ON A CLASS OF DOUBLY TRANSITIVE PERMUTATION GROUPS[1]

BY

NOBORU ITO

Let Ω be the set of symbols $1, \cdots, m+1$. Let $\mathfrak{G}$ be a doubly transitive permutation group on Ω in which no nontrivial permutation leaves three symbols fixed. Such a group $\mathfrak{G}$ will be called a Zassenhaus group.

On the structure of Zassenhaus groups Feit [4] proved recently the following elegant theorem: Let $\mathfrak{G}$ be a Zassenhaus group of degree $m + 1$, which contains no normal subgroup of order $m + 1$. Then m must be a power of a prime number: $m = p^e$. Let $\mathfrak{M}$ be a Sylow p-subgroup of $\mathfrak{G}$, and let $\mathfrak{M}'$ be the commutator subgroup of $\mathfrak{M}$. Then the index of $\mathfrak{M}'$ in $\mathfrak{M}$ must be smaller than $4q^2$, where q is the order of the subgroup $\mathfrak{Q}$, which consists of all the permutations leaving each of the symbols 1 and 2 fixed. Moreover if $\mathfrak{M}$ is abelian, then $q \geqq (m-1)/2$.

Now the purpose of this paper is to prove the following.

THEOREM. *If m is odd, then $\mathfrak{M}$ must be abelian.*

1. In the following $\mathfrak{G}$ denotes always a Zassenhaus group of even degree $m + 1$, which contains no normal subgroup of order $m + 1$. Let Γ_i $(i = 0, 1, 2)$ be the set of all the permutations in $\mathfrak{G}$, each of which fixes just i symbols of Ω. Then according to our assumptions on $\mathfrak{G}$ we obtain the following decomposition of $\mathfrak{G}$ into its mutually disjoint subsets: $\mathfrak{G} = \Gamma_0 + \Gamma_1 + \Gamma_2 + \{1\}$, where 1 is the identity element of $\mathfrak{G}$.

Since $\mathfrak{G}$ is doubly transitive, $\mathfrak{G}$ possesses an irreducible character $\mathbf{B}$, whose values can be written as follows:

$$(1) \qquad \mathbf{B}(X) = \begin{cases} m & \text{for } X = 1, \\ 1 & \text{for } X \in \Gamma_2, \\ 0 & \text{for } X \in \Gamma_1, \\ -1 & \text{for } X \in \Gamma_0. \end{cases}$$

2. Let $\mathfrak{G}_1$ be the subgroup of $\mathfrak{G}$, which consists of all the permutations leaving the symbol 1 fixed. Then we can choose an $\mathfrak{M}$ in the theorem of Feit in the following way: $\mathfrak{M}$ is a normal subgroup of $\mathfrak{G}_1$ and satisfies the conditions that $\mathfrak{G}_1 = \mathfrak{M}\mathfrak{Q}$ and $\mathfrak{M} \cap \mathfrak{Q} = 1$. Now we assume that

(2.1) $\mathfrak{M}$ *is not abelian.*

Therefore the purpose of our proof is to derive a contradiction from this

Received April 5, 1961.

[1] This research was supported in part by the United States Air Force.

assumption, which is achieved at the end of this paper. The following facts about $\mathfrak{Q}$ are known [4, Lemma 3.3]:

(2.2) *$\mathfrak{Q}$ is cyclic, q is odd > 1, $m \equiv 1 \pmod{q}$, the normalizer of $\mathfrak{Q}$ in $\mathfrak{G}$ is a dihedral group of order $2q$, and the centralizer of every nonidentity element of $\mathfrak{Q}$ coincides with $\mathfrak{Q}$.*

In particular $\mathfrak{M}$ is the commutator subgroup of $\mathfrak{G}_1$. Let $\eta_0, \eta_1, \cdots, \eta_{q-1}$ be the linear characters of $\mathfrak{G}_1$, where η_0 is the principal character of $\mathfrak{G}_1$, and $\eta_{i+(q-1)/2} = \bar{\eta}_i$ for $i = 1, \cdots, \frac{1}{2}(q-1)$. Let X be an element of Γ_2. Then by the double transitivity of $\mathfrak{G}$ there exists an element X^* in $\mathfrak{Q}$, which is conjugate to X.

Now let $\mathbf{A}_i$ denote the character of $\mathfrak{G}$ induced by η_i $(i = 1, \cdots, \frac{1}{2}(q-1))$. Then $\mathbf{A}_1, \cdots, \mathbf{A}_{(q-1)/2}$ are distinct irreducible characters of $\mathfrak{G}$, and the values of $\mathbf{A}_i$ can be written as follows [4, pp. 182–183]:

$$\mathbf{A}_i(X) = \begin{cases} m+1 & \text{for} \quad X = 1, \\ \eta_i(X^*) + \bar{\eta}_i(X^*) & \text{for} \quad X \in \Gamma_2, \\ 1 & \text{for} \quad X \in \Gamma_1, \\ 0 & \text{for} \quad X \in \Gamma_0. \end{cases} \tag{2}$$
$$(i = 1, \cdots, \tfrac{1}{2}(q-1)).$$

Let $X \neq 1$ be an element of $\mathfrak{Q}$. Then by (2) we have

$$\begin{aligned} \textstyle\sum_{i=1}^{(q-1)/2} \mathbf{A}_i(X)\bar{\mathbf{A}}_i(X) &= \textstyle\sum_{i=1}^{(q-1)/2} (\eta_i(X) + \bar{\eta}_i(X))\overline{(\eta_i(X) + \bar{\eta}_i(X))} \\ &= \textstyle\sum_{i=1}^{q-1} \eta_i(X)\bar{\eta}_i(X) + \sum_{i=1}^{q-1} \eta_i^2(X). \end{aligned}$$

Since the order of $\mathfrak{Q}$ is odd, $\eta_1^2, \cdots, \eta_{q-1}^2$ are all distinct and are the same as $\eta_1, \cdots, \eta_{q-1}$ in some order. Therefore we have

$$\textstyle\sum_{i=1}^{q-1} \eta_i(X)\bar{\eta}_i(X) = \sum_{i=0}^{q-1} \eta_i(X)\bar{\eta}_i(X) - 1 = q - 1$$

and

$$\textstyle\sum_{i=1}^{q-1} \eta_i^2(X) = \sum_{i=0}^{q-1} \eta_i(X) - 1 = -1.$$

Thus we have obtained the following equation:

$$\textstyle\sum_{i=1}^{(q-1)/2} \mathbf{A}_i(X)\bar{\mathbf{A}}_i(X) = q - 2. \tag{3}$$

3. LEMMA A. *Any irreducible character* $\mathbf{X}$ *of* $\mathfrak{G}$ *different from* $\mathbf{E}$, $\mathbf{B}$, *and* $\mathbf{A}_i$ $(i = 1, \cdots, \frac{1}{2}(q-1))$ *has degree divisible by q, where* $\mathbf{E}$ *is the principal character of* $\mathfrak{G}$.

Proof. Let $X \neq 1$ be any element of $\mathfrak{Q}$. By (2.2) the centralizer of X in $\mathfrak{G}$ is $\mathfrak{Q}$. By the orthogonality relations for the group characters we have

$$\begin{aligned} q &= \mathbf{E}(X)\bar{\mathbf{E}}(X) + \mathbf{B}(X)\bar{\mathbf{B}}(X) + \textstyle\sum_{i=1}^{(q-1)/2} \mathbf{A}_i(X)\bar{\mathbf{A}}_i(X) \\ &\quad + \mathbf{X}(X)\bar{\mathbf{X}}(X) + \cdots \\ &= q + \mathbf{X}(X)\bar{\mathbf{X}}(X) + \cdots \qquad \text{(by (3))}. \end{aligned}$$

Thus we have $\mathbf{X}(X) = 0$. Again by the orthogonality relations for the group characters we have

$$\mathbf{X}(1) = \sum_{X \in \mathfrak{Q}} \mathbf{X}(X) \equiv 0 \pmod{q}.$$

4. Let X and Y be two distinct elements of $\mathfrak{Q}$. Assume that there exists an element Z of $\mathfrak{G}$ such that $Y = Z^{-1}XZ$. Then Y belongs to $\mathfrak{Q} \cap Z^{-1}\mathfrak{Q}Z$, which implies by (2.2) that $\mathfrak{Q} = Z^{-1}\mathfrak{Q}Z$ and $Y = X^{-1}$. Thus the elements of Γ_2 fall into $\frac{1}{2}(q-1)$ classes of conjugate elements in $\mathfrak{G}$. Let $\mathfrak{L}_1, \cdots, \mathfrak{L}_{(q-1)/2}$ be the classes of conjugate elements in $\mathfrak{G}$ from Γ_2.

The following fact is known [4, Lemma 3.4]:

(4.1) *$\mathfrak{G}$ contains only one class of involutions, and there are mq involutions in $\mathfrak{G}$. No element $\neq 1$ of $\mathfrak{M}$ is the product of two involutions.*

Let $\mathfrak{K}_1, \cdots, \mathfrak{K}_n$ be the classes of conjugate elements in $\mathfrak{G}$ from Γ_0, where $\mathfrak{K}_1$ is the class of involutions. Then using (2.2), (4.1), and [2, Lemmas (2.A) and (2.B)] we have

$$\mathfrak{K}_1^2 = \sum_{i=1}^{n} c_i \mathfrak{K}_i + q \sum_{i=1}^{(q-1)/2} \mathfrak{L}_i + mq \cdot 1, \tag{4}$$

where c_i is explained as follows: Let G_i be an element in $\mathfrak{K}_i$. Then for $i > 1$, c_i equals the number of involutions in $\mathfrak{G}$, which transform G_i into G_i^{-1}, and $c_1 + 1$ equals the number of involutions in the centralizer of an involution.

If either $i = 1$ or $i > 1$ and $c_i > 0$, then the class $\mathfrak{K}_i$ and the elements in $\mathfrak{K}_i$ are called real. (Though the usual definitions of real class and real element are more general [2, p. 565], they coincide in this particular case, by Lemma B below, with ours.)

Put $G_1 = J$. Applying the orthogonality relations of group characters and using (1) and (2), we obtain from (4) the following equation of Brauer-Fowler [2, (23)][2]

$$c_i = \frac{mq}{m+1}\left(1 - \frac{1}{m} + \sum_{\mathbf{Z}} \frac{\mathbf{Z}(J)^2\mathbf{Z}(G_i)}{\mathbf{Z}(1)}\right), \tag{5}$$

where $\mathbf{Z}$ ranges over all the irreducible characters of $\mathfrak{G}$ distinct from $\mathbf{E}$, $\mathbf{B}$, and $\mathbf{A}_i$ $(i = 1, \cdots, \frac{1}{2}(q-1))$.

5. LEMMA B. *Every class $\mathfrak{K}_i$ is real.*

Proof. For some $i > 1$ let us assume that $c_i = 0$. Then we have from (5) the equation

$$1 - \frac{1}{m} + \sum_{\mathbf{Z}} \frac{\mathbf{Z}(J)^2\mathbf{Z}(G_i)}{\mathbf{Z}(1)} = 0.$$

---

[2] See W. BURNSIDE, *Theory of groups of finite order*, 2nd ed., Cambridge, University Press, 1911, p. 288.

Since $m = p^e$, it can be seen at once from this equation that there must be an irreducible character $\mathbf{X}$ of $\mathfrak{G}$ distinct from $\mathbf{E}$, $\mathbf{B}$, and $\mathbf{A}_i$ $(i = 1, \cdots, \frac{1}{2}(q-1))$ whose degree is divisible by m. By Lemma A the degree of $\mathbf{X}$ is divisible by q, too. Since m and q are relatively prime, we have $\mathbf{X}(1) = xmq$. Since the order of $\mathfrak{G}$ equals the sum of the squares of the degrees of all the irreducible characters of $\mathfrak{G}$, we have the inequality $(m+1)mq > x^2m^2q^2$, which implies that $m + 1 > x^2mq$. This is a contradiction, because q is greater than 1 by (2.2).

As an important consequence of Lemma B we have

LEMMA C. *$\mathfrak{G}$ possesses only one 2-block of the highest defect, namely the principal 2-block $B_1(2)$.*

Proof. By a theorem of Brauer-Nesbitt [3, Theorem 2] it is enough to show that the centralizer of a Sylow 2-subgroup $\mathfrak{T}$ of $\mathfrak{G}$ is contained in $\mathfrak{T}$. Assume that an element $X \neq 1$ of odd order is commutative with every element of $\mathfrak{T}$. By (4.1) and (2.2), X must belong to Γ_0. Hence X is real by Lemma B. Then the centralizer $\mathfrak{C}(X)$ of X has index 2 in the generalized centralizer of X, which consists of all the elements Y such that $Y^{-1}XY = X^{\pm 1}$. Since $\mathfrak{C}(X)$ contains the Sylow 2-subgroup $\mathfrak{T}$ of $\mathfrak{G}$, this is a contradiction.

6. LEMMA D. $m + 1 \equiv 0 \pmod 4$.

Proof. If not, the order of $\mathfrak{G}$ is not divisible by 4, and $\mathfrak{G}$ contains a normal subgroup of index 2, which contains $\mathfrak{M}$. Therefore by Sylow's theorem the normalizer of $\mathfrak{M}$ contains an involution, which implies the commutativity of $\mathfrak{M}$, contradicting our assumption (2.1).

LEMMA E. *The number of irreducible characters in $B_1(2)$ is less than $\frac{1}{2}p^2$.*

Proof. By Lemma D we have $p \equiv -1 \pmod 4$ and $e \equiv 1 \pmod 2$. Hence

$$\frac{m+1}{p+1} = \frac{1-(-p)^e}{1-(-p)} = 1 + (-p) + \cdots + (-p)^{e-1} \equiv 1 \pmod 2.$$

Put $p + 1 = 2^a b$, where b is an odd number. Then the order of a Sylow 2-subgroup of $\mathfrak{G}$ equals 2^a. By a theorem of Brauer-Feit [1, Theorem 1] the number of irreducible characters in $B_1(2)$ is at most 2^{2a-2}. We see that

$$2^{2a-2} \leqq \tfrac{1}{4}(p+1)^2 < \tfrac{1}{2}p^2.$$

7. Let $\mathfrak{M} = \mathfrak{M}_1 \supset \mathfrak{M}_2 \supset \cdots \supset \mathfrak{M}_r \supset 1$ be a series of normal subgroups of $\mathfrak{M}$. It is called a principal $\mathfrak{Q}$-series, if every $\mathfrak{M}_i$ is $\mathfrak{Q}$-invariant and there is no $\mathfrak{Q}$-invariant normal subgroup of $\mathfrak{M}$ between $\mathfrak{M}_i$ and $\mathfrak{M}_{i+1}$, which is distinct from $\mathfrak{M}_i$ and $\mathfrak{M}_{i+1}$ $(i = 1, \cdots, r; \mathfrak{M}_{r+1} = 1)$. Put $\mathfrak{M}:\mathfrak{M}' = p^d$.

LEMMA F. *Let $\mathfrak{M} = \mathfrak{M}_1 \supset \mathfrak{M}_2 \supset \cdots \supset \mathfrak{M}_r \supset 1$ be a principal $\mathfrak{Q}$-series of $\mathfrak{M}$. Then we have $\mathfrak{M}_2 = \mathfrak{M}'$ and $\mathfrak{M}_i:\mathfrak{M}_{i+1} = p^d$ $(i = 1, \cdots, r)$. In particular we have $e = rd$ with odd r, $d > 1$.*

Proof. Since it is well known that the degrees of all the irreducible representations of a finite cyclic group over a prime field are equal, it is enough to prove $\mathfrak{M}_2 = \mathfrak{M}'$. It is clear that $\mathfrak{M}_2 \supseteqq \mathfrak{M}'$. If $\mathfrak{M}_2 \neq \mathfrak{M}'$, then we have $\mathfrak{M}:\mathfrak{M}_2 \equiv 1 \pmod q$ and $\mathfrak{M}_2:\mathfrak{M}' \equiv 1 \pmod q$. Therefore we have

$$\mathfrak{M}:\mathfrak{M}_2 \geqq 2q+1, \quad \mathfrak{M}_2:\mathfrak{M}' \geqq 2q+1, \quad \text{and} \quad \mathfrak{M}:\mathfrak{M}' \geqq 4q^2+4q+1,$$

which contradicts the theorem of Feit. Therefore we must have $\mathfrak{M}_2 = \mathfrak{M}'$.

Let $1 = p^{f_1} < p^{f_2} < p^{f_3} < \cdots < p^{f_s}$ be the degrees of all the irreducible characters of $\mathfrak{M}$. Let e_i^* be the number of irreducible characters of $\mathfrak{M}$ of degree p^{f_i} $(i = 2, \cdots, s)$. Put $e_1^* + 1 = p^d$. Then by Lemma F, $e_1^* + 1$ is the number of linear characters of $\mathfrak{M}$. By the orthogonality relations for the group characters we have

$$m = p^d + e_2^* p^{2f_2} + \cdots + e_s^* p^{2f_s}. \tag{6}$$

The following fact is known [4, Lemma 2.2]:

(7.1) *e_i^* is divisible by q $(i = 1, \cdots, s)$. $\mathfrak{G}_1$ possesses $e_i = e_i^*/q$ irreducible characters $\phi_{i1}, \cdots, \phi_{ie_i}$ of degree $p^{f_i}q$, which are induced by the characters of $\mathfrak{M}$.*

Since p is odd, $\mathfrak{M}$ has no real irreducible character except the principal character. Therefore e_i^* is even $(i = 1, \cdots, s)$. Since q is odd, e_i is also even $(i = 1, \cdots, s)$.

8.[3] The centralizer of any element of $\mathfrak{M} - \{1\}$ is contained in $\mathfrak{G}_1$. By (7.1) every character ϕ_{ij} vanishes outside $\mathfrak{M}$, and e_i is even $(i = 1, \cdots, s;$ $j = 1, \cdots, e_i)$. Let ϕ_{ij}^* be the character of $\mathfrak{G}$ induced by ϕ_{ij}. Then by theorems of Suzuki [5, Lemmas 4 and 5] we have $\phi_{ij}^*(X) = \phi_{ij}(X)$ for any element of $\mathfrak{M} - \{1\}$, and there exist e_i different irreducible characters $\mathbf{C}_{ij}$ $(j = 1, \cdots, e_i)$ of $\mathfrak{G}$ for each i $(i = 1, \cdots, s)$, and the decomposition of ϕ_{ij}^* into its irreducible components can be written as follows (by using (1) and (2)):

$$(7_i) \qquad \begin{aligned} \phi_{i1}^* &= \varepsilon_i \mathbf{C}_{i1} + a_{ii}\textstyle\sum_{j=1}^{e_i} \mathbf{C}_{ij} + p^{f_i}\sum_{i=1}^{(q-1)/2} \mathbf{A}_i + p^{f_i}\mathbf{B} + \Delta_i^*, \\ &\vdots \\ \phi_{ie_i}^* &= \varepsilon_i \mathbf{C}_{ie_i} + a_{ii}\textstyle\sum_{j=1}^{e_i} \mathbf{C}_{ij} + p^{f_i}\sum_{i=1}^{(q-1)/2} \mathbf{A}_i + p^{f_i}\mathbf{B} + \Delta_i^* \end{aligned}$$

$$(i = 1, \cdots, s),$$

where $\varepsilon_i = \pm 1$, a_{ii} and $a_{ii} + \varepsilon_i$ are nonnegative integers, and Δ_i^* is a linear combination of irreducible characters of $\mathfrak{G}$, which are distinct from $\mathbf{E}$, $\mathbf{B}$, $\mathbf{C}_{ij}$ $(j = 1, \cdots, e_i)$, and $\mathbf{A}_k$ $(k = 1, \cdots, \frac{1}{2}(q-1))$, with nonnegative integral coefficients.

LEMMA G. *All the characters $\mathbf{C}_{ij}$ $(j = 1, \cdots, e_i;\ i = 1, \cdots, s)$ are different.*

[3] See [5, Section II].

Proof. First assume that some $\mathbf{C}_{ij}$ is real. Then since the order of $\mathfrak{G}_1$ is odd, the principal character is the only real character of $\mathfrak{G}_1$. Let $\phi_{ij'}$ be the complex-conjugate character of ϕ_{ij}. Then j and j' are different. From (7_i) we have the equation $\phi_{ij}^* - \phi_{ij'}^* = \varepsilon_i(\mathbf{C}_{ij} - \mathbf{C}_{ij'})$. Transferring to complex-conjugate characters we have $\phi_{ij'}^* - \phi_{ij}^* = \varepsilon_i(\mathbf{C}_{ij} - \bar{\mathbf{C}}_{ij'})$. Adding these two equations we have

$$0 = \varepsilon_i(2\mathbf{C}_{ij} - \mathbf{C}_{ij'} - \bar{\mathbf{C}}_{ij'}),$$

which implies that $\mathbf{C}_{ij} = \mathbf{C}_{ij'}$. This contradicts a theorem of Suzuki [5, Lemma 5]. Hence no $\mathbf{C}_{ij}$ is real.

Now we assume that there exist two different numbers i and k such that $\mathbf{C}_{ij} = \mathbf{C}_{kl}$ for some j and l $(j = 1, \cdots, e_i;\ l = 1, \cdots, e_k)$. Let $\phi_{ij'}$ and $\phi_{kl'}$ be the complex-conjugate characters of ϕ_{ij} and ϕ_{kl}. Then from (7_i) and (7_k) we have the equation

$$\phi_{ij}^* - \phi_{ij'}^* = \varepsilon_i(\mathbf{C}_{ij} - \bar{\mathbf{C}}_{ij}) = \pm\varepsilon_k(\mathbf{C}_{kl} - \bar{\mathbf{C}}_{kl}) = \pm(\phi_{kl}^* - \phi_{kl'}^*).$$

In particular for any element X from $\mathfrak{M} - \{1\}$ we have by a theorem of Suzuki [5, Lemma 4]

$$\phi_{ij}(X) - \phi_{ij'}(X) = \pm(\phi_{kl}(X) - \phi_{kl'}(X)),$$

which contradicts the linear independence of $\phi_{11}, \cdots, \phi_{se_s}$.

Now the systems of equations $(7_1), \cdots, (7_s)$ can be rewritten as follows:

$$(7)\quad \begin{aligned}
\phi_{11}^* &= \varepsilon_1 \mathbf{C}_{11} + a_{11}\textstyle\sum_{i=1}^{e_1} \mathbf{C}_{1i} + a_{12}\sum_{i=1}^{e_2} \mathbf{C}_{2i} + \cdots \\
&\qquad + a_{1s}\textstyle\sum_{i=1}^{e_s} \mathbf{C}_{si} + \sum_{i=1}^{(q-1)/2} \mathbf{A}_i + \mathbf{B} + \Delta_1 . \\
&\ \vdots \\
\phi_{1e_1}^* &= \varepsilon_1 \mathbf{C}_{1e_1} + a_{11}\textstyle\sum_{i=1}^{e_1} \mathbf{C}_{1i} + a_{12}\sum_{i=1}^{e_2} \mathbf{C}_{2i} + \cdots \\
&\qquad + a_{1s}\textstyle\sum_{i=1}^{e_s} \mathbf{C}_{si} + \sum_{i=1}^{(q-1)/2} \mathbf{A}_i + \mathbf{B} + \Delta_1 , \\
&\ \vdots \\
\phi_{s1}^* &= a_{s1}\textstyle\sum_{i=1}^{e_1} \mathbf{C}_{1i} + \cdots + a_{s,s-1}\sum_{i=1}^{e_{s-1}} \mathbf{C}_{s-1,i} + \varepsilon_s \mathbf{C}_{s1} \\
&\qquad + a_{ss}\textstyle\sum_{i=1}^{e_s} \mathbf{C}_{si} + p^{f_s}\sum_{i=1}^{(q-1)/2} \mathbf{A}_i + p^{f_s}\mathbf{B} + \Delta_s , \\
&\ \vdots \\
\phi_{se_s}^* &= a_{s1}\textstyle\sum_{i=1}^{e_1} \mathbf{C}_{1i} + \cdots + a_{s,s-1}\sum_{i=1}^{e_{s-1}} \mathbf{C}_{s-1,i} + \varepsilon_s \mathbf{C}_{se_s} \\
&\qquad + a_{ss}\textstyle\sum_{i=1}^{e_s} \mathbf{C}_{si} + p^{f_s}\sum_{i=1}^{(q-1)/2} \mathbf{A}_i + p^{f_s}\mathbf{B} + \Delta_s ,
\end{aligned}$$

where the a_{ij} are nonnegative integers and Δ_i is a linear combination of irreducible characters of $\mathfrak{G}$, which are distinct from $\mathbf{E}$, $\mathbf{B}$, $\mathbf{A}_k$ $(k = 1, \cdots, \frac{1}{2}(q-1))$, and $\mathbf{C}_{ij}$ $(i = 1, \cdots, s;\ j = 1, \cdots, e_i)$, with nonnegative integral coefficients. Let $\mathbf{X}$ be a linear combination of irreducible characters of $\mathfrak{G}$ with integral coefficients: $\sum_{\mathbf{Z}} a_{\mathbf{Z}}\, \mathbf{Z}$, where $\mathbf{Z}$ ranges over all irreducible characters of $\mathfrak{G}$. Then the number $\sum_Z a_Z^2$ is called the norm of X. Now the following two facts about the system of equations (7) are known [5, Lemma 4]:

(8.1) *The norm of* ϕ_{1i}^* *equals* $q+1$ $(i = 1, \cdots, e_1)$.

(8.2) *The norm of* $p^{f_j - f_i}\phi_{ik}^* - \phi_{jl}^*$ $(i<j)$ *equals* $p^{2(f_j - f_i)} + 1$ $(i, j = 1, \cdots, s; k = 1, \cdots, e_i; l = 1, \cdots, e_j)$.

9. LEMMA H.

$$(8) \qquad 2 + e_1 + e_2 + \cdots + e_s < \tfrac{1}{2}p^2.$$

Proof. The number of distinct $\mathbf{C}_{ij}$'s equals $e_1 + e_2 + \cdots + e_s$. Hence by Lemmas C and E it is enough to show that the degrees of the $\mathbf{C}_{ij}$ are odd. Now by the reciprocity theorem of Frobenius we obtain from (1), (2), and (7) the equation valid for all elements of $\mathfrak{G}_1$

$$C_{ij} = \cdots + a_{i-1,i}\sum_{k=1}^{e_{i-1}}\phi_{i-1,k} + (\varepsilon_i\phi_{ij} + a_{ii}\sum_{k=1}^{e_i}\phi_{ik}) + a_{i+1,i}\sum_{k=1}^{e_{i+1}}\phi_{i+1,k} + \cdots.$$

Since all the e_i's are even and the degrees of all the ϕ_{kl}'s are odd, we see that $\mathbf{C}_{ij}(1) \equiv 1 \pmod 2$.

Now we can prove the following:

LEMMA I. (i) $f_{2l+1} = ld \quad (l = 0, 1, \cdots)$;

$f_{2l} = \tfrac{1}{2}((2l-1)d - 1) \quad (l = 1, 2, \cdots)$,

(ii) $e_{2l+1} = (p^d - 1)/q \quad (l = 0, 1, \cdots)$;

$e_{2l} = p(p^d - 1)/q \quad (l = 1, 2, \cdots)$,

(iii) $r = s$.

Proof. By Lemma F, our assertion is true for f_1 and e_1. Then from (6) we obtain the equation

$$(6') \quad p^d(p^d - 1)(p^{(r-2)d} + \cdots + p^d + 1) = e_2^*\,p^{2f_2} + \cdots + e_s^*\,p^{2f_s}.$$

Since d is odd, we have $2f_2 < d$. If $2f_2 < d - 1$, we obtain from (6′) the congruence $e_2^* \equiv 0 \pmod{p^2}$, which implies the congruence $e_2 \equiv 0 \pmod{p^2}$. This contradicts Lemma G. Hence we must have $2f_2 = d - 1$.

Now let $\mathfrak{M} = \mathfrak{M}_1 \supset \mathfrak{M}_2 \supset \mathfrak{M}_3 \supset \cdots$ be a principal $\mathfrak{Q}$-series of $\mathfrak{M}$, and let us consider the factor group $\mathfrak{M}/\mathfrak{M}_3$ of order p^{2d} of $\mathfrak{M}$. By Lemma F, $\mathfrak{M}_2/\mathfrak{M}_3$ is the commutator subgroup of $\mathfrak{M}/\mathfrak{M}_3$. Hence it is easily seen that $\mathfrak{M}_2/\mathfrak{M}_3$ is the center of $\mathfrak{M}/\mathfrak{M}_3$. Since d is odd, the degree of any irreducible character of $\mathfrak{M}/\mathfrak{M}_3$ divides[4] $p^{(d-1)/2}$. Then from above we see that the degrees of all the

[4] The square of the degree of an irreducible character of a p-group divides the index of the center in the whole group.

nonlinear irreducible characters of $\mathfrak{M}/\mathfrak{M}_3$ must be equal to $p^{(d-1)/2}$. Let e_2' be the number of irreducible characters of degree $p^{(d-1)/2}$ of $\mathfrak{M}/\mathfrak{M}_3$. Then corresponding to (6) we have the following equation $p^{2d} = p^d + e_2' p^{d-1}$, which implies $e_2' = p(p^d - 1)$. Since clearly $e_2' \leqq e_2^*$, and since $e_2 < p^2$ by Lemma H, we have the following inequality:

$$(9) \qquad (p^d - 1)/q < p.$$

Now let us assume $k > 1$ and that our assertion is true for e_i and f_i $(i = 1, \cdots, k-1)$. Then it follows from our assumption that

$$\begin{aligned}\textstyle\sum_{i=1}^{k-1} e_i^* p^{2f_i} &= (p^d - 1) + p(p^d - 1)p^{d-1} + (p^d - 1)p^{2d} + \cdots \\ &= p^{(k-1)d} - 1.\end{aligned}$$

Now from (6) we obtain the following equation

$$(6'') \quad p^{(k-1)d}(p^d - 1)(p^{(r-k)d} + \cdots + p^d + 1) = e_k^* p^{2f_k} + \cdots .$$

This implies the inequality $(k-1)\,d \geqq 2f_k$. If $(k-1)\,d \geqq 2f_k + 2$, then from (6″) we have the congruence $e_k^* \equiv 0 \pmod{p^2}$, and therefore the congruence $e_k \equiv 0 \pmod{p^2}$, contradicting Lemma H. Hence we must have

$$(k-1)\,d = \begin{cases} 2f_k & \text{if k is odd,} \\ 2f_k + 1 & \text{if k is even.} \end{cases}$$

Putting these values in (6″) we have

$$(p^d - 1)(1 + p^d + \cdots) = e_k^* + e_{k+1}^* p^{2f_{k+1} - 2f_k} + \cdots \quad \text{when } k \text{ is odd,}$$

$$p(p^d - 1)(1 + p^d + \cdots) = e_k^* + e_{k+1}^* p^{2f_{k+1} - 2f_k} + \cdots \quad \text{when } k \text{ is even.}$$

From these equations we have

$$p^d - 1 \equiv e_k^* \pmod{p^2} \quad \text{when } k \text{ is odd,}$$

$$p(p^d - 1) \equiv e_k^* \pmod{p^2} \quad \text{when } k \text{ is even.}$$

These imply the congruences

$$e_k \equiv (p^d - 1)/q \quad \text{when } k \text{ is odd,}$$

$$e_k \equiv p(p^d - 1)/q \quad \text{when } k \text{ is even.}$$

Both sides of these congruences are positive and less than p^2 by (9) and Lemma H. Hence these congruences turn out to be equations. Thus our induction argument completes the proof of (i) and (ii).

Finally from (i) and (ii) we have $1 + \sum_{k=1}^{s} e_k^* p^{2f_k} = p^{sd}$. And on the other hand the left-hand side of this equation equals p^{rd}, the order of $\mathfrak{M}$. Hence we have $r = s$.

10. LEMMA J. $q = (p^d - 1)/2$.

Proof. It is a classical result that the number of real irreducible characters of a group equals the number of real classes of the group. $\mathbf{E}$, $\mathbf{B}$, and $\mathbf{A}_i$ $(i = 1, \cdots, \frac{1}{2}(q-1))$ are real characters of $\mathfrak{G}$ (by (1) and (2)). $\{1\}$, the class of involutions and $\frac{1}{2}(q-1)$ classes of conjugate elements of Γ_2 are real. On the other hand $\mathbf{C}_{ij}$ $(i = 1, \cdots, s; j = 1, \cdots, e_i)$ are nonreal characters of $\mathfrak{G}$. There are the same number of nonreal classes of conjugate elements of Γ_1. Hence if there is no real character of $\mathfrak{G}$ distinct from $\mathbf{E}$, $\mathbf{B}$, and $\mathbf{A}_i$ $(i = 1, \cdots, \frac{1}{2}(q-1))$, then by Lemma B, Γ_0 contains only one, namely, the class of involutions. In particular this implies the equation $m + 1 = 2^h$. Since by the theorem of Feit $m = p^e$, we have $m = p$, contradicting our assumption (2.1). Therefore there exists a real irreducible character $\mathbf{R}$ of $\mathfrak{G}$ distinct from $\mathbf{E}$, $\mathbf{B}$, and $\mathbf{A}_i$ $(i = 1, \cdots, \frac{1}{2}(q-1))$.

Now in (7) let $\Delta_i = b_i \mathbf{R} + \cdots$ $(i = 1, \cdots, s)$. Then by the reciprocity theorem of Frobenius we have the equation valid for any element of $\mathfrak{G}_1$

$$\mathbf{R} = \sum_{i=1}^{s} (b_i \sum_{j=1}^{e_i} \phi_{ij}).$$

In particular this implies

$$\mathbf{R}(1) = \sum_{i=1}^{s} b_i e_i p^{2f_i} q.$$

Since $e_i \equiv 0 \pmod{(p^d - 1)/q}$ $(i = 1, \cdots, s)$ by Lemma I, we obtain $\mathbf{R}(1) \equiv 0 \pmod{p^d - 1}$. As the degree of an irreducible character of $\mathfrak{G}$, $\mathbf{R}(1)$ divides the order $(m+1)mq$ of $\mathfrak{G}$. Therefore we have $m + 1 \equiv 0 \pmod{(p^d - 1)/q}$. On the other hand, since $p^d - 1$ is a divisor of $m - 1 = p^{rd} - 1$, we have $(p^d - 1)/q = 2$.

On account of Lemma J the second part of Lemma I can be rewritten as follows:

LEMMA I (ii′).
$$e_{2l+1} = 2 \qquad (l = 0, 1, \cdots),$$
$$e_{2l} = 2p \qquad (l = 1, 2, \cdots).$$

11. LEMMA K. *Let* $\mathbf{X}$ *be any irreducible character of* $\mathfrak{G}$ *distinct from* $\mathbf{E}$, $\mathbf{B}$, *and* $\mathbf{A}_i$ $(i = 1, \cdots, \frac{1}{2}(q-1))$. *Let p divide* $\mathbf{X}(1)$ *with the exact exponent*[5] $\nu(X(1))$. *Then we have*

$$sd - \nu(X(1)) \geqq d + 1.$$

Proof. (I) Let $\mathbf{X} = \mathbf{R}$ be real, and put $\mathbf{R}(1) = rq$ (by Lemma A). As in the proof of Lemma J let us assume $\Delta_i = b_i \mathbf{R} + \cdots$ $(i = 1, \cdots, s)$. Then using Lemma I (ii′) we have the following equation:

$$r = 2(b_1 + pb_2 p^{(d-1)/2} + b_3 p^d + \cdots).$$

Let us assume $b_1 = \cdots = b_{k-1} = 0$ and $b_k \neq 0$ $(k = 1, 2, \cdots)$. Then from

[5] Let n be an integer. Then $\nu(n)$ denotes the exact exponent with which n is divisible by p.

this equation we have

$$(10) \qquad r = \begin{cases} 2(b_k p^{(k-1)d/2} + pb_{k+1} p^{(kd-1)/2} + \cdots) & \text{if } k \text{ is odd,} \\ 2(pb_k p^{((k-1)d-1)/2} + b_{k+1} p^{kd/2} + \cdots) & \text{if } k \text{ is even.} \end{cases}$$

Now by (10) it is enough to show that

$$b_k < p^{(d+1)/2} \quad \text{if } k \text{ is odd,}$$

$$b_k < p^{(d-1)/2} \quad \text{if } k \text{ is even.}$$

In fact if this can be shown, we see that

$$sd - \nu(r) \geqq \tfrac{1}{2}(2sd - kd - 1) \geqq \tfrac{1}{2}(sd - 1) \geqq d + 1.$$

If $k = 1$, then since the norm of $\phi_{11}^* = \cdots + b_1 \mathbf{R} + \cdots$ by (8.1) equals $q + 1 = \frac{1}{2}(p^d + 1) < p^{d+1}$, we have $b_1 < p^{(d+1)/2}$.

If $k > 1$ and odd, then since the norm of

$$\begin{aligned} p^{(d+1)/2}\phi_{k-1,1} - \phi_{k1}^* = \cdots &+ (p^{(d+1)/2}a_{k-1,k-1} + p^{(d+1)/2}\varepsilon_{k-1} - a_{k,k-1})\mathbf{C}_{k-1,1} \\ &+ \textstyle\sum_{j=2}^{2p} (p^{(d+1)/2}a_{k-1,k-1} - a_{k,k-1})\mathbf{C}_{k-1,j} + \cdots \\ &- b_k \mathbf{R} + \cdots \end{aligned}$$

by (8.2) equals $p^{d+1} + 1$, we have $b_k < p^{(d+1)/2}$.

If k is even, then since the norm of $p^{(d-1)/2}\phi_{k-1,1}^* - \phi_{k1}^*$ by (8.2) equals $p^{d-1} + 1$, we have as above $b_k < p^{(d-1)/2}$.

(II) Let us assume $\mathbf{X} = \mathbf{C}_{kj}$ and put $\mathbf{C}_{kj}(1) = cq$ (by Lemma A). Using the reciprocity theorem of Frobenius we obtain the following equations (by (7) and Lemma I (ii′))

$$c = \begin{cases} 2(a_{1k} + pa_{2k} p^{(d-1)/2} + \cdots) + \varepsilon_k p^{(k-1)d/2} & \text{if } k \text{ is odd,} \\ 2(a_{1k} + pa_{2k} p^{(d-1)/2} + \cdots) + \varepsilon_k p^{((k-1)d-1)/2} & \text{if } k \text{ is even.} \end{cases}$$

Unless $a_{1k} = \cdots = a_{k-1,k} = 0$, the situation is exactly the same as case (I). Hence we can assume that $a_{1k} = \cdots = a_{k-1,k} = 0$. Then the above equations can be rewritten as follows:

$$(11) \qquad c = \begin{cases} 2(a_{kk} p^{(k-1)d/2} + pa_{k+1,k} p^{(kd-1)/2} + \cdots) + \varepsilon_k p^{(k-1)d/2} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } k \text{ is odd,} \\ 2(pa_{kk} p^{((k-1)d-1)/2} + a_{k+1,k} p^{kd/2} + \cdots) + \varepsilon_k p^{((k-1)d-1)/2} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } k \text{ is even.} \end{cases}$$

By (11) the case where k is even is trivial, because $2pa_{kk} + \varepsilon_k$ is prime to p. Hence we can assume that k is odd. Again by (11) it is enough to show that $2a_{kk} + \varepsilon_k < p^{(d+1)/2}$, and hence it is enough to show that

$$2a_{kk}^2 + 2\varepsilon_k a_{kk} < \tfrac{1}{2}(p^{d+1} - 1).$$

If $k = 1$, then since the norm of

$$\phi_{11}^* = (a_{11} + \varepsilon_1)\mathbf{C}_{11} + a_{11}\mathbf{C}_{12} + \cdots$$

by (8.1) equals $q + 1 = \frac{1}{2}(p^d + 1)$, we have

$$(a_{11} + \varepsilon_1)^2 + a_{11}^2 \leqq \tfrac{1}{2}(p^d + 1),$$

which implies that

$$2a_{11}^2 + 2\varepsilon_1 a_{11} \leqq \tfrac{1}{2}(p^d - 1) < \tfrac{1}{2}(p^{d+1} - 1).$$

If $k > 1$, then the norm of

$$\begin{aligned} p^{(d+1)/2}\phi_{k-1,1}^* - \phi_{k1}^* = \cdots &+ (p^{(d+1)/2}a_{k-1,k-1} + p^{(d+1)/2}\varepsilon_{k-1} - a_{k,k-1})\mathbf{C}_{k-1,1} \\ &+ \textstyle\sum_{j=2}^{2p} (p^{(d+1)/2}a_{k-1,k-1} - a_{k,k-1})\mathbf{C}_{k-1,j} \\ &- (\varepsilon_k + a_{kk})\mathbf{C}_{k1} - a_{kk}\mathbf{C}_{k2} + \cdots \end{aligned}$$

by (8.2) equals $p^{d+1} + 1$. Therefore it is enough to show that

$$\begin{aligned} &(p^{(d+1)/2}a_{k-1,k-1} + p^{(d+1)/2}\varepsilon_{k-1} - a_{k,k-1})^2 \\ &\qquad + (2p - 1)(p^{(d+1)/2}a_{k-1,k-1} - a_{k,k-1})^2 \geqq \tfrac{1}{2}(p^{d+1} + 1). \end{aligned}$$

Put $x = p^{(d+1)/2}a_{k-1,k-1} - a_{k,k-1}$. Then it is easy to see that the minimal value of the quadratic form in x

$$(x + p^{(d+1)/2}\varepsilon_{k-1})^2 + (2p - 1)x^2$$

is not less than $\frac{1}{2}(p^{d+1} + 1)$.

12. LEMMA L. *The number c_i in (5) satisfies the congruences*

$$c_i + q \equiv 0 \pmod{p^{d+1}},$$

which implies in particular that $c_i \geqq q + 3$ (for every i).

Proof. On account of (5) we have

$$c_i = \frac{mq}{m+1}\left(1 - \frac{1}{m} + \sum_{\mathbf{Z}} \frac{\mathbf{Z}(J)^2\mathbf{Z}(G_i)}{\mathbf{Z}(1)}\right),$$

where $\mathbf{Z}$ ranges over all the irreducible characters of $\mathfrak{G}$ distinct from $\mathbf{E}$, $\mathbf{B}$, and $\mathbf{A}_i$ ($i = 1, \cdots, \frac{1}{2}(q - 1)$). Then by Lemma K we obtain

$$c_i \equiv c_i(m + 1) \equiv -q \pmod{p^{d+1}}.$$

Hence by Lemma J we obtain $c_i + \frac{1}{2}(p^d - 1) = ap^{d+1}$, where a is a natural number. Therefore we have

$$c_i \geqq p^{d+1} - \tfrac{1}{2}(p^d - 1) \geqq \tfrac{1}{2}(p^d + 5).$$

Now we can derive a required contradiction as follows. From (4) we have the following equation

$$\tfrac{1}{2}(m - 1)(q + 1) = c_1 l_1 + \cdots + c_n l_n, \tag{12}$$

where $l_i\, mq$ is the number of elements in the class $\mathfrak{K}_i$ $(i = 1, \cdots, n)$. On the other hand, we have from the decomposition $\mathfrak{G} = \Gamma_0 + \Gamma_1 + \Gamma_2 + \{1\}$ the following equation

$$(13) \qquad \tfrac{1}{2}(m + 1) - (m - 1)/2q = l_1 + \cdots + l_n .$$

Since $c_i \geqq q + 3$ for every i by Lemma L, we obtain from (12) and (13) the following inequality

$$\tfrac{1}{2}(m - 1)(q + 1) \geqq (q + 3)(\tfrac{1}{2}(m + 1) - (m - 1)/2q).$$

This implies that

$$0 \geqq (q - 3)m + 2q^2 + 5q + 3.$$

This is a contradiction.

Bibliography

1. R. Brauer and W. Feit, *On the number of irreducible characters of finite groups in a given block*, Proc. Nat. Acad. Sci. U.S.A., vol. 45 (1959), pp. 361–365.
2. R. Brauer and K. Fowler, *On groups of even order*, Ann. of Math. (2), vol. 62 (1955), pp. 565–583.
3. R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. (2), vol. 42 (1941), pp. 556–590.
4. W. Feit, *On a class of doubly transitive permutation groups*, Illinois J. Math., vol. 4 (1960), pp. 170–186.
5. W. Feit, M. Hall, Jr., and J. G. Thompson, *Finite groups in which the centralizer of any non-identity element is nilpotent*, Math. Zeitschrift, vol. 74 (1960), pp. 1–17.
6. M. Suzuki, *On finite groups with cyclic Sylow subgroups for all odd primes*, Amer. J. Math., vol. 77 (1955), pp. 657–691.

University of Chicago
Chicago, Illinois
Nagoya University
Nagoya-Chikusa, Japan