J. Math. Soc. Japan
Vol. 20, No. 4, 1968

Finite simple groups with short chains of subgroups

By Koichiro HARADA

(Received March 25, 1968)

§ 1. Introduction.

Let G be a finite group. Let $G=G_0>G_1>\cdots>G_n=1$ be a chain of subgroups of G, where G_i is a proper subgroup of G_{i-1} $(1\leqq i\leqq n)$. Then we say that the chain has length n. For a fixed group G we denote by $l(G)$ the maximal number of n, where the chain ranges all possible ones. We call $l(G)$ the length of G.

In his papers [**16**], [**17**] Z. Janko has proved that if G is a finite non-abelian simple group whose length $l(G)$ is at most four, then G is isomorphic to $PSL(2, p)$ for some prime p. Moreover, he has proved that if $l(G)$ is at most five, then G is isomorphic to $PSL(2, q)$ for some prime power q.

In this note we shall prove the following extention of the above theorem of Z. Janko.

THEOREM 1. *Let G be a finite non-abelian simple group whose length $l(G)$ is at most seven. Then G is isomorphic to one of the following groups:*

(1) *$PSL(2, q)$, for a suitable prime power q,*

(2) *$PSU(3, 3^2)=U_3(3)$, $PSU(3, 5^2)=U_3(5)$,*

(3) *A_7 the alternating group of degree seven,*

(4) *M_{11} the Mathieu group of degree* 11,

(5) *J the Janko group of order* 175560 [**18**].

The proof of the theorem proceeds by considering the structure of centralizers of involutions and the Sylow 2-subgroups of G. Assuming that there exists a simple group G which is not isomorphic to any one of the groups mentioned above, we are able to prove that the order of the Sylow 2-subgroups of G has to be at least 2^7, which is clearly contrary to our hypothesis $l(G)\leqq 7$.

J. G. Thompson has conjectured in [**23**] that if the Sylow 2-subgroup S of a finite simple group G is maximal in G, then S should be dihedral. We shall prove that this conjecture is true if the order of S is less than or equal to 64 (Lemma 7).

In the last section of this note, we shall prove some elementary lemmas on the Sylow 2-subgroups of finite groups. For instance we shall show the following lemma.

LEMMA. *If a Sylow 2-subgroup S of a finite group G is generalized* *dihedral, then G has a normal subgroup of index 2 or S is the direct product of a dihedral group with an elementary abelian group.*

Our notation is fairly standard.

G' ………… the commutator subgroup of a group G.

$K(G)$ ……… the maximal normal subgroup of odd order of G.

$Z(G)$ ……… the center of G.

$Z^*(G)$ ……… the preimage of $Z(G/K(G))$ in G.

$D(G)$ ……… the Frattini subgroup of G.

$G^\#$ ………… the set of non-identity elements of G.

$\langle a, b, \cdots\rangle$ …… the group generated by the elements $a, b, \cdots$.

Z_n ………… a cyclic group of order n.

D_n ………… a dihedral group of order n.

$H < G$ ……… H is a proper subgroup of G.

$H \lhd G$ ……… H is a normal subgroup of G.

$x \overset{G}{\sim} y$ ……… an element x is conjugate with y in G.

Let H be a subgroup of a finite group G. If two elements x, y of H are conjugate to one another in G, then we often say that x is fused with y in G. A central involution is an element of order 2 which is contained in the center of a Sylow 2-subgroup of G. If an element x of a subgroup H of G is not fused with any element $(\neq x)$ of H in G, then we call x an isolated element in H. The abbreviation S_p-subgroup stands for Sylow p-subgroup. All groups considered will be finite.

We shall use frequently the following recent result of P. Fong [7].

THEOREM 2. *Let S be a 2-group of order 64. If S appears as an S_2-subgroup of a simple group, then S is isomorphic to one of the following groups:*

1. *a dihedral group,*
2. *a semi-dihedral group,*
3. *an S_2-subgroup of the Mathieu group M_{12} of degree 12,*
4. *a group of exponent 4 or*
5. *a direct product of a four-group $Z_2 \times Z_2$ with a semi-dihedral group of order 16.*

Moreover if $|S| \leqq 32$, then only the following four groups can appear as S_2-subgroups of simple groups.

1. *an elementary abelian group,*
2. *a dihedral group,*
3. *a semi-dihedral group or*
4. *a wreath product $Z_4 \wr Z_2$.*

§ 2. Proof of Theorem.

Let G be a finite non-abelian simple group all of whose chains of subgroups have length at most seven, i.e. $l(G) \leqq 7$. We shall then prove that G is isomorphic to one of the groups: $PSL(2, q)$, $U_3(3)$, $U_3(5)$, A_7, M_{11} or J. First we note that the groups mentioned above satisfy the condition $l(G) \leqq 7$ if we choose a suitable prime power q. This is checked by direct computation. The proof of our theorem proceeds by induction.

By way of contradiction we assume that

(A) *G is not isomorphic to any one of the simple groups mentioned above.* In particular we may assume that an S_2-subgroup of G is not dihedral by a theorem of D. Gorenstein and J. Walter [**11**]. We consider the order of an S_2-subgroup S of G. We claim;

LEMMA 1. $|S| > 4$.

PROOF. By a theorem of W. Feit and J. G. Thompson [**5**], it follows that $|S| > 1$. Burnside's splitting theorem shows that $|S| > 2$. $|S| > 4$ follows from the assumption that S is not dihedral.

LEMMA 2. $|S| > 8$.

PROOF. Suppose $|S| = 8$. Then, since a quaternion group can not be an S_2-subgroup of a simple group (R. Brauer and M. Suzuki [**4**]), S has to be an elementary abelian 2-group. By a theorem of D. Gorenstein [**10**], the centralizer $C(\tau)$ is non-solvable for some involution τ of G. Since S is elementary, $C(\tau)$ is a splitting extention of $\langle \tau \rangle$ (W. Gaschütz [**8**]). We can write as $C(\tau) = \langle \tau \rangle \times H$. Since $l(H) \leqq 5$, by a theorem of Janko [**17**] H contains a composition factor F which is isomorphic to $PSL(2, q)$, $q \geqq 5$. Put $F = I/J$ where $H \triangleright I \triangleright J$. Since $l(F) \geqq 4$, J is a cyclic group of odd prime order or $J = \{1\}$. If $q = 3^2$, then $l(PSL(2, 3^2)) = 5$. Therefore $C(\tau) \cong Z_2 \times PSL(2, 3^2)$. Now suppose $q \neq 3^2$. Then, since the Schur multiplier of $PSL(2, q)$ is at most 2, I is written in the form $I \cong J \times F_1$, where $F_1 \cong F$. Since $I' = F_1$, F_1 is a normal subgroup of H. By a theorem of J. Walter ([**25**], Corollary to Theorem), we conclude that $C(\tau) = \langle \tau \rangle \times F_1$. If $q > 5$, then $q = 3^{2n+1}$ $(n \geqq 1)$ by a theorem of Z. Janko and J. Thompson [**19**]. And by a theorem of H. Ward [**24**], G is divisible by $q^3 \geqq 3^9$, contrary to our hypothesis $l(G) \leqq 7$. Hence we have $q = 5$. We now conclude that $G \cong J$ by a theorem of Z. Janko [**18**], contrary to our hypothesis (A).

LEMMA 3. $|S| > 16$.

PROOF. Assume $|S| = 16$. Then by a theorem of P. Fong [**7**], S is an elementary abelian group or a semi-dihedral group.

Case (i). S is elementary.

By a theorem of [**10**], S has to contain an involution τ whose centralizer $C(\tau)$ is non-solvable. Since S is elementary, we can set $C(\tau) = \langle \tau \rangle \times H$ by a theorem of Gaschütz [8]. Next we shall show that

$$(*)\qquad C(\tau)=\langle\tau,\sigma\rangle\times F,$$

where $\langle\tau,\sigma\rangle$ is a four-group and $F\cong PSL(2,p)$, $p\geqq 5$ a prime. Since H is non-solvable with $l(H)\leqq 5$, H has a composition factor F_1 which is isomorphic to $PSL(2,q)$. If an S_2-subgroup of F_1 is of order 8, then $H\cong F_1\cong PSL(2,8)$, for $l(PSL(2,8))=5$. This is impossible by [19]. Therefore F_1 is a proper composition factor of H. And we can easily see that $|Z(H)|=2$ or F_1 can be regarded as a normal subgroup of index 2 of H. If $|Z(H)|=2$, since S is elementary our statement $(*)$ is true, for H is a splitting central extention of $PSL(2,p)$ by $Z(H)$. If F_1 is a normal subgroup of index 2 of H, then an involution τ_1 of $H-F_1$ induces an automorphism of F_1 of order 2. Since a Sylow 2-subgroup of H is elementary, τ_1 induces an inner automorphism of F_1. Therefore there exists an involution τ_2 of F_1 such that $\tau_1\tau_2$ commutes with every element of F_1. If we set $\sigma=\tau_1\tau_2$ and $F_1=F$ then our statement $(*)$ is true. It can now be shown easily that the normalizer $N(S)$ of S has order divisible by 3. Since $N(S)$ is solvable with $l(N(S))\leqq 6$, we have $|N(S)|=2^4\cdot 3\cdot r$, where $r=1$ or a prime. Since the fusion of S is determined in $N(S)$, we can conclude $r>1$ and $C(S)=S$ by a theorem of G. Glauberman. Since $N(S)/C(S)$ is a subgroup of $GL(4,2)\cong A_8$, we have $r=3$, 5 or 7. Let K be a complement of S in $N(S)$. Then K acts on S by conjugation. If $|K|=15$ or 21, K fixes at least one involution in S. This conflicts with $Z(N(S))\cap S=1$. Hence r must be 3. Since $\langle\tau,\sigma\rangle$ is invariant under the action of K the order of $N(\langle\tau,\sigma\rangle)/C(\langle\tau,\sigma\rangle)$ is divisible by 3. On the other hand we have shown that $C(\langle\tau,\sigma\rangle)=\langle\tau,\sigma\rangle\times F$ by $(*)$. Hence we have $l(N(\langle\tau,\sigma\rangle))=7$. This contradicts our hypothesis. Thus the case (i) is eliminated.

Case (ii). S is semi-dihedral.

Since G is a simple group, involutions of G are contained in a single conjugate class and the centralizer $C(\tau)$ of any involution of G has a normal subgroup of index 2 and $C(\tau)$ has no normal subgroup of index 4 (see W. Wong [26]). Put $H=C(\tau)/\langle\tau\rangle$. Then H has dihedral S_2-subgroups. By a theorem of D. Gorenstein and J. Walter [11], we shall easily see that $H/K(H)=PGL(2,q)$. Since $l(H)\leqq 5$, we have $K(H)=\{1\}$ and q is a prime p, or $q=3$.

Suppose $q=3$. In order to lead a contradiction, it suffices to prove that $C(\tau)$ has an abelian 2-complement (W. Wong [26]). If $K(H)=\{1\}$. This is trivial. If $K(H)>\{1\}$. Then $K(H)$ is a cyclic group of odd prime order r. Therefore $H/C_H(K(H))$ is a cyclic group, hence of order 1 or 2. Hence H has an abelian 2-complement, and since $PGL(2,3)$ is solvable, the same is true for $C(\tau)$.

Next suppose $q\geqq 5$. Then $K(H)=\{1\}$ and q is a prime p. It is now easy to see that $C(\tau)$ is a non splitting central extention of $PGL(2,p)$ by $\langle\tau\rangle$.

Therefore $C(\tau)$ is isomorphic to one of the groups K_p or K_p'. Here according to Schur ([20], p. 122) K_q and K_q' (q: a prime power) are defined as follows.

Let w be a primitive root in the Galois field $GF(q^2)$ with q^2 elements. Put $u=w^{\frac{q+1}{2}\cdot s}$, where $q-1=2^r\cdot s$, s: odd. We introduce two elements U, U' as follows;

$$U=\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \qquad U'=\begin{pmatrix} u^{2^{r-1}+1} & 0 \\ 0 & u^{2^{r-1}-1} \end{pmatrix}.$$

Now K_q, K_q' are the following groups:

$$K_q=SL(2,q)+U\cdot SL(2,q), \qquad K_q'=SL(2,q)+U'\cdot SL(2,q).$$

Since K_p has an S_2-subgroup of generalized quaternion type, we can exclude the possibility that $C(\tau)\cong K_p$. Therefore $C(\tau)\cong K_p'$. If $p\equiv -1 \pmod 4$, we can easily see that K_p' is isomorphic to $GL(2,p)/L$ where L is a subgroup of $Z(GL(2,p))$ and of order $\frac{p-1}{2}$. Therefore by a theorem of R. Brauer [1], we have $G\cong PSL(3,p)$ or M_{11}. It is checked directly that M_{11} is the only group with our property $l(G)\leqq 7$. This is a contradiction.

Therefore we may assume $p\equiv 1 \pmod 4$. If $p=5$, then K_5' has order $2^4\cdot 3\cdot 5$ and is isomorphic to the centralizer of an involution of the simple group $U_3(5)$. In § 3, we shall characterize $U_3(5)$ by this property. Therefore in order to prove our lemma it suffices to prove that $p=5$.

Now suppose $p>5$. We shall apply the theory of modular characters on groups with S_2-subgroups of semi-dihedral type. We summarize the results of R. Brauer [2], III, § 8.

Let G_1 be a finite group with semi-dihedral Sylow 2-subgroup of order 2^n. Then the principal 2-block $B_0(2)$ of G_1 consists of $4+2^{n-2}$ irreducible characters. Four of these, denoted by $X_0=1$, X_1, X_2, X_3 have odd degrees $x_i=X_i(1)$. The remaining characters, denoted by X_4, $X^{(j)}$; $j=\pm1, \pm3, \cdots, \pm(2^{n-3}-1)$ or $2, 4, \cdots, 2^{n-2}-2$ have even degrees $x_4=X_4(1)$, $x=X^{(j)}(1)$ for all j. Furthermore the following relations hold;

$$1+\delta_1 x_1=-\delta_2 x_2-\delta_3 x_3, \qquad 1+\delta_2 x_2=\delta_2 x_4. \tag{1}$$

Here two of δ_i are -1, and one is $+1$.

There exists an irreducible character φ in the principal 2-block of the centralizer $C(\tau_1)$ of a central involution τ_1 of G_1 and a sign ε, an integer m with

$$\varphi(1)=\varepsilon(m+1), \qquad m\equiv 1+2^{n-2} \pmod{2^{n-1}}, \qquad \operatorname{sign} m=\varepsilon, \tag{2}$$

where $\varphi=\varepsilon\varphi_1^J$ in the notation of [2], III.

If G_1 has no normal subgroup of index 2 then the order of G_1 is given by

(3) $$|G_1|=\frac{|C(\tau_1)|^3}{|C(\tau_1,\tau')|^2}\cdot\frac{x_1(x_1+\delta_1)}{(x_1-\delta_1 m)}\cdot\frac{m+1}{m},$$

where τ' is a involution of $C(\tau_1)$ different from τ_1. We have the additional relations

(4) $$x_1x_2=m^2x_3,$$

(5) $$x_1\equiv\delta_1(2-m)\ (\mathrm{mod}\ 2^n).$$

We note that (1) and (4) imply that

(6) $$-m^2(1+\delta_1x_1)=\delta_2(m^2+\delta_1x_1)x_2.$$

Now we shall apply these results to our group G. Since $C(\tau)\cong K_p'$ ($p\equiv 1$ (mod 4)), the first 2-block of K_p' consists of the characters whose degrees are 1, p, $p-1$, $p+1$. (Since both of K_p and K_p' are the representation group of $PGL(2, p)$, the degrees of irreducible characters of K_p and those of K_p' have one to one correspondence. The table of characters of K_p is found in [**20**], p. 136.) Therefore comparing (2) we have $\varepsilon(m+1)=p+1$. It follows that $m=p$ and $\varepsilon=1$.

Since $|C(\tau)|=2p(p^2-1)$ and $|C(\tau,\tau')|=2(p+1)$, (3) is replaced by

(7) $$|G|=2p^2(p-1)^3(p+1)^2\frac{x_1(x_1+\delta_1)}{(x_1-\delta_1 p)^2}.$$

We have to distinguish two subcases.

Subcase (1). $p^2\,|\,|G|$.

In this case we do not use the theory of modular characters. Let P_0 be an S_p-subgroup of $C(\tau)$. Then by considering the structure of $C(\tau)\cong K_p'$ we conclude that the order of $N(P_0)$ is divisible by $2p^2(p-1)$. If $N(P_0)$ is solvable then $|N(P_0)|=2p^2(p-1)=2^3p^2r$ ($r=p-1/4$), for $l((N(P_0)))\leqq 6$. And by Sylow's theorem it is easy to prove that S_p-subgroup P_1 of $N(P_0)$ is normal in $N(P_0)$. Denote a complement of P_1 in $N(P_0)$ by K. We may assume that $K\ni\tau$. K acts on the chain

$$P_1>P_0>\{1\}$$

by conjugation. Since $p-1$ is not divisible by 8, it follows directly that τ stabilizes the above chain. Hence $[\tau, P_1]=1$, which is not true. Next suppose $N(P_0)$ is non solvable. Then the group $N(P_0)/P_0$ has a composition factor F which is isomorphic to $PSL(2, q)$. Since $N(P_0)/P_0$ contains an element of order 8 and an S_2-subgroup of F is dihedral, $N(P_0)$ must be divisible by 16. Therefore an element of order 4 centralizes P_0 which is impossible by the structure of $C(\tau)$. Thus we have led a contradiction in this case.

Subcase (2). $p^2\nmid|G|$.

Since $l(PSL(2, p))\leqq 4$ for our prime p, we can set $p-1=4r$, $p+1=2st$

where r, s, t are prime numbers or 1 ($r>1$, since $p>5$). We shall prove the following statement.

(*) $r^3 \nmid |G|$.

By way of contradiction, suppose $r^3 \mid |G|$. Let R_0 be an S_r-subgroup of $C(\tau)$. Then $N(R_0)$ is divisible by $r\cdot 4(p-1)=16r^2$. If $N(R_0)$ is solvable, then $|N(R_0)|=16r^2$, for $l(N(R_0))\leqq 6$. Therefore $|C(R_0)|=8r^2$ and an S_2-subgroup of $C(R_0)$ is cyclic. Hence $N(R_0)$ is r-closed. Let R_1 be S_r-subgroup of $N(R_0)$. Then $N(R_1)$ is divisible by r^3 and $l(N(R_1))$ is at least seven, contrary to our hypothesis. If $N(R_0)$ is non-solvable, $N(R_0)/R_0$ has a composition factor F which is isomorphic to $PSL(2, q)$. S_2-subgroup of F must be of order 8 and maximal in F, which is clearly impossible. For F contains a subgroup which is isomorphic to the symmetric group of degree 4. Hence the statement (*) is proved.

By (5) $x_1-\delta_1 p\equiv 2\delta_1(1-p) \pmod{16}$. Therefore $x_1-\delta_1 p$ is divisible by 8. On account of (7), since r^3 does not divide G, r has to divide $x_1-\delta_1 p$. Hence we can set $x_1-\delta_1 p=8rpa=2a(p-1)p$, where a is an integer.

By (6) we have

$$p^2(\delta_1+x_1)\equiv 0 \pmod{x_1+\delta_1 p^2}.$$

Hence

$$p^4-p^2\equiv 0 \pmod{x_1+\delta_1 p^2}.$$

Since x_1 is not divisible by p^2, $x_1+\delta_1 p^2$ is not divisible by p^2, and

$$p^2-1\equiv 0 \pmod{2a(p-1)+\delta_1+\delta_1 p}.$$

Put

$$p^2-1=b(2a(p-1)+\delta_1(p+1)). \tag{8}$$

Then

$$b\equiv 0 \left(\mathrm{mod}\ \frac{p-1}{2}\right).$$

If we set

$$b=\frac{p-1}{2}b'$$

then (8) is replaced by

$$p+1=b'\left(a(p-1)+\frac{\delta_1}{2}(p+1)\right). \tag{9}$$

Therefore

$$p+1\geqq a(p-1)+\frac{\delta_1}{2}(p+1)\geqq a(p-1)-\frac{1}{2}(p+1).$$

This implies (note that $p\geqq 13$)

$$a\leqq\frac{3}{2}\cdot\frac{p+1}{p-1}<2.$$

Hence we have $a=1$. If $\delta_1=1$ in (9), then we have

$$b'=1, \qquad p=3$$

contrary to our assumption $p>5$. Therefore $\delta_1=-1$ and we get

$$b'=2+\frac{8}{p-3}.$$

Hence $p=5, 7$ or 11 which again contradicts our assumption that $p>5$ and $p\equiv 1 \pmod 4$. Thus we have get a contradiction, and have proved Lemma 3.

LEMMA 4. $|S|>32$.

PROOF. Suppose $|S|=32$. Then by a theorem of P. Fong, S is isomorphic to one of the following groups:

(1) an elementary abelian group,

(2) a semi-dihedral group or

(3) a wreath product $Z_4 \int Z_2$.

Case (1). S is elementary.

Since S has to be contained in $N(S)$ properly, the order of $N(S)$ is $2^5 \cdot p$ where p is an odd prime number. And $N(S)$ is a Frobenius group with its kernel S. Therefore the centralizer $C(\tau)$ of an involution τ of G has a normal 2-complement, hence solvable. Therefore G is isomorphic to one of the groups $PSL(2, q)$ by a theorem of D. Gorenstein [**10**], contrary to our assumption (A).

Case (2). S is semi-dihedral.

Let τ be an involution of G. Then by the same argument as in the proof of Lemma 3, $C(\tau)/\langle\tau\rangle \cdot K(C(\tau))$ is isomorphic to $PGL(2, p)$. For this prime p, $PSL(2, p)$ has an S_2-subgroup T of order 8. Since the length $l(PSL(2, p))$ must be less than 5, T is a maximal subgroup of $PSL(2, p)$ which is clearly impossible by considering the structure of $PSL(2, p)$.

Case (3). S is isomorphic to $Z_4 \int Z_2$.

P. Fong [**6**] has studied the simple groups with S_2-subgroups which is isomorphic to $Z_4 \int Z_2$. He has proved if the centralizer of an involution τ of G is solvable, then G is isomorphic to $U_3(3)$. In our case, since $l(C(\tau))\leqq 6$, it is easy to prove that $C(\tau)$ is solvable (for the detail, see P. Fong [**6**], pp. 70~71). Hence $G\cong U_3(3)$ which contradicts our assumption (A).

LEMMA 5. $|S|>64$.

PROOF. Suppose $|S|=64$. Then S is a maximal subgroup of G. Therefore in order to prove Lemma 5, it suffices to show the following lemma.

LEMMA 6. *If the S_2-subgroup S of a simple group G has order* 64, *then S can not be maximal in G.* (In this lemma we do not assume that $l(G)\leqq 7$).

PROOF. By way of contradiction, assume that there exists a simple group G whose S_2-subgroup S has order 64 and is maximal in G. Since $N(S)=S$, Burnside's splitting theorem shows that S can not be abelian. If G has only one conjugate class of involutions, then G is a (CIT) group in the sense of M. Suzuki [21] and so G is isomorphic to $PSL(2, 2^n)$, $Sz(2^n)$, $PSL(2, 9)$, $PSL(3, 4)$ or $PSL(2, p)$ where p is a Fermat prime or a Mersenne prime. In the groups mentioned above, there exist no group with maximal S_2-subgroups of order 64. Therefore G has at least two conjugate classes of involutions. We now soon see that S can not be dihedral or semi-dihedral. Moreover S can not be isomorphic to an S_2-subgroup of the Mathieu group M_{12} by a theorem of R. Brauer and P. Fong [3].

Since $N(S)=S$, any two central involutions of S are not conjugate with each other in G. Let τ be a central involution of S. Then by a theorem of G. Glauberman [9], τ must be fused with a certain non-central involution σ of S. $S_1=C(\sigma)$ is an S_2-subgroup of G which is different from S. Since $S\cap S_1\supset Z(S)\ni\tau$ and $C(\tau)=S$, we have $S\cap S_1\supset\langle Z(S), Z(S_1)\rangle$. If the group $Z(S)\cap Z(S_1)$ is non trivial, there exists an involution ρ whose centralizer in G contains two S_2-subgroups of order 64. This contradicts the maximality of S. Hence $S_1\cap S\supset Z(S)\times Z(S_1)$. In particular $|Z(S)|\leqq 4$. Moreover, if $|Z(S)|=4$, $Z(S)\times Z(S_1)$ can be normal in neither S nor S_1. For if $T=Z(S)\times Z(S_1)$ is normal, say, in S, then $N(T)=S$ by the maximality of S. Hence $U=S\cap S_1$ is of order at least 32. Therefore $N(U)\supset\langle S, S_1\rangle$ which is a contradiction.

Next we shall prove the following two statements.

[I] *A central involution τ of S is not fused with any involution σ $(\neq\tau)$ of $Z_2(S)$, where $Z_2(S)$ is the second term of the upper central series of S.*

[II] *The nilpotent class of S is at least three.*

PROOF. [I] Suppose $\tau \overset{G}{\sim} \sigma\in Z_2(S)$ and put $S_1=C(\sigma)$. Then S_1 is an S_2-subgroup of G. Since $C_S(\sigma)\supset S'$ $([S', Z_2(S)]=\{1\})$, $S\cap S_1$ contains S' and is normal in S. Therefore we have $N(S\cap S_1)=S$ so that $S=S_1$. Since any two central involutions are not conjugate with one another, we conclude $\tau=\sigma$. [II] follows directly from [I] and a theorem of G. Glauberman [9].

Now we refer the list of 2-group of order 64 due to M. Hall and K. Senior [14]. By a theorem of P. Fong [7] and by the above argument, S must be a 2-group of exponent 4 and the nilpotent class of S must be at least three. $|Z(S)|$ must be less than 8 and S must contain a subgroup isomorphic to $Z\times Z$ where $Z\cong Z(S)$. Of 267 2-groups of order 64, there are six groups which can not be eliminated trivially from the knowledge of M. Hall and K. Senior's list. Those are S_{123}, S_{128}, S_{252}, S_{253}, S_{259}, S_{260}. Here S_i is a 2-group of number i in the list of M. Hall and K. Senior.

We shall eliminate these six groups separately. In the following proof, $\alpha_1, \alpha_2, \cdots, \alpha_6, \beta_1, \beta_2$ are the same group elements as that of M. Hall and K. Senior's list.

We introduce new notation.

$\Omega_1(X)$······a subgroup generated by all the elements of order p in a p-group X.

$\mho^1(X)$······a subgroup generated by x^p's where x ranges over all the elements in a p-group X.

(a) $S \cong S_{123}$. S has a maximal subgroup $T=\langle \beta_2, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ which is isomorphic to $Z_2 \times Z_2 \times D_8$. All involutions of S are contained in T. By Lemma 16 which will be stated in § 4, any element $\rho_1 \in S-T$ has to be fused with an element $\rho_2 \in T$. If so, ρ_1^2 is fused with ρ_2^2. In particular $\alpha_5^2=\alpha_3 \overset{G}{\sim} \alpha_1$, for $\mho^1(T)=\langle \alpha_1 \rangle$. Since $\alpha_3 \in Z_2(S)$, this is impossible by [I].

(b) $S \cong S_{128}$. $Z(S)$ is a four-group and S has only one elementary abelian group of order 16. That is $T=\langle \beta_2, \alpha_1, \alpha_2, \alpha_3 \rangle$. Hence $T \triangleleft S$. As remarked earlier this is impossible.

(c) $S \cong S_{252}$. S contains a maximal subgroup $T=\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \rangle$ which contains all the involutions of S. As in the case of $S=S_{123}$ we have $\alpha_6^2=\alpha_5 \overset{G}{\sim} \alpha \in \mho^1(T)=\langle \alpha_1, \alpha_2 \rangle$. Since $\alpha_2 \overset{S}{\sim} \alpha_1 \cdot \alpha_2$, we may assume that $\alpha_5 \overset{G}{\sim} \alpha_1$, or $\alpha_5 \overset{G}{\sim} \alpha_2$. Suppose $\alpha_5 \overset{G}{\sim} \alpha_1$ and take an element x of G such that $\alpha_5^x=\alpha_1$ and $C_S(\alpha_5)^x \subset S$ (Lemma 14, § 4). Then $(C_S(\alpha_5)')^x=(\langle \alpha_1, \alpha_2, \alpha_5, \alpha_6 \rangle')^x=\langle \alpha_1 \rangle^x \subset \Omega_1(S')$ $=\langle \alpha_1, \alpha_2 \rangle$. Therefore $\alpha_1^x=\alpha_2$ or $\alpha_1 \cdot \alpha_2$. Since $\langle \alpha_1, \alpha_2 \rangle \subset Z_2(S)$, this is impossible by [I]. Next suppose $\alpha_5 \overset{G}{\sim} \alpha_2$ and take an element y such that $\alpha_5^y=\alpha_2$ and $C_S(\alpha_5)^y \subset S$. Then, since $\alpha_1^y \in \langle \alpha_1, \alpha_2 \rangle$, we have $\alpha_1^y=\alpha_1$. Hence $y \in C(\alpha_1)$ $=S$ which is clearly impossible.

(d) $S \cong S_{253}, S_{260}$. Let σ be any involution of $S-Z_2(S)$. Then we have $C_S(\sigma)'=\langle \alpha_1 \rangle$. Therefore if α_1 is conjugate with σ in G, then α_1 is fused into $\Omega_1(S')-\{\alpha_1\}$. This is not true, since $\Omega_1(S') \subset Z_2(S)$ for both of S_{253}, S_{260}.

(e) $S \cong S_{259}$. There exist two types of involutions in $S-Z_2(S)$. One is an involution whose centralizer is isomorphic to $Z_2 \times D_8$. The other is one whose centralizer is a unique elementary abelian 2-group of order 16. If a central involution α_1 is fused with an involution σ of the former type, then there exists an element $x \in G$ such that $C_S(\sigma)^x \subset S$ and $\sigma^x=\alpha_1$. Since $C_S(\sigma)'=\langle \alpha_1 \rangle$ and $\Omega_1(S') \subset Z_2$, we have $\alpha_1^x \in Z_2(S)-\{\alpha_1\}$, which is impossible by [I]. If α_1 is fused with the latter type of involution σ, then $S_1=C(\sigma)$ is an S_2-subgroup of G and $S \cap S_1=C_S(\sigma)$ is normal in S. As remarked above, this is again impossible.

Thus we have proved Lemma 6.

Groups	S_{123}	S_{128}	S_{252}	S_{253}	S_{259}	S_{260}
Generators	$\beta_2, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$		$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6$		$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6$	
Defining Relations	$[\alpha_3, \alpha_4]=[\alpha_2, \alpha_5]=\alpha_1$ $[\alpha_4, \alpha_5]=\alpha_2$ $\alpha_1^2=\alpha_2^2=\alpha_3^2=1,\ \alpha_5^2=\alpha_3$ $\beta_2^2=1$		$[\alpha_3, \alpha_5]=[\alpha_2, \alpha_6]=\alpha_1$ $[\alpha_4, \alpha_5]=[\alpha_3, \alpha_6]=\alpha_2$ $[\alpha_4, \alpha_6]=\alpha_2\alpha_3$ $\alpha_1^2=\alpha_2^2=\alpha_5^2=1,$ $\alpha_3^2=\alpha_1,\ \alpha_6^2=\alpha_5$		$[\alpha_3, \alpha_5]=[\alpha_2, \alpha_6]=\alpha_1$ $[\alpha_4, \alpha_5]=\alpha_2$ $[\alpha_4, \alpha_6]=\alpha_3$ $\alpha_1^2=\alpha_2^2=\alpha_3^2=\alpha_5^2=\alpha_6^2=1$	
	$\alpha_4^2=1$	$\alpha_4^2=\beta_2$	$\alpha_4^2=\alpha_2$	$\alpha_4^2=\alpha_1\alpha_2$	$\alpha_4^2=1$	$\alpha_4^2=\alpha_1$
$Z(S)$	$\langle\beta_2, \alpha_1\rangle$		$\langle\alpha_1\rangle$		$\langle\alpha_1\rangle$	
$Z_2(S)$	$\langle\beta_2, \alpha_1, \alpha_2, \alpha_3\rangle$		$\langle\alpha_1, \alpha_2\rangle$		$\langle\alpha_1, \alpha_2, \alpha_3\rangle$	
S'	$\langle\alpha_1, \alpha_2\rangle$		$\langle\alpha_1, \alpha_2, \alpha_3\rangle$		$\langle\alpha_1, \alpha_2, \alpha_3\rangle$	

REMARK. In Defining Relations, all the non-identity commutators are given.

Now we are able to give a final contradiction. By Lemma 5, we conclude $|S| \geqq 128$. Therefore $l(S) \geqq 7$, contrary to our hypothesis on G. Thus we have proved our main theorem.

Next lemma which was stated in Introduction will be proved easily, if we use the argument in the proof of our theorem especially of Lemma 6. We omit the detail.

LEMMA 7. *Let S be an S_2-subgroup of a simple group G. If S is not dihedral and $|S| \leqq 64$, then S cannot be maximal in G.*

§ 3. A characterization of $U_3(5)$.

In this section we shall prove the following theorem.

THEOREM. *Let G be a finite group with the conditions;*

(i) *G contains an involution τ whose centralizer $C(\tau)$ is isomorphic to K_5'* (*p.* 659),

(ii) *G does not contain a normal subgroup of index* 2.

Then G is isomorphic to the simple group $U_3(5)$.

Let G be a finite group satisfying the conditions (i) and (ii). We first prove several lemmas.

LEMMA 8. *A Sylow 2-subgroup of $C(\tau)$ is also a Sylow 2-subgroup of G. All the involutions of G are contained in a single conjugate class.*

PROOF. Since the Sylow 2-subgroups of $C(\tau)$ are semi-dihedral, our assertion is clear.

LEMMA 9. *G is simple.*

PROOF. First we shall show that $G=[G, G]$. By way of contradiction, assume that N is a normal subgroup of G of prime index p. By the condition (ii), we have $p \neq 2$. Let S be a Sylow 2-subgroup of N, then $G=N(S) \cdot N$. On the other hand, considering the structure of $C(\tau)$, we easily see that $N(S)=S$. Therefore $G=N$. This is a contradiction.

Next assume that N is a non trivial normal subgroup of G. Then by the previous argument the factor group G/N must be non solvable. If a Sylow 2-subgroup $\bar{S}$ of G/N has order 4, then there exists an element $\bar{x}$ of order 3 in G/N such that $\bar{S}^{\bar{x}}=\bar{S}$. Therefore $N(S)>S$ for a Sylow 2-subgroup S of G. This is impossible. Hence N is a solvable group (note that $|S|=16$). Therefore we may assume that N is an elementary abelian p-group P ($p \neq 2$). We easily see that there exists an involution τ_1 such that $C(\tau_1) \cap P>1$. We may assume $\tau_1=\tau$. Considering the structure of $C(\tau)$, we see that $C(\tau) \cap P$ is a cyclic subgroup of order 3 or 5. Since $C(\tau) \cap P$ is invariant by $C(\tau)$, there exists an element of order 4 in $C(\tau)$ which centralizes $C(\tau) \cap P$. This again contradicts with the structure of $C(\tau)$. Thus we have proved our lemma.

Since the Sylow 2-subgroup of G is semi-dihedral, we can apply a theorem of R. Brauer which is previously stated in § 2, pp. 659~660. We use the same notation as there.

LEMMA 10. *For our group G we have $m=5$ and* $|G|=2^9\cdot 3^2\cdot 5^2\cdot\frac{x_1(x_1+\delta_1)}{(x_1-5\delta_1)^2}$.

PROOF. Since $m=p=5$, our assertion is clear from § 2, (7).

LEMMA 11. *Denote by $v_p(a)$ the exact exponent with which p divides a. Then*

(i) *if* $v_5(|G|)=1$, *then* $|G|=2^4\cdot 3^2\cdot 5\cdot 7\cdot 17=85{,}680$,

(ii) *if* $v_5(|G|)=2$, *then* $|G|=2^4\cdot 3^2\cdot 5^2\cdot 19=68{,}400$,

(iii) *if* $v_5(|G|)\geqq 3$, *then* $|G|=2^4\cdot 3^2\cdot 5^3\cdot 7=126{,}000$.

PROOF.

(i) As $x_1(x_1+\delta_1)$ divides $|G|$ (§ 2, (1)), $(x_1-5\delta_1)^2$ is a factor of $2^9\cdot 3^2\cdot 5^2$. As $v_2(x_1+\delta_1)=1$ by § 2, (5), we have $x_1-5\delta_1=2^3\cdot 5\cdot a$ where $a=1$ or 3. Hence $x_1=40a+5\delta_1$. On account of § 2, (6) we have

$$-5^2(\delta_1+x_1)\equiv 0 \mod (x_1+5^2\delta_1).$$

Since

$$-5^2(\delta_1+x_1)=-5^2(x_1+5^2\delta_1)+5^2(5^2-1)\delta_1,$$

we have

$$24\equiv 0 \mod (8a+6\delta_1).$$

Hence $a=1$, $\delta_1=-1$. Hence $|G|=2^4\cdot 3^2\cdot 5\cdot 7\cdot 17$.

(ii) By Lemma 10, we have $v_5(x_1)=2$ or 0. If $v_5(x_1)=2$, then $x_1=2^3\cdot 5a+5\delta_1\equiv 0 \pmod{25}$, where $a=1$ or 3. Hence $a=3$, $\delta_1=1$. This forces $v_5(x_1)=3$ which contradicts with $v_5(|G|)=2$. Therefore $v_5(x_1)=0$. Hence $x_1=2^3\cdot a+5\delta_1$, where $a=1$ or 3. On account of § 2, (6) we have $24\equiv 0 \pmod{2^3\cdot a+30\delta_1}$. Therefore $a=3$, $\delta_1=-1$ and $|G|=2^4\cdot 3^2\cdot 5^2\cdot 19$.

(iii) On account of the formula

$$|G|=2^9\cdot 3^2\cdot 5^2\cdot\frac{x_1(x_1+\delta_1)}{(x_1-5\delta_1)^2}$$

we have $v_5(x_1)\geqq 3$.

On the other hand $x_1-5\delta_1\leqq 2^3\cdot 3\cdot 5=120$. This forces $x_1=125$ and $\delta_1=1$. Hence $|G|=2^4\cdot 3^2\cdot 5^3\cdot 7$.

LEMMA 12. *The cases* (i) *and* (ii) *of Lemma* 11 *can not occur.*

PROOF. Using the Sylow's theorem and comparing the structure of $C(\tau)$, we can prove that G is not simple. The details of the computation are omitted. (Remark. In his paper [13] M. Hall has announced that there exist no simple groups of orders $2^4\cdot 3^2\cdot 5\cdot 7\cdot 17$ and $2^4\cdot 3^2\cdot 5^2\cdot 19$).

LEMMA 13. *G is a group satisfying the following properties;*

(i) *G is a doubly transitive permutation group on Ω of* 126 *letters,*

(ii) *the subgroup H consisting of all the elements leaving a fixed letter α invariant contains a normal subgroup Q which is regular on $\Omega-\{\alpha\}$,*

(iii) *H/Q is a cyclic group of order* 8.

PROOF. First we consider the order of the normalizer of a Sylow 5-subgroup Q of G. Since $|G|=2^4\cdot 3^2\cdot 5^3\cdot 7$, we have $|Q|=5^3$. As G has an irreducible character X_1 of 5-defect 0, there exists another Sylow 5-subgroup Q_1 such that $Q\cap Q_1=\{1\}$ (J. A. Green [**12**]). Therefore $n_5=|G|/|N(Q)|\geqq 125+1$. By Sylow's theorem we have two possibilities $n_5=2^4\cdot 3\cdot 7$ or $2\cdot 3^2\cdot 7$. Assume $n_5=2^4\cdot 3\cdot 7$ (i.e. $|N(Q)|=3\cdot 5^3$). Then since $n_5\not\equiv 1 \pmod{25}$, there exist two Sylow 5-group Q_1 and Q_2 such that $|Q_1\cap Q_2|=25$. Put $L=Q_1\cap Q_2$ and $M=N(L)$. Then M/L contains at least two Sylow 5-subgroups. Let $\bar{Q}$ be a Sylow 5-group of M/L. Then comparing the structure of $N(Q)$, M/L has a normal 5-complement. We easily see that $\bar{Q}$ centralizes every Sylow p-subgroup of M/L for $p=2, 3$ and 7. This is clearly impossible. We have thus shown $n_5=126$. Therefore G can be regarded as a permutation group on 126 Sylow 5-subgroups under conjugation. Since there exist two Sylow 5-subgroups Q, Q_1 such that $Q\cap Q_1=\{1\}$, G is doubly transitive. Therefore (i) and (ii) of Lemma 13 are proved. Put $N(Q)=K\cdot Q$, $K\cap Q=\{1\}$. Then K is a stabilizer of two letters (two Sylow 5-groups). By the double transitivity of G, there exists an involution w normalizing K. Therefore K is a cyclic group or a quaternion group (note that $\langle w, K\rangle=S$). As $8\nmid 124$, the unique involution τ of K commutes with a certain element $\pi\neq 1$ of Q. Let $Q_0=C(\tau)\cap Q$, then $|Q_0|=5$ and K normalizes Q_0. Since every element of order 4 does not commute with a 2-regular element of G, K must be cyclic. Thus all the assertions are proved.

In [**15**], we have shown that a finite group satisfying the condition (i), (ii), (iii) of Lemma 13 is isomorphic to $U_3(5)$. Thus we have proved our theorem.

§ 4. Lemmas on S_2-subgroups of finite groups.

Let G be a finite group of even order and S be one of the Sylow 2-subgroups of G. We fix S once for all. Let x be an element of S and K be the conjugate class of G which contains x. Put $K_1=S\cap K$.

DEFINITION. An element y of K_1 is called an extreme element if $|C_S(y)|\geqq|C_S(z)|$ for every $z\in K_1$. (R. Brauer [**2**].)

LEMMA 14. *If y is an extreme element of S, then $C_S(y)$ is a Sylow 2-subgroup of $C(y)$. Furthermore, for every element $x\in K_1$ there exists an isomorphism θ of $C_S(x)$ into $C_S(y)$ such that $x^\theta=y$.*

PROOF. Using Sylow's fundamental theorem, we easily get our lemma.

LEMMA 15. *If a 2-element x of G normalizes the center $Z(S)$ of S, then x centralizes $Z(S)$.*

PROOF. Since $N(Z(S))/C(Z(S))$ is a group of odd order, we have our lemma.

LEMMA 16. *If an element x of S is not fused with any element of a maximal subgroup M of S and x^{2n} is not fused with any element of $S-M$ for* *every $n \geqq 1$ then the index $[G; G']$ is even.*

PROOF. Consider the transfer mapping T from G into S/M. Then the image xT of x is

$$xT \equiv \prod_{i=1}^{r} x_i x^{n_i} x_i^{-1} \pmod{M},$$

where $\sum_{i=1}^{r} n_i = [G:S]$, n_i $(1 \leqq i \leqq r)$ is the least integer such that $x_i x^{n_i} x_i^{-1}$ is contained in S and $\{x_i \ (1 \leqq i \leqq r)\}$ is a subset of one of the representatives of the coset space G/S. Since x is a 2-element, n_i is a power of 2 $(1 \leqq i \leqq r)$. By the condition on x, if $n_i \geqq 2$ then $x_i x^{n_i} x_i^{-1} \in M$. Hence

$$xT \equiv \prod{}' x_i x x_i^{-1} \pmod{M},$$

where the product ranges on all i such that $n_i = 1$. Since $x_i x x_i^{-1} \in S - M$, we can put $x_i x x_i^{-1} = x m_i$ where $m_i \in M$. Hence

$$xT \equiv x^s \pmod{M},$$

where $s = \sum_{i=1}^{r} n_i - \sum_{n_i \geqq 2}' n_i$. Since $\sum_{i=1}^{r} n_i$ is odd, s is odd. Therefore the homomorphism T of G into S/M is non-trivial. This follows our lemma.

COROLLARY 1 (Thompson). *If an involution x of S is not fused with any involution of a maximal subgroup M of S, then the index $[G:G']$ is even.*

COROLLARY 2. *Let M be a maximal subgroup of S. If the order of every element of M is less than the order of every element of $S-M$, the index $[G:G']$ is even.*

DEFINITION. A non-abelian 2-group T is called a generalized dihedral group if T contains an abelian subgroup A of index 2 such that the order of every element of $T-A$ is 2.

DEFINITION. A 2-group T is called a DE-group if T is a direct product of a dihedral group with an elementary abelian group.

LEMMA 17. *If S is a generalized dihedral group, then the index $[G:G']$ is even or S is a DE-group.*

PROOF. Let M be a maximal abelian subgroup of S. Then $[S:M]=2$ and every element of $S-M$ is of order 2. If $a \in S-M$, then a induces an automorphism of M which inverts every element of M. Suppose that S is not a DE-group. Then M is an abelian group of type $(n_1, n_2, \cdots, n_s)$ where $n_1, n_2 > 2$. Furthermore assume that the index $[G:G']$ is odd. Then a is fused with an involution of M by Corollary 1. Since every involution of M is a central involution of S, the centralizer $C(a)$ of a in G contains a Sylow 2-subgroup of G. Let T be a Sylow 2-subgroup of $C(a)$ such that $T \supset C_S(a)$. Since $Z(T)$ is an elementary abelian group of order 2^s and $C_S(a)$ is an elementary abelian group of order 2^{s+1}, we can conclude $Z(T) \subset C_S(a)$ by the structure of T. Let Z be a subset of $Z(S)$ defined as follows;

$$Z=\{z\in Z(S) \mid \text{there exists an element } y \text{ of } M \text{ such that } y^2=z\}\,.$$

Then Z is a subgroup of $Z(S)$ and $|Z|\geqq 2^2$. Hence $Z\cap Z(T)>1$. Let $z\in Z \cap Z(T)$ and $y^2=z$. Then y normalizes $Z(T)$ but does not centralize $Z(T)$, for $a^y=y^{-1}ay=ay^2=az\in Z(T)$. By Lemma 15 this is impossible.

LEMMA 18. *If S contains a maximal subgroup M which is elementary abelian then the index $[G:G']$ is even or S is a DE-group.*

PROOF. Suppose S is not a DE-group and the index $[G:G']$ is odd. Then $S-M$ contains at least one involution by Corollary 2. Let a be an involution of $S-M$. Then a induces an automorphism of M of order 2. If $z^a\neq z$ for some element z of M then $\langle z, a\rangle$ is a dihedral group of order 8, and $\langle z^a, z\rangle$ is an a-invariant four-group. Next we shall prove that M has the form;

$$M=\langle z_1^a, z_1\rangle\times\langle z_2^a, z_2\rangle\times\cdots\times\langle z_s^a, z_s\rangle\times W$$

where W is a subgroup of $Z(S)$. Indeed, since every involution of $GL(n, 2)$ $(|M|=2^n)$ is conjugate with

$$\begin{pmatrix} & 1 & & & & & & & \\ 1 & & & & & & & 0 & \\ & & & 1 & & & & & \\ & & 1 & & & & & & \\ & & & & \ddots & & & & \\ & & & & & & 1 & & \\ & & & & & 1 & & & \\ & & & & & & & 1 & \\ & 0 & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix}$$

our assertion is clear. If $[M:Z(S)]=2$, then $M=\langle z_1^a, z_1\rangle\times W$. Therefore, since S is not a DE-group, $[M:Z(S)]\geqq 2^2$. If an element az, $z\in M$, is of order 4, then $(az)^2=z^az\in Z(S)$. Since the index $[G:G']$ is odd, $(az)^2$ is fused with a certain involution b of $S-M$ by Lemma 16. We may take $a=b$. Let S_1 be a Sylow 2-subgroup of $C(a)$ such that $S_1\supset C_S(a)=\langle a, Z(S)\rangle$. If $C_S(a)\supset Z(S_1)$, then $Z(S_1)=\langle a, T_1\rangle$ where $T_1\subset Z(S)$ and $[Z(S):T_1]=2$. Put $M_1=\langle z_1^a, z_1\rangle \times\langle z_2^a, z_2\rangle\times\cdots\times\langle z_s^a, z_s\rangle$. Then $|Z(S)\cap M_1|\geqq 2^2$, because $s\geqq 2$. Hence $Z(S) \cap M_1\cap T_1>1$. Take $z\in Z(S)\cap M_1\cap T_1$ and write $z=yy^a$. Then y normalizes $\langle a, T_1\rangle=Z(S_1)$ but does not centralize $Z(S_1)$, this is impossible by Lemma 15. Therefore $\langle a, Z(S)\rangle\cdot Z(S_1)$ is an elementary abelian 2-group which contains $\langle a, Z(S)\rangle$ properly. Put $T_2=\langle a, Z(S)\rangle$. Consider the groups $N(T_2)/C(T_2)$ and $C(T_2)$. We have proved that $|C(T_2)|_2\geqq 2^2\cdot|Z(S)|$. Since $Z=\langle z_1, z_2, \cdots, z_r\rangle \subset N(T_2)$ and $Z\cap C(T_2)=1$, we get $|N(T_2)/C(T_2)|_2\geqq 2^r=[M:Z(S)]$. Hence $|G|_2\geqq 2^2\cdot|M|>|S|$. This is impossible. ($|C(T_2)|_2\cdots$ denotes the exact exponent with which 2 divides $|C(T_2)|\cdots$.)

LEMMA 19. *Suppose that the Frattini subgroup of S is cyclic. If for every element a of S, $C_S(a)$ is not elementary then $Z^*(G)\supset\Omega_1(D(S))$.*

PROOF. Let a be an element of order 4. Then $a^2 \in D(S)$. Since $D(S)$ is cyclic, a^2 is the unique generator z of $\Omega_1(D(S))$. If $Z^*(G) \not\supset \Omega_1(D(S))$ then z is conjugate with some element $b \neq z$ of S. By Lemma 14, there exists an isomorphism θ from $C_S(b)$ into S such that $b^\theta = z$. Since $C_S(b)$ is not elementary $C_S(b)$ contains an element a of order 4. If $a^\theta = y$ then $(a^2)^\theta = z^\theta = y^2 = z$. This is a contradiction.

DEFINITION. An extra-special 2-group S is defined as follows: S is a 2-group such that $[S, S] = D(S) = Z(S)$ and all are of order 2.

COROLLARY 4. *If S is an extra special 2-group, then S is a dihedral group of order 8, or $Z^*(G) \supset Z(S)$.*

PROOF. If $Z^*(G) \not\supset Z(S)$, then for some element a, $C_S(a)$ is elementary by Lemma 19. Since S is an extra-special 2-group we have $[S : C_S(a)] = 2$. Therefore $|Z(S)| \geqq \sqrt{|C_S(a)|}$ (refer the proof of Lemma 18). Hence $|C_S(a)| = 4$ and S is a dihedral group of order 8.

Nagoya University

References

[1] R. Brauer, On finite Desarguesian planes. II, Math. Zeit., **91** (1966), 124–151.

[2] R. Brauer, Some applications of the theory of blocks of characters of finite groups. II, J. Algebra, **1** (1964), 307–334, III., J. Algebra, **3** (1966), 225–255.

[3] R. Brauer and P. Fong, A characterization of the Mathieu group M_{12} of degree 12, Trans. Amer. Math. Soc., **122** (1966), 18–47.

[4] R. Brauer and M. Suzuki, On finite groups of even order whose 2-Sylow group is a quaternion group, Proc. Nat. Acad. Sci. U. S. A., **45** (1959), 1757–1759.

[5] W. Feit and J. G. Thompson, Solvability of groups of odd order, Pac. J. Math., **13** (1963), 775–1029.

[6] P. Fong, Some Sylow subgroups of order 32 and a characterization of $U(3, 3)$, J. Algebra, **6** (1967), 65–76.

[7] P. Fong, Sylow 2-subgroups of small order I, II, (to appear).

[8] W. Gaschütz, Zur Erweiterung theorie der endlichen Gruppen, J. reine angew. Math., **190** (1952), 93–107.

[9] G. Glauberman, Central elements in core free groups, J. Algebra, **4** (1966), 403–420.

[10] D. Gorenstein, Finite group in which Sylow 2-subgroups are abelian and centralizers of involutions are solvable, Canad. J. Math., **17** (1965), 860–906.

[11] D. Gorenstein and J. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. I, II, III, J. Algebra, **2** (1965), 85–151, 218–270, 364–393.

[12] J. A. Green, Blocks of modular representations of a finite group, Math. Zeit., **70** (1959), 430–445.

[13] M. Hall, A search for simple groups of orders less than one million (to appear).

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

[15] K. Harada, A characterization of the simple group $U_3(5)$ (to appear).

[16] Z. Janko, Finite groups with invariant fourth maximal subgroups, Math. Zeit.,

82 (1963), 82–89.
[17] Z. Janko, Finite simple groups with short chains of subgroups, Math. Zeit., **84** (1964), 428–437.
[18] Z. Janko, A new finite simple group with abelian Sylow 2-subgroups and its characterization, J. Algebra, **3** (1966), 147–186.
[19] Z. Janko and J. G. Thompson, On a class of finite simple groups on Ree, J. Algebra, **4** (1966), 274–292.
[20] I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, J. reine angew. Math., **132** (1907), 85–137.
[21] M. Suzuki, Finite groups with nilpotent centralizers, Trans. Amer. Math. Soc., **69** (1961), 425–470.
[22] M. Suzuki, A characterization of the 3-dimensional projective unitary group over a finite field of odd characteristic, J. Algebra, **2** (1965), 1–14.
[23] J. G. Thompson, A special class of non-solvable groups, Math. Zeit., **72** (1960), 458–462.
[24] H. Ward, On Ree's series of simple groups, Trans. Amer. Math. Soc., **121** (1966), 62–89.
[25] J. Walter, Finite groups with abelian Sylow 2-subgroups of order 8, Invent. Math., **2** (1967), 332–376.
[26] W. J. Wong, On finite groups whose 2-sylow subgroups have cyclic subgroups of index 2, J. Austral. Math. Soc., **4** (1964), 90–112.

Added in proof. The statement [II] on page 663 is a special case of a theorem of Deskins. Our proof, however, depends upon a theorem of Glauberman.

Errata. After galley proof was ready, Professor D. Gorenstein pointed out a gap in my paper [**15**]. Therefore "$U_3(5)$" of Theorem 1 should be chainged into "a simple group of order 126,000 satisfying the condition of Lemma 13".