 1$ or $q = 1$ which is impossible. This completes the proof of the theorem.

Corollary 8.17. M is a p-group.

Proof. As we commented in the introduction, M is nilpotent by a theorem of Thompson. Hence it is the product of its Sylow p-subgroups. The theorem now gives the result.

IX. ON THE ORDER OF GROUPS SATISFYING (A3).

As was indicated in the introduction, there are infinitely many doubly transitive groups satisfying (A1). If a group satisfies (A1) and is not doubly transitive we have shown that H has β orbits on which it is represented regularly, where $\beta \neq 0$. We have shown that only one group exists satisfying (A1) with mq even and $\beta \neq 0$.

In this section we will show that for $\beta \neq 0$ and fixed, there exist only a finite number of groups satisfying (A3). In fact their order is bounded by β^{12}. However we have not concentrated on trying to establish a good bound, but only a bound -- assuring that the number of groups for $\beta \neq 0$ and fixed is finite.

Theorem 9.1. Suppose G satisfies (A3). Let $(\varphi_0, 1_H^*) = a$. Then $m + 1 \leq \beta$ or $a = 1$ and $m = \frac{\beta}{6} q + 1$.

Proof. The proof is divided into four cases, according as $\epsilon = \pm 1$ and m divides $\varphi_0(1)$ or $\varphi_1(1)$. These are the only alternatives by Theorem 7.9.

Case 1. Suppose $\epsilon = 1$ and $m | \varphi_0(1)$.

Since $m | \varphi_0(1)$, φ_0 is 0 on $M^\#$. Combining this information with $\epsilon = +1$ we get

$$a = (\varphi_0, 1_H^*) = (\varphi_0 |_H, 1_H) = \frac{1}{mq}[\varphi_0(1) + m(q-1)]$$

Hence

$$mqa = \varphi_0(1) + m(q - 1)$$

or

$$\varphi_0(1) = mq(a - 1) + m .$$

Thus we have

$$\varphi_1(1) = mq(a - 1) + m + 1 .$$

It is easily seen that $q \nmid \varphi_1(1)$. Hence $\varphi_1(1) \mid mn$. Since $(\varphi_1(1), m) = 1$, $\varphi_1(1) \mid n$. $\varphi_1(1) < n$, since otherwise $\varphi_1(1)^2 > mnq$, which is impossible. Therefore there exists an integer $k > 0$ such that

$$(9.2) \qquad (km + 1)[(a-1)mq + m + 1] = n = \beta mq + m + 1.$$

1) If $a = 1$ we get

$$(km + 1 + k)m = (\beta q + 1)m .$$

This implies

$$k(m + 1) = \beta q .$$

Now $q \mid m-1$. Therefore $(q, m+1) = 1$, since q is odd. Thus $q \mid k$ and $(m+1) \mid \beta$. Certainly $m+1 \leq \beta$ since $\beta \neq 0$.

2) If $a > 1$ (9.2) yields

$$(a-1)mqk + mk + k + (a-1)q + 1 = \beta q + 1$$

by subtracting 1 from both sides and dividing by m. Thus

$$(a-1)mq + m = \frac{(\beta - a + 1)}{k} q + 1 .$$

Therefore

$$(a-1)m < \frac{\beta - a + 1}{k} \leq \beta - a + 1 \leq \beta .$$

Hence

$$m + 1 \leq \beta .$$

Case 2. Suppose $\epsilon = -1$, and $m \mid \varphi_0(1)$.

We have immediately that φ_0 is 0 on $M^{\#}$ and hence

$$a = (\varphi_0 |_H, 1_H) = \frac{\varphi_0(1) - m(q-1)}{mq} .$$

From this we get

$$\varphi_0(1) = mq(a+1) - m$$

and

$$\varphi_1(1) = (a+1)mq - m - 1 .$$

As in the previous case $\varphi_1(1) \mid n$ and $\varphi_1(1) < n$. Hence $k > 0$ exists such that

$$(km - 1)[(a+1)mq - m - 1] = \beta mq + m + 1 .$$

Subtracting 1 from both sides and dividing by m we get

$$\beta q + 1 = (a+1)kmq - km - k - (a+1)q + 1$$

or

$$k[(a+1)mq - m - 1] = (\beta + a + 1)q .$$

Since $q \nmid (m+1)$, $q \mid k$. Hence

$$(a+1)mq - m - 1 < \beta + a + 1 .$$

Thus

$$mq - m - 1 < \beta + 1$$

or

$$m + 1 \leq \beta .$$

Case 3. Suppose $\epsilon = -1$, and $m \mid \varphi_1(1)$.

Since $m \mid \varphi_1(1)$, and $\epsilon = -1$, φ_0 is 1 on $M^{\#}$. Thus

$$a = \frac{\varphi_0(1) + m - 1 - m(q - 1)}{mq}$$

This gives

$$\varphi_0(1) = mq(a+1) - 2m + 1 .$$

As in the previous case, $\varphi_0(1) \mid n$. Therefore an integer k exists such that

$$[(a+1)mq - 2m + 1](km+1) = (\beta q+1)m + 1 .$$

Subtracting 1 from both sides and dividing by m we get

$$(a+1)mqk - 2mk + k + (a+1)q - 2 = \beta q + 1$$

or

$$k[(a+1)mq - 2m + 1] = (\beta - a - 1)q + 3 .$$

If we consider the last equation (mod q) we get

$$k \equiv -3 \pmod{q}$$

1) If $k > q$, then

$$(a+1)mq - 2m + 1 < \beta - a .$$

This gives

$$[(a+1)q - 2]m < \beta - 1$$

or

$$m + 1 < \beta .$$

2) If $k = q - 3$, $k \neq 0$ since $q \neq 3$. We get

$$(a+1)mq - 2m + 1 = \beta - a - 1 + \frac{3(\beta - a)}{q - 3} .$$

Now

$$m(q-2) \leq m[(a+1)q - 2] = \beta - a - 2 + \frac{3(\beta - a)}{q - 3} \leq \beta - 2 + \frac{3\beta}{q-3} .$$

Hence

$$m \leq \frac{\beta - 2}{q - 2} + \frac{3\beta}{(q-3)(q-2)} \leq \frac{\beta - 2}{3} + \frac{\beta}{2} = \frac{5}{6}\beta - \frac{2}{3} .$$

Therefore we have

$$m + 1 \leq \beta .$$

Case 4. Suppose $\epsilon = 1$ and $m \mid \varphi_1(1)$. In the same manner as in the previous cases we get

$$\varphi_0(1) = mq(a-1) + 2m - 1 .$$

We must have $\varphi_0(1) \mid n$ and $\varphi_0(1)^2 < mnq$. Therefore there exists $k > 0$ such that

$$[(a-1)mq + 2m - 1][km - 1] = (\beta q + 1)m + 1 .$$

This yields

$$(a-1)mkq + 2km - k - (a-1)q = \beta q + 3 .$$

1) If $a > 1$ we get

$$(a-1)(mk-1) + 1 < \beta .$$

Thus

$$mk < \beta$$

and

$$m + 1 \leq \beta .$$

2) Suppose $a = 1$. Then

$$2km - k = \beta q + 3$$

implies $k \equiv 3 \pmod{q}$. $k \neq 0$ since $q \neq 3$. We have

$$2m = \frac{\beta q + 3}{k} + 1 .$$

If $k > q$,

$$m < \frac{\beta}{2} + 1$$

or

$$m + 1 \leq \beta .$$

If $k = 3$

$$m = \frac{\beta}{6} q + 1 .$$

This completes the proof of Theorem 9.1.

In the case where $k = 3$ and $m = \frac{\beta}{6} q + 1$ we extend our analysis. Since m is odd and $m \equiv 1 \pmod{q}$ we get easily that $12 | \beta$. Let $\beta = 2\delta$. Then $m = 2\delta q + 1$. We have

$$n = 1 + 2\delta q + 1 + 12\delta[2\delta q + 1] q .$$

Simple calculation gives

$$n = 2(3\delta q + 1)(4\delta q + 1)$$

$$\varphi_0(1) = 4\delta q + 1$$

and

$$\varphi_1(1) = 2(2\delta q + 1).$$

In this case we would like to show that q is bounded by a simple function of β.

Lemma 9.3. In the situation just described, $q < 4\beta + 8$.

Proof. By Theorem 7.7,

$$mn[\varphi_0(1) - \varphi_0(\omega)]^2 = |C(\omega)|^2 \varphi_0(1)\varphi_1(1) .$$

Substituting and simplifying accordingly we get

$$|C(\omega)|^2 = (3\delta q + 1)[\varphi_0(1) - \varphi_0(\omega)]^2 .$$

By Lemma 3.9,

$$|K_\omega| \leq mq[12\delta + 1] .$$

This gives

$$n \leq |C(\omega)|(12\delta + 1) .$$

Substituting, we get

$$2(3\delta q+1)^{\frac{1}{2}}(4\delta q+1) \leq (\varphi_0(1) - \varphi_0(\omega))(12\delta + 1) .$$

Now

$$\varphi_0(1) - \varphi_0(\omega) \leq 2\varphi_0(1) = 2(4\delta q + 1) .$$

Thus

$$(3\delta q + 1)^{\frac{1}{2}} \leq 12\delta + 1$$

or

$$(\frac{\beta}{4} q + 1) \leq \beta^2 + 2\beta + 1 .$$

This gives

$$q \leq 4\beta + 8$$

and the proof is complete.

Theorem 9.4. If G satisfies (A3), $|G| < \beta^{12}$, that is, there are at most a finite number of groups satisfying (A3) for fixed $\beta \neq 0$.

Proof. Either $q < m < \beta$, or $q \leq 4\beta + 8 < \beta^2$ since $\beta \geq 12$ in this case. Hence $q < \beta^2$ in any case. Either $m < \beta$ or $m = \frac{\beta}{6} q + 1 \leq \frac{\beta}{6}(\beta^2) + 1 \leq \beta^3$ since $\beta \geq 12$ in this case. In any event, $m \leq \beta^3$. $n = 1 + m + \beta mq$ is even and hence β is even. Thus $n \leq \beta + \beta^6 \leq \beta^7$. Hence $|G| = mnq \leq \beta^{12}$, and the proof is complete.

REFERENCES

1. Brauer, R. and K. A. Fowler, "On groups of even order," Ann. of Math. (2), 62 (1955), 565-583.

2. Burnside, W., Theory of Groups of Finite Order. Dover, New York, 1955.

3. Curtis, W. and I. Reiner, Representation Theory of Finite Groups and Associative Algebras. Interscience, New York, 1962.

4. Feit, W., "On a class of doubly transitive permutation groups," Illinois Jnl. Math. 4 (1960), 170-186.

5. __________, "On groups which contain Frobenius groups as subgroups," First Symposium in Pure Mathematics. Amer. Math. Soc., New York, 1959.

6. __________, and J. Thompson, "Finite groups which contain a self-centralizing subgroup of order 3," Nagoya Math. Jnl., 19 (1961), 185-197.

7. Hall, M., The Theory of Groups. Macmillan, New York, 1959.

8. Ito, N., "On a class of doubly transitive permutation groups," Illinois Jnl. Math., 6 (1962), 341-352.

9. Ree, R., "Sur une famille de groupes de permutations doublement transitifs," Canadian Jnl. of Math., 16 (1964), 797-820.

10. Reynolds, W., "Modular representations of finite groups," Report on the Summer Institute on Finite Groups, (1960), 181-217.

11. Suzuki, M., "A new type of simple groups of finite order," Proc. Nat. Acad. Sci. U.S.A., 46 (1960), 868-870.

12. __________, "Finite groups with nilpotent centralizers," Trans. Amer. Math. Soc., 99 (1961), 425-470.

13. __________, "On a class of doubly transitive groups," Ann. of Math., 75 (1962), 105-145.

14. __________, "On a class of doubly transitive groups: II," Ann. of Math., 79 (1964), 514-589.

15. __________, "Two characteristic properties of (ZT)-groups," Osaka Math. Jnl., 15 (1963), 143-150.

16. Thompson, J., "Finite groups with fixed-point-free automorphisms of prime order," Proc. Nat. Acad. Sci. U. S. A., 45 (1959), 578-581.

17. Zassenhaus, H., "Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen," Abh. Math. Sem. Univ. Hamburg, 11 (1936), 17-40.

18. __________, The Theory of Groups. 2nd ed., Chelsea, New York, 1958.