ON A CLASS OF DOUBLY TRANSITIVE PERMUTATION GROUPS

BY

G. Glauberman

Let G be a finite permutation group. We say that G is a *Zassenhaus group* if G is doubly transitive and if no non-identity element of G leaves three or more symbols fixed. The Zassenhaus groups have been determined by Zassenhaus [7, 8], Feit [3], Suzuki [6], and Ito [5]. In this paper we present an alternate proof of Ito's result.

Theorem (Ito). *Let G be a Zassenhaus group of degree $m + 1$ that does not contain a regular normal subgroup. If m is a power of an odd prime p, then G has an Abelian Sylow p-subgroup.*

Our proof uses the notation of Feit [3]. Let N be the subgroup of G fixing one symbol, and let Q be the subgroup of G fixing an additional symbol. Let $g = |G|$ and $q = |Q|$. Since G has no regular normal subgroup, G is not a Frobenius group, and $q > 1$. Thus N acts as a Frobenius group on the symbols it moves. Let M be the regular normal subgroup of N. Thus $|M| = m$, and

$$N = MQ, \quad M \cap Q = 1, \quad |N| = mq, \quad g = (m + 1)|N| = (m + 1)mq.$$

We require the following result of Frobenius and Schur [4, (3.5), page 23]:

Theorem (Frobenius-Schur). *Let χ be an irreducible complex character of a finite group G. Let*

$$\nu(\chi) = (1/|G|) \textstyle\sum_{x \in G} \chi(x^2).$$

Then

(i) $\nu(\chi) = 0$ *if χ is not real-valued;*

(ii) $\nu(\chi) = 1$ *if χ is the character of a representation of G over the real numbers; and*

(iii) $\nu(\chi) = -1$ *otherwise.*

The following result is a slight variation on Lemma 4 of [1].

Theorem (Brauer). *Let G be a finite group of even order and let M be a subgroup of G. Suppose τ is an involution of G and U is a subset of M such that no element of U is a product of two conjugates of τ. Let θ be a generalized character of M that vanishes on $M - U$, and let θ^* be the generalized character of G induced by θ. Then*

$$\sum (\theta^*, \chi)_G \, \chi(\tau)^2/\chi(1) = 0,$$

where χ ranges over all the irreducible characters of G.

Proof. Let $x \in U$. Since x is not a product of two conjugates of τ, a well-

Received September 1, 1967.

known formula ((21), page 580, of [2]) yields

$$0 = \sum \frac{\chi(\tau)^2\chi(x^{-1})}{\chi(1)}.$$

Multiply the above equation by $\theta(x)$ and sum over all $x \in U$. We obtain

$$0 = \sum \frac{\chi(\tau)^2(\theta, \chi \mid_M)_M \mid M \mid}{\chi(1)}.$$

By the Frobenius Reciprocity Theorem, $(\theta, \chi\,|_M)_M = (\theta^*, \chi)_G$. This completes the proof of Brauer's Theorem.

We may now prove Ito's Theorem. Assume G satisfies the hypothesis of the theorem. By Lemma 3.1 of [3] we have

(1) $C(y) \subset M$ *for* $y \in M - \{1\}$;

(2) $M \cap xMx^{-1} = 1$ *for* $x \in G - N(M)$;

and $N(M) = MQ = N$. Now, MQ is a Frobenius group, so M must be Abelian if q is even (Satz 1 of [7]). Thus we may assume that q is odd. The proof of Lemma 3.2 of [3] shows that we may assume that

(3) *G is generated by the conjugates of M in G.*

Let us assume (3), and assume that q is odd. By Lemma 3.4 of [3], we obtain the following:

(4) *There is only one conjugate class of involutions in G; it contains mq elements. No elements of $M - \{1\}$ is a product of two involutions.*

We also obtain some consequences regarding the characters of M, N, and G. Here we use the notation of [3]. Let $\zeta_0, \zeta_1, \cdots$ be the irreducible characters of M, and let $z_i = \zeta_i(1)$. Denote by ζ_i^* and $\tilde{\zeta}_i$ the characters of G and N respectively induced by ζ_i. Let Let $\eta_0, \eta_1, \cdots, \eta_{q-1}$ be the irreducible characters of N which contain M in their kernels. Assume that ζ_0 and η_0 are principal characters and that $\bar{\eta}_i = \eta_{i+(q-1)/2}$ for $i = 1, \cdots, (q-1)/2$. By (18) and (19) of [3], the characters $\eta_1^*, \eta_2^*, \cdots, \eta_{(q-1)/2}^*$ are distinct and irreducible, and

(5) $$\eta_{i+(q-1)/2}^* = \eta_i^*, \qquad i = 1, 2, \cdots, (q-1)/2.$$

Since M is nilpotent, we may assume that $z_1 = 1$. Let $\zeta = \zeta_1$. Denote the restriction of a character θ of G to a subgroup H by $\theta\,|_H$. By (18) and (20) of [3] and by the Frobenius Reciprocity Theorem, we have

(6) $$\| \zeta^* \|^2 = q + 1,$$

and

(7) $(\zeta^*, \eta_i)_G$

$$= (\zeta, \eta_i\,|_M)_M = (1/m)(m + 1 + \textstyle\sum_{x \in M-\{1\}} \zeta(x)) = (1/m)m = 1$$

for $i = 1, \cdots, (q-1)/2$.

Recall that G is given as a permutation group. For each $x \in G$, let $\varphi(x)$ be the number of symbols fixed by x and let $\Gamma(x) = \varphi(x) - 1$. Let χ_0 be the principal character of G. By (2.3), (8.3), and (9.9) of [4], Γ is an irreducible character of G and

$$\eta_0^* = \varphi = \chi_0 + \Gamma. \tag{8}$$

Since $\varphi(x) = 1$ for all $x \in M - \{1\}$,

$$(\zeta^*, \Gamma)_G = (\zeta, \Gamma|_M)_M = (1/m)\zeta(1)\Gamma(1) = 1. \tag{9}$$

Similarly,

$$(\zeta^*, \chi_0)_G = (\zeta, \chi_0|_M)_M = (\zeta, \zeta_0)_M = 0. \tag{10}$$

By (5) and (8), we obtain

$$\begin{aligned} \zeta_0^* = (\tilde{\zeta}_0)^* &= (\eta_0 + \eta_1 + \cdots + \eta_{q-1})^* \\ &= \chi_0 + \Gamma + 2\eta_1^* + \cdots + 2\eta_{(q-1)/2}^*. \end{aligned} \tag{11}$$

Let $O(G)$ be the set of all elements of odd order in G. By considering cyclic subgroups of G, it is easy to see that the mapping given by $x \to x^2$ is a permutation of $O(G)$. Suppose $x \in G - O(G)$. By (1), x does not centralize any non-identity element of M. Hence x is not conjugate to an element of M, and $\zeta^*(x) = 0$. Similarly, $\zeta^*(x^2) = 0$ unless x is an involution. By (4) and (10), we have

$$\begin{aligned} &\textstyle\sum_{x\in G} \zeta^*(x^2) \\ &= qm\zeta^*(1) + \textstyle\sum_{x\in O(G)} \zeta^*(x^2) = qmq(m+1) + \textstyle\sum_{x\in O(G)} \zeta^*(x) \\ &= qg + \textstyle\sum_{x\in G} \zeta^*(x) = qg. \end{aligned} \tag{12}$$

For every irreducible character χ of G, let $c(\chi)$ be the multiplicity of χ in ζ^*, and define $\nu(\chi)$ as in the Frobenius-Schur Theorem. Then $\zeta^* = \sum c(\chi)\chi$. By (12),

$$q = (1/g)\textstyle\sum_{x\in G} \zeta^*(x^2) = (1/g)\sum_\chi c(\chi) \sum_{x\in G} \chi(x^2) = \sum_\chi c(\chi)\nu(\chi).$$

But by (6), $q + 1 = \sum c(\chi)^2$. Hence

$$1 = (q+1) - q = \textstyle\sum c(\chi)(c(\chi) - \nu(\chi)). \tag{13}$$

By the Frobenius-Schur Theorem, $\nu(\chi) = 0, 1$, or -1 for each irreducible character χ. Thus every summand in (13) is a nonnegative integer. Consequently, (13) shows that $c(\chi_1) = 1$ and $\nu(\chi_1) = 0$ for a unique irreducible character χ_1 and that

$$c(\chi) = \nu(\chi) = 1 \quad \text{or} \quad c(\chi) = 0, \quad \text{if } \chi \neq \chi_1. \tag{14}$$

Since $\nu(\chi_1) = 0$, χ_1 is not real-valued. Therefore,

$$\chi_1 \neq \chi_0, \Gamma, \eta_1^*, \cdots, \eta_{(q-1)/2}^*. \tag{15}$$

Let S be the set of all irreducible characters χ for which $c(\chi) \neq 0$ and $\chi \neq \chi_1, \Gamma, \eta_1^*, \cdots, \eta_{(q-1)/2}^*$. By (7), (9), (10), (14), and (15),

(16) $\quad \zeta_1^* = \zeta^* = \chi_1 + \Gamma + \eta_1^* + \cdots + \eta_{(q-1)/2}^* + \sum_{\chi \epsilon S} \chi, \quad$ and $\quad \chi_0 \notin S.$

Let $\mu = \zeta_1 - \zeta_0$, and let μ^* be the generalized character of G induced by μ. By (11) and (16),

(17) $\quad \mu^* = \zeta_1^* - \zeta_0^* = \chi_1 - \chi_0 - \eta_1^* - \cdots - \eta_{(q-1)/2}^* + \sum_{\chi \epsilon G} \chi.$

Let τ be an involution in G. As N has odd order,

$$\eta_1^*(\tau) = \cdots = \eta_{(q-1)/2}^*(\tau) = 0.$$

Since $\mu(1) = 0$ and no element of $M - \{1\}$ is a product of two involutions, Brauer's Theorem and (17) yield

$$0 = -1 + \chi_1(\tau)^2/\chi_1(1) + \sum_{\chi \epsilon S} \chi(\tau)^2/\chi(1).$$

Thus

(18) $$\chi_1(\tau)^2 \leqq \chi_1(1).$$

By (25.4), page 152 of [4], every irreducible character of N that does not contain M in its kernel has the form $\tilde{\zeta}_i$ for some $i > 0$; conversely, $\tilde{\zeta}_i$ is an irreducible character of N for every $i > 0$. Let n be the number of distinct characters of the form $\tilde{\zeta}_i$. We may assume that $\tilde{\zeta}_1, \cdots, \tilde{\zeta}_n$ are distinct. Now, $\tilde{\zeta}_1(1) = q\zeta_1(1) = q$; for some positive integer t we may assume that $\tilde{\zeta}_1, \cdots, \tilde{\zeta}_t$ have degree q and that $\tilde{\zeta}_{t+1}, \cdots, \tilde{\zeta}_n$ have larger degree (or that $t = n$).

Since N has odd order, none of the characters $\tilde{\zeta}_i$ is real-valued. Hence t and n are even, and we may assume that $\tilde{\zeta}_{2i-1}$ and $\tilde{\zeta}_{2i}$ are complex conjugates for $i = 1, 2, \cdots, n/2$. Since

$$\tilde{\bar{\zeta}}_{2i-1} = \bar{\tilde{\zeta}}_{2i-1} = \tilde{\zeta}_{2i} \quad \text{if } 1 \leqq i \leqq n/2,$$

we may assume that $\zeta_{2i} = \bar{\zeta}_{2i-1}$ for $i = 1, 2, \cdots, n/2$. Let $\chi_2 = \bar{\chi}_1$. As $\nu(\chi_1) = 0$, $\chi_2 \neq \chi_1$. By (14) and (16),

(19) $\quad \zeta_2^* = \bar{\zeta}_1^* = \overline{\zeta_1^*} = \chi_2 + \Gamma + \eta_1^* + \cdots + \eta_{(q-1)/2}^* + \sum_{\chi \epsilon S} \chi.$

Suppose $3 \leqq i \leqq n$. An easy argument shows that $\zeta_i^*(x) = \tilde{\zeta}_i(x)$ whenever $x \epsilon M - \{1\}$. Moreover, $\tilde{\zeta}_1 - \tilde{\zeta}_2$ vanishes on 1 and on $N - M$. Therefore, by (16) and (19),

$$\begin{aligned}(\chi_1 - \chi_2, \zeta_i^*)_G = (\zeta_1^* - \zeta_2^*, \zeta_i^*)_G &= (\tilde{\zeta}_1^* - \tilde{\zeta}_2^*, \zeta_i^*)_G \\ &= (\tilde{\zeta}_1 - \tilde{\zeta}_2, \zeta_i^* |_N)_N = (\tilde{\zeta}_1 - \tilde{\zeta}_2, \tilde{\zeta}_i)_N = 0.\end{aligned}$$

Hence

(20) $$(\chi_1, \zeta_i^*)_G = (\chi_2, \zeta_i^*)_G \quad \text{if } 3 \leqq i \leqq n.$$

Since inner products of characters are integers,

$$(\chi_2, \zeta_i^*)_G = \overline{(\chi_2, \zeta_i^*)_G} = (\bar{\chi}_2, \overline{\zeta_i^*})_G = (\chi_1, \bar{\zeta}_i^*)_G.$$

Thus, by (20),

$$(21) \qquad (\chi_1, \zeta^*_{2i-1})_G = (\chi_1, \zeta^*_{2i})_G \quad \text{if } 2 \leqq i \leqq n/2.$$

Assume that $3 \leqq i \leqq t$. Then $\tilde{\zeta}_i(1) = q = \tilde{\zeta}_1(1)$, so $z_i = z_1 = 1$. Our proof of (16) depends only on the assumption that $z_1 = 1$, and therefore a similar equation is valid for ζ^*_i. Hence ζ^*_i is the sum of a unique non-real irreducible character of G and several real-valued irreducible characters of G. By (20),

$$(22) \qquad (\chi_1, \zeta^*_i)_G = 0 \quad \textit{if } 3 \leqq i \leqq t.$$

Consider the restriction of χ_1 to N. By (5), (8), and (15), $(\chi_1, \lambda^*)_G = 0$ for every irreducible character λ of N that contains M in its kernel. By the Frobenius Reciprocity Theorem, $(\chi_1|_N, \lambda)_N = 0$ for every such λ. Consequently, $\chi_1|_N$ has the form $\sum \alpha_i \tilde{\zeta}_i$ for some nonnegative integers $\alpha_1, \alpha_2, \cdots, \alpha_n$. By (16), (19), (21), and (22),

$$(23) \qquad \chi_1|_N = \tilde{\zeta}_1 + \textstyle\sum_{t/2<i\leqq n/2} \alpha_{2i}(\tilde{\zeta}_{2i-1} + \tilde{\zeta}_{2i}).$$

Suppose $t < i \leqq n$. Since $z_i > 1$ and M is a p-group, z_i is a power of p. Now, $\tilde{\zeta}_i(1) = qz_i$. By (23) we obtain

$$\chi_1(1) \equiv \tilde{\zeta}_1(1) \equiv 0, \qquad \text{mod } q,$$

$$\chi_1(1) \equiv \tilde{\zeta}_1(1) \equiv q \not\equiv 0, \quad \text{mod } p,$$

and

$$\chi_1(1) \equiv \tilde{\zeta}_1(1) + \textstyle\sum_{t/2<i\leqq n/2} 2\alpha_{2i}\tilde{\zeta}_{2i-1}(1) \equiv \tilde{\zeta}_1(1) \equiv q \not\equiv 0 \quad \text{mod } 2.$$

Let $\chi_1(1) = qx$, and let $m = p^e$. Since $g = qm(m+1) = qp^e(m+1)$, x divides $m + 1$.

Let τ be an involution in G. Since $\tau^2 = 1$, the eigenvalues of a matrix representing τ are 1 and -1. Suppose 1 occurs with multiplicity a and -1 occurs with multiplicity b. Then

$$\chi_1(\tau) \equiv a - b \equiv a + b \equiv \chi_1(1) \not\equiv 0 \quad \text{mod } 2.$$

Therefore, $\chi_1(\tau) \neq 0$. By (4), τ has mq conjugates in G. Therefore, $mq\chi_1(\tau)/\chi_1(1)$ is an algebraic integer. Since $\chi_1(1) = qx$, x divides $m\chi_1(\tau)$. As x divides $m + 1$, x divides $\chi_1(\tau)$. By (18), $x^2 \leqq \chi_1(\tau)^2 \leqq \chi_1(1) = xq$. Thus $\chi_1(1) \leqq qx \leqq q^2$. However, by (28) of [3], we obtain

$$q^4 \geqq \chi_1(1)^2 \geqq 1 + (\tfrac{1}{2})(q-1)(m+1).$$

Therefore, $q^4 > (q/4)(m+1)$, and

$$(24) \qquad m < 4q^3.$$

Since N is a Frobenius group, q divides $m - 1$. Let d be the smallest positive integer such that q divides $p^d - 1$. By the Euclidean Algorithm, the congruence $p^e \equiv 1 \text{ mod } q$, implies that d divides e. Let $e = kd$. Since q is odd and $p^d - 1$ is even, $2q$ divides $p^d - 1$. By (24),

$$4q^3 > m = p^e = p^{kd} \geqq (2q+1)^k.$$

Therefore, $k = 1$ or 2.

Suppose $k = 2$. Since p is odd, $m \equiv (p^d)^2 \equiv 1 \bmod 4$, so $m + 1 \equiv 2 \bmod 4$. No involution in G fixes any of the permuted symbols. Therefore every involution is a product of $(m+1)/2$ disjoint transpositions and is thus an odd permutation. Consequently, the even permutations in G form a normal subgroup of index two, contrary to our assumption that the conjugates of M generate G. Hence $k = 1$, and $m = p^d$. Let M' be the derived group of M. Then N/M' is a Frobenius group, so q divides $|M/M'| - 1$ and $|M/M'|$ is a power of p^d. Since $|M| = p^d$, $M' = 1$. This completes the proof of Ito's Theorem.

The author thanks the National Science Foundation and the Sloan Foundation for their support.

BIBLIOGRAPHY

1. R. BRAUER, *Some applications of the theory of blocks of characters of finite groups II*, J. Algebra, vol. 1 (1964), pp. 307–334.
2. R. BRAUER AND K. A. FOWLER, *On groups of even order*, Ann. of Math. (2), vol. 62 (1955), pp. 565–583.
3. W. FEIT, *On a class of doubly transitive permutation groups*, Illinois J. Math., vol. 4 (1960), pp. 170–186.
4. ———, *Characters of finite groups*, mimeographed notes, Mathematics Department, Yale University, 1965.
5. N. ITO, *On a class of doubly transitive permutation groups*, Illinois J. Math., vol. 6 (1962), pp. 341–352.
6. M. SUZUKI, *On a class of doubly transitive groups*, Ann. of Math., vol. 75 (1962), pp. 105–145.
7. H. ZASSENHAUS, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg, vol. 11 (1934), pp. 17–40.
8. H. ZASSENHAUS, *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg., vol. 11 (1935), pp. 187–220.

UNIVERSITY OF CHICAGO
CHICAGO, ILLINOIS
UNIVERSITY OF WARWICK
COVENTRY, ENGLAND