FINITE GROUPS WITH NILPOTENT CENTRALIZERS[1]

BY

MICHIO SUZUKI

Introduction. The purpose of this paper is to clarify the structure of finite groups satisfying the following condition:

(CN): the centralizer of any nonidentity element is nilpotent.

Throughout this investigation we consider only groups of finite order. A group is called a (P)-group if it satisfies a group theoretical property (P). In this paper we shall clarify the structure of nonsolvable (CN)-groups and classify them as far as possible. This goal has been attained in a sense which we shall explain later.

If we replace in (CN) the assumption of nilpotency by being abelian we get a stronger condition (CA). The structure of (CA)-groups has been known. In fact after an initial attempt by K. A. Fowler in his thesis [8], Wall and the author have shown that a nonsolvable (CA)-group of even order is isomorphic with $LF(2, q)$ for some $q = 2^n > 2$. A few years later the author [12] has succeeded in proving a particular case of Burnside's conjecture for (CA)-groups, namely a nonsolvable (CA)-group has an even order. Quite recently Feit, M. Hall and Thompson [7] have proved the Burnside's conjecture for (CN)-groups. We can therefore consider groups of even order and focus our attention to the centralizers of involutions.

We consider the condition (CIT):

(CIT): a group is of even order and the centralizer of any involution is a 2-group.

There is no apparent connection between the class of (CN)-groups and the class of (CIT)-groups. But a nonsolvable (CN)-group is a (CIT)-group (Theorem 4 in Part I). This theorem reduces the study of nonsolvable (CN)-groups to that of (CIT)-groups. Both properties (CN) and (CIT) are obviously hereditary to subgroups (provided that we consider only subgroups of even order in the case of (CIT)). Although it is true that a homomorphic image of a (CN)-group is also a (CN)-group (this statement is false for infinite groups), it is not an obvious statement. On the other hand it is not difficult to show that a factor group of a (CIT)-group is a (CIT)-group, provided that the order is even. This is due to the following characterization of (CIT)-groups: namely a (CIT)-group is a group of even order containing no element of order $2p$ with $p > 2$ and vice versa. This makes the study of (CIT)-groups somewhat easier. The large part of this paper concerns the structure of (CIT)-groups.

There is an important subclass of (CIT)-groups. Zassenhaus [18] has considered a group G satisfying the following condition:

(Z): G is faithfully represented as a doubly transitive permutation group in which only the identity leaves three distinct letters invariant.

The degree of this permutation group is called the degree of a (Z)-group G. If we denote this degree as $1+N$, the number N is a power of a prime number unless G contains a normal subgroup of order $N+1$ (cf. Feit [5]). We shall denote by (ZT) the following conditions on G:

(ZT): G is a (Z)-group of odd degree and G is not a Frobenius group.

It is not too difficult to see that a (ZT)-group is a simple (CIT)-group (Theorem 1 in Part I). One of the main results in this investigation is that the class of simple (CIT)-groups consists of (ZT)-groups and some classical linear fractional groups (see Part III). Precisely we have

THEOREM. *Let G be a simple nonabelian* (CIT)-*group. Then G is one of the following types*:

    (i) *a* (ZT)-*group*,
    (ii) LF(2, p) *with a Fermat prime or a Mersenne prime p*,
    (iii) LF(2, 9) *or*
    (iv) LF(3, 4).
Conversely any one of the above types of groups is a simple (CIT)-*group.*

Thus the study of simple (CIT)-groups is reduced completely to the study of (ZT)-groups. If $q=2^n>2$, the group LF(2, q) is an example of (ZT)-groups. In fact until quite recently this family of groups was the only example of (ZT)-groups. Recently the author [15] has given another infinite family of (ZT)-groups $G(q)$ for $q=2^{2n+1}>2$. The author has been unable to decide whether there would be more (ZT)-groups. Only fragmental results are known for the general (ZT)-groups. The author hopes to return to this subject in the future and would like to remark here that a (ZT)-group is isomorphic with LF(2, q) if and only if the order is divisible by 3. Hence the orders of groups $G(q)$ and all the remaining (ZT)-groups, if any, are prime to 3. Moreover a simple (CIT)-group is one of linear fractional groups if (and of course only if) the order is divisible by 3.

The above theorem solves the problem we had at the beginning. If G is a simple nonabelian (CN)-group, then G is one of the groups mentioned above. Here again the classification would not be complete unless we know the structure of general (ZT)-groups which remain to be investigated.

The author has also been unable to decide whether a nonsolvable (CIT)-group is a (CN)-group or not. So far all the known nonsolvable (CIT)-groups are (CN)-groups. As a matter of fact if every (ZT)-group is a (CN)-group, then all the nonsolvable (CIT)-groups would be (CN)-groups.

Part I discusses a characterization of (ZT)-groups which may be considered as a generalization of the result of Wall and the author. The second

part is a study of general (CIT)-groups. More detailed study of semi-simple (CIT)-groups occupies the long third part, where the theorem stated before is proved in a more general form. The main results of this paper have been published in a short note [16].

We use standard notations throughout. For a subset X of a group G let $N_G(X)$ denote the normalizer of X in G. The centralizer of X is denoted by $C_G(X)$. Theorems or lemmas of the same part are quoted just by numbers. On the other hand quotations from other parts are indicated by inserting the number of the part from which quotation is made. For instance Lemma 5 means the fifth lemma of the same part, but Lemma I.2 indicates it is the second lemma of Part I.

Part I. A characterization of (ZT)-groups

1. **Preliminary remarks on (ZT)-groups.** Let G be a (ZT)-group of degree $q+1$. Then q is a power of 2 by a theorem of Feit [5]. Let F denote the subgroup of G which leaves one letter invariant. Then F is a Frobenius group of order qd where d is a divisor of $q-1$. Let Q be the Sylow 2-group of F and K be a subgroup of order d. Then F is a semi-direct product of Q and K, and coincides with $N_G(Q)$.

Lemma 1. *If τ is an involution of Q, then $C_G(\tau)$ is contained in Q.*

In general we denote by $I(\sigma)$ the set of letters left invariant by σ. Then $I(\rho\sigma\rho^{-1})$ consists of the letters of the form $\rho(a)$ with $a \in I(\sigma)$. Hence if ρ commutes with σ, then ρ leaves the set $I(\sigma)$ fixed. If τ is an involution of Q, $I(\tau)$ consists of a single letter so that $C_G(\tau)$ must be contained in Q. Incidentally Lemma 1 proves that the group F is a Frobenius group since every non-identity element of K induces an automorphism of Q which leaves only the identity invariant.

Lemma 2. *If N is a normal subgroup of G containing Q, then two involutions of N are conjugate in N.*

Proof. First of all remark that any involution of G is contained in N since N is a normal subgroup containing a Sylow 2-group. Since Q is not normal in N, there is a conjugate subgroup Q' of Q which is different from Q. Take involutions $\tau \in Q$ and $\tau' \in Q'$. If the order of $\tau\tau'$ is even, there is an involution τ'' commuting with both τ and τ'. By Lemma 1, τ and τ' would be in the same Sylow 2-group of G. This contradicts the choice of τ and τ'. Hence the order of $\tau\tau'$ is odd and τ is conjugate to τ' in the group generated by τ and τ'. If π is another involution of Q, π is conjugate to τ' in N. Hence π is conjugate to τ in N, proving the assertion.

If for two involutions τ and π of Q we have $\pi = \rho^{-1}\tau\rho$, then $\rho^{-1}Q\rho \cap Q$ contains π. Hence $\rho^{-1}Q\rho$ coincides with Q, that is, $\rho \in F$. Hence the index d is equal to the number of involutions in Q. This implies in particular that the

normal subgroup N of Lemma 2 contains F. Since Q is a Sylow 2-group, we must have $N_G(Q)N = G$. We conclude therefore that G is the only normal subgroup of G containing Q.

THEOREM 1. *A* (ZT)-*group* G *is a nonabelian simple* (CIT)-*group.*

Proof. By Lemma 1 G is a (CIT)-group. We need only to show its simplicity. Assume the contrary. Let H be the smallest proper normal subgroup of G. By the preceding argument H does not contain the subgroup Q. Let R be the intersection $Q \cap H$. The group $H \cap F$ is a normal subgroup of F. Since F is a Frobenius group, $H \cap F$ is contained in Q. Hence we have $H \cap F = H \cap F \cap Q = R$. Suppose that $R \neq e$. Then H contains all the involutions of G. If R contains more than one involution, we have $N_H(R) \neq R$ since involutions of R are conjugate in $N_H(R)$. This is not the case because

$$R \neq N_H(R) \subseteq N_G(Q) \cap H = H \cap F.$$

Hence R contains only one involution. R is therefore either cyclic or a generalized quaternion group. If R is cyclic, a theorem of Burnside [4, §243] shows the existence of a normal subgroup H_1 of H such that $H = RH_1$. This contradicts the minimum choice of H. If R is a generalized quaternion group, H is not simple by a theorem of Brauer and Suzuki [3]. Since H is minimum, H is characteristic simple. If H is not simple, it is a direct product of isomorphic simple groups. Such a group has more than one involution in a Sylow 2-group. This is a contradiction. Hence we must have $R = e$. Then the group Q induces fixed-point-free automorphisms in H by Lemma 1. Q is again either cyclic or a generalized quaternion group. Let N be the maximal normal subgroup of odd order. A theorem of Burnside or a theorem of Brauer and Suzuki [3] can be applied to show that G/N contains a central involution. Since G is a (CIT)-group the quotient group G/N is also a (CIT)-group. This implies that G/N is a 2-group and that $G = QN$. The group G is therefore a Frobenius group contrary to the definition of a (ZT)-group.

2. **A characterization of** (ZT)-**groups.** In this section we shall characterize (ZT)-groups by some group theoretical properties. For $\sigma \in G$ we denote by $C_G^*(\sigma)$ the totality of elements of G which transform σ into σ or σ^{-1}.

THEOREM 2. *Let* G *be a group and* H *a subgroup of* G. *Let* H_0 *denote the subgroup of* H *generated by involutions of* H. *Suppose that the following two conditions are satisfied:*

(1) $C_G^*(\sigma) \subseteq H$ *for any* $\sigma \neq 1$ *of* H, *and*

(2) *the center of* H_0 *is not trivial.*

Then we have one of the following four cases:

(i) H_0 *is a normal subgroup of* G,

(ii) *a Sylow 2-group of* G *is cyclic,*

(iii) *a Sylow 2-group of* G *is a generalized quaternion group, or*

(iv) G *is a* (ZT)-*group and* H *is a Sylow 2-group of* G.

Proof of this theorem requires a few lemmas of which the first is the following:

LEMMA 3. *Under the assumptions of Theorem 2, H is a group of even order containing a Sylow 2-group of G.*

Proof. By the assumption (2) the group H_0 contains more than one element. Hence there is at least one involution in H. The order of H is obviously even. The last assertion is a particular case of the next lemma.

LEMMA 4. *Let H be a subgroup of G satisfying the condition*

(1'): $C_G(\sigma) \subseteq H$ *for any $\sigma \neq 1$ of H.*

Then H is a Hall subgroup of G.

Proof. It suffices to show that a Sylow group of H is a Sylow subgroup of G. Let S be a Sylow subgroup of H. By way of contradiction suppose that S is not a Sylow subgroup of G. By a theorem of Sylow S is contained in a Sylow group S' of G. There is a subgroup T of S' containing S as a proper normal subgroup. By a property of p-groups S contains a central element $\sigma \neq 1$ of T. Hence we have

$$C_G(\sigma) \supseteq T \underset{\neq}{\supseteq} S.$$

Since S was a Sylow group of H, H can not contain T. Hence $C_G(\sigma)$ is not a part of H violating the condition (1').

LEMMA 5. *The condition (1) in Theorem 2 implies the condition (1') of Lemma 4 and the condition*

(1'')   *if $\sigma \neq 1$ of H is a product of two involutions τ and τ' of G, then τ is contained in H.*

Proof. From the definition it is clear that $C_G(\sigma) \subseteq C_G^*(\sigma)$. Hence the condition (1') is a consequence of the condition (1). Suppose that $\sigma = \tau\tau'$. Then τ transforms σ into σ^{-1}. Hence $\tau \in C_G^*(\sigma) \subseteq H$.

For any group G let $n(G)$ denote the number of involutions in G.

LEMMA 6. *Let H be a subgroup of G satisfying the condition (1'') of Lemma 5. Then we have*

$$n(G) \leqq n(H) + [G:H] - 1.$$

Proof. Consider any coset X modulo H. If $X = H$, X contains exactly $n(H)$ involutions. Suppose $X \neq H$. If X contains two different involutions τ and τ', then the product $\tau\tau'$ is an element of H and $\tau\tau' \neq 1$. By the condition (1'') τ is an element of H. This is not the case. Hence any coset $\neq H$ contains at most one involution. The inequality follows immediately.

We shall return to the proof of Theorem 2 and assume the conditions (1'), (1''), (2). Let us assume that H_0 is not a normal subgroup of G. Remark that we have $n(H) = n(H_0)$ by definition. Since H_0 is not normal in G, there is a conjugate subgroup H_1 of H_0 different from H_0. We want to show that $H_1 \cap H$ contains no involution. Suppose that it does. Take one, say τ, of involutions in $H_1 \cap H$. By (2) there is an element $\pi \neq 1$ which is in the center of H_1. Then τ commutes with π, since $\tau \in H_1$. By the condition (1') we conclude that π belongs to H since $\pi \in C_G(\tau) \subseteq H$. Again by (1') $C_G(\pi)$ is contained in H. $C_G(\pi)$ certainly contains H_1. Therefore H_1 is a subgroup of H and is generated by involutions. By definition H_1 coincides with H_0. Hence $H_1 \cap H$ contains no involution. Thus we have

$$n(H_1) + n(H) \leq n(G).$$

On the other hand we get $n(G) \leq n(H) + [G:H] - 1$ by Lemma 6. Hence we have

$$n(H) = n(H_1) \leq [G:H] - 1.$$

It follows from Lemma 3 that every involution of G is conjugate to an involution of H. If τ is an involution of H, the number of involutions conjugate to τ is the index $[G: C_G(\tau)]$ which is a multiple of $[G:H]$, since by (1') $C_G(\tau)$ is a subgroup of H. Hence if there are more than one conjugate class of involutions, or there is an involution not contained in the center of H, then we have $n(G) \geq 2[G:H]$. Then we get

$$2[G:H] \leq n(H) + [G:H] - 1, \quad \text{or} \quad [G:H] + 1 \leq n(H).$$

This contradicts the inequality $n(H) \leq [G:H] - 1$. Hence there is exactly one class of involutions in G, and H contains a central involution τ. If τ' is another involution of H, $C_G(\tau')$ is a subgroup of H by (1') and has the same order as $C_G(\tau) = H$. Hence every involution of H lies in the center of H. The group H_0 is an elementary abelian subgroup of the center of H and $C_G(H_0) = H$.

Let L be the normalizer $N_G(H_0)$ of H_0. Since $H = C_G(H_0)$, H is a normal subgroup of L. Burnside's argument shows that two involutions of H are conjugate in L. Hence $t = [L:H] = n(H)$. Since t is odd, no coset $\neq H$ modulo H in L contains any involution. We have therefore

$$[G:H] = n(G) \leq n(H) + [G:H] - [L:H].$$

This implies that every coset modulo H outside of L contains exactly one involution.

If Y is a coset modulo L and if $Y \neq L$, Y consists of t cosets modulo H and all those cosets are outside of L. Hence Y contains exactly t involutions $\tau_1, \cdots, \tau_t$. Then $\tau_i \tau_t (1 \leq i < t)$ are $t-1$ elements of L. If Z is another coset $\neq L$ modulo L, Z contains t involutions $\pi_1, \cdots, \pi_t$. Suppose that we have $\tau_1 \tau_t = \pi_1 \pi_i$. Then $\rho = \tau_1 \tau_t$ is an element of L and commutes with $\tau_1 \pi_1$. We want

to conclude that $\tau_1\pi_1$ is an element of L and hence the coset Z coincides with Y. We need a lemma.

LEMMA 7. *Suppose an element $\rho \neq 1$ of L is a product of two involutions. Then $C_G(\rho)$ is contained in L.*

Proof. Suppose that an element σ outside of L commutes with ρ. The cosets modulo H outside of L contain exactly one involution. Hence we may write σ as a product $\eta\tau$ where $\eta \in H$ and τ is an involution. Since $\sigma \notin L$, τ is not contained in H. The equation $\rho\sigma = \sigma\rho$ implies that $\eta^{-1}\rho\eta = \tau\rho\tau$. Hence we get $\rho^{-1}\eta^{-1}\rho\eta = \rho^{-1}\tau\rho\tau$. It is clear that the group $\{H, \rho\}$ contains H as a normal subgroup. Hence the commutator $\rho^{-1}\eta^{-1}\rho\eta$ is an element of H. H contains therefore the product of two involutions τ and $\rho^{-1}\tau\rho$. The condition (1″) says that $\tau \in H$. This is not the case.

This lemma and the argument of this part are essentially ideas of Feit [6]. Returning to the proof of Theorem 2, we see that each coset $\neq L$ modulo L contributes exactly $t-1$ elements of L and there is no coincidence. Hence by counting the number of elements of L we get an inequality

$$[L: e] \geq [H: e] + (t - 1)([G: L] - 1).$$

Denote by h the order of H and by m the index $[G: L]$. Since $t = [L: H]$ we have an inequality

$$(t - 1)(h - m + 1) \geq 0,$$

which implies that either $t = 1$ or $h + 1 \geq m$.

Since $t = n(H)$, the equality $t = 1$ occurs only when H contains exactly one involution. This is the case only if a Sylow 2-group of H is either a cyclic group or a generalized quaternion group. By Lemma 3, we have the case (ii) or (iii) accordingly.

If G is a (Z)-group of odd degree $1+q$ but not a (ZT)-group, then G contains a normal subgroup G_1 of order $1+q$. Then a Sylow group Q of G induces fixed-point-free automorphisms of G_1 and hence Q is either cyclic or a generalized quaternion group. Hence in order to finish the proof of Theorem 2 it suffices to show that G is a (Z)-group, assuming $t > 1$.

Suppose that a conjugate subgroup $\rho^{-1}H\rho$ intersects with L nontrivially. By Lemma 4 H is a Hall subgroup of L and is normal in L by definition. Hence the intersection $L \cap \rho^{-1}H\rho$ is a part of H. If $\sigma \neq 1$ is an element of $L \cap \rho^{-1}H\rho$, $C_G(\sigma)$ contains both H_0 and $\rho^{-1}H_0\rho$ and is contained in H. We have therefore $\rho^{-1}H_0\rho = H_0$ and hence $\rho^{-1}H\rho = H$. We have assumed that H_0, and hence H, is not normal in G. There must be a conjugate subgroup H_1 of H different from H. Then $H_1 \cap L = e$, which means two distinct elements of H_1 belong to different cosets modulo L. Hence we obtain an inequality

$$[G: L] \geq 1 + [H_1: e], \quad \text{or} \quad m \geq 1 + h.$$

Combined with the reverse inequality $m \leq 1+h$ we get an equality $m = 1+h$.

We shall represent G as a permutation group Γ on the cosets modulo L. The degree of this representation is $m = 1+h$ and is odd. L is the subgroup consisting of elements leaving one symbol invariant. We claim that the group H is transitive on cosets $L\mu \neq L$ so that the group is at least doubly transitive. Take a coset $L\mu$ and suppose an element $\sigma \neq 1$ of H leaves $L\mu$ invariant. Then we have $L\mu\sigma = L\mu$, which implies that $\mu\sigma\mu^{-1} \in L$. As shown before this is possible only when $\mu\sigma\mu^{-1}$ belongs to H. Hence $\mu \in N_G(H_0) = L$. Since $m = 1+h$, H is transitive on cosets $\neq L$.

Let ϕ be the character of the representation Γ. Since Γ is doubly transitive, ϕ is decomposed as a sum of two irreducible characters over the complex number field: $\phi = 1 + \chi$ (cf. [4, §207]). For any element σ of G the value of ϕ is the number of symbols left invariant by σ. Suppose that $C_1, \cdots, C_k$ are the totality of conjugate classes of G containing no element of H. Let g_i be the number of elements in C_i and x_i the value of ϕ on C_i. If $x_i > 0$, then x_i is at least 2. The identity leaves exactly $m = 1+h$ symbols invariant and each nonidentity of H leaves exactly one symbol fixed. The orthogonality relations yield two equations:

$$2g = \sum_{\sigma \in G} \phi(\sigma)^2 \quad \text{and} \quad g = \sum_{\sigma \in G} \phi(\sigma).$$

Using the values of ϕ we obtain

$$2g = m^2 + m(h-1) + \sum_i x_i^2 g_i$$

and

$$g = m + m(h-1) + \sum_i x_i g_i.$$

Hence by subtracting twice the second equation from the first one we have

$$\sum_i x_i(x_i - 2)g_i = 0.$$

Since $x_i = 0$ or $x_i \geq 2$, $x_i(x_i - 2)$ is non-negative. Hence for any i, either $x_i = 0$ or $x_i = 2$. This shows that the identity is the only element which leaves three different symbols invariant. G is a (Z)-group by definition and the assertion of Theorem 2 is proved.

COROLLARY. *Let H be a nilpotent subgroup of even order in G. Assume that H satisfies the condition* (1') *of Lemma 4. Then we have one of the four cases:*
(i) *H is a normal subgroup of G,*
(ii) *a Sylow 2-group of G is cyclic,*
(iii) *a Sylow 2-group of G is a generalized quaternion group or*
(iv) *G is a (ZT)-group and H is a Sylow 2-group of G.*

Proof. Let H_0 be the subgroup of H generated by involutions of H. Since H is nilpotent, the center of H_0 is not trivial. This proves the second condition (2) for H. By Lemma 4, H is a Hall subgroup of G. Suppose an element $\sigma \neq 1$ of H is a product of two involutions τ and τ'. Then τ is contained in $C_G^*(\sigma)$. If the order of σ is odd, then $C_G(\sigma)$ contains a Sylow 2-group of H. Since H is a Hall subgroup we have $C_G^*(\sigma) = C_G(\sigma)$ and hence $C_G^*(\sigma)$ is contained in H by (1'). Hence $\tau \in H$. On the other hand if the order of σ is even, a power of σ commutes with τ. By (1') τ must be an element of H. Thus the condition (1'') of Lemma 5 is satisfied. Hence Theorem 2 can be applied. We need only to show the first case of Theorem 2 implies the normality of H. Suppose that H is not normal. Then there is a conjugate subgroup H_1 of H and $H_1 \neq H$. Since H_0 is normal, H_1 contains H_0. By a property of nilpotent groups H_0 contains a central element of H_1. By (1') we get a contradiction.

We remark that the assumption of the nilpotency of H can be replaced by the following one. H is a direct product of a 2-group and any group of odd order.

The next theorem is a particular case of Theorem 2 and characterizes (ZT)-groups among simple groups of composite order.

THEOREM 3. *Let G be a group and H a subgroup of G satisfying the conditions (1) and (2) (or (1'), (1'') and (2)) of Theorem 2. If G is a simple group of order greater than 2, then G is a (ZT)-group. Conversely any (ZT)-group contains a subgroup satisfying the conditions (1) and (2).*

Proof. By Theorem 2 we have one of four cases for G. Suppose that H_0 is normal in G. Then being a characteristic subgroup of H_0, the center C of H_0 is a normal subgroup of G. Obviously C is an abelian group of even order. Hence if G is simple, C coincides with G and is a group of order 2.

If a Sylow 2-group S is cyclic, G contains by a theorem of Burnside [4] a normal subgroup N such that $G = NS$ and $N \cap S = e$. If G is simple we have $N = e$ so that $G = S$. Again the order of G must be 2.

If G is simple its Sylow 2-group can not be a generalized quaternion group by a theorem of Brauer and the author [3]. Hence the only possibility remaining is the last case (iv).

If conversely G is a (ZT)-group, its Sylow 2-group H satisfies the condition (1) (cf. the proof of Lemma 1). The condition (2) is trivial since H is a 2-group.

3. **Applications.** The next two theorems are also corollaries to Theorem 2.

THEOREM 4. *A nonsolvable (CN)-group is a (CIT)-group.*

Proof. Let G be a nonsolvable (CN)-group. By a theorem of Feit, M. Hall and Thompson [7], the order of G is even. By way of contradiction suppose that G is not a (CIT)-group. Then there are nilpotent subgroups of even

order which are not a 2-group. Among them choose one, say M, with the largest possible order. Since M is nilpotent M is a direct product of a 2-group M_0 and a group of odd order. Consider a Sylow 2-group Q containing M_0. If $Q \neq M_0$, there is a subgroup T of Q containing M_0 as a proper normal subgroup. Then M_0 contains a central element $\sigma \neq 1$ of T. The centralizer $C_G(\sigma)$ contains T as well as M and by assumption $C_G(\sigma)$ is nilpotent. This contradicts the definition of M. Hence M contains a Sylow 2-group Q. If $M = Q \times K$, K contains at least two elements by definition. Let ρ be an element $\neq 1$ of the center of K. It is clear that $C_G(\rho)$ is a nilpotent subgroup containing M. From the maximal choice $C_G(\rho) = M$. Similarly if τ is a nonidentity element of the center of Q, we have $C_G(\tau) = M$. We want to show that the group M satisfies the condition (1'). Let σ be any element $\neq 1$ of M. If $\sigma \in K$, $C_G(\sigma)$ is by definition a nilpotent group containing Q. Since Q is a Sylow 2-group Q is a direct factor of $C_G(\sigma)$. Hence $C_G(\sigma) \subseteq C_G(\tau) = M$. If $\sigma \notin K$, a power π of σ is a nonidentity element of Q. $C_G(\pi)$ is a nilpotent group containing $C_G(\sigma)$ and K. If $C_G(\pi) = R \times S$ where R is a 2-group and S is of odd order, K is a part of S. If $S \neq K$, there is a subgroup of S containing K as a proper normal subgroup. Then there is an element $\neq 1$ of K whose centralizer contains M as a proper subgroup. This is not the case. Hence we have

$$C_G(\pi) = R \times K \subseteq C_G(\rho) = M.$$

By the above corollary we have one of the four cases. If the group M is normal G/M is a solvable group, since all the Sylow groups are cyclic (cf. Zassenhaus [19]). If a Sylow group of G is either a cyclic group or a generalized quaternion group, then the factor group G/N by the maximal normal subgroup N of odd order contains a central involution (cf. the last part of the proof of Theorem 1). If τ is an involution of G, τN is the central involution of G/N and $G = NC_G(\tau)$. By assumption $C_G(\tau)$ is nilpotent. Since $G/N \cong C_G(\tau)/N \cap C_G(\tau)$, G/N is also nilpotent. Since the order of N is odd, N is solvable by a theorem of Feit, M. Hall and Thompson [7]. Hence in both cases G is a solvable group contrary to the assumption. Since M is not a Sylow 2-group, the last case (iv) can not happen either. Hence G is a (CIT)-group.

THEOREM 5. *Let G be a (CIT)-group and S a Sylow 2-group of G. Assume that Sylow 2-groups of G are independent. Then we have one of the following:*
(i) *S is normal,*
(ii) *S is cyclic,*
(iii) *S is a generalized quaternion group or*
(iv) *G is a (ZT)-group.*

Proof. If $\sigma \neq 1$ is an element of S and if $\rho \sigma = \sigma \rho$, then σ is contained in both S and $\rho^{-1} S \rho$. Since Sylow 2-groups are independent by assumption, $\rho^{-1} S \rho$ coincides with S. This means that ρ is an element of $N_G(S)$. Since G is a

(CIT)-group the order of ρ is a power of 2. Since $\rho \in N_G(S)$, ρ must be an element of S. Therefore the group S satisfies the condition $(1')$ of Lemma 4. The corollary of Theorem 2 proves the assertion of Theorem 5.

PART II. PROPERTIES OF GENERAL (CIT)-GROUPS

1. **The structure of solvable** (CIT)-**groups.** In this section we shall study the structure of solvable (CIT)-groups. The first theorem is however proved in a slightly more general form.

THEOREM 1. *Let G be a* (CIT)-*group. Assume that G contains a proper normal subgroup of odd order. Then G is a solvable group. In this case G contains an abelian normal subgroup A of odd order such that $G = AS$ for a Sylow 2-group S of G and no element $\neq 1$ of A commutes with an element $\neq 1$ of S.*

Proof. By assumption G contains proper normal subgroups of odd order. Let N be one of them. Since the order of G is even there is a Sylow 2-group S of G such that $S \cap N = e$. If τ is a central involution of S, τ induces an automorphism of order 2 in N, which leaves only the identity invariant. Hence by a result of Burnside N is abelian and τ maps any element of N into its inverse. If S contains another involution τ', τ' would also map every element of N into its inverse. Then the product $\tau\tau'$ would be an involution of S which commutes with every element of N. This is a contradiction to the condition (CIT). Hence S contains only one involution. Such a 2-group is either a cyclic group or a generalized quaternion group. Thus the proof of Theorem 1 is reduced to the proof of the following proposition.

PROPOSITION 1. *Suppose that a Sylow 2-group S of a* (CIT)-*group G is either a cyclic group or a generalized quaternion group. Then G contains an abelian normal subgroup A of odd order such that $G = AS$ and no element $\neq 1$ of S commutes with an element $\neq 1$ of A. In particular G is a Frobenius group.*

Proof. Let A be the normal subgroup of G with the greatest possible odd order. As before A is abelian. If S is cyclic, A satisfies the condition $G = AS$ by a theorem of Burnside [4, §243]. On the other hand if S is a generalized quaternion group, the group G/A contains a central involution by a theorem of Brauer and Suzuki [3]. There is an involution τ of S such that the coset τA is in the center of G/A. If σ is any element of G, the element $\sigma^{-1}\tau\sigma$ generates a Sylow 2-group of the subgroup $\{A, \tau\}$. Hence by a Sylow's theorem there is an element ρ of A such that $\sigma^{-1}\tau\sigma = \rho^{-1}\tau\rho$. Then the element $\sigma\rho^{-1}$ belongs to the centralizer of τ in G which is by assumption the group S. Hence $\sigma\rho^{-1} \in S$ and so we have $G = SA$. Since every element $\neq 1$ of S induces a fixed-point-free automorphism of A, the group G is a Frobenius group and the proposition follows immediately.

The solvability of G in Theorem 1 follows from the condition $G = AS$. The above theorem is supplemented by the next theorem.

THEOREM 2. *Let G be a solvable* (CIT)*-group. If G contains no proper normal subgroup of odd order, G has a series of normal subgroups*

$$G \supset L \supset N \supset e$$

such that G/L and L/N are cyclic groups of relatively prime orders, N is a 2-group and the extension of G over N splits. If moreover the order G/N is even, the group G/L is a 2-group and induces fixed-point-free automorphisms of L/N.

Proof. Since G is solvable, G contains a proper normal subgroup of prime power order. By assumption all proper normal subgroups are of even order. Hence G contains a normal subgroup which is a 2-group. Let N be the normal subgroup of the greatest possible 2-power order. Then $N \neq e$.

Suppose that the group G/N is of odd order. If T is a Sylow p-group for some odd prime p, the group NT is a Frobenius group by the condition (CIT). Hence T is a cyclic group. By a result of Zassenhaus [19] there is a normal subgroup L of G such that both G/L and L/N are cyclic and the orders are relatively prime. The splitting of the extension of G over N is proved by a theorem of Schur [20, p. 125].

Assume that the order of G/N is even. Then the group G/N is a (CIT)-group containing a proper normal subgroup of odd order. By Theorem 1 there is a normal subgroup L of G such that $G \supset L \supset N$, G/L is a 2-group and L/N is an abelian group of odd order. As shown before every Sylow group belonging to an odd prime is cyclic. This implies that L/N is cyclic. The group G/L is isomorphic with a Sylow 2-group of G/N which is either a cyclic group or a generalized quaternion group. On the other hand the group G/N is a Frobenius group. Hence the group G/L is isomorphic with a subgroup of the group of automorphisms of L/N. Since L/N is cyclic, G/L must be abelian. Hence the group G/L is also cyclic.

The only thing left is to show that the extension of G over N splits. By the splitting theorem of Schur [20] L contains a subgroup H such that

$$L = NH \quad \text{and} \quad N \cap H = e.$$

Since L is solvable, the subgroup $\sigma^{-1}H\sigma$ for $\sigma \in G$ is conjugate to H in L. This implies that $G = LK$ with $K = N_G(H)$. Since $L = NH$ and $H \subseteq K$, we have $G = NK$. On the other hand $K \cap L$ is the normalizer of H in L and hence

$$K \cap L = (K \cap N) \times H.$$

From the condition (CIT) it follows that $K \cap N = e$. Therefore the subgroup K is a complement of N in G.

2. **Remarks on general** (CIT)**-groups.** Using Proposition 1 the theorem at the end of Part I may be stated in the following form.

THEOREM 3. *Let G be a* (CIT)*-group. If Sylow 2-groups are independent, then G is either a solvable Frobenius group or a* (ZT)*-group.*

Proof. Let S be a Sylow 2-group of G. If G is not a (ZT)-group, we have one of the following two cases: (1) S is normal or (2) S is either cyclic or a generalized quaternion group. In the first case all Sylow groups of G/S are cyclic. Hence by a theorem of Burnside G is solvable. The solvability in the case (2) is shown in Proposition 1.

THEOREM 4. *Let G be a nonsolvable* (CIT)-*group. Then the maximal solvable normal subgroup of G is a 2-group.*

Proof. Let N be the maximal solvable normal subgroup of G. Suppose that $N \neq e$. Since N is solvable, N contains a characteristic subgroup $M \neq e$ of prime power order. Then M is a normal subgroup of G. Since G is assumed to be nonsolvable M is a 2-group by Theorem 1. We may assume that M has the greatest possible order.

By way of contradiction suppose that N is larger than M, and consider the group G/M. If the group G/M is of odd order all Sylow groups of G/M are cyclic, since G is a (CIT)-group. This would imply the solvability of G/M and hence of G. This contradicts the assumption. If the group G/M is of even order G/M is a (CIT)-group. Since $N \neq M$, G/M would contain a normal subgroup of odd order. This would imply again the solvability of G/M by Theorem 1. Hence we must have $M = N$.

3. **The family $\mathfrak{H}$ of 2-subgroups of G.** In the following discussion on the structure of general (CIT)-groups a family of 2-subgroups of G attracts our attention.

Let $\mathfrak{H}$ be the collection of 2-subgroups of G defined by the following properties: $H \in \mathfrak{H}$ if (1) $H \neq e$, (2) $N_G(H)$ contains at least two Sylow 2-groups and (3) H is the maximal normal 2-subgroup of $N_G(H)$.

LEMMA 1. *The family $\mathfrak{H}$ of 2-subgroups of G is empty if and only if Sylow 2-groups of G are independent.*

Proof. If $\mathfrak{H}$ is not empty we can take a subgroup H which belongs to $\mathfrak{H}$. Then by (2) the normalizer $N = N_G(H)$ contains at least two Sylow 2-groups. If Q and Q' are Sylow 2-groups of N, $Q \cap Q'$ contains H and $H \neq e$ by (1). By a theorem of Sylow Q and Q' are contained in Sylow 2-groups P and P' of G respectively. Since $Q \neq Q'$, P is different from P'. Thus $P \neq P'$ and

$$P \cap P' \supseteq H \neq e.$$

Sylow 2-groups are therefore not independent.

Conversely assume that Sylow 2-groups are not independent. Let D be a maximal intersection of Sylow 2-groups. Then $D \neq e$ by assumption. If $D = P_1 \cap P_2$ for Sylow 2-groups P_1 and P_2, the normalizers of D in P_1 and P_2 are larger than D by a property of 2-groups. Hence the normalizer N of D contains at least two Sylow 2-groups. Since D is a maximal intersection, D must be the maximal normal 2-group of N. Hence D is in $\mathfrak{H}$.

Sometimes the following lemma is useful.

LEMMA 2. *If $D \neq e$ is a 2-subgroup of G such that $N_G(D)$ contains at least two Sylow 2-groups, then there exists a subgroup H in $\mathfrak{H}$ such that*

$$H \supseteq D \quad and \quad N_G(H) \supseteq N_G(D).$$

Proof. Let D_1 be the maximal normal 2-subgroup of $N_G(D)$. Then

$$D_1 \supseteq D \quad and \quad N_G(D_1) \supseteq N_G(D).$$

Hence $N_G(D_1)$ contains at least two Sylow 2-groups. We shall define a sequence of subgroups D_i by induction. Suppose D_j for $j < i$ have been defined and satisfy the properties

$$D_{i-1} \supseteq D_{i-2} \supseteq \cdots \supseteq D \quad and \quad N_{i-1} \supseteq N_{i-2} \supseteq \cdots \supseteq N_G(D)$$

where $N_j = N_G(D_j)$. Let D_i be the maximal normal 2-subgroup of N_{i-1}. Then clearly we have

$$D_i \supseteq D_{i-1} \quad and \quad N_i \supseteq N_{i-1}.$$

Since G is a finite group the sequence $\{D_i\}$ must terminate after a finite number of steps. If $H = \cup D_i$, $H = D_n$ for large values of n. By definition H is the maximal normal 2-group of $N_G(D_n) = N_G(H)$. This is the third requirement for H to be a member of $\mathfrak{H}$. The first two are also satisfied as is seen from the construction. Hence H is in $\mathfrak{H}$.

The family $\mathfrak{H}$ is a partly ordered set by the usual order relation defined by inclusion. Thompson [17] has introduced another order in $\mathfrak{H}$ so as to make another partly ordered set. We define a relation $\gg$ in $\mathfrak{H}$ in the following way. Let $H_i \in \mathfrak{H}$ for $i = 1, 2$. Denote by N_i the normalizer of H_i in G, by n_i the order of N_i and by 2^{e_i} the order of a 2-Sylow subgroup of N_i. We define

$$H_1 \gg H_2 \quad if \quad (1)\ e_1 > e_2, \quad or \quad (2)\ e_1 = e_2, n_1 > n_2, \quad or \quad (3)\ H_1 = H_2.$$

It is easy to see that the relation defined above satisfies the usual three axioms for an order and the set $\mathfrak{H}$ becomes a partly ordered set. In the following we shall refer to this order as the Thompson order in order to distinguish it from the usual one.

4. Conjugacy of involutions in (CIT)-groups. This section is devoted to the proof of the following theorem.

THEOREM 5. *Let G be a (CIT)-group and N the maximal normal 2-subgroup of G. If the order of G/N is even, G contains an involution outside of N and any two involutions not contained in N are conjugate to each other.*

Before entering the proof which is quite involved, we remark that if G is nonsolvable the order of G/N is by Theorem 4 automatically even. We need a few lemmas, of which the first is the following.

LEMMA 3. *Assume that a* (CIT)-*group* G *contains two Sylow 2-groups* S *and* S' *such that* $S \cap S' = e$. *Then all the involutions form a single conjugate class.*

Proof. By assumption $S \neq e$, so that we can take an involution τ_0 in the center of S. By way of contradiction suppose that there exists an involution τ which is not conjugate to τ_0. By assumption the centralizer $C_G(\tau)$ is a 2-group. By a theorem of Sylow $C_G(\tau)$ is conjugate to a subgroup of S. We may therefore assume that S contains $C_G(\tau)$. Take an arbitrary Sylow 2-group T of G. Then there is a central involution τ' of T such that τ' is not conjugate to τ. Then there is another involution π of G which commutes with both τ and τ'. Hence we have

$$\pi \in C_G(\tau) \cap C_G(\tau') \subseteq S \cap T.$$

This implies in particular that $S \cap T \neq e$. Since T was arbitrary we get a contradiction to the assumption. Therefore involutions form a single conjugate class.

LEMMA 4. *Let* G *and* N *be as stated in Theorem 5. Assume that the order of* G/N *is even. If there are two Sylow 2-groups* S *and* S' *of* G *such that* $S \cap S' = N$, *then the conclusions of Theorem 5 hold.*

Proof. Consider the natural homomorphism ϕ of G onto G/N. Then the groups $\phi(S)$ and $\phi(S')$ are Sylow 2-groups of G/N satisfying the condition $\phi(S) \cap \phi(S') = e$. We apply Lemma 3 to the group G/N and conclude that involutions of G/N form a single conjugate class. Let π and π' be central involutions of $\phi(S)$ and $\phi(S')$ respectively. The subgroup $\{\pi, \pi'\}$ generated by π and π' is a dihedral group containing $\{\pi\}$ as a Sylow 2-group. Let H be the subgroup of G containing N such that $\phi(H) = \{\pi, \pi'\}$. Then H is a solvable (CIT)-group. If H contains a normal subgroup T of odd order, every element of T must commute with any element of N. By the condition (CIT) T must be trivial. Hence H satisfies the assumption of Theorem 2. Since N is clearly the maximal normal 2-group of H, the extension of H over N splits. This means that there is a subgroup D of H isomorphic with the dihedral group $\{\pi, \pi'\}$. Hence D contains involutions τ such that $\phi(\tau) = \pi$. Since $\tau \notin N$ we have proved the first assertion of existence. If σ is any involution of G outside of N, the element $\phi(\sigma)$ is an involution of G/N and is conjugate to π'. We may therefore assume that $\phi(\sigma) = \pi'$. If σ is not conjugate to τ the order of $\sigma\tau = \rho$ must be even. Hence by assumption it is a power of 2. Then the same is true for $\phi(\rho) = \pi\pi'$. This is, however, not the case since no element except the identity commutes with both π and π'. Hence σ is conjugate to τ in G as claimed.

The next lemma is more complicated to prove, but this is the final step in the proof of Theorem 5.

LEMMA 5. *Let G and N be as stated before. If the order of G/N is even, G contains Sylow 2-groups S and S' satisfying*

$$S \cap S' = N.$$

Proof. We use the inductive argument on the order of G.

Suppose $N \neq e$. The group G/N is by assumption a (CIT)-group of order less than that of G. Since N is the maximal normal 2-subgroup of G, the group G/N does not contain any proper normal 2-group. By inductive hypothesis there are Sylow groups T and T' of G/N such that $T \cap T' = e$. We take subgroups S and S' of G such that $S/N = T$ and $S'/N = T'$. Then we have $S \cap S' = N$ and both S and S' are Sylow 2-groups of G.

Assume that $N = e$. If Sylow 2-groups are independent, Lemma 5 is trivially true. We assume that Sylow 2-groups are not independent. Let $\mathfrak{H}$ be the family of 2-subgroups of G defined in the previous section. By Lemma 1 and by the assumption just made the family $\mathfrak{H}$ is not empty. We remark that for any $H \in \mathfrak{H}$ the normalizer $N_G(H)$ is a proper subgroup of G so that we may apply inductive hypothesis to $N_G(H)$, since we have assumed that $N = e$.

For each $H \in \mathfrak{H}$ let $O(H)$ denote the set of elements of $N_G(H)$ outside of H: $O(H) = N_G(H) - H$. Let Z be the subgroup of the center of a Sylow 2-group generated by involutions. For any subgroup K of G let $V(K)$ denote the subgroup of K generated by subgroups of K which are conjugate to Z in G. Clearly the subgroup $V(K)$ is a normal subgroup of $N_G(K)$.

Assume that there is a subgroup H in $\mathfrak{H}$ satisfying the condition that $O(H)$ contains an involution conjugate to some element of Z. By inductive hypothesis $N_G(H)$ contains two Sylow 2-groups P and P' such that $P \cap P' = H$. By Lemma 4 involutions in $O(H)$ are conjugate to each other. We can take two involutions τ and τ' of $N_G(H)$ in such a way that $\tau H(\tau'H)$ belongs to the center of $P/H(P'/H)$. Since we assumed that $O(H)$ contains an involution conjugate to an element of Z, τ must belong to the center of some Sylow 2-group and the same is true for τ'. Hence both $S = C_G(\tau)$ and $S' = C_G(\tau')$ are Sylow 2-groups of G. Suppose that $S \cap S' \neq e$. Then there exists an involution π in $S \cap S'$ and $C_G(\pi)$ contains τ and τ'. By assumption $C_G(\pi)$ is a 2-group. Hence τ and τ' generate a 2-group Q. The group QH/H contains both τH and $\tau'H$, and has a nontrivial center because it is a 2-group. Hence the centralizer of τH in $N_G(H)/H$ contains at least two elements of the centralizer of $\tau'H$. This is, however, impossible since the centralizer of τH is P/H and that of $\tau'H$ is P'/H. Hence $S \cap S' = e$ as was to be shown.

We want to derive a contradiction out of the assumption that for any $H \in \mathfrak{H}$, $O(H)$ contains no involution conjugate to an element of Z. By way of contradiction suppose that $O(H) \cap \sigma^{-1}Z\sigma = \varnothing$ for any $\sigma \in G$ and $H \in \mathfrak{H}$. This assumption implies that $V(H) = V(N_G(H))$ for all $H \in \mathfrak{H}$. In particular we have $V(H) \neq e$.

Let H_0 be a subgroup of $\mathfrak{H}$ which is maximal in the Thompson order.

Let P be a Sylow 2-group of $M = N_G(H_0)$. Consider the subgroup $V = V(H_0)$. V is a normal subgroup of M. Hence $N_G(V)$ contains M. If P is not a Sylow 2-group of G, P is contained in a 2-group T as a proper normal subgroup. Since $V = V(P)$, $N_G(V)$ contains T. By Lemma 2 there is a subgroup H of $\mathfrak{H}$ such that $H \supseteq V$ and $N_G(H) \supseteq N_G(V)$. Since $N_G(H) \supseteq T \underset{\neq}{\supseteq} P$, the subgroup H would be larger than H_0 in the Thompson order. This is impossible since we took H_0 to be maximal. Hence P is a Sylow subgroup of G. Similarly we see that $N_G(V) = M$. It follows now that the subgroup H_0 is uniquely determined by P. Namely H_0 is the maximal normal 2-group of $N_G(V)$ where $V = V(P)$. We denote $H_0 = H(P)$.

We shall show that if P and P' are two Sylow 2-groups of G and if $P \cap P' \neq e$, then $P \cap P' \supseteq H(P)$.

First of all we remark that the relation $P \cap P' \supseteq H(P)$ implies that $H(P') = H(P)$. In fact if a Sylow 2-group T contains $H(P)$, T contains $V(P) = V$. Hence $V(T) = V$. This implies that $H(T) = H(P)$. In order to prove the above statement we suppose, by way of contradiction, that there is a pair of Sylow 2-groups P and P' such that $P \cap P' \neq e$ and $P \cap P' \underset{\neq}{\supseteq} H(P)$. Denote by D the intersection $P \cap P'$ and assume that we have chosen a pair P and P' so as to make the order of D as large as possible under the two restrictions.

Suppose that $N_G(D)$ contains only one Sylow 2-group Q. Let P'' be a Sylow 2-group of G containing Q. by a property of 2-groups D is different from $N_P(D)$ and also from $N_{P'}(D)$. Hence $P'' \cap P \supseteq N_P(D) \neq D$. Since D has a maximal order, we conclude that

$$P'' \cap P \supseteq H(P).$$

Similarly we get $P'' \cap P' \supseteq H(P')$. But as remarked before these relations yield equations

$$H(P) = H(P'') = H(P') \quad \text{and} \quad D = P \cap P' \supseteq P \cap P' \cap P'' \supseteq H(P).$$

This is not the case. Thus $N_G(D)$ contains at least two Sylow groups.

Suppose that D is not the maximal normal 2-group of $N_G(D)$. By Lemma 2 there is a subgroup D' of $\mathfrak{H}$ such that $D' \supseteq D$ and $N_G(D') \supseteq N_G(D)$. Since D does not belong to $\mathfrak{H}$, D' is larger than D. The group $P \cap N_G(D)$ contains D properly. We take a Sylow 2-group P_1 of G containing $(P \cap N_G(D))D'$. Then the intersection $P \cap P_1$ contains $P \cap N_G(D)$ and hence larger than D. From the maximal choice we get

$$P \cap P_1 \supseteq H(P) = H(P_1).$$

Similarly if P_1' is a Sylow 2-group of G containing $(P' \cap N_G(D))D'$, we have

$$P' \cap P_1' \supseteq H(P') = H(P_1').$$

On the other hand we see that $P_1 \cap P_1'$ contains D'. In the same way as above we get $P_1 \cap P_1' \supseteq H(P_1) = H(P_1')$. Hence we conclude that

$$D = P \cap P' \supseteq P \cap P_1 \cap P' \cap P_1' \supseteq H(P).$$

This is a contradiction. Hence D must be a subgroup of $\mathfrak{H}$.

In general we remark that a subgroup H of $\mathfrak{H}$ is an intersection of Sylow subgroups of G. In fact let $Q_1, \cdots, Q_i, \cdots$ be Sylow groups of $N_G(H)$. Then the intersection $\cap_i Q_i$ is the maximal normal 2-group of $N_G(H)$ and hence $H = \cap_i Q_i$. By a theorem of Sylow each Q_i is contained in a Sylow group P_i of G. Let D denote the intersection $\cap_i P_i$. By definition D contains H. If H is a proper subgroup of D, there is a subgroup K of D which contains H as a proper normal subgroup. Hence $D \cap N_G(H) \supseteq K \neq H$. On the other hand for each i, $P_i \cap N_G(H)$ is a 2-group containing Q_i. Since Q_i is a Sylow group of $N_G(H)$, we must have $P_i \cap N_G(H) = Q_i$. Hence $D \cap N_G(H) = \cap_i P_i \cap N_G(H) = \cap Q_i = H$, which is a contradiction. Hence $H = \cap_i P_i$ is an intersection of Sylow groups of G. As a consequence we remark that if a subgroup K of G contains $N_G(H)$, then the maximal normal 2-subgroup of K is contained in H.

We have shown that if there is a pair of Sylow 2-groups P and P' such that $P \cap P' \neq e$ and $P \cap P' \not\supseteq H(P)$, then there is an intersection $D = P_1 \cap \cdots \cap P_k$ of Sylow subgroups of G such that $D \in \mathfrak{H}$ and $D \not\supseteq H(P_1)$. Consider such a subgroup D which is maximal with respect to the Thompson order. Let Q be a Sylow 2-group of $N_G(D)$. Suppose that Q is not a Sylow group of G. Then there is a 2-group T containing Q as a proper normal subgroup. The subgroup $V_0 = V(D)$ is normal in $N_G(D)$ and at the same time normal in T since

$$V_0 = V(N_G(D)) = V(Q).$$

Hence there is a subgroup D_1 of $\mathfrak{H}$ such that

$$D_1 \supseteq V_0, \qquad N_G(D_1) \supseteq N_G(V_0) \supseteq N_G(D)$$

and D_1 is larger than D in the Thompson order. Since $D_1 \in \mathfrak{H}$, D_1 is the maximal normal 2-group of $N_G(D_1)$ and hence by a remark at the end of the preceding paragraph we conclude that $D_1 \subseteq D$. Since we have assumed that $D \not\supseteq H(P_1)$, D_1 does not contain $H(P)$ for any Sylow 2-group P containing D_1. This contradicts the maximal choice of D. Hence Q is a Sylow 2-group of G. If so, by assumption

$$V(D) = V(N_G(D)) = V(Q)$$

and hence $V(Q)$ is a part of D. Since P_1 is another Sylow 2-group containing D, $V(P_1)$ coincides with $V(Q)$ and is also contained in D. By definition $H(P_1)$ is the maximal normal 2-subgroup of $N_G(V(P_1))$. On the other hand since $V(P_1)$ is a part of D, we see that $N_G(V(P_1)) \supseteq N_G(D)$. It follows that D contains $H(P_1)$. This is a contradiction to our assumption. Hence if two Sylow 2-groups P and P' intersect nontrivially, then $P \cap P'$ contains $H(P)$.

Incidentally this part of the argument proves a more general proposition.

Let p be an arbitrary prime number and $\mathfrak{H}_p$ be the family of p-subgroups defined in a similar way as $\mathfrak{H}$ in the third section. For subgroups X and U of G, let $V(X:U)$ denote the subgroup of X generated by conjugate subgroups of U contained in X.

PROPOSITION 2. *Suppose that the family $\mathfrak{H}_p$ is not empty and that there exists a subgroup U of G such that*

$$V(H:U) \neq e \quad and \quad V(H:U) = V(N_G(H):U)$$

for all $H \in \mathfrak{H}_p$. Then a Sylow p-subgroup S of G contains a subgroup K satisfying the following properties: (1) $K \in \mathfrak{H}_p$, (2) $K = V(S:K)$ and (3) if T is another Sylow p-subgroup of G and if $S \cap T \neq e$, then $S \cap T \supseteq K$.

The subgroup $H(S)$ defined in the above proof satisfies the required properties. The first and the last properties are obvious. As for the second property we can prove a stronger result, that K is strongly closed in S. In fact if a conjugate subgroup K' of K intersects nontrivially with S, then K' is contained in a subgroup S' conjugate to S. Then $S \cap S' \neq e$ and this implies, by (3), that $S \cap S' \supseteq K'$. Since $K = H(S)$ and $K' = H(S')$ we conclude that $K = K'$.

In this formulation the actual meaning of $V(X:U)$ is not essential. We can replace $V(X:U)$ by a function V defined on p-subgroups satisfying certain conditions. If $p = 2$ we can say something about the involutions of G. Assume moreover that G contains no proper normal 2-subgroup. Then the subgroup K of Proposition 2 is not normal. There is a subgroup $K' \neq K$, which is conjugate to K. Let P be a Sylow 2-group containing K'. We take two involutions τ and τ' such that $\tau \in K$ and $\tau' \in P$. Let D denote the subgroup generated by τ and τ'. If the order of D is divisible by 4, there are Sylow 2-groups Q and Q' of D such that $Q \ni \tau$, $Q' \ni \tau'$ and $Q \cap Q' \neq e$. Q and Q' are contained in Sylow 2-groups S and S' of G respectively: $Q \subseteq S$ and $Q' \subseteq S'$. Since $\tau \in K$, $S \cap K \neq e$ and we conclude that $S \supseteq K$. The involution τ' is an element of $P \cap S'$ and $P \supseteq K'$. Hence by (3) of Proposition 2 we have $S' \supseteq K'$. Since $S \cap S' \supseteq Q \cap Q' \neq e$, we have again by (3) $S \supseteq K'$ which implies that $K = K'$. This contradiction proves that the order of D is not divisible by 4. Hence τ and τ' are conjugate in D and a fortiori in G. It follows therefore that involutions of G form a single conjugate class. Moreover we conclude that there is no involution in $S - K$, since K is strongly closed in S. As a matter of fact every involution of S is contained in the center of K. This last situation is however impossible in our case of Lemma 5, since there is an involution in $S - K$ by inductive hypothesis. Thus we have proved Lemma 5 and at the same time the proof of Theorem 5 is finished. Moreover we have the following corollary to Proposition 2.

COROLLARY. *Let G be a (CIT)-group having no proper normal 2-group. Assume that the family $\mathfrak{H}$ of 2-subgroups defined in the third section is not empty.*

Then there is no subgroup U of G for which the conditions

$$v(H:U) \neq e \quad and \quad V(H:U) = V(N_G(H):U)$$

are satisfied for all $H \in \mathfrak{H}$.

5. Intersections of Sylow groups. In the following we assume always that G is a (CIT)-group, G contains no proper solvable normal subgroup and Sylow 2-groups are not independent. Theorems 4 and 5 show that G contains one and only one class of conjugate elements containing involutions. If $\mathfrak{H}$ is the family of 2-subgroups defined in the third section, this set $\mathfrak{H}$ is not empty.

LEMMA 6. *If $H \in \mathfrak{H}$, there is a pair of Sylow 2-groups T and T' of G such that $H = T \cap T'$.*

Proof. Let N denote the normalizer $N_G(H)$. By Lemma 5 there are Sylow 2-groups Q and Q' of N such that $Q \cap Q' = H$. Then Q and Q' are contained in Sylow groups T and T' of G. We have

$$Q = T \cap N \quad and \quad Q' = T' \cap N.$$

If $T \cap T'$ contains H properly, there is a subgroup U of $T \cap T'$ which contains H as a proper normal subgroup. Hence

$$T \cap T' \cap N \supseteq U \neq H.$$

On the other hand $T \cap T' \cap N = Q \cap Q' = H$. Hence we must have $T \cap T' = H$.

LEMMA 7. *Let Z be a subgroup of the center of a Sylow 2-group of G. If a Sylow 2-group P contains an involution of Z, then P contains Z.*

Proof. Let τ be the involution of Z contained in P. If C is the center of P, every element of C commutes with τ. Hence $C \subseteq C_G(\tau)$. On the other hand by assumption $C_G(\tau) = S$ is a Sylow 2-group of G containing Z. Hence $C \subseteq S$ and this implies that $Z \subseteq C_G(C) = P$.

In the rest of this section we consider a fixed subgroup Z of the center of some Sylow 2-group of G. As before the subgroup $V(U) = V(U:Z)$ is the subgroup of U generated by all the conjugate subgroups of Z which are contained in U.

LEMMA 8. *There are subgroups H and W of G satisfying the conditions $H \in \mathfrak{H}$, W is conjugate to Z, $N_G(H) \supseteq W$ and $W \cap H = e$.*

Proof. Since Z is a subgroup $\neq e$ of the center of some Sylow 2-group of G, $V(N_G(H))$ is not trivial. Hence by the corollary to Proposition 2, there is a subgroup H of $\mathfrak{H}$ such that $V(N_G(H)) \neq V(H)$. This means that there is a conjugate subgroup W of Z contained in $N_G(H)$ but not in H. We need only

to show that $W \cap H = e$. By Lemma 6, there is a pair of Sylow 2-groups T and T' of G satisfying $T \cap T' = H$. If $W \cap H \neq e$, we have

$$W \cap T \supseteq W \cap H \neq e \quad \text{and} \quad W \cap T' \supseteq W \cap H \neq e.$$

Hence by Lemma 7 we conclude that W is contained in both T and T'. This is a contradiction since $T \cap T' = H$ does not contain W.

LEMMA 9. *Let $\mathfrak{H}_1$ be the family of 2-subgroups of G defined by the conditions: A subgroup H is in $\mathfrak{H}_1$ if and only if $H \in \mathfrak{H}$ and there is a conjugate subgroup W of Z such that*

$$W \subseteq N_G(H) \quad \text{and} \quad W \cap H = e.$$

If a subgroup H of $\mathfrak{H}_1$ is maximal in $\mathfrak{H}_1$ in the usual inclusion, then Sylow 2-subgroups of $N_G(H)/H$ are independent.

Proof. Let G' denote the factor group $N_G(H)/H$. In G' we denote the normalizer of X simply by $N(X)$. Let $\mathfrak{H}'$ be the family of 2-subgroups of G' defined in a similar way as $\mathfrak{H}$. It is necessary to show that $\mathfrak{H}'$ is empty. By way of contradiction suppose that $\mathfrak{H}'$ is not empty.

The group WH/H is a subgroup of G'. Let W' denote the subgroup of WH/H generated by involutions. First of all suppose that there is a subgroup K' of $\mathfrak{H}'$ such that

$$V(K' : W') \neq V(N(K') : W').$$

Take a subgroup K of G such that $K/H = K'$. Elements of G in $N(K')$ form a subgroup N which is the normalizer of K in $N_G(H)$. Since $K' \in \mathfrak{H}'$, $N_G(K)$ contains at least two Sylow 2-groups. Hence by Lemma 2, there is a subgroup H_1 of $\mathfrak{H}$ such that

$$H_1 \supseteq K \quad \text{and} \quad N_G(H_1) \supseteq N_G(K) \supseteq N.$$

By definition of K, there is a subgroup U such that U is conjugate to W in $N_G(H)$ and the subgroup of U generated by involutions is contained in N but not in K. Lemma 5 applied to $N(K')$ shows that there is a pair of Sylow 2-groups Q_1 and Q_2 of N such that $Q_1 \cap Q_2 = K$. Q_i is contained in a Sylow 2-group P_i of $N_G(H_1)$. Then we have $P_1 \cap P_2 \supseteq H_1$. Hence

$$H_1 \cap N \subseteq P_1 \cap P_2 \cap N = Q_1 \cap Q_2 = K.$$

This implies that there is an involution in U which is not contained in H_1. If $H_1 \cap U \neq e$, any Sylow group of G containing H_1 contains U by Lemma 7. Hence U would be a subgroup of H_1. We conclude therefore $H_1 \cap U = e$. This is a contradiction, since $U \subseteq N_G(H_1)$, $H_1 \supseteq K \supsetneq H$ and H was chosen to be maximal subject to those restrictions.

Suppose that there are subgroups of $\mathfrak{H}'$ containing W'. Among them pick one, say L', maximal with respect to the Thompson order. Then we have

$$V(L' : W') = V(N(L') : W')$$

and this group is not equal to e since $L' \supseteq W'$. In a similar way as before $N(L')$ contains a Sylow 2-group Q' of G'. Consider subgroups L, N and Q such that $L/H = L'$, $N/H = N(L')$ and $Q/H = Q'$. Q is a Sylow 2-group of $N_G(H)$ and is contained in a Sylow 2-group S of G. By Theorem 5 Q contains an involution outside of L which is conjugate in $N_G(H)$ to an element of W. Hence there is a subgroup V such that V is conjugate to W in $N_G(H)$ but $V \cap Q \nsubseteq L$. Then we have $V \cap S \neq e$, which implies by Lemma 7 that $V \subseteq S$. This means that $V \subseteq S \cap N_G(H) = Q$. Hence VH/H is a subgroup of $N(L')$ but VH/H contains an involution outside of L'. Hence $V(L': W')$ is smaller than $V(N(L'): W')$; a contradiction.

Hence there is no subgroup of $\mathfrak{H}'$ containing W'. By Theorem 5 involutions form a single conjugate class of G'. Hence each involution of W' is in the center of some Sylow 2-group of G' containing W'. There is however only one Sylow 2-group containing W'. In fact if there are more than one, there would be a member of $\mathfrak{H}'$ containing W'. Hence W' is contained in the center of a Sylow 2-group, which implies that $V(N(L'): W') \neq e$ for any 2-subgroup L' of G'. This is however a contradiction to the corollary of Proposition 2, since

$$V(L': W') = V(N(L'): W')$$

for all $L' \in \mathfrak{H}'$. This finishes the proof of Lemma 9.

PROPOSITION 3. *Let G be a* (CIT)-*group containing no proper solvable normal subgroup, and Z be a subgroup of the center of a Sylow 2-group of G. Then there is a maximal intersection D of Sylow 2-groups of G satisfying the following property: the group $N_G(D)$ contains a conjugate subgroup W of Z such that $W \cap D = e$.*

Proof. This proposition is trivial if Sylow 2-groups of G are independent. Hence we assume the contrary throughout the proof.

Let $\mathfrak{H}_2$ be the family of 2-subgroups of G which is defined as follows. A subgroup H is in $\mathfrak{H}_2$ if and only if $H \in \mathfrak{H}_1$ (see Lemma 9 for the definition) and the Sylow 2-groups of $N_G(H)/H$ are independent. Lemma 9 says that $\mathfrak{H}_2$ is a nonempty subfamily of $\mathfrak{H}$. We shall prove that if D is a subgroup of $\mathfrak{H}_2$ containing the largest number of involutions, then D is a maximal intersection of Sylow 2-groups of G.

First of all we remark that the subgroup $V(H: Z) = V(H)$ contains all the involutions of H. In fact since $H \in \mathfrak{H}$ there is by Lemma 6 a pair of Sylow 2-groups T and T' of G such that $T \cap T' = H$. If τ is an involution of H, τ is in T and T'. By Theorem 5 τ is contained in a conjugate subgroup U of Z. By Lemma 7 U is contained in both T and T' and hence in $H = T \cap T'$. Definition of $V(H)$ implies that $V(H) \supseteq U$. This proves the remark.

Suppose, by way of contradiction, that the subgroup D is not a maximal

intersection. Then there are Sylow 2-groups Q and Q' of G such that $I = Q \cap Q'$ is a maximal intersection containing D. Being a maximal intersection, I is a member of $\mathfrak{H}$. Since I contains D properly, $I \cap N_G(D)$ contains D properly. Hence by Theorem 5 I contains an involution which is not contained in D. Thus the number of involutions of I is larger than that of D.

For each $H \in \mathfrak{H}$ let $n(H)$ denote the number of involutions in H. Let $\mathfrak{H}^*$ denote the subfamily of $\mathfrak{H}$ consisting of H with $n(H) > n(D)$. Then $\mathfrak{H}^*$ is not empty as is seen from the preceding argument.

We want to show that $V(H) = V(N_G(H))$ for all $H \in \mathfrak{H}^*$. Again suppose the contrary. Take one of the groups in $\mathfrak{H}^*$, say H, such that

$$V(H) \neq V(N_G(H)).$$

The last part of the proof of Lemma 8 shows that such an H belongs to $\mathfrak{H}_1$. Let H_1 be a group containing H and maximal in $\mathfrak{H}_1$ (with respect to the usual order). Then $n(H_1) \geq n(H)$ and so $H_1 \in \mathfrak{H}^*$. By Lemma 9 Sylow 2-groups of $N_G(H_1)/H_1$ are independent. This contradicts the definition of D since $n(H_1) > n(D)$ and $H_1 \in \mathfrak{H}_2$.

Consider a group K which belongs to $\mathfrak{H}^*$ and is maximal in the Thompson order. Let P be a Sylow 2-group of $N_G(K)$. Then we have

$$V = V(K) = V(N_G(K))$$

and V contains as many involutions as K. From the definition $N_G(V)$ contains $N_G(K)$. Suppose that P is not a Sylow 2-group of G. Then as before P is not a Sylow 2-group of $N_G(V)$. By Lemma 2 there is a subgroup K_1 of $\mathfrak{H}$ such that $K_1 \supseteq V$ and $N_G(K_1) \supseteq N_G(V)$. Since $K_1 \supseteq V$, we have

$$n(K_1) \geq n(K) > n(D),$$

which means $K_1 \in \mathfrak{H}^*$. The second relation implies that K_1 is larger than K in the Thompson order. This is a contradiction to the definition of K. On the other hand if P is a Sylow 2-group of G, $N_G(K)$ contains an involution outside of K by Theorem 5. By Lemma 7, we get $V(N_G(K)) \neq V(K)$ which is again a contradiction. This proves that D is a maximal intersection of Sylow groups.

Part III. Structure of semi-simple (CIT)-groups

1. **Preliminary remarks.** Throughout this third part we consider only a (CIT)-group G containing no proper solvable normal subgroup, namely we assume that G is semi-simple. If Sylow 2-groups are independent, G is a (ZT)-group (Theorem II.3). The purpose of this part is to determine the structure of G when Sylow 2-groups are not independent. Theorem II.5 and Proposition II.3 are essential in this study. By Proposition II.3, we know the existence of a 2-group H satisfying the following properties: H is a max-

imal intersection of Sylow 2-groups of G and the group $N_G(H)$ contains a conjugate subgroup W of Z such that $W \cap H = e$. Here Z is a fixed subgroup of the center of some Sylow 2-group. The first part of the discussion is to determine the structure of $N_G(H)$. Throughout this part the letter H is reserved for one of the subgroups satisfying the above conditions, on which we focus our attention. Let N denote the group $N_G(H)$.

LEMMA 1. *Let P be a Sylow 2-group of N and S a Sylow 2-group of G containing P. If Z_0 is the part of the center of P generated by involutions, then Z_0 is contained in the center of S.*

Proof. By definition Z_0 is a part of $C_G(H)$ which is a normal subgroup of N. Since H is a maximal intersection, H is the maximal normal 2-subgroup of N. Hence $Z_0 \subseteq C_G(H) \cdot H \subseteq H$. If τ is an involution of Z_0, $C_G(\tau)$ is a Sylow 2-group of G by Theorem II. 5. Since H is a maximal intersection, $C_G(\tau)$ must be equal to S. Hence Z_0 is in the center of S.

LEMMA 2. *If τ is an involution of the center of H, then τ is contained in the center of some Sylow 2-group of N and this Sylow group is uniquely determined.*

Proof. By assumption $S = C_G(\tau)$ contains H. By Theorem II.5 S is a Sylow 2-group of G. Hence there is a subgroup Q of S which contains H as a proper normal subgroup. Then Q is in N. There is a Sylow 2-group P of N containing Q and a Sylow 2-group T of G containing P. Then $T \cap S$ contains Q. Since H is a maximal intersection of Sylow groups we must have $T = S$. Then $P = T \cap N = S \cap N$ contains τ in the center.

2. **The structure of G when the center of a Sylow 2-group is cyclic.** This section is devoted to the study of semi-simple (CIT)-groups in which the center of Sylow 2-groups is cyclic.

LEMMA 3. *If the center of a Sylow 2-group is cyclic, then N/H is a dihedral group of order 6.*

Proof. As before let P denote a Sylow 2-group of N and S be a Sylow 2-group of G containing P. By assumption the center of S is cyclic. It follows from Lemma 1 that the center of P is also a cyclic group.

By Theorem II.5 there is an involution τ of P not contained in H. Let P' be another Sylow 2-group of N. Take involutions π and π' in the center of P and P' respectively. Since $P \cap P' = H$, both π and π' belong to the center of H. Consider the conjugate element $\pi'' = \tau^{-1} \pi' \tau$ of π'. This is another element of the center of H. Hence π' and π'' commute. The product $\pi' \pi''$ of π' and π'' is an involution and commutes with τ. Since we took τ outside of H, τ is not an element of P' and does not commute with π'. Hence $\pi' \pi'' \neq 1$ and it is an element of the center of P (see Lemma 2). Hence $\pi = \pi' \pi''$ and τ leaves the subgroup $U = \{\pi, \pi'\}$ generated by π and π' invariant. Similarly if τ' is an involution of P' not contained in H, τ' leaves U invariant. The

group U is an abelian group of order 4 and clearly in the center of H. On the other hand

$$C_G(U) = C_G(\pi) \cap C_G(\pi') = H.$$

Since $N_G(U)$ contains τ and τ' we conclude that the group $N_G(U)/H$ is a group of order 6 isomorphic to the symmetric group of three letters. In the preceding argument the choices of P, P', τ or τ' are arbitrary. Hence any pair of involutions in N/H generates a group of order 6, provided that those involutions are not in the same Sylow 2-groups. If however τ and τ_1 are two involutions in P, then both τ and τ_1 transform π' into $\pi\pi'$. Hence $\tau\tau_1$ commutes with π'. This means $\tau\tau_1 \in H$. Hence the group P/H contains only one involution. By Proposition II.1, N/H contains an abelian normal subgroup A/H and $N = PA$. Since N/H is a (CIT)-group every element of A/H is a product of involutions. Hence the order of any element of A/H is 3. Since the group N is solvable, the group A/H must be cyclic. Hence A/H is a cyclic group of order 3 and at the same time N/H is a group of order 6 which is a dihedral group.

PROPOSITION 1. *Let G be a semi-simple* (CIT)-*group. Assume that the center of a Sylow 2-group is cyclic. Then this center is actually a group of order 2. If D is any maximal intersection of Sylow 2-groups, then the group $N_G(D)/D$ is a dihedral group of order 6 and the center of D is of rank 2.*

Proof. Apply Proposition II.3 taking Z to be the center of a Sylow 2-group. Then there is a maximal intersection H of Sylow 2-groups such that $N_G(H)$ contains a conjugate subgroup W of Z and $W \cap H = e$. Then WH/H is a part of a Sylow group of $N_G(H)/H$. By Lemma 3 $N_G(H)/H$ is a group of order 6. This proves the first assertion. The second part can be proved in a similar way as before.

LEMMA 4. *Let A be a direct product of two cyclic 2-groups of the same order. If A admits an automorphism θ of order 2 which leaves exactly two elements fixed, then the order of A is 4.*

Proof. We shall use additive notations. Let $A = \{u\} + \{v\}$ with $nu = nv = 0$ and $n = 2^m$. We may assume that $u_0 = ku$ $(k = 2^{m-1})$ is the only fixed element besides the identity by θ. Write down θ explicitly by

$$\theta(u) = au + bv \quad \text{and} \quad \theta(v) = cu + dv.$$

Since ku is fixed, we get

$$a \equiv 1 \quad \text{and} \quad b \equiv 0 \pmod 2.$$

Since kv is not invariant but is mapped to $k(u+v)$, we get

$$c \equiv d \equiv 1 \pmod 2.$$

We have

$$\theta(xu + yv) = (ax + cy)u + (bx + dy)v.$$

Hence θ leaves $xu+yv$ invariant if and only if we have

$$ax + cy \equiv x, \qquad bx + dy \equiv y \pmod{n}.$$

Hence if $b \equiv 0 \pmod{4}$, then the element $2^{m-2}u$ or $2^{m-2}u+2^{m-1}v$ would be invariant by θ according as $a \equiv 1 \pmod{4}$ or $a \equiv 3 \pmod{4}$. Suppose the order of A is greater than 4. Then $m \geq 2$ and the assumption $b \equiv 0 \pmod{4}$ produces an invariant element besides ku. On the other hand if b is not divisible by 4, the order of θ can not be 2. If so, we would have $a^2+bc \equiv 1 \pmod{n}$. Since $a^2 \equiv 1 \pmod{4}$ we would get $bc \equiv 0 \pmod{4}$, a contradiction. Hence the order of A must be 4.

LEMMA 5. *Under the same assumptions as in Proposition* 1, *a Sylow 2-group* S *contains an involution* π *such that the order of* $C_S(\pi)$ *is* 4.

Proof. Consider maximal intersections of Sylow 2-groups contained in S. Assume that none of those maximal intersections is a maximal subgroup of S. Let H be one of the maximal intersections in S which has the maximal possible order. Let V denote the center of H. By Proposition 1 the group $N_G(H)/H$ is a dihedral group of order 6. By assumption the group $P = S \cap N_G(H)$ is a proper subgroup of S. Hence there is a subgroup T of S containing P as a proper normal subgroup of index 2. Since T is not a part of $N_G(H)$, T contains an element σ which transforms H onto a subgroup H' of P where $H' \neq H$. Let V' be the center of H'. Again by Proposition 1 V is an abelian group of rank 2. $V \cap V'$ is contained in the center of P. By Lemma 1, $V \cap V'$ is cyclic. Hence there is an involution π of V which is not contained in $V \cap V'$. We may assume that $V = U \times W$ where $U \supseteq V \cap V'$ and $W \ni \pi$. Suppose that two elements π and $\sigma^{-1}\pi\sigma$ commute. Then $\rho = \pi\sigma^{-1}\pi\sigma$ is an involution of P which is not contained in $V \cap V'$. From the choice of σ, $\sigma^{-2}\pi\sigma^2$ is an involution of V. Hence $\sigma^{-1}\rho\sigma$ is either ρ itself or ρ times the involution τ of $V \cap V'$. Hence σ leaves the subgroup X generated by ρ and τ invariant. If α is any element of P, α leaves both H and H' invariant. Hence α leaves the groups $\{\tau, \pi\}$ and $\{\tau, \sigma^{-1}\pi\sigma\}$ invariant. This means $\alpha^{-1}\pi\alpha = \pi$ or $\pi\tau$, and

$$\alpha^{-1}(\sigma^{-1}\pi\sigma)\alpha = \sigma^{-1}\pi\sigma \quad \text{or} \quad \sigma^{-1}\pi\sigma\tau.$$

Hence $\alpha^{-1}\rho\alpha = \rho$ or $\rho\tau$. Since τ is in the center of S we conclude that $\alpha^{-1}X\alpha = X$. Therefore $N_G(X) \supseteq \{P, \sigma\} = T$. Since X is a noncyclic abelian group of order 4, $N_G(X)$ contains a normal 2-group Y of larger order than H. Y is contained in a maximal intersection. This contradicts the definition of H. Hence π does not commute with $\sigma^{-1}\pi\sigma$. Hence π is not contained in H'. This implies that $H' \cap W = e$ and $W \cong P/H'$. The group W is a group of order 2. At the same time we see that $\{\pi\}$ is a maximal cyclic group of V. Since $N_G(H)/H$ is a dihedral group of order 6, there is an automorphism of H of order 3 which

leaves only the identity invariant. Hence $\{\tau\}$ is also a maximal cyclic group of V. This implies that V is a group of order 4. By a theorem of Neumann [10], the central quotient group H/V is abelian. Since $H' \cap W = e$, we get $H' \cap V = U$. Hence we get

$$H/U = (V/U) \times (H \cap H')/U \quad \text{and} \quad H \cap H'/U \cong H/V.$$

Thus we conclude that the group H/U is abelian. Hence the commutator subgroup of H is contained in U. Since H admits an automorphism which maps U onto W, the commutator subgroup of H must be in $U \cap W = e$. The group H itself is therefore abelian. Hence H coincides with the center V which is as shown above a group of order 4. Clearly H is the centralizer of π in S and this proves our assertion.

Suppose that there is a maximal intersection D which is a maximal subgroup of S. By Proposition 1 $N_G(D)/D$ is again of order 6. Let V be the center of D. Since D admits an automorphism of order 3 which leaves only the identity fixed, by a theorem of Neumann the group D/V is abelian. Moreover we see that V is a direct product of two cyclic 2-groups of the same order. By Theorem II.5, S contains an involution π which is not contained in D. The element π induces an automorphism of V which leaves exactly two elements, since the center of S is of order 2. By Lemma 4 the order of V is 4. The group $T = C_G(\pi)$ is a Sylow 2-group of G by assumption, and $H = S \cap T$ is the centralizer of π in S. If H is a maximal subgroup of S we can apply the similar argument as before, and conclude that the order of H is 4. Suppose that H is not a maximal subgroup of S. Let τ denote the central involution of S. V contains another involution ρ. Since ρ leaves the group $K = \{\tau, \pi\}$ invariant, ρ leaves $H = C_G(K)$ invariant. Let P be the group generated by H and ρ. Since $H \not\ni \rho$, we get $H \cap V = U = \{\tau\}$. Since D is a maximal subgroup, $D \cap H$ is maximal in H. Hence we get

$$(D \cap H) \cap V = U \quad \text{and} \quad V \cup (D \cap H) = P \cap D.$$

Hence we get $H \cap D/U \cong P \cap D/V$. The last group is abelian since it is a subgroup of D/V. Since D does not contain π, we get

$$H = (H \cap D) \cup W$$

where $W = \{\pi\}$. Hence we get

$$H/U = (H \cap D)/U \times UW/U.$$

The group $H \cap D/U$ is abelian as shown before. Therefore H/U must be abelian. There is an automorphism of H which maps U onto W. It follows that H itself is abelian. Then the group $P \cap D$ is also abelian since it is a direct product of $\{\rho\}$ and $H \cap D$. Therefore $H \cap D$ is contained in the center of P. A similar consideration on T (instead of S) shows that H contains a maximal subgroup Y which is the center of a subgroup of T covering H. The inter-

section $D \cap H \cap Y$ consists of elements which commute with some element of order 3. Hence we have $D \cap H \cap Y = e$, which means the order of H is 4.

PROPOSITION 2. *Let G be a semi-simple* (CIT)-*group. Assume that the center of a Sylow 2-group is cyclic. Then the structure of Sylow 2-groups is as follows. A Sylow group S is generated by two elements σ and π satisfying conditions*

$$\sigma^{2^n} = \pi^2 = 1 \quad and \quad \pi^{-1}\sigma\pi = \sigma^{-1} \quad or \quad \sigma^{-1+2^{n-1}}$$

This is a direct consequence of Lemma 5 and Lemma 4 of [11]. One of the above types is a dihedral group. The other one contains a dihedral group as a maximal subgroup. This dihedral group is generated by all the involutions. Another noncyclic maximal subgroup is a generalized quaternion group.

THEOREM 1. *Let G be a semi-simple* (CIT)-*group. If a Sylow 2-group is a dihedral group, then G is one of the linear fractional groups* LF(2, q).

Proof. By Theorem II.5 involutions of G form a single conjugate class. Hence G does not contain a normal subgroup of index 2. If X is a cyclic subgroup of even order of G the order of X is a power of 2. If Y is another cyclic subgroup of G and if $X \cap Y \neq e$, then $X \cap Y$ contains an involution τ. Hence both X and Y are contained in the centralizer of τ which is by the condition (CIT) a Sylow 2-group. Therefore $X \cup Y$ is contained in a cyclic group. We can apply a theorem of Brauer, Suzuki and Wall [2]. It follows that G is isomorphic with LF(2, q) for some prime power q.

More precisely we have

THEOREM 2. *Only the following values of q are possible in Theorem 1.*

$$q = p = 2^n + 1, \quad a \; Fermat \; prime,$$
$$q = p = 2^n - 1, \quad a \; Mersenne \; prime,$$
$$q = 9 \quad or \quad q = 4.$$

Proof. If q is even, Sylow 2-groups of LF(2, q) are elementary abelian groups of order q. They are of dihedral type only if $q = 4$. Assume that q is odd. Then it is known (cf. Burnside [4, Chapter 20]) that the centralizer of an involution is a dihedral group of order $q+1$ or $q-1$ according as $q \equiv -1$ or $+1$ (mod 4). Hence by assumption $q \pm 1$ is a power of 2.

Let $q = p^m$ and $q+1 = 2^n$. Then $n \geq 2$. If m is even,

$$q + 1 = p^m + 1 \equiv 2 \pmod 4.$$

This is impossible. If $m = 2k+1$, then

$$q + 1 = (p + 1)l \quad where \quad l = p^{2k} - p^{2k-1} + \cdots + 1.$$

Hence $l \equiv 2k+1 \equiv 1 \pmod 2$. On the other hand l is a power of 2. Hence $l = 1$ and $q = p = 2^n - 1$ is a Mersenne prime.

Let $q - 1 = 2^n$. If m is odd, the same method as above shows that $q = p$ is a Fermat prime. If m is even, then $q = r^2$ and

$$q - 1 = (r + 1)(r - 1) = 2^n.$$

Since the greatest common divisor of $r + 1$ and $r - 1$ is 2, we must have $r - 1 = 2$ and $q = 9$.

THEOREM 3. *Let G be a semi-simple* (CIT)*-group. Assume that a Sylow 2-group is not a dihedral group but the center is cyclic. Then G is the group M_9, in the notation of Zassenhaus* [18], *of order* 720, *which is the projective group of one variable over the near-field of* 9 *elements.*

Proof. By assumptions the structure of a Sylow group S is the second one given in Proposition 2. Since the center of S contains only one involution, the normalizer of S in G coincides with S. From the defining relations it follows that the commutator subgroup T of S is a cyclic group. Consider the inter-section $D = S \cap \sigma^{-1} T \sigma$ for $\sigma \in G$. If D is not contained in T, then the order of D is either 4 or 2. If the order is 4, D and T contain the central involution in common. Hence σ commutes with the central involution of S. Then D would be a subgroup of T. Hence for all $\sigma \in G$, $D = S \cap \sigma^{-1} T \sigma$ is either a group of order 2 or a part of T. Hence the maximal dihedral subgroup P of S contains all those intersections and actually is generated by them. By a theorem of Grün [9], G contains a normal subgroup H of index 2 such that $H \cap S = P$.

The group H is a semi-simple (CIT)-group with dihedral Sylow 2-groups. Hence by Theorem 1 H is one of linear fractional groups. Let Q be a Sylow 3-group of H. Then $[N_G(Q) : N_H(Q)] = 2$. If Q is cyclic, Q contains a characteristic subgroup Q_0 of order 3. Then $C_G(Q_0)$ is a group of odd order by assumption and

$$[N_G(Q_0) : C_G(Q_0)] = 2.$$

Since $N_G(Q_0) \supseteq N_G(Q)$, $N_H(Q)$ would be a group of odd order. This is not the case since H is one of linear groups. Hence Q is not cyclic. By Theorem 2 and the subgroup theorem of Gierster (cf. [4]), H is isomorphic with LF(2, 9). G is then isomorphically represented by a permutation group on Sylow 3-groups. The degree is 10 and this permutation group is at least doubly transitive. Since the subgroup leaving one object fixed is a Frobenius group of order 72, it is triply transitive. A theorem of Zassenhaus [18] may be applied to conclude that G is isomorphic with M_9.

3. The structure of a Sylow 2-group whose center is not cyclic. In this section we shall assume that G is a semi-simple (CIT)-group, S is a Sylow 2-group of G, the center Z of S is not cyclic and Sylow 2-groups are not independent. The purpose is to determine the structure of S. Again Theorem II.5 and Proposition II.3 are prominent.

PROPOSITION 3. *Under the above assumptions the center Z is elementary abelian. There exists a maximal intersection H of Sylow 2-groups such that $N_G(H)$ contains a subgroup W which is conjugate to Z and $W \cap H = e$, and $N_G(H)/H$ is isomorphic with* $\mathrm{LF}(2, q)$ *for some* q.

Proof. Apply Proposition II.3 taking Z to be the center. There exists a maximal intersection H of Sylow 2-groups such that $N = N_G(H)$ contains a conjugate subgroup W of Z and $W \cap H = e$. Since H is a maximal intersection, Sylow 2-groups of N/H are independent. By assumption a Sylow group of N/H contains a subgroup isomorphic with Z. Since Z is assumed to be non-cyclic, Sylow groups of N/H are neither cyclic nor generalized quaternion groups. By Theorem II.3 the group N/H is a (ZT)-group.

Let H_0 be the subgroup of the center of H generated by involutions. If $\tau \in H_0$, τ is contained in the center of a Sylow 2-group of N by Lemma 2. If P is a Sylow 2-group of N, we denote by $I(P)$ the set of involutions in the center of P. Then $I(P)$ is a subset of H_0 and every involution of H_0 is contained in some $I(P)$. If P' is another Sylow 2-group of N, $I(P')$ has no element in common with $I(P)$. Let $I(P)$ contain $q - 1$ involutions. If N/H contains exactly $n + 1$ Sylow 2-groups, n being the order of Sylow groups of N/H, then H_0 contains exactly $(q - 1)(n + 1)$ involutions. The order m of H_0 is then

$$(q - 1)(n + 1) + 1 = qn - n + q = m.$$

All the numbers q, n and m are powers of 2 (cf. Feit's theorem in [5]). Since $I(P)$ is contained in the center of a Sylow 2-group by Lemma 1 and since P contains a subgroup W which is conjugate to the center Z, q is a divisor of n. Suppose $q < n$. Clearly we have $m \geq q^2$. Hence $m \equiv 0 \pmod{2q}$. But

$$m = qn - n + q \equiv q \pmod{2q}.$$

This contradiction proves that $q = n$. This implies many things. First of all the order of W is q, since it is a multiple of q and is a divisor of n. Secondly the group W contains at least $q - 1$ involutions and so W is an elementary abelian group of order q. Finally W is isomorphic with a Sylow 2-group of N/H, since

$$P/H \cong WH/H \cong W.$$

N/H is a (ZT)-group with abelian Sylow 2-groups so that by a theorem of Zassenhaus it is isomorphic with $\mathrm{LF}(2, q)$. Thus Proposition 3 has been proved completely.

PROPOSITION 4. *Let W be the subgroup of $N = N_G(H)$ in Proposition 3. N contains a cyclic group U of order $q - 1$ such that $C_G(W)U$ is the normalizer of $C_G(W)$.*

Proof. The subgroup W is conjugate to Z so that $C_G(W) = S$ is a Sylow 2-group of G. By Theorem II.5 any two involutions of W are conjugate in G.

If τ_1 and τ_2 are involutions of W, there exists an element σ of G such that $\tau_2 = \sigma^{-1}\tau_1\sigma$. Then $C_G(\tau_2) = \sigma^{-1}C_G(\tau_1)\sigma$. Since $C_G(\tau_1) = C_G(\tau_2) = S$, the element σ is in the normalizer $N_G(S)$ of S. By Proposition 3 the group N/H is isomorphic with LF$(2, q)$. Hence there is an element ρ of order $q-1$ which transforms the Sylow 2-group P of N containing W into itself. If $\tau \in W$ is an involution, ρ transforms the group $\{\tau, H\}$ into another subgroup which is generated by H and an involution π of W. There is an element σ of N which transforms τ into π. The element $\sigma^{-1}\rho$ leaves the subgroup $\{\tau, H\}$ invariant. Hence $\sigma^{-1}\rho \in P$. This implies that σ is an element of $\{P, \rho\}$ and has an order $q-1$. The subgroup U generated by σ satisfies the conditions of Proposition 4.

LEMMA 6. *In the notation of Proposition 4 the extension of N over H splits.*

Proof. Let σ be a generator of the subgroup U in Proposition 4. Since $N/H \cong$ LF$(2, q)$, there is a dihedral group of order $2(q-1)$ of N/H containing HU/H. If this dihedral group is D/H, D is a solvable subgroup of N with H as a maximal normal 2-group. By Theorem II.2 the extension of D over H splits. Hence N contains an involution τ such that $\tau^{-1}\sigma\tau = \sigma^{-1}$. Again since N/H is LF$(2, q)$, there is an involution π in W such that the coset $\pi\tau H$ is of order 3 in N/H. This implies that the order of $\pi\tau$ is actually 3. We want to show that the group L generated by W, σ and τ is isomorphic with LF$(2, q)$. If this has been done, L is a complement of H in N.

Since $(\pi\tau)^3 = 1$ we have $\tau\pi\tau = \pi\tau\pi$. If π' is any element of W, $\pi' = \rho^{-1}\pi\rho$ for some power ρ of σ. Hence we have

$$\tau\pi'\tau = \tau\rho^{-1}\pi\rho\tau = \rho\tau\pi\tau\rho^{-1} = \rho\pi\rho^{-1} \cdot \rho^2\tau\rho\pi\rho^{-1}.$$

This means that every element of L can be written as either $\pi'\rho$ or $\pi'\rho\tau\pi''$ with π', $\pi'' \in W$ and $\rho \in U$. This expression is unique because $\tau W\tau \cap \{W, U\} = e$. Hence the order of L is $q(q^2-1)$. Since L is a (CIT)-group with abelian Sylow 2-groups, L must be isomorphic with LF$(2, q)$ (cf. [13] or [6]).

LEMMA 7. *The group N/H in the notation of Proposition 4 is isomorphic with* LF$(2, 4)$.

Proof. Let L be a complement of H in N. Lemma 6 shows that there exists such a complement. Let H_0 be the subgroup of the center of H generated by involutions. In the proof of Proposition 3 we have shown that the order of H_0 is q^2. Let P be the Sylow 2-group of N containing W. Then using the same notation as in Lemma 6 the group $\tau^{-1}P\tau$ is another Sylow 2-group of N. Since $\tau^{-1}U\tau = U$, U is contained in the normalizer of $\tau^{-1}P\tau$. Let X be the part of center of P generated by involutions and Y the same of $\tau^{-1}P\tau$. Since $\tau^{-1}P\tau \neq P$, we have $X \cap Y = e$ and $H_0 = X \times Y$ as is seen from the proof of Proposition 3. We remark that both X and Y are invariant by σ. Let α be an involution of X. Since the order of X is q every involution of X is conjugate to α by

some element of U. Moreover every involution of H_0 is in the center of some Sylow 2-group of N. Hence H_0 is a minimum normal subgroup of H_0L.

We shall obtain the explicit forms of automorphisms of H_0 induced by elements σ, τ, and π (the notations being the same as in the proof of Lemma 6). The groups XU and YU are the Frobenius groups of order $q(q-1)$. Here X and Y are considered as the additive group of the field F of q elements, and the element σ induces a scalar multiplication (cf. Zassenhaus [18]) by a generator of its multiplicative group. The element τ exchanges X and Y. The element π is in W. Hence π commutes with every element of X. Let η be any involution of Y. Then $\xi = \eta\pi^{-1}\eta\pi$ is an element of H_0, which commutes with π. Hence ξ is an involution of X. Thus we have

$$\pi^{-1}\eta\pi = \xi\eta \qquad\qquad \text{with } \xi \in X.$$

Since $Y = \tau^{-1}X\tau$ we may write $\eta = \tau^{-1}\lambda\tau$ for $\lambda \in X$. In this case we have $\xi = \lambda$: that is

$$\pi^{-1}(\tau^{-1}\lambda\tau)\pi = \lambda\tau^{-1}\lambda\tau.$$

To show this equation we use the equation $(\tau\pi)^3 = 1$ or $\tau\pi\tau = \pi\tau\pi$. We have

$$\tau^{-1}(\xi\eta)\tau = \tau^{-1}\xi\tau\lambda = \tau^{-1}\pi^{-1}\eta\pi\tau = \pi\tau\pi\lambda\pi\tau\pi = \xi\eta.$$

Since $H_0 = X \times Y$ we get $\lambda = \xi$.

Let Δ be the totality of endomorphisms of H_0 which commute with automorphisms induced by L. Since H_0 is a minimum normal subgroup of $K = H_0L$, the set Δ is a (skew) field by Schur's lemma. Since X is the totality of elements of H_0 left invariant by π, Δ must leave X invariant. Since τ exchanges X and Y, Y is also left invariant by Δ. On X every element of Δ commutes with ρ which induces a scalar multiplication. Hence elements of Δ are also scalar multiplications by elements of F on X. The same is true on Y. Since τ exchanges X and Y, the multipliers in X and Y must coincide. If $0 \neq \alpha \in F$, the scalar multiplication in X is defined by

$$\xi^\alpha = \alpha^{-1}\xi\alpha,$$

where α in the right side is considered as an element of U. The scalar multiplication in Y is however defined by

$$\eta^\alpha = \tau\xi^\alpha\tau \qquad\qquad \text{if } \eta = \tau\xi\tau.$$

Let θ be the mapping on H_0 defined by

$$\theta(\xi\eta) = \xi^\alpha\eta^\alpha \qquad\qquad \text{for } \xi \in X, \eta \in Y.$$

We shall show that $\theta \in \Delta$ and hence Δ is isomorphic with F. We have

$$\theta(\sigma^{-1}(\xi\eta)\sigma) = \theta(\sigma^{-1}\xi\sigma\sigma^{-1}\eta\sigma) = (\sigma^{-1}\xi\sigma)^\alpha(\sigma^{-1}\eta\sigma)^\alpha.$$

From the definition

$$(\sigma^{-1}\xi\sigma)^\alpha = \alpha^{-1}\sigma^{-1}\xi\sigma\alpha = \sigma^{-1}\alpha^{-1}\xi\alpha\sigma = \sigma^{-1}\xi^\alpha\sigma.$$

Suppose $\eta = \tau\zeta\tau$ ($\zeta \in X$). Then

$$\sigma^{-1}\eta\sigma = \sigma^{-1}\tau\zeta\tau\sigma = \tau\sigma\zeta\sigma^{-1}\tau.$$

Hence by definition

$$(\sigma^{-1}\eta\sigma)^\alpha = \tau(\sigma\zeta\sigma^{-1})^\alpha\tau = \tau\sigma\zeta^\alpha\sigma^{-1}\tau = \sigma^{-1}\tau\zeta^\alpha\tau\sigma = \sigma^{-1}\eta^\alpha\sigma.$$

Hence θ commutes with the automorphism induced by σ. From the definition it follows that θ commutes with the automorphism induced by τ. As for π we have

$$\theta(\pi(\xi\tau\zeta\tau)\pi) = \theta(\xi\zeta\tau\zeta\tau) = \xi^\alpha\zeta^\alpha\tau\zeta^\alpha\tau$$

$$= \pi(\xi^\alpha\tau\zeta^\alpha\tau)\pi = \pi\theta(\xi\tau\zeta\tau)\pi.$$

Thus we have shown that $\theta \in \Delta$. Since $\Delta \cong F$, the group K is isomorphic with a group of matrices over F. The correspondence is given by

$$\sigma \rightarrow \begin{pmatrix} \lambda & & \\ & \lambda^{-1} & \\ & & 1 \end{pmatrix}, \qquad \tau \rightarrow \begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix}, \qquad \pi \rightarrow \begin{pmatrix} 1 & & \\ 1 & 1 & \\ & & 1 \end{pmatrix}.$$

and the group H_0 corresponds to the totality of matrices

$$\begin{pmatrix} 1 & & \\ & 1 & \\ \xi & \eta & 1 \end{pmatrix}.$$

The subgroup W is the totality of conjugate elements of π by elements of U. We see that the subgroups $\{W, U\}$ and $\{X, U\}$ are isomorphic under the following isomorphism ϕ:

$$\phi: \begin{pmatrix} \lambda & & \\ \lambda^{-1}\mu & \lambda^{-1} & \\ & & 1 \end{pmatrix} \rightarrow \begin{pmatrix} \lambda^2 & & \\ & \lambda^{-2} & \\ \mu & & 1 \end{pmatrix}.$$

The group W is the center of some Sylow 2-group of G. Hence there is an element β of G which transforms X onto W. The element β transforms U into a group $\beta^{-1}U\beta$ which is a subgroup of $N_G(W)$. Since U and $\beta^{-1}U\beta$ are two subgroups of order $q-1$ in $N_G(W)$, they are conjugate in $N_G(W)$. We may therefore assume that $\beta^{-1}U\beta$ coincides with U:

$$\beta^{-1}U\beta = U, \quad \text{or} \quad \beta^{-1}\sigma\beta = \sigma^k.$$

Moreover we may assume that β maps the element τ_1 onto π, where

$$\tau_1 = \begin{pmatrix} 1 & & \\ & 1 & \\ 1 & & 1 \end{pmatrix}.$$

The group $N_G(U)$ is a group of even order since it contains the involution τ. Since G is a (CIT)-group, the group $C_G(U)$ is of odd order. Hence the group $N_G(U)/C_G(U)$ is a group of even order and is abelian, since U is a cyclic group. From the condition (CIT) it follows that the order of $N_G(U)/C_G(U)$ and in particular the order of β is a power of 2. Again by (CIT) the involution which is a power of β maps every element of U into its inverse. If β^z is the involution we have

$$\beta^{-z}\sigma\beta^z = \sigma^{kz} = \sigma^{-1}.$$

On the other hand β induces an isomorphism ψ of $\{X, \sigma\}$ onto $\{W, \sigma\}$. The mapping $\phi \circ \psi$ is an isomorphism of $\{X, \sigma\}$ which maps τ_1 into itself and sends σ into σ^{2k}. From the property of $\{X, \sigma\}$ it follows that $2k$ is a power of 2. (The mapping $\sigma \to \sigma^{2k}$ is an automorphism of $GF(q)$.) Hence $k = 2^\nu$. If $q = 2^\mu$, we have a congruence

$$2^{\nu z} \equiv -1 \pmod{2^\mu - 1}.$$

Let us choose two integers x and y in such a way that

$$\nu z = x\mu + y \quad \text{and} \quad 0 \leq y < \mu,$$

Then we have

$$2^{\nu z} \equiv 2^{x\mu+y} \equiv 2^\nu \equiv -1 \pmod{2^\mu - 1}.$$

Hence we have

$$2^\mu + 1 > 2^\nu + 1 \geq 2^\mu - 1.$$

This implies either $2^\nu + 1 = 2^\mu$ or $2^\nu + 1 = 2^\mu - 1$. The first case happens only when $y = 0$ and $\mu = 1$, while the second case is possible only when $y = 1$ and $\mu = 2$. Since we have assumed that the center of Sylow 2-groups is not cyclic, $q = 2^\mu$ must be more than 2. We have therefore $\mu = 2$ and $q = 4$.

PROPOSITION 5. *Under the assumptions of Proposition 3, Sylow 2-groups of G are isomorphic with the group of matrices*

$$\begin{pmatrix} 1 & & \\ \alpha & 1 & \\ \beta & \gamma & 1 \end{pmatrix} \qquad \alpha, \beta, \gamma \in GF(4).$$

Proof. In the proof of Lemma 7 we have shown that the group $K = H_0L$ is isomorphic with a group of matrices over GF(4). The structure of Sylow 2-groups of K is the one given above.

Consider the group N of Proposition 3. If P is one of the Sylow 2-groups of N, P admits an automorphism of order 3 which leaves only the identity invariant. Hence by a theorem of Neumann [10] the quotient group of P by its center is abelian. If Z is the center of P, Z is contained in H and the group H/Z is abelian since it is a subgroup of P/Z. If Z' is the center of another Sylow 2-group P', H/Z' is also abelian. Since $Z \cap Z' = e$ we conclude that H is abelian. Let S be a Sylow 2-group of G containing P. Then S admits an automorphism of order 3 which leaves only the identity element invariant. By a theorem of Neumann [10] the central quotient group of S is abelian. On the other hand the center of S is contained in H. Hence S is contained in the normalizer of H. This means that P is identical with S.

Set $T = C_G(W)$, the notation W being the same as in Proposition 4. Then the group T is a Sylow 2-group of G containing Z, the center of S. Let D denote the intersection $S \cap T$. Since $D \supseteq Z$, D is a normal subgroup of S. At the same time it is a normal subgroup of T, since the center of T is W. Consider the subgroup Y defined in Lemma 7: i.e. the subgroup of the center of Sylow 2-group P' of N generated by involutions. Then we have $Y \cap D = e$ as is seen from the proof of Lemma 7. Hence the group D is in the family $\mathfrak{H}_1$ of Part II. Since Sylow 2-groups of $N_G(D)/D$ are abelian, D is a maximal intersection of Sylow groups because $N_G(D)/D$ is a (CIT)-group. We can apply the consideration of this section to D instead of H. In particular Proposition 3 and Lemma 7 applied to D show that the group $N_G(D)/D$ is isomorphic with LF(2, 4). Hence the index $[S:D]$ is 4. Since $D \cap Y = e$ we conclude that

$$H = (H \cap D) \cup Y, \quad \text{or} \quad H = (H \cap D) \times Y.$$

This means that Y is a direct factor of H. Since there is an automorphism of H which exchanges Y and X, X is another direct factor of H. It is easily seen that $H_0 = X \cup Y$ is a direct factor of H. The definition of H_0 is however the subgroup of the center of H generated by involutions. Since H is abelian, H_0 contains all the involutions of H. No direct factor except the group itself can contain all the involutions. Hence we get $H_0 = H$. The group N coincides with K and the assertion has been proved.

4. Distribution of real elements.

LEMMA 8. *If a product $\sigma = \tau\tau'$ of two involutions τ and τ' has an odd order > 1, the centralizer $C_G(\sigma)$ is an abelian group and every element of $C_G(\sigma)$ is a product of two involutions. Moreover $C_G(\sigma)$ is the centralizer of any nonidentity element in it.*

Proof. Let A denote the centralizer $C_G(\sigma)$. Since τ transforms σ into its

inverse, τ transforms A into itself. By assumption G is a (CIT)-group and hence every element of A has an odd order. Therefore τ commutes with no element of A except the identity. By a result of Burnside τ transforms every element of A into its inverse. This implies that A is abelian and that every element of A is a product of two involutions. If $1 \neq \rho \in A$, ρ is a product of two involutions. Hence as shown before $C_G(\rho)$ is abelian. Clearly $C_G(\rho)$ contains A and hence $C_G(\rho)$ coincides with A.

LEMMA 9. *If an element $\sigma \neq 1$ of G is a product of two involutions, σ is contained in a unique maximal abelian Hall subgroup A of G and the index $[N_G(A):A]$ is a power of 2 not more than 8.*

Proof. The group $A = C_G(\sigma)$ is a maximal abelian group so that the uniqueness is trivial. By Lemma I.4 and by the last assertion of Lemma 8, A is a Hall subgroup of G. The group $B = N_G(A)/A$ induces automorphisms of A which are fixed-point-free. Hence Sylow groups of B are either cyclic or a generalized quaternion group. Since the index $[N_G(A):A]$ is even, B contains a central involution. By the condition (CIT) B must be a 2-group. From the structure of Sylow 2-groups given in Proposition 5, the order of B is at most 8.

We remark that the index $[N_G(A):A]$ divides the order of A minus 1. Let $A_1, \cdots, A_s$ be a system of maximal abelian subgroups of G containing products of two involutions. We may assume that any such maximal abelian subgroup of G is conjugate to one and only one of the A_i ($i=1, 2, \cdots, s$). Let n_i denote the order of A_i and l_i be the index $[N_G(A_i):A_i]$. Let m be defined by the equation:

$$m = \sum_i (n_i - 1)/l_i.$$

PROPOSITION 6. *The order g of G is equal to*

$$7872 + 4096m.$$

Proof. By Proposition 5, we know the structure of Sylow 2-groups of G. From the proof we see that each involution of G is contained in exactly 9 Sylow 2-groups. One of them is the centralizer of the involution. Let it be S. S contains two elementary abelian subgroups of order 16, which intersect in a group of order 4. Hence S contains 27 involutions. There are four more Sylow 2-groups containing each elementary abelian subgroup of order 16. Hence in these 9 Sylow 2-groups there are exactly $27 + 8 \cdot 12 = 123$ involutions.

Let τ be an involution of G. If τ' is another involution, the product $\tau\tau'$ has an odd order if τ' is not one of those 123 involutions. By Lemma 9, the products $\tau\tau'$ are distributed in conjugate subgroups of A_i. Suppose that $\tau\tau'$ is conjugate to another product $\tau\tau''$ of involutions. Then there is an element ρ of G such that $\rho^{-1}(\tau\tau')\rho = \tau\tau''$. Since τ transforms $\tau\tau'$ and $\tau\tau''$ into their inverses, $\rho^{-1}\tau\rho$ is conjugate to τ in the group $\{\tau, \tau''\}$. Hence we may assume

that ρ commutes with τ. This implies that there are exactly 64 products $\tau\tau''$ conjugate to the given $\tau\tau'$. Each maximal abelian subgroup A_i contributes $(n_i-1)/l_i$ classes. There are exactly m classes containing products of two involutions whose orders are odd. G contains $g/64$ involutions. Hence there are $g/64-123$ products $\tau\tau'$ of odd order. Each conjugate class contains exactly 64 such products. Hence we have

$$(g/64) - 123 = 64m.$$

The following lemma is used in order to reduce the number of cases which we have to analyze in the later part of proof (cf. §7).

LEMMA 10. *If for some i, $n_i-1=l_i$ or $2l_i$, then n_i is either 3, 5 or 9.*

Proof. By Lemma 9, l_i is a power of 2 not more than 8. Hence in the first case n_i is 3, 5 or 9, while in the second case n_i is 5, 9 or 17. The value 17 is eliminated because if $l_i=8$, the group $N_G(A_i)/A_i$ is a quaternion group which cannot act on cyclic groups without fixed points.

5. **Characters of $N_G(S)$.** Let S be a Sylow 2-group of G. We can determine the irreducible characters of $M=N_G(S)$ without difficulty. First of all we prove the following lemma.

LEMMA 11. *G has three classes containing elements of order 4.*

Proof. Consider an element π of order 4. The element π is contained in the Sylow 2-group $S=C_G(\pi^2)$. S contains three classes of elements of order 4 whose squares are π^2. If π' is another element of order 4, π' is conjugate to π'' such that $\pi''^2=\pi^2$. The element π'' is conjugate to π in G if and only if they are conjugate in S. Therefore G has three classes containing elements of order 4.

This lemma is true for all subgroups containing M. In particular M itself has three classes of elements of order 4.

LEMMA 12. *M has three linear characters, 5 characters of degree 3 and a character of degree 12.*

Proof. From the structure of S given in Proposition 5, we see that the center Z of S is the commutator subgroup of S. Hence S has 16 linear characters and 3 characters of degree 4. The 3 characters of degree 4 are conjugate in M, giving a character of degree 12 of M. Fifteen nonprincipal linear characters are distributed into 5 classes of conjugate characters, each class containing 3 conjugate characters. Thus M has 5 characters of degree 3.

The group S contains two elementary abelian subgroups H and H' of order 16. $H\cap H'$ is the center Z of S. There are three classes C_1, C_2 and C_3 of involutions in M. C_1 consists of central involutions of S, C_2 is the set of involutions in H not contained in Z and C_3 is the similar set of H'. Characters of degree 3 are given in the following table:

	$C_2,$	C_3	C
$\theta_1, \theta_2, \theta_3$	-1		$*$
θ_4	3	-1	-1
θ_5	-1	3	
θ_0		3	3

In the table the class C contains elements of order 4. All characters take the value 3 on C_1. The last character θ_0 is the sum of three linear characters of M.

6. **Decomposition of induced characters.** As usual θ^* means the character of G induced by a character θ. If ϕ is a character (irreducible or not), we denote by $w(\phi)$ the norm of ϕ, i.e., the average of the absolute value squared:

$$w(\phi) = (1/g) \sum_{\sigma \in G} |\phi(\sigma)|^2.$$

PROPOSITION 7. *W have* $\theta_4^* = \theta_5^*$ *and for* $i, j = 1, 2, 3$

$$w(\theta_i^* - \theta_j^*) = 2, \quad w(\theta_i^* - \theta_4^*) = 5, \quad w(\theta_0^* - \theta_4^*) = 7, \quad w(\theta_0^* - \theta_i^*) = 18.$$

This is proved by a straightforward computation of induced characters. The same result may be obtained if we consider the decomposition in the group N first and apply the method described in [14]. The first equation implies that the decomposition of θ_i^* ($i = 1, 2, 3$) takes the form

$$\theta_i^* = \epsilon \Theta_i + \Delta \qquad\qquad (\epsilon = \pm 1).$$

The characters Θ_1, Θ_2 and Θ_3 have the same degree and take the same value everywhere except on classes containing elements of order 4.

LEMMA 13. *If a character ϕ of G takes the constant value on classes of elements of order 4, then ϕ contains the characters Θ_i with the same multiplicity.*

Proof. The character $\Theta_i - \Theta_j$ ($i \neq j$; $i, j = 1, 2, 3$) vanishes everywhere except on classes of elements of order 4. If ϕ takes the value c on these classes, we have

$$\sum_{\sigma \in G} \phi(\sigma^{-1})(\Theta_i(\sigma) - \Theta_j(\sigma)) = \sum_{\sigma \in G} c(\Theta_i(\sigma) - \Theta_j(\sigma)) = 0.$$

The orthogonality relation yields the assertion.

As a special case of this lemma we conclude that θ_4^* contains the characters Θ_i with the same multiplicity. The decomposition of θ_4^* is of the following form:

$$\theta_4^* = a \sum \Theta_i + \sum a_\mu X_\mu, \qquad\qquad a, a_\mu \geq 0,$$

where the characters X_μ are not the principal character 1. We shall denote further

$$\theta_i^* - \theta_4^* = \epsilon\Theta_i + x\sum\Theta_k + \sum x_\mu X_\mu, \qquad\qquad (i = 1, 2, 3)$$
$$\theta_0^* - \theta_4^* = 1 + y\sum\Theta_k + \sum y_\mu X_\mu.$$

Then

$$\theta_0^* - \theta_i^* = 1 - \epsilon\Theta_i + (y - x)\sum\Theta_k + \sum (y_\mu - x_\mu)X_\mu.$$

It follows from Proposition 7 that

(1) $$(x + \epsilon)^2 + 2x^2 + \sum x_\mu^2 = 5,$$

(2) $$1 + 3y^2 + \sum y_\mu^2 = 7,$$

$$1 + 2(y - x)^2 + (y - x - \epsilon)^2 + \sum (y_\mu - x_\mu)^2 = 18.$$

Under the above two equations the last one is equivalent to

(3) $$3xy + \epsilon y + \sum x_\mu y_\mu = -3.$$

If θ_6 is the character of M with degree 12, we have

$$\theta_6^* = \theta_1^* + \theta_2^* + \theta_3^* + \theta_4^*.$$

Using the reciprocity law of Frobenius we can compute the values of each irreducible character on 2-singular classes in terms of the coefficients of decompositions. We shall state the result in the following table.

(4) Θ_k: $45x + y + 15\epsilon + 64a;$ $y - 3x - \epsilon;$ $x + y + \epsilon\theta_k,$
X_μ: $45x_\mu + y_\mu + 64a;$ $y_\mu - 3x_\mu;$ $x_\mu + y_\mu.$

In the above table the first number is the degree, the second is the value on the class of involutions and the last one is the value on classes containing elements of order 4. The orthogonality relations together with (1), (2) and (3) yield

(5) $$3ay + \sum a_\mu y_\mu = 2,$$

and

(6) $$a(3x + \epsilon) + \sum a_\mu x_\mu = -3.$$

   7. Exceptional characters. Consider a maximal abelian group $A = A_i$ of the fourth section. If $w_i = (n_i - 1)/l_i > 1$, then we can associate to A w_i irreducible characters of G as exceptional characters (cf. [1] or [12]). These exceptional characters satisfy various properties. First of all the exceptional characters have the same degree and take the same value on classes not containing elements of A. If a character is exceptional for one of A_i, then it is nonexceptional for the rest of the A_i. From the above property of exceptional

characters it follows that the characters Θ_j are not exceptional for any A_i.

We have so far assigned exceptional characters for those A_i which satisfy the relation $w_i > 1$. In this way $\sum w_i$ characters are associated, where the summation is over those indices i with $w_i > 1$. If there are indices for which $w_i = 1$, then there are still unassigned characters remaining. This is because each A_i contributes w_i conjugate classes and the number of irreducible characters is equal to the number of conjugate classes. Therefore we can assign an irreducible character to an abelian group A_i with $w_i = 1$ as an exceptional character in such a way that this character is nonexceptional for any other A_j and different from the principal character or Θ_k. Thus we have m exceptional characters. If $w_i > 1$ for all i, the set of exceptional characters is determined uniquely by the structure of G. On the other hand if $w_i = 1$ for some i, the set is not unique. In this case we shall fix a set and consider the characters in it as exceptional characters.

8. **Sketch of the proof.** The purpose here is to prove the following theorem.

THEOREM 4. *Let G be a semi-simple* (CIT)-*group. If Sylow 2-groups are not independent and have a noncyclic center, then G is isomorphic with the linear fractional group* LF(3, 4).

The first part of proof is to determine the order of G. It is known (cf. [1]) that if the order of the centralizer of involutions is given then the order of G is bounded. Hence the determination of the structure of G is certainly possible by a finite process. The following is a rough sketch of how to obtain the possible orders for G.

From the table (4) we see that if $x_\mu = y_\mu = 0$, the character X_μ vanishes on 2-singular classes and its degree is a multiple of 64. Thus the character X_μ is of defect 0 for 2. Conversely if a character X_μ is defect 0 for 2, we have $x_\mu = y_\mu = 0$. It follows from the equations (1) and (2) that the number of characters with positive defect for 2 is bounded. Rough estimate gives a bound 10 besides 1 and Θ_k. Among m exceptional characters we suppose that there are s characters of positive defect for 2. By a theorem on characters the order g of G is the sum of the square of degrees. We decompose the summation into three parts:

$$g = \sum_1 + \sum_2 + \sum_3$$

where $\sum_1$ is the summation over nonexceptional characters, $\sum_2$ is over exceptional characters with positive defect for 2 and $\sum_3$ ranges over exceptional characters of defect 0. In $\sum_3$ each term is at least $(64)^2$ and the number of summands is $m - s$. Using Proposition 6 we have

$$7872 + (64)^2 m \geqq \sum_1 + \sum_2 + (m - s)(64)^2,$$

or

$$7872 + (64)^2 s \geqq \sum_1 + \sum_2.$$

Since s is at most 10, the above inequality gives a bound for the degrees of characters of positive defect for 2. The equations (1), (2) and (3) are used in conjunction with the table (4) to reduce the possibility. The equations (5) and (6) can also be used. If the table (4) has been completed for characters of positive defect for 2, then we use the formula (cf. [1])

$$(64)^2(n(S) - 1) = g(\sum t^3/f)$$

where $n(S)$ is the number of involutions in S, t is the value on involutions, f is the degree and the summation ranges over all characters of positive defect for 2. This determines a possible order of G. It turns out that 20160 is the only possibility for the order.

We discuss a few cases in detail and leave the remaining cases to the readers. The equation (2) implies that $y^2 \leqq 1$, and (1) yields $x^2 \leqq 1$. Assume $y = x = 0$. Then the possibilities for x_μ, y_μ are as follows.

(A)
$$\begin{matrix} 2\epsilon_1, & \epsilon_2, & \epsilon_3, & 0, & 0 \\ -\epsilon_1, & -\epsilon_2, & 0, & \epsilon_4, & \epsilon_5 \end{matrix}$$

(B)
$$\begin{matrix} \epsilon_1, & \epsilon_2, & \epsilon_3, & \epsilon_4, & \epsilon_5, & \epsilon_6, & 0 \\ -\epsilon_1, & -\epsilon_2, & -\epsilon_3, & 0, & 0, & 0, & \epsilon_7. \end{matrix}$$

In the above table the first line gives the values for y_μ and the second line, for x_μ. The ϵ_i are either 1 or -1. Consider the first case (A). Degrees of characters X_μ are as follows (cf. (4)).

$$-43\epsilon_1, \quad -44\epsilon_2, \quad \epsilon_3, \quad 45\epsilon_4, \quad 45\epsilon_5 \pmod{64}.$$

The value of s is certainly at most 5. This bound can be reduced to 3. Exceptional characters for A_j have the same degree. Hence if X_i $(i \leqq 5)$ is exceptional for A_k, we have $w_k \leqq 2$, and $n_k = 3$, 5 or 9. If $w_k = 2$, then X_4 and X_5 are exceptional for A_k and $n_k = 5$ or 9. The degree of Θ is congruent to 15ϵ (mod 64). We have

$$20160 \geqq 1 + 3(\Theta)^2 + \sum_{i=1}^{5} (X_i)^2$$

where (X) is the degree of a character X. We have $(\Theta) \leqq 78$. From the congruence for (Θ) we conclude that $(\Theta) = 15$ or 49.

Assume that $(\Theta) = 49$. Then we have

$$\sum_{i=1}^{5} (X_i)^2 \leqq 12956.$$

The equations (5) and (6) are

$$2a_1\epsilon_1 + a_2\epsilon_2 + a_3\epsilon_3 = 2 \quad \text{and} \quad a_1\epsilon_1 + a_2\epsilon_2 - a_4\epsilon_4 - a_5\epsilon_5 = 2.$$

If $a_3 > 1$, $(X_3) \geqq 127$ and this is impossible. Hence $a_3 = 1$. The first equation shows that a_2 is odd. Therefore a_2 is also 1. Then ϵ_2 must be 1 and $(X_2) = 20$. We have two cases:

$$a_1 = 0, \quad \epsilon_1 = -1, \quad \epsilon_3 = 1, \qquad (X_1) = 43, \quad (X_3) = 65;$$

$$a_1 = 1, \quad \epsilon_1 = 1, \qquad \epsilon_3 = -1, \quad (X_1) = 21, \quad (X_3) = 63.$$

Accordingly we have $a_4\epsilon_4 + a_5\epsilon_5 = -1$ or 0. In the first case $(X_4) \neq (X_5)$ and $s \leqq 2$. Hence we must have $(X_4) = 45$ and $(X_5) = 19$. In the second case we must have $a_4 = a_5 = 0$ and $\epsilon_4 = \epsilon_5 = 1$. Hence $(X_4) = (X_5) = 45$. The values of these characters on involutions are as follows:

$$-5, \quad 4, \quad 1, \quad -3, \quad 3,$$
$$5, \quad 4, \quad -1, \quad -3, \quad -3.$$

The computed value of g is not an integer in either case. We have used the following result which is also useful in other cases.

LEMMA 14. *G has only one linear character.*

Proof. The proof depends on the structure of N in Lemma 7. Combined with Proposition 5 we see that the group N/H is a simple group of order 60 and N contains the normalizer of a Sylow group of G. It follows that the group N coincides with its commutator subgroup. Hence the commutator subgroup of G contains N. The only normal subgroup containing the normalizer of a Sylow group is the whole group. Hence G coincides with its commutator subgroup. This proves Lemma 14.

We have treated one particular case. The remaining cases can be studied similarly. Except one case when $\epsilon = y = 1$ and $x = -1$ in (1) and (2) we find some contradiction. The values of x_μ, y_μ are then computed as follows:

$$\epsilon_1, \quad \epsilon_2, \quad \epsilon_3, \quad 0, \quad 0;$$
$$-\epsilon_1, \quad 0, \quad 0, \quad \epsilon_4, \quad \epsilon_5.$$

The first line gives the values for y_μ, while the second, for x_μ. The values ϵ_i are 1 or -1. Degrees are obtained from the table (4) as follows:

$$-44\epsilon_1, \quad \epsilon_2, \quad \epsilon_3, \quad 45\epsilon_4, \quad 45\epsilon_5 \quad (\bmod 64).$$

The degree of Θ_k is conjugate to -29 (mod 64). Hence $a \geqq 1$ and $(\Theta) \geqq 35$. The number s is at most 4 by Lemma 10. We have

$$1 + 3(\Theta)^2 + \sum_{i=1}^{5} (X_i)^2 \leqq 24256.$$

Then $(\Theta) \leqq 90$ and we get the value 35 for (Θ) and $a = 1$. The equations (5) and (6) are

$$a_1\epsilon_1 + a_2\epsilon_2 + a_3\epsilon_3 = -1 \quad \text{and} \quad -a_1\epsilon_1 + a_4\epsilon_4 + a_5\epsilon_5 = -1.$$

The congruence relations for degrees show that

$$(X_1) \geqq 20, \quad (X_2) \geqq 63, \quad (X_3) \geqq 63, \quad (X_4) \geqq 19, \quad (X_5) \geqq 19$$

and

$$1 + 3(35)^2 + \sum_{i=1}^{5} (X_i)^2 \geqq 12736.$$

If $a_2 > 1$, then we get $(X_2) \geqq 127$ which is impossible. Hence $a_2 = a_3 = 1$. The value of a_1 must be odd and hence $a_1 = 1$. If $\epsilon_1 = -1$, then $\epsilon_2 + \epsilon_3 = 0$. Hence by Lemma 10 the number s is at most 3. This is impossible because $(X_1) = 108$. We have therefore $\epsilon_1 = 1$. This implies that $\epsilon_2 + \epsilon_3 = -2$, $(X_1) = 20$ and $(X_2) = (X_3) = 63$. Moreover $a_4\epsilon_4 + a_5\epsilon_5 = 0$, which implies $a_4 = a_5$. If $a_4 \neq 0$, we have $s \leqq 3$ as before. Then we have too much contribution from X_4 and X_5. Hence we have $a_4 = a_5 = 0$, $\epsilon_4 = \epsilon_5 = 1$ and $(X_4) = (X_5) = 45$.

The values on involutions are computed from the table (4). We have

$$\Theta = 3, \quad X_1 = 4, \quad X_2 = X_3 = -1, \quad X_4 = X_5 = -3.$$

The group order g is then 20160. There is one more character X_6 of degree 64. It is not difficult to compute the table of characters of G but we shall not enter into the details.

9. **Final step of the proof.** We have shown that the order of G is 20160 and G contains a subgroup N of order $16 \cdot 60$. Here N is the subgroup $N_G(H)$ of a subgroup H of order 16 as in §2. The index $[G:H]$ is 21. If we represent G as a transitive permutation group Γ_N on the cosets mod N, then the character of Γ_N is $1 + X_1$. This implies the double transitivity of Γ_N [4, §207]. If S is a Sylow 2-group of G containing H, S contains another elementary abelian subgroup H'. If N' is the normalizer of H' in G, the argument of the third section can be applied to H' as well. We conclude that N' is also a subgroup of index 21. Hence the transitive representation $\Gamma_{N'}$ on the cosets mod N' is doubly transitive.

We consider the set $\mathfrak{R}$ of subgroups conjugate to H and the set $\mathfrak{L}$ consisting of conjugate subgroups of H'. The elements of $\mathfrak{R}$ are called points and the elements of $\mathfrak{L}$ are lines. A point P is on a line l if and only if $P \cap l \neq e$. In exactly the same way as Propositions 14, 15 and 16 of [13, II], we can prove the following lemma.

LEMMA 15. *The sets $\mathfrak{R}$ and $\mathfrak{L}$ equipped with the incidence relation defined above form a projective plane $\mathfrak{P}$ of order 4. The plane $\mathfrak{P}$ is Desarguesian and the group G is a group of collineations of $\mathfrak{P}$.*

In the proof of this lemma the double transitivity plays an essential role. The full group G_0 of collineations of $\mathfrak{P}$ contains the group G_1 of all the uni-

modular projective linear transformations as a normal subgroup and the index $[G_0: G_1]$ is 6. If we identify our group G as a subgroup of G_0, the intersection $G \cap G_1$ is a normal subgroup of G and its index in G is at most 6. On the other hand by Lemma 14 we know that G coincides with its commutator subgroup. Hence $G \cap G_1$ must be identical with G, which means $G_1 \supseteq G$. The order of G_1 is however the same as that of G. Therefore G coincides with G_1. This proves the assertion of Theorem 4.

10. Concluding remarks. The results we have obtained are summarized as follows.

THEOREM 5. *Let G be a nonsolvable* (CIT)-*group. Then the maximal solvable normal subgroup N of G is a 2-group. The factor group G/N is one of the following types:*

$$a \ (ZT)\text{-}group, \quad LF(2, q), \quad LF(3, 4) \quad or \quad M_9.$$

The first part is proved in Theorem II.4. The second part is proved in Theorems II.3, III.1, III.3 and III.4. For the possible values of q in the second case see Theorem III.2.

The structure of N is not arbitrary. The theorem of Neumann [10] we have referred to several times before shows that if the order of G is divisible by 3 the central quotient group of N is abelian. The class of N is therefore at most 2. We can say a little more. If $N \neq e$, every Sylow group for an odd prime number in the quotient group G/N is cyclic by Theorem II.2. This eliminates $LF(2, 9)$, $LF(3, 4)$ and M_9 from the possibility for G/N. If p is a Mersenne prime, the normalizer of a Sylow p-group in G/N is a meta-cyclic group without center. Such a group can not operate on any abelian group without fixed points. Hence if $N \neq e$ the group G/N is not $LF(2, p)$ for any Mersenne prime.

On the other hand if p is a Fermat prime, G/N can be isomorphic with $LF(2, p)$ even if $N \neq e$. In this case however N must be abelian. This can be shown as follows. It follows from the structure of $LF(2, p)$ that G/N contains subgroups isomorphic with the alternating group of four letters. It is easy to show that there are four subgroups U, V, X and Y such that

$$X \supseteq U \supseteq N, \qquad Y \supseteq V \supseteq N, \qquad U \cup V = G$$

and both X/N and Y/N are isomorphic with the alternating group of four letters. Moreover the groups U and V are 2-groups. Then the groups U and V are normal subgroups of X and Y respectively, and X/U, Y/V induce automorphisms of order 3. Let U_0 and V_0 denote the centers of U and V respectively. By a theorem of Neumann [10] the groups U/U_0 and V/V_0 are abelian. Since N contains $C_G(N)$ both U_0 and V_0 are subgroups of N. Hence the commutator subgroup of N is contained in $U_0 \cap V_0$. On the other hand $U_0 \cap V_0$ consists of elements which commute with every element of $U \cup V$. We have chosen U and V in such a way that $G = U \cup V$. Hence we have

$U_0 \cap V_0 = e$. This proves that N is abelian. A similar argument can be applied if the group G/N is isomorphic with LF$(2, 2^{2n})$.

A partial converse statement of Theorem 5 is true. We have the following theorem

THEOREM 6. *If G is any one of the following groups: a (ZT)-group, LF$(2, p)$ with a Fermat or Mersenne prime p, LF$(2, 9)$, LF$(3, 4)$ or M_9, then G is a semi-simple (CIT)-group.*

For (ZT)-groups this is proved in Theorem I.1. For LF$(2, q)$ this follows from the subgroup theorem of Gierster. It is easy to check the assertion for LF$(3, 4)$ or M_9. Except the last group M_9, all groups are simple.

For linear groups in Theorem 6 it is easy to see and actually is known that they are (CN)-groups. It is not yet known whether every (ZT)-group is a (CN)-group. There are only two types of (ZT)-groups known: namely a series of LF$(2, 2^n)$ and another infinite series discovered in [15] recently. All these groups are (CN)-groups (cf. [15]). Theorem I.4 proves that a nonsolvable (CN)-group is a (CIT)-group. As to the converse of this proposition we have the following theorem.

THEOREM 7. *A nonsolvable (CIT)-group G is a (CN)-group if and only if the quotient group G/N is a (CN)-group where N is the maximal solvable normal subgroup of G.*

Proof. Suppose that a nonsolvable (CIT)-group G is a (CN)-group. Then N is a 2-group by Theorem II.4. Consider the group $H = G/N$ and take an element ξ of G/N. If the order of ξ is even, then $C_H(\xi)$ is a 2-group. Assume that the order of ξ is odd. There is an element σ of G such that $\xi = \sigma N$ and the order of σ is odd. Let K be the subgroup of G such that $K/N = C_H(\xi)$. If $\rho \in K$, then $\sigma^{-1}\rho^{-1}\sigma\rho$ belongs to N. The cyclic groups $\{\sigma\}$ and $\{\rho^{-1}\sigma\rho\}$ are conjugate in $\{N, \sigma\}$. There is an element ν of N such that

$$\nu^{-1}\rho^{-1}\sigma\rho\nu = \sigma^k.$$

Since $\rho^{-1}\sigma\rho = \sigma\mu$ with $\mu \in N$, we get $\sigma\mu\nu = \nu\sigma^k$. This implies that $\sigma^k = \sigma$ and $\rho\nu \in C_G(\sigma)$. Hence we have

$$K = C_G(\sigma)N \quad \text{and} \quad C_H(\xi) \cong K/H \cong C_G(\sigma)/C_G(\sigma) \cap N.$$

This proves that G/N is a (CN)-group.

Conversely suppose that G/N is a (CN)-group. Take an element σ of G. If $C_G(\sigma) \cap N \neq e$, then σ is an element of 2-power order by the condition (CIT). If $C_G(\sigma) \cap N = e$, then the group $C_G(\sigma)N/N$ is contained in the centralizer of the element σN in G/N. If G/N is a (CN)-group, $C_G(\sigma)N/N$ is nilpotent. This group is however isomorphic with $C_G(\sigma)$ because $C_G(\sigma) \cap N = e$. Hence G is a (CN)-group.

It follows from Theorem 7 and the remark made just before Theorem 7 that all the nonsolvable (CIT)-groups known so far are (CN)-groups.

Added in proof. Recently the author has classified the (ZT)-groups. According to his result LF$(2, q)$ and the groups $G(q)$ of [15] are the only (ZT)-groups. Hence a nonsolvable (CIT)-group is a (CN)-group (cf. Theorem III.7). For the proof see the author's forthcoming paper in Annals of Mathematics.

BIBLIOGRAPHY

1. R. Brauer and K. A. Fowler, *On groups of even order*, Ann. of Math. vol. 62 (1955) pp. 565–583.
2. R. Brauer, M. Suzuki and G. E. Wall, *A characterization of the one-dimensional unimodular projective groups over finite fields*, Illinois J. Math. vol. 2 (1958) pp. 718–745.
3. R. Brauer and M. Suzuki, *On finite groups whose 2-Sylow group is a generalized quaternion group*, Proc. Nat. Acad. Sci. U.S.A. vol. 45 (1959) pp. 1757–1759.
4. W. Burnside, *The theory of groups of finite order*, Cambridge, 1911.
5. W. Feit, *On a class of doubly transitive permutation groups*, Illinois J. Math. vol. 4 (1960) pp. 170–186.
6. ———, *A characterization of the simple groups* SL$(2, 2^a)$, Amer. J. Math. vol. 82 (1960) pp. 281–300.
7. W. Feit, M. Hall and J. G. Thompson, *Finite groups in which the centralizer of any non-identity element is nilpotent*, Math. Z. vol. 74 (1960) pp. 1–17.
8. K. A. Fowler, Thesis, University of Michigan, 1952.
9. O. Grün, *Beiträge zur Gruppentheorie.* I, Crelle's J. vol. 174 (1936) pp. 1–14.
10. B. H. Neumann, *Groups with automorphisms that leave only the neutral element fixed*, Arch. Math. vol. 7 (1956) pp. 1–5.
11. M. Suzuki, *A characterization of simple groups* LF$(2, p)$, J. Univ. Tokyo vol. 6 (1951) pp. 259–293.
12. ———, *The nonexistence of a certain type of simple groups of odd order*, Proc. Amer. Math. Soc. vol. 8 (1957) pp. 686–695.
13. ———, *On characterizations of linear groups.* I and II, Trans. Amer. Math. Soc. vol. 92 (1959) pp. 191–219.
14. ———, *Applications of group characters*, Proceedings of Symposia in Pure Mathematics, vol. 1, American Mathematical Society, 1959, pp. 88–99.
15. ———, *A new type of simple groups of finite order*, Proc. Nat. Acad. Sci. U.S.A. vol. 46 (1960) pp. 868–870.
16. ———, *Investigations on finite groups*, Proc. Nat. Acad. Sci. U.S.A. vol. 46 (1960) pp. 1611–1614.
17. J. G. Thompson, Thesis, University of Chicago, 1959.
18. H. Zassenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg vol. 11 (1936) pp. 17–40.
19. ———, *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg vol. 11 (1936) pp. 187–220.
20. ———, *Lehrbuch der Gruppentheorie.* I, Leipzig-Berlin, B. G. Teubner, 1937.

UNIVERSITY OF ILLINOIS,
    URBANA, ILLINOIS