A CHARACTERIZATION OF THE ONE-DIMENSIONAL UNIMODULAR PROJECTIVE GROUPS OVER FINITE FIELDS[1]

In commemoration of G. A. Miller

BY

R. BRAUER, M. SUZUKI, AND G. E. WALL[2]

Let q be a power of a prime number, and denote by $LF(2, q)$ the group of all one-dimensional unimodular projectivities over the field Γ_q with q elements, i.e., of all linear fractional transformations

$$z' = \frac{az + b}{cz + d}$$

of determinant 1 with coefficients a, b, c, d in Γ_q. As is well known, $LF(2, q)$ is simple for $q \geqq 4$. The order of $LF(2, q)$ is $q(q + 1)(q - 1)/2$ for odd q and $q(q + 1)(q - 1)$ for even q.

It is our aim to give a group-theoretical characterization of these groups $LF(2, q)$. We shall prove

THEOREM. *Let $\mathfrak{G}$ be a group of finite order g which satisfies the following conditions*:

(I) *g is even*;

(II) *if $\mathfrak{A}$ and $\mathfrak{B}$ are two cyclic subgroups of $\mathfrak{G}$ of even orders, and if $\mathfrak{A} \cap \mathfrak{B} \neq \{1\}$, then there exists a cyclic subgroup $\mathfrak{Z}$ of $\mathfrak{G}$ which includes both $\mathfrak{A}$ and $\mathfrak{B}$*;

(III) *$\mathfrak{G}$ coincides with its commutator subgroup.*

Then $\mathfrak{G} \cong LF(2, q)$ where $q \geqq 4$ is a prime power.

We begin in I with an elementary discussion of groups which satisfy these conditions. Two cases, A and B, have to be considered. In Case A, the 2-Sylow group $\mathfrak{T}$ of $\mathfrak{G}$ is dihedral, and in Case B, $\mathfrak{T}$ is abelian of type $(2, 2, \cdots, 2)$. These two cases are treated in II and III respectively. The final result is obtained by applying a theorem of Zassenhaus [2] concerning doubly transitive permutation groups. We shall give some extensions of our theorem in a subsequent paper.

Received January 12, 1959.

[1] The results of this paper were obtained more or less independently by the three authors. Rather than publish three different papers, we preferred to combine our investigations.

The result for Case B has also been obtained by K. A. Fowler in his thesis, University of Michigan, 1952.

[2] Part of the work of the first two authors was done under an NSF contract.

I. Groups of type (S)

We shall say that a finite group $\mathfrak{G}$ is of type (S), if the following two conditions are satisfied:

(I) The group $\mathfrak{G}$ is of even order g.

(II) If $\mathfrak{A}$ and $\mathfrak{B}$ are two maximal cyclic subgroups of even orders, then either $\mathfrak{A} = \mathfrak{B}$ or $\mathfrak{A} \cap \mathfrak{B} = \{1\}$.

It follows from (II) that if two cyclic subgroups of even order of $\mathfrak{G}$ have an intersection different from $\{1\}$, then both are included in the same maximal cyclic subgroup of $\mathfrak{G}$. In particular, the elements of the two subgroups commute with each other. Moreover, if the two subgroups have the same order, they must be equal.

The following remarks are fairly obvious.

(I.A) *If $\mathfrak{G}$ has type (S), every subgroup $\mathfrak{H}$ of even order has type (S).*

Indeed, if $\mathfrak{A}_0$ and $\mathfrak{B}_0$ are two maximal subgroups of even order of $\mathfrak{H}$, and if $\mathfrak{A}_0 \cap \mathfrak{B}_0 \neq \{1\}$, then $\mathfrak{A}_0$ and $\mathfrak{B}_0$ are both subgroups of a cyclic subgroup $\mathfrak{Z}$ of $\mathfrak{G}$, and, because of the maximality of $\mathfrak{A}_0$ and $\mathfrak{B}_0$ in $\mathfrak{H}$, we have $\mathfrak{A}_0 = \mathfrak{H} \cap \mathfrak{Z}$, $\mathfrak{B}_0 = \mathfrak{H} \cap \mathfrak{Z}$.

(I.B) *Let $\mathfrak{G}$ be a group of type (S), and let G be an element of even order. If $G^r \neq 1$ for some exponent r, then the cyclic groups $\{G\}$ and $\{G^r\}$ have the same normalizer,*

$$\mathfrak{N}(\{G\}) = \mathfrak{N}(\{G^r\}). \tag{I1}$$

Proof. It is clear that $\mathfrak{N}(\{G\}) \subseteqq \mathfrak{N}(\{G^r\})$. Conversely, if $X \in \mathfrak{N}(\{G^r\})$, then $G^r \in \{G\} \cap X^{-1}\{G\}X$. Since the cyclic groups $\{G\}$ and $X^{-1}\{G\}X$ have a nontrivial intersection, and since they have the same order, they are equal. This means that $X \in \mathfrak{N}(\{G\})$, and hence we have (I1).

As a corollary, we have

(I.C) *Let $\mathfrak{G}$ be a group of type (S). Let G be an element of even order, and let I be the element of order 2 which is a power of G. Then*

$$\mathfrak{N}(\{G^r\}) = \mathfrak{C}(I) \tag{I2}$$

for all r for which $G^r \neq 1$.

(I.D) *Let $\mathfrak{G}$ be of type (S). Let I be an involution (i.e., an element of order 2) of $\mathfrak{G}$. If p is an odd prime dividing the order $c(I)$ of the centralizer $\mathfrak{C}(I)$ of I, then $\mathfrak{C}(I)$ includes a p-Sylow group $\mathfrak{P}$ of $\mathfrak{G}$.*

Proof. Let P be an element of order p of $\mathfrak{C}(I)$. If $X \in \mathfrak{C}(P)$, then $X \in \mathfrak{N}(\{IP\})$ and, by (I2), $X \in \mathfrak{C}(I)$. In particular, if P belongs to the p-Sylow group $\mathfrak{P}$ of $\mathfrak{G}$, the center of $\mathfrak{P}$ is included in $\mathfrak{C}(I)$. If we now replace P by an element of order p of the center of $\mathfrak{P}$, our argument shows that $\mathfrak{P} \subseteqq \mathfrak{C}(I)$.

(I.E) *Let $\mathfrak{G}$ be of type (S). Let I be an involution, and let p be an odd prime dividing $c(I)$. Then the p-Sylow groups of $\mathfrak{G}$ are cyclic.*

Indeed, by (I.D), a p-Sylow group $\mathfrak{P}$ of $\mathfrak{G}$ lies in $\mathfrak{C}(I)$. If $\mathfrak{P}$ were not cyclic, we could find two distinct subgroups $\{P_1\}$ and $\{P_2\}$ of $\mathfrak{P}$ of order p, and then

$$I \in \{IP_1\} \cap \{IP_2\}.$$

Since $\{IP_1\}$ and $\{IP_2\}$ both have the same order $2p$, this implies $\{IP_1\} = \{IP_2\}$, and hence $\{P_1\} = \{P_2\}$. This is a contradiction.

We next study the 2-Sylow groups of $\mathfrak{G}$.

(I.F) *If $\mathfrak{G}$ is of type (S), the 2-Sylow group $\mathfrak{T}$ of $\mathfrak{G}$ is of one of the following types:*

(a) *$\mathfrak{T}$ is cyclic.*

(b) *$\mathfrak{T}$ is abelian of type $(2, 2, \cdots, 2)$.*

(c) *$\mathfrak{T}$ is dihedral: $\mathfrak{T} = \{A, B\}$ with $A^{2^m} = 1$, $B^2 = 1$, $B^{-1}AB = A^{-1}$.*

Proof. By (I.A), $\mathfrak{T}$ itself is of type (S). If all elements $T \neq 1$ of $\mathfrak{T}$ have order 2, we have case (b). Suppose that $\mathfrak{T}$ contains elements R of order $r \geqq 4$. If I is an involution in the center of $\mathfrak{T}$, then

$$R^2 \in \{R\} \cap \{IR\},$$

and since R and IR have the same order r, and since $R^2 \neq 1$, it follows that $\{R\} = \{IR\}$, whence $I \in \{R\}$. Thus, $I = R^{r/2}$.

Let A be an element of maximal order r of $\mathfrak{T}$; $r \geqq 4$. If B is an element of order $\geqq 4$ of $\mathfrak{T}$, then as just shown, $I \in \{A\}$ and $I \in \{B\}$. Since $\{A\}$ is a maximal cyclic subgroup of $\mathfrak{T}$, it follows that $B \in \{A\}$. In particular, $\{A\}$ is the only maximal cyclic subgroup of $\mathfrak{T}$ of order $\geqq 4$. It follows that $\{A\}$ is normal in $\mathfrak{T}$. If $\mathfrak{T} = \{A\}$, we have case (a).

Suppose then that $\{A\} \neq \mathfrak{T}$. If $B \notin \{A\}$, B has order 2, and, as $AB \notin \{A\}$, AB also has order 2. Thus, $B^2 = 1$, $ABAB = 1$, whence $B^{-1}AB = A^{-1}$. Hence, if A has order 2^m, we have

$$A^{2^m} = 1, \qquad B^2 = 1, \qquad B^{-1}AB = A^{-1}.$$

If B_1 is any element of $\mathfrak{T}$ with $B_1 \notin \{A\}$, then we also have $B_1^{-1}AB_1 = A^{-1}$. Then $B_1 B^{-1} \in \mathfrak{C}(A)$. If we had $B_1 B^{-1} \notin \{A\}$, we would have $(B_1 B^{-1})^{-1} A (B_1 B^{-1}) = A^{-1} \neq A$; $B_1 B^{-1} \notin \mathfrak{C}(A)$. Thus, $B_1 B^{-1} \in \{A\}$, $B_1 \in \{A\}B$. It follows that $\mathfrak{T} = \{A, B\}$. Hence $\mathfrak{T}$ is dihedral.

We now study the centralizers in $\mathfrak{G}$ of the involutions in the center of a 2-Sylow group $\mathfrak{T}$ of $\mathfrak{G}$. It will not be necessary to consider the case that $\mathfrak{T}$ is cyclic.

(I.G) *Let $\mathfrak{G}$ be of type (S). Let $\mathfrak{T}$ be a 2-Sylow group of $\mathfrak{G}$, and let T be an involution in the center of $\mathfrak{T}$.*

(1) *If $\mathfrak{T}$ is abelian of type $(2, 2, \cdots, 2)$ and of order $2^r > 4$, then $\mathfrak{C}(T) = \mathfrak{T}$.*

(2) *If* $\mathfrak{T}$ *is abelian of type* (2, 2), *then* $\mathfrak{C}(T) = \mathfrak{T}\mathfrak{V}$ *where* $\mathfrak{V}$ *is cyclic of odd order* v. *Moreover,* $B^{-1}VB = V^{-1}$ *for* $B \in \mathfrak{T}$, $B \neq 1, T$; $V \in \mathfrak{V}$.

(3) *If* $\mathfrak{T} = \{A, B\}$ *is dihedral of order* $2^{m+1} \geqq 8$, $A^{2^m} = 1$, $B^2 = 1$, $B^{-1}AB = A^{-1}$, *then* $\mathfrak{C}(T) = \{A, B, \mathfrak{V}\}$ *where* $\mathfrak{V}$ *is cyclic of odd order* v, $\mathfrak{V} \subseteqq \mathfrak{C}(A)$, *and* $B^{-1}VB = V^{-1}$ *for* $V \in \mathfrak{V}$.

Proof. (α) Suppose that V is an element of odd order of $\mathfrak{C}(T)$; $V \neq 1$. By (I.B), $\mathfrak{N}(\{V\}) = \mathfrak{N}(\{TV\}) = \mathfrak{C}(T)$. If J is an involution of $\mathfrak{C}(T)$, we must have $J^{-1}VJ \in \{V\}$, say $J^{-1}VJ = V^j$. Since J has order 2, then $V^{j^2} = V$. Assume that the order of V is a prime power p^s. Since $j^2 \equiv 1 \pmod{p^s}$ and p is odd, $j \equiv \pm 1 \pmod{p^s}$. If $j \equiv 1 \pmod{p^s}$, $J^{-1}VJ = V$, and then $V \in \{JV\} \cap \{TV\}$, which implies $J = T$. Thus, for $J \neq T$, we have $J^{-1}VJ = V^{-1}$. Since this holds for all elements V of odd prime power of $\mathfrak{C}(T)$, it holds for all elements V of $\mathfrak{C}(T)$ of odd order.

$$\text{(I3)} \qquad J^{-1}VJ = V^{-1} \quad \text{if} \begin{cases} V \in \mathfrak{C}(T), & V \text{ of odd order,} \\ J \in \mathfrak{C}(T), & J \text{ an involution, } J \neq T. \end{cases}$$

(β) If $\mathfrak{T}$ is abelian of type $(2, 2, \cdots, 2)$ and order $2^r > 4$, then (I3) would hold for all $2^r - 2$ elements $J \neq 1, T$ of $\mathfrak{T}$. If we choose two such elements J and J_1 such that $J_1 \neq J, JT$, we have a contradiction.

(γ) Suppose that $\mathfrak{T}$ is abelian of type (2, 2). Then $\mathfrak{T}$ is a 2-Sylow subgroup of $\mathfrak{C}(T)$. If $J \in \mathfrak{T}$, $J \neq 1, T$, then J and JT are not conjugate in $\mathfrak{C}(T)$. Indeed, if we had $X^{-1}JX = JT$ with $X \in \mathfrak{C}(T)$, then $X^{-1}JTX = J$. Thus, $X^2 \in \mathfrak{C}(J)$, and then $X^2 \in \mathfrak{C}(\{T, J\}) = \mathfrak{C}(\mathfrak{T})$. Since the order of $\{X, \mathfrak{C}(\mathfrak{T})\}$ cannot be divisible by 8, and since $X \in \mathfrak{N}(\mathfrak{T})$, we find $X \in \mathfrak{C}(\mathfrak{T})$, a contradiction. Thus, no two distinct elements of $\mathfrak{T}$ are conjugate in $\mathfrak{C}(T)$. It follows from Burnside's Theorem that $\mathfrak{C}(T)$ has a normal subgroup $\mathfrak{V}$ of index 4. Then $\mathfrak{C}(T) = \mathfrak{T}\mathfrak{V}$. Since J maps every element V of $\mathfrak{V}$ on its inverse, $\mathfrak{V}$ is abelian. But the Sylow groups of $\mathfrak{V}$ are cyclic by (I.E), and $\mathfrak{V}$ itself is cyclic.

(δ) Suppose now that $\mathfrak{T}$ is dihedral and of order $\geqq 8$. Clearly, $\{A\}$ is a 2-Sylow subgroup of $\mathfrak{C}(A)$. Since no two distinct elements of $\{A\}$ are conjugate in $\mathfrak{C}(A)$, Burnside's Theorem shows that we may set $\mathfrak{C}(A) = \{A\}\mathfrak{V}$ where $\mathfrak{V}$ is a normal subgroup of $\mathfrak{C}(A)$ of odd order v. Then

$$\mathfrak{C}(A) = \{A\} \times \mathfrak{V}.$$

If W is an element of odd order of $\mathfrak{C}(T)$, then $T \in \{A\} \cap \{TW\}$. It follows that A commutes with TW and hence with W. Thus, $W \in \mathfrak{C}(A)$. Thus, every p-Sylow group of $\mathfrak{C}(T)$ lies in $\mathfrak{C}(A)$ for odd p. Since $\mathfrak{C}(A) \subseteqq \mathfrak{C}(T)$, it follows that $(\mathfrak{C}(T) : \mathfrak{C}(A))$ is a power of 2. But $\mathfrak{T} = \{A, B\} \in \mathfrak{C}(T)$, $A \in \mathfrak{C}(A)$, $B \notin \mathfrak{C}(A)$, and we see that

$$\mathfrak{C}(T) = \{\mathfrak{T}, \mathfrak{V}\} = \{B, \mathfrak{C}(A)\}.$$

Again, (I3) implies that $\mathfrak{V}$ is abelian, and then (I.E) shows that $\mathfrak{V}$ is cyclic. This completes the proof of (I.G).

We shall consider the case (2), $r = 2$ as a special case of (3) taking $m = 1$, $A = T$. In this sense, the dihedral group of order 4 is the abelian group of type (2, 2).

If we assume that $\mathfrak{G}$ is a group of type (S) such that $\mathfrak{G}$ does not have a normal subgroup of index 2, the case (a) of (I.F) is excluded (by Burnside's Theorem). We then have to consider the following cases:

Case A. $\mathfrak{T}$ is dihedral of order $2^{m+1}, m \geqq 1$. We set $\mathfrak{V} = \{V\}$ and $H = AV$. Then $\mathfrak{C}(T) = \{H, B\}$ with

$$H^h = 1, \qquad B^2 = 1, \qquad B^{-1}HB = H^{-1},$$

where $h = 2^m v$.

Case B. $\mathfrak{T}$ is abelian of type $(2, 2, \cdots, 2)$, $(\mathfrak{T}:1) \geqq 4$. Here $\mathfrak{C}(T) = \mathfrak{T}$ for $T \in \mathfrak{T}$, $T \neq 1$.

If $m = 1, v = 1$ in Case A, we may consider this as Case B with $(\mathfrak{T}:1) = 4$. Consequently, in dealing with Case A, we may assume that $h \geqq 4$.

II. The Case A

1. Assumptions

We assume that $\mathfrak{G}$ is a group of type (S) which does not have a normal subgroup of index 2 and that we have Case A in the notation of I. Fully stated our assumptions are

(I) $\mathfrak{G}$ is a finite group of even order g.

(II) If $\mathfrak{A}$ and $\mathfrak{B}$ are two maximal cyclic subgroups of $\mathfrak{G}$ of even order, then either $\mathfrak{A} = \mathfrak{B}$ or $\mathfrak{A} \cap \mathfrak{B} = \{1\}$.

(III) There does not exist a normal subgroup of index 2 in $\mathfrak{G}$.

(IV) The 2-Sylow subgroups of $\mathfrak{G}$ are dihedral.

Let $\mathfrak{T}$ be a 2-Sylow subgroup of $\mathfrak{G}$. If its order is 2^{m+1} with $m \geqq 1$, we can set $\mathfrak{T} = \{A, B\}$ where

$$A^{2^m} = 1, \qquad B^2 = 1, \qquad B^{-1}AB = A^{-1}. \tag{1}$$

We set

$$T = A^{2^{m-1}}. \tag{2}$$

Then T has order 2.

2. The centralizer $\mathfrak{C}(T)$ of T

As shown by (I.G), the centralizer $\mathfrak{C}(T)$ is dihedral too. We shall denote its order by $2h$. Then

$$(\mathfrak{C}(T):\{1\}) = 2h = 2^{m+1}v; \qquad (v, 2) = 1. \tag{3}$$

If V is an element of order v in $\mathfrak{C}(T)$, and if we set

$$H = AV, \tag{4}$$

then $AV = VA$, and $\mathfrak{C}(T) = \{H, B\}$;

$$H^h = 1, \qquad B^{-1}HB = H^{-1}. \tag{5}$$

Since $\mathfrak{T}$ is a 2-Sylow subgroup of $\mathfrak{G}$, 2^{m+1} is the exact power of 2 in g. By (I.D), we can set

$$g = 2^{m+1}vg_0, \qquad (g_0, 2^{m+1}v) = 1. \tag{6}$$

The number h is even, and we shall set

$$s = h/2 - 1. \tag{7}$$

The case $h = 2$ may be considered as part of Case B so that we may assume

$$s \geqq 1. \tag{8}$$

(II.A) *In $\mathfrak{G}$, every element of $\mathfrak{C}(T)$ is conjugate to a power H^α of H. Two powers H^α and H^β are conjugate in $\mathfrak{G}$ if and only if $H^\beta = H^{\pm\alpha}$. Thus, the elements*

$$1, \quad H^{s+1} = T; \qquad H, \quad H^2, \quad \cdots, \quad H^s \tag{9}$$

form a full system of representatives for those classes of conjugate elements of $\mathfrak{G}$ in which the order is not relatively prime to $2h = 2^{m+1}v$. We have

$$c(1) = g, \qquad c(T) = 2h; \qquad c(H^\alpha) = h \quad \text{for} \quad H^\alpha \neq 1, T. \tag{10}$$

Proof. In the dihedral group $\mathfrak{C}(T) = \{H, B\}$, the elements (9) together with the elements B and BH form a full system of representatives for the classes of conjugate elements. The elements 1 and T form classes by themselves, while the class of H^α for $H^\alpha \neq 1, T$ consists of H^α and $H^{-\alpha}$. The class of B consists of all elements BH^ρ with even ρ and the class of BH of all elements BH^σ with odd σ.

Since $T = H^{h/2} = H^{s+1}$ is a power of H, it follows from (I.C) that $\mathfrak{N}(\{H^r\}) = \mathfrak{N}(\{T\}) = \mathfrak{C}(T)$ for $H^r \neq 1$. Consequently, two powers H^α and H^β can be conjugate in $\mathfrak{G}$ only if they are conjugate in $\mathfrak{C}(T)$, and this is the case if and only if $H^\beta = H^{\pm\alpha}$. Moreover, for $H^r \neq 1$, we have $\mathfrak{C}(H^r) \subseteqq \mathfrak{N}(\{H^r\}) \subseteqq \mathfrak{C}(T)$. This implies that the order of the centralizer of $H^r \neq 1$ in $\mathfrak{G}$ is the order of the centralizer of H^r in $\mathfrak{C}(T)$. This order is $2h$ for $H^r = T$ and h for $H^r \neq 1, T$. Since $c(1) = g$, the equations (10) are true.

We show next that the elements T, B, $BH^v = BA^v$ are conjugate in $\mathfrak{G}$. Let $\mathfrak{T}^*$ denote the subgroup of $\mathfrak{T}$ generated by all quotients XY^{-1} of elements X, Y of $\mathfrak{T}$ which are conjugate in $\mathfrak{G}$. If X is a power $H^r \neq 1, T$, then $Y = H^{\pm r}$, since the order of H^r is different from 2 and H^r is not conjugate to the involutions B, BH^v. Thus, $XY^{-1} = 1$, or $XY^{-1} = H^{2r}$. For $X = 1$, we have $Y = 1$, $XY^{-1} = 1$. If no two different ones of the elements T, B, BH^v are conjugate in $\mathfrak{G}$, then $\mathfrak{T}^* = \{A^2\}$. If two, but not all three, elements T, B, BH^v are conjugate in $\mathfrak{G}$, then $\mathfrak{T}^*$ is one of the groups $\{A^2, BT^{-1}\}$, $\{A^2, BH^vT^{-1}\}$, $\{A^2, BH^vB^{-1}\}$. Since $\mathfrak{T}/\{A^2\}$ is abelian of type (2, 2), the

group $\mathfrak{T}$ cannot be generated by A^2 and one further element. Hence $\mathfrak{T}^* \neq \mathfrak{T}$. Now, the generalization of Burnside's Theorem shows that the 2-Sylow group of $\mathfrak{G}/\mathfrak{G}'$ is isomorphic with $\mathfrak{T}/\mathfrak{T}^*$. Hence $\mathfrak{G}/\mathfrak{G}'$ has an order divisible by 2. Then $\mathfrak{G}$ has a normal subgroup of index 2. But this is a contradiction to condition (III). Hence T, B, and BH^v are conjugate in $\mathfrak{G}$. Since v is odd, then T, B, BH are conjugate in $\mathfrak{G}$.

If X has an order divisible by a prime factor p of $2^{m+1}v$, and if P is a power of X whose order is p, then $X \in \mathfrak{C}(P)$. If $p = 2$, the preceding argument shows that P is conjugate to T in $\mathfrak{G}$. If $p \neq 2$, it follows from (I.D) and (I.E) that P is conjugate to an element of the form H^r. Then X is conjugate to an element of $\mathfrak{C}(T)$ or even of $\mathfrak{C}(H^r) \subset \mathfrak{C}(T)$. This concludes the proof of (II.A).

3. The restrictions of the irreducible characters of $\mathfrak{G}$ to $\mathfrak{H} = \{H\}$

Set $\mathfrak{H} = \{H\}$. If ε is a fixed primitive h^{th} root of unity, let ε_j denote the irreducible character of $\mathfrak{H}$ defined by

$$\varepsilon_j(H^r) = \varepsilon^{jr} \qquad (r = 0, 1, \cdots, h-1). \tag{11}$$

Then $\varepsilon_i = \varepsilon_j$ if and only if $i \equiv j \pmod{h}$. Clearly,

$$\varepsilon_{-s}, \varepsilon_{-s+1}, \cdots, \varepsilon_{s-1}, \varepsilon_s, \varepsilon_{s+1} \tag{12}$$

are all the irreducible characters of $\mathfrak{H}$.

If $\chi^{(1)}, \chi^{(2)}, \cdots, \chi^{(k)}$ are the irreducible characters of $\mathfrak{G}$, we can set

$$\chi^{(\mu)} \mid \mathfrak{H} = \sum_{j=-s}^{s+1} a_{\mu j}\, \varepsilon_j \qquad (\mu = 1, 2, \cdots, k) \tag{13}$$

with nonnegative rational integers $a_{\mu j}$. Since $\chi^{(\mu)}(H^r) = \chi^{(\mu)}(H^{-r})$, we see that

$$a_{\mu j} = a_{\mu,-j}. \tag{14}$$

It follows from (13) that

$$a_{\mu j} = (1/h) \sum_{X \in \mathfrak{H}} \chi^{(\mu)}(X) \bar{\varepsilon}_j(X). \tag{15}$$

(II.B) *If* $u = (g - 2h)/h^2$, *then, for* $0 \leqq i, j \leqq s+1$, *we have*

$$\sum_{\mu=1}^{k} a_{\mu i}\, a_{\mu j} = \begin{cases} u & \text{for } i \neq j, \\ u+1 & \text{for } i = j;\ i \neq 0, s+1, \\ u+2 & \text{for } i = j;\ i = 0 \text{ or } i = s+1. \end{cases} \tag{16}$$

Proof. Since $a_{\mu j}$ is rational, we have, by (15)

$$\sum_{\mu=1}^{k} a_{\mu i}\, a_{\mu j} = \sum_{\mu=1}^{k} a_{\mu i}\, \bar{a}_{\mu j} = (1/h^2) \sum_{X,Y} \bar{\varepsilon}_i(X) \varepsilon_j(Y) \sum_{\mu=1}^{k} \chi^{(\mu)}(X) \bar{\chi}^{(\mu)}(Y).$$

Here, the inner sum on the right is 0, if X and Y are not conjugate in $\mathfrak{G}$, while in the other case, the value is $c(X)$. On account of (II.A), we find

$$\sum_{\mu=1}^{k} a_\mu a_{\mu j} = \frac{1}{h^2} g + \frac{1}{h^2} 2h\bar{\varepsilon}_i(T)\varepsilon_j(T) + \frac{h}{h^2} \sum_{X \in \mathfrak{H}, X \neq 1, T} \bar{\varepsilon}_i(X)(\varepsilon_j(X) + \varepsilon_j(X^{-1})).$$

By the orthogonality relation for the characters of $\mathfrak{H}$, we have

$$\frac{1}{h} \sum_{X \in \mathfrak{H}} \bar{\varepsilon}_i(X)(\varepsilon_j(X) + \bar{\varepsilon}_j(X)) = \begin{cases} 0 & \text{for } i \neq j, \\ 1 & \text{for } i = j;\ i \neq 0, s+1, \\ 2 & \text{for } i = j;\ i = 0 \text{ or } i = s+1, \end{cases}$$

where we assumed $0 \leqq i, j \leqq s+1$. If this is subtracted from the preceding equation, and if $2\bar{\varepsilon}_i(T)\varepsilon_j(T) = \bar{\varepsilon}_i(T)(\varepsilon_j(T) + \bar{\varepsilon}_j(T))$ is taken into account, we obtain

$$\sum_{\mu=1}^{k} a_{\mu i} a_{\mu j} - \begin{cases} 0 \\ 1 \\ 2 \end{cases} = \frac{1}{h^2} g - \frac{2}{h}.$$

This yields (16).

If with each of the characters $\chi^{(\mu)}$, there is associated a complex number z_μ, we arrange these k numbers z_μ in the form of a column. We define the inner product of two such columns in the usual manner. In particular, let $\mathfrak{a}_i$ denote the column consisting of the numbers $a_{\mu i}$ with fixed i. Because of (14), it will be sufficient to consider the columns

$$\mathfrak{a}_0, \quad \mathfrak{a}_{s+1}; \qquad \mathfrak{a}_1, \quad \mathfrak{a}_2, \quad \cdots, \quad \mathfrak{a}_s.$$

Now, (16) can be written in the form

$$\begin{aligned} \mathfrak{a}_i \mathfrak{a}_j &= u && \text{for } i \neq j;\ 0 \leqq i, j \leqq s+1, \\ \mathfrak{a}_i^2 &= u + 1 && \text{for } i = 1, 2, \cdots, s, \\ \mathfrak{a}_i^2 &= u + 2 && \text{for } i = 0, \text{ and for } i = s+1. \end{aligned} \tag{17}$$

It follows from (15) that

$$a_{\mu j} - a_{\mu 1} = \frac{1}{h} \sum_{X \in \mathfrak{H}, X \neq 1} \chi^{(\mu)}(X)(\bar{\varepsilon}_j(X) - \bar{\varepsilon}_1(X)).$$

If Y is either 1 or an element of $\mathfrak{G}$ which is not conjugate to a power H^r of H, and if we multiply here by $\bar{\chi}^{(\mu)}(Y)$ and add over $\mu = 1, 2, \cdots, k$, the orthogonality relations for the $\chi^{(\mu)}$ show that we obtain 0. Replacing Y by Y^{-1}, we have

(II.C) *Let Y be an element of $\mathfrak{G}$ which is not conjugate in $\mathfrak{G}$ to a power $H^r \neq 1$. If $\chi(Y)$ denotes the column consisting of the numbers $\chi^{(\mu)}(Y)$, we have*

$$(\mathfrak{a}_j - \mathfrak{a}_1) \cdot \chi(Y) = 0 \qquad (j = 0, 1, \cdots, s+1). \tag{18}$$

In particular,

$$(\mathfrak{a}_j - \mathfrak{a}_1) \cdot \chi(1) = 0 \qquad (j = 0, 1, \cdots, s+1). \tag{19}$$

4. The exceptional characters of $\mathfrak{G}$

Assume first that $s > 1$. We shall say that an irreducible character $\chi^{(\mu)}$ of $\mathfrak{G}$ is *exceptional*, if not all the coefficients in $\alpha_2 - \alpha_1$, $\alpha_3 - \alpha_1$, $\cdots$, $\alpha_s - \alpha_1$ belonging to $\chi^{(\mu)}$ are 0.

(II.D) *Suppose that $s \geqq 2$. There exist exactly s exceptional characters of $\mathfrak{G}$. These can be taken for $\chi^{(1)}$, $\chi^{(2)}$, $\cdots$, $\chi^{(s)}$ in such an order that*

$$a_{ij} = a + \tau\delta_{ij} \qquad (\text{for } i, j = 1, 2, \cdots, s) \tag{20}$$

where a is a fixed rational integer and where $\tau = \pm 1$.

Proof. Let j range over $2, 3, \cdots, s$. It follows from (17) that

$$(\alpha_j - \alpha_1)^2 = 2.$$

Since the coefficients of $\alpha_j - \alpha_1$ are rational integers, only two of these coefficients have values different from 0, and these values are ± 1. Now (19) shows that one of the values is $+1$ and the other is -1, since the coefficients of $\chi(1)$ are the degrees of the $\chi^{(\mu)}$ and hence positive.

Assume that $s \geqq 3$. If j' also is one of the values $2, 3, \cdots, s$, then (17) shows that

$$(\alpha_j - \alpha_1)(\alpha_{j'} - \alpha_1) = 1 \qquad \text{for } j \neq j'.$$

Hence α_j and $\alpha_{j'}$ must have an equal coefficient ± 1 in one and the same row, while in all other rows at least one of them has the coefficient 0.

Choose $\chi^{(1)}$ such that $\alpha_2 - \alpha_1$ and $\alpha_3 - \alpha_1$ have the same coefficient ± 1 in the first row, and denote the value of this coefficient by $-\tau$.

We claim that we can arrange the characters $\chi^{(1)}, \chi^{(2)}, \cdots, \chi^{(k)}$ in such an order that the matrix M of the columns $\alpha_2 - \alpha_1$, $\alpha_3 - \alpha_1$, $\cdots$, $\alpha_s - \alpha_1$ has the form

$$M = \begin{pmatrix} -\tau & -\tau & -\tau & \cdots & -\tau \\ \tau & 0 & 0 & \cdots & 0 \\ 0 & \tau & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \tau \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{21}$$

Since the coefficient τ must appear in $\alpha_2 - \alpha_1$ and in $\alpha_3 - \alpha_1$ in different rows, we can choose $\chi^{(2)}$, $\chi^{(3)}$ such that the first two columns $\alpha_2 - \alpha_1$ and $\alpha_3 - \alpha_1$ have the form given in (21). If $s = 3$, we are finished. If $s \geqq 4$, then $\alpha_4 - \alpha_1$ must have either the coefficient $-\tau$ in the first row or the coefficient τ both in the third and fourth row. The latter case is impossible, since the two nonvanishing coefficients of $\alpha_4 - \alpha_1$ have different values. Thus, we have $-\tau$ in the first row of $\alpha_4 - \alpha_1$, and if $\chi^{(4)}$ is chosen suitably,

the coefficient τ appears in the fourth row. Continuing in this manner we see that the $s-1$ columns $\mathfrak{a}_j - \mathfrak{a}_1$ can be assumed to have the form given in (21).

We see at once that this result is true for $s = 2$ too. Here, we may take $\tau = 1$, choosing $\chi^{(1)}$, $\chi^{(2)}$ such that $\mathfrak{a}_2 - \mathfrak{a}_1$ has coefficient 1 in the first row and -1 in the second row.

It is evident from (21) that we have exactly s exceptional characters, and, in our notation, they are the characters $\chi^{(1)}, \chi^{(2)}, \cdots, \chi^{(s)}$. Moreover, by (17), $\mathfrak{a}_1(\mathfrak{a}_i - \mathfrak{a}_1) = -1$ for $i = 2, 3, \cdots, s$. Using the form (21) of $\mathfrak{a}_j - \mathfrak{a}_1$, we obtain $a_{11}(-\tau) + a_{j1}\tau = -1$, whence $a_{i1} = a_{11} - \tau$ for $i = 2, 3, \cdots, s$. Adding $\mathfrak{a}_1$ and $\mathfrak{a}_j - \mathfrak{a}_1$ (given in (21)), $j = 2, 3, \cdots, s$, we see that $a_{ii} = a_{11}$, $a_{ij} = a_{11} - \tau$ for $i \neq j$. This completes the proof of (II.D); $a = a_{11} - \tau$.

(II.E) *The s exceptional characters $\chi^{(1)}, \chi^{(2)}, \cdots, \chi^{(s)}$ have the same degree f. Moreover, we have*

$$\chi^{(1)}(Y) = \chi^{(2)}(Y) = \cdots = \chi^{(s)}(Y)$$

for every element Y of $\mathfrak{G}$ which is not conjugate to a power of H.

This is an immediate consequence of (18) and (19) combined with (21).

5. The values of the characters of $\mathfrak{G}$ for the elements $H^r \neq 1$

We now determine the columns $\mathfrak{a}_0 - \mathfrak{a}_1$ and $\mathfrak{a}_{s+1} - \mathfrak{a}_1$. It follows from (17) that we have

$$(22)\quad (\mathfrak{a}_0 - \mathfrak{a}_1)^2 = 3, \qquad (\mathfrak{a}_{s+1} - \mathfrak{a}_1)^2 = 3, \qquad (\mathfrak{a}_0 - \mathfrak{a}_1)(\mathfrak{a}_{s+1} - \mathfrak{a}_1) = 1,$$

$$(23)\quad \mathfrak{a}_0(\mathfrak{a}_j - \mathfrak{a}_1) = 0, \qquad \mathfrak{a}_{s+1}(\mathfrak{a}_j - \mathfrak{a}_1) = 0 \qquad \text{for } j = 2, 3, \cdots, s.$$

Then (22) shows that $\mathfrak{a}_0 - \mathfrak{a}_1$ and $\mathfrak{a}_{s+1} - \mathfrak{a}_1$ both have three nonvanishing coefficients, and these have the values ± 1. At least in one row, both columns have an equal coefficient ± 1. If there were another row in which both had nonvanishing coefficients, then the three nonvanishing coefficients in both columns would appear in the same three rows, and then $(\mathfrak{a}_0 - \mathfrak{a}_1) - (\mathfrak{a}_{s+1} - \mathfrak{a}_1)$ would have only one nonvanishing coefficient ± 2. Then again (19) leads to a contradiction, since all $\chi^{(\mu)}(1)$ are positive.

Thus, we have exactly one row in which $\mathfrak{a}_0 - \mathfrak{a}_1$ and $\mathfrak{a}_{s+1} - \mathfrak{a}_0$ have a nonvanishing coefficient, and these two coefficients are equal and ± 1. There are two other rows in which $\mathfrak{a}_1 - \mathfrak{a}_0$ has a nonvanishing coefficient and two further rows in which $\mathfrak{a}_{s+1} - \mathfrak{a}_0$ has a nonvanishing coefficient. It follows from (19) that the three nonvanishing coefficients of $\mathfrak{a}_1 - \mathfrak{a}_0$ cannot all have the same sign. The same is true for $\mathfrak{a}_{s+1} - \mathfrak{a}_0$.

The equations (23) combined with (21) show that the first s coefficients of $\mathfrak{a}_0$ all have the same value a_{10}. By (20), the first s coefficients of $\mathfrak{a}_0 - \mathfrak{a}_1$ then are

(24) $$a_{10} - a - \tau, \quad a_{10} - a, \quad a_{10} - a, \quad \cdots, \quad a_{10} - a.$$

Since these coefficients are all equal to 0, $+1$, or -1, we have either $a_{10} = a$ or $a_{10} = a + \tau$. A similar argument applies to $\mathfrak{a}_{s+1} - \mathfrak{a}_1$. The first s coefficients here are

(25) $$a_{1,s+1} - a - \tau, \quad a_{1,s+1} - a, \quad \cdots, \quad a_{1,s+1} - a, \text{ and } \quad a_{1,s+1} = a \text{ or } a + \tau.$$

We wish to show that $a_{10} = a_{1,s+1} = a$. This is clear for $s \geqq 4$ since otherwise in (24) or in (25), there appear three or more coefficients $\tau = \pm 1$, which has been seen to be impossible.

Before dealing with the cases $s = 3$ and $s = 2$, let us first observe that if $\chi^{(j)}$ is the unit character, then (13) shows that $a_{j0} = 1$, $a_{jv} = 0$ for $v \neq 0$. Hence $\chi^{(j)}$ is not exceptional. We may then choose our notation such that $j = s + 1$, that is, such that $\chi^{(s+1)}$ is the unit character.

Assume now that $s = 3$. If we had $a_{10} = a_{1,s+1} = a + \tau$, then (24) and (25) show that both columns $\mathfrak{a}_0 - \mathfrak{a}_1$ and $\mathfrak{a}_{s+1} - \mathfrak{a}_0$ would have nonzero coefficients in rows 2 and 3, which is impossible. If one of a_{10}, $a_{s+1,0}$ is a and the other is $a + \tau$, the first three coefficients of $\mathfrak{a}_0 - \mathfrak{a}_{s+1}$ are equal, and their value is $\tau = \pm 1$. Moreover, the coefficient in the fourth row is ± 1, and as $(\mathfrak{a}_0 - \mathfrak{a}_{s+1})^2 = 4$ by (17), all other coefficients vanish. By (II.E), $\chi^{(1)}$, $\chi^{(2)}$, $\chi^{(3)}$ have the same degree f, while the unit character $\chi^{(4)}$ has degree 1. By (19), $(\mathfrak{a}_0 - \mathfrak{a}_{s+1})\chi(1) = (\mathfrak{a}_0 - \mathfrak{a}_1)\chi(1) - (\mathfrak{a}_{s+1} - \mathfrak{a}_1)\chi(1) = 0$, and hence $\pm 3f \pm 1 = 0$. This is impossible. Again, we must have $a_{10} = a_{1,s+1} = a$ for $s = 3$.

Take $s = 2$. If $a_{10} = a_{1,s+1} = a + \tau$, we simply replace $a + \tau$ by a, τ by $-\tau$, and we interchange $\chi^{(1)}$ and $\chi^{(2)}$. It is seen easily that (20) remains valid and that we have the desired case $a_{10} - a_{s+1,0} = a$. If $a_{10} = a + \tau$, $a_{s+1,0} = a$, it follows from (13) and (14) that

$$\chi^{(1)} \mid \mathfrak{H} = \tau(\varepsilon_0 + \varepsilon_1 + \varepsilon_1^{-1}) + a\sum_{i=-s}^{s+1} \varepsilon_i .$$

Since here $h = 6$, we see that

$$\chi^{(1)}(H) = 2\tau, \qquad \chi^{(1)}(H^2) = 0.$$

Now, H^2 is an element of order 3. Since the degree f of $\chi^{(1)}$ is congruent to $\chi^{(1)}(H^2)$ modulo a prime ideal divisor of 3, we have $f \equiv 0 \pmod 3$. Then $g\chi^{(1)}(H)/c(H)f = 2\tau g/3h = \tau g/9$, and since we have an algebraic integer, we find $g \equiv 0 \pmod 9$. This is inconsistent with (6).

Similarly, if $a_{10} = a$, $a_{1,s+1} = a + \tau$, a contradiction is obtained by considering $\chi^{(2)}$. We find here

$$\chi^{(2)} \mid \mathfrak{H} = \tau(\varepsilon_3 + \varepsilon_2 + \varepsilon_2^{-1}) + a\sum_{i=-2}^{3} \varepsilon_i ,$$

$$\chi^{(2)}(H) = -2\tau, \qquad \chi^{(2)}(H^2) = 0,$$

which again leads to $g \equiv 0 \pmod 9$, in contradiction to (6). Thus we may again assume that we have $a_{10} = a_{1,s+1} = a$. This is then true for $s \geqq 2$.

It now follows from (24), (25) that the first coefficient in $\mathfrak{a}_0 - \mathfrak{a}_1$ and $\mathfrak{a}_{s+1} - \mathfrak{a}_1$ is $-\tau$ and the next $s-1$ coefficients are 0. In the row $s+1$ belonging to the unit characters, we have the coefficients 1 and 0 respectively. Our previous results show that we may choose $\chi^{(s+2)}$, $\chi^{(s+3)}$, $\chi^{(s+4)}$ such that $\mathfrak{a}_0 - \mathfrak{a}_1$ has a coefficient ± 1 in the row $s+2$ and $\mathfrak{a}_{s+1} - \mathfrak{a}_1$ has coefficients ± 1 in the rows $s+3$, $s+4$, while all other coefficients in the two columns vanish. Collecting these results (cf. (13), (14), (20)) we find

$$
\begin{aligned}
\chi^{(i)} \mid \mathfrak{H} &= \tau(\varepsilon_i + \varepsilon_{-i}) + a\textstyle\sum_{j=-s}^{s+1} \varepsilon_j, \quad i = 1, 2, \cdots, s,\\
\chi^{(s+1)} \mid \mathfrak{H} &= \varepsilon_0,\\
\chi^{(s+2)} \mid \mathfrak{H} &= \delta_2 \varepsilon_0 + a_{s+2,1} \textstyle\sum_{j=-s}^{s+1} \varepsilon_j,\\
\chi^{(s+3)} \mid \mathfrak{H} &= \delta_3 \varepsilon_{s+1} + a_{s+3,1} \textstyle\sum_{j=-s}^{s+1} \varepsilon_j,\\
\chi^{(s+4)} \mid \mathfrak{H} &= \delta_4 \varepsilon_{s+1} + a_{s+4,1} \textstyle\sum_{j=-s}^{s+1} \varepsilon_j,\\
\chi^{(s+\mu)} \mid \mathfrak{H} &= a_{s+\mu,1} \textstyle\sum_{j=-s}^{s+1} \varepsilon_j,
\end{aligned} \tag{26}
$$

where $\delta_2, \delta_3, \delta_4 = \pm 1$. We set $\delta_1 = 1$.

We note that this result remains valid for $s = 1$. Indeed, we have here only the columns $\mathfrak{a}_0, \mathfrak{a}_2, \mathfrak{a}_1 = \mathfrak{a}_{-1}$. As before, there will be exactly one row in which $\mathfrak{a}_0 - \mathfrak{a}_1$ and $\mathfrak{a}_2 - \mathfrak{a}_1$ have a nonvanishing coefficient. The coefficient in this row will be the same in both columns and will be denoted by τ; the corresponding character is taken as $\chi^{(1)}$. The characters $\chi^{(2)}$, $\chi^{(3)}$ can be chosen such that $\mathfrak{a}_0 - \mathfrak{a}_1$ has coefficients ± 1 in the corresponding rows, and the characters $\chi^{(4)}$, $\chi^{(5)}$ such that $\mathfrak{a}_2 - \mathfrak{a}_1$ has coefficients ± 1 in the corresponding rows. Then (26) holds again.

We write χ_μ for $\chi^{(s+\mu)}$, $\mu > 0$. We then have the result

(II.F) *The irreducible characters of* $\mathfrak{G}$ *can be denoted by* $\chi^{(1)}, \chi^{(2)}, \cdots, \chi^{(s)}$, $\chi_1, \chi_2, \cdots, \chi_m$ *with* $m \geqq 4$ *in such a manner that we have for* $H^r \neq 1$

$$
\begin{aligned}
\chi^{(i)}(H^r) &= \tau(\varepsilon^{ir} + \varepsilon^{-ir}), && i = 1, 2, \cdots, s,\\
\chi_j(H^r) &= \delta_j, && j = 1, 2,\\
\chi_j(H^r) &= \delta_j(-1)^r, && j = 3, 4,\\
\chi_j(H^r) &= 0, && j \geqq 5.
\end{aligned} \tag{27}
$$

Indeed, this follows from (26), if we note that $\sum_{i=-s}^{s+1} \varepsilon_i$ vanishes for all $H^r \neq 1$.

6. Congruences for the degrees of the characters of $\mathfrak{G}$

If ψ is any character of $\mathfrak{S}(T)$, it follows from the orthogonality relations that

$$\psi(1) + (h/2)\psi(B) + (h/2)\psi(BH) + \textstyle\sum_{H^r \neq 1} \psi(H^r) \equiv 0 \pmod{2h}.$$

If ψ is the restriction of a character of $\mathfrak{G}$, then, by (II.A), $\psi(B) = \psi(BH) = \psi(T)$. Combining this with (27), we find

(II.G) *If f is the degree of the exceptional characters $\chi^{(i)}$, and if f_j is the degree of χ_j, $j = 1, 2, \cdots, m$, then*

$$
\begin{aligned}
f &\equiv 2\tau && \pmod{2h} \\
f_j &\equiv \delta_j && \pmod{2h} && (j = 1, 2) \\
f_j &\equiv h + \delta_j && \pmod{2h} && (j = 3, 4) \\
f_j &\equiv 0 && \pmod{2h} && (j \geqq 5).
\end{aligned} \tag{28}
$$

Proof. For $\psi = \chi^{(i)} \mid \mathfrak{C}(T)$, our congruence reads

$$f + h\tau((-1)^{h/2} + (-1)^{h/2}) + \tau \sum_{H^r \neq 1} (\varepsilon_i(H^r) + \bar{\varepsilon}_i(H^r)) \equiv 0 \pmod{2h}.$$

The orthogonality relations for the characters of $\mathfrak{H}$ show that

$$2 + \sum_{H^r \neq 1} (\varepsilon_i(H^r) + \bar{\varepsilon}_i(H^r)) = 0.$$

This yields $f \equiv 2\tau \pmod{2h}$. Similarly, for $j = 1, 2$

$$f_j + \delta_j h + \delta_j \sum_{H^r \neq 1} 1 \equiv 0 \pmod{2h}.$$

Here, $\sum_{H^r \neq 1} 1 = h - 1$, and hence $f_j \equiv \delta_j \pmod{2h}$. The proof of the last 2 congruences (28) is analogous.

(II.H) *We have*

$$1 + \delta_2 \chi_2(X) = \tau\chi^{(j)}(X), \qquad \delta_3 \chi_3(X) + \delta_4 \chi_4(X) = \tau\chi^{(j)}(X)$$

for elements X of $\mathfrak{G}$ which are not conjugate to element $H^r \neq 1$. In particular,

$$1 + \delta_2 f_2 = \tau f, \qquad \delta_3 f_3 + \delta_4 f_4 = \tau f. \tag{29}$$

This follows from $(a_0 - a_1)\chi(X) = 0$, $(a_{s+1} - a_1)\chi(X) = 0$ in conjunction with the values of the coefficients of the columns $a_0 - a_1$ and $a_{s+1} - a_1$ obtained above (χ_1 was the unit character, $\delta_1 = 1$).

7. The class relation

Let $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_k$ denote the classes of conjugate elements where we choose that notation such that $1 \in \mathfrak{K}_1$, $T \in \mathfrak{K}_2$, $H^j \in \mathfrak{K}_{2+j}$ for $j = 1, 2, \cdots, s$ (cf. (II.A)), and where $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_t$ $(t \geqq 2 + s)$ are the classes consisting of the "real" elements G of $\mathfrak{G}$, i.e., the elements G which are conjugate to their reciprocals G^{-1}.

We work in the group algebra Γ of $\mathfrak{G}$ over the field of rational numbers or rather in the center Z of Γ. If K_j denotes the sum of the elements in $\mathfrak{K}_j$, then $K_1, K_2, \cdots, K_k$ form a basis of Z. In particular, we have an equation

$$K_2^2 = \sum_{j=1}^{k} c_j K_j. \tag{30}$$

Here, c_j denotes the number of ordered pairs (X, Y) of elements of $\mathfrak{K}_2$ such that XY is equal to a fixed element $G_j \in \mathfrak{K}_j$. Since X, Y have order 2, the equation $XY = G_j$ implies $G_j^{-1} = YX = Y^{-1}G_j X$. Conversely, if X has order 2, and if $XG_j X^{-1} = G_j^{-1}$, then for $Y = XG_j$, we have $XY = G_j$, and $Y^2 = XG_j XG_j = G_j^{-1}G_j = 1$. Thus Y has order 2, except when $Y = 1$, $G_j = X$. This latter case arises only if G_j has order 2, i.e., if $j = 2$. Thus

(II.I) *If G_j is a representative of $\mathfrak{K}_j$, then for $f \neq 2$ the number c_j in* (30) *denotes the number of elements X of order 2 which satisfy the equation*

$$X^{-1}G_j X = G_j^{-1}.$$

For $j = 2$, c_j is one less than the number of X of order 2 which satisfy the corresponding equation.

If $j = 1$, c_1 is simply the number of elements of order 2, i.e., the number of elements of $\mathfrak{K}_2$. By (II.A), $c_1 = g/2h$. For $j = 2$, we may take $G_j = T$, and $c_2 + 1$ is the number of elements of order 2 which commute with T. It follows from (II.A) that $c_2 + 1 = h + 1$, $c_2 = h$. For $3 \leqq j \leqq 2 + s$, we may choose $G_j = H^{j-2}$. Since

$$X^{-1}G_j X = G_j^{-1} \quad \text{implies} \quad X \in \mathfrak{N}(\{H^{j-2}\}) = \mathfrak{C}(T),$$

(cf. (I.C)), the number c_j denotes the number of elements of order 2 of the dihedral group $\mathfrak{C}(T)$ which transform H^{j-2} into its reciprocal $(H^{j-2})^{-1}$. Hence $c_j = h$ for $j = 3, \cdots, 2 + s$. If $2 + s < j \leqq t$, the elements G_j and G_j^{-1} are conjugate in $\mathfrak{G}$. Hence there exist exactly $c(G_j)$ elements X in $\mathfrak{G}$ such that $X^{-1}G_j X = G_j^{-1}$. Then X^2 commutes with G_j. If the order of X^2 contained a prime factor of $2^{m+1}v = 2h$, by (II.A), X^2 would belong to one of the classes $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_{2+s}$. Moreover, for $X^2 \neq 1$, $\mathfrak{C}(X^2)$ would consist only of elements which lie in the same $s + 2$ classes. This is impossible for $j > s + 2$ since $G_j \in \mathfrak{C}(X^2)$. Hence $X^2 = 1$. Thus we have exactly $c(G_j)$ elements X of order 2 for which $X^{-1}G_j X = G_j^{-1}$ and $c_j = c(G_j)$ for $2 + s < j \leqq t$. Finally, for $j > t$, the elements G_j and G_j^{-1} are not conjugate, and $c_j = 0$.

If we count the number of elements of $\mathfrak{G}$ appearing as summands on both sides of (30), we have

$$(g/c(T))^2 = \sum_{j=1}^{k} c_j(g/c(G_j)).$$

Substituting the values of c_j just found, this yields

$$\frac{g^2}{4h^2} = \frac{g}{2h} + \frac{g}{2h}h + \sum_{j=3}^{s+2}\frac{g}{h}h + \sum_{j=s+3}^{t}\frac{g}{c(G_j)}c(G_j).$$

This yields

$$g^2/4h^2 = g/2h + g/2 + g(t - 2),$$

whence

$$t - 2 = (g - 2h - 2h^2)/4h^2. \tag{31}$$

8. The degrees of the irreducible characters of $\mathfrak{G}$

It will be necessary to separate the cases $\tau = 1$ and $\tau = -1$.

The case $\tau = 1$. It follows from (29) that $\delta_2 = 1$ since $\tau f = f > 0$. As shown by (29), the character χ_2 must be real, since $\tilde{\chi}_2$ cannot be equal to any of the characters except χ_2. If $f_2 = 1$, then $\mathfrak{G}$ would have a linear character $\chi_2 \neq \chi_1$, $\chi_2^2 = \chi_1$. Since the multiplicative group of linear characters is isomorphic with $\mathfrak{G}/\mathfrak{G}'$, it would follow that $\mathfrak{G}/\mathfrak{G}'$ has even order. This is impossible, if $\mathfrak{G}$ does not have a normal subgroup of index 2. Hence $f_2 \neq 1$, and (28) shows that $f_2 \geqq 2h + 1$. Now (29) shows that $f \geqq 2h + 2$. Interchanging χ_3 and χ_4 if necessary, we see from (29) that we may assume $\delta_3 = 1$. By (28), $f_3 \geqq h + 1$, $f_4 \geqq h + \delta_4$, $f_j \geqq 2h$ for $j \geqq 5$. Thus

$$f \geqq 2h + 2, \quad f_1 = 1, \quad f_2 \geqq 2h + 1, \quad f_3 \geqq h + 1, \quad f_4 \geqq h + \delta_4, \quad f_j \geqq 2h \quad \text{for} \quad j \geqq 5. \tag{32}$$

Since we have $s = h/2 - 1$ characters $\chi^{(i)}$, we shall have $k - s - 4 = k - h/2 - 3$ characters χ_j with $j \geqq 5$.

Now, the order g is the sum of the squares of the degrees of the irreducible characters. This yields

$$g \geqq (h/2 - 1)(2h + 2)^2 + 1 + (2h + 1)^2 + (h + 1)^2 + (h + \delta_4)^2 + (k - h/2 - 3)4h^2. \tag{33}$$

On account of (31), g can be written in the form

$$g = 4h^2(t - 2) + 2h + 2h^2.$$

Substituting this in (33), we have, after simplification,

$$4h^2 t \geqq 4kh^2 + 2\delta_4 h - 2h. \tag{34}$$

If $\delta_4 = 1$, this yields $t \geqq k$. Since $k \geqq t$, we have $k = t$, and we must have the equality sign everywhere in (32). If $\delta_4 = -1$, we still can conclude $k = t$, and we see that the left side in (33) exceeds the right side by $4h$. Thus, we must have an inequality in (32) for some j. If we write the inequality in (32) in the form $f_j > f_j^*$, then (28) shows that

$$f_j \geqq f_j^* + 2h.$$

Since $f_j^2 \geqq f_j^{*2} + 4hf_j^* + 4h^2$, we can add $4hf_j^* + 4h^2$ on the right-hand side of (33) and (34). This leads to a contradiction. Thus,

(II.J) *If* $\tau = 1$, *we have* $g = 4h^2k - 6h^2 + 2h$, $\delta_2 = \delta_3 = \delta_4 = 1$,

$$f = 2h + 2, \quad f_1 = 1, \quad f_2 = 2h + 1,$$

$$f_3 = f_4 = h + 1, \quad f_j = 2h \quad \text{for} \quad j \geqq 5.$$

The Case $\tau = -1$. Here $\delta_2 = -1$ by (29) and, after interchanging χ_3 and χ_4 if necessary, we may assume that $\delta_3 = -1$. Then (29) reads

$$f_2 - 1 = f, \qquad f_3 - \delta_4 f_4 = f. \tag{29*}$$

We separate the cases $\delta_4 = 1$ and $\delta_4 = -1$.

Subcase $\delta_4 = +1$. It follows from (28) that $f \geqq 2h - 2$, and hence $f_2 \geqq 2h - 1$. Moreover $f_4 \geqq h + 1$, and (29*) shows that $f_3 \geqq 3h - 1$. Also $f_j \geqq 2h$ for $j \geqq 5$.

Instead of (33), we find here

$$g \geqq (h/2 - 1)(2h - 2)^2 + 1 + (2h - 1)^2 + (3h - 1)^2 + (h + 1)^2 + (k - h/2 - 3)4h^2. \tag{33*}$$

Then (34) can be replaced by

$$4h^2 t \geqq 4h^2 k. \tag{34*}$$

It follows that we must have $k = t$, and that we must have equalities in all estimates

$$f = 2h - 2, \quad f_1 = 1, \quad f_2 = 2h - 1, \quad f_3 = 3h - 1, \quad f_4 = h + 1, \quad f_j = 2h \text{ for } j \geqq 5.$$

Subcase $\delta_4 = -1$. Here,

$$f \geqq 2h - 2, \quad f_2 \geqq 2h - 1, \quad f_3 \geqq h - 1, \quad f_4 \geqq h - 1, \quad f_j \geqq 2h \text{ for } j \geqq 5.$$

Then

$$g \geqq (h/2 - 1)(2h - 2)^2 + 1 + (2h - 1)^2 + (h - 1)^2 + (h - 1)^2 + (k - h/2 - 3)4h^2.$$

This leads to

$$4th^2 \geqq 4kh^2 - 8h^2. \tag{34**}$$

If one of the degrees f_j has a value larger than the estimate f_j^* used here, by (28), $f_j \geqq f_j^* + 2h$, and we can add a term $4hf_j^* + 4h^2$ on the right-hand side of (34**). If $j \geqq 5$, this is an additional term $12h^2$, which is impossible as $t \leqq k$. If $1 \leqq j \leqq 4$, it follows from (29) that we must have inequality for two values of j, and again, this gives a contradiction. Finally, if $f > f^*$, we have an additional term $(h/2 - 1)(4h(2h - 2) + 4h^2)$. Again, we have a contradiction. It follows that the degrees have the values used in the estimates and that the equality sign holds in (34**), that is, that $t = k - 2$. Thus

(II.J*) *If* $\tau = -1$, *then we can assume* $\delta_2 = \delta_3 = -1$,

$$f = 2h - 2, \quad f_1 = 1, \quad f_2 = 2h - 1, \quad f_j = 2h \text{ for } j \geqq 5.$$

Case (a) *If* $\delta_4 = 1$, *then*

$$f_3 = 3h - 1, \qquad f_4 = h + 1, \qquad k = t, \quad \text{and} \quad g = 4kh^2 - 6h^2 + 2h.$$

Case (b) *If* $\delta_4 = -1$, *then*

$$f_3 = f_4 = h - 1, \qquad t = k - 2, \qquad g = 4kh^2 - 14h^2 + 2h.$$

9. The order g

It follows easily from the basic properties of the group characters that the coefficients c_j in (30) are given by the formula

$$c_j = \frac{g}{c(T)^2} \sum_{\mu=1}^{k} \frac{\chi^{(\mu)}(T)^2 \chi^{(\mu)}(G_j)}{\chi^{(\mu)}(1)}, \tag{35}$$

where $\chi^{(\mu)}$ ranges over all irreducible characters of $\mathfrak{G}$, and where $G_j \in \mathfrak{R}_j$. For $G_j = H$, we had $c_j = h$, $c(T) = 2h$. Now (27) yields $\chi^{(j)}(T) = \pm 2$, and we find from (27), (II.J), (II.J*), if either $\tau = 1$, or $\tau = -1$, $\delta_4 = -1$, that

$$4h^3 = g\left(\frac{4}{2h + 2\tau}\left(\tau \sum_{j=1}^{s} (\varepsilon^j + \varepsilon^{-j})\right) + \frac{1}{1} + \frac{\tau}{2h + \tau} + 2\frac{-\tau}{h + \tau}\right).$$

Now, $\sum_{j=1}^{s} (\varepsilon^j + \varepsilon^{-j}) + 1 + (-1) = 0$, whence $\sum_{j=1}^{s} (\varepsilon^j + \varepsilon^{-j}) = 0$, and

$$4h^3 = g\,\frac{2h^2 + 3h\tau + 1 + h\tau + 1 - 4h\tau - 2}{(2h + \tau)(h + \tau)} = \frac{2h^2}{(2h + \tau)(h + \tau)}\,g,$$

whence

$$g = 2h(2h + \tau)(h + \tau). \tag{36}$$

On the other hand, if $\tau = -1$, $\delta_4 = 1$, the same method yields

$$4h^3 = g\left(1 - \frac{1}{2h - 1} + \frac{1}{3h - 1} - \frac{1}{h + 1}\right),$$

whence we find mod $h - 1$ that

$$4 \equiv g(1 - 1 + \tfrac{1}{2} - \tfrac{1}{2}) \equiv 0.$$

(Note that $h - 1$ is relatively prime to $2h - 1$, $3h - 1$, and $h + 1$ since h is even.) But then $h - 1$ divides 4, which is impossible for $h \neq 2$, and $h = 2$ was excluded. Thus, this case is impossible; in (II.J*), the subcase $\delta_4 = 1$ is excluded, and we have

$$\delta_2 = \tau, \qquad \delta_3 = \tau, \qquad \delta_4 = \tau. \tag{II.J**}$$

10. The elements R and the elements S

Let R denote any element whose order contains a prime factor p' of $h + \tau$, and let S denote any element whose order contains a prime factor p of $2h + \tau$. Since any two of $2h$, $2h + \tau$, $h + \tau$ are relatively prime, it follows

from (36) that f_2 is divisible by the full power of p dividing g; cf. (II.J), (II.J*). Hence

$$\chi_2(S) = 0. \tag{37}$$

Similarly, f_3, f_4 are divisible by the full power of p' dividing g and we have

$$\chi_3(R) = \chi_4(R) = 0. \tag{38}$$

It follows from (II.H) that $\chi^{(j)}(S) = \tau$, $\chi^{(j)}(R) = 0$, $\chi_2(R) = -\tau$. Clearly, $R \neq S$. Hence no element can have an order divisible by primes p and p'. In conjunction with (II.A), this yields

(II.K) *For every element R, $c(R)$ divides $h + \tau$, and for every element S, $c(S)$ divides $2h + \tau$.*

Apply now (35) taking $G_j = R$. We find (cf. (36))

$$c_j = \frac{g}{4h^2}\left(1 - \frac{\tau}{2h + \tau}\right) = \frac{h + \tau}{2h}\, 2h = h + \tau.$$

Since $c_j \neq 0$, the class $\mathfrak{K}_j$ is real, and we have

$$c(R) = h + \tau \tag{39}$$

for every R.

Similarly, taking $G_j = S$ in (34), we find

$$c_j = \frac{g}{4h^2}\left(\frac{4s}{2h + 2\tau}\,\chi^{(1)}(S) + \frac{1}{h + \tau}\,(\chi_3(S) + \chi_4(S)) + 1\right);$$

cf. (II.E), (II.J), (II.J*), (II.J**). But $\chi_3(S) + \chi_4(S) = \chi^{(1)}(S)$ by (II.H), and we have

$$c_j = \frac{g}{4h^2}\left(\frac{(h - 2)\tau + \tau}{h + \tau} + 1\right) = \frac{2h + \tau}{2h}\, h(1 + \tau).$$

Hence, if $\tau = 1$, the class $\mathfrak{K}_j$ is real, and

$$c(S) = 2h + 1 \qquad \text{for} \quad \tau = 1.$$

If $\tau = -1$, the class $\mathfrak{K}_j$ is not real. Since there exist only two nonreal classes (as $k = t + 2$), we have exactly two classes containing elements S. This implies that $2h - 1$ is a prime power in this case.[3]

Actually this result holds for $\tau = 1$ too. Indeed, by (II.J) and (36), $2hk - 3h + 1 = 2h^2 + 3h + 1$ for $\tau = 1$, whence $k = h + 3$. Since we have $s + 2 = h/2 + 1$ classes containing elements 1, T, and H^j, we have $h/2 + 2$ classes containing elements R and S. The orthogonality relation

[3] If $2h - 1$ were divisible by two distinct primes p_1 and p_2, we would have elements S of orders p_1 and of orders p_2. For $\tau = 1$, S and S^{-1} are not conjugate. We would have at least four classes of elements S.

for χ_2, χ_0 yields

$$(2h + 1) + g/2h + s(g/h) - \sum_R 1 = 0.$$

This shows that the number of elements R is equal to

$$2h + 1 + (2h + 1)(h + 1)(1 + 2s)$$
$$= (2h + 1)(1 + (h + 1)(h - 1)) = (2h + 1)h^2.$$

By (39) each class $\mathfrak{K}_j$ consisting of elements R contains

$$g/(h + 1) = (2h + 1)(2h)$$

such elements, and hence there are $h/2$ classes consisting of elements R. Thus there are exactly two classes consisting of elements S. As already remarked,[4] this is only possible if $2h + \tau$ is a power p^n of a prime,

$$2h + \tau = p^n. \tag{40}$$

We had shown above that $c(S) = 2h + \tau$ for $\tau = 1$. We can now prove that this holds for $\tau = -1$. Indeed, since $k = t + 2$, we have two nonreal classes in this case, and these must be the classes containing the elements S. If S is chosen such that S occurs in the center of the p-Sylow group $\mathfrak{P}$, then $c(S) = p^n = 2h + \tau = 2h - 1$. Since the other class is represented by S^{-1}, we have $c(S^{-1}) = 2h - 1$ for the elements of this class. Hence

$$c(S) = 2h + \tau. \tag{41}$$

11. The groups $\mathfrak{N}$ and $\mathfrak{S}$ and their normalizers

(II.L) *The group $\mathfrak{G}$ has an abelian subgroup $\mathfrak{N}$ of order $h + \tau$. The centralizer $\mathfrak{C}(R)$ of each element R can be taken for $\mathfrak{N}$.*

Proof. Our previous results show that for each element R, we have

$$c(R) = h + \tau,$$

that the elements of $\mathfrak{C}(R)$ different from 1 are of the type R again, and that R is real. Now, Theorem (4D) of [1] shows that $\mathfrak{N} = \mathfrak{C}(R)$ is abelian.

It follows from Theorem (4F) of [1] that if the order of the normalizer $\mathfrak{N}(\mathfrak{N})$ is $w(h + \tau)$, then w divides $h + \tau - 1$, and we can set

$$g = w(h + \tau)(1 + N(h + \tau))$$

with integral $N \geqq 0$. Hence $w(1 + N(h + \tau)) = 2h(2h + \tau)$, whence $w \equiv 2h(2h + \tau) \pmod{h + \tau}$. Hence $w \equiv -2\tau(-\tau) \equiv 2 \pmod{h + \tau}$. Since $w \leqq h + \tau - 1$, we must have $w = 2$. Thus

[4] Since the case $\tau = -1$ has been settled above, we may assume $\tau = 1$. Here, $c(S) = 2h + 1$. If $2h + 1$ were divisible by two distinct primes p_1 and p_2, we would have classes of elements S of each of the orders p_1, p_2, and $p_1 p_2$.

(II.M) *The normalizer of the subgroup* $\mathfrak{R}$ *in* (II.L) *has the order* $2(h + \tau)$.

As a consequence, we have

(II.N) *If an element* R *is conjugate to a power* R^μ *in* $\mathfrak{G}$, *then* $R^\mu = R^{\pm 1}$.

Indeed, if $G^{-1}RG = R^\mu$, and if we take $\mathfrak{R} = \mathfrak{C}(R)$, then $G^{-1}\mathfrak{R}G = \mathfrak{R}$. Hence $G \in \mathfrak{N}(\mathfrak{R})$, and by (II.M) $G^2 \in \mathfrak{R}$, $R^{\mu^2} = R$, $\mu^2 \equiv 1 \pmod{h + \tau}$. Since $h + \tau$ is odd, then $\mu \equiv \pm 1 \pmod{h + \tau}$.

If $\tau = 1$, the element S belongs to a real class, and the same argument as used in (II.L) shows that $\mathfrak{C}(S) = \mathfrak{S}$ is abelian. In order to have the same result for $\tau = -1$, we have to use a more complicated procedure.

(II.O) LEMMA. *Let* $\mathfrak{G}$ *be any finite group. Let* p *be a prime dividing the order* g *of* $\mathfrak{G}$, *and make the following assumptions*:

(a) *If* Q *is an element of prime power order* $q^\alpha > 1$, $p \neq q$, *the order of* $\mathfrak{N}(\{Q\})$ *is not divisible by* p.

(b) *A generalized quaternion group does not appear as a subgroup of* $\mathfrak{G}$.

Then either the p*-Sylow subgroup of* $\mathfrak{G}$ *is normal in* $\mathfrak{G}$, *or any two distinct* p*-Sylow subgroups have intersection* $\{1\}$.

Proof. Suppose that there exist two distinct p-Sylow subgroups $\mathfrak{P}$ and $\mathfrak{P}_1$ with $\mathfrak{P} \cap \mathfrak{P}_1 = \mathfrak{D} \neq \{1\}$. Choose $\mathfrak{P}$ and $\mathfrak{P}_1$ so that $\mathfrak{D}$ has maximal order. Then $\mathfrak{P} \cap \mathfrak{N}(\mathfrak{D}) \supset \mathfrak{D}$, $\mathfrak{P}_1 \cap \mathfrak{N}(\mathfrak{D}) \supset \mathfrak{D}$, and

$$(\mathfrak{P} \cap \mathfrak{N}(\mathfrak{D})) \cap (\mathfrak{P}_1 \cap \mathfrak{N}(\mathfrak{D})) = \mathfrak{D}.$$

Hence $\mathfrak{N}(\mathfrak{D})$ has two distinct p-Sylow subgroups whose intersection is not $\{1\}$.

Choose a principal series of $\mathfrak{N}(\mathfrak{D})$ through $\mathfrak{D}$, and let $\mathfrak{B}$ be the last group different from $\{1\}$ in this series. Since $\mathfrak{B} \subseteqq \mathfrak{D}$, $\mathfrak{B}$ is a p-group and hence abelian of type $(p, p, \cdots, p)$. Choose a normal subgroup $\mathfrak{A}$ of $\mathfrak{N}(\mathfrak{D})$ such that (1) $\mathfrak{A} \supseteqq \mathfrak{B}$, (2) $\mathfrak{A}$ has at least two distinct p-Sylow subgroups, and (3) $\mathfrak{A}$ has minimal order, subject to the previous conditions.

Since $\mathfrak{B}$ is normal in $\mathfrak{A}$, the transformation of $\mathfrak{B}$ by an element $A \in \mathfrak{A}$ can be described by a matrix $[A]$ with coefficients in the Galois field with p elements, and the mapping $A \to [A]$ is a homomorphism. Let q denote the smallest prime factor $\neq p$ of $(\mathfrak{A}:1)$. Since $\mathfrak{A}$ cannot be a p-group, such a prime q exists. Let $\mathfrak{Q}$ be a q-Sylow group of $\mathfrak{A}$, and let $Q \in \mathfrak{Q}$, $Q \neq 1$. The assumption (a) shows that Q cannot commute with an element $B \neq 1$ of $\mathfrak{B}$. Hence the linear transformation belonging to $[Q]$ does not leave a vector $\neq 0$ fixed. It follows that $\mathfrak{Q}$ cannot have a subgroup of type (q, q). It follows that $\mathfrak{Q}$ is cyclic, $\mathfrak{Q} = \{Q_0\}$ say. Suppose that two distinct powers Q and Q^μ are conjugate in $\mathfrak{A}$. We may then find an element A of prime power order p_0^γ such that $A^{-1}QA = Q^\nu \neq Q$, $A \in \mathfrak{A}$. Then p_0 must be different from q. Since p_0 must divide $q - 1$, it follows from our choice of q that p_0 can only be p itself. But this is excluded by the assumption (a).

Hence no two distinct elements of $\mathfrak{Q}$ are conjugate in $\mathfrak{A}$. Now, Burnside's Theorem shows that $\mathfrak{A}$ has a normal subgroup $\mathfrak{A}_0$ consisting of the elements of $\mathfrak{A}$ of orders prime to q. Clearly, $\mathfrak{A}_0$ is even normal in $\mathfrak{N}(\mathfrak{D})$. Moreover, all p-Sylow subgroups of $\mathfrak{A}$ appear in $\mathfrak{A}_0$ and $\mathfrak{B} \subseteqq \mathfrak{A}_0$. This shows that $\mathfrak{A}_0$ satisfies the conditions (1), (2) imposed on $\mathfrak{A}$, and as $\mathfrak{A}_0 \subset \mathfrak{A}$, we have a contradiction. The lemma (II.O) has been proved.

We use (II.O) to show that for any element S, the group $\mathfrak{C}(S)$ is abelian. If p is as in (40), and if $\mathfrak{P}$ is the p-Sylow subgroup of $\mathfrak{G}$, we have to show that $\mathfrak{P}$ is abelian, since we know that $c(S)$ divides $2h + \tau$; cf. (II.K). As already remarked, we may assume that $\tau = -1$. If we choose $S_0 \neq 1$ in the center of $\mathfrak{P}$, we certainly have $c(S_0) = p^n$. Since every element S is conjugate to S_0 or S_0^{-1} in the case $\tau = -1$, $c(S) = p^n$. Hence every element S appears in the center of some p-Sylow subgroup. If $\mathfrak{P}$ is not abelian, there must exist two distinct p-Sylow subgroups whose intersection is different from $\{1\}$. Since the condition (b) of (II.O) is satisfied for our $\mathfrak{G}$, it remains to check condition (a) of (II.O). Since $q \neq p$, an element Q of order $q^\alpha > 1$ is either conjugate to an element of H or to an element R. If we had $P^{-1}QP = Q^\nu$, $Q^\nu = Q^{\pm 1}$; cf. (II.A), (II.N). But since

$$c(P) = 2h + \tau,$$

we cannot have $P^{-1}QP = Q$. If $P^{-1}QP = Q^{-1}$, P would have even order, which is equally impossible. Hence we have a contradiction.
Thus,

(II.P) *The p-Sylow group $\mathfrak{P}$ of order $2h + \tau = p^n$ of $\mathfrak{G}$ is abelian.*

Two elements of $\mathfrak{P}$ are conjugate in $\mathfrak{G}$ if and only if they are conjugate in $\mathfrak{N}(\mathfrak{P})$. Since $c(P) = 2h + \tau$ for every $P \neq 1$ in $\mathfrak{P}$ (P being of type (S)), we see that the number of conjugates of P belonging to $\mathfrak{P}$ is equal to $(\mathfrak{N}(\mathfrak{P}):\mathfrak{P})$. But since we have two classes of elements S, it follows that

$$2(\mathfrak{N}(\mathfrak{P}):\mathfrak{P}) = p^n - 1.$$

Hence $\mathfrak{N}(\mathfrak{P})$ has the order

$$\tfrac{1}{2}p^n(p^n - 1) = \begin{cases} (2h + 1)h & \text{for } \tau = 1, \\ (2h - 1)(h - 1) & \text{for } \tau = -1. \end{cases}$$

12. Proof of the main theorem

Since $\mathfrak{G}$ has a subgroup $\mathfrak{N}(\mathfrak{P})$ of order $(2h + 1)h$ for $\tau = 1$ and of order $(2h - 1)(h - 1)$ for $\tau = -1$, it follows that $\mathfrak{G}$ has a representation $\mathfrak{Z}$ as a transitive group of permutations in $2(h + 1)$ or $2h$ letters respectively.

The case $\tau = 1$. After removing the unit character from the character of $\mathfrak{Z}$, we have a character of degree $2h + 1$ which no longer contains the unit character. It follows from (II.J) that this character must be irreducible and equal to χ_2. Hence $\mathfrak{Z}$ has the character $\chi_1 + \chi_2$. Since two distinct

irreducible constituents appear, $\mathfrak{Z}$ is doubly transitive. The number

$$\chi_1(G) + \chi_2(G)$$

gives the number of symbols left fixed by $\mathfrak{Z}(G)$. It follows from (27) that this is 2 for $G = H^r \neq 1$. For $G = S$, it is 1 by (37), and since

$$\chi_2(R) = -\tau$$

as remarked in connection with (38), it is 0 for R. Hence no $\mathfrak{Z}(G)$ with $G \neq 1$ leaves three letters fixed. Because of the double transitivity, the subgroup leaving two letters fixed has order $g/(2h + 2)(2h + 1) = h$, and the subgroup leaving one letter fixed has order $h(2h + 1)$. The elements of order 2 leave two letters fixed.

The case $\tau = -1$. Here, the character of $\mathfrak{Z}$ has the form $\chi_1 + \chi$ where χ is a character of degree $2h - 1$. It follows from (II.J*) that $\chi = \chi_2$.

Again, $\mathfrak{Z}$ is doubly transitive. It follows here from (27) that the elements $\mathfrak{Z}(H^r)$ for $H^r \neq 1$ do not leave any letter fixed. The elements $\mathfrak{Z}(R)$ leave two letters fixed, and the elements $\mathfrak{Z}(S)$ leave one letter fixed. No element $\mathfrak{Z}(G)$, $G \neq 1$, then leaves three letters fixed.

The subgroup for which $\mathfrak{Z}(G)$ leaves two letters fixed has order

$$(2h - 1)(h - 1),$$

and the subgroup for which $\mathfrak{Z}(G)$ leaves two letters fixed has order $h - 1$.

In both cases, $\mathfrak{Z}$ is faithful. Indeed, the degree is at least 3 and only $\mathfrak{Z}(1)$ leaves three letters fixed.

We now apply Zassenhaus' method; cf. [2]. We have a group of permutations of $N + 1$ letters, doubly transitive, such that only the identity leaves three letters fixed. The order of the group is

$$\tfrac{1}{2}(N + 1)N(N - 1), \qquad N = 2h + \tau.$$

In the case $\tau = -1$, Zassenhaus' assumptions are not quite satisfied, since the subgroup leaving two letters fixed does not contain elements of order 2. However, the method still works. This yields the result:

$$\mathfrak{G} \cong LF(2, 2h + \tau) \qquad (\tau = \pm 1).$$

III. The Case B

1. Assumptions

We assume here

(I) $\mathfrak{G}$ is a finite group of type (S).

(II) The 2-Sylow subgroup $\mathfrak{T}$ of $\mathfrak{G}$ is abelian of type $(2, 2, \cdots, 2)$, of order $2^a > 2$.[5]

(III) $\mathfrak{G}$ does not have a proper normal subgroup which includes $\mathfrak{T}$, and $\mathfrak{G} \neq \mathfrak{T}$.

[5] For $a = 2$ assume also that $\mathfrak{C}(T) = \mathfrak{T}$ for $T \in \mathfrak{T}$, $T \neq 1$; cf. (1).

As shown in I, it follows from (I) and (II) that for $a \geqq 3$, we have

$$\mathfrak{C}(T) = \mathfrak{T}$$

for $T \in \mathfrak{T}$, $T \neq 1$. The case $a = 2$, $\mathfrak{C}(T) \neq \mathfrak{T}$ for some $T \in \mathfrak{T}$, $T \neq 1$ has been treated in II. Hence we assume that if $a = 2$, we still have

$$\mathfrak{C}(T) = \mathfrak{T} \qquad \text{for} \quad T \in \mathfrak{T}, \quad T \neq 1. \tag{1}$$

2. The classes of involutions

(III.A) *All elements of order 2 of $\mathfrak{G}$ belong to the same class of conjugate elements.*

Proof. Suppose that X and Y are two involutions which belong to different classes. Then by Lemma (3A) of [1], there exists an involution Z such that $Z \in \mathfrak{C}(X)$, $Z \in \mathfrak{C}(Y)$. If $X \in \mathfrak{T}$, it follows from (1) that

$$Z \in \mathfrak{C}(X) = \mathfrak{T}, \qquad Y \in \mathfrak{C}(Z) = \mathfrak{T}.$$

Hence all the elements of the class of Y belong to $\mathfrak{T}$. By reasons of symmetry, the same is true for the class of X. It follows that $\mathfrak{T}$ consists of full classes of conjugate elements. Hence $\mathfrak{T}$ is normal in $\mathfrak{G}$, and this has been excluded.

3. The normalizer of $\mathfrak{T}$

Let $\mathfrak{N} = \mathfrak{N}(\mathfrak{T})$. It is clear that two elements of $\mathfrak{T}$ are conjugate in $\mathfrak{G}$ if and only if they are conjugate in $\mathfrak{N}$. Hence the class of T ($T \in \mathfrak{T}$, $T \neq 1$) in $\mathfrak{N}$ consists of all elements $\neq 1$ of $\mathfrak{T}$. Thus,

$$2^a - 1 = (\mathfrak{N}:(\mathfrak{N} \cap \mathfrak{C}(T)) = (\mathfrak{N}:\mathfrak{T}).$$

It follows that

$$(\mathfrak{N}:1) = (2^a - 1)2^a.$$

Any two different 2-Sylow groups $\mathfrak{T}$ and $\mathfrak{T}_1$ have intersection $\{1\}$. Indeed, if $T_0 \in \mathfrak{T} \cap \mathfrak{T}_1$, and if we had $T_0 \neq 1$, we would find

$$\mathfrak{C}(T_0) = \mathfrak{T} \quad \text{and} \quad \mathfrak{C}(T_0) = \mathfrak{T}_1.$$

It is now clear that the number of 2-Sylow groups of $\mathfrak{G}$ is congruent to 1 (mod 2^a). If we denote this number by $1 + 2^a N$, we have $N \geqq 1$, since $\mathfrak{T}$ is not normal in $\mathfrak{G}$. Hence $(\mathfrak{G}:\mathfrak{N}) = 1 + 2^a N \geqq 1 + 2^a$, and we have

$$g = 2^a(2^a - 1)(1 + 2^a N) \geqq (2^a + 1)2^a(2^a - 1). \tag{2}$$

4. The class relation

Let $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_k$ denote the classes of conjugate elements of $\mathfrak{G}$ where we choose the notation such that $1 \in \mathfrak{K}_1$, $T \in \mathfrak{K}_2$ for T of order 2, and such that $\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_t$ are real. Let K_j denote the sum of the elements of $\mathfrak{K}_j$ taken in the group algebra of $\mathfrak{G}$ over the field of rational numbers. It

follows from [1], (2A), (4B), that

$$K_2^2 = (g/2^a)K_1 + (2^a - 2)K_2 + \sum_{j=3}^{t} c(G_j)K_j, \tag{3}$$

where G_j denotes a representative of $\mathfrak{R}_j$. Comparing the number of elements of $\mathfrak{G}$ appearing on both sides of (3), we find

$$g^2/2^{2a} = g/2^a + 2^a(g/2^a) - 2(g/2^a) + (t - 2)g,$$

whence

$$g = (t - 1)2^{2a} - 2^a. \tag{4}$$

5. The degrees of the irreducible characters of $\mathfrak{G}$

Let $\chi_1, \chi_2, \cdots, \chi_k$ denote the irreducible characters of $\mathfrak{G}$; let

$$f_j = \chi_j(1)$$

be the degree of χ_j. Take χ_1 as the unit character.

If we set $\chi_j(T) = z_j$, then z_j is a rational integer. The orthogonality relations for $\chi_j \mid \mathfrak{T}$ yield

$$f_j + (2^a - 1)z_j = b_j 2^a, \tag{5}$$

where b_j is a nonnegative rational integer, the multiplicity of the unit character in $\chi_j \mid \mathfrak{T}$. We choose our notation so that $z_j > 0$ for $j = 1, 2, \cdots, r$; $z_j < 0$ for $j = r + 1, r + 2, \cdots, r + s$; $z_j = 0$ for $j = r + s + 1, \cdots, k$. Except for $j = 1$, we do not have $z_j = f_j$, since otherwise $\mathfrak{T}$ would belong to the kernel of χ_j, and this is excluded by the assumption (III). It follows from (5) that we can set

$$f_j = z_j + 2^a c_j \tag{6}$$

with rational integers c_j. Since $z_j < f_j$ for $j \neq 1$, we have here

$$c_j \geqq 1 \qquad \text{for } j = 2, 3, \cdots, r. \tag{6a}$$

For $j = r + 1, \cdots, r + s$, we have $c_j = b_j - z_j \geqq -z_j$, that is,

$$c_j \geqq |z_j| \qquad \text{for } j = r + 1, \cdots, r + s. \tag{6b}$$

Finally

$$c_j \geqq 1 \qquad \text{for } j = r + s + 1, \cdots, k. \tag{6c}$$

Now $g = \sum_{j=1}^{k} f_j^2$. Since $k \geqq t$, it follows from (4) that some of the f_j with $j \geqq 2$ must be smaller than 2^a. It follows from (6) that this can only be so in the case of (6b). Since $\sum_{j=1}^{k} |\chi_j(T)|^2 = c(T) = 2^a$, we have

$$\sum_{j=1}^{r+s} z_j^2 = 2^a. \tag{7}$$

Thus, $|z_j| < 2^a$, and we must have $c_j = 1$, $z_j = -1$.

Suppose that we have b values of j for which $z_j = -1$, $c_j = 1$, that is,

$f_j = 2^a - 1$. Since $z_1 = 1$, it follows from (7) that

$$b \leqq 2^a - 1. \tag{8}$$

The term $f_1 = 1$ and the b terms $2^a - 1$ contribute

$$1 + b(2^a - 1)^2 = b2^{2a} - 2^{a+1}b + b + 1$$

to $\sum_{j=1}^{k} f_j^2 = g$. Hence, for the remaining $k - b - 1$ terms, we have, by (4),

$$\begin{aligned} \sum{}' f_j^2 &= g - b2^{2a} + 2^{a+1}b - b - 1 \\ &= (t - b - 1)2^{2a} - 2^a + 2^{a+1}b - b - 1. \end{aligned} \tag{9}$$

Since k is the number of all classes of conjugate elements of $\mathfrak{G}$, and t the number of "real" classes, we have $k \geqq t$. If $k > t$, then $k \geqq t + 2$, as the non-real classes appear in pairs. Then, there appear

$$k - b - 1 \geqq (t - b - 1) + 2$$

terms $f_j^2 \geqq 2^{2a}$ on the left-hand side of (9), and this side is at least

$$(t - b - 1)2^{2a} + 2 \cdot 2^{2a}.$$

By (8), $2^{a+1}b \leqq 2 \cdot 2^{2a}$, and (9) leads to a contradiction. Thus, $t = k$ and we have

(III.B) *All classes of $\mathfrak{G}$ are real.*

Suppose that some of the f_j in (9) were at least $2^{a+1} - 2$. Then

$$f_j^2 = 2^{2a+2} - 2^{a+3} + 4 = 3 \cdot 2^{2a} + 2^{2a} - 8 \cdot 2^a + 4,$$

and we see that the left side of (9) would be at least

$$(k - b - 1)2^{2a} + 3 \cdot 2^{2a} - 8 \cdot 2^a + 4.$$

Because $k = t$, (9) yields

$$3 \cdot 2^{2a} - 8 \cdot 2^a + 4 \leqq -2^a + 2^{a+1}b - b - 1.$$

Using (8), we obtain $2^{a+1}b \leqq 2 \cdot 2^{2a} - 2 \cdot 2^a$, and hence

$$2^{2a} + 6 \leqq 5 \cdot 2^a.$$

This is certainly false for $a \geqq 3$, since $2^{2a} \geqq 8 \cdot 2^a$. It is also false for $a = 2$. Hence all f_j satisfy $f_j < 2 \cdot 2^a - 2$. Now (6) shows that we must have $c_j = 1$ in the case of (6a) and (6c). If $|z_j| \geqq 3$ in the case of (6b), then $c_j \geqq 3$ and $f_j = z_j + 3 \cdot 2^a \geqq -2^a + 3 \cdot 2^a$, since $|z_j| < 2^a$ by (7). This is impossible. If $z_j = -2$, then $c_j \geqq 2$ and $f_j \geqq 2 \cdot 2^a - 2$, which was also excluded. If $z_j = -1$ and $c_j \geqq 2$, we have likewise a contradiction. Hence we must have

$z_j = -1$, $c_j = 1$. This yields the result:

(III.C) *The degrees of the irreducible representations of* $\mathfrak{G}$ *have the following values:*

$$f_1 = 1, \qquad f_j = z_j + 2^a, \qquad j = 2, 3, \cdots, r,$$

with $z_j > 0$,

$$f_j = 2^a - 1, \qquad j = r+1, \cdots, r+s,$$

and $s = b$,

$$f_j = 2^a, \qquad \text{for } j > r+s+1.$$

Moreover, (cf. (7)),

$$\sum_{j=1}^{r} z_j^2 + s = 2^a. \tag{10}$$

By the orthogonality relations, we also have

$$0 = \sum_j f_j \chi_j(T) = \sum_j f_j z_j = 1 + \sum_{j=2}^{r}(2^a + z_j)z_j - s(2^a - 1).$$

This yields $2^a(\sum_{j=2}^{r} z_j - s) + 2^a = 0$, and hence

$$\sum_{j=2}^{r} z_j = s - 1. \tag{11}$$

The coefficient $2^a - 2$ of K_2 in (3) can be expressed by the characters in the form

$$2^a - 2 = \frac{g}{2^{2a}} \sum_j \frac{\chi_j(T)^3}{f_j}. \tag{12}$$

Because of the values obtained for the f_j and $z_j = \chi_j(T)$, the sum here is

$$1 + \sum_{j=2}^{r} \frac{z_j^3}{2^a + z_j} - s\,\frac{1}{2^a - 1}.$$

Now,

$$\frac{z_j^3}{2^a + z_j} = \frac{z_j^2}{(2^a/z_j) + 1} \geqq \frac{z_j^2}{2^a + 1},$$

and the sum is at least equal to

$$1 + \frac{1}{2^a + 1}\sum_{j=2}^{r} z_j^2 - s\,\frac{1}{2^a - 1} = 1 + \frac{2^a - s - 1}{2^a + 1} - s\,\frac{1}{2^a - 1};$$

cf. (10). Thus, (12) yields

$$(2^a - 2)2^{2a} \geqq g\,\frac{2^{2a} - 1 + 2^{2a} - s2^a - 2^a - 2^a + s + 1 - s2^a - s}{(2^a + 1)(2^a - 1)},$$

$$(2^a - 2)2^{2a}(2^a + 1)(2^a - 1) \geqq g(2^{2a+1} - 2^{a+1}s - 2^{a+1}). \tag{13}$$

Combining this with (2), we find

$$2^a - 2 \geqq 2^{a+1} - 2s - 2, \qquad 2s \geqq 2^a.$$

On the other hand, by (11) and (10)

$$s = \sum_{j=1}^{r} z_j \leqq \sum_{j=1}^{r} z_j^2 = 2^a - s, \tag{14}$$

whence $2s \leqq 2^a$. It follows that $2s = 2^a$; moreover, in (13) and (14) the equality sign must hold. This implies that $g = (2^a + 1)2^a(2^a - 1)$, that $z_1 = z_2 = \cdots = z_r = 1$, and, finally, that $r = s$. This yields the results

(III.D) $\mathfrak{G}$ *has the order* $g = (2^a + 1)2^a(2^a - 1)$.

(III.E) $\mathfrak{G}$ *has exactly* $2^{a-1} - 1$ *degrees* $2^a + 1$, *and* 2^{a-1} *degrees* $2^a - 1$, *and one degree* 1. *All other degrees are* 2^a.

It remains to find the number of degrees 2^a. Combining (4) with the value of g, and the equation $t = k$, we have $(k - 1)2^a - 1 = (2^a - 1)(2^a + 1)$, whence $k - 1 = 2^a$. Since we have 2^a degrees 1, $2^a + 1$, $2^a - 1$, we have exactly one degree 2^a.

(III.E*) *There is exactly one degree* 2^a; $k = 2^a + 1$.

6. The main result

Since $\mathfrak{G}$ has a subgroup $\mathfrak{N}$ of order $(2^a - 1)2^a$, that is, of index $2^a + 1$, it follows that $\mathfrak{G}$ has a transitive representation $\mathfrak{Z}$ by permutations of $2^a + 1$ objects. If the character of $\mathfrak{Z}$ is $\chi_1 + \chi$, then χ is a character of $\mathfrak{G}$ of degree 2^a which no longer contains χ_1. Comparison with (III.E), (III.E*) shows that $\chi = \chi_k$. Since χ_k is irreducible, $\mathfrak{Z}$ is doubly transitive.

If R is an element of $\mathfrak{G}$ whose order is divisible by a prime factor p of $2^a + 1$, then all characters χ_j of degree $2^a + 1$ vanish for R. Likewise, if S is an element of $\mathfrak{G}$ whose order is divisible by a prime factor p' of $2^a - 1$, then $\chi_l(S) = 0$ for all χ_l of degree $2^a - 1$. Thus $\chi_j(R)\chi_j(S) = 0$ for $1 < j < k$. Now the orthogonality relations for group characters yield $\chi_k(R)\chi_k(S) + 1 = 0$. Since χ_k is the only irreducible character of its degree, its values are rational integers. It follows that $\chi_k(R) = \pm 1$, $\chi_k(S) = \mp 1$. Thus $\chi_k(X)$ for $X \neq 1$ is 0, $+1$, or -1, and the character of $\mathfrak{Z}$ for $X \neq 1$ has only the values 1, 2, 0. In particular, the representation $\mathfrak{Z}$ is faithful. Moreover, no $\mathfrak{Z}(X)$ with $X \neq 1$ leaves three objects fixed. It follows that $\mathfrak{Z}$ is triply transitive: The subgroup leaving one letter fixed has order $2^a(2^a - 1)$; the subgroup leaving two letters fixed has order $2^a - 1$; the subgroup leaving three letters fixed has order 1.

Now, Zassenhaus' results apply. It follows that $\mathfrak{G} = LF(2, 2^a)$.

7. Groups $\mathfrak{G}$ which satisfy the assumptions (I), (II), but not the assumption (III)

If $\mathfrak{G}$ satisfies the assumptions (I) and (II), but not the assumption (III), let $\mathfrak{G}_0$ be a seminormal subgroup of $\mathfrak{G}$ of minimal order which includes the 2-Sylow subgroup $\mathfrak{T}$. Then $\mathfrak{G}_0 \neq \mathfrak{G}$. Again $\mathfrak{G}_0$ satisfies the assumptions (I) and (II). If $\mathfrak{G}_0 \neq \mathfrak{T}$, then $\mathfrak{G}_0$ will satisfy the assumptions (I), (II), (III). Hence $\mathfrak{G}_0 = LF(2, 2^a)$.

Let $\mathfrak{G}_1$ be a group which precedes $\mathfrak{G}_0$ in a composition series from $\mathfrak{G}$ to $\mathfrak{G}_0$. Then $\mathfrak{G}_0$ is normal in $\mathfrak{G}_1$. If $T \in \mathfrak{T}$, $T \neq 1$, and if $X \in \mathfrak{G}_1$, then $X^{-1}TX$ is an

involution of $\mathfrak{G}_0$ and hence conjugate to T in $\mathfrak{G}_0$. Thus $X^{-1}TX = Y^{-1}TY$ with $Y \in \mathfrak{G}_0$. It follows that $XY^{-1} \in \mathfrak{C}(T)$. Since $c(T) = 2^a$, $\mathfrak{C}(T) = \mathfrak{T}$, and we find $X \in \mathfrak{T}Y \subseteq \mathfrak{G}_0$. Hence $\mathfrak{G}_1 = \mathfrak{G}_0$, a contradiction.

Thus, $\mathfrak{G}_0 = \mathfrak{T}$. Suppose

$$\mathfrak{G} \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{H}_r = \mathfrak{T}$$

is a composition series from $\mathfrak{G}$ to $\mathfrak{T}$. Suppose we know already that $\mathfrak{T}$ is normal in $\mathfrak{H}_l$ for some l. Then $\mathfrak{T}$ is characteristic in $\mathfrak{H}_l$ and hence normal in $\mathfrak{H}_{l-1}$. This shows that $\mathfrak{T}$ is normal in $\mathfrak{G}$,

$$\mathfrak{G} = \mathfrak{N}(\mathfrak{T}).$$

Since $\mathfrak{N}(\mathfrak{T})/\mathfrak{C}(\mathfrak{T})$ is isomorphic with a subgroup $\mathfrak{M}$ of $LH(a, 2)$ in the usual manner, we have here $\mathfrak{G}/\mathfrak{T} \cong \mathfrak{M}$. In our case, no element $M \neq 1$ of $\mathfrak{M}$ has a fixed point. Also, $\mathfrak{M}$ has odd order. It follows that all Sylow subgroups of $\mathfrak{M}$ are cyclic, and this implies that $\mathfrak{M}$ is soluble. Hence $\mathfrak{G}$ is soluble too. Thus, we have

(III.F) *Let $\mathfrak{G}$ satisfy the assumptions*: (I) *$\mathfrak{G}$ is of type (S).* (II) *The 2-Sylow subgroup $\mathfrak{T}$ of $\mathfrak{G}$ is abelian of type $(2, 2, \cdots, 2)$, order $2^a \geqq 4$. For $a = 2$ assume also that $\mathfrak{C}(T) = \mathfrak{T}$ for $T \in \mathfrak{T}$, $T \neq 1$.*

If $\mathfrak{G}$ does not satisfy the assumption (III), *then $\mathfrak{T}$ is normal in $\mathfrak{G}$, and $\mathfrak{G}$ is soluble.*

References

1. R. Brauer and K. A. Fowler, *On groups of even order*, Ann. of Math. (2), vol. 62 (1955), pp. 565–583.
2. H. Zassenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg, vol. 11 (1936), pp. 17–40.

Harvard University
Cambridge, Massachusetts
University of Illinois
Urbana, Illinois
University of Sydney
Sydney, Australia