

## On the finite group with a complete partition

Michio SUZUKI.

(Received Jan. 15, 1950)

A *partition* of a group  $G$  is a system  $\{H_i\}$  of subgroups of  $G$  such that every element of  $G$  except the unit element is contained in one and only one of the groups  $H_i$ .  $H_i$  are called components of this partition. A partition of  $G$  is called *complete*, when all of its components are cyclic. A group with a complete partition is called *completely decomposable* (c. d.).

Of course not every group has a complete partition. In this paper we shall deal with finite groups with a complete partition, and determine the structure of such groups, when they are non-simple. Our main theorem is the following:

*Let  $G$  be a non-simple, non-solvable c.d. group. Then  $G$  is isomorphic to the full linear fractional group of one variable over a finite field whose characteristic is greater than 2.*

The author has, however, not yet been able to determine the structure of c.d. simple groups. Well-known simple groups  $LF(2, p^n)$  are clearly c.d., and it is conjectured that no other c.d. simple group exists. Every known simple group contains one of  $LF(2, p^n)$  as its subgroup, so  $LF(2, p^n)$  may be regarded as the "least" simple group. It is suggested by this fact, as it seems to the author, that the problem to find the structure of c.d. simple groups would be an interesting and important one.

Finite groups with complete partitions have been considered by Kontorovitch [1]<sup>1)</sup> and [2]. His results will be sharpened to theorems 1, 2 and 3 of this paper and will play fundamental role in our study. This paper is written, so as to be read without reference to Kontorovitch, so that the results of §1 of this paper are essentially the same with his. In §2 we shall determine the structure of c.d. solvable groups, and give the complete classification of such groups. In §3 we shall give some remarks on the structure of c.d. groups and shall prove in §4 the main theorem stated above. Our proof of this theorem is based on a characterization of linear

---

(1) The numbers in brackets refer to the bibliography at the end of the paper.

groups as permutation groups, due to Zassenhaus [3]. In fact we show that non-solvable, non-simple c.d. groups are representable as triply transitive permutation groups, and then apply the theorem of Zassenhaus cited above.

Finally, the author wishes to express his hearty thanks to Mr. N. Itê, who gave him many useful remarks. Due to his suggestions and advices, the proofs of theorems 1 and 5 were made considerably shorter than the author's original one, and the author owes to him the lemma 6 of this paper. Moreover the author expresses here his sincere thanks to Prof. S. Iyanaga and K. Iwasawa for their kind encouragement throughout this work.

### § 1. Preliminaries

**Lemma 1.** *A group is c.d., if and only if two arbitrary maximal cyclic subgroups are identical or have no element in common except the unit element.*

*Proof.* Suppose a group  $G$  to be c.d., and let  $\{H_i\}$  be its complete partition. Take two arbitrary maximal cyclic subgroups  $Z_1$  and  $Z_2$  of  $G$  such that  $Z_1 \cap Z_2 \cong e$ , and put  $Z_1 = \{a\}$  and  $Z_2 = \{b\}$ . Because of the definition of  $\{H_i\}$   $a$  is contained in one of its components, say  $H_1$ . Similarly  $b$  is in  $H_k$ . We have then  $\{a\} = Z_1 \subseteq H_1$  and  $\{b\} = Z_2 \subseteq H_k$ . Since  $Z_1 \cap Z_2 \cong e$ , we conclude that  $Z_1 = H_1 = H_k = Z_2$ .

Conversely suppose that every pair of distinct maximal cyclic subgroups of a group  $G$  has no element in common except the unit element. Consider a system  $\{H_i\}$  of subgroups of  $G$ , consisting of all its maximal cyclic subgroups. This system  $\{H_i\}$  gives then clearly a complete partition of  $G$ . q.e.d.

The following lemma is an easy consequence of lemma 1 and is often used in the course of this study.

**Lemma 2.** *Any subgroup of a c.d. group is itself c.d.*

Now we obtain

**Lemma 3.** *Let  $G$  be a nilpotent c.d. group. Then  $G$  is either cyclic or of prime power order.*

*Proof.* Let  $\{H_i\}$  be a complete partition of  $G$ . It is sufficient to prove that  $G$  is cyclic when it is not of prime power order. Take an element  $a$  of prime power order, say of order  $p^m$ . Then  $a$  is contained in one of the components, say  $H_1$ . Let  $b$  be another element of order  $q^n$ , where  $q$  is also a prime,  $\neq p$ . The subgroup  $\{a, b\}$ , generated by  $a$  and  $b$ , is cyclic and hence by the definition of the system  $\{H_i\}$ ,  $\{a, b\}$  is contained in  $H_1$ .

Since  $b$  is any element of order  $q^n$ , this implies that  $H_1$  contains the  $q$ -Sylow subgroup of  $G$ . Hence we must have  $H_1 = G$  and  $G$  is cyclic.

*Remark.* The proof of lemma 3 shows the validity of the following general proposition which includes our lemma 3 as a special case.

*If a nilpotent group has a proper partition (that is, consisting of more than one component in the reduced form), then it is of prime power order.*

Some of our results hold also good under weaker conditions than stated in this paper, on which we shall not enter here.<sup>2)</sup>

In the following we shall call a  $p$ -group a  $p$ -group of type  $p$ , when all of its elements other than the identity are of order  $p$ . Such a group is clearly c.d. Now we have

**Theorem 1.** *A  $p$ -group is c.d., if and only if it is one of the following types: (1) a cyclic group, (2) a  $p$ -group of type  $p$ , or (3) a dihedral group.*

*Proof.* Let  $G$  be a c.d.  $p$ -group which contains an element  $a$  of order  $p^2$ . By lemma 2 the subgroup  $\{a\}$  generated by  $a$  contains all elements of order  $p$  which commute with  $a$ . Hence  $\{a\}$  is only one cyclic subgroup of  $G$  whose order is  $p^2$  and so it is clearly self-conjugate in  $G$ . If  $\{a\}$  is contained in the center of  $G$ ,  $G$  has only one subgroup of order  $p$ . Hence  $G$  is either cyclic or a generalized quaternion group<sup>3)</sup>, and the latter is clearly not c.d. Hence  $G$  must be cyclic. If  $\{a\}$  is not contained in the center of  $G$ , the centralizer  $H$  of  $\{a\}$  is a proper subgroup of  $G$  and self-conjugate in  $G$ . Since  $G/H$  is isomorphic to some subgroup of the group of all automorphisms of  $\{a\}$ , the index  $(G:H)$  is  $p$ .  $H$  is c.d. by lemma 2 and  $\{a\}$  is contained in the center of  $H$ . Hence  $H$  is a cyclic subgroup of index  $p$ . The structure of such a group as  $G$  is known<sup>4)</sup> and it shows that  $G$  is a dihedral group.

The converse statement is almost obvious. q.e.d.

We shall call a group  $G$  to be of type  $D$ , or strictly of type  $D_p$ , when  $G$  is directly decomposable and satisfies the following conditions:  $G =$

(2) For instance, our main theorem, theorem 9 of this paper, holds good when  $G$  is a non-simple, non-solvable, abelian decomposable group, which has a partition consisting of abelian components. We owe this generalization to N. Itô. Cf. the forthcoming paper of N. Itô. In addition we can determine the structure of groups, which are not c. d., but whose proper subgroups are all c. d. Such groups are proved to be solvable and have very simple structures.

(3) Zassenhaus [5], p. 112.

(4) See for instance Zassenhaus [5], p. 114.

$G_1 \times G_2$ , where  $G_1$  is a cyclic group of order  $p$  ( $p$  is a prime number), and  $G_2 = \{a, b\}$ ,  $a^n = b^n = 1$ ,  $bab^{-1} = a^r$ ,  $(n, p(r-1)) = 1$  and  $r^n \equiv 1 \pmod{n}$ .

We can easily see that a group of type  $D$  is solvable and c.d. Now we shall prove

**Theorem 2.** *If a c.d. group is directly decomposable, then it is one of the following types: (1) a cyclic group, (2) a  $p$ -group of type  $p$ , or (3) a group of type  $D$ .*

*Proof.* Let  $G$  be a directly decomposable c.d. group:  $G = G_1 \times G_2$ . If  $G$  is a  $p$ -group, then  $G$  is of type  $p$  by theorem 1. We may, therefore, assume that  $G$  is not a  $p$ -group. If both  $G_1$  and  $G_2$  are cyclic, then by lemma 3  $G$  is either cyclic or of prime power order. Then we may assume moreover one of its direct components, say  $G_2$ , is not cyclic. If  $G_2$  were of prime power order, say of order  $r^m$  ( $r$  is a prime),  $G_1$  should not be of order  $r^m$ . Take then a  $p$ -Sylow subgroup  $T$  of  $G_1$ , where  $p$  is a prime,  $\not\equiv r$ .  $T \cup G_2$  should be c.d. and nilpotent so  $G_2$  should be cyclic by lemma 3. This is not the case. Hence  $G_2$  is not of prime power order.

Take any  $p$ -Sylow subgroup  $T_p$  of  $G_1$  and any  $q$ -Sylow subgroup  $S_q$  of  $G_2$ , where  $p$  and  $q$  are two distinct primes. Since  $T_p \cup S_q = T_p \times S_q$ , both  $T_p$  and  $S_q$  are cyclic by lemma 3. If  $S_q$  were not self-conjugate in  $G_2$ ,  $S_q$  should be conjugate to another  $q$ -Sylow subgroup  $S'_q$  of  $G_2$ . Since again  $T_p \cup S'_q = T_p \times S'_q$ ,  $T_p \cup S'_q$  should be cyclic. Hence  $T_p \cup S_q$  and  $T_p \cup S'_q$  should be two cyclic subgroups, containing  $T_p$  in common. By lemma 1 there should exist a maximal cyclic subgroup of  $T_p \times G_2$  containing both  $T_p \cup S_q$  and  $T_p \cup S'_q$ . But  $S_q$  and  $S'_q$  are two distinct  $q$ -Sylow subgroups of  $T_p \times G_2$ , and there is no cyclic subgroup of  $G_2$  containing both  $S_q$  and  $S'_q$ . This contradiction shows that  $S_q$  is a cyclic normal subgroup of  $G_2$ .<sup>5)</sup> Since  $q$  is any prime other than  $p$ , the  $q$ -Sylow subgroup of  $G_2$  is self-conjugate whenever  $q \not\equiv p$ . This implies that  $G_1$  must coincide with  $T_p$ , and the order of  $G_2$  is divisible by  $p$ , as we assumed that  $G_2$  is not cyclic. At the same time we see that the Sylow  $p$ -complement<sup>6)</sup> of  $G_2$ , which we shall denote by  $N$ , is a cyclic normal subgroup of  $G_2$ .

Take any  $p$ -Sylow subgroup  $S_p$  of  $G_2$ , then  $G_1 \times S_p$  is a  $p$ -Sylow sub-

(5) This method, which shows us the normality of Sylow subgroups, is often used in the course of this study.

[6] A Sylow  $p$ -complement of a group of order  $g = p^\alpha g'$ ,  $(p, g') = 1$ , is a subgroup of  $G$  of order  $g'$ . Such a subgroup does not always exist. Cf. papers of P. Hall; Proc. London Math. Soc. 3 (1928), 12 (1937) etc.

group of  $G$  and c.d. Hence  $G_1 \times S_p$  is of type  $p$ . This implies that  $G_1$  is a cyclic group of order  $p$ . To conclude our proof of this theorem we have only to prove that  $S_p$  is also cyclic and that the centralizer of  $S_p$  in  $G_2$  coincides with  $S_p$ . Take any subgroup  $H$  of  $N$  with prime power order, and consider a subgroup  $K = G_1 \times (S_p \cup H)$ . If the centralizer  $H^*$  of  $H$  in  $S_p \cup H$  were not equal to  $H$ ,  $H^*$  should be directly decomposable and so nilpotent. So  $G_1 \times H^*$  should be also nilpotent, but its  $p$ -Sylow subgroup is not cyclic. This is a contradiction. Hence we have  $H^* = H$ . Therefore  $S_p \cong (S_p \cup H)/H$  is isomorphic to some subgroup of the group of all automorphisms of  $H$ , and it shows that  $S_p$  is cyclic. Hence  $S_p$  is of order  $p$ . This completes our proof.

**Theorem 3.** *A group  $G$  is c.d. and its center contains at least two elements, if and only if  $G$  is one of the following types: (1) a cyclic group, (2) a  $p$ -group of type  $p$ , (3) a dihedral group whose order is divisible by 4, or (4) a group of type  $D$ .*

*Proof.* Let  $G$  be a c.d. group and  $Z$  be its center. By our assumption we have  $Z \cong e$ . Denote by  $Z_p$  the  $p$ -Sylow subgroup of  $Z$  and by  $S_q$  the  $q$ -Sylow subgroup of  $G$ . If  $p \neq q$ ,  $Z_p \cup S_q = Z_p \times S_q$ , and so by lemma 3  $Z_p \cup S_q$  is cyclic. By the same method as in the proof of the theorem 2,  $S_q$  is a normal subgroup of  $G$ . Hence if  $Z$  is not of prime power order,  $G$  is cyclic. We may, therefore, assume that  $Z$  is of prime power order, say of order  $p^n$ . Let  $S_p$  be one of  $p$ -Sylow subgroups of  $G$ . Then  $S_p$  contains  $Z$ . If  $S_p = G$ , theorem 1 shows that  $G$  is one of the types (1), (2) and (3) of this theorem. We may, therefore, assume that  $S_p \neq G$ . If we take a prime factor  $q$  of the order of  $G$  other than  $p$ ,  $S_q$  is a cyclic normal subgroup of  $G$ , so the Sylow  $p$ -complement  $N$  of  $G$  exists and is a cyclic normal subgroup of  $G$ . If  $S_p$  were self-conjugate,  $G$  should be nilpotent. This is not the case. Hence  $S_p$  is not self-conjugate. Since any conjugate subgroup of  $S_p$  contains  $Z$ ,  $S_p$  is not cyclic. Then  $S_p$  is by theorem 1 either a  $p$ -group of type  $p$  or a dihedral group.

a) Suppose that  $S_p$  is a  $p$ -group of type  $p$ . Take a subgroup  $H = S_p S_q$  of  $G$ , generated by  $S_p$  and the  $q$ -Sylow subgroup  $S_q$  of  $G$  ( $p \neq q$ ). Then the centralizer  $U$  of  $S_q$  in  $H$  is self-conjugate in  $H$  and  $H/U$  is cyclic, as it is isomorphic to some subgroup of the group of all automorphisms of  $S_q$ . On the other hand,  $U$  is a direct product of  $S_p \cap U$  and  $S_q$ . Hence  $S_p \cap U$  is cyclic by lemma 3, so that  $S_p$  is of order  $p^2$ . Hence  $G$  is directly de-

composable and is of type  $D$  by theorem 2.

b) Suppose next  $S_p$  to be of dihedral type. As above we consider again a subgroup  $H = S_p S_q$  of  $G$ . If we take the centralizer  $U$  of  $S_q$  in  $H$ , both  $T = U \cap S_p$  and  $S_p/T \cong S_p/U \cap S_p \cong H/U$  are cyclic. Hence  $T$  is a cyclic normal subgroup of  $S_p$  with index 2. Since  $T$  is self-conjugate in  $H = S_p S_q$  and  $q$  is any prime factor of the order of  $G$  other than  $p$ ,  $T$  is self-conjugate in  $G$ . If the normalizer  $N_p$  of  $S_p$  in  $G$  were not equal to  $S_p$ ,  $N_p$  should be directly decomposable against theorem 2. So we have  $S_p = N_p$ . The factor group  $\bar{G} = G/T$  contains a normal subgroup  $\bar{N} = NT/T$  and  $(\bar{G} : \bar{N}) = 2$ . The element of  $\bar{S} = S_p/T$  induces then an automorphism  $\sigma$  of order 2 in  $\bar{N}$  and  $\sigma$  fixes only one element of  $\bar{N}$ . Hence  $\bar{G}$  must be of dihedral type.<sup>7)</sup> Since  $T \cup N = T \times N$  and since  $S_p$  is a dihedral group,  $G$  itself is a dihedral group. The converse statement is obvious.

Essentially the same theorems as the above three theorems are also obtained by Kontorovitch [1] and [2].

## § 2 The structure of c.d. solvable groups

In this paragraph we determine the structure of c.d. solvable groups. We shall call in general the maximal solvable normal subgroup of a group its *radical*, and consider c.d. groups whose radicals are distinct from  $e$ . C.d. solvable groups are of course such groups, but it will turn out at the end of this paragraph that, conversely, all these groups are solvable. We shall first prove the following lemmas.

**Lemma 4.** *If a c.d. group  $G$  contains an elementary abelian  $p$ -group  $N$  as its normal subgroup, then for a prime  $q, \neq p$ , the  $q$ -Sylow subgroup of  $G$  is one of the following types: (1) a cyclic group, (2) a dihedral group or (3) an abelian group of type (1, 1). If moreover one of  $q$ -Sylow subgroup of  $G$  is either of type (2) or (3), then the order of  $N$  is  $p$ .*

*Proof.* Let  $q$  be any prime factor of the order of  $G$  other than  $p$ , and  $S_q$  be one of  $q$ -Sylow subgroups of  $G$ . We shall show that if  $S_q$  is not cyclic but a  $q$ -group of type  $q$ , then  $S_q$  is of order  $q^2$ . Take a subgroup  $H = S_q N$ . By a lemma of Zassenhaus<sup>8)</sup>  $H$  contains an element  $a$  of order  $pq$ . Put then  $V = \{a^q\}$ .  $V$  is clearly a subgroup of  $N$ , and is contained in the center of  $\{N, a\}$ . Hence by theorem 3  $\{N, a\}$  must be cyclic. This

(7) Cf. Zassenhaus [3], Satz 1.

(8) Zassenhaus [4], Satz 3.

implies that  $(N : e) = p$ . Let  $U$  be the centralizer of  $N$  in  $H$ . Then  $U$  is a direct product of  $N$  and  $U \cap S_q$  which implies by lemma 3 that  $U \cap S_q$  is cyclic. Clearly  $U$  is also self-conjugate in  $H$  and  $H/U$  is cyclic. This implies that  $S_q$  is of order  $q^2$ . The second assertion of this lemma is already proved in this case when  $S_q$  is of type  $q$ .

Now assume  $S_q$  to be a dihedral group.  $S_q$  contains an abelian group  $T$  of order 4 and of type (1,1). Then the same consideration as above (for a subgroup  $K = NT$ ) shows that  $(N : e) = p$ . This completes the proof.

**Lemma 5.** *If a c.d. group  $G$  contains a normal subgroup  $N$  of order  $p$  ( $p$  is a prime), then  $G$  is a  $J$ -group.<sup>9)</sup>*

*Proof.* Let  $Z$  be the centralizer of  $N$  in  $G$ . If  $Z = G$ , our lemma is an easy consequence of theorem 3. We may assume that  $Z \neq G$ .  $Z$  is clearly a normal subgroup of  $G$  and  $G/Z$  is cyclic, as it is isomorphic to some subgroup of the group of all automorphisms of  $N$ . Put  $d = (G : Z)$ , then we have  $d \mid p-1$ . The structure of  $Z$  is known by theorem 3. The groups of the types (1), (3) and (4) in theorem 3 have a normal series, consisting of characteristic subgroups, all of whose factor groups are of prime order, then if  $Z$  is of such types,  $G$  has also a principal series, all of whose factor groups are of prime order, that is,  $G$  is a  $J$ -group. If  $Z$  is a  $p$ -group of type  $p$ , we consider a central series

$$Z = Z_r \supseteq Z_{r-1} \supseteq \dots \supseteq Z_0 = e$$

of  $Z$ , where  $Z_i/Z_{i-1}$  is the center of  $Z/Z_{i-1}$  ( $i=1,2,\dots,r$ ). When we regard each  $Z_i/Z_{i-1}$  as a  $G/Z$ -module,  $Z_i/Z_{i-1}$  is decomposable into simple  $G/Z$ -modules, and since  $d = (G : Z)$  divides  $p-1$ , each simple  $G/Z$ -module is one dimensional. This implies that  $G$  has a principal series, all of whose factor groups are of prime order, that is,  $G$  is again a  $J$ -group.

**Theorem 4.** *Let  $G$  be a c.d. group, containing a normal subgroup of order  $p$  ( $p$  is a prime). Then  $G$  is one of the following types :*

- (1).....(4) as in theorem 3, or
- (5)  $G = \{a, b\}$ ,  $a^n = b^m = 1$ ,  $bab^{-1} = a^r$ ,  $(n, m(r-1)) = 1$ ,  
 $r^m \equiv 1 \pmod{n}$  and if  $r^{m'} \equiv 1 \pmod{n'}$  ( $m' \mid m$ ,  $n' \mid n$ ) then

---

(9) A  $J$ -group is a group possessing a principal series, all of whose factor groups are of prime order. This group is also characterized by the property that it is a group with a lattice of subgroups which satisfies the Jordan-Dedekind chain condition. Cf. K. Iwasawa, Jour. of Sci. Univ. of Tokyo (1941).

we have  $m' = m$ , or

(6)  $G = S_p H$ , where  $S_p$  is a normal subgroup of  $G$  and a  $p$ -group of type  $p$ ,  $H$  is a cyclic subgroup of order  $d$  and  $d \mid p-1$ .

*Proof.* We shall prove that if a c.d. group  $G$  contains a normal subgroup of order  $p$  and if its center coincides with  $e$ ,  $G$  is either of type (5) or (6) in this theorem. Let  $G$  be a c.d. group whose center coincides with  $e$ , and  $N$  be its normal subgroup of order  $p$ . By lemma 5,  $G$  is a  $J$ -group and hence we may assume that  $p$  is the greatest prime factor of the order of  $G^{(10)}$ . We shall denote by  $Z$  the centralizer of  $N$  in  $G$ . By our assumption we have  $Z \cong G$ , and  $Z$  is a normal subgroup of  $G$ . The factor group  $G/Z$  is then cyclic and its order  $d$  divides  $p-1$ . Since  $Z$  is a c.d. group and its center contains  $N$ ,  $Z$  is a cyclic group, a  $p$ -group of type  $p$ , a dihedral group or a group of type  $D$  as in theorem 3. By our assumption  $p$  is the greatest prime factor of the order of  $G$ , so that  $Z$  is neither a dihedral group nor a group of type  $D$ . Hence  $Z$  is either cyclic or a  $p$ -group of type  $p$ .

a) Suppose first  $Z$  to be cyclic. Then  $Z$  is clearly a maximal cyclic subgroup. Put  $Z = \{a\}$  and take an element  $b$  of  $G$  which generates  $G$  mod  $Z$ . Since  $G$  is c.d., it holds clearly  $\{a\} \cap \{b\} = e$ . Let  $n$  and  $m$  be the orders of  $a$  and  $b$  respectively. We shall show that  $n$  and  $m$  are relatively prime. If  $n$  and  $m$  had a common prime factor  $q$ , there should exist two subgroups  $U$  and  $V$  of order  $q$  such that  $U \subseteq \{a\}$  and  $V \subseteq \{b\}$ . Then denote by  $K$  the centralizer of  $V$  in  $G$ .  $K$  should contain clearly  $U$  and  $H = \{b\}$ . Hence  $K$  should be non-cyclic. If  $K$  were a group of type  $D$ ,  $U$  should not be self-conjugate in  $K$ . This is not the case. Hence  $K$  should be either a  $q$ -group of type  $q$  or a dihedral group. But since  $U$  is self-conjugate in  $K$ ,  $K$  should be a  $q$ -group of type  $q$ . Hence we should have  $H = V$  and this implies that  $U$  should be contained in the center of  $G$  against our assumption. Hence we have  $(n, m) = 1$ , and every Sylow subgroup of  $G$  is cyclic. Moreover since  $G$  is c.d., every conjugate subgroup of  $H$  coincides with  $H$  or has no element in common except the unit element with  $H$ . Hence  $G$  is a group of type (5) in this theorem.

b) Suppose next that  $Z$  is a  $p$ -group of type  $p$ . Then  $Z$  is a  $p$ -Sylow subgroup of  $G$  and we have a group of type (6).

---

(10) Cf. Iwasawa loc cit. (9)



*Remark.* Groups of types (1).....(5) in this theorem are clearly c.d., but groups of type (6) are not always c.d. The condition on a group of type (6) to be c.d. will be given later (see theorem 6).

**Lemma 6.**<sup>(11)</sup> *Let  $G$  be a c.d. group having a normal subgroup  $N$ . If  $N$  is an abelian group of order  $p^n$  and of type  $(1,1,\dots,1)$  with  $n > 2$  and  $p > 2$ , then  $p$ -Sylow subgroup of  $G$  is self-conjugate in  $G$ .*

*Proof.* Take a prime factor  $q$  of the order of  $G$  other than  $p$ , then lemma 4 shows that  $q$ -Sylow subgroups of  $G$  are cyclic. First we shall prove that  $G$  has no element of order  $pq$ . Assume to the contrary that  $G$  had an element  $a$  of order  $pq$ . Let  $H$  be the centralizer of the element  $a^q$ . Since  $N$  meets the center of  $S_p$ , we should have  $H \cap N \neq e$ . By our assumptions  $H$  should be a group of type  $D$  (by theorem 3), and  $H \cap N$  should be self-conjugate in  $H$ , so  $H \cap N$  should coincide with  $\{a^q\}$ . On the other hand, since  $N$  should contain  $\{a^q\}$ ,  $H$  should contain  $N$  too. This is a contradiction. Hence  $G$  has no element of order  $pq$ .

We shall now prove this lemma by induction on the order of  $G$ . Take the least prime factor  $q$  of the order of  $G$  other than  $p$  and one of  $q$ -Sylow subgroups  $S_q$ . If the order of the normalizer  $N_q$  of  $S_q$  in  $G$  is not divisible by  $p$ ,  $S_q$  is clearly contained in the center of  $N_q$ . Hence by a theorem of Burnside<sup>(12)</sup>  $G$  has a self-conjugate Sylow  $q$ -complement  $H_q$ . By hypothesis of induction  $S_p$  is self-conjugate in  $H_q$  and so in  $G$ .

Assume that  $p$  divided the order of  $N_q$ . We shall take a  $p$ -Sylow subgroup  $P$  of  $N_q$ , and a subgroup  $Q$  of  $S_q$ , whose order is  $q$ . Then  $P$  should not be self-conjugate in  $N_q$ . In the subgroup  $K = N \cdot P \cdot Q$ ,  $NP$  should be a  $p$ -Sylow subgroup and maximal. Because of  $p > 2$ ,  $NP$  should be a  $p$ -group of type  $p$ , and so a regular  $p$ -group in the sense of P. Hall<sup>(13)</sup>. Since  $P$  should not be self-conjugate in  $N_q$ ,  $NP$  also should be non-normal in  $K$ . Hence by a theorem of Wielandt<sup>(14)</sup>  $Q$  should be self-conjugate in  $K$ . This leads us to the contradiction that  $NQ = N \times Q$  and  $G$  should have an element of order  $pq$ . Hence we have our lemma 6.

**Theorem 5.** *Let  $G$  be a c.d. group having a solvable normal subgroup*

(11) This lemma is due to N. Itô, who simplified the proof of the next theorem using this lemma

(12) Zassenhaus [5], p. 133.

(13) Cf. P. Hall, Proc. London Math. Soc. 2-36 (1932).

(14) Cf. H. Wielandt, Crelle 182 (1940).

other than  $e$ . Then  $G$  is one of the following types :

- (1).....(6) as in theorem 4, or  
 (6)\* similar to (6) in theorem 4 but without the condition  $d|p-1$ , or  
 (7) the symmetric group of four letters.

*Proof.* By assumption of this theorem  $G$  has a solvable normal subgroup other than  $e$ , so we can take an elementary abelian normal subgroup  $N$  of order  $p^n$ . We have only to prove that  $G$  is either of the type (6)\* or (7) when  $n$  is greater than one:  $n > 2$ .

If  $p > 2$ , the  $p$ -Sylow subgroup  $S_p$  of  $G$  is self-conjugate by lemma 6. Then in virtue of a theorem of Schur<sup>(15)</sup> there is a Sylow  $p$ -complement  $H$ . By lemma 4 every Sylow subgroup of  $H$  is cyclic. This implies that  $H$  is solvable<sup>(16)</sup> and has a normal subgroup of prime order. Hence by theorem 4  $H$  is either cyclic or a group of type (5) in theorem 4. On the other hand,  $G$  has no element of order  $pq$ , so that every subgroup of  $H$ , whose order is the product of two primes, is cyclic by a lemma of Zassenhaus<sup>(17)</sup>. Hence  $H$  must be cyclic and we have a group of type (6)\*.

Suppose next that  $p=2$ . Take one of 2-Sylow subgroups  $S$  of  $G$  containing  $N$ . If  $S$  is a 2-group of type 2, it is abelian and so is the centralizer of  $N$ . Hence  $S$  is self-conjugate in  $G$ . We can show that  $G$  is a group of type (6)\* in the similar way as above. If  $S$  is a dihedral group,  $N$  is of order 4 and  $S$  is of order 8. The centralizer of  $N$  must clearly coincide with  $N$ . Hence we have  $(G : N) \leq 6$ , as  $G/N$  is isomorphic to a subgroup of the group of all automorphisms of  $N$ . On the other hand,  $(G : N)$  is divisible by 2 and also by at least one other prime number. Hence we have  $(G : N) = 6$  and so  $(G : e) = 24$ . This implies that  $G$  is isomorphic to the symmetric group of four letters.<sup>(18)</sup>

**Corollary.** *A c.d. group whose radical differs from  $e$  is solvable.*

This theorem shows clearly the structure of c.d. solvable groups. The groups of types (1).....(5) and (7) are c.d., as easily shown, but the groups of types (6) and (6)\* are not always c.d. We shall now give a condition on groups of types (6) or (6)\* to be c.d.

Let  $G$  be a group of type (6) or (6)\* in theorem 5, i.e.  $G = SH$ ,

(15) Zassenhaus [5], p. 125.

(16) Zassenhaus [4], Satz 4.

(17) Cf. (8).

(18) Zassenhaus [5], p. 111.

where  $S$  is a  $p$ -Sylow subgroup of  $G$  and self-conjugate, and  $H$  is a cyclic subgroup. Then  $H$  is regarded as an operator domain of  $S$ . We shall call a subgroup  $U$  of  $S$  an  $H$ -subgroup when it holds  $hUh^{-1} \subseteq U$  for any element  $h$  of  $H$ , and a series of subgroups of  $S$

$$S = U_0 \supset U_1 \supset \dots \supset U_r = e$$

an  $H$ -composition series when  $U_i$  is a maximal self-conjugate  $H$ -subgroup of  $U_{i-1}$  ( $i=1,2,\dots,r$ ). Then each factor group  $U_{i-1}/U_i$  is an abelian group of order  $p^{n_i}$  and of the type  $(1,1,\dots,1)$ , and is a simple  $H$ -module when we regard  $H$  as its operator domain.

Take now in general a simple  $H$ -module  $V$ . Then  $V$  is a representation module of  $H$ . When this representation of  $H$  is isomorphic, we shall call  $V$  an *irreducible*  $H$ -module. Since  $H$  is an operator domain of  $V$ , we can construct the extension of  $V$  by  $H$ . A simple  $H$ -module  $V$  is irreducible if and only if this extension of  $V$  by  $H$  has no element of order  $p q$  ( $q > 1$ ). Now we shall prove

**Theorem 6.** *Let  $G$  be a group of type (6) or (6)\* in theorem 5.  $G$  is c.d. if and only if each factor group of an  $H$ -composition series of  $S$  is an irreducible  $H$ -module.*

*Proof.* Suppose  $G$  to be c.d.  $G$  has then no element of order  $p q$  ( $q > 1$ ) as in the proof of lemma 6. Hence each factor group of an  $H$ -composition series of  $S$  is irreducible. Suppose conversely that each factor group of an  $H$ -composition series of  $S$  is irreducible. Then  $G$  has no element of order  $p q$  ( $q > 1$ ). Take two distinct conjugate subgroups  $H_1$  and  $H_2$  of  $H$ . If  $H_1 \cap H_2 = K \neq e$ , the centralizer  $Z$  of  $K$  should contain both  $H_1$  and  $H_2$ . Since  $H_1 \neq H_2$ , it should hold  $Z \cap S \supseteq (H_1 \cup H_2) \cap S = T \neq e$ . We should have  $T \cup K = T \times K$  and  $G$  should have an element of order  $p q$  ( $q > 1$ ). This is a contradiction. Hence two distinct conjugate subgroups of  $H$  have no element in common except the unit element. Let  $\{P_i\}$  be a complete partition of  $S$ . Then the system  $\{P_i, H, H_1, H_2, \dots\}$ , consisting of  $\{P_i\}$  and of all distinct conjugate subgroups  $H, H_1, \dots$  of  $H$  gives a complete partition of  $G$ .

### §3. Two remarks on c.d. groups

Theorems 5 and 6 in the last paragraph shows that the factor group of a c.d. solvable group is itself c.d. This proposition holds, however, good for general c.d. groups.

**Theorem 7.** *Any factor group of a c.d. group is itself c.d.*

*Proof.* We shall prove this theorem by induction on the length of a principal series. Let  $G$  be a c.d. group and  $N$  be its normal subgroup. Using induction we have only to prove our theorem in the case when  $N$  is a minimal normal subgroup. If  $N$  is solvable, by theorem 5  $G$  is also solvable and our theorem follows from theorems 5 and 6. If  $N$  is not solvable, we take a  $p$ -Sylow subgroup  $S_p$  of  $N$ . Denote by  $N_p$  the normalizer of  $S_p$  in  $G$ , then we have  $N_p N = G$ , and  $N_p$  is solvable. Since  $G/N \cong N_p/N_p \cap N$ ,  $G/N$  is c.d. too.

*Remark.* Theorem 7 does not hold for infinite groups. For example, the free group with  $n$  generators ( $n > 2$ ) is c.d.,<sup>(19)</sup> but its factor groups are not always c.d.

**Theorem 8.** *Let  $G$  be a c.d. non-solvable, non-simple group, and  $N$  be its minimal normal subgroup. Then we have  $(G : N) = 2$ .*

*Proof.* We shall prove our theorem by induction on the order of  $G$ . By theorem 2  $N$  is a simple group. Take a Sylow subgroup  $S$  of  $N$  and its normalizer  $H$  in  $G$ . Then we have  $NH = G$  and  $G/N \cong H/H \cap N$  is solvable. Suppose that  $G/N$  were not simple. Take a maximal subgroup  $M$  of  $G$  containing  $N$ , then we should have  $(M : N) = 2$  by the hypothesis of induction, so  $(G : N)$  should be equal to 4. Since  $N$  is simple, its 2-Sylow subgroup  $T$  is not cyclic if  $T \neq e$ . Take a 2-Sylow subgroup  $U$  of  $G$  containing  $T$ . If  $U$  were a dihedral group,  $T$  should be cyclic. Hence  $U$  should be a 2-group of type 2 and so abelian. Take now the normalizer  $V$  of  $U$  in  $G$ , then by a theorem of Burnside  $V \neq U$ .  $V$  should be a group of type (6) or (6)\*. We should, however, have  $V/U \cap N \cong (U/U \cap N) \times (V \cap N/U \cap N)$  against the theorem 6. Hence  $(G : N) = q$  is a prime.

We shall now prove that  $q = 2$ . We shall denote by  $S$  a  $q$ -Sylow subgroup of  $G$ . Assume first that  $q$  did not divide the order of  $N$ . Take the centralizer  $T$  of  $S$  in  $G$ , then we should have  $T = S \times Z$ , where  $Z \subseteq N$ .  $Z$  should, therefore, be cyclic, and  $T$  should be a maximal cyclic subgroup of  $G$ . Hence the normalizer of  $Z$  in  $N$  should coincide with  $Z$ , if  $Z \neq e$ . This is however a contradiction, as the normalizer of a  $p$ -Sylow subgroup of  $Z$ , which is clearly a Sylow subgroup of  $G$ , should be equal to  $Z$  and so  $N$  should not be simple by a theorem of Burnside. Hence  $Z$  should be equal to  $e$ . Take any prime factor  $p$  of the order of  $N$ , and one of its

(19) Cf. M. Takahasi, Osaka Math. Jour. 1 (1948).

$p$ -Sylow subgroups  $S_p$ . Let  $N_p$  be the normalizer of  $S_p$  in  $G$ . Then we have  $N_p N = G$ , so that the order of  $N_p$  is divisible by  $q$ . As  $S \cap N = e$ ,  $G$  should have no element of order  $qr$  ( $r > 1$ ). Hence  $N_p$  should not be of types (1), (2), (3), (4) and (7) in theorem 5. If  $N_p$  were of type (6) or (6)\*, the normalizer of  $S_p$  in  $N$  should coincide with  $S_p$ . Since  $S_p$  is a  $p$ -group of type  $p$  and so regular in the sense of P. Hall,  $N$  should be non-simple by a theorem of Wielandt.<sup>20</sup> If  $N_p$  were of type (5), the normalizer of  $S_p$  in  $N$  should be cyclic and so  $N$  should not be simple again by a theorem of Burnside. Hence  $q$  must divide the order of  $N$ .

Take then the normalizer  $N_q$  of  $S$  in  $G$ .  $N_q$  is solvable by theorem 5.  $N_q$  is clearly neither of types (4) and (7) in theorem 5, nor of types (6) and (6)\* by theorem 6. If  $N_q$  were of types (1) or (5) in theorem 5,  $S$  should be cyclic and be contained in the center of  $N_q$  so that  $N$  should be non-simple by a theorem of Burnside. If  $N_q$  were a  $q$ -group of type  $q$ , the  $q$ -factor-commutator group of  $G$  should be isomorphic to that of  $S$  by a theorem of Wielandt. This leads us to a contradiction. Hence  $N_q$  is a dihedral group which implies that  $q=2$ . q.e.d.

§ 4. The structure of non-solvable, non-simple c.d. groups

In this paragraph we shall determine the structure of non-solvable, non-simple c.d. groups. Let  $G$  be such a group, and  $N$  be its minimal normal subgroup. These notations will be fixed throughout this paragraph.

By theorem 8 we have

$$(1) \quad (G : N) = 2.$$

Let  $S$  be one of the 2-Sylow subgroups of  $G$ . Then the proof of theorem 8 shows that  $S$  is a dihedral group. By a theorem of Grün<sup>21</sup> we have  $G/N \cong S / (N(S)' \cap S) \amalg_{t \in G} (S \cap S'^t)$ , where  $N(S)$  is the normalizer of  $S$  in  $G$ ,  $S'$  is the conjugate subgroup  $tSt^{-1}$  ( $t \in G$ ) of  $S$  and the accent means the commutator subgroup. We shall hereafter use the notation such as  $S^t$  in the sense of  $tSt^{-1}$ , and  $N(S)$  and the accent are used in the sense of the normalizer in  $G$  and the commutator subgroup respectively. Now since  $N(S)$  is c.d.,  $N(S)$  coincides with  $S$  and therefore we have  $G/N \cong S/S' \amalg_{t \in G} (S \cap S'^t)$ . By the structure of  $S$ ,  $S'$  is a cyclic subgroup whose index  $(S : S')$  is 4, and hence  $S'$  is the intersection of all the maximal subgroups of  $S$ . So the index of  $T = \amalg_{t \in G} (S \cap S'^t)$  in  $S$  is 2, and

(20) Cf. (14).

(21) O. Grün, Crelle **174** (1935), or Zassenhaus [5], p. 134.

$T$  is not cyclic. Hence the maximal intersections of two distinct 2-Sylow subgroups are not equal to  $e$ . Take one of these maximal intersections  $D$ , and its normalizer  $N(D)$  in  $G$ . Then  $N(D)$  contains a self-conjugate group, but its 2-Sylow subgroups are not self-conjugate. By theorem 5  $N(D)$  is either a dihedral group or the symmetric group of four letters  $\mathfrak{S}_4$ .  $G$  is not 2-normal<sup>(22)</sup> by a theorem of Grün, so there is at least one intersection  $D$  which is not cyclic by a theorem of Burnside<sup>(23)</sup>. For such non-cyclic a intersection  $D$ , we have  $N(D) \cong \mathfrak{S}_4$ .

$S$  has one maximal dihedral subgroup  $T^*$  other than  $T$ . Every element of order 2 in  $T$  is conjugate to each other in  $G$ . On the other hand, if we take two elements  $a, b$  order 2 contained in  $T^*$  but not in  $T$ ,  $a$  is conjugate to  $b$  in  $G$  but is not conjugate to any element of order 2 in  $T$ . For otherwise we should have  $S=T$ . Let  $z$  be the center of  $S$ ,  $N_1$  the centralizer of  $z$  in  $G$ , and  $N_2$  the centralizer of  $a$  in  $G$ . Then both  $N_1$  and  $N_2$  are dihedral groups, and they are not conjugate in  $G$ .  $N_i$  ( $i=1,2$ ) has a cyclic subgroup  $Z_i$  of index 2. Let now  $Z$  be a maximal cyclic subgroup of an even order, and  $U$  the 2-Sylow subgroup of  $Z$ . Then  $U$  is contained in some 2-Sylow subgroup  $S^*$  and so  $U$  is conjugate to some subgroup of  $S$  in  $G$ . This implies that  $Z$  is conjugate to  $Z_1$  or  $Z_2$  in  $G$ .

Now we shall prove the following lemma.

**Lemma 7.** *Two distinct  $p$ -Sylow subgroup  $S$  and  $S^*$  have no element in common except the unit element, when  $p > 2$ .*

*Proof.* We shall assume that  $S \cap S^* \neq e$  and  $S \neq S^*$ , and prove that  $p=2$ . Put  $S \cap S^* = D$ . We shall assume that  $D$  is the maximal intersection of  $p$ -Sylow subgroups. Theorem 5 shows that  $N(D)$  is solvable and is a group of type (3), (4) or (7) in theorem 5. If  $N(D)$  is a dihedral group or  $\mathfrak{S}_4$ , then we have  $p=2$ . We may, therefore, assume that  $N(D)$  is a group of type (4):  $N(D) = G_1 \times G_2$ , where  $G_1$  is of order  $p$  and  $G_2 = PZ$  ( $P$  is of order  $p$  and  $Z$  is a self-conjugate cyclic subgroup of  $G_2$ ). Then we have  $D = G_1$  and  $D \cup Z = V$  is a maximal cyclic subgroup of  $G$ . Take any prime factor  $q$  of the order of  $Z$ , and let  $Z_q$  be the  $q$ -Sylow subgroup of  $Z$ . Since  $V$  is a maximal cyclic subgroup of  $G$ ,  $Z_q$  is a  $q$ -Sylow subgroup of  $G$ . Any element of  $N(Z_q)$  fixes  $Z_q$  (i.e. transforms  $Z_q$  into itself), so also  $V$ . This implies that any element of  $N(Z_q)$  fixes  $D$  too, and  $N(Z_q) \subseteq N(D)$ . Hence we have  $N(Z_q) = N(D)$ . On the other hand

(22) Cf. O. Grün loc. cit. (21), or Zassenhaus [5], p. 135

(23) Zassenhaus [5], p. 103.

we have  $N(Z_q)N=G$ , as  $Z_q$  is a  $q$ -Sylow subgroup of  $G$  and a fortiori of  $N$ . Hence the index  $(N(Z_q):N(Z_q)')$  is divisible by 2. Since  $(N(Z_q):N(Z_q)')=p^2$ , we must have  $p=2$ . This proves our lemma 7.

Now we shall return to our  $N_1, N_2, Z_1$  or  $Z_2$ , and put

$$\begin{aligned} (G : N_1) &= m_1 & \text{and} & & (N_1 : e) &= 2n_1, \\ (G : N_2) &= m_2 & \text{and} & & (N_2 : e) &= 2n_2. \end{aligned}$$

Then it holds

$$(2) \quad (G : e) = g = 2n_1 m_1 = 2n_2 m_2.$$

As  $G$  is c.d., the number of elements, other than  $e$ , which are conjugate to some element of  $N_i$  in  $G$ , is  $m_i(n_i-1)$ .

Let  $S_p$  be any  $p$ -Sylow subgroup of  $G$  ( $p > 2$ ). Suppose first that  $S_p$  is not cyclic. Then we shall denote the normalizer of  $S_p$  by  $N_p$ , and put

$$(G : N_p) = m_p, \quad (N_p : S_p) = l_p \quad \text{and} \quad (S_p : e) = n_p,$$

where  $p$  runs through prime factors of  $G$  such that  $S_p$  are not cyclic. Then we have

$$(3) \quad g = m_p l_p n_p,$$

and by lemma 7 the number of elements other than  $e$ , contained in some  $p$ -Sylow subgroups of  $G$ , is  $m_p(n_p-1)$ . If  $S_p$  is cyclic, we shall take the maximal cyclic subgroup  $Z$  containing  $S_p$ . Consider now maximal cyclic subgroups of odd orders of  $G$  each of which contains some Sylow subgroup of  $G$ . Some of them may be conjugate in  $G$ . We take now a representative  $Z_\alpha$  from each conjugate class of these groups. Let  $Z_\alpha, \alpha \in A$ , be all these representatives. For any  $\alpha \in A$  we shall put

$$(G : N_\alpha) = m_\alpha, \quad (N_\alpha : Z_\alpha) = l_\alpha \quad \text{and} \quad (Z_\alpha : e) = n_\alpha,$$

where  $N_\alpha = N(Z_\alpha)$ . Then we have

$$(4) \quad g = m_\alpha l_\alpha n_\alpha \quad (\alpha \in A),$$

and the number of elements, other than  $e$ , which are conjugate to some element of  $Z_\alpha$ , is clearly  $m_\alpha(n_\alpha-1)$ .

We shall now decompose the set of all prime factors of the order of  $G$  into two classes  $\Pi_1$  and  $\Pi_2$ , where  $\Pi_1$  consists of all the odd prime

factors  $p$  such that  $S_p$ ,  $p$ -Sylow subgroup of  $G$ , is not cyclic and  $\Pi_2$  consists of all other prime factors. Then  $G$  has no element of order  $p_1 d$ , where  $p_1 \in \Pi_1$  and  $d > 1$ . For, if  $G$  had an element  $a$  of order  $p_1 d$ , the maximal intersection of  $p_1$ -Sylow subgroups should not be equal to  $e$ , as the normalizer of  $\{a^d\}$  should be a group of type  $D$ .

Take any maximal cyclic subgroup  $Z$  of  $G$ . If  $Z$  is of an even order,  $Z$  is conjugate to  $Z_1$  or  $Z_2$  in  $G$  as proved above. We shall now assume that  $Z$  is an odd order. If  $Z$  contains some Sylow subgroup of  $G$ ,  $Z$  is conjugate to some  $Z_\alpha$  ( $\alpha \in A$ ). Suppose now  $Z$  contains no Sylow subgroup of  $G$ . If we take a prime factor  $p$  of the order of  $Z$ ,  $p$ -Sylow subgroups of  $G$  are not cyclic, so  $p \in \Pi_1$ . Hence  $Z$  is of order  $p$  and is contained in some  $p$ -Sylow subgroup of  $G$ . Hence we have

$$(5) \quad g = 1 + m_1(n_1 - 1) + m_2(n_2 - 1) + \sum_{\gamma} m_{\gamma}(n_{\gamma} - 1),$$

where  $\gamma$  runs through the domain  $\Gamma = A + \Pi_1$ . By (2) of this paragraph, (5) is written in the form

$$(6) \quad m_1 + m_2 - 1 = \sum_{\gamma} m_{\gamma}(n_{\gamma} - 1).$$

$G$  has clearly  $m_1 + m_2$  elements of order 2. We shall now count the number of pairs of two elements of order 2. This number is clearly  $\frac{1}{2}(m_1 + m_2)(m_1 + m_2 - 1)$ . On the other hand, such a pair of elements generates a dihedral subgroup of  $G$ . Hence we shall be able to count this number in another way, i.e. by the enumeration of dihedral subgroups of  $G$ .

We shall first prove the following lemma.

**Lemma 8.** *In the same notations as above, any dihedral subgroup  $D$  of  $G$  is contained in some conjugate subgroup  $H$  of  $N_1$ ,  $N_2$ ,  $N_p$  or  $N_\alpha$ . If the order of  $D$  is greater than 4, this conjugate subgroup  $H$  is uniquely determined by  $D$ .*

*Proof.* Let  $D$  be any dihedral subgroup of  $G$ . Then  $D$  has a cyclic subgroup  $Z$  of index 2. If  $Z$  is contained in a maximal cyclic subgroup of an even order,  $Z$  is conjugate to some subgroup of  $Z_1$  or  $Z_2$  in  $G$ . Hence  $D$  is contained in some conjugate subgroup of  $N_1$  or  $N_2$ . If the order of  $Z$  is greater than 2, this conjugate subgroup of  $N_i$  containing  $D$  is nothing but the normalizer  $N(Z)$  and is uniquely determined by  $D$ . Let now  $Z^*$  be the maximal cyclic subgroup of  $G$  containing  $Z$ , and let its order be odd. If  $Z^*$  contains some Sylow subgroup of  $G$ ,  $Z^*$  is conjugate to some  $Z_\alpha$ . Hence  $D$  is contained in some conjugate subgroup of  $N_\alpha$ , which is



again the normalizer of  $Z$ . If  $Z^*$  contains no Sylow subgroup of  $G$ ,  $Z^*$  is of order  $p$  and is contained in some  $p$ -Sylow subgroup. As  $p$  belongs clearly to  $\Pi_1$ ,  $D$  is contained in some conjugate subgroup  $H$  of  $N_p$ . By lemma 7  $H$  is again uniquely determined by  $D$ . This completes the proof.

Now we shall enumerate the number of pairs of elements of order 2 of  $G$  in the following manner.

a) Denote by  $K_\gamma$  the number of pairs of elements, which generate dihedral subgroups of some conjugate subgroup of  $N_\gamma$  ( $\gamma \in \Gamma$ ). Then since  $N_\gamma$  ( $\gamma \in \Gamma$ ) is the normalizer of some Sylow subgroup of  $G$ , we have  $G = NN_\gamma$  ( $\gamma \in \Gamma$ ). Hence by (1) of this paragraph the order of  $N_\gamma$  is even. As the order of  $S_p$  or  $Z_\alpha$  is odd, we have then

$$(7) \quad l_\gamma \equiv 0 \pmod{2} \quad (\gamma \in \Gamma).$$

Each  $N_\gamma$  contains  $n_\gamma$  elements of order 2, so the number of pairs, generating dihedral subgroups of  $N_\gamma$  is  $\frac{1}{2}n_\gamma(n_\gamma - 1)$ .  $N_\gamma$  has  $m_\gamma$  conjugate subgroups in  $G$  and no pair of these  $m_\gamma$  conjugate subgroups of  $N_\gamma$  has a dihedral subgroup in common by lemma 8. Hence we see that

$$K_\gamma = \frac{1}{2} m_\gamma n_\gamma (n_\gamma - 1) \quad (\gamma \in \Gamma).$$

b) Next denote by  $K_1$  the number of pairs, generating dihedral subgroups of  $N_1$  and whose orders are greater than 4.  $N_1$  has  $1 + n_1$  elements of order 2, one of which, say  $a$ , is contained in the center of  $N_1$ . For any  $b$  in  $N_1$ , the pair  $(a, b)$  generates a group of order 4 if  $a \neq b$ . Hence the number of pairs, generating dihedral subgroups of  $N_1$  whose orders are greater than 4, is  $\frac{1}{2}n_1(n_1 - 2)$ . Since  $N_1$  has  $m_1$  conjugate subgroups, we conclude that

$$K_1 = \frac{1}{2} m_1 n_1 (n_1 - 2).$$

c) Similarly the number  $K_2$  of pairs, generating dihedral subgroups which are conjugate to some subgroup of  $N_2$  and whose orders are greater than 4, is  $\frac{1}{2}m_2n_2(n_2 - 2)$ .

d) Finally we consider the number  $K_0$  of pairs which generate abelian groups of order 4 and of type (1,1). Let  $S$  be again one of 2-Sylow subgroups of  $G$ , and put  $T = \Pi_{\hat{e}G}(S \cap S')$ . Then  $T$  is a dihedral subgroup of index 2.  $S$  has another maximal dihedral subgroup, which we shall denote by  $T^*$ . Take abelian subgroups  $U$  and  $U^*$  of order 4 and

of type (1, 1) in  $T$  and  $T^*$  respectively. Then any non-cyclic abelian subgroup of order 4 of  $S$  is conjugate to  $U$  or  $U^*$  in  $S$ , but  $U$  and  $U^*$  are not conjugate *even in*  $G$ . For if  $U$  were conjugate to  $U^*$  in  $G$ ,  $T$  should be equal to  $S$  against (1) of this paragraph<sup>(24)</sup>. Since any non-cyclic abelian subgroup of order 4 is conjugate to some subgroup of  $S$ , all such subgroups of  $G$  are distributed into two conjugate classes  $\mathbf{C}$  and  $\mathbf{C}^*$ . We may assume that  $U \in \mathbf{C}$  and  $U^* \in \mathbf{C}^*$ . We shall now count the number of subgroups contained in  $\mathbf{C}$  and  $\mathbf{C}^*$ . Since two arbitrary subgroups of order 2 in  $U$  are conjugate in  $G$ ,  $U$  is contained in at least two distinct 2-Sylow subgroups of  $G$ , and so its normalizer is isomorphic to  $\mathfrak{S}_4$ : the symmetric group of four letters. Hence the number of conjugate subgroups of  $U$  is  $g/24$ . On the other hand,  $U^*$  is contained in one 2-Sylow subgroup of  $G$ . So the normalizer of  $U^*$  is a dihedral group of order 8 and the number of subgroups in  $\mathbf{C}^*$  is  $g/8$ . Hence  $G$  contains  $(g/24 + g/8) = g/6$  abelian, non-cyclic subgroups of order 4. Therefore, the number  $K_0$  is clearly equal to  $3 \times g/6 = g/2$ .

By lemma 8  $K_0 + K_1 + K_2 + \sum_{\tau} K_{\tau}$  is clearly the total number of pairs of elements of order 2; that is

$$(8) \quad (1/2)(m_1 + m_2)(m_1 + m_2 - 1) = (g/2) + (1/2)m_1n_1(n_1 - 2) \\ + (1/2)m_2n_2(n_2 - 2) + \sum_{\tau \in \Gamma} (1/2)m_{\tau}n_{\tau}(n_{\tau} - 1).$$

By (2),  $m_1n_1 = m_2n_2 = g/2$ , then (8) gives

$$(m_1 + m_2)(m_1 + m_2 - 1) = (g/2)(n_1 + n_2) - g + \sum_{\tau} m_{\tau}n_{\tau}(n_{\tau} - 1).$$

Dividing both side by  $g$  and using (3) and (4), we have

$$(9) \quad (m_1 + m_2) \left( \frac{m_1 + m_2 - 1}{g} \right) = \frac{n_1 + n_2}{2} - 1 + \sum_{\tau} \frac{n_{\tau} - 1}{l_{\tau}}.$$

On the other hand, we obtain by (6) the following formula.

$$\frac{m_1 + m_2 - 1}{g} = \sum_{\tau \in \Gamma} \frac{n_{\tau} - 1}{n_{\tau}l_{\tau}}$$

Hence we have

---

(24) Cf. a theorem of Grün, loc. cit. (21).

$$(m_1 + m_2) \left( \sum_{\gamma} \frac{n_{\gamma} - 1}{n_{\gamma} l_{\gamma}} \right) = \frac{n_1 + n_2}{2} - 1 + \sum_{\gamma} \frac{n_{\gamma} - 1}{l_{\gamma}},$$

$$\sum_{\gamma} \frac{m_1 + m_2}{n_{\gamma}} \frac{n_{\gamma} - 1}{l_{\gamma}} = \frac{n_1 + n_2}{2} - 1 + \sum_{\gamma} \frac{n_{\gamma} - 1}{l_{\gamma}},$$

or

$$(10) \quad \sum_{\gamma} \left( \frac{m_1 + m_2}{n_{\gamma}} - 1 \right) \cdot \frac{n_{\gamma} - 1}{l_{\gamma}} = \frac{n_1 + n_2}{2} - 1.$$

By the definition of  $\Gamma$ , it holds clearly  $g = n_1 n_2 \prod_{\gamma \in \Gamma} n_{\gamma}$ . Put now  $g = n_1 n_2 n_{\gamma} k_{\gamma}$ , then

$$m_1 = \frac{1}{2} n_2 n_{\gamma} k_{\gamma} \quad \text{and} \quad m_2 = \frac{1}{2} n_1 n_{\gamma} k_{\gamma}.$$

So we see

$$(11) \quad \frac{m_1 + m_2}{n_{\gamma}} = \frac{n_1 + n_2}{2} k_{\gamma}, \quad (\gamma \in \Gamma).$$

By the structure of  $N_{\gamma}$  we have

$$(12) \quad n_{\gamma} \equiv 1 \pmod{l_{\gamma}} \quad (\gamma \in \Gamma).$$

Now (10) and (11) give

$$(13) \quad \sum_{\gamma} \left( \frac{n_1 + n_2}{2} k_{\gamma} - 1 \right) \frac{n_{\gamma} - 1}{l_{\gamma}} = \frac{n_1 + n_2}{2} - 1.$$

Taking (12) into consideration, (13) implies that  $\Gamma$  consists of only one suffix  $\gamma$  and  $k_{\gamma} = 1$ ,  $n_{\gamma} - 1 = l_{\gamma}$ . We shall now write  $N$ ,  $n$  or  $l$  instead of  $N_{\gamma}$ ,  $n_{\gamma}$  or  $l_{\gamma}$ . Then we have

$$(14) \quad n = l + 1$$

and

$$(15) \quad g = n_1 n_2 n.$$

Moreover (6) is written in the form

$$\frac{1}{2} n_2 n + \frac{1}{2} n_1 n - 1 = \frac{1}{l} n_1 n_2 (n - 1),$$

or

$$(16) \quad n_1 n + n_2 n = 2 + 2n_1 n_2.$$

Now  $G$  contains an element of order  $l$ . Since  $l \equiv 0 \pmod{2}$  by (7),  $l$  must divide either  $n_1$  or  $n_2$ . In the following we may assume, in choosing suitable notations, that  $l$  divides  $n_1$ , i.e. we shall put

$$(17) \quad n_1 = ls, \quad (s: \text{integer}, > 0).$$

(16) gives then  $n_2 \equiv 2 \pmod{l}$ , or

$$(18) \quad n_2 = lt + 2, \quad (t: \text{integer}, > 0).^{25)}$$

From (14), (16), (17) and (18) we obtain

$$ls(l+1) + (lt+2)(l+1) = 2 + 2ls(lt+2),$$

or

$$ls + lt + 2 + t = 2lst + 3s.$$

Hence

$$\begin{aligned} \frac{1}{t} + \frac{1}{s} + \frac{2}{lst} + \frac{1}{ls} &= 2 + \frac{3}{tl}, \\ \frac{1}{t} + \frac{1}{s} + \frac{1}{ls} &= 2 + \frac{2}{lt} \left(1 - \frac{1}{s}\right) + \frac{1}{lt}. \end{aligned}$$

Since  $s \geq 1$ , it holds

$$(19) \quad \frac{1}{t} + \frac{1}{s} + \frac{1}{ls} > 2.$$

On the other hand, we have  $l \geq 2$  by (7). Hence (19) implies

$$(20) \quad s = t = 1.$$

Thus we conclude that  $n_1 = l = n - 1$  and  $n_2 = l + 2 = n + 1$ .

$G$  is now representable as a transitive permutation group on the cosets mod  $N$ . Since  $N$  is of index  $n+1$ , the degree of this permutation group  $G_N$  is  $n+1$ .  $N$  contains a subgroup  $H$  of order  $n$ . ( $H$  was written as  $S_p$

---

(25) If  $t=0$ , an easy computation shows that the order  $g$  of  $G$  is 24, so that  $G$  is solvable.

or  $Z_a$  in our old notations). Clearly any conjugate subgroup of  $N$  except  $N$  has no element, other than  $e$ , in common with  $H$ . So  $G_N$  is doubly transitive. Since  $(l, n) = 1$ ,  $N$  contains a cyclic subgroup  $Z$  of order  $l$  such that  $N = HZ$ .  $Z$  is conjugate to  $Z_1$  or  $Z_2$  in the old notations, and so is contained in two distinct conjugate subgroups of  $N$ . Hence  $Z$  consists of elements of  $G_N$  which fix two letters of the permutation. Since the order  $l$  of  $Z$  is  $n-1$  and any pair of conjugate subgroups of  $Z$  has no element in common other than  $e$ ,  $G_N$  must be triply transitive and all elements of  $G_N$  except  $e$  fix at most two letters. Hence by the method of Zassenhaus<sup>26)</sup> we can construct the "almost field" (Fastkörper)  $F$  corresponding to  $N$ . In our case  $Z$  is of order  $n-1$ , so every element of  $F$  other than 0 has its inverse, i.e.  $F$  is complete (vollständig), and is surely a field, since  $Z$  is cyclic. Hence  $F$  is a finite field with  $n$  elements, and  $G_N$  is isomorphic to the full linear fractional group of one variable over  $F$ . Since  $n-1 \equiv 0 \pmod{2}$  by (7), the characteristic of  $F$  is greater than 2. Thus we have proved the following theorem.

**Theorem 9.** *Let  $G$  be a non-solvable, non-simple c.d. group. Then  $G$  is isomorphic to the full linear fractional group of one variable over a finite field whose characteristic is greater than 2.*

Conversely we can easily prove that the full linear fractional group of one variable over a finite field  $F$  is always c.d., and it is non-solvable when  $F$  has at least four elements. Moreover it is non-simple if the characteristic of  $F$  is greater than 2.

Mathematical Institute,  
Tokyo University.

### Bibliography :

- [1] Kontorovitch P. Sur la representation d'un groupe fini sous la forme d'une somme directe de sous-groupes, I. Rec. Math. (Mat. Sbornik) **5** (47) (1939) p. 283-296;
- [2] II; Rec. Math. (Mat. sbornik) **7** (49) (1940) p. 27-33.
- [3] Zassenhaus H. Kennzeichnung endlicher linearer Gruppen als Permutationsgruppe Hamb. Abh. **11**. (1936) s. 17-40.
- [4] Zassenhaus H. Ueber endliche Fastkörper, Hamb. Abh. **11** (1936) s. 187-220.
- [5] Zassenhaus H. Lehrbuch der Gruppentheorie I. (1937).

---

(26) Zassenhaus [3].