A CHARACTERIZATION OF THE MATHIEU GROUP $\mathfrak{M}_{12}$

BY

RICHARD BRAUER AND PAUL FONG [1]

In this paper we give a characterization of the simple Mathieu group $\mathfrak{M}_{12}$ of order 95,040. The character table of $\mathfrak{M}_{12}$ was computed by Frobenius [6], and from his results it can be immediately seen that there exists an element F in $\mathfrak{M}_{12}$ of order 8 such that (i) the cyclic subgroup $\langle F\rangle$ generated by F is self-centralizing, (ii) F is conjugate to its odd powers. Elementary arguments show that there is then a Sylow 2-subgroup $\mathfrak{P}$ of $\mathfrak{M}_{12}$, of order 64, such that (i), (ii) hold in $\mathfrak{P}$. We are thus led to a consideration of 2-groups $\mathfrak{P}$ of order 64 in which (i), (ii) hold, and groups $\mathfrak{G}$ containing $\mathfrak{P}$ as a Sylow 2-subgroup. Our main result is the following:

THEOREM (6A). *Let $\mathfrak{G}$ be a finite group of order $64g'$, where g' is odd. Suppose there is an element F of order 8 in $\mathfrak{G}$ such that $\langle F\rangle$ is self-centralizing in some Sylow 2-subgroup $\mathfrak{P}$, and F is conjugate to its odd powers in $\mathfrak{P}$. Then one of the following possibilities hold*:

(a) *$\mathfrak{G}$ has a subgroup of index 2.*

(b) *$\mathfrak{G}$ has one class of involutions.*

(c) *If $O_{2'}(\mathfrak{G})$ is the maximal normal subgroup of $\mathfrak{G}$ of odd order, then $\mathfrak{G}/O_{2'}(\mathfrak{G}) \simeq \mathfrak{G}_{1344}$ or $\mathfrak{M}_{12}$, where $\mathfrak{G}_{1344}$ is a uniquely determined nonsimple, nonsolvable group of order 1344, and $\mathfrak{M}_{12}$ is the Mathieu group on 12 symbols.*

In particular, the only simple group with more than one class of involutions satisfying the assumptions of the theorem is $\mathfrak{M}_{12}$. A recent characterization of $\mathfrak{M}_{12}$ by Wong [11], where additional assumptions on the centralizer of a center involution were made, is included in the above result.

In §1, 2-groups $\mathfrak{P}$ in which (i), (ii) hold are investigated. It will be shown in §2 that if such a group $\mathfrak{P}$ is a Sylow subgroup of a group $\mathfrak{G}$ with no subgroups of index 2, then the structure of $\mathfrak{P}$ is completely determined. The possible distributions of the involutions of $\mathfrak{P}$ into the conjugate classes of $\mathfrak{G}$ fall essentially into three cases I, II, III. In I, $\mathfrak{G}$ has one class of involutions; in II, III $\mathfrak{G}$ has two classes of involutions. The §§4–6 are largely concerned with cases II, III, which

Received by the editors February 15, 1965.

(1) This research was partially supported by the Air Force contract AF 49 (638)-1381, and by the National Science Foundation contract NSF GP-1610. We would like to thank the referee for his careful reading of the manuscript and for his valuable suggestions.

correspond to part (c) of the above theorem. Case I is incomplete as yet, but we hope to continue the work later on.

NOTATION. All groups $\mathfrak{G}$ considered are finite. If $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$, we write $\mathfrak{H} \leqq \mathfrak{G}$; in case $\mathfrak{H}$ is normal in $\mathfrak{G}$, we write $\mathfrak{H} \trianglelefteq \mathfrak{G}$. If $\mathfrak{A}$ is a subset of $\mathfrak{G}$, then $\mathfrak{N}(\mathfrak{A})$ and $\mathfrak{C}(\mathfrak{A})$ are the normalizer and centralizer of $\mathfrak{A}$ in $\mathfrak{G}$; their orders are respectively $n(\mathfrak{A})$ and $c(\mathfrak{A})$. At times it will be necessary to attach a subscript $\mathfrak{G}$ to $\mathfrak{N}_{\mathfrak{G}}(\mathfrak{A})$ and $\mathfrak{C}_{\mathfrak{G}}(\mathfrak{A})$ when $\mathfrak{A}$ is contained in several groups. The subgroup of $\mathfrak{G}$ generated by $\mathfrak{A}$ will be denoted by $\langle\mathfrak{A}\rangle$. If $\mathfrak{A}$ consists of only one element A, we will write A for $\mathfrak{A}$.

Let p be a fixed rational prime; v will then be the exponential valuation of the rational numbers determined by p, normalized by setting $v(p) = 1$. If $G \in \mathfrak{G}$, we will write $v(G)$ for $v(c(G))$. G is a p-element, a p-regular element, or a p-singular element if G has order a power of p, relatively prime to p, or divisible by p respectively. Each $G \in \mathfrak{G}$ is a unique product $G = G_1G_2$, where G_1 is a p-element, G_2 is p-regular, and each G_i is a power of G. G_1 is called the p-factor of G, G_2 the p-regular or p'-factor of G. If P is a p-element, then the section $S(P)$ of P is the set $\{G \in \mathfrak{G} \mid p\text{-factor of } G \text{ is conjugate to } P \text{ in } \mathfrak{G}\}$. An S_p-subgroup of $\mathfrak{G}$ is a Sylow p-subgroup of $\mathfrak{G}$.

If $\mathfrak{P}$ is an S_p-subgroup of $\mathfrak{G}$, we will denote the $\mathfrak{P}$-conjugate classes by ccl(P), where P is a representative of the class. At times all the elements of the class will be displayed between the parenthesis signs. If two classes of $\mathfrak{P}$ are conjugate in $\mathfrak{G}$, we will say they are fused in $\mathfrak{G}$. A class of $\mathfrak{P}$ which is not fused to any other $\mathfrak{P}$-class is said to be isolated. The symbol $\sim$ will mean conjugate to. The transform of A by G is $G^{-1}AG = A^G$; we write $G\colon A \to G^{-1}AG$.

1. Let $\mathfrak{P}$ be a 2-group of order 64 satisfying the following condition: There exists a self-centralizing element F of order 8 which is conjugate in $\mathfrak{P}$ to its odd powers, i.e.

(i) $\mathfrak{C}(F) = \langle F\rangle$,

(ii) $F \sim F^3 \sim F^5 \sim F^7$.

The determination of the structure of $\mathfrak{P}$ will proceed in several steps.

(a) Let $\mathfrak{N}$ be the normalizer of $\langle F\rangle$. By conditions (i), (ii) $\mathfrak{N}$ has order 32, and hence $\mathfrak{N} \trianglelefteq \mathfrak{P}$. Moreover, $\mathfrak{N}/\langle F\rangle$ is abelian of type $(2,2)$, since the automorphism group of Z_8 is noncyclic.

(b) Let the class of F be ccl$(F,F^3,F^5,F^7,F_1,F_1^3,F_1^5,F_1^7)$. $\mathfrak{P}$ permutes by transformation the elements of ccl(F) among themselves. In particular $F_1^{-1}FF_1 \in \text{ccl}(F)$. Condition (i) implies $F_1^{-1}FF_1 = F^\alpha$ for some α. Thus $F_1 \in \mathfrak{N}$ and $F_1^2 \in \langle F\rangle$. Replacing F_1 by F_1^3 if necessary, we may assume that $F_1^2 = F^2$. Let $\mathfrak{F} = \langle F, F_1\rangle$; $\mathfrak{F}$ has order 16, and at least 8 elements of order 8. A check of the groups of order 16, which are completely known, shows that we may take $\alpha = 5$. If we set $X = F_1F$, then $\mathfrak{F}$ is the group $\langle X, F \mid X^2 = F^8 = 1, XFX = F^5\rangle$. The class ccl($F$) can then be written as ccl$(F,F^3,F^5,F^7,XF,XF^3,XF^5,XF^7)$.

The center of $\mathfrak{F}$ is $\langle F^2\rangle$; for notational convenience, set $J = F^4$. Since $\mathfrak{F}$ is generated by ccl(F), $\mathfrak{F} \trianglelefteq \mathfrak{P}$. It is easily seen that the conjugate classes of $\mathfrak{P}$ in $\mathfrak{F}$ are

$$\mathrm{ccl}(F),\ \mathrm{ccl}(F^2,F^{-2}),\ \mathrm{ccl}(J),\ \mathrm{ccl}(1),\ \mathrm{ccl}(XF^2,XF^{-2}),\ \mathrm{ccl}(X,XJ).$$

(c) For any $P\in\mathfrak{P}$, $P:F\to\mathrm{ccl}(F)$, $X\to\mathrm{ccl}(X)$. Since there are 8 possible images for F and 2 for X, there are in all 16 possible actions for P. If $P:F\to F$, $X\to X$, then P centralizes $\mathfrak{F}$, and hence belongs to the center $\mathfrak{Z}\mathfrak{F}$ of $\mathfrak{F}$. A comparison of the orders of $\mathfrak{P}$ and $\mathfrak{Z}\mathfrak{F}$ implies that all 16 possibilities occur. In particular, there exist elements N and E in $\mathfrak{P}$ such that

$$N:\begin{array}{l} F\to F^{-1},\\ X\to X, \end{array}\qquad E:\begin{array}{l} F\to XF,\\ X\to XJ. \end{array} \tag{1.1}$$

$N\in\mathfrak{N}$, so that $\mathfrak{N}=\langle N,X,F\rangle$. However, $E\notin\mathfrak{N}$, and so $\mathfrak{P}=\langle E,N,X,F\rangle = \langle E,N,F\rangle$.

(d) Now $N^2: F\to F$, and thus $N^2\in\langle F\rangle$. Since $N\notin\mathfrak{C}(F^2)$, N^2 must be 1 or J. We write $N^2 = J^\rho$, where $\rho = 0$ or 1. Also $E^2: F\to F^5$, $X\to X$ so that $E^2X\in\mathfrak{C}(\mathfrak{F})$ or $E^2X\in\mathfrak{Z}\mathfrak{F}$. If $E^2X = 1$ or J, then $E\in\mathfrak{C}(X)$, which is not the case. We may thus write $E^2 = XF^2J^\sigma$, where $\sigma = 0$ or 1. To complete the description of $\mathfrak{P}$, it remains to compute $E^{-1}NE$. Now $E^{-1}NE: X\to X$, $F\to F^3$, so that $E^{-1}NE(NX)^{-1}\in\mathfrak{C}(\mathfrak{F})$. Hence $E^{-1}NE = F^{2\tau}NX = NXF^{-2\tau}$. Since we may replace E by F^2E in (1.1), we may assume $\tau = 0$ or 1. We have proved the first part of

PROPOSITION (1A). *Let $\mathfrak{P}$ be a 2-group of order 64 such that there exists a self-centralizing element F of order 8 conjugate in $\mathfrak{P}$ to its odd powers. Set $F^4 = J$. Then $\mathfrak{P}$ has a normal series*

$$\langle F\rangle \trianglelefteq \langle X,F\rangle \trianglelefteq \langle N,X,F\rangle \trianglelefteq \langle E,N,X,F\rangle = \mathfrak{P}$$

where $X^2 = 1$, $XFX = FJ$; $N^2 = J^\rho$, $N^{-1}XN = X$, $N^{-1}FN = F^{-1}$; $E^2 = XF^2J^\sigma$, $E^{-1}NE = NXF^{-2\tau}$, $E^{-1}XE = XJ$, $E^{-1}FE = XF$. Here ρ,σ,τ are 0 or 1. The commutator subgroup $\mathfrak{P}'$ of $\mathfrak{P}$ is $\langle X,F^2\rangle$; $\mathfrak{P}/\mathfrak{P}'$ is of type (2,2,2). The center of $\mathfrak{P}$ is $\langle J\rangle$.

Proof. It is clear from the above relations that $\mathfrak{P}'\geqq\langle X,F^2\rangle$, and that $\langle X,F^2\rangle\trianglelefteq\mathfrak{P}$. Modulo $\langle X,F^2\rangle$ the generators E,N,F of $\mathfrak{P}$ commute and have exponent 2. The assertions about $\mathfrak{P}'$ and $\mathfrak{P}/\mathfrak{P}'$ now follow. $\mathfrak{Z}\mathfrak{P}$ must lie in $\langle F\rangle$. Since $N\notin\mathfrak{C}(F^2)$, $\mathfrak{Z}\mathfrak{P} = \langle J\rangle$. This completes the proof. These groups are incidentally the ones on pp. 222 and 224 of Hall-Senior [7] (2).

(2) These groups were pointed out to us by Professor P. N. Burgoyne.

The following remarks are easy consequences of (1A). Each element of $\mathfrak{P}$ is uniquely expressible in the form $E^iN^jX^kF^m$, where $i,j,k = 0,1$; and $0 \leqq m \leqq 7$. We have

$$(1.2)\quad F\colon \begin{array}{l} E \to EXJ, \\ N \to NF^2, \\ X \to XJ, \end{array} \quad X\colon \begin{array}{l} E \to EJ, \\ N \to N, \\ F \to FJ, \end{array} \quad N\colon \begin{array}{l} E \to EXF^{2\tau}, \\ X \to X, \\ F \to F^{-1}, \end{array} \quad E\colon \begin{array}{l} N \to NXF^{-2\tau}, \\ X \to XJ, \\ F \to XF. \end{array}$$

In particular, the subgroups $\langle E^2, EF\rangle$, $\langle F^2, EF\rangle$ for $\sigma = 1$ and the subgroups $\langle NF, X\rangle = \langle NXF, X\rangle$, $\langle NF^{-1}, X\rangle = \langle NXF^{-1}, X\rangle$ are dihedral of order 8.

For later use it will be necessary to have a complete set of representatives of the conjugate classes of $\mathfrak{P}$, and the centralizers of these representatives. In the tables below the columns contain from left to right (i) a representative of the class, (ii) the elements of the class, (iii) the centralizer of the representative, (iv) the order of the representative, (v) the square of the representative. The calculations for the most part are straightforward; the details are omitted in such cases.

(a) Classes in $\mathfrak{F}$. The results in this case are easily derived from the steps leading up to the proof of (1A).

F	$F^{2i+1}, XF^{2i+1}, 0 \leqq i \leqq 3$	$\langle F\rangle$	8	F^2
F^2	F^2, F^{-2}	$\langle \mathfrak{P}', F, EN\rangle$	4	J
XF^2	XF^2, XF^{-2}	$\langle \mathfrak{P}', E, NF\rangle$	4	J
J	J	$\mathfrak{P}$	2	1
X	X, XJ	$\langle \mathfrak{P}', N, EF\rangle$	2	1
1	1	$\mathfrak{P}$	1	1

(b) Classes in $\mathfrak{N} - \mathfrak{F}$. Under repeated transformations by F and E, we have $N \sim NF^{2i}, N \sim NXF^{2i}, NF \sim NF^{2i+1}, NXF \sim NXF^{2i+1}$ for $0 \leqq i \leqq 3$. Since $\mathfrak{C}(N) \geqq \langle N, X, J\rangle$ has order $\geqq 8$, the class ccl(N) contains exactly 8 elements. If $\tau = 0$, $\mathfrak{C}(NF) \geqq \langle E\rangle\langle NF\rangle, \mathfrak{C}(NXF) \geqq \langle EX\rangle\langle NXF\rangle$; both centralizers have order $\geqq 16$. If $\tau = 1$, $\mathfrak{C}(NF) \geqq \langle E^2, EF\rangle\langle NF\rangle$, $\mathfrak{C}(NXF) \geqq \langle E^2, EF\rangle\langle NXF\rangle$ also have order $\geqq 16$. The classes of NF, NXF therefore each contain exactly 4 elements.

N	$NF^{2i}, NXF^{2i}, 0 \leqq i \leqq 3$	$\langle N, X, J\rangle$	$2^{1+\rho}$	J^ρ
NF	NF, NF^3, NF^5, NF^7	$\langle E\rangle\langle NF\rangle$ if $\tau = 0$, $\langle E^2, EF\rangle\langle NF\rangle$ if $\tau = 1$	$2^{1+\rho}$	J^ρ
NXF	NXF, NXF^3, NXF^5, NXF^7	$\langle EX\rangle\langle NXF\rangle$ if $\tau = 0$ $\langle E^2, EF\rangle\langle NXF\rangle$ if $\tau = 1$	$2^{2-\rho}$	$J^{1+\rho}$

(c) Classes in $\mathfrak{P} - \mathfrak{N}$. Under repeated transformations by F, we have $E \sim EX \sim EJ \sim EXJ$, $EF^2 \sim EXF^2 \sim EXF^{-2} \sim EF^{-2}$, $EF \sim EXF \sim EXF^5 \sim EF^5$, $EF^3 \sim EXF^3 \sim EXF^{-1} \sim EF^{-1}$. If $\tau = 0$ we may use the results on $\mathfrak{C}(NF)$ and the fact that $EXF^2 = E^3$ or E^{-1} to conclude that $\mathfrak{C}(E) = \mathfrak{C}(EXF^2) \geqq \langle E\rangle\langle NF\rangle$, the latter being a subgroup of order 16. The classes $\mathrm{ccl}(E)$, $\mathrm{ccl}(EXF^2)$ then each have exactly 4 elements. If $\tau = 0$, $N: EF \to EXF^{-1}$; $\mathrm{ccl}(EF)$ then has exactly 8 elements, since $\mathfrak{C}(EF) \geqq \langle EF, X, J\rangle$. If $\tau = 1$, $N: E \to EXF^2$ and $\mathrm{ccl}(E)$ has exactly 8 elements. Note that E is then a self-centralizing element of order 8 con-ugate to its odd powers. If $\tau = 1$, then $\mathfrak{C}(EF) \geqq \langle EF\rangle\langle X, NF\rangle$, $\mathfrak{C}(EF^3) \geqq \langle EF^3\rangle\langle X, NF^{-1}\rangle$, both centralizers then having order $\geqq 16$. The classes $\mathrm{ccl}(EF), \mathrm{ccl}(EF^3)$ each contain exactly 4 elements.

E	E, EX, EXJ, EJ	$\langle E\rangle\langle NF\rangle$	8	E^2	
EXF^2	$EF^2, EXF^2, EXF^{-2}, EF^{-2}$	$\langle E\rangle\langle NF\rangle$	8	E^{-2}	$\tau = 0$,
EF	$EF^{2i+1}, EXF^{2i+1}, 0 \leqq i \leqq 3$	$\langle EF\rangle\langle X, J\rangle$	$2^{2-\sigma}$	$J^{1-\sigma}$	
E	EF^{2i}, EXF^{2i}, $0 \leqq i \leqq 3$	$\langle E\rangle$	8	E^2	
EF	EF, EXF, EXF^5, EF^5	$\langle EF\rangle\langle X, NF\rangle$	$2^{2-\sigma}$	$J^{1-\sigma}$	$\tau = 1$·
EF^3	$EF^3, EXF^3, EXF^{-1}, EF^{-1}$	$\langle EF^3\rangle\langle X, NF^{-1}\rangle$	$2^{2-\sigma}$	$J^{1-\sigma}$	

Under repeated transformations by F and X, we have $EN \sim ENJ \sim ENXF^2 \sim ENXF^{-2}$, $ENF^2 \sim ENF^{-2} \sim ENX \sim ENXJ$. If $\tau = 0$, then N: $EN \to ENX$; since EN has order 8, $\mathrm{ccl}(EN)$ has exactly 8 elements. If $\tau = 1$, then $\mathfrak{C}(EN) \geqq \langle EN\rangle\langle F^2, EF\rangle$, $\mathfrak{C}(ENX) \geqq \langle ENX\rangle\langle F^2, EF\rangle$; both centralizers have order $\geqq 16$, so that $\mathrm{ccl}(EN)$, $\mathrm{ccl}(ENX)$ each contain exactly 4 elements. Finally, if $\tau = 0$, ENF, ENF^{-1}, ENF^3 have order 8. Since N: $ENF \to ENXF^{-1}$, and $\mathfrak{C}(ENF) \geqq \langle E, X, NF\rangle$ has order $\geqq 32$, $\mathrm{ccl}(ENF)$ has just 2 elements. Multiplication by J yields another class $ENF^5 \sim ENXF^3$. Transformation of ENF^3 by E, N, F respectively yield ENF^{-1}, $ENXF^{-3}$, $ENXF$. Since $\mathfrak{C}(ENF^3) \geqq \langle ENF^3\rangle\langle X\rangle$, $\mathrm{ccl}(ENF^3)$ has exactly 4 elements. If $\tau = 1$, transformation of ENF by E, N, F respectively give ENF^{-1}, $ENXF^{-3}$, $ENXF^{-1}$, and since $\mathfrak{C}(ENF) \geqq \langle \mathfrak{P}', ENF\rangle$, ccl (ENF) has exactly 4 elements. Multiplication by yields the remaining class.

EN	$ENF^{2i}, ENXF^{2i}, 0 \leqq i \leqq 3$	$\langle EN\rangle$	8	$F^{\pm 2}$	
ENF	$ENF, ENXF^{-1}$	$\langle E, X, NF\rangle$	8	$XF^{\pm 2}$	$\tau = 0$,
ENF^{-3}	$ENF^{-3}, ENXF^3$	$\langle E, X, NF\rangle$	8	$XF^{\pm 2}$	
ENF^3	$ENF^3, ENF^{-1}, ENXF^{-3}, ENXF$	$\langle ENF^3\rangle\langle X\rangle$	8	$XF^{\pm 2}$	
EN	$EN, ENJ, ENXF^2, ENXF^{-2}$	$\langle EN\rangle\langle F^2, EF\rangle$	$3 + (-1)^{\rho+\sigma}$	$J^{1+\rho+\sigma}$	
ENX	$ENX, ENXJ, EN^2F, ENF^{-2}$	$\langle ENX\rangle\langle F^2, EF\rangle$	$3 - (-1)^{\rho+\sigma}$	$J^{\rho+\sigma}$	
ENF	$ENF, ENF^{-1}, ENXF^{-3}, ENXF^{-1}$	$\langle \mathfrak{P}', ENF\rangle$	4	$XJ^{1+\rho+\sigma}$	$\tau = 1$.
ENF^3	$ENF^3, ENF^{-3}, ENXF, ENXF^3$	$\langle \mathfrak{P}', ENF\rangle$	4	$XJ^{\rho+\sigma}$	

2. Let $\mathfrak{P} = \mathfrak{P}(\rho, \sigma, \tau)$ be the group of order 64 considered in §1. We assume in this section that $\mathfrak{P}$ is a Sylow subgroup of a larger group $\mathfrak{G}$. Let $\mathfrak{P}^{\#}$ be the focal subgroup of $\mathfrak{P}$ in $\mathfrak{G}$, i.e. $\mathfrak{P}^{\#}\langle QP^{-1} \,|\, Q = P \in \mathfrak{P}$ and $Q \sim P$ in $\mathfrak{G}\rangle$. The S_2-subgroup of $\mathfrak{G}/\mathfrak{G}'$ is then isomorphic to $\mathfrak{P}/\mathfrak{P}^{\#}$ by [1], Theorem 8.

LEMMA (2A). *$E^2 \nsim F^2$ in $\mathfrak{G}$.*

Proof. Suppose $E^2 \sim F^2$ in $\mathfrak{G}$. Since $\langle E^2\rangle$ and $\langle F^2\rangle$ are normal in $\mathfrak{P}$, there exists by Burnside's theorem [12, Lemma, p. 139] a $G \in \mathfrak{N}(\mathfrak{P})$ such that G: $\langle E^2\rangle \to \langle F^2\rangle$; since $F^2 \sim F^{-2}$ in $\mathfrak{P}$ we may assume that G: $E^2 \to F^2$, and that G has odd order. G then permutes the four self-centralizing cyclic subgroups of $\mathfrak{P}$ of order 8, $\langle F\rangle, \langle XF\rangle, \langle EN\rangle, \langle ENX\rangle$ if $\tau = 0$; $\langle F\rangle, \langle XF\rangle, \langle E\rangle, \langle EF^2\rangle$ if $\tau = 1$. Hence G fixes one of these subgroups, and then G would fix E^2 or F^2, which is impossible. Thus $E^2 \nsim F^2$ in $\mathfrak{G}$.

LEMMA (2B). *Suppose $Y \sim Z$, where Y, Z are elements of order 2 or 4 in $\mathfrak{P}$, and $vc_{\mathfrak{P}}(Y) = 3$, $vc_{\mathfrak{P}}(Z) = 5$. Then $\mathrm{ccl}(J)$ is not isolated.*

Proof. The assumptions imply that $Y \in \mathrm{ccl}(N)$ or $\mathrm{ccl}(EF)$ if $\tau = 0$, $Y \in \mathrm{ccl}(N)$ if $\tau = 1$. Suppose $\mathrm{ccl}(J)$ is isolated. Let $\mathfrak{C}^0(Y) = \langle T \in \mathfrak{C}(J) \,|\, T: Y \to Y$ or $YJ\rangle$, and let $\mathfrak{L} = \mathfrak{C}^0_{\mathfrak{P}}(Y) = \mathfrak{C}^0(Y) \cap \mathfrak{P}$. $\mathfrak{L} = \langle \mathfrak{P}', N\rangle$ or $\langle \mathfrak{P}', EF\rangle$ according as $Y = N$ or $Y = EF$; thus $\mathfrak{L} \trianglelefteq \mathfrak{P}$. Since $\mathrm{ccl}(J)$ is isolated, $Y \sim Z$ in $\mathfrak{C}(J)$. In particular, there exists $G \in \mathfrak{C}(J)$ such that G: $Y \to Z$, and we may assume G: $\mathfrak{C}^0(Y) \to \mathfrak{C}^0(Z)$. Let $\mathfrak{P}_1$ be an S_2-subgroup of $\mathfrak{C}^0(Y)$ containing $\mathfrak{L}$; $\mathfrak{P}_1$ is then a Sylow subgroup of $\mathfrak{G}$. If $\mathfrak{L} \trianglelefteq \mathfrak{P}_1$, then there exists an $H \in \mathfrak{N}(\mathfrak{L})$ such that H: $\mathfrak{P}_1 \to \mathfrak{P}$. If Z_1 is the image of Y under H, then necessarily $vc_{\mathfrak{P}}(Z_1) = 5$ and $Z_1 \in \mathfrak{P}'$. In particular, the images of E^2, F^2 under H are elements of $\mathfrak{L}$ not commuting with Z_1; in other words, they lie in $\mathfrak{L} - \mathfrak{P}' = \mathrm{ccl}(Y)$. But then $E^2 \sim F^2$, which is impossible by (2A). Hence $\mathfrak{L}$ is not a normal subgroup of $\mathfrak{P}_1$. Choose $\mathfrak{W}$ such that $\mathfrak{L} \lhd \mathfrak{W} \lhd \mathfrak{P}_1$, and an S_2-subgroup $\mathfrak{P}_2$ of $\mathfrak{G}$ such that $\mathfrak{W} < \mathfrak{P}_2 \leqq \mathfrak{N}(\mathfrak{L})$. Then there exists an $H \in \mathfrak{N}(\mathfrak{L})$ such that H: $\mathfrak{P} \to \mathfrak{P}_2$. Since H must fix J, there are elements Y_1, Y_2 in $\mathrm{ccl}(Y)$ such that $H: Y_1 \to Y_2$. This implies $vc_{\mathfrak{P}_2}(Y) = 3$. However, $vc_{\mathfrak{P}_2}(Y) \geqq 4$, since $vc_{\mathfrak{P}_1}(Y) = 5$. Thus $\mathrm{ccl}(J)$ is not isolated.

PROPOSITION (2C). *If $\tau = 0$, then $\mathfrak{P}^{\#} < \mathfrak{P}$ and $\mathfrak{G}$ has a subgroup of index 2.*

Proof. From the tables in §1, J is the only involution in $\mathfrak{P}$ which is a square in $\mathfrak{P}$. Suppose $G: Y \to J$ for some $Y \neq J$ in $\mathfrak{P}$ and some G in $\mathfrak{G}$. We may assume $G: \mathfrak{C}_{\mathfrak{P}}(Y) \to \mathfrak{P}$. Let $\mathfrak{P}_1$ be an S_2-subgroup of $\mathfrak{C}(Y)$ containing $\mathfrak{C}_{\mathfrak{P}}(Y)$. For every $T \in \mathfrak{P}_1, T^4 \in \langle Y\rangle$. If $vc_{\mathfrak{P}}(Y) \geqq 4$, we may assume $Y = X$, NF, or NXF; then $ENF \in \mathfrak{C}_{\mathfrak{P}}(Y)$. But this is impossible, since $(ENF)^4 = J$. If $vc_{\mathfrak{P}}(Y) = 3$, we may assume $Y = N$ or EF. If $Y = N$, then G must transform NX into $\mathrm{ccl}(N)$ or $\mathrm{ccl}(EF)$ by what has just been proved. If $G: NX \to \mathrm{ccl}(N)$, then $G: X = N\,(NX) \to J\,\mathrm{ccl}(N) = \mathrm{ccl}(N)$, which is impossible. If $G: NX \to \mathrm{ccl}(EF)$, then $G: X \to J\,\mathrm{ccl}(EF) = \mathrm{ccl}(EF)$, which is also impossible. If $Y = EF$, a similar argument can be applied to EFX. Thus $\mathrm{ccl}(J)$ is isolated.

Let $Y=N$ or EF, and suppose $Y\sim NF$ or $Y\sim NXF$. Then there exists a $G\in\mathfrak{G}$ with $G:Y\to NF$ or NXF, and $G:\mathfrak{C}_{\mathfrak{P}}(Y)\to\mathfrak{C}_{\mathfrak{P}}(NF)$ or $\mathfrak{C}_{\mathfrak{P}}(NXF)$ by (2B). Now $X\in\mathfrak{C}_{\mathfrak{P}}(Y)$; therefore $G:X\to \mathrm{ccl}(NF)$ or $\mathrm{ccl}(NXF)$. But this is impossible by (2B), since it would imply $Y\sim X$. Hence the only possible fusions among elements of order 2 and 4 are between X, NF or $NXF\,|\,N, EF\,|\,E^2, NF$ or $NXF\,|\,F^2, NF$ or NXF. By (2A) the only possible fusions among elements of order 8 are between $F, EN\,|\,E, EF^2, ENF, ENF^{-3}, ENF^3$. These fusions, if they occur, contribute at most $\langle\mathfrak{P}', E, NF\rangle$ to $\mathfrak{P}^{\#}$, and thus $\mathfrak{P}^{\#}<\mathfrak{P}$.

From now on we assume $\tau=1$, since we want to find out which $\mathfrak{P}$ can occur as an S_2-subgroup of a group without subgroups of index 2.

LEMMA (2D). *Suppose $\tau=1$ and* $\mathrm{ccl}(J)$ *is not isolated. Then $\rho=0, \sigma=1$. Moreover $X\sim J$, and after a suitable relabeling of the generators E, N, F, we may assume $E^2\sim ENF^3$, $F^2\sim ENF$, $N\sim EF$.*

Proof. There exists $Y\neq J$ in $\mathfrak{P}$ such that $Y\sim J$ in $\mathfrak{G}$. We first show we may take $Y=X$. Choose $G\in\mathfrak{G}$ such that $G:Y\to J$ and $G:\mathfrak{C}_{\mathfrak{P}}(Y)\to\mathfrak{P}$. If $vc_{\mathfrak{P}}(Y)=4$, then J is a square in $\mathfrak{C}_{\mathfrak{P}}(Y)$. Its image under G is an involution $\neq J$ which is a square in $\mathfrak{P}$. Hence G: $J\to\mathrm{ccl}(X)$ and $X\sim J$. If $Y=N$, and if $G:NX\to\mathrm{ccl}(X)$ or $\mathrm{ccl}(Y_1)$ with $vc_{\mathfrak{P}}(Y_1)=4$, then $X\sim J$. But if $G:NX\to\mathrm{ccl}(N)$, then $G:X=N(NX)\to J\,\mathrm{ccl}(N)=\mathrm{ccl}(N)$. Hence $X\sim J$ in all cases.

Let $\mathfrak{U}=\mathfrak{C}_{\mathfrak{P}}(X)=\langle\mathfrak{P}', EF, N\rangle$, and let $\mathfrak{P}_1$ be an S_2-subgroup of $\mathfrak{C}(X)$ containing $\mathfrak{U}$. Since $\mathfrak{U}\lhd\mathfrak{P}$, $\mathfrak{U}\lhd\mathfrak{P}_1$, there exists $B\in\mathfrak{N}(\mathfrak{U})$ such that $B:\mathfrak{P}\to\mathfrak{P}_1$, B: $J\to X$. Furthermore, B necessarily maps $X\to XJ$, and hence $B:XJ\to J$. We may therefore assume B has order a power of 3, if we only use the properties that $B\in\mathfrak{N}(\mathfrak{U})$, and B: $J\to X\to XJ\to J$ in the remainder of this proof. If $\rho=1$, the 8 elements of $\mathrm{ccl}(N)\subseteq\mathfrak{U}$ are mapped by B onto 8 elements of $\mathfrak{U}$ whose squares are X. Since there are only 4 such elements in $\mathfrak{U}$, ρ must be 0. Similarly, to show $\sigma=1$, the same argument can be applied to the 8 elements of $\mathrm{ccl}(EF)\cup\mathrm{ccl}(EF^3)$. B maps E^2, F^2 onto elements of $\mathfrak{U}$ whose squares are X. Since the map $E\to F$, $F\to E, N\to N$ defines an automorphism of $\mathfrak{P}$, we may assume $F^2\sim ENF$, $E^2\sim ENF^3$. Indeed, if $E^2\sim ENF$, then in the new notation $F^2\sim FNE\sim EFN\sim ENF$. Finally, $B:\mathrm{ccl}(N)\to\mathrm{ccl}(N)\cup\mathrm{ccl}(EF)\cup\mathrm{ccl}(EF^3)$, the latter being a characteristic set of $\mathfrak{U}$. Suppose $B:\mathrm{ccl}(N)\to\mathrm{ccl}(N)$. Since B has order a power of 3, and $\mathrm{ccl}(N)$ has 8 elements, it follows that B fixes at least two elements $N_1\neq N_2$ of $\mathrm{ccl}(N)$. But then B would fix $N_1N_2^{-1}\in\mathfrak{P}'$, which is impossible. Hence $N\sim EF^{\alpha}$ for some $\alpha=1$ or 3. The map $E\to F^3, F\to E, N\to N$ defines an automorphism of $\mathfrak{P}$ which interchanges $\mathrm{ccl}(E)$, $\mathrm{ccl}(F)$, as well as $\mathrm{ccl}(ENF)$, $\mathrm{ccl}(ENF^3)$, so that we may assume $\alpha=1$.

COROLLARY (2E). *Under the assumptions of* (2D) *there is a $B\in\mathfrak{G}$ of order a power of* 3 *such that*

$$B:\ J\to X\to XJ\to J.$$

Moreover, B either fuses ccl(N), ccl(EF), ccl(EF^3) *or B fuses* ccl(N), ccl(EF) *and* B: ccl$(EF^3) \to$ ccl(EF^3). *In either case B maps the union of these three classes onto itself.*

LEMMA (2F). *Suppose $\tau = 1$. Let Y be one of the elements $EN, NF, ENX, NXF, EF, EF^3$; and Z one of the elements X, E^2, F^2. Let $\mathfrak{L} = \langle \mathfrak{P}', EN, NF \rangle$. If $Y \sim Z$ in $\mathfrak{G}$, then there exists a $G \in \mathfrak{G}$ such that $G: J \to J$, $Y \to Z$, and $\mathfrak{C}_{\mathfrak{P}}(Y) \to \mathfrak{L} \cap \mathfrak{C}_{\mathfrak{P}}(Z)$.*

Proof. We first show that $Y \sim Z$ in $\mathfrak{C}(J)$. If Y, Z have order 4, then $Y^2 = Z^2 = J$, and this is clear. Suppose then that $Z = X$. Let $\mathfrak{P}_1$ be an S_2-subgroup of $\mathfrak{C}(X)$ such that $\mathfrak{P}_1 \geqq \mathfrak{C}_{\mathfrak{P}}(X)$. Then X, XJ, J are the only involutions in $\mathfrak{P}_1$ which are squares of elements in $\mathfrak{P}_1$, since they are already squares of elements in $\mathfrak{C}_{\mathfrak{P}}(X)$. Now there exists $A \in \mathfrak{G}$ such that $A: \mathfrak{C}_{\mathfrak{P}}(Y) \to \mathfrak{P}_1$, and $A: Y \to X$. Since J is a square in $\mathfrak{C}_{\mathfrak{P}}(Y)$, A: $J \to J$ or XJ. If A: $J \to J$, then $Y \sim X$ in $\mathfrak{C}(J)$. If A: $J \to XJ$, then ccl(J) is not isolated. If B is the element of (2E), then AB: $J \to J$, $Y \to XJ$, and $Y \sim X$ in $\mathfrak{C}(J)$. Thus in all cases, $Y \sim Z$ in $\mathfrak{C}(J)$.

Let $\mathfrak{C}^0(Y) = \langle T \in \mathfrak{C}(J) \mid T: Y \to Y \text{ or } YJ \rangle$. $\mathfrak{L}$ is then $\mathfrak{C}^0(Y) \cap \mathfrak{P}$ and $\mathfrak{L} \lhd \mathfrak{P}$. Let $\mathfrak{P}_1$ be an S_2-subgroup of $\mathfrak{C}^0(Y)$ containing $\mathfrak{L}$. By the above, $(\mathfrak{P}_1 : \mathfrak{L}) = 2$ and $\mathfrak{L} \lhd \mathfrak{P}_1$. Let $G \in \mathfrak{N}(\mathfrak{L})$ such that G: $\mathfrak{P}_1 \to \mathfrak{P}$. G fixes J, since J is the only involution in $\mathfrak{L}$ which is a square in $\mathfrak{L}$. The image of Y under G has a centralizer in $\mathfrak{P}$ of order 32, and hence belongs to one of the classes ccl(X), ccl(E^2), ccl(F^2). Since no two of these classes can be fused in $\mathfrak{G}$, we may assume $G: Y \to Z$. In particular, $G: \mathfrak{C}_{\mathfrak{P}}(Y) \to \mathfrak{C}_{\mathfrak{P}}(Z) \cap \mathfrak{L}$.

In the table below the entry in the T_i-row and T_j-column is the number of elements in $\mathfrak{C}_{\mathfrak{P}}(T_i) \cap \text{ccl}(T_j)$. The union of the classes indexing the columns is $\mathfrak{L}$.

(2.1)

	1	J	X	NF	NXF	EN	ENX	EF	EF^3	E^2	F^2
NF	1	1	0	2	2	4	0	2	2	2	0
NXF	1	1	0	2	2	0	4	2	2	2	0
EN	1	1	0	4	0	2	2	2	2	0	2
ENX	1	1	0	0	4	2	2	2	2	0	2
EF	1	1	2	2	2	2	2	4	0	0	0
EF^3	1	1	2	2	2	2	2	0	4	0	0
X	1	1	2	0	0	0	0	4	4	2	2
E^2	1	1	2	4	4	0	0	0	0	2	2
F^2	1	1	2	0	0	4	4	0	0	2	2

PROPOSITION (2G). *Suppose $\tau = 1$. If* ccl(J) *is isolated in $\mathfrak{G}$, then $\mathfrak{P}^{\#} < \mathfrak{P}$.*

Proof. (a) Suppose ccl(N) is isolated. The only possible fusions are between $ENF, ENF^3 \mid X, E^2, F^2, NF, NXF, EN, ENX, EF, EF^3$. In this case

$$\mathfrak{P}^{\#} \leqq \langle \mathfrak{P}', EN, NF \rangle < \mathfrak{P},$$

and we are done. Thus we may assume ccl(N) is not isolated.

(b) Suppose $\mathrm{ccl}(X)$ is isolated. Let Y be one of EN, NF, ENX, NXF. If $G: N \to Y$ we may assume $G: \mathfrak{C}_{\mathfrak{P}}(N) \to \mathfrak{C}_{\mathfrak{P}}(Y)$. In particular the image of X under G is not in $\mathrm{ccl}(X)$, since $\mathfrak{C}_{\mathfrak{P}}(Y) \cap \mathrm{ccl}(X) = \varnothing$, and this is impossible. By (2F), (2.1) $Y \nsim E^2$, $Y \nsim F^2$, since either fusion implies that $\mathrm{ccl}(X)$ is not isolated. Hence $vc(Y) = 4$; by (2F), (2.1) it also follows that $Y \nsim EF$, $Y \nsim EF^3$. (The results of (2F) and (2.1) are valid in case $vc(Y) = 4$.) Also $N \nsim E^2$, $N \nsim F^2$ by (2B). The only possible fusions in $\mathfrak{G}$ are between $N, EF, EF^3 \mid NF, NXF, EN, ENX \mid ENF, ENF^3$. But then $\mathfrak{P}^\# \leqq \langle \mathfrak{P}', ENF, N, EF \rangle < \mathfrak{P}$ and we are done. Thus we may assume $\mathrm{ccl}(X)$ is not isolated.

(c) Suppose $\sigma = 0$. Then N, NF, ENX have order $2^{\rho+1}$; EN, NXF have order $2^{2-\rho}$; EF, EF^3 have order 4. By (a) and (2B), $N \sim Y$ for some $Y \in \mathfrak{P}$ with $vc_{\mathfrak{P}}(Y) = vc(Y) = 4$. Let $G \in \mathfrak{G}$ such that $G: N \to Y$ and $G: \mathfrak{C}_{\mathfrak{P}}(N) \to \mathfrak{C}_{\mathfrak{P}}(Y)$. Now $\mathfrak{C}_{\mathfrak{P}}(N) \cap \mathrm{ccl}(N) = \{N, NJ, NX, NXJ\}$; but $\mathfrak{C}_{\mathfrak{P}}(Y) \cap (\mathrm{ccl}(NF) \cup \mathrm{ccl}(ENX))$ has only 2 elements by (2.1). Hence G necessarily fuses $\mathrm{ccl}(N)$ with $\mathrm{ccl}(EF^\alpha)$ for some $\alpha = 1$ or 3. In other words, we may assume $Y = EF^\alpha$. In particular, $\rho = 1$, and N, NF, ENX have order 4. If $\mathfrak{C}^0_{\mathfrak{P}}(N) = \langle T \in \mathfrak{P} \mid T: N \to N \text{ or } NJ \rangle$, we may further assume $G: \mathfrak{C}^0_{\mathfrak{P}}(N) \to \mathfrak{C}^0_{\mathfrak{P}}(EF^\alpha) = \mathfrak{L}$, $\mathfrak{L}$ as in (2F). By (2F), (2.1) the 4 elements of $\mathrm{ccl}(N)$ in $\mathfrak{C}^0_{\mathfrak{P}}(N) - \mathfrak{C}_{\mathfrak{P}}(N)$ are mapped by G into

$$(\mathrm{ccl}(EF^\beta) \cup \mathrm{ccl}(NF) \cup \mathrm{ccl}(ENX)) \cap (\mathfrak{C}^0_{\mathfrak{P}}(EF^\alpha) - \mathfrak{C}_{\mathfrak{P}}(EF^\alpha)),$$

where $\beta = 1$ or 3, $\beta \neq \alpha$. Thus $N \sim EF \sim EF^3$ or $N \sim EF^\alpha \sim NF \sim ENX$ by (2.1). Suppose we have the latter case. Then $EF^\alpha \sim NF$ implies by (2F), (2.1) that E^2 is fused to one of NF, ENX or EF^α and hence $N \sim E^2$, which is impossible by (2B). Suppose we have the first case $N \sim EF \sim EF^3$. By (b) $\mathrm{ccl}(X)$ is not isolated and hence $X \sim EN$ or $X \sim NXF$. If $X \sim EN$, then by (2F), (2.1) and (2A), $NF \sim EF \sim EF^3 \sim N$, and necessarily $ENX \sim E^2$. The fusions introduced are $X \sim EN$, $N \sim EF \sim EF^3 \sim NF$, $E^2 \sim ENX$. Similarly, if $X \sim NXF$, then $X \sim NXF$, $N \sim EF \sim EF^3 \sim ENX$, $F^2 \sim NF$. Thus $X \sim EN$ or $X \sim NXF$, but not both. The only other possible fusions are $ENF \sim ENF^3$. In all cases, $\mathfrak{P}^\# \leqq \langle \mathfrak{P}', EN, F \rangle$ or $\mathfrak{P}^\# \leqq \langle \mathfrak{P}', NF, E \rangle$, and so $\mathfrak{P}^\# < \mathfrak{P}$.

(d) Suppose $\sigma = 1$. Then N, EN, NF have order $2^{\rho+1}$; NXF, ENX have order $2^{2-\rho}$; EF, EF^3 have order 2. By (a) and (2B), $N \sim Y$ for some $Y \in \mathfrak{P}$ with $vc_{\mathfrak{P}}(Y) = vc(Y) = 4$. We may assume $Y = EN$, NF, or EF^α for some $\alpha = 1$ or 3. Let $G \in \mathfrak{G}$ such that $G: N \to Y$ and $\mathfrak{C}_{\mathfrak{P}}(N) \to \mathfrak{C}_{\mathfrak{P}}(Y)$. If $\mathfrak{C}^0_{\mathfrak{P}}(N) = \langle T \in \mathfrak{P} \mid T: N \to N \text{ or } NJ \rangle$, we may further assume $G: \mathfrak{C}^0_{\mathfrak{P}}(N) \to \mathfrak{C}^0_{\mathfrak{P}}(Y) = \mathfrak{L}$, $\mathfrak{L}$ as in (2F). The 4 elements of $\mathrm{ccl}(N)$ in $\mathfrak{C}^0_{\mathfrak{P}}(N) - \mathfrak{C}_{\mathfrak{P}}(N)$ are mapped into $\mathfrak{L} - \mathfrak{C}_{\mathfrak{P}}(Y)$; hence if $Y = EN$ or NF, then $N \sim EF^\alpha$. Therefore $N \sim EF^\alpha$ for some $\alpha = 1$ or 3 and $\rho = 0$. In particular, it follows that $E^2 \nsim NXF$, $F^2 \nsim ENX$, $ENX \nsim NXF$. Indeed, if any of these were not the case, then by (2F), (2.1) $E^2 \sim F^2$ which is impossible by (2A). By (b) $\mathrm{ccl}(X)$ is not isolated. If $X \sim NF$, then $F^2 \sim NXF$, $EN \sim EF \sim EF^3$ by (2F), (2.1). The only possible fusions in $\mathfrak{G}$ are $X \sim NF$, $EN \sim EF \sim EF^3 \sim N$, $ENF \sim ENF^3$, $F^2 \sim NXF$, $E^2 \sim ENX$. If $E^2 \sim ENX$

occurred, then by (2F), (2.1) NF would be fused to one of EN, EF, EF^3, and hence $X \sim N$, which is impossible by (2B). Computing $\mathfrak{P}^{\#}$, we have $\mathfrak{P}^{\#} \leqq \langle \mathfrak{P}', E, NF \rangle < \mathfrak{P}$, and we are done. If $X \sim EN$, then by a similar argument, the only possible fusions are $X \sim EN$, $NF \sim EF \sim EF^3 \sim N$, $ENF \sim ENF^3$ $E^2 \sim ENX$, and $\mathfrak{P}^{\#} \leqq \langle \mathfrak{P}', EN, F \rangle < \mathfrak{P}$. We may finally suppose $X \sim EF^{\beta}$, $\beta = 1$ or 3, $\beta \neq \alpha$. By (2F), (2.1) we then have $E^2 \sim ENX$, $F^2 \sim NXF$, $NF \sim EN \sim EF^{\alpha} \sim N$, $X \sim EF^{\beta}$.

(e) Since $N \sim NF^2 \sim EN$, there exist $G_1, G_2 \in \mathfrak{G}$ such that $G_1 : N \to EN$, $\mathfrak{C}_{\mathfrak{P}}(N) \to \mathfrak{C}_{\mathfrak{P}}(EN)$ and $G_2 : NF^2 \to EN$, $\mathfrak{C}_{\mathfrak{P}}(NF^2) \to \mathfrak{C}_{\mathfrak{P}}(EN)$. In particular, G_1 and G_2 both map X into $\mathrm{ccl}(EF^{\beta}) \cap \mathfrak{C}_{\mathfrak{P}}(EN)$. Conjugating if necessary by an element in $\mathfrak{C}_{\mathfrak{P}}(EN)$, we may assume both G_1 and G_2 map X onto EF^{β}. Set $G = G_1 G_2^{-1}$; then $G : J \to J$, $X \to X$, $N \to NF^2$. If $\mathfrak{A} = \langle X, J \rangle$, $\mathfrak{H} = \mathfrak{C}(\mathfrak{A})$, then $\langle \mathfrak{A}, F^2, EF, N \rangle$ is an S_2-subgroup of $\mathfrak{H}$. In particular, the S_2-subgroups of $\mathfrak{H}/\mathfrak{A}$ are elementary abelian of order 8. Modulo $\mathfrak{A}$ the following elements represent the elements of an S_2-subgroup of $\mathfrak{H}/\mathfrak{A}$: $1\ F^2\ EF\ N\ EF^3\ NF^2\ ENF^{-1}\ ENF$. Moreover, $N \sim NF^2$ in $\mathfrak{H}/\mathfrak{A}$ by the above. By Burnside's theorem we see that either all the nonidentity representatives above are fused in $\mathfrak{H}/\mathfrak{A}$, or 6 of them are fused in sets of 3 each. But this is impossible, since 5 of them have squares in $\langle J \rangle$ and 2 of them have squares in $\mathrm{ccl}(X)$. This completes the proof.

Remark. We note that if $\mathfrak{P} = \mathfrak{P}(\rho, \sigma, \tau)$ with $\rho = 0$, $\sigma = \tau = 1$, and if $\mathfrak{A} = \langle J, X \rangle$, then as a consequence of (e), the group $\mathfrak{C}(\mathfrak{A})$ has a normal 2-complement.

Proposition (2H). *Let $\rho = 0$, $\sigma = 1$, $\tau = 1$. If $\mathfrak{G}$ has no subgroups of index 2, then after a suitable relabeling of the generators E, N, F, there are exactly three possibilities for the fusion of involutions of $\mathfrak{P}$.*

I. $J \sim X \sim N \sim EF \sim EF^3 \sim NF \sim EN$,

II. $J \sim X \sim N \sim EF$, $EF^3 \sim NF \sim EN$,

III. $J \sim X \sim EF^3$, $N \sim EF \sim NF \sim EN$.

In all three cases, $E^2 \sim ENX \sim ENF^3$, $F^2 \sim NXF \sim ENF$.

Proof. The following are consequences of (2D) and (2F), (2.1): $E^2 \nsim NXF$, $F^2 \nsim ENX$, since either fusion implies $E^2 \sim F^2$. Secondly, if $X \sim EF^{\alpha}$ for some $\alpha = 1$ or 3, then $E^2 \sim ENX$, $F^2 \sim NXF$, $NF \sim EN \sim EF^{\beta}$, where $\beta = 1$ or 3, $\beta \neq \alpha$. By (2G) and (2E), $J \sim X$, $N \sim EF$, $E^2 \sim ENF^3$, $F^2 \sim ENF$. Suppose $N \sim X$. Then $EF \sim X$, and we have either cases I or II. Suppose that neither case I nor case II holds. If $X \sim J$ is fused to no other class, then the only possible fusions in $\mathfrak{G}$ are between

$$X \sim J \,\big|\, E^2 \sim ENF^3 \,\big|\, F^2 \sim ENF \,\big|\, N \sim EF, EF^3 \,\big|\, NF, EN$$

by (2F), (2.1). But then $\mathfrak{P}^{\#} \leqq \langle \mathfrak{P}', ENF, EF \rangle < \mathfrak{P}$, which is impossible. Thus $X \sim Y$ for some $Y \in \mathfrak{P}$ with $vc_{\mathfrak{P}}(Y) = 4$. If $Y = EF^3$, then we have case III by an above remark. If $Y = NF$, then $EN \sim EF \sim EF^3 \sim N$ by (2F), (2.1). In order that $\mathfrak{P}^{\#} = \mathfrak{P}$, E^2 must be fused to ENX. But then $EF \sim X$ by (2F), (2.1) and $N \sim X$, which has been excluded. Similarly, if $Y = EN$, a contradiction is also obtained. This completes the proof.

Summarizing the results of §§1, 2, we have:

THEOREM (2I). *Let $\mathfrak{G}$ be a finite group of order $64m$, m odd. Let $\mathfrak{P}$ be an S_2-subgroup of $\mathfrak{G}$. Suppose there is an element $F \in \mathfrak{P}$ of order 8 which is self-centralizing in $\mathfrak{P}$ and conjugate to its odd powers in $\mathfrak{P}$. If $\mathfrak{G}$ has no subgroups of index 2, then $\mathfrak{P}$ is isomorphic to $\mathfrak{P}(\rho, \sigma, \tau)$ of (1A), with $\rho = 0$, $\sigma = \tau = 1$. Furthermore, if notation is chosen suitably, the possibilities for the fusion of the 2-power classes of $\mathfrak{G}$ are*

I. $F|E|E^2 \sim ENX \sim ENF^3|F^2 \sim NXF \sim ENF|J \sim X \sim N \sim EF \sim EF^3 \sim NF \sim EN$,

II. $F|E|E^2 \sim ENX \sim ENF^3|F^2 \sim NXF \sim ENF|J \sim X \sim N \sim EF|EF^3 \sim NF \sim EN$,

III. $F|E|E^2 \sim ENX \sim ENF^3|F^2 \sim NXF \sim ENF|J \sim X \sim EF^3|N \sim EF \sim NF \sim EN$.

Let $\mathfrak{P}$ be the 2-group of (2I). The character table of $\mathfrak{P}$ is easily seen to be

(2.2)

E	F	F^2	NXF	ENF	E^2	ENX	ENF^3	EN	NF	EF^3	EF	N	X	J	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	−1	−1	1	−1	−1	−1	−1	1	1	−1	1	1	1
1	−1	1	−1	−1	1	1	−1	1	−1	−1	−1	1	1	1	1
1	−1	1	1	1	1	−1	1	−1	1	−1	−1	−1	1	1	1
−1	1	1	1	−1	1	−1	−1	−1	1	−1	−1	1	1	1	1
−1	1	1	−1	1	1	1	1	1	−1	−1	−1	−1	1	1	1
−1	−1	1	−1	1	1	−1	1	−1	−1	1	1	1	1	1	1
−1	−1	1	1	−1	1	1	−1	1	1	1	1	−1	1	1	1
0	0	2	−2	0	−2	0	0	0	2	0	0	0	−2	2	2
0	0	2	2	0	−2	0	0	0	−2	0	0	0	−2	2	2
0	0	−2	0	0	2	−2	0	2	0	0	0	0	−2	2	2
0	0	−2	0	0	2	2	0	−2	0	0	0	0	−2	2	2
0	0	−2	0	0	−2	0	0	0	0	2	−2	0	2	2	2
0	0	−2	0	0	−2	0	0	0	0	−2	2	0	2	2	2
0	0	0	0	2	0	0	−2	0	0	0	0	0	0	−4	4
0	0	0	0	−2	0	0	2	0	0	0	0	0	0	−4	4

The irreducible characters of $\mathfrak{P}$ will be denoted by ζ_i, $1 \leq i \leq 16$ in the above order.

3. We will require certain facts from the theory of blocks. The terminology is taken from [3]. Let $\mathfrak{G}$ be a group of order $g = p^a g'$, where p is a fixed prime

number not dividing g'. If B is a block of $\mathfrak{G}$, then the restrictions χ_μ^0 of the irreducible characters χ_μ in B to the p-regular classes generate a module M_B over Z. Any basis $\{\phi_\rho\}$ of M_B will be called a basic set ϕ_B of B. We will always assume that when B is the 1-block of $\mathfrak{G}$, then the constant function 1 is in ϕ_B. Once a basic set ϕ_B for B has been chosen, the corresponding decomposition numbers $d_{\mu\rho}$ and Cartan invariants $c_{\rho\sigma}$ of B are defined by

$$\chi_\mu^0 = \sum_\rho d_{\mu\rho}\phi_\rho \quad \text{for } \chi_\mu \in B,\ \phi_\rho \in \phi_B,$$

$$c_{\rho\sigma} = \sum_\mu d_{\mu\rho} d_{\mu\sigma} \quad \text{for } \phi_\rho, \phi_\sigma \in \phi_B.$$

$(c_{\rho\sigma})$ is the matrix of a positive-definite quadratic form. If ϕ_B is replaced by another basic set, the form is replaced by an equivalent form. The irreducible modular characters of $\mathfrak{G}$ in B form a basic set, and if $(c_{\rho\sigma})$ is the corresponding Cartan matrix, then it is well known that $\sum_\sigma c_{\rho\sigma}\phi_\sigma(1) \equiv 0 \pmod{p^a}$. From this and the above remarks, it follows that the analogous congruence holds for any basic set of B.

Let P be a p-element of $\mathfrak{G}$. Let B^* run over the blocks of $\mathfrak{C}(P)$, and for each B^*, assume that a basic set ϕ_{B^*} has been selected. If V runs over p-regular elements of $\mathfrak{C}(P)$, the corresponding generalized decomposition numbers $d_{\mu\rho}^P$ are defined by

$$\chi_\mu(PV) = \sum d_{\mu\rho}^P \phi_\rho^P(V),$$

where the sum is over all $\phi_\rho^P \in \phi_{B^*}$ and all B^*. If B is the 1-block of $\mathfrak{G}$, then the above sum need only be taken over the basic set of the 1-block of $\mathfrak{C}(P)$ [3, Theorem 3]. For notational convenience, the column $(d_{\mu\rho}^P)$ will be denoted by $\mathfrak{d}_\rho^P$; its μth entry $d_{\mu\rho}^P$ will be denoted by $(\mathfrak{d}_\rho^P)_\mu$.

Assume from now on that B and B^* are the 1-blocks of $\mathfrak{G}$ and $\mathfrak{C}(P)$ respectively. Define for $\chi_\lambda, \chi_\mu \in B$,

$$S_{\lambda\mu}^P = \frac{1}{c(P)} \sum \chi_\lambda(PV)\bar{\chi}_\mu(PV), \tag{3.1}$$

where V runs over all p-regular elements of $\mathfrak{C}(P)$. Then by [4] $S_{\lambda\mu}^P = \sum_{\rho,\sigma} d_{\lambda\rho}^P \bar{d}_{\mu\sigma}^P \gamma_{\rho\sigma}^P$, where $(\gamma_{\rho\sigma}^P)$ is the inverse matrix of $C^P = (c_{\rho\sigma}^P)$, the matrix of Cartan invariants of B^*. In particular, if $d = \nu(P)$, then $p^d(\gamma_{\rho\sigma}^P)$ is an integral matrix. Let Q^P denote the quadratic form determined by $p^d(\gamma_{\rho\sigma}^P)$; Q^P is positive-definite.

Let $1 = P_1, P_2, \cdots, P_r$ be a complete set of representatives for the classes of p-elements of $\mathfrak{G}$. Then from the ordinary orthogonality relation $(\chi_\lambda, \chi_\mu)_{\mathfrak{G}} = \delta_{\lambda\mu}$ grouped according to the p-sections of $\mathfrak{G}$, we have

$$\sum_{i=1}^r S_{\lambda\mu}^{P_i} = \delta_{\lambda\mu} = \begin{cases} 1 & \lambda = \mu, \\ 0 & \lambda \neq \mu. \end{cases}$$

In particular, for $\lambda=\mu$, $\sum_{i=1}^{r} p^a\, S_{\lambda\lambda}^{P_i}=p^a$. This latter equation will be referred to as the method of contribution. If $d_{\lambda\rho}^{P}$ is a rational integer for all ϕ_ρ^P in ϕ_{B^*}, and if $\nu(P)=d$, then $p^a S_{\lambda\lambda}^{P}$ is a rational integer $\geqq p^{a-d}m$, where m is the minimum value of the quadratic form Q^P for nonzero integral vectors. By [4] we also have the following congruence:

$$p^a S_{\lambda\lambda}^{P} \equiv p^a x_\lambda^2 S_{1,1}^{P} \pmod{\mathfrak{p}p^{h_\lambda}},$$

where χ_1 is the 1-character of $\mathfrak{G}$, $\chi_\lambda\in B$, $\nu(x_\lambda)=h_\lambda$ is the so-called height of χ_λ, and $\mathfrak{p}$ is a prime ideal divisor of p in a suitably large algebraic number field. We will refer to this congruence as the νth method of contribution.

If the columns $\mathfrak{d}_\rho^P$ of the 1-block B have been determined for all p-singular sections of $\mathfrak{G}$, and B has k irreducible characters χ_λ, then any set of integral, linearly independent columns of length k orthogonal to the given $\mathfrak{d}_\rho^P$ and having a maximal subdeterminant of value 1 is then the set of decomposition numbers of B relative to some basic set [3, §5]. The corresponding Cartan invariants can then be computed. This technique will be used considerably in the next two sections.

The following remarks may aid in the computations to follow.

(1) If $G\in\mathfrak{z}\mathfrak{G}$ and G has order p^α, then the p-blocks of $\mathfrak{G}$ and $\mathfrak{G}/\langle G\rangle$ are in 1-1 correspondence. The Cartan invariants of a block of $\mathfrak{G}$ are obtained by multiplying the Cartan invariants of the corresponding block of $\mathfrak{G}/\langle G\rangle$ by p^α [3, §2].

(2) If $\mathfrak{G}$ has a normal p-complement, then each p-block consists of one modular character. In particular, the Cartan matrix of a block of defect d is (p^d) [5, §2].

(3) Let $\mathfrak{D}$ be the dihedral group $\langle A,B \mid A^4=B^2=ABAB=1\rangle$ of order 8. Let $\mathfrak{G}$ be a finite group with $\mathfrak{D}$ as S_2-subgroup. The classes of involutions in $\mathfrak{D}$ are represented by A^2, B, AB. Let C be the Cartan matrix of the 1-block for the prime 2. Then one and only one of the following holds: (i) $\mathfrak{G}$ has 3 classes of involutions, $C=(8)$; (ii) $\mathfrak{G}$ has 2 classes of involutions,

$$A^2\sim B \text{ or } A^2\sim AB, \quad C=\begin{pmatrix}3&1\\1&3\end{pmatrix};$$

(iii) $\mathfrak{G}$ has 1 class of involutions,

$$C=\begin{bmatrix}2&0&-1\\0&2&-1\\-1&-1&3\end{bmatrix}.$$

This can be proved by the techniques of this paragraph easily; the details will be omitted.

4. From now on $\mathfrak{G}$ will be a finite group with no subgroups of index 2 satisfying the assumptions of (2I). By that result the classes of 2-elements fall into one of three cases, which we will denote by I, II, III in the notation of (2I). We

now compute the Cartan invariants of the 1-block for the 2-singular sections of $\mathfrak{G}$ and of $\mathfrak{H} = \mathfrak{C}(J)$. Accordingly, if Y is a representative of a 2-section, C^Y and $\tilde{C}^Y$ will denote the matrix of Cartan invariants of the 1-block of $C(Y)$ and $C_{\mathfrak{H}}(Y)$ respectively. In particular, $C^Y = \tilde{C}^Y$ for $Y = E, F, E^2, F^2, J$. As we shall see, these matrices are for $\mathfrak{G}$

$$
(4.1)\qquad
\begin{array}{|ccccc|l}
E & F & E^2 & F^2 & EN & \\
\hline
8 & 8 & \begin{pmatrix} 12 & 4 \\ 4 & 12 \end{pmatrix} & \begin{pmatrix} 12 & 4 \\ 4 & 12 \end{pmatrix} & - & \text{in I}, \\
8 & 8 & 32 & 32 & \begin{pmatrix} 6 & 2 \\ 2 & 6 \end{pmatrix} & \text{in II}, \\
8 & 8 & 32 & 32 & 16 & \text{in III} \\
\hline
\end{array}
$$

and for $\mathfrak{H}$

$$
(4.2)\qquad
\begin{array}{|cccccccccc|l}
E & F & ENF & ENF^3 & E^2 & F^2 & N & X & EN & J & \\
\hline
8 & 8 & 16 & 16 & \begin{pmatrix} 12 & 4 \\ 4 & 12 \end{pmatrix} & \begin{pmatrix} 12 & 4 \\ 4 & 12 \end{pmatrix} & 8 & 32 & - & \begin{bmatrix} 10 & 2 & 4 & 4 & 2 \\ 2 & 10 & 4 & 4 & 2 \\ 4 & 4 & 10 & 2 & 2 \\ 4 & 4 & 2 & 10 & 2 \\ 2 & 2 & 2 & 2 & 4 \end{bmatrix} & \text{in I}, \\
8 & 8 & 16 & 16 & 32 & 32 & 8 & 32 & 16 & \begin{pmatrix} 6 & 2 \\ 2 & 22 \end{pmatrix} & \text{in II, III}. \\
\hline
\end{array}
$$

Lemma (4A). *The only fusion in $\mathfrak{H}$ among the 2-elements are the following:*

$$E^2 \sim ENX, \quad F^2 \sim NXF, \quad EF \sim EF^3 \sim NF \sim EN \sim X \quad \textit{in } \mathrm{I},$$

$$E^2 \sim ENX, \quad F^2 \sim NXF, \quad EF^3 \sim NF \sim EN, \quad X \sim EF \quad \textit{in } \mathrm{II},$$

$$E^2 \sim ENX, \quad F^2 \sim NXF, \quad EF \sim NF \sim EN, \quad X \sim EF^3 \quad \textit{in } \mathrm{III}.$$

In particular, the labeling of the columns in (4.2) *is as indicated.*

Proof. Since $ENX \sim E^2$, $NXF \sim F^2$ in $\mathfrak{G}$, and their squares are J, these fusions occur in $\mathfrak{H}$. The elements in ccl(ENF), ccl(ENF^3) have squares X or XJ. Hence these classes are not fused in $\mathfrak{H}$ to E^2, F^2, ENX, NXF. We have thus listed the fusions of elements of order 4. If $X \sim EF$ in $\mathfrak{G}$, then $EF^3 \sim NF \sim EN$ and $X \sim EF$ in $\mathfrak{H}$ by (2F), (2.1). Similarly, if $X \sim EF^3$ in $\mathfrak{G}$, then $EF \sim NF \sim EN$ and $X \sim EF^3$ in $\mathfrak{H}$. In either case, the focal subgroup $\mathfrak{P}^{\#}$ of $\mathfrak{P}$ in $\mathfrak{H}$ contains $\langle \mathfrak{P}', EN, NF \rangle$ and thus $(\mathfrak{P} : \mathfrak{P}^{\#}) \leqq 2$. By (2G) $\mathfrak{P}^{\#} \neq \mathfrak{P}$, and hence ccl$(N)$ is isolated in $\mathfrak{H}$.

Corollary (4B). *$\mathfrak{H}$ has a normal subgroup $\tilde{\mathfrak{H}}$ of index* 2, *but none of index* 4. *Moreover*, $\tilde{\mathfrak{H}} \cap \mathfrak{P} = \langle \mathfrak{P}', EN, NF \rangle$. *Hence $\mathfrak{H}$ has a linear character λ of order* 2 *with* $\lambda(E) = \lambda(F) = \lambda(N) = -1$.

We now turn to the entries of (4.1) and (4.2). $\langle F \rangle, \langle E \rangle$ are S_2-subgroups of $\mathfrak{C}(F), \mathfrak{C}(E)$ respectively. Since $\mathfrak{C}(F), \mathfrak{C}(E)$ have normal 2-complements, $C^F, C^E, \tilde{C}^F, \tilde{C}^E$ are as indicated.

$\mathfrak{C}(F^2)$ has as an S_2-subgroup the subgroup $\mathfrak{Q} = \langle X, F, ENF \rangle$ of order 32. If residue classes modulo $\langle F^2 \rangle$ are denoted by a dot, then $\dot{\mathfrak{Q}}$ has order 8. If $M = ENF$, then $\dot{M}^4 = 1$, $\dot{M}^2 = \dot{X}$, $\dot{F}^2 = 1$, $\dot{F}\dot{M}\dot{F} = \dot{M}^{-1}$, and $\dot{\mathfrak{Q}}$ is dihedral. The classes of involutions are represented by $\dot{X}, \dot{F}, \dot{M}\dot{F}$. If $\dot{X} \sim \dot{M}\dot{F}$ in $\mathfrak{C}(F^2)/\langle F^2 \rangle$, then $X \sim EN$ or ENX. This is possible only in I, and indeed, occurs in that case. For since $X \sim EN$ in I in $\mathfrak{G}$, there is a $G \in \mathfrak{G}$ such that $G: EN \to X$. By (2F), (2.1), we may assume $G: F^2 \to F^{\pm 2}$, and since $F^2 \sim F^{-2}$ in $\mathfrak{C}(X)$, we may even assume G: $F^2 \to F^2$. If $\dot{X} \sim \dot{F}$ in $\mathfrak{C}(F^2)/\langle F^2 \rangle$, then $X \sim F^{2i+1}$ for some i, which is impossible. The situation for $\mathfrak{C}(E^2)$ is similar; an S_2-subgroup of $\mathfrak{C}(E^2)$ is $\langle X, E, ENF \rangle$. Thus $C^{E^2}, C^{F^2}, \tilde{C}^{E^2}\, \tilde{C}^{F^2}$ are as indicated.

In cases II, III, $\mathfrak{C}(EN)$ has $\langle EN \rangle \times \langle F^2, NF \rangle$ as S_2-subgroup, where $\mathfrak{Q} = \langle F^2, NF \rangle$ is dihedral of order 8. If residue classes modulo $\langle EN \rangle$ are denoted by a dot, then the classes of involutions of $\dot{\mathfrak{Q}}$ are represented by $\dot{J}$, $N\dot{F}$, $N\dot{F}^3$. Suppose we are in case II. If $\dot{J} \sim N\dot{F}^3$, then $J \sim NF^3$ or $J \sim (EN)(NF^3) = EF^3$ in $\mathfrak{C}(EN)$, which is impossible. If $\dot{J} \sim N\dot{F}$, then $J \sim NF$ or $J \sim EF$ in $\mathfrak{C}(EN)$, and only the latter can occur in case II. To see that this does occur, replace EN by the element Y in $\mathrm{ccl}(EF^3)$ which is fixed by the element B in $(2E)$. In $\mathfrak{C}(Y)/\langle Y \rangle$, B fuses two classes of involutions, and so

$$C^{EN} = \begin{pmatrix} 6 & 2 \\ 2 & 6 \end{pmatrix}.$$

Suppose we are in III. If $\dot{J} \sim \dot{N}F$, then $J \sim NF$ or $J \sim EF$, which is impossible. If $\dot{J} \sim N\dot{F}^3$, then necessarily $J \sim EF^3$ in $\mathfrak{C}(EN)$. To see that this does not occur, take as a representative of the class of EN in $\mathfrak{G}$ the element EF. $\mathfrak{C}(EF)$ has $\langle EF \rangle \times \langle NXF, X \rangle$ as S_2-subgroup. Moreover, if $J \sim EF^3$ in $\mathfrak{C}(EN)$, then $J \sim X$ in $\mathfrak{C}(EF)$, and there is an $A \in \mathfrak{G}$ such that $A: X \to J$, $EF \to EF$. On the other hand, by (2E) there is a $B \in \mathfrak{G}$ such that $B: J \to X$, $N_1 \to \mathrm{ccl}(EF)$, where $N_1 \in \mathrm{ccl}(N)$. Since EF has 4 conjugates in $\mathfrak{C}_{\mathfrak{P}}(X)$, we may assume $B: N_1 \to EF$. Then $BA: J \to J$, $N_1 \to EF$. If $\mathfrak{P}^{\#}$ is the focal subgroup of $\mathfrak{P}$ in $\mathfrak{C}(J)$, then $ENF \in \mathfrak{P}^{\#}$, which contradicts (4B). Thus $J \nsim EF^3$ in $\mathfrak{C}(EN)$, and $C^{EN} = (16)$. This proves the validity of (4.1).

In $\mathfrak{H}/\langle J \rangle$ let small letters denote residue classes of corresponding capital letters. By (4A) the following are representatives of the classes of 2-elements of $\mathfrak{H}/\langle J \rangle$.

$$e,\ f,\ enf,\ e^2, f^2, x,\ en,\ n,\ 1$$

except that in case I, *en* is to be omitted. For $Y \in \mathfrak{H}$, let $\mathfrak{C}^0(Y)$ be the inverse image in $\mathfrak{H}$ of the centralizer $\dot{\mathfrak{C}}(y)$ of y in $\mathfrak{H}/\langle J\rangle$. Then $\mathfrak{C}_{\mathfrak{H}}(Y) \trianglelefteq \mathfrak{C}^0(Y)$, and the index is 1 or 2. In particular, if $\mathfrak{C}(Y)$ has a normal 2-complement, so do $\mathfrak{C}_{\mathfrak{H}}(Y)$ and $\mathfrak{C}^0(Y)$. If y is a representative of a 2-section of $\mathfrak{H}/\langle J\rangle$, let $\dot{C}^y$ be the matrix of Cartan invariants of the 1-block of $\dot{\mathfrak{C}}(y)$. We then have $\dot{C}^e = \dot{C}^f = (8)$. $\dot{\mathfrak{C}}(enf)$ has $\langle enf\rangle \times \langle f^2\rangle$ as an S_2-subgroup, so that $\dot{\mathfrak{C}}(enf)$ has a normal 2-complement, and $\dot{C}^{enf} = (8)$. For $\dot{\mathfrak{C}}(e^2)$ and $\dot{\mathfrak{C}}(f^2)$ the above remarks apply in cases II, III, so that $\dot{C}^{e^2} = \dot{C}^{f^2} = (32)$ in these cases. In case I $\dot{\mathfrak{C}}(f^2)/\langle f^2\rangle$ has as an S_2-subgroup $\mathfrak{Q} \times \langle N\rangle \pmod{\langle F^2\rangle}$, where $\mathfrak{Q} = \langle X, F, ENF\rangle$. $\dot{\mathfrak{C}}(f^2)/\langle f^2\rangle$ has a normal subgroup of index 2 with dihedral S_2-subgroups. Moreover, the center of $\mathfrak{Q} \times \langle N\rangle \pmod{\langle F^2\rangle}$ is not contained in this subgroup From our earlier remarks and [5] (3B), it follows that

$$\dot{C}^{f^2} = \begin{pmatrix} 12 & 4 \\ 4 & 12 \end{pmatrix}.$$

Similarly,

$$\dot{C}^{e^2} = \begin{pmatrix} 12 & 4 \\ 4 & 12 \end{pmatrix}.$$

$\dot{\mathfrak{C}}(x)$ has a normal 2-complement by the remark following (2G), so that $\dot{C}^x = (32)$. $\dot{\mathfrak{C}}(n)$ has $\langle n, e^2, f^2\rangle$ as S_2-subgroup, elementary abelian of order 8. Thus $\dot{\mathfrak{C}}(n)/\langle n\rangle$ has an S_2-subgroup of type (2,2), whose involutions modulo $\langle n\rangle$ are $e^2, f^2, x = e^2f^2$. If these are fused in $\dot{\mathfrak{C}}(n)/\langle n\rangle$, then e^2, f^2, x are fused in $\dot{\mathfrak{C}}(n)$ which is impossible. Thus $\dot{\mathfrak{C}}(n)$ has a normal 2-complement, and $\dot{C}^n = (8)$. Finally, in cases II, III, $\mathfrak{C}_{\mathfrak{H}}(EN)$ has $\langle EN\rangle \times \langle F^2, NF\rangle$ as an S_2-subgroup, and there are no fusions of involutions in $\mathfrak{C}_{\mathfrak{H}}(EN)/\langle EN\rangle$, since J is isolated in $\mathfrak{H}$. Thus $\mathfrak{C}_{\mathfrak{H}}(EN)$ and $\dot{\mathfrak{C}}(en)$ have normal 2-complements, and $\dot{C}^{en} = (16)$. Summarizing the calculations of this paragraph, we have

(4.3)

	e	f	enf	e^2	f^2	x	n	en	
	8	8	8	$\begin{pmatrix} 12 & 4 \\ 4 & 12 \end{pmatrix}$	$\begin{pmatrix} 12 & 4 \\ 4 & 12 \end{pmatrix}$	32	8	—	in I,
	8	8	8	32	32	32	8	16	in II, III.

The entries of (4.2) are now clear, except for those under J.

Let χ_1 be the 1-character of $\mathfrak{H}$. Then $d^e_{1,1} = d^f_{1,1} = d^{enf}_{1,1} = 1$. The existence of the character λ of (4B) shows that the nonzero entries under e, f, enf, n are four 1's and four -1's. These nonzero generalized decomposition numbers exhaust the characters of height 0, and hence the 1-block $\tilde{B}$ of $\mathfrak{H}$ has exactly 8 characters of height 0. After a rearrangement if necessary, we may assume by the orthogonality relations that χ_i for $1 \leqq i \leqq 8$ are as below:

(4.4)

e	f	enf	n
1	1	1	1
−1	−1	−1	−1
1	1	−1	−1
−1	−1	1	1
1	−1	1	−1
−1	1	−1	1
1	−1	−1	1
−1	1	1	−1

Cases II, III. For $1 \leqq \mu \leqq 8$, $d_{\mu 1}^{en}$ are odd integers occurring in pairs; hence they are ± 1, since $\sum_\mu (d_{\mu 1}^{en})^2 = 16$. The remaining nonzero entries in $\mathfrak{d}_1^{en}$ are even integers whose squares add up to 8. Hence these are ± 2, and we may assume they occur for χ_9, χ_{10}. If there is a χ_{11} in the 1-block $\dot{B}$ of $\mathfrak{H}/\langle J \rangle$, consider χ_{11} restricted to $\langle en, nf^3 \rangle$ in II, to $\langle en, nf \rangle$ in III. These subgroups are abelian of type (2,2), and their involutions are fused in $\mathfrak{H}$. Hence $3\chi_{11}(en) \equiv \chi_{11}(1) \pmod 4$. Since $\chi_{11}(en) = 0$, χ_{11} has height $\geqq 2$, and thus each of the numbers $\chi_{11}(e^2)$, $\chi_{11}(f^2)$, $\chi_{11}(x)$ is nonzero and divisible by 4 by the νth method of contribution. But then $4^2 + 4^2 + 4^2 > 32$, and this is impossible by the method of contribution applied to χ_{11}. $\dot{B}$ then has exactly 10 irreducible characters, and therefore 2 modular characters for the 1-section. For $i = 9, 10$, $\chi_i(e^2)$, $\chi_i(f^2)$, $\chi_i(x) = \pm 2$, since ± 6 is too large. The matrix of generalized decomposition numbers for $\dot{B}$ can now be essentially completed. A $\chi \in \dot{B}$ cannot assume ± 3 more than once on e^2, f^2, x by the method of contribution. Orthogonality relations are then sufficient to compute the remaining entries with the uncertainties indicated below. We omit the details.

(4.5)

e	f	enf	e^2	f^2	x	n	en	1	
1	1	1	1	1	1	1	1	1	0
−1	−1	−1	1	1	1	−1	1	1	0
1	1	−1				−1	τ_1	0	τ_1
−1	−1	1				1	τ_1	0	τ_1
1	−1	1				−1	τ_2	0	τ_2
−1	1	−1	$\mathfrak{S}_\alpha$	$\mathfrak{S}_\beta$	$\mathfrak{S}_\gamma$	1	τ_2	0	τ_2
1	−1	−1				1	τ_3	0	τ_3
−1	1	1				−1	τ_3	0	τ_3
0	0	0	$2\omega_1$	$2\omega_1$	$2\omega_1$	0	$-2\omega_1$	0	$2\omega_1$
0	0	0	$2\omega_2$	$2\omega_2$	$2\omega_2$	0	$2\omega_2$	$-\omega_2$	$-\omega_2$

Here $\tau_i, \omega_i = \pm 1$, $\{\alpha, \beta, \gamma\}$ is a permutation of $\{1, 2, 3\}$, and

$$
\mathfrak{S}_1 = \begin{bmatrix} -3\tau_1 \\ -3\tau_1 \\ \tau_2 \\ \tau_2 \\ \tau_3 \\ \tau_3 \end{bmatrix}, \quad \mathfrak{S}_2 = \begin{bmatrix} \tau_1 \\ \tau_1 \\ -3\tau_2 \\ -3\tau_2 \\ \tau_3 \\ \tau_3 \end{bmatrix}, \quad \mathfrak{S}_3 = \begin{bmatrix} \tau_1 \\ \tau_1 \\ \tau_2 \\ \tau_2 \\ -3\tau_3 \\ -3\tau_3 \end{bmatrix}. \tag{4.6}
$$

The columns under 1 are determined by the methods of §3. $\tilde{C}^J$ is then

$$
\begin{pmatrix} 6 & 2 \\ 2 & 22 \end{pmatrix}.
$$

If f_1^J, f_2^J are the degrees of the functions in the corresponding basic set, then $f_1^J = 1$ since ϕ_1^J is the constant 1. Since $6f_1^J + 2f_2^J \equiv 0 \pmod{64}$, we see that $f_2^J \equiv -3 \pmod{32}$. This will be important later on.

The matrix of generalized decomposition numbers for the 1-block $\tilde{B}$ of $\mathfrak{H}$ in cases II, III can now be completed. A calculation of the S_2-subgroups shows that except for ENF and ENF^3, all entries under the various representatives $\neq J$ of the 2-singular sections from characters faithful on J are 0. Moreover, the nonzero entries for ENF, ENF^3 are rational even integers whose squares add up to 8. This implies the existence of χ_{11}, χ_{12} as indicated below. Since there are at least 13 columns, there is one more character χ_{13}. The entries of χ_{11}, χ_{12}, χ_{13} under J and 1 are easily determined by orthogonality relations. The arrangement of the signs is achieved by interchanging χ_{11} and χ_{12} and replacing either by its negative if necessary. The matrix of generalized decomposition numbers for $\tilde{B}$ in cases II, III is

$$
\begin{array}{ccccccccccccc}
E & F & E^2 & F^2 & ENF & ENF^3 & X & N & EN & \multicolumn{2}{c}{J} & \multicolumn{2}{c}{1} \\
\hline
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
-1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & & & -1 & -1 & & -1 & \tau_1 & 0 & \tau_1 & 0 & \tau_1 \\
-1 & -1 & & & 1 & 1 & & 1 & \tau_1 & 0 & \tau_1 & 0 & \tau_1 \\
1 & -1 & \mathfrak{S}_\alpha & \mathfrak{S}_\beta & 1 & 1 & \mathfrak{S}_\gamma & -1 & \tau_2 & 0 & \tau_2 & 0 & \tau_2 \\
-1 & 1 & & & -1 & -1 & & 1 & \tau_2 & 0 & \tau_2 & 0 & \tau_2 \\
1 & -1 & & & -1 & -1 & & 1 & \tau_3 & 0 & \tau_3 & 0 & \tau_3 \\
-1 & 1 & & & 1 & 1 & & -1 & \tau_3 & 0 & \tau_3 & 0 & \tau_3 \\
0 & 0 & 2\omega_1 & 2\omega_1 & 0 & 0 & 2\omega_1 & 0 & -2\omega_1 & 0 & 2\omega_1 & 0 & 2\omega_1 \\
0 & 0 & 2\omega_2 & 2\omega_2 & 0 & 0 & 2\omega_2 & 0 & 2\omega_2 & -\omega_2 & -\omega_2 & -\omega_2 & -\omega_2 \\
\hline
0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 & 0 & -1 & 1 & 1 & -1 \\
0 & 0 & 0 & 0 & -2 & 2 & 0 & 0 & 0 & -1 & 1 & 1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -3 & 1 & 3
\end{array} \tag{4.7}
$$

where ω_i, $\tau_i = \pm 1$, and $\mathfrak{S}_\alpha, \mathfrak{S}_\beta, \mathfrak{S}_\gamma$ are as in (4.6). C^J is then

$$\begin{pmatrix} 6 & 2 \\ 2 & 22 \end{pmatrix}$$

as indicated in (4.2).

Case I. Let $\dot{B}$ be the 1-block of $\mathfrak{H}/\langle J\rangle$. Then no $\chi_i \in \dot{B}$ is zero on x, since x is in the center of $\mathfrak{P}/\langle J\rangle$. If $\chi_i(x) = \pm 3$ for some $1 \leqq i \leqq 8$, then this occurs at least twice, so that $\sum_{i=1}^{8}\chi_i(x)^2 \geqq 24$. Since the remaining $\chi_i \in \dot{B}$ have height $\geqq 1$, this would imply that $\dot{B}$ has $\leqq$ 10 characters, which is impossible. Thus we may assume $\chi_i(x) = \chi_{i+1}(x) = \tau_i$ for $i = 3,5,7$, $\tau_i = \pm 1$. The $\chi_i \in \dot{B}$ for $i \geqq 9$ cannot have height $\geqq 2$; otherwise the contribution from e^2, f^2, x would be too large. Hence these χ_i have height 1, and necessarily $\chi_i(x) = 2\tau_i$, $\tau_i = \pm 1$. In particular, $\dot{B}$ has 14 characters and 5 functions in the basic set from the 1-section. The quadratic forms Q^{E^2} and Q^{F^2} associated to $\mathfrak{C}(E^2)$ and $\mathfrak{C}(F^2)$ are $3u^2 - 2uv + 3v^2 = 2u^2 + 2v^2 + (u-v)^2$, which has a minimum of 3 for nonzero rational integral vectors. If a $\chi_i \in \dot{B}$ has height 0, then the sum of the contributions from $E^2, F^2, J, 1$ must be $64 - 34 = 30$. We express this as

$$2Q^{E^2} + 2Q^{F^2} + Q^J + Q^1 = 30.$$

Now $Q^J, Q^1 \geqq 1$. Since $d_{i1}^{E^2} - d_{i2}^{E^2}$ and $d_{i1}^{F^2} - d_{i2}^{F^2}$ are necessarily odd, Q^{E^2} and Q^{F^2} are $\leqq 11$. If (u,v) are the decomposition numbers of χ_i under E^2 or F^2, and if we allow for a possible change of sign $(u,v) \to (-u,-v)$ and a possible interchange $(u,v) \to (v,u)$, then the only possible values for (u,v) are $(1,0)$ and $(2,1)$. If $\chi_i \in \dot{B}$ has height 1, then $u + v \equiv 2 \pmod 4$. The method of contributions implies that Q^{E^2} and $Q^{F^2} \leqq 30$. With the same conventions as before, the only possible values for (u,v) are $(1,1)$ and $(2,0)$. Consider the entries under E^2 for all $\chi_i \in \dot{B}$. If there are a,b,c,d rows of type $(1,0), (2,1), (1,1), (2,0)$ respectively, then from the equality $\sum u^2 + \sum v^2 = 24$, we have $a + b = 8$, $c + d = 6$, $a + 5b + 2c + 4d = 24$. Thus $b = 0$, $d = 2$. The entries can then be determined by the orthogonality relations. Similarly so for the entries under F^2. The generalized decomposition numbers for $\dot{B}$ for the 2-singular sections of $\mathfrak{H}/\langle J\rangle$ have now been determined, and are as below. There are then 6 characters of $\tilde{B}$ faithful on $\langle J\rangle$. Two of them, say χ_{15}, χ_{16}, are nonzero on ENF, ENF^3. The columns under J and 1 can then be found by the methods of §3. The matrix for $\tilde{B}$ in case I is (4.8), where $\tau_i = \pm 1$. $\tilde{C}^J$ is then as in (4.2).

5. In addition to the assumptions made on $\mathfrak{G}$ on §4, we also assume $\mathfrak{G}$ has more than one class of involutions. This excludes case I.

Lemma (5A). *Let χ be a character of $\mathfrak{G}$. Then*

(i) $\chi(E) \equiv \chi(F) \pmod 2$,

(ii) $\chi(E^2) \equiv \chi(F^2) \equiv \chi(EN) \equiv \chi(J) \pmod 4$,

(iii) $\chi(J) \equiv 2\chi(E) - \chi(F^2) \equiv 2\chi(F) - \chi(E^2) \pmod 8$,

(iv) $-2\chi(E) - 2\chi(F) + \chi(F^2) + \chi(E^2) + 2\chi(EN) \equiv 0 \pmod 8$.

(4.8)

E	F	ENF	ENF^1	E^2		F^2		N	X	J					1				
1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	1	0	0	0	0
−1	−1	−1	−1	1	0	1	0	−1	1	1	0	0	0	0	1	0	0	0	0
1	1	−1	−1	0	τ_3	0	τ_3	−1	τ_3	0	τ_3	0	0	0	0	τ_3	0	0	0
−1	−1	1	1	0	τ_3	0	τ_3	1	τ_3	0	τ_3	0	0	0	0	τ_3	0	0	0
1	−1	−1	−1	0	τ_5	τ_5	τ_5	1	τ_5	0	0	τ_5	0	0	0	0	τ_5	0	0
−1	1	1	1	0	τ_5	τ_5	0	−1	τ_5	0	0	τ_5	0	0	0	0	τ_5	0	0
1	−1	1	1	τ_7	0	0	τ^1	−1	τ_7	0	0	0	τ^2	0	0	0	0	τ^2	0
−1	1	−1	−1	τ_7	0	0	τ^2	1	τ_7	0	0	0	τ^2	0	0	0	0	τ^2	0
0	0	0	0	$-\tau_9$	$-\tau_9$	$-\tau_9$	τ_9	0	$2\tau_9$	τ_9	τ_9	τ_9	τ_9	τ_9	τ_9	τ_9	τ_9	τ_9	τ_9
0	0	0	0	$-\tau_{10}$	$-\tau_{10}$	$-\tau_{10}$	τ_{10}	0	$2\tau_{10}$	0	0	0	0	$-\tau_{10}$	0	0	0	0	$-\tau_{10}$
0	0	0	0	$-\tau_{11}$	$-\tau_{11}$	$2\tau_{11}$	0	0	$2\tau_{11}$	$-\tau_{11}$	0	$-\tau_{11}$	0	0	$-\tau_{11}$	0	$-\tau_{11}$	0	0
0	0	0	0	$-\tau_{12}$	$-\tau_{12}$	0	$2\tau_{12}$	0	$2\tau_{12}$	0	$-\tau_{12}$	0	$-\tau_{12}$	0	0	$-\tau_{12}$	0	$-\tau_{12}$	0
0	0	0	0	$2\tau_{13}$	0	$-\tau_{13}$	$-\tau_{13}$	0	$2\tau_{13}$	$-\tau_{13}$	0	0	$-\tau_{13}$	0	$-\tau_{13}$	0	0	$-\tau_{13}$	0
0	0	0	0	0	$2\tau_{14}$	$-\tau_{14}$	$-\tau_{14}$	0	$2\tau_{14}$	0	$-\tau_{14}$	$-\tau_{14}$	0	0	0	$-\tau_{14}$	$-\tau_{14}$	0	0
0	0	2	−2	0	0	0	0	0	0	1	1	1	1	0	−1	−1	−1	−1	0
0	0	−2	2	0	0	0	0	0	0	1	1	1	1	0	−1	−1	−1	−1	0
0	0	0	0	0	0	0	0	0	0	−1	1	−1	1	0	1	−1	1	−1	0
0	0	0	0	0	0	0	0	0	0	−1	1	1	−1	0	1	−1	−1	1	0
0	0	0	0	0	0	0	0	0	0	−1	−1	0	0	−1	1	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0	−1	−1	−1	0	0	1	1	1

Proof. (i) is obvious, since $\chi(E)$ and $\chi(F)$ are rational integers congruent to $\chi(1)\pmod 2$. The others follow by restricting χ to $\mathfrak{P}$ and computing $(\chi,\phi)_{\mathfrak{P}}$, where ϕ is a suitable generalized character of $\mathfrak{P}$. For (ii) take ϕ to be respectively $\zeta_{15}-\zeta_{16}$, $\zeta_9-\zeta_{10}$, $\zeta_{13}-\zeta_{14}$ in the notation of (2.2). For (iii) take ϕ to be $\zeta=\zeta_1-\zeta_5$, which yields $2\chi(E)+\chi(F^2)+2\chi(E^2)+2\chi(EN)+\chi(J)\equiv 0 \pmod 8$. By (ii) $2\chi(F^2)\equiv 2\chi(E^2)$, $2\chi(EN)\equiv 2\chi(J) \pmod 8$. Substitution of these gives the first part of (iii). The second part is proved similarly. For (iv) take $\phi=2\zeta_1-\zeta_9$, and use the congruence $2\chi(EN)\equiv 2\chi(J)\pmod 8$.

Let B be the 1-block of $\mathfrak{G}$. If Y is a representative of a 2-singular section of $\mathfrak{G}$, we assume a basic set $\phi_B=\{\phi_\rho^Y\}$ has been chosen for the 1-block of $\mathfrak{C}(Y)$ such that the corresponding Cartan invariants are as in (4.1), and for $Y=J$, as in (4.2). Denote by f_ρ^Y the degree of ϕ_ρ^Y ; ϕ_1^Y is always the 1-character of $\mathfrak{C}(Y,)$, so that $f_1^Y=1$. In particular, $f_2^{EN}\equiv -3 \pmod 8$ in case II, and $f_2^J\equiv -3 \pmod{32}$. The corresponding columns of generalized decomposition numbers are then denoted by $\mathfrak{d}_\rho^Y$, except that in the case where $\mathfrak{C}(Y)$ has a normal 2-complement and there is but one such column, we will drop the index 1. For $\chi_i\in B$, $\chi_i(Y)=\sum_\rho(\mathfrak{d}_\rho^Y)_i f_\rho^Y$, where $(\mathfrak{d}_\rho^Y)_i$ is the entry $d_{i\rho}^Y$.

Define the following columns of rational integers, indexed by the $\chi_i\in B$.

$$\mathfrak{a}=\frac{\mathfrak{d}^F-\mathfrak{d}^E}{2},\qquad \mathfrak{b}=\frac{\mathfrak{d}^F+\mathfrak{d}^E}{2},\qquad \mathfrak{w}=\begin{cases}\dfrac{\mathfrak{d}_1^{EN}+\mathfrak{d}_2^{EN}-\mathfrak{d}^{F^2}}{4} & \text{in II,}\\[2ex] \dfrac{\mathfrak{d}^{EN}-\mathfrak{d}^{F^2}}{4} & \text{in III,}\end{cases}$$

$$\mathfrak{S}=\frac{\mathfrak{d}_1^J-3\mathfrak{d}_2^J+\mathfrak{d}^{F^2}-2\mathfrak{d}^E}{8},\qquad \mathfrak{A}=\frac{\mathfrak{d}^{F^2}-\mathfrak{d}^{E^2}}{4},$$

$$\mathfrak{u}=\begin{cases}\dfrac{\mathfrak{d}^{F^2}+\mathfrak{d}^{E^2}+2(\mathfrak{d}_1^{EN}+\mathfrak{d}_2^{EN})-2\mathfrak{d}^F-2\mathfrak{d}^E}{8} & \text{in II,}\\[2ex] \dfrac{\mathfrak{d}^{F^2}+\mathfrak{d}^{E^2}+2\mathfrak{d}^{EN}-2\mathfrak{d}^F-2\mathfrak{d}^E}{8} & \text{in III.}\end{cases}$$

That these columns are rational integral follows from (5A) and the congruences $f_2^{EN}\equiv -3 \pmod 8$, $f_2^J\equiv -3\pmod{32}$. The inner products of these columns and the ones indicated are

(5.1)

	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{w}$	$\mathfrak{S}$	$\mathfrak{A}$	$\mathfrak{u}$	$\mathfrak{d}_1^J$	$\mathfrak{d}^{EN}$	$\mathfrak{d}_1^{EN}$	$\mathfrak{d}_2^{EN}$
$\mathfrak{a}$	4	0	0	1	0	0	0	0	0	0
$\mathfrak{b}$	0	4	0	−1	0	−2	0	0	0	0
$\mathfrak{w}$	0	0	3	−1	−2	0	0	4	2	2
$\mathfrak{S}$	1	−1	−1	4	2	1	0	0	0	0
$\mathfrak{A}$	0	0	−2	1	4	0	0	0	0	0
$\mathfrak{u}$	0	−2	0	1	0	3	0	4	2	2

where $\mathfrak{d}^{EN}$ occurs in III; $\mathfrak{d}_1^{EN},\mathfrak{d}_2^{EN}$ in II. By (5A),(iii) and the congruence

$\chi(E) \equiv \chi(E^2)$ (mod 2), it follows that $\mathfrak{A} \equiv \mathfrak{a}$ (mod 2). We note that $\mathfrak{a}$ and $\mathfrak{b}$ are orthogonal to the column $\chi(1)$ of degrees.

We now determine the entries of these columns. $\mathfrak{w}$ and $\mathfrak{u}$ have norm 3, and thus have 3 entries ± 1. $\mathfrak{a}, \mathfrak{b}, \mathfrak{S}, \mathfrak{A}$ have norm 4, and since $\mathfrak{a}\mathfrak{S} = 1$, $\mathfrak{b}\mathfrak{S} = -1$, each of these must have 4 entries ± 1. We can choose five characters χ such that by replacing χ by $-\chi$ if necessary, we have

$\mathfrak{w}$	$\mathfrak{A}$	$\mathfrak{a}$	$\mathfrak{b}$
1	0	0	b_1
1	-1	1	b_2
1	-1	-1	b_3
0	1	1	b_4
0	1	-1	b_5

By orthogonality $b_3 = b_4$, $b_2 = b_5$, $b_1 = -b_2 - b_3$. Suppose $b_i \neq 0$ for some $2 \leqq i \leqq 5$. Then one of $\chi_i(E), \chi_i(F)$ is ± 2, and the other is 0; say that $\chi_i(E) = \pm 2$, $\chi_i(F) = 0$. If χ_i has height 1, then by (5A), (ii) $\chi_i(F^2) \equiv \chi_i(E^2) \equiv \chi_i(EN) \equiv 2 \pmod 4$. The contribution to χ_i from E, F^2, E^2, EN is then 64, which is too large. If χ_i has height $\geqq 2$, then $\chi_i(F^2) \equiv \chi_i(E^2) \equiv 0 \pmod 4$. But (5A), (iii) implies $\chi_i(J) + \chi_i(F^2) \equiv 4 \pmod 8$ and the same congruence with the roles of E and F interchanged implies that $\chi_i(J) + \chi_i(E^2) \equiv 0 \pmod 8$. Thus one of $\chi_i(E^2), \chi_i(F^2)$ is nonzero, and the method of contribution again leads to a contradiction. The argument for the case $\chi_i(E) = 0$, $\chi_i(F) = \pm 2$ is similar. Thus $b_i = 0$ for $2 \leqq i \leqq 5$, and $b_1 = 0$ as well.

We now rearrange the characters in B so that χ_1 is the 1-character and the others are as indicated below:

(5.2)

$\mathfrak{b}$	$\mathfrak{a}$	$\mathfrak{A}$	$\mathfrak{w}$	$\mathfrak{u}$
1	0	0	0	0
1	0	0	0	-1
1	0	0	0	-1
1	0	0	0	0
0	1	-1	1	0
0	-1	-1	1	0
0	1	1	0	0
0	-1	1	0	0
0	0	0	1	0
0	0	0	0	1

The entries of $\mathfrak{u}$ are determined easily from (5.1). Since $\mathfrak{A}$ is known, the method of contributions implies that $(\mathfrak{d}^{E^2}, \mathfrak{d}^{F^2})_i = \pm(1,1)$ for $1 \leqq i \leqq 4$, and $(\mathfrak{d}^{E^2}, \mathfrak{d}^{F^2})_i = \pm(1,-3)$ or $\pm(-3,1)$ for $5 \leqq i \leqq 8$. Furthermore, knowledge of

$\mathfrak{u}$ and $\mathfrak{w}$ imply that $(\mathfrak{d}^{E^2},\mathfrak{d}^{F^2})_i=(-2,-2)$ for $i=9$, and $(2,2)$ for $i=10$. The signs of $(\mathfrak{d}^{E^2},\mathfrak{d}^{F^2})_i$ for $i=2,3,4$ can be determined by the equation $\mathfrak{u}\mathfrak{d}^{E^2}=4$. Since $\mathfrak{d}^{E^2},\mathfrak{d}^{F^2}$ have norm 32, each has exactly two ± 3's for $5 \leqq i \leqq 8$. The products $\mathfrak{w}\mathfrak{d}^{E^2}=0$, $\mathfrak{w}\mathfrak{d}^{F^2}=-8$ determine the signs completely. If the characters are arranged as in (5.2), then

F	E	E^2	F^2
1	1	1	1
1	1	−1	−1
1	1	−1	−1
1	1	1	1
1	−1	1	−3
−1	1	1	−3
1	−1	−3	1
−1	1	−3	1
0	0	−2	−2
0	0	2	2

.

In particular, χ_9,χ_{10} have height 1, and by (5A)(iii) χ_i has height $\geqq 3$ for $i \geqq 11$; these χ_i then actually have height 3 or 4 by [4].

The columns $\mathfrak{d}^{EN},\mathfrak{d}_1^{EN}+\mathfrak{d}_2^{EN}$ in cases II, III respectively are now completely determined from $\mathfrak{w}$ and $\mathfrak{d}^{F^2}$. In II the entries of $\mathfrak{d}_1^{EN},\mathfrak{d}_2^{EN}$ can be determined as follows: $(\mathfrak{d}_1^{EN}+\mathfrak{d}_2^{EN})_i=\pm 1$ for $1\leqq i\leqq 8$, 2 for $i=9,10$. Since $\mathfrak{d}_\rho^{EN}$ has norm 6, the nonzero entries are ± 1. The product $\mathfrak{u}\mathfrak{d}_1^{EN}=2$ shows that one of $(\mathfrak{d}_1^{EN})_2$, $(\mathfrak{d}_1^{EN})_3$ is -1 and the other is 0, since $(\mathfrak{d}_1^{EN})_{10}=(\mathfrak{d}_2^{EN})_{10}=1$. Since χ_2,χ_3 may be interchanged at this point, we may assume $(\mathfrak{d}_1^{EN})_2=-1$. From the equality $\mathfrak{b}\mathfrak{d}_1^{EN}=0$, we have $(\mathfrak{d}_1^{EN})_3=(\mathfrak{d}_1^{EN})_4=0$. This completely determines the entries under EN except for the arrangement $(\mathfrak{d}_1^{EN},\mathfrak{d}_2^{EN})_i$ for $5\leqq i\leqq 8$. Here (1,0) can occur for $i=5$ and 8, or for $i=6$ and 7; the remaining entries are $(0,1)$. This point will be settled below.

Let $s_i=(\mathfrak{S})_i$. Then $\mathfrak{S}\mathfrak{b}=-1$, $\mathfrak{S}\mathfrak{u}=1$ imply that $s_2+s_3+s_4=-1$, $-s_2-s_3+s_{10}=1$, so that $s_4=-s_{10}$. Also $\mathfrak{S}\mathfrak{a}=1$, $\mathfrak{S}\mathfrak{A}=1$ imply that $s_5=s_8$ and $s_7-s_6=1$. In particular, one of the numbers s_6,s_7 is ± 1, and the other is 0. The quadratic form Q^J is $10u^2+2v^2+(u-v)^2$. The method of contribution then implies the following: If χ_i has height 0, then $(\mathfrak{d}_1^J,\mathfrak{d}_2^J)_i$, up to a sign change, can only be (1,0), (01), (1,2), $(-1,2)$, (0,3), and for $5\leqq i\leqq 8$, only the first three are possible. If χ_i has height 1, then only $(1,1)$, (0,2) are possible; if χ_i has height 3, only (1,3) is possible. If χ_i has height 4, the method of contribution yields a contradiction. Since $s_i=0$ or ± 1, the definition of $\mathfrak{S}$ forces the conclusion $(\mathfrak{d}_1^J,\mathfrak{d}_2^J)_i=(1,0)$ for $i=5$ and 8; thus $s_5=s_8=0$. Similarly, $(\mathfrak{d}_1^J,\mathfrak{d}_2^J)_i=(0,1)$ or $(-1,-2)$ for $i=6,7$, and the latter can occur only in III by the method of contribution. Thus, if $s_6=-1$, $s_7=0$, then $(\mathfrak{d}_1^J,\mathfrak{d}_2^J)_i=(0,1)$; if

$s_6 = 0$, $s_7 = 1$, then $(\mathfrak{d}_1^J, \mathfrak{d}_2^J)_i = (-1, -2)$. We call these two possibilities IIIa, IIIb respectively. Suppose $s_4 = 0$. Then one of $s_2, s_3 = \pm 1$, and the other is 0. There must then be characters χ_{11}, χ_{12} in B such that $s_{11} \neq 0$, $s_{12} \neq 0$. For $i = 11, 12$, $(\mathfrak{d}_1^J, \mathfrak{d}_2^J)_i = \pm(1,3)$, and since $\mathfrak{d}_1^J$ has norm 6, $(\mathfrak{d}_1^J)_i = 0$ for $i = 9$ or 10. But this contradicts the fact that $\mathfrak{d}_2^J$ has norm 22. Thus $s_4 \neq 0$, and we easily see that $s_4 = -1$, $s_{10} = 1$, $s_2 = s_3 = 0$. s_9 can be found from $\mathfrak{S}\mathfrak{w} = -1$. If $s_9 = 0$, B contains one more character χ_{11} for which $s_{11} = 1$. The matrix of decomposition numbers can now be completed, the uncertainty remaining in II under EN being settled from $\mathfrak{d}_1^J \mathfrak{d}_1^{EN} = 0$. We omit the details.

The complete matrices are in cases II, IIIa, IIIb respectively

(5.3)

F	E	F^2	E^2	EN		J		1		
1	1	1	1	1	0	1	0	1	0	0
1	1	−1	−1	−1	0	0	−1	0	2	1
1	1	−1	−1	0	−1	0	−1	−1	−1	−1
1	1	1	1	0	1	−1	2	0	−1	0
1	−1	−3	1	0	1	1	0	0	−1	0
−1	1	−3	1	1	0	0	1	0	0	1
1	−1	1	−3	1	0	0	1	0	0	1
−1	1	1	−3	0	1	1	0	0	−1	0
0	0	−2	−2	1	1	−1	−1	0	1	−1
0	0	2	2	1	1	0	−2	−1	1	0
0	0	0	0	0	0	−1	−3	1	−2	1

The matrix of Cartan invariants of B is

$$\begin{bmatrix} 4 & -2 & 2 \\ -2 & 14 & 0 \\ 2 & 0 & 6 \end{bmatrix}.$$

If f_1, f_2, f_3 are the degrees of the corresponding basic set, then $f_1 = 1$, $f_2 \equiv -9 \pmod{32}$, $f_3 \equiv -11 \pmod{32}$.

(5.4)

F	E	F^2	E^2	EN	J		1			
1	1	1	1	1	1	0	1	0	0	0
1	1	−1	−1	−1	0	−1	0	1	2	1
1	1	−1	−1	−1	0	−1	−1	−1	−1	−1
1	1	1	1	1	−1	2	0	0	−1	0
1	−1	−3	1	1	1	0	0	0	−1	0
−1	1	−3	1	1	0	1	0	0	0	1
1	−1	1	−3	1	0	1	0	0	0	1
−1	1	1	−3	1	1	0	0	0	−1	0
0	0	−2	−2	2	−1	−1	0	0	1	−1
0	0	2	2	2	0	−2	−1	0	1	0
0	0	0	0	0	−1	−3	1	0	−2	1

.

The matrix of Cartan invariants is

$$\begin{bmatrix} 4 & 1 & -2 & 2 \\ 1 & 2 & 3 & 2 \\ -2 & 3 & 14 & 0 \\ 2 & 2 & 0 & 6 \end{bmatrix}.$$

$f_1 = 1$, $f_2 \equiv 32 \pmod{64}$, $f_3 \equiv 7 \pmod{64}$, $f_4 \equiv -11 \pmod{32}$.

(5.5)

F	E	F^2	E^2	EN	J		1		
1	1	1	1	1	1	0	1	0	0
1	1	−1	−1	−1	0	−1	0	1	−1
1	1	−1	−1	−1	0	−1	0	−1	−1
1	1	1	1	1	−1	2	−1	0	2
1	−1	−3	1	1	1	0	−1	0	2
−1	1	−3	1	1	−1	−2	0	0	1
1	−1	1	−3	1	−1	−2	0	0	1
−1	1	1	−3	1	1	0	−1	0	2
0	0	−2	−2	2	0	2	1	0	−3
0	0	2	2	2	0	−2	0	0	−2

The Cartan matrix is

$$\begin{bmatrix} 5 & 0 & -9 \\ 0 & 2 & 0 \\ -9 & 0 & 29 \end{bmatrix}.$$

$f_1 = 1$, $f_2 \equiv 0 \pmod{32}$, $f_3 \equiv 29 \pmod{64}$.

6. We now use the methods of [2] to complete the investigations of cases II and III. We recall the following facts: Let $\mathfrak{G}$ be a finite group of even order g. Let p be a prime, and P a p-element of $\mathfrak{G}$. Let $\tilde{\mathfrak{G}}$ be a subgroup of order $\tilde{g}$ such that $\tilde{\mathfrak{G}} \geqq \mathfrak{C}^*(P) = \langle G \in \mathfrak{G} \mid G^{-1}PG = P^{\pm 1} \rangle$. If J_α and J_β are two involutions of $\mathfrak{G}$, and $\{\phi^P_\rho\}$ is a basic set for a p-block of $\mathfrak{C}(P)$, then

$$g \sum \chi_\mu(J_\alpha)\chi_\mu(J_\beta)d^P_{\mu\rho}/x_\mu = \tilde{g}c(J_\alpha)c(J_\beta) \sum h_{\mu\alpha}h_{\mu\beta}\tilde{d}^P_{\mu\rho}/\tilde{x}_\mu. \tag{6.1}$$

Here on the left χ_μ runs over the irreducible characters of the block B of $\mathfrak{G}$ corresponding to the block b of $\mathfrak{C}(P)$, $x_\mu = \chi_\mu(1)$, and $d^P_{\mu\rho}$ are the corresponding generalized decomposition numbers. On the right, $h_{\mu\alpha} = \sum_\lambda \tilde{\chi}_\mu(\tilde{J}_{\alpha,\lambda})/\tilde{c}(\tilde{J}_{\alpha,\lambda})$, $\tilde{\chi}_\mu$ runs over characters of the block $\tilde{B}$ of $\tilde{\mathfrak{G}}$ corresponding to b, $\tilde{x}_\mu = \tilde{\chi}_\mu(1)$, $\tilde{d}^P_{\mu\rho}$ are the corresponding generalized decomposition numbers, and $\{\tilde{J}_{\alpha,\lambda}\}$ ranges over a set of representatives of the conjugate classes of $\tilde{\mathfrak{G}}$ contained in the conjugate class of J_α in $\mathfrak{G}$. For notational convenience, we will let $L(J_\alpha, J_\beta, \mathfrak{d}^P_\rho)$, $R(J_\alpha, J_\beta, \mathfrak{d}^P_\rho)$ denote the left-hand side, the right-hand side of (6.1) respectively.

In the applications to follow, we will always take $p=2$ and $\mathfrak{b}$ the 1-block of $\mathfrak{C}(P)$. It then follows that B and $\tilde{B}$ are the 1-blocks of $\mathfrak{G}$ and $\tilde{\mathfrak{G}}$ respectively. As a second remark, we note that if $\tilde{\mathfrak{G}}$ has a normal 2-complement, then the characters $\tilde{\chi}_\mu$ in the 1-block of $\tilde{\mathfrak{G}}$ can be identified with the irreducible characters θ_μ of an S_2-subgroup $\mathfrak{Q}$ of $\tilde{\mathfrak{G}}$. Moreover, if J_α, J_β, P are in $\mathfrak{Q}$, then $c(J_\alpha)^{-1}c(J_\beta)^{-1}R(J_\alpha, J_\beta, \mathfrak{b}_1^P)$ is equal to

$$\tilde{g} \sum_\mu \sum_\lambda \frac{\theta_\mu(\tilde{J}_{\alpha,\lambda})}{\tilde{c}(\tilde{J}_{\alpha,\lambda})} \sum_\nu \frac{\theta_\mu(\tilde{J}_{\beta,\nu})}{\tilde{c}(\tilde{J}_{\beta,\nu})} \frac{\tilde{d}^P_{\mu 1}}{\theta_\mu(1)}$$

$$(6.2) \qquad = \tilde{g} \sum_{\lambda,\nu} \sum_\mu \frac{\theta_\mu(\tilde{J}_{\alpha,\lambda})\theta_\mu(\tilde{J}_{\beta,\nu})\theta_\mu(P)}{\theta_\mu(1)c_{\mathfrak{Q}}(\tilde{J}_{\alpha,\lambda})c_{\mathfrak{Q}}(\tilde{J}_{\beta,\nu})} \frac{c_{\mathfrak{Q}}(\tilde{J}_{\alpha,\lambda})c_{\mathfrak{Q}}(\tilde{J}_{\beta,\nu})}{\tilde{c}(\tilde{J}_{\alpha,\lambda})\tilde{c}(\tilde{J}_{\beta,\nu})}$$

$$= (\tilde{\mathfrak{G}}:\mathfrak{Q}) \sum_{\lambda,\nu} a_{\mathfrak{Q}}(\tilde{J}_{\alpha,\lambda}, \tilde{J}_{\beta,\nu}, P) \frac{c_{\mathfrak{Q}}(\tilde{J}_{\alpha,\lambda})c_{\mathfrak{Q}}(\tilde{J}_{\beta,\nu})}{\tilde{c}(\tilde{J}_{\alpha,\lambda})\tilde{c}(\tilde{J}_{\beta,\nu})}$$

where $a_{\mathfrak{Q}}(\tilde{J}_{\alpha,\lambda}, \tilde{J}_{\beta,\nu}, P)$ is the multiplicity of the class sum of P in $\mathfrak{Q}$ in the product of the class sums of $\tilde{J}_{\alpha,\lambda}$ and $\tilde{J}_{\beta,\nu}$. We assume in this that the elements $\tilde{J}_{\alpha,\lambda}$ and $\tilde{J}_{\beta,\nu} \in \mathfrak{Q}$. Finally, we note that (6.1) can be added over linear combinations of the $d^P_{\mu\rho}$ for varying $\tilde{\mathfrak{G}}, P$, and ρ. If $\mathfrak{y}$ is such a combination of the $\mathfrak{b}^P_\rho$ we understand by the equality $L(J_\alpha, J_\beta, \mathfrak{y}) = R(J_\alpha, J_\beta, \mathfrak{y})$ the result obtained by first applying (6.1) to the various $\mathfrak{b}^P_\rho$, and then summing appropriately. We now turn to the situation at the end of §5.

Case III. Set $\beta = f_2^J$, $\beta \equiv -3 \pmod{32}$. If we set $\tilde{\mathfrak{G}} = \mathfrak{C}^*(F)$ and $\mathfrak{C}^*(E)$, and compute $L(J,J,\mathfrak{b}) = R(J,J,\mathfrak{b})$, and $L(J,EN,\mathfrak{b}) = R(J,EN,\mathfrak{b})$, we find that

$$(6.3) \qquad \begin{aligned} 1 + \frac{\beta^2}{x_2} + \frac{\beta^2}{x_3} + \frac{(2\beta-1)^2}{x_4} &= 0, \\ 1 + \frac{\beta}{x_2} + \frac{\beta}{x_3} + \frac{2\beta-1}{x_4} &= 0. \end{aligned}$$

Here the right-hand sides are computed by observing that $\mathfrak{C}^*(E)$, $\mathfrak{C}^*(F)$ have normal 2-complements, and that E, F do not occur in III in the appropriate product of involutions. Subtracting the second from the first, and cancelling $\beta - 1$, which is permissible since $\beta \equiv -3 \pmod{32}$, we have

$$(6.4) \qquad \frac{\beta}{x_2} + \frac{\beta}{x_3} + 2\frac{2\beta-1}{x_4} = 0.$$

Substituting (6.4) into (6.3) then yields $1 - (2\beta-1)/x_4 = 0$, or $x_4 = 2\beta - 1$. Thus J is in the kernel of χ_4. By (6.3) $\beta/x_2 + \beta/x_3 + 2 = 0$. Since $\chi_2(J) = \chi_3(J) = -\beta$, and $|\beta| \leqq |x_2|, |x_3|$, we see that $x_2 = x_3 = -\beta$, and hence J belongs to the kernel of χ_i for $1 \leqq i \leqq 4$.

In IIIb, $x_2 = f_2 - f_3$, $x_3 = -f_2 - f_3$; thus $f_2 = 0, f_3 = \beta$. But $\chi_6(J) = -1-2\beta$, and $x_6 = \beta$. Since $|1+2\beta| \leqq |\beta|$, we must have $\beta = -1$, which contradicts the congruence $\beta \equiv -3 \pmod{32}$. Thus IIIb is impossible. We henceforth assume we have IIIa. In this case, $\chi_4(J) = x_4$ implies that $f_3 = 1 - 2\beta$.

If $\tilde{\mathfrak{G}} = \mathfrak{C}^*(EN), \mathfrak{C}^*(F^2)$ respectively, and we compute $L(J,J,\mathfrak{w}) = R(J,J,\mathfrak{w})$, then

$$\frac{1}{x_5} + \frac{\beta^2}{x_6} + \frac{(1+\beta)^2}{x_9} = 0. \tag{6.5}$$

Here the right-hand side is computed by noting that $\mathfrak{C}^*(EN)$, $\mathfrak{C}^*(F^2)$ have normal 2-complements, and by using (6.2). If we substitute $x_5 = -f_3$, $x_6 = f_4$, $x_9 = f_3 - f_4$ into (6.5) and simplify, we obtain the equality $f_4 + \beta f_3 = 0$, so that $f_4 = 2\beta^2 - \beta$. The equality $\chi_2(J) = x_2$ implies $f_2 = -2(\beta-1)^2$. Summarizing, we have

$$f_1 = 1,\ f_2 = -2(\beta-1)^2,\ f_3 = 1 - 2\beta,\ f_4 = \beta(2\beta - 1).$$

Let $\mathfrak{K} = \bigcap$ kernel of χ_i for $i = 1,2,3,4$. Since $J \in \mathfrak{K}, \mathfrak{K}$ must contain the subgroup $\mathfrak{A} = \langle J, X, EF^3\rangle$ of $\mathfrak{P}$ generated by the elements of $\mathfrak{P}$ conjugate in $\mathfrak{G}$ to J. $\mathfrak{A}$ is abelian of type $(2,2,2)$. Since F^2, $N \notin \mathfrak{K}$, $\mathfrak{A}$ is an S_2-subgroup of $\mathfrak{K}$. Assume now that $\mathfrak{G}$ has no normal $2'$-subgroups $\neq 1$. Let $\mathfrak{N}$ be a minimal normal subgroup of $\mathfrak{G}$ contained in $\mathfrak{K}$. Since $|\mathfrak{N}|$ is even, $\mathfrak{A} \leqq \mathfrak{N}$.

Suppose $\mathfrak{A} \neq \mathfrak{N}$. Since $\mathfrak{N}$ is characteristically simple and $\mathfrak{A}$ is an S_2-subgroup of $\mathfrak{N}$, it follows that $\mathfrak{N}$ is simple. Hence $\mathfrak{W} = \mathfrak{N}_{\mathfrak{N}}(\mathfrak{A})/\mathfrak{C}_{\mathfrak{N}}(\mathfrak{A})$ has order $7 \cdot 3^x$ with $x = 0$ or 1. Clearly $\mathfrak{P}$ stabilizes $\mathfrak{W}$, so we may view $\mathfrak{P}/\mathfrak{A}$ as a group of operators of $\mathfrak{W}$. If $P \in \mathfrak{P}$ and $P\mathfrak{A}$ centralizes $\mathfrak{W}$, then $\mathfrak{W}$ leaves $\mathfrak{A} \cap \mathfrak{C}(P)$ invariant. Since $\mathfrak{A}$ is an irreducible $\mathfrak{W}$-group, it follows that $\mathfrak{A} \leqq \mathfrak{C}(P)$, so $P \in \mathfrak{P} \cap \mathfrak{C}(\mathfrak{A}) = \mathfrak{A}$. Thus $\mathfrak{P}/\mathfrak{A}$ is faithfully represented on $\mathfrak{W}$. This is impossible, since $|\mathfrak{P} : \mathfrak{A}| = 8$ and $|\mathfrak{W}|$ divides $3 \cdot 7$. Thus $\mathfrak{A} = \mathfrak{N}$.

Since $\mathfrak{A}$ is a self-centralizing normal subgroup of $\mathfrak{P}$, it follows that $\mathfrak{C}(\mathfrak{A}) = \mathfrak{A} \times \mathfrak{D}$, where $\mathfrak{D}$ has odd order. Hence $\mathfrak{D}$ char $\mathfrak{C}(\mathfrak{A}) \lhd \mathfrak{G}$, so $\mathfrak{D} = 1$. Thus $\mathfrak{G}/\mathfrak{A}$ is isomorphic to a subgroup of $GL(3,2)$ of order $\equiv 0 \pmod 8$ which has no subgroup of index 2. Hence $\mathfrak{G}/\mathfrak{A} \simeq GL(3,2)$. The group $\mathfrak{G}$ exists and is unique by [11].

Case II. Set $\alpha = f_2^{EN}$, $\beta = f_2^{J}$; $\alpha \equiv -3 \pmod 8$, $\beta \equiv -3 \pmod{32}$. If we take $\tilde{\mathfrak{G}} = \mathfrak{C}^*(E)$, $\mathfrak{C}^*(F)$ and compute $L(J,J,\mathfrak{b}) = R(J,J,\mathfrak{b})$, and $L(EN,EN,\mathfrak{b}) = R(EN,EN,\mathfrak{b})$, we find that

$$1 + \frac{\beta^2}{x_2} + \frac{\beta^2}{x_3} + \frac{(2\beta-1)^2}{x_4} = 0,$$

$$1 + \frac{1}{x_2} + \frac{\alpha^2}{x_3} + \frac{\alpha^2}{x_4} = 0.$$

The right-hand sides are 0 by observing that $\mathfrak{C}^*(F)$, $\mathfrak{C}^*(E)$ have normal 2-complements, and that in II, E, F do not occur in the appropriate products of involutions. Expressing the degrees x_i in terms of $1 = f_1, f_2, f_3$ and simplifying, we get

$$\alpha^2 - \frac{f_2(1+f_2+f_3)}{2f_2+f_3} = 0, \tag{6.6}$$

$$\beta^2(f_2-\alpha^2+4(1+f_2+f_3)) - 4\beta(1+f_2+f_3) - (1+f_2+f_3)(f_2-1) = 0, \tag{6.7}$$

(6.6) and (6.7) can be used to eliminate f_3; a little manipulation then gives the equation

$$f_2^2(\beta^2-\alpha^2) + 2\alpha^2 f_2(\beta-1)^2 + \alpha^2(\alpha^2\beta^2-(2\beta-1)^2) = 0. \tag{6.8}$$

If $\alpha^2 \neq \beta^2$, then the above equation factors into $(\beta^2-\alpha^2)(f_2-\lambda)(f_2-\mu)=0$, where

$$\lambda = \frac{\alpha-2\alpha\beta-\alpha^2\beta}{\beta+\alpha}, \quad \mu = \frac{-\alpha+2\alpha\beta-\alpha^2\beta}{\beta-\alpha}. \tag{6.9}$$

If $\alpha^2 = \beta^2$, then $\alpha = \beta$ from the congruences $\alpha \equiv -3 \pmod 8$, $\beta \equiv -3 \pmod{32}$. In this case, $f_2 = -(\alpha^2+2\alpha-1)/2$.

If we take $\tilde{\mathfrak{G}} = \mathfrak{C}^*(F^2)$, $\mathfrak{C}^*(EN)$, and compute $L(J,J,\mathfrak{w}) = R(J,J,\mathfrak{w})$, we have

$$\frac{g}{c(J)^2}\left[\frac{(1+\beta)^2}{f_2-f_3} - \frac{1}{f_2} + \frac{\beta^2}{f_3}\right] = \frac{-c(F^2)}{c(F^2,N)^2},$$

or

$$g = -c(J)^2 \; \frac{c(F^2)}{c(F^2,N)^2}\,\frac{f_2f_3(f_2-f_3)}{(\beta f_2+f_3)^2}. \tag{6.10}$$

Apply now the methods at the beginning of this section to the situation $\mathfrak{G} = \mathfrak{C}(J)$, $\tilde{\mathfrak{G}} = \mathfrak{C}^*(F^2)$, and $L(X,X,\mathfrak{d}^{F^2}) = R(X,X,\mathfrak{d}^{F^2})$. Using (4.7), we see that $L(X,X,\mathfrak{d}^{F^2}) = 2c(J)(\beta+3)^2/\beta(\beta+1)$. On the other hand, in $\mathfrak{C}(J)$ X is fused only to EF, and $(\mathrm{ccl}(X)\cup\mathrm{ccl}(EF))^2$ does not involve F^2. Thus $R(X,X,\mathfrak{d}^{F^2}) = 0$. and we must have $\beta = -3$. This already shows that $\alpha \neq \beta$; otherwise, $f_2 = -1$, whereas $f_2 \equiv -9 \pmod{32}$. Hence $f_2 = \lambda$ or μ of (6.9). If $f_2 = \lambda$, then $\alpha - 2\alpha\beta - \alpha^2\beta \equiv 0 \pmod{\beta+\alpha}$, and $\alpha+\beta$ divides $\beta(1-\beta)^2$. If $f_2 = \mu$, then $-\alpha+2\alpha\beta-\alpha^2\beta \equiv 0 \pmod{\beta-\alpha}$, and $\alpha-\beta$ divides $\beta(1-\beta)^2$. In either case, $\alpha \pm 3$ divides 48. Only a small number of possibilities can occur for α, and since $f_2 \equiv -9, f_3 \equiv -11 \pmod{32}$, a check of these shows that only the following solution exists:

$$\alpha = 5, \quad \beta = -3, \quad f_2 = 55, \quad f_3 = -11.$$

The degrees of the characters in B are then 1, 55, 55, 55, 11, 11, 99, 45, 66, 54, 120. In particular, $\mathfrak{G}$ has a rational character χ_6 of degree 11 faithful on $\mathfrak{P}$. Assume now that $\mathfrak{G}$ has no normal $2'$-subgroups $\neq 1$. Then by a theorem of Schur's, the order g of $\mathfrak{G}$ divides $2^6\cdot 3^6\cdot 5^2\cdot 7\cdot 11$.

The characters in the 1-block of $\mathfrak{C}(J)/\langle J\rangle$ have degrees 1, 1, 3, 3, 3, 3, 3, 3, 6, 2 by (4.7). Let $\theta = \theta_j$, for some j where $3 \leqq j \leqq 8$. If $\mathfrak{K}/\langle J\rangle$ is the kernel of θ, then for a suitable choice of j, the only nontrivial elements of $\mathfrak{P}/\langle J\rangle$ in $\mathfrak{K}/\langle J\rangle$ are the elements in the class of e^2. Since θ is a rational character, $(\mathfrak{C}(J):\mathfrak{K})$ is of the form $2^s 3^t$, so that $\mathfrak{C}(J)/\mathfrak{K}$ is solvable. If we now choose θ so that the only nontrivial elements of $\mathfrak{P}/\langle J\rangle$ in the kernel $\mathfrak{K}_1/\langle J\rangle$ of θ are the elements in the class of f^2, then a similar argument shows that $\mathfrak{C}(J)/\mathfrak{K}_1$ is solvable of order $2^{s'}3^{t'}$. But $\mathfrak{K} \cap \mathfrak{K}_1 \cap \mathfrak{P} = \langle J\rangle$. It now follows that if $\mathfrak{M}$ is the maximal normal $2'$-subgroup of $\mathfrak{C}(J)$, then $\mathfrak{C}(J)/\mathfrak{M}$ is solvable, and its order is of the form $2^a 3^b$. Since $\mathfrak{C}(J)/\mathfrak{M}$ has only one block for the prime 2 by [5], the order of $\mathfrak{C}(J)/\mathfrak{M}$ is then 192. Set $m = |\mathfrak{M}|$.

The values of α, β, f_2, f_3, and (6.10) show that the order of $\mathfrak{G}$ is

$$g = 2^5 \cdot 3^3 \cdot 5 \cdot 11 m \frac{m}{c(F^2, N)} \frac{c(F^2)}{c(F^2, N)}. \tag{6.11}$$

We note that $c(F^2,N) \mid c(F^2)$, and $c(F^2,N) \mid 64m$, the latter being true, since no 3-element of $\mathfrak{C}(J)/\mathfrak{M}$ commutes with N. In particular, $3^4 \nmid m$ since $g \mid 2^6 \cdot 3^6 \cdot 5^2 \cdot 7 \cdot 11$.

Suppose p divides m, where $p = 7$ or 5. Since $7^2 \nmid g$, $5^3 \nmid g$, (6.11) implies that $p \mid c(F^2, N)$. Thus there exists an element Y in $\mathfrak{M} \cap \mathfrak{C}(F^2)$ of order p. In particular, by (5.3) $\chi_6(JY) = \chi_6(F^2Y) = 3$ and so $\chi_6(Y) \equiv 3 \pmod 4$. Since $\chi_6(Y)$ can assume only the value 4 for $p = 7$, and the values 6 or 1 for $p = 5$, this is impossible. Thus $m \mid 27$ and $g \mid 2^6 \cdot 3^6 \cdot 5 \cdot 11$.

Let S be an element in $\mathfrak{G}$ of order 11, and let $\mathfrak{S} = \langle S\rangle$. If $\mathfrak{N}(\mathfrak{S}) = \mathfrak{C}(\mathfrak{S})$, then $\mathfrak{G}$ would have a normal 11-complement. In particular, $\mathfrak{S}$ would normalize an S_2-subgroup $\mathfrak{P}_1$ of $\mathfrak{G}$ and hence centralize the central involution of $\mathfrak{P}_1$, which is impossible. Thus $\mathfrak{N}(\mathfrak{S}) \neq \mathfrak{C}(\mathfrak{S})$. The order of $\mathfrak{N}(\mathfrak{S})/\mathfrak{C}(\mathfrak{S})$ is necessarily a divisor $\neq 1$ of 10. The index $(\mathfrak{G}:\mathfrak{N}(\mathfrak{S}))$ is then of the form $32 \cdot 5 \cdot 3^\alpha$, $32 \cdot 3^\alpha$, or $64 \cdot 3^\alpha$, where $0 \leqq \alpha \leqq 6$. By Sylow's theorem, this index is $\equiv 1 \pmod{11}$, and thus must be $64 \cdot 3^3$. If $m \neq 1$, then there would exist an element T of order 3 in $\mathfrak{C}(S)$. Since $\chi_6(ST) \equiv \chi_6(T) \pmod{11}$ and $\chi_6(ST) = 0$, we would have $\chi_6(T) \equiv 0 \pmod{11}$ and this is impossible. Thus $m = 1$.

We have now shown that $g = 2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95{,}040$. Suppose $\mathfrak{G}$ has proper normal subgroups; among these choose $\mathfrak{N}$ minimal. If $\mathfrak{G}/\mathfrak{N}$ has even order, then there would exist an irreducible character $\neq 1$ in the 1-block of $\mathfrak{G}/\mathfrak{N}$ which would then belong to the 1-block B of $\mathfrak{G}$. But this is impossible, since the nontrivial characters in B are faithful. If $\mathfrak{G}/\mathfrak{N}$ has odd order, then $\mathfrak{P}$ is an S_2-subgroup of $\mathfrak{N}$. If $\mathfrak{N}$ has no subgroups of index 2, then $\mathfrak{N}$ has necessarily two classes of involutions, and the preceding work shows that $\mathfrak{N}$ has order 95,040. Hence $\mathfrak{N}$ is solvable, and $\mathfrak{N} = \mathfrak{P}$. which is impossible. Thus $\mathfrak{C}$ is simple. By a theorem of Stanton [10], $\mathfrak{G}$ must be the Mathieu group $\mathfrak{M}_{12}$. Summarizing the results of this paper, we have

THEOREM (6A). *Let $\mathfrak{G}$ be a finite group of order $64g'$, where g' is odd. Suppose there is an element F of order* 8 *in $\mathfrak{G}$ such that F is self-centralizing in some S_2-subgroup $\mathfrak{P}$, and F is conjugate to its odd powers in $\mathfrak{P}$. Then one of the following possibilities hold:*

(a) $\mathfrak{G}$ *has a subgroup of index* 2.

(b) $\mathfrak{G}$ *has one class of involutions.*

(c) *If* $O_{2'}(\mathfrak{G})$ *is the maximal normal subgroup of* $\mathfrak{G}$ *of odd order, then* $\mathfrak{G}/O_{2'}(\mathfrak{G}) \simeq \mathfrak{G}_{1344}$ *or* $\mathfrak{M}_{12}$, *where* $\mathfrak{G}_{1344}$ *is a uniquely specified nonsimple, nonsolvable group of order* 1344, *and* $\mathfrak{M}_{12}$ *is the Mathieu group on* 12 *symbols.*

COROLLARY (6B). *The only simple group satisfying the assumptions of* (6A) *and having more than one class of involutions is* $\mathfrak{M}_{12}$.

REFERENCES

1. R. Brauer, *A characterization of the characters of groups of finite order*, Ann. of Math. (2) **57** (1953), 357–377.

2. ———, *Investigations on groups of even order*. I, Proc. Nat. Acad. Sci. U. S. A. **47** (1961), 1891–1893.

3. ———, *Some applications of the theory of blocks of characters of finite groups*. I, J. Algebra **1** (1964), 152–167.

4. 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. **45** (1959), 361–365.

5. P. Fong, *On the characters of p-solvable groups*, Trans. Amer. Math. Soc. **98** (1961). 263–284.

6. G. Frobenius, *Über die Charaktere der mehrfach transitiven Gruppen*, S-B. Preuss. Akad. Wiss. (Berlin) (1904), 558–571.

7. M. Hall and J. Senior, *The groups of order* 2^n $(n \leqq 6)$, Macmillan, New York, 1964,

8. P. Hall and G. Higman, *On the p-length of p-soluble groups*, Proc. London Math. Soc, **6** (1956), 1–42.

9. I. Schur, *Über eine Klasse von endlichen Gruppen linearer Substitutionen*, S-B. Preuss. Akad Wiss. (Berlin) (1905), 77–91.

10. R. Stanton, *The Mathieu groups*, Canad. J. Math. 3 (1951), 164–174.

11. W. J. Wong, *A characterization of the Mathieu group* M_{12}, Math. Z. **84** (1964), 378–388.

12. H. Zassenhaus, *The theory of groups*, Chelsea, New York, 1949.

HARVARD UNIVERSITY,
CAMBRIDGE, MASSACHUSETTS
UNIVERSITY OF CALIFORNIA,
BERKELEY, CALIFORNIA