ABSTRACT

This thesis is concerned with finite p-groups, in particular, 2-groups. Section 3 gives two definitions of a p-group; their equivalence is proved when the group in concern is of finite order. The existence of Sylow p-subgroups of a finite group is proved. Some consequences of this theorem are given. The properties of p-groups are discussed. The Frattini subgroup of a p-group is studied; this subgroup is shown to be closely related with the Burnside's basis theorem. Section 7 shows how the Burnside's basis theorem may be applied in obtaining a limitation for the order of automorphism group Aut(G) of a p-group G. More theorems regarding the limitation for the order of Aut(G) are obtained. The structure of 2-groups is discussed. Immediately after this discussion, the groups in concern are classified into Abelian and non-Abelian using a method suggested by Burnside [1]. Other methods used for classification of 2-groups are described. The relation between the orders of 2-groups and their class numbers are discussed. In particular, the class numbers of the dihedral, generalized quaternion, and semi-dihedral groups are obtained. The properties of elementary Abelian 2-groups are given. The dihedral and quaternion groups are compared.

p-GROUPS, IN PARTICULAR, 2-GROUPS

by

Rosario Y. Tan

A thesis submitted to the Faculty of
Graduate Studies and Research in partial fulfilment
of the requirements for the degree of Master of Science.

Department of Mathematics,
McGill University,
Montreal.

February 1969

ACKNOWLEDGEMENT

I would like to thank Professor H. Schwerdtfeger for suggesting the topic as well as his helpful criticism and supervision of my work during the year.

CONTENTS

p-GROUPS, IN PARTICULAR, 2-GROUPS

1. Introduction.

Lagrange's theorem states that in a finite group G of order n, the order of every subgroup of G is a divisor of n. On the other hand, there need not be a subgroup of order m for every divisor m of n. For example, the alternating group A_4 of degree 4 contains no subgroup of order 6 although 6 divides 12 which is the order of A_4. However it is true that when p is a prime divisor of n, then G contains a subgroup of order p. This theorem was first observed by Cauchy. It was extended later by the Norwegian mathematician L. Sylow to that " G contains a subgroup H of order p^m if p^m is the highest power of a prime p dividing n". Such a subgroup H is thus called a Sylow p-subgroup. Sylow proved further that the number of Sylow p-subgroups is $\equiv 1 \pmod{p}$, and that all Sylow p-subgroups are conjugate. Combining the Sylow theorems with Lagrange's theorem, it follows that every group must arise from those groups whose orders are powers of prime numbers dividing the order of the group. The study of groups of arbitrary orders is thus shifted to those groups whose orders are powers of prime numbers, also called prime-power groups or simply p-groups.

The object of this thesis is to give an account on p-groups with illustration on 2-groups. In studying these p-groups more closely, it will be shown that 2-groups possess more interesting properties than other classes of p-groups.

2. Notation.

$\langle x, y, \ldots \mid * \rangle$	..... the group generated by x, y, ... operating under the relations *.
$Z(G) = Z$	..... the center of G .
J	..... the set of all integers.
J^+	..... the set of all integers $j > 0$.
S_n	..... the symmetric group of degree n.
A_n	..... the alternating group of degree n.
$\mid G \mid$	..... the number of elements in G , or the order of G.
$\phi(G)$	..... the Frattini subgroup of G.
$[G:H]$	..... the index of H in G.
$[G,H]$	..... the group generated by $[a,b]$ such that $a \in G$ and $b \in H$.

For elements x and y of a group G,

$[x,y]$	..... $x^{-1}y^{-1}xy$.
$\mid x \mid$	..... the order of x.
$Cl(x)$	..... the class of x.

$C(x)$ ..... the centralizer of x.

$N(x)$ ..... the normalizer of x.

Further notation is standard. (See Scott [1], p 471-474)

3. Definition.

We start by giving two definitions of p-groups. Early writers (Miller [1], P. Hall [1], Burnside [1]) defined p-groups as

Definition 1. A p-group is a group whose order is a power of the prime p.

Later writers (M. Hall [1], Scott [1]) defined p-groups as

Definition 2. A p-group is a group all of whose elements have orders a power of the prime p.

The main difference between these two definitions is that in definition (1), the group in concern is clearly finite. Whereas in definition (2), the group in concern may be either finite or infinite. However, when the group is finite, the two definitions of p-groups are equivalent. We proceed to prove this.

Definition (1) $\Rightarrow$ Definition (2).

Let G be a group of order p^m, and let a be any element of G. Then by Lagrange's theorem, $|a| \mid p^m$. Since

p is a prime, we must have $|a| = p^r$ with $r \leq m$. Therefore G is a p-group in the sense of definition (2).

Definition (2) $\Longrightarrow$ Definition (1).

Let $|G| = n$, and suppose that $q \neq p$ is a prime divisor of n. Then by Cauchy's theorem, G contains an element x of order q. But this is a contradiction. Therefore $n = p^m$ for some natural number m, and G is a p-group in the sense of definition (1).

Q.E.D.

In this thesis, we shall confine our attention to definition (1).

4. Sylow Theorems.

As we noted in the introduction, the discovery of Sylow p-subgroups results in the study of p-groups. It is to be expected then that many properties of p-groups are consequences of the Sylow theorems. In this section, we shall prove these theorems, and from these we shall draw some consequences.

Theorem 4.1. (First Sylow theorem) If G is a group of order $p^r s$, p and s need not be relatively prime, then G contains a subgroup of order p^r.

Proof. We prove by induction on $|G|$. The theorem

is trivial when $s = 1$. We may therefore assume that $s > 1$. For $a \in G$, we consider $|Cl(a)|$. If $|Cl(a)| = 1$ for all $a \in G$, then G is Abelian. Hence G contains an element x of order p (Ledermann [1], p 126), and the group $G/\langle x\rangle$ is of order $p^{r-1}s$. Therefore by inductive hypothesis, $G/\langle x\rangle$ contains a subgroup $H/\langle x\rangle$ of order p^{r-1}, and by the lattice theorem (Scott [1], p 27), the corresponding subgroup H of G is of order p^r. We may therefore assume that $|Cl(a)| = h_a > 1$ for at least one a of G. If $(h_a,p) = 1$, then since $|G| = |Cl(a)|\,|N(a)|$, it follows that $p^r \mid |N(a)|$. Therefore by inductive hypothesis, $N(a)$ contains a subgroup H of order p^r. In any other possibility for h_a, we have $p \mid h_a$ for all $a \in G$ for which $|Cl(a)| = h_a > 1$. Then from the class equation of G, $p \mid |Z|$. Therefore Z contains an element z of order p. The group $G/\langle z\rangle$ is of order $p^{r-1}s$; so by the induction assumption, it contains a subgroup $K/\langle z\rangle$ of order p^{r-1}, and the corresponding subgroup K of G is of order p^r. This completes the proof.

Q.E.D.

Two consequences of this theorem are

Corollary 4.2. If p^m is the highest power of the prime p dividing the order of G, then G contains a subgroup of order p^m.

Corollary 4.3. (Cauchy's theorem) If G is a finite

group whose order is divisible by a prime p, then G contains a subgroup of order p.

Theorem 4.4. (Second and third Sylow theorems) Let G be a group of order $p^m s$, $(p,s) = 1$. Then the number of Sylow p-subgroups is $\equiv 1 \pmod{p}$ and is a divisor of s; all Sylow p-subgroups are conjugate.

Proof. Let K and H be any Sylow p-subgroups of G. We define an equivalence relation on Cl(K) as follows: For a subgroup $A \in Cl(K)$, a subgroup $B \in Cl(A)$ iff there exists $h \in H$ such that $B = h^{-1}Ah$. This is an equivalence relation. First, $A \in Cl(A)$ for all $A \in Cl(K)$. Next if $B \in Cl(A)$ so that $B = h^{-1}Ah$, where $h \in H$. Then $A = hBh^{-1}$, and so $A \in Cl(B)$. Finally if $B \in Cl(A)$ and $A \in Cl(D)$, so that $B = h_1^{-1}Ah_1$, and $A = h_2^{-1}Dh_2$ for some $h_1, h_2 \in H$. Then $B = (h_2h_1)^{-1}D(h_2h_1)$ which implies that $B \in Cl(D)$. The equivalence classes under this equivalence relation consist of subgroups which are conjugate under transformation by elements of H. If $A \neq H$, then $|Cl(A)| = [H:H \cap N(A)] > 1$. Since H is a p-group, it follows that $p \mid |Cl(A)|$ if $A \neq H$, and obviously $|Cl(H)| = 1$ if $H \in Cl(K)$. Thus we have

$$|Cl(K)| \equiv \begin{cases} 0 \pmod{p} & \text{if } H \notin Cl(K), \\ 1 \pmod{p} & \text{if } H \in Cl(K). \end{cases}$$

The case where $H \notin Cl(K)$ cannot arise, since $H = K$ shows that $|Cl(K)| \equiv 1 \pmod{p}$. Therefore $H \in Cl(K)$ and the

number of Sylow p-subgroups is of the form $1 + kp$, $k \in J_0^+$. Now $1 + kp \nmid p^m$; on the other hand, $1 + kp \mid p^m s$, hence $1 + kp \mid s$. This completes the proof.

Q.E.D.

Corollary 4.5. Let S_p be a Sylow p-subgroup of a group G. Then S_p is the only Sylow p-subgroup of G iff it is normal in G.

Proof. Let S_p' be any Sylow p-subgroup of G. Then by the Sylow theorem, $S_p' = x^{-1}S_p x$ for some $x \in G$. But since $S_p = x^{-1}S_p x$ for all $x \in G$, hence $S_p = S_p'$; i.e., S_p is unique. Conversely, suppose that S_p is not normal in G. Then $S_p = x^{-1}S_p x$ for some $x \in G$. Now by the Sylow theorem, $x^{-1}S_p x = S_p'$ is a Sylow p-subgroup which is distinct from S_p. Therefore S_p is not unique, a contradiction.

Q.E.D.

Two interesting theorems regarding a Sylow p-subgroup and its normalizer are

Theorem 4.6. Let S_p be a Sylow p-subgroup of a group G, $N(S_p)$ the normalizer of S_p, and let H be any subgroup of G such that $N(S_p) \subseteq H$. Then $H = N(H)$.

Proof. It suffices to show that $N(H) \subseteq H$. Suppose that $n \in N(H)$ so that $n^{-1}Hn = H$. Since $N(S_p) \subseteq H$, and since all Sylow p-subgroups are conjugate, $n^{-1}S_p n = h^{-1}S_p h$ for some $h \in H$. Hence $hn^{-1}S_p = S_p hn^{-1}$, which implies that

$hn^{-1} \in N(S_p) \subseteq H$. Therefore $n \in H$.

Q.E.D.

Theorem 4.7. Let G be a group of order $p^m s$, $(p,s) = 1$, and let H be a p-subgroup but not a Sylow p-subgroup of G. Then H is a proper subgroup of its normalizer.

Proof. The theorem is obvious if $p \nmid |Cl(H)|$, since then $p^m \mid |N(H)|$, and so $N(H)$ contains a Sylow p-subgroup S_p with $|S_p| > |H|$. Therefore there exists an element $x \in S_p \subseteq N(H)$ with $x^{-1}Hx = H$ and $x \notin H$; i.e., $H \subset N(H)$. On the other hand, if $|Cl(H)| = pk$, $k \in J$, then H transforms the pk subgroups conjugate to H in systems of transitivity whose degree are 1 or numbers divisible by p. Since H is conjugate to itself, there are at least p subgroups conjugate to H which are transformed into themselves by H. Therefore $H \subset N(H)$.

Q.E.D.

As a consequence of this, we have

Corollary 4.8. Let G be a p-group of order p^m, and H a maximal subgroup of G. Then H is normal in G.

Proof. Since H is not a Sylow p-subgroup, $H \subset N(H) \subseteq G$ (Theorem 4.7). But H is a maximal subgroup of G. Therefore we must have $N(H) = G$ and so H is normal in G.

Q.E.D.

Further properties of p-groups will be given in the following section.

5. Properties of p-Groups.

Notation: In this section, G will always stand for a p-group.

Theorem 5.1. G contains at least one self-conjugate element of order p.

Proof. Suppose that $|G| = p^m$. Then from the class equation of G, we have

$$p^m = |Z| + \sum\{|Cl(x)| \mid x \in S\},$$

where S is some subset of G. Since $p \mid |Cl(x)|$ for each $x \in S$, $p \mid |Z|$. Therefore Z, and hence G contains a self-conjugate element of order p.

Q.E.D.

This theorem does not apply to infinite p-groups (in the sense of definition (2), See Scott [1], p 216).

Theorem 5.2. Every proper normal subgroup H of G contains at least one self-conjugate element of G which is of order p.

Proof. Since H is a subgroup of G, there is a subset T of H such that the class equation of H is

$$|H| = |Z \cap H| + \sum\{|Cl(x)| \mid x \in T\}.$$

By assumption, H is normal in G. Hence $|Cl(x)| = [G:C(x)]$ which is divisible by p; and since H is a p-group, it follows

that $p \mid |Z \cap H|$. Therefore H contains at least one self-conjugate element of G which is of order p.

Q.E.D.

Theorem 5.3. If K is a normal subgroup of G, and $|K| = p$, then K is contained in the center Z.

Proof. By Theorem 5.2, $Z \cap K \neq E$, and $Z \cap K \subseteq K$. But since $|K| = p$, which implies that K contains no proper subgroup. Therefore $K = Z \cap K \subseteq Z$ or $K \subseteq Z$.

Q.E.D.

Theorem 5.4. The commutator subgroup G' of G is contained in the Frattini subgroup $\phi(G)$ of G.

Proof. The Frattini subgroup of a group K is the intersection of all maximal subgroups of K. Now, let M be a maximal subgroup of G. Then the group G/M is of order p, and so it is cyclic. Since the commutator subgroup of a group is the smallest normal subgroup for which the factor group is Abelian (Schenkman [1] , p 76), it follows that $G' \subseteq M$ for every maximal subgroup M of G. Therefore $G' \subseteq \phi(G)$.

Q.E.D.

Theorem 5.5. The Frattini subgroup of G is the smallest normal subgroup for which the factor group is elementary Abelian.

Proof. An Abelian group with prime exponent p is

called elementary Abelian (Zassenhaus [1], p 142). $G/\Phi(G)$ is Abelian by Theorem 5.4. Now let M be any maximal subgroup of G. Then $x^p \in M$ for all $x \in G$. Since M is arbitrary, it follows that $x^p \in \Phi(G)$. Therefore $G/\Phi(G)$ contains no element of order p^2, and it must be of type $(1,1,\ldots,1)$; i.e., $G/\Phi(G)$ is elementary Abelian. Next suppose that N is a normal subgroup of G such that G/N is elementary Abelian. Then by a theorem of Dlab V. [1], $\Phi(G/N) = \cap(G/N)^p$, where p ranges over the prime divisors of the order of G/N. But since G/N is elementary Abelian, it follows that $\Phi(G/N) = \cap(G/N)^p = N$. Therefore $\Phi(G) \subseteq N$.

Q.E.D.

An immediate consequence of this is

Corollary 5.6. If G is elementary Abelian, then $\Phi(G) = E$.

Theorem 5.7. If G is non-cyclic, then the factor group G/G' cannot be cyclic.

Proof. We assume the contrary and let $G/G' = \langle G'x \rangle$ with $x \in G$. Then $G = G'\langle x \rangle$. Since $G' \subseteq \Phi(G)$ (Theorem 5.4), and since $\Phi(G)$ is the set of non-generators of G, (by this we mean that $\Phi(G)$ has the property that whenever K is a subgroup of G such that $G = \Phi(G)K$, then $G = K$. See M. Hall [1], p 156) hence $G = G'\langle x \rangle = \langle x \rangle$; this implies that G is cyclic which is a contradiction. Therefore the theorem is true.

Q.E.D.

Theorem 5.8. If G is non-Abelian of order p^m, then $|G'| \neq p^{m-1}$.

Proof. Suppose that $|G'| = p^{m-1}$. Then the group G/G' is of order p, hence it is cyclic. But this is impossible (Theorem 5.7). Therefore $|G'| \neq p^{m-1}$.

Q.E.D.

For the center Z of G, we have

Theorem 5.9. If G is non-Abelian of order p^m, then $|Z| \neq p^{m-1}$.

Proof. Here again we prove by the contrary and suppose that $|Z| = p^{m-1}$. Then G/Z is of order p, so it is cyclic. But then $G = \langle Z, x \rangle = Z\langle x \rangle$ is Abelian, which is a contradiction. Therefore the theorem is true.

Q.E.D.

Theorem 5.10. If G is of order p^2, then G is Abelian.

Proof. By Theorem 5.9, $|Z| \neq p$. But by Theorem 5.1, $|Z| \geq p$. Hence the only possibility for the order of Z is that $|Z| = p^2 = |G|$. Therefore G is Abelian.

Q.E.D.

Theorem 5.11. If G is non-Abelian of order p^4, then G' is Abelian.

Proof. This follows directly from Theorems 5.8 and 3.10.

Q.E.D.

Theorem 5.12. If G is non-Abelian of order p^5, then G' is Abelian.

In order to prove this theorem, we employ a lemma of C. Hobby [1], which we state as

Theorem 5.13. Let G be a p-group of order p^m $(m \geq 3)$, and H a non-Abelian subgroup of order p^3. Then H is not the Frattini subgroup $\Phi(G)$ of G.

Proof. Suppose that $H = \Phi(G)$. Then by the Sylow theorem, there is a subgroup N of G such that $N \lhd H$ and $|N| = p^2$; moreover N is normal in G, hence $[G:C(N)] \leq p$ (Blackburn [1]). Therefore $C(N)$ is a maximal subgroup of G so that $H \subseteq C(N)$. Now $N \subset H \subseteq C(N)$ implies that $N \subseteq Z(H)$. But the center of H is of order p (Theorem 5.9). This contradiction proves the theorem.

Q.E.D.

Proof of Theorem 5.12. The possible choices for the order of G' are p, p^2, and p^3. (p^4 is ruled out by Theorem 5.8.) If G' is of order p or p^2, then G' is Abelian (Theorem 5.10). There remains to show that G' is Abelian when $|G'| = p^3$. Suppose that G' is non-Abelian. We want to show that on this assumption we shall arive at a contradiction, and the theorem will be proved. Now the group G/G' is Abelian and of order p^2. It cannot be cyclic since G is non-cyclic (Theorem 5.7). Hence G/G' must be elementary

Abelian, so that $\Phi(G) \subseteq G'$ (Theorem 5.5). On the other hand, we always have $G' \subseteq \Phi(G)$. Therefore $G' \subseteq \Phi(G) \subseteq G'$ implies that $G' = \Phi(G)$. But a non-Abelian group of order p^3 cannot be the Frattini subgroup of any other p-group (Theorem 5.13). Therefore G' is Abelian. This completes the proof.

Q. E.D.

Theorem 5.14. If H is a normal subgroup of G, and $[G:H] = p^2$, then $G' \subseteq H$.

Proof. This follows directly from Theorem 5.10 and from the minimality of the commutator subgroup of a group.

Q.E.D.

From the fact that every p-group G has a non-trivial center, and that its central quotient group G/Z has the same property, it follows that every p-group G possesses a sequence of normal subgroups.

$$E = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{m-1} \subseteq K_m = G \qquad (1)$$

such that K_i/K_{i-1} belongs to the center of G/K_{i-1}, where $i = 1, 2, \ldots, m$. Series (1) is called a central series of G, and the number m is its length. (See P. Hall [1]).

We next define two important central series which result from the study of p-groups. These definitions arise from a paper of P. Hall [1].

Definition 5.1. The upper central series of a p-group

G is a sequence of characteristic subgroups of G

$$E = Z_0 \subseteq Z_1 \subseteq \ldots \subseteq Z_{c-1} \subseteq Z_c = G \qquad (2)$$

such that Z_i/Z_{i-1} is the center of G/Z_{i-1}, $i = 1, \ldots, c$.

Definition 5.2. The lower central series of a p-group G is a sequence of characteristic subgroups

$$E = H_{c'+1} \subseteq H_{c'} \subseteq \ldots \subseteq H_2 \subseteq H_1 = G \qquad (3)$$

such that $H_i = [H_{i-1}, G]$, $i = 2, \ldots, c'+1$.

Series (1), (2), and (3) are related by the following theorem.

Theorem 5.15. (i) $K_i \subseteq Z_i$ $(i = 0, 1, \ldots, c)$; and (ii) $H_i \subseteq K_{m-i+1}$ $(i = 1, 2, \ldots, c')$.

Proof. (i) We prove by induction on i. The result is trivial when $i = 0$. Suppose then that for some i, $K_i \subseteq Z_i$. Since K_{i+1}/K_i belongs to the center of G/K_i, $[K_{i+1}, G] \subseteq K_i \subseteq Z_i$. Hence in the homomorphism of G onto G/Z_i, every element of K_{i+1} corresponds to a self-conjugate element of G/Z_i; i.e., $K_{i+1} \subseteq Z_{i+1}$. Therefore $K_i \subseteq Z_i$ for all i. This proves (i). (ii) Here we again employ mathematical induction on i. The result is obvious when $i = 1$. Now, suppose that for some i, $H_i \subseteq K_{m-i+1}$. Then by the definition, $H_{i+1} = [H_i, G] \subseteq [K_{m-i+1}, G] \subseteq K_{m-i}$. Therefore $H_i \subseteq K_{m-i+1}$ for all i.

Q.E.D.

This theorem shows that $m \geq c$ and $m \geq c'$; hence $c = c'$. That is, the upper and lower central series of a p-group G have finite length, and both have the same length c. The number c is called the class of G.

Definition 5.3. The class of a p-group G is the least number c such that $Z_c = G$ (P. Hall [1]).

P. Hall [1] has shown that if $2i > c$, where c is the class of G, then H_i is Abelian. From this it is clear then that the commutator subgroup of a p-group of order p^m ($m \geq 3$) and class 2 or 3 must be Abelian. But the commutator subgroup of a p-group of order p^5 and class 4 is also Abelian (Theorem 5.12). (In fact we shall show later that the commutator subgroup of a 2-group of order 2^m ($m \geq 3$), and class m-1 is always Abelian.) Therefore the converse of this inequality is not true.

Kurosh [1] defined a nilpotent group as a group which possesses at least one central series. He also defined a solvable group as a group K which satisfies one of the following conditions:

(i) K has a finite solvable normal series.

(ii) K has a finite solvable invariant series.

(iii) The derived series of K terminates in the identity after a finite number of steps.

From these definitions, it follows that every p-group is nilpotent as well as solvable.

It is worthwhile to note here that not every p-group (in the sense of definition (2)) is nilpotent, for we have already mentioned that there exist infinite p-groups whose centers consist of the identity alone.

Scott [1] has shown

Theorem 5.16. The principal series of a p-group G has factors of order p.

Proof. The principal (or chief) series of a group H is a chain of characteristic subgroups of H

$$H = A_0 \supseteq A_1 \supseteq \ldots \supseteq A_n = E$$

such that for each i, A_i is a maximal normal subgroup of A_{i-1}. Now let $E = Z_0 \subseteq Z_1 \subseteq \ldots \subseteq Z_c = G'$ be the upper central series of G. By the definition, the factor groups Z_i/Z_{i-1} $(i = 1, \ldots, c)$ are Abelian; hence for each i, Z_i/Z_{i-1} has a composition series whose factors have order p. Then by the lattice theorem, G possesses a chain of subgroups

$$G = K_r \supseteq \ldots K_1 \supseteq K_0 = E$$

such that for each i, K_i/K_{i-1} is of order p, and refines the upper central series. There remains to show that $K_i \lhd G$. By construction, there is some j such that $Z_{j-1} \subseteq K_i \subseteq Z_j$, so $K_i/Z_{j-1} \subseteq Z_j/Z_{j-1}$ which is the center of G/Z_{j-1}. Hence $K_i/Z_{j-1} \lhd G/Z_{j-1}$, and so $K_i \lhd G$. Therefore the chain of subgroups which has been constructed is a principal series of G.

Q.E.D.

We quote M. Hall [1] for the definition of supersolvable group.

Definition 5.4. A group K is supersolvable if it possesses a finite series

$$K = A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_r = E$$

such that each factor group A_{i-1}/A_i ($i = 1, \ldots, r$) is cyclic.

Theorem 5.17. G is supersolvable.

Proof. This follows from Theorem 5.16 that in a principal series of G, each factor group has order p and is therefore cyclic.

Q.E.D.

6. The Frattini Subgroup of a p-Group.

In section 3, we have given some properties of a p-group in connection with its Frattini subgroup. We shall extend their relation further. One of the most important theorems regarding the Frattini subgroup of a p-group is

Theorem 6.1. (Burnside's basis theorem) Let G be a p-group, $\Phi(G)$ the Frattini subgroup of G, $|G/\Phi(G)| = p^d$. Then the following hold.

(i) If $G/\Phi(G) = \langle \Phi(G)x_1, \Phi(G)x_2, \ldots, \Phi(G)x_d \rangle$, then $G = \langle x_1, x_2, \ldots, x_d \rangle$;

(ii) If $G = \langle y_1, y_2, \ldots, y_s \rangle$, then there exists a subset

$\{ y_{i_1}, y_{i_2}, \ldots, y_{i_d} \} \subseteq \{ y_1, y_2, \ldots, y_s \}$ such that $G = \langle y_{i_1}, y_{i_2}, \ldots, y_{i_d} \rangle$.

Proof. (i) Suppose that $G \neq \langle x_1, x_2, \ldots, x_d \rangle$, then by the Sylow theorem, $\langle x_1, x_2, \ldots, x_d \rangle$ is contained in a maximal subgroup M of G. Since $\Phi(G) \subseteq M$, it follows that $\langle \Phi(G), x_1, x_2, \ldots, x_d \rangle \subseteq M$, and so $\langle \Phi(G)x_1, \Phi(G)x_2, \ldots, \Phi(G)x_d \rangle \subseteq M/\Phi(G) \subset G/\Phi(G)$. Therefore $G/\Phi(G) \neq \langle \Phi(G)x_1, \ldots, \Phi(G)x_d \rangle$ which is a contradiction. This proves (i).

(ii) Since the Frattini subgroup of a group is the set of non-generators, it follows that $G = \langle \Phi(G), y_1, y_2, \ldots, y_s \rangle$. Now, in the homomorphism of G onto $G/\Phi(G)$, let $y_i \longrightarrow \Phi(G)y_i$. Then $G/\Phi(G) = \langle \Phi(G)y_1, \Phi(G)y_2, \ldots, \Phi(G)y_s \rangle$. But since $G/\Phi(G)$ is elementary Abelian, a minimal basis of $G/\Phi(G)$ contains $d \leq s$ elements. If $\{ y_{i_1}, y_{i_2}, \ldots, y_{i_d} \} \subseteq \{ y_1, y_2, \ldots, y_s \}$ such that $G/\Phi(G) = \langle \Phi(G)y_{i_1}, \Phi(G)y_{i_2}, \ldots, \Phi(G)y_{i_d} \rangle$, then by (i), $G = \langle y_{i_1}, y_{i_2}, \ldots, y_{i_d} \rangle$. This completes the proof.

Q.E.D.

This theorem shows that a minimal basis of a p-group G may be obtained from the representatives in G of any minimal basis of the group $G/\Phi(G)$. When we come to the group Aut(G) of automorphisms of G, we shall show how the burnside's basis theorem may be applied in obtaining a limitation for the order of Aut(G).

From Theorem 5.13, we know that not every p-group can

function as Frattini subgroup of some other p-groups. The following theorem which was proved by C. Hobby [1] is another instance of this case.

Theorem 6.2. Let H be a non-Abelian subgroup of a p-group G, and suppose that the index of H' in H is p^2. Then $H \neq \Phi(G)$.

Proof. Suppose that $H = \Phi(G)$. Then by Theorem 5.16, H' contains a normal subgroup N of G with $|H'/N| = p$. Since N is normal and contained in $\Phi(G)$, hence by a theorem of Gaschutz [1], $\Phi(G/N) = \Phi(G)/N = H/N$. Also $|H/N| = |H/H'||H'/N| = p^3$; and $H'/N \neq E$ so that H/N is non-Abelian. We therefore obtain H/N as a non-Abelian group of order p^3 and $H/N = \Phi(G/N)$ contradicting Theorem 5.13. Therefore $H \neq \Phi(G)$.

Q.E.D.

In determining whether a given group is nilpotent or not, it has been proved (M. Hall [1], p 157) that in a nilpotent group, the Frattini subgroup always contains the derived group. On the other hand, Wielandt, H (M. Hall [1], p 157) proved that if the Frattini subgroup of a finite group G contains the derived group, then G is nilpotent. The condition that G is finite is necessary for this theorem does not apply in general to infinite groups. Recently, besides Hobby who has dealt in particular the Frattini subgroup of a p-group (in the sense of definition (2)), other writers such as

Dlab, V [1] and Korinek, V [1] have dealt with the Frattini subgroup of a more general class of groups.

7. Groups of Automorphisms of p-Groups.

While it is true that every p-group G has a non-trivial center, its group Aut(G) of automorphisms need not join the same property. For example, let G be the four-group. Then Aut(G) is isomorphic with the symmetric group S_3 which is centerless. But note that 2 divides the order of Aut(G) so that the order of Aut(G) is bounded below. In this section, we shall show the relation between a p-group and its group of automorphisms, and from this we shall obtain some limitation for the order of Aut(G).

When a non-Abelian p-group G is given, the order of Aut(G) is not readily found except for a few cases. But when G is elementary Abelian, we have

Theorem 7.1. If G is an elementary Abelian p-group whose order is p^m, then the order of Aut(G) is of the form

$$f(p^m) = (p^m - 1)(p^m - p)\ldots(p^m - p^{m-1}).$$

Proof. Since G is elementary Abelian, a minimal basis of G consists of m elements. Suppose that $\{s_1, s_2, \ldots, s_m\}$ is a fixed basis of G, and $\{s_1', s_2', \ldots, s_m'\}$ is any other

basis of G. Then the mapping $s_i \longrightarrow s_i^f$, $i = 1, 2, \ldots, m$, defines an automorphism of G so that the order of Aut(G) is equal to the number of ways in choosing a basis for G. Now there are $p^m - 1$ possibilities for s_1. After choosing s_1, there are $p^m - p$ possibilities for s_2. Continuing this process until all m generators have been chosen. There are therefore $(p^m - 1)(p^m - p)\ldots(p^m - p^{m-1})$ distinct ways in which a set of independent generators may be chosen. Hence $| \text{Aut}(G) | = f(p^m)$.

Q.E.D.

From this theorem we may deduce that when a p-group G is cyclic of order p, then Aut(G) is cyclic of order p-1. In particular, when p = 2, then Aut(G) is the identical automorphism. In general, when a p-group G of order p^m (p an odd prime) is cyclic, then Aut(G) is also cyclic and of order $p^{m-1}(p-1)$ (Burnside [1]). But when $p = 2$, we have

Theorem 7.2. If G is a cyclic group of order 2^m ($m > 2$), then Aut(G) is Abelian and of type (m-2,1).

Proof. Let a be a fixed element of G such that $G = \langle a \rangle$. Since G is cyclic, there is only one element of order 2^{m-1} in G; hence there are 2^{m-1} elements of order 2^m. If b is any one of these, then the mapping $f(a) = b$ defines an automorphism of G. Since the congruence

$$x^{2^{m-1}} \equiv 1 \pmod{2^m}$$

has no primitive root, Aut(G) is non-cyclic. Now $5^{2^{m-2}} \equiv 1 \pmod{2^m}$ but $5^{2^{m-3}} \not\equiv 1 \pmod{2^m}$, hence the automorphism $h(a) = a^5$ generates the cyclic group $\langle h \rangle$ of order 2^{m-2}; on the other hand, the automorphism $g(a) = a^{-1}$ is of order 2 and not contained in $\langle h \rangle$. Therefore $\text{Aut}(G) = \langle h \rangle \times \langle g \rangle$ is Abelian and type $(m-2,1)$.

Q.E.D.

From this theorem, we deduce some special cases for the order of Aut(G). When the group G is cyclic of order 4, then Aut(G) is of order 2, and is therefore cyclic. When G is elementary Abelian of order 4, then Aut(G) has order 6 (Theorem 7.1). Now there are only two groups of order 6; one cyclic and one non-Abelian which is isomorphic with the symmetric group S_3 (Ledermann [1], p 49). Since Aut(G) is non-cyclic, it follows that $\text{Aut}(G) \approx S_3$. We therefore see that the group of automorphisms of a p-group need not have a non-trivial center. However the order of Aut(G) is always divisible by p if the p-group G is Abelian.

Theorem 7.3. If G is an Abelian group of order p^m $(m \geq 2)$, then $p \mid |\text{Aut}(G)|$.

Proof. The theorem is obviously true when G is either cyclic or elementary Abelian. In any other possibility for G, G is the direct product of cyclic groups $C_1, \ldots, C_t$ of orders $p^{m_1}, \ldots, p^{m_t}$, respectively. (This follows from the

fundamental theorem for finite Abelian groups. See M. Hall [1].) Without lose of generality, we may assume that $m_1 \geq 2$ and $t > 1$. Since C_1 is cyclic of order p^{m_1}, $Aut(C_1)$ has an element f of order p. For $x \in G$, x can be written uniquely as $x = s_1 s_2 \ldots s_t$ with $s_i \in C_i$, and the mapping $f^*(x) = f(s_1)s_2 \ldots s_t$ defines an automorphism of G. But $|f^*| = |f| = p$. Therefore $p \mid |Aut(G)|$.

Q.E.D.

As a matter of fact, this theorem is a particular case of a theorem of Hilton [1]. Hilton proved that if the order of an Abelian group G is divisible by p^m, then the order of Aut(G) is divisible by $p^{m-1}(p-1)$. Using this theorem, we see that Theorem 7.3 may be replaced by

Theorem 7.3*. If G is an Abelian group of order p^m, then $p^{m-1}(p-1) \mid |Aut(G)|$. In particular, when $p = 2$, then $2^{m-1} \mid |Aut(G)|$.

We have mentioned in section 6 that the Burnside's basis theorem may be applied in obtaining a limitation for the order of Aut(G). This fact was first considered by P. Hall [1]. The results were stated in M. Hall [1] as

Theorem 7.4. Let G be a p-group of order p^m, $\Phi(G)$ the Frattini subgroup of G, $|G/\Phi(G)| = p^d$. Then $|Aut(G)| \mid p^{d(m-d)} f(p^d)$, where $f(p^d) = (p^d - 1)\ldots(p^d - p^{d-1})$.

Proof. Since the group $G/\Phi(G)$ is elementary Abelian

(Theorem 5.5), its group of automorphisms is of order $f(p^d)$ (Theorem 7.1). Now by the Burnside's basis theorem, there is an ordered generating set $X = (x_1, x_2, \ldots, x_d)$ of G. We assert that there are $p^{d(m-d)}f(p^d)$ such ordered generating sets of G. Consider the mapping $x_i \longrightarrow a_i$, $i = 1, 2, \ldots, d$, of X onto a basis of $G/\Phi(G)$, the basis of $G/\Phi(G)$ may be chosen in $f(p^d)$ ways, and for each a_i, any of the p^{m-d} elements in the cosets of $\Phi(G)$ mapped onto a_i is a permissible choice for x_i. Since there are d elements in an ordered generating set, there are therefore $p^{d(m-d)}f(p^d)$ ordered generating sets of G. Now every automorphism of G induces a permutation on the X's. But since an automorphism fixing any set X fixes every product of the x_i in X, and so the entire group G; hence it is the identical automotphism. Therefore the group Aut(G) may be regarded as a regular permutation group on the X's, so that the sets X are permuted among themselves in transitive constituents each of which contains the same number of sets equal to the order of Aut(G). Therefore $|\mathrm{Aut}(G)| \mid p^{d(m-d)}f(p^d)$.

Q.E.D.

As a consequence of this theorem, we have

Corollary 7.5. The order of the group $\mathrm{Aut}(G, \| G/\Phi(G))$ of automorphisms of G which fixes the group $G/\Phi(G)$ elementwise is a divisor of $p^{d(m-d)}$.

Proof. This follows from the fact that an automorphism of G which fixes the group $G/\Phi(G)$ elementwise induces a regular permutation on the $p^{d(m-d)}$ ordered generating sets X of G; and by repeating the same argument of Theorem 7.5, we have the corollary.

Q.E.D.

Having dealt in some detail with the upper bound for the order of Aut(G), where G is a p-group, our next inquiry is the lower bound of $|\mathrm{Aut}(G)|$. When G is an Abelian p-group, we have Theorem 7.3*. For non-Abelian p-groups, the first result was obtained by Herstein and Adney [1] in year 1952. They proved

Theorem 7.6. Let G be a finite group of order $p^m s$, $(p,s) = 1$ and $m \geq 2$. Then the order of Aut(G) is divisible by p.

Proof. We prove by the contrary. Suppose that $p^2 \mid |G|$ but $p \nmid |\mathrm{Aut}(G)|$. Since $G/Z \approx \mathrm{Inn}(G)$, the group of inner automorphisms of G, which is a normal subgroup of Aut(G) (M. Hall [1], p 85), hence $p \nmid |\mathrm{Aut}(G)|$ implies that $p \nmid |G/Z|$, and so $p^m \mid |Z|$, where p^m is the highest power of p dividing $|G|$. Therefore every Sylow p-subgroup S_p of G is contained in Z and hence it is the center of its normalizer. Then by a theorem of Burnside (Zassenhaus [1], p 139), G contains a normal subgroup H with $[G:H] = |S_p|$.

Clearly $H \cap S_p = E$ and $HS_p = G$; i.e., $G = S_p \times H$. Now S_p is Abelian and of order p^m $(m \geq 2)$, hence $Aut(S_p)$ contains an element f of order p. For $a \in G$, a can be written uniquely as $a = sh = hs$ where $s \in S_p$ and $h \in H$; and the mapping $f^*(a) = f(s)h$ defines an automorphism of G which is of order p. This implies that $p \mid |Aut(G)|$ contradicting our assumption. Therefore the theorem is true.

Q.E.D.

In this theorem, the group G need not be a p-group. But it certainly must be finite, for there are infinite groups whose groups of automorphisms consist of 2 elements only. For example, in a p-quasicyclic group $C_{p^\infty} = \{a_n,\ n \in J^+ \mid a_{n-1}^p = a_n,\ a_1^p = e\}$, (Schenkman [1], p 86) the group $Aut(C_{p^\infty})$ contains no element of order p unless $p = 2$, in which case the only non-trivial automorphism maps each element of the group onto its inverse; and clearly $p^2 \mid |C_{p^\infty}|$ for any prime p.

With the result obtained by Herstein and Adney, many writers have attempted to work on the same subject. After a deep investigation with the center and the Sylow p-subgroups of a finite group G, Scott [2] in the year 1953, extended the theorem of Herstein and Adney. He proved that if the order of a finite group G is divisible by p^3, then the order of Aut(G) is divisible by p^2. In his paper, Scott made a

conjecture that there is a function $f(m)$ such that if the order of the group G is divisible by $p^{f(m)}$, then the order of Aut(G) is divisible by p^m. A year later, Schenkman [2] published a paper suceeding Scott's conjecture. Schenkman proved that if G is a finite non-Abelian group whose commutator subgroup is contained in the center Z of G, then the order of G divides the order of Aut(G).

In all these theorems, the group G in concern need not be a p-group. Applying the theorem of Schenkman to our p-groups, we see that if G is a p-group and class 2, then its order divides the order of Aut(G) since the commutator subgroup of a class 2 p-group is always contained in the center of the group.

8. Structure Theorems of 2-Groups.

Generally speaking, groups can be divided into Abelian and non-Abelian. For finite Abelian groups, their structure is completely determined (up to isomorphism) by a theorem which states that a finite Abelian group is the direct product of cyclic groups of prime power order (M. Hall [1], p 41). Thus the number of distinct types of Abelian p-groups of order p^m is equal to the number of partitions of m with regard to addition. For example, let $m = 7$. There are 14

ways of partitioning 7 with regard to addition, hence there are 14 isomorphisms classes of Abelian groups of order p^7. These may be written as: (7); (6,1); (5,2); (5,1,1); (4,3); (4,2,1); (4,1,1,1); (3,3,1); (3,2,1,1); (3,1,1,1,1); (2,2,2,1); (2,2,1,1,1); (2,1,1,1,1,1); (1,1,1,1,1,1,1).

When G is a non-Abelian p-group, the case is not simple. It is more complicated when $p = 2$. This will be shown in the following theorems.

Theorem 8.1. Let G be a non-Abelian group of order 2^m, and let it contain a cyclic subgroup of index 2. Then G belongs to one of the following types:

$m \geq 3$

(1) Generalized quaternion group,

$$a^{2^{m-1}} = e, \quad b^2 = a^{2^{m-2}}, \quad bab^{-1} = a^{-1}.$$

(2) Dihedral group,

$$a^{2^{m-1}} = e, \quad b^2 = e, \quad bab^{-1} = a^{-1}.$$

$m \geq 4$

(3) Semi-dihedral group,

$$a^{2^{m-1}} = e, \quad b^2 = e, \quad bab^{-1} = a^{-1+2^{m-2}}.$$

(4) $$a^{2^{m-1}} = e, \quad b^2 = e, \quad bab^{-1} = a^{1+2^{m-2}}.$$

Proof. If G contains an element a of order 2^{m-1}, then $\langle a \rangle$ as a maximal subgroup of G, is normal in G. For $b \notin \langle a \rangle$, we have $b^2 = a^s \in \langle a \rangle$, and $bab^{-1} = a^r$ where $r^2 \equiv 1 \pmod{2^{m-1}}$ but $r \not\equiv 1 \pmod{2^{m-1}}$ since G is non-Abelian.

It follows that there are three choices for $r \bmod 2^{m-1}$ namely: $r = -1$, $-1 + 2^{m-2}$, $1 + 2^{m-2}$. Since $ba^sb^{-1} = a^s$, we have $a^{sr} = a^s$ or $rs \equiv s \pmod{2^{m-1}}$ as a condition on s. When $r = -1$, then $-s \equiv s \pmod{2^{m-1}}$ implies that $2s \equiv 0 \pmod{2^{m-1}}$ or $s \equiv 0 \pmod{2^{m-2}}$. Therefore $a^s = e$ or $a^s = a^{2^{m-2}}$. Hence with $r = -1$, we have the generalized quaternion group or the dihedral group. When $m = 3$, these are the only groups. Next suppose that $m \geq 4$, and $r = -1 + 2^{m-2}$. Then $(-1 + 2^{m-2})s \equiv s \pmod{2^{m-1}}$ implies that $s(2 - 2^{m-2}) \equiv 0 \pmod{2^{m-1}}$ or $s \equiv 0 \pmod{2^{m-2}}$. Therefore $a^s = e$ or $a^s = a^{2^{m-2}}$. In the latter case, we have $b_1^2 = e$ where $b_1 = ab$. Hence either a and b or a and b_1 satisfy the relations of type (3). Finally suppose that $m \geq 4$, and $r = 1 + 2^{m-2}$. Then $(1 + 2^{m-2})s \equiv s \pmod{2^{m-1}}$ implies that $2^{m-2}s \equiv 0 \pmod{2^{m-1}}$ or $s = 2s_1$ (say). We find i by the congruence $i(1 + 2^{m-3})s_1 \equiv 0 \pmod{2^{m-2}}$, and set $b_1 = a^ib$. Then $b_1ab_1^{-1} = a^{1+2^{m-2}}$ so that a and b_1 satisfy the relations of type (4) in the theorem. This completes the proof.

Q.E.D.

There is only one type for a non-Abelian p-group G (p an odd prime) of order p^m which contains an element of order p^{m-1}. This group is defined by the relations

$$a^{p^{m-1}} = e, \quad b^p = e, \quad bab^{-1} = a^{1+p^{m-2}}.$$ (See M. Hall [1], p 187).

Theorem 8.2. Let G be a 2-group of order 2^m ($m \geq 3$) and maximal class. Then G has the following properties:

(1) $Z \subseteq G'$.

(2) G' is cyclic of type $(m-2)$.

(3) G contains cyclic subgroups of index 2.

Proof. We prove by induction on m. When $m = 3$, the dihedral and quaternion groups of order 8 are of maximal class. Each group contains elements of order 4, and the subgroup $Z = G'$ is of order 2. Suppose then that $m > 3$. Since G is of maximal class, $|Z| = 2$, and G/Z is of order 2^{m-1} and maximal class. Therefore by the induction assumption, G/Z contains a cyclic subgroup $A/Z = \langle Zx \rangle$ of index 2 in G/Z. By the lattice theorem, $A = \langle Z, x \rangle$ is a subgroup of index 2 in G. Clearly A is Abelian. We assert that it is cyclic. Suppose it is not. Then $A = Z \times \langle x \rangle$, and $\langle x^{2^{m-3}} \rangle$ being characteristic in A, is normal in G. Since it is of order 2, it is contained in Z which is a contradiction. Therefore $A = \langle a \rangle$ is cyclic, and $G = \langle A, y \rangle$. Since A is normal in G, the mapping $f(a) = [a,y]$ is a homomorphism of A onto G'. Now $a \in \mathrm{Ker}(f)$ iff $f(a) = [a,y] = e$; which is so iff $a \in Z$. Hence $\mathrm{Ker}(f) = Z$, and $A/Z \approx G'$. Since A/Z is cyclic of type $(m-2)$, this implies that G' is cyclic of type $(m-2)$. The proof is now complete.

Q.E.D.

As a consequence of this theorem, we have

Corollary 8.3. If G is a 2-group of order 2^m and contains an Abelian subgroup A of index 2, and if $Z \subseteq G'$, then $A/Z \approx G'$.

M. Hall and Senior [1] have shown

Theorem 8.4. Let G be a 2-group of order 2^m and class 2 with center Z of order 2. Then G is the central product of dihedral and quaternion groups.

Proof. Here again we prove by induction on m. When $m = 3$, G is a non-Abelian group of order 8; hence it is either dihedral or quaternion. Suppose now that $m > 3$. Since G is non-Abelian, there are elements x, y with $[x,y] = e$. Then the centralizers $C(x)$ and $C(y)$ are both of index 2 in G; and so $C(x) \cap C(y) = H$ is of index 4 in G. Let $K = \langle x,y \rangle$. Then $G = KH$ and $K \cap H = Z$. Since $[K,H] = E$, $Z(H) = Z$. Therefore G is the central product of K and H. By the induction assumption, H is the central product of dihedral and quaternion groups. On the other hand, since $K/K \cap H \approx KH/H$, $|K| = |K \cap H||G/H| = 8$ so that K is either dihedral or quaternion. The theorem now follows.

Q.E.D.

Theorem 8.5. If G is a 2-group of order 2^m which contains only one subgroup of order 2, then G is either

cyclic or generalized quaternion.

Proof. We prove by induction on m that G is cyclic or generalized quaternion. The result is obvious when $m = 1$. We may therefore assume that $m > 1$. If G contains a subgroup H of index 2, then by the induction assumption, H is cyclic. Hence G is either cyclic or one of types (1) through (4) of Theorem 8.1. But each of these groups contains more than one subgroup of order 2 except the generalized quaternion group. There remains to be considered the case where every subgroup of index 2 is generalized quaternion. We shall show that this situation can not happen. First let $m = 4$ and a subgroup Q of index 2 be the quaternion group. Then $Q = \langle a, b \quad a^4 = e, \quad b^2 = a^2, \quad bab^{-1} = a^{-1} \rangle$ and $G = Q + Qx$ where $x \notin Q$ but $x^2 \notin Q$. Now x must transform one of the subgroups of Q namely $\langle a \rangle$, $\langle b \rangle$, $\langle cb \rangle$ into itself. Without lose of generality, we may suppose this to be $\langle a \rangle$. Then $c^{-1}ac = a$ or $c^{-1}ac = a^{-1}$. The first case implies that $\langle a,c \rangle$ is an Abelian group of index 2 contrary to our assumption. The latter case implies that $(cb)^{-1}a(cb) = a$ so that $\langle a, cb \rangle$ is an Abelian group of index 2, again a contradiction. Next suppose $m \geq 5$, and a subgroup H of index 2 be a generalized quaternion group. Then $H = \langle a, b \mid a^{2^{m-2}} = e, \quad b^2 = a^{2^{m-3}}, \quad bab^{-1} = a^{-1} \rangle$ and $G = H + Hx$. Since $\langle a \rangle$ is the only subgroup of order 2^{m-2} in H and all elements of H not in $\langle a \rangle$ are of order 4,

hence $x^{-1}ax = a^r$ and $x^2 = a^ib$ or $x^2 = a^i$. If $x^2 = a^ib$, then $x^{-2}ax^2 = a^{-1} = x^{-1}a^rx = a^{r^2}$ so that $r^2 \equiv -1 \pmod{2^{m-2}}$ which is impossible. If $x^2 = a^i$, then $\langle a,x \rangle$, as a subgroup of index 2, is generalized quaternion. Hence $c^{-1}ac = a^{-1}$, $(cb)^{-1}a(cb) = a$ so that $\langle a,cb \rangle$ is an Abelian group of index 2, a contradiction. This completes our proof of the theorem.

Q.E.D.

Theorem 8.5 can be extended in the following sense.

Theorem 8.6. If G is a 2-group of order 2^m which contains only one subgroup of order 2^r, $1 < r < m$, then G is cyclic.

Proof. Here again we prove by induction on m. When $m = 3$ (in which case $r = 2$), each of the five groups of order 8 contains more than one subgroup of order 4 except the cyclic group of order 8. On the other hand, if a group G of order 2^m contains only one subgroup H of order 2^{m-1}, then H must be the Frattini subgroup $\Phi(G)$ of G. Suppose that x is an element of G which is not in $\Phi(G)$ such that $G = \Phi(G)\langle x \rangle$, then we have $G = \langle x \rangle$; i.e., G is cyclic. This proves the theorem for $m = 3$ and for all cases with $r = m-1$. We may therefore assume that $1 < r < m-1$ and $m > 3$. Let H be the unique subgroup of order 2^r, then H is contained in a maximal subgroup M of G. Since

$1 < r < m-1$, hence by the induction assumption, M is cyclic; and so H, as a subgroup of a cyclic group, is also cyclic. Now every element of order 2 or 4 is contained in a subgroup of order 2^r, $r \geq 2$, and hence in H. But H, being cyclic, contains only one subgroup of order 2 and one of order 4. Therefore by Theorem 8.5, G is cyclic or generalized quaternion. Since a generalized quaternion group contains more than one subgroup of order 4, it follows that G is cyclic. This completes the proof.

Q.E.D.

This theorem applies also to any p-group, where p is an odd prime. In fact a p-group (p an odd prime) of order p^m which contains only one subgroup of order p^r, $1 \leq r \leq m$, is necessarily cyclic. (See Burnside [1], p 131.)

9. Classification of 2-Groups.

We shall now illustrate the forgoing theorem by classifying all groups of order 2^m ($1 \leq m \leq 4$).

Since 2 is a prime number, there is only one group of this order and it is cyclic.

A group of order 4 is by Theorem 5.10 an Abelian group. There are therefore two isomorphism classes: (2); (1,1).

For groups of order 8, there are three Abelian types: (3); (2,1); (1,1,1).

In considering a non-Abelian group G of order 8, we first suppose that G contains an element a of order 4. Then by Theorem 8.1, G must belong to one of the following:

Dihedral group:

$a^4 = e, \quad b^2 = e, \quad bab^{-1} = a^{-1}.$

Quaternion group:

$a^4 = e, \quad b^2 = a^2, \quad bab^{-1} = a^{-1}.$

Next suppose that G contains no element of order greater than 2. Then every element of G is of order 2 except the identity, so that G is Abelian the case which has already been considered. Thus these two groups exhaust all the possibilities for non-Abelian groups of order 8. There are therefore 5 groups of order 8; three Abelian and two non-Abelian.

We next consider groups of order 16. There are five Abelian types of this order: (4); (3,1); (2,2); (2,1,1); (1,1,1,1).

A non-Abelian group G of order 16 which contains an element of order 8, must by Theorem 8.1, belong to one of the following:

$a^8 = e, \quad b^2 = e, \quad bab^{-1} = a^5.$

Dihedral group:

$a^8 = e, \quad b^2 = e, \quad bab^{-1} = a^{-1}.$

Generalized quaternion:

$a^8 = e, \quad b^2 = a^4, \quad bab^{-1} = a^{-1}.$

Semi-dihedral:

$a^8 = e, \quad b^2 = e, \quad bab^{-1} = a^3.$

Next suppose that G contains an invariant cyclic group $\langle a \rangle$ of order 4 but contains no element of order 8. We consider the following cases.

(i) Suppose that $a \in Z$. Then we must have $\langle a \rangle = Z$ and $G/\langle a \rangle$ can only be of type (1,1) (Theorem 5.9). There can be no element $x \in G$ with $x^4 \in \langle a \rangle$ and $x^3 \notin \langle a \rangle$ for otherwise $G = \langle a,x \rangle$ would be Abelian contrary to our assumption. Hence there must be elements $b, c \notin \langle a \rangle$ and both are of order 2. Since $b \notin Z$, and since $c^{-2}bc^2 = b$, it follows that $c^{-1}bc = ba^r$, where $r \equiv 0 \pmod{2^{m-3}}$. Therefore there is a single type defined by the relations

$$a^4 = e, \quad b^2 = e, \quad c^2 = e, \quad c^{-1}bc = ba^2,$$

$$b^{-1}ab = a, \quad c^{-1}ac = a.$$

(ii) Suppose next that G contains no self-conjugate element of order 4, and that $\langle a \rangle$ is a self-conjugate cyclical subgroup of order 4. If $G/\langle a \rangle$ is cyclic, then $x^4 \in \langle a \rangle$ for all $x \in G$. Suppose that b is any element of order 4 which is not contained in $\langle a \rangle$. Since G is

non-Abelian and $\langle a \rangle$ is normal, we have $b^{-1}ab = a^{-1}$. There is therefore a single type defined by the relations

$$a^4 = e, \quad b^4 = e, \quad b^{-1}ab = a^{-1}.$$

Next if $G/\langle a \rangle$ is non-cyclic, then $x^2 \in \langle a \rangle$ for all $x \in G$. Suppose that $Z \not\subset \langle a \rangle$. Then G must contain an element $b \in Z - \langle a \rangle$ with $b^2 = e$. If c is any other element not in $\langle a,b \rangle$, then $\langle a,c \rangle$ is a normal subgroup of order 8 and $\langle a,c \rangle \cap \langle b \rangle = E$. Hence G is the direct product of a group of order 8 and a group of order 2. There are therefore two types corresponding to the two non-Abelian groups of order 8.

$$a^4 = e, \quad b^2 = e, \quad b^{-1}ab = a^{-1}, \quad c^2 = e, \quad c^{-1}ac = a, \quad c^{-1}bc = b.$$

$$a^4 = e, \quad b^2 = a^2, \quad b^{-1}ab = a^{-1}, \quad c^2 = e, \quad c^{-1}ac = a, \quad c^{-1}bc = b.$$

Next suppose that G contains no element of order 8 and no self-conjugate cyclical subgroup of order 4. Clearly G contains elements of order 4. Let a be one of these, then $\langle a \rangle$ is normal in a non-cyclical subgroup $\langle a,b \rangle$ of order 8. If c is any other element of G which is not in $\langle a,b \rangle$, then since $a \notin Z$, $c^{-1}ac = ab$. There is again a single type defined by the relations

$$a^4 = e, \quad b^2 = e, \quad c^2 = e, \quad b^{-1}ab = a, \quad c^{-1}bc = b, \quad c^{-1}ac = ab.$$

Finally suppose that G contains no element of order

greater than 2. Then every element of G is of order 2 except the identity. But this implies that G is an elementary Abelian group. Hence these groups exhaust all the possibilities for non-Abelian groups of order 16. There are therefore fourteen types of groups of order 16; five Abelian and nine non-Abelian.

This method of determining groups of prime power order was suggested by Burnside [1]. In his text, Burnside classified all groups of order p^4, p an odd prime, and he showed that there are fifteen distinct types of groups of this order.

The nine non-Abelian groups of order 16 which have just been determined can also be classified into two classes according as the group G is of class 2 or 3.

If the group G is of class 2, then the commutator subgroup G' must have order 2, and so the center Z has order 4. If G is of class 3, then G' is of order 4, and so Z is of order 2. Since the automorphism group of a cyclic group of order 8 is non-cyclic (Theorem 7.2), it follows that there are three non-isomorphic non-Abelian split extentions; one of these has derived group of order 2, and the other two have derived groups of order 4 (Schenkman [1], p 94). Since the generalized quaternion group of order 16 has derived group of order 4, it follows that there are three groups of maximal

class with derived group of order 4 namely: the dihedral, generalized quaternion, and semi-dihedral groups of order 16, hence there are six groups of class 2 with derived group of order 2.

The above methods used in classifying groups of order 16 are clearly not applicable in classifying groups of order 32 or 64, for there is no apparent limit to the complication of a prime-power group. As we pass from the groups of order 8 to those of order 16, then to those of order 32, and so on, at each step new structural phenomena make their appearance. For this reason, those authors who have constructed p-groups on an extensive scale have found it necessary as a preliminary to split the problems up by introducing some system of classification. Thus Bagnera, who was the first to determine all the groups of order p^5, where p is an odd prime, made use of certain numerical invariants, notably the number of independent generators and the number of inner automorphisms, and also of the presence or absence of an Abelian subgroup of index p. Schreier, in his well-known paper on the same subject, employs the fact that the commutator subgroup G' of a group G of order p^5 is necessarily Abelian, and classifies these groups according to the type invariants of the Abelian groups G' and G/G'.

These methods, admirable as they are for the purpose

for which they were devised, would need to be supplemented, as we passed to groups of higher and higher orders, owing to the gradually increasing complexity of the groups concerned. We therefore ask whether it would not be possible to introduce a system of classification which would apply without modification to all p-groups. The answer to this question has been given by P. Hall [2].

Recently M. Hall and Senior [1] employed the methods outlined by P. Hall and classified all the groups of order 64. They showed that there are in fact 267 groups of this order which clarify the one determined by Miller [1] who showed that there are 294 groups of order 64.

10. Class Numbers of 2-Groups.

From the results of section 9, it is clear that for each natural number n, there are only finitely many non-isomorphic groups having n for their order. Similarly, there are only finitely many non-isomorphic finite groups having a given number k of classes of conjugate elements. We call the number k the class number of the group. It is well known that Abelian groups have maximum class number. On the other hand, a p-group G of order p^m and maximum

class m-1 has a minimum class number. In fact, Poland [1] has shown

Theorem 10.1. The class number k of a quaternion group, dihedral group, or a semi-dihedral group is given by $k = 2^{m-2} + 3$.

Proof. Suppose that G is quaternion $\langle a, b \mid a^{2^{m-1}} = e,\ b^2 = a^{2^{m-2}},\ b^{-1}ab = a^{-1} \rangle$, or dihedral $\langle a, b \mid a^{2^{m-1}} = e,\ b^2 = e,\ b^{-1}ab = a^{-1} \rangle$. Then in each of these two cases, $G = \{a^s b^t \mid s = 1, \ldots, 2^{m-1},\ t = 1, 2\}$ and $Z = \langle a^{2^{m-2}} \rangle$, $|Z| = 2$. Now $a^r(a^s b)a^{-r} = a^{s+r}(ba^{-r}b^{-1})b = a^{s+2r}b$, and $b(a^s b)b^{-1} = (ba^s b^{-1})b = a^{-s}b$. If $a^s \in G - Z$, then $C(a^s) = \langle a \rangle$ and so $|Cl(a^s)| = 2$, and there must be $(2^{m-1} - 2)/2 = 2^{m-2} - 1$ such conjugate sets. Since for $1 \leq s \leq 2^{m-1}$, $Cl(a^s b) = \{a^{\pm(s-2r)} \mid r \in J\}$ hence $|Cl(a^s b)| = 2^{m-2}$. The 2^{m-1} elements of the form $a^s b$ split into two classes. Therefore $k = (2^{m-2} - 1) + 2 + 2 = 2^{m-2} + 3$.

Next suppose that G is semi-dihedral $\langle a, b \mid a^{2^{m-1}} = e,\ b^2 = e,\ bab^{-1} = a^{-1+2^{m-2}} \rangle$. Here again $Z = \langle a^{2^{m-2}} \rangle$, $|Z| = 2$ so that the elements of the form a^s fall into two conjugate sets of one element each, and $2^{m-2} - 1$ conjugate sets of two elements each. Now $a^r(a^s b)a^{-r} = a^{s+r}(ba^{-r}b^{-1})b = a^{s+r}(a^{r-r2^{m-2}})b$, and

$b(a^s b)b^{-1} = (ba^s b^{-1})b = a^{-s+s2^{m-2}}b$. Hence $Cl(a^s b) \supseteq \{ a^{s-4t}b \mid t \in J \} \cup \{a^{s+2+2^{m-2}}\}$ so that $|Cl(a^s b)| > 2^{m-1}/4 = 2^m/8$. Since $|Z| = 2$, the centralizer of any element $a^s b$ must have order at least 4. Therefore $|Cl(a^s b)| = 2^{m-2}$, and again we have $k = (2^{m-2} - 1) + 2 + 2 = 2^{m-2} + 3$.

Q.E.D.

Theorem 10.2. If G is a p-group whose defining relations are given by

$$a^{p^{m-1}} = e, \quad b^p = e, \quad bab^{-1} = a^{1+p^{m-2}},$$

then the class number k of G is $k = p^{m-1} + p^{m-2} - p^{m-3}$.

Proof. We first obtain the conjugates of the element of the form $a^s b^t$. (i) $a^{-1}(a^s b^t)a = a^{s-1}(b^t a b^{-t})b^t = a^{s-1}(a^{[1+p^{m-2}]t}b^t) = a^{s+tp^{m-2}}b^t$, and (ii) $b(a^s b^t)b^{-1} = ba^s b^{-1}b^t = a^{s+sp^{m-2}}b^t$. Therefore $Cl(a^s b^t) = \{ a^{r(s,t)p^{m-2}}a^s b^t \mid r \in J \}$. Hence $a^s b^t \in Z$ iff $t \equiv 0 \pmod p$ by (i), or $s \equiv 0 \pmod p$ by (ii). Thus $Z = \langle a^p \rangle$ and $|Z| = p^{m-2}$. If $a^s b^t \in G - Z$, then two conjugates are equal iff $a^{r(s,t)p^{m-2}} = a^{q(s,t)p^{m-2}}$ or $r(s,t) \equiv q(s,t) \pmod p$. It follows that $|Cl(a^s b^t)| \leq p$. Since $a^s b^t \notin Z$, the $p^m - p^{m-2}$ elements of G split into $(p^m - p^{m-2})/p = p^{m-1} - p^{m-3}$ conjugate sets of p elements each. Therefore $k = p^{m-2} + (p^{m-1} - p^{m-3})$.

Q.E.D.

Combining Theorems 10.1 and 10.2, we have the following theorem which gives the relation between the order of a 2-group and the number of its conjugate sets.

Theorem 10.3. If G is a non-Abelian 2-group of order 2^m $(m \geq 3)$ which contains a cyclic subgroup of index 2, then $2^m \leq 4(k(G) - 3)$, where $k(G)$ is the class number of G.

Proof. Let S be the set of non-Abelian 2-groups H such that H has a cyclic subgroup of index 2. Then $G \in S$, and $|G| = g = 2^m$. By Theorems 10.1 and 10.2, $k(G) = 2^{m-2} + 3$ or $2^{m-1} + 2^{m-2} - 2^{m-3}$; and $2^{m-2} + 3 \leq 2^{m-2} + 3(2^{m-3}) = 2^{m-1} + 2^{m-2} - 2^{m-3}$. Define the mapping $f_S : \{|H| \mid H \in S\} \longrightarrow J^+$ by $f_S(|H|) = |H|/4 - 3$. Then $f_S(|H|) \leq k(H)$ for all $H \in S$. Clearly f_S is strictly monotonic increasing real valued function. Hence for any k in the range of f_S, $f_S^{-1}(k)$ is an upper bound for the order of any $H \in S$ such that $k(H) \leq k$. Therefore $g = 2^m \leq f_S^{-1}(k(G)) = 4(k(G) - 3)$.

Q.E.D.

Theorem 10.4. Let G be a 2-group of order 2^m, $k(G)$ the class number of G; and let r be any given natural number. Then $k(G) \leq r$ only if $m \leq (2r - 1)/3$.

Proof. Let $m = 2n - i$, where $n \in J_0^+$, $i = 0$ or 1. Then $k(G) \geq 3n + 2^i$ (Poland [1], p 91), and $3n + 2^i$

is equal to $3m/2 + 1$ or $3(m-1)/2 + 2$. Now $3(m-1)/2 + 2 = 3m/2 + 1/2 < 3m/2 + 1$. Therefore $k(G) \geq 3(m-1)/2 + 2$. With $r = 1$ or 2, and $k(G) \leq r$, $|G| = 1$ or 2 and the theorem is true.

Q.E.D.

The importance of least upper bound for the order of a group G, given k which is the class number of G, is reflected in the theory of group representations. It has been known that the number of irreducible representations of a group equals its class number (M. Hall [1] , p 267). Thus for example given a group G of order g, its class number must be greater than some minimum number t and so in searching for the irreducible representations of G one must have at least t. We now ask whether the result of Theorem 10.4 is a least upper bound for 2-groups. That is, given any number r, do there exist groups G with $k(G) \geq r$ and $|G| = 2^{(2k(G) - 1)/3}$? Such groups, by Theorem 10.4, would have minimum class number $k(G)$, and their orders would have odd exponent. First, suppose that $|G| = 2^1 = 2$. Then $(2k(G) - 1)/3 = 1$ implies that $k = 2$ and clearly the group $G = \langle x \mid x^2 = e \rangle$ has order 2 and class number 2. Second, if $|G| = 2^3 = 8$, then $(2k(G) - 1)/3 = 3$ implies that $k = 5$ and by Theorem 10.1, the quaternion and the dihedral groups satisfy this. Next suppose that $|G| = 2^5 = 32$. Then $(2k(G) - 1)/3 = 5$ implies that $k = 8$.

But no group of order 32 has class number less than 11 (M. Hall and Senior [1]). Since no list of groups of order $2^7 = 128$ exists, we cannot check further. But we have an indication that the result of Theorem 10.4 is not a least upper bound.

Poland [1] had attempted to establish a formula as a possible greatest lower bound for the class numbers of 2-groups whose order is greater than 16, and he had shown that if $|G| = 2^{2n+i}$, where $n \in J^+$, $i = 0$ or 1, $2n + i \geq 32$, then $k(G) \geq 3(n+1) + 2^i$. Since there is no group of order $2^8 = 256$ and having class number 16 (Poland [1] , p 114), so that the result obtained is nct a greatest lower bound. Thus the problem in finding a greatest lower bound for the class numbers of 2-groups still remains unsolved.

We next prove a theorem of Hirsch [1] restricted to p-groups.

Theorem 10.5. Let G be a p-group of order p^m, and k the class number of G. Then

$$p^m \equiv k \pmod{(p^2-1)} \quad \text{if } p \text{ is odd, and}$$

$$p^m \equiv k \pmod{3} \quad \text{if } p = 2.$$

Proof. For $x, y \in G$, consider the equation

$$x^{-1}y^{-1}xy = e. \qquad (1)$$

Suppose that $|Cl(x)| = p^r$. Then $|C(x)| = p^{m-r}$, and

hence the total number of solutions in G of the equation (1) is

$$\sum_{i=1}^{k} p^{r_i}(p^{m-r_i}) = kp^m$$

Among the solutions there occur $x = e$, $y = e$. For all other solutions consider the Abelian group $\langle x, y \rangle$. Suppose that $\langle x, y \rangle$ is cyclic of order p^r. Then the number of ways in which the group can be generated by two of its elements is

$$p^{2r} - p^{2r-2} = p^{2r-2}(p^2 - 1) \equiv 0 \pmod{(p^2-1)},$$

since either x or y must be of order p^r, and of the possible p^{2r} pairs we have to rule out only those in which the orders of both x and y are less than p^r. Next suppose that $\langle x,y \rangle$ is Abelian of type (p^{r_1},p^{r_2}). We distinguish two cases.

(i) Suppose that $r_1 = r_2$. Then x and y are independent generators of the group. This yields

$$(p^{2r_1} - p^{2r_1-2}) \left[(p^{2r_1} - p^{2r_1-2}) - (p^{r_1} - p^{r_1-1})\right]$$

choices, and this number is clearly $\equiv 0 \pmod{(p^2-1)}$.

(ii) Suppose that $r_1 > r_2$. Then either x is of order p^{r_1} and y of order p^{r_2} relative to $\langle x \rangle$ or vice versa. Hence we obtain

$$(p^{r_1-1})(p-1)p^{r_2-1})(p-1)(p^{r_1} + p^{r_1-1})$$

choices and again this number is $\equiv 0 \pmod{(p^2-1)}$. Since in all cases, the number of solutions of equation (1) which

are different from $x = e$, $y = e$ are $\equiv 0 \pmod{(p^2-1)}$, hence we have

$$kp^m \equiv 1 \pmod{(p^2-1)}.$$

Now, $p^2 \equiv 1 \pmod{(p^2-1)}$ and so $p^{2m} \equiv 1 \pmod{(p^2-1)}$. Therefore $p^m \equiv k \pmod{(p^2-1)}$. In particular, when $p = 2$, we have $2^m \equiv k \pmod 3$. This completes the proof.

Q.E.D.

11. Some Special 2-Groups.

In this section, we shall discuss some special types of 2-groups.

For elementary Abelian 2-groups, we have

Theorem 11.1. Let A be the elementary Abelian 2-group of order 2^m. Then every group G of order m is a subgroup of the group $\mathrm{Aut}(A)$.

Proof. We note that $\mathrm{Aut}(A)$ contains a subgroup which is isomorphic with the symmtric group S_m. By Cayley's theorem, every group G of order m is isomorphic with some subgroup of S_m. Therefore by law of transitivity, G is isomorphic with some subgroup of $\mathrm{Aut}(A)$.

Q.E.D.

In section 7 we have determined the order of $\mathrm{Aut}(A)$;

Burnside ([1] , p 117) has shown that this group is isomorphic with the linear homogeneous group, which is of great importance in many branches of analysis.

Another interesting property of elementary Abelian 2-groups is

Theorem 11.2. In an elementary Abelian 2-group of order 2^m, every element is of order 2 except the identity. Conversely, a group of order 2^m such that every element is of order 2 except the identity, is necessarily an elementary Abelian 2-group.

Proof. First statement follows directly from the definition of elementary Abelian group. Now suppose that for all $a, b \in G$, $a^2 = e$, $b^2 = e$. Then $a = a^{-1}$, $b = b^{-1}$, and $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$, so that G is Abelian. Clearly G is elementary Abelian since 2 is the smallest prime number (with the exception of 1).

Q.E.D.

This theorem does not apply to other classes of p-groups, where p is an odd prime, for there are non-Abelian p-groups all of whose elements, except the identity, have order p. For example a group of order p^4 with the defining relations

$$a^p = b^p = c^p = d^p = e, \quad d^{-1}cd = ca$$

is a non-Abelian group all of whose elements, except e, are

of order p (see Burnside [1] , p 143).

Theorem 11.3. Let G be an elementary Abelian group of order 2^m and let it possess an automorphism f of order 2. Then there is a subgroup H of G such that $|H| \geq \sqrt{2^m}$ and such that $f(x) = x$ for all $x \in H$.

Proof. Let $H = \{x \in G \mid f(x) = x\}$. Then H is a subgroup of G. For if $x, y \in G$ such that $f(x) = x$ and $f(y) = y$, then $f(xy^{-1}) = f(x)f(y^{-1}) = xy^{-1}$. Now let $z \in G - H$. Then $f(z) \in \langle z, H \rangle$. For if $f(z) = z'$, then since $|f| = 2$, $f(zz') = z'z = zz'$ so that $zz' \in H$ or $z' \in z^{-1}H = zH$. Hence for every element $x \in G - H$, $f(x) = xy$, where $y \in H$. Now if $f(x) = xy$ and $f(x') = x'y$, then $f(xx') = xyx'y = xx'y^2 = xx'$, so that $x' \in xH$, and conversly. Therefore $[G:H] \leq |H|$; that is $(|H|)^2 \geq 2^m$ or $|H| \geq \sqrt{2^m}$.

Q.E.D.

We quote M. Hall and Senior [1] for the definition of capable groups.

Definition 11.1. A group is called capable if it can function as a group of inner automorphisms of some other group.

Theorem 11.4. Let G be an elementary Abelian 2-group of order 2^m ($m \geq 2$). Then G is capable.

The proof of this theorem follows from a lemma which was proved by M. Hall and Senior ([1] , p 13).

Lemma. Let $H = \langle x_1, \ldots, x_r \rangle$ and suppose that H contains an element $a \neq e$ such that $a \in \langle x_i \rangle$ for each i, then there exists no group G with $G/Z \approx H$.

Proof. We assume the contrary and suppose that f is an isomorphism of G/Z onto H such that $f(a) = Zb$, $f(x_i) = Zy_i$, $i = 1, \ldots, r$. Then since $a \in \langle x_i \rangle$, $a = x_i^{m_i}$ for some $m_i \in J^+$, and so $f(a) = f(x_i)^{m_i} = Zy_i^{m_i} = Zb$, which implies that $by_i^{-m_i} \in Z$. Therefore $by_i = y_i b$ for each i. But $G = \langle Z, y_1, \ldots, y_r \rangle$. Hence $b \in Z$ so that $f(a) = Zb = Z$ implies that $a = e$, which is a contradiction.

Q.E.D.

Corollary 11.5. If G is a finite Abelian group, then G is capable iff its two largest invariants are equal.

Proof. For suppose that $G = \langle x_1 \rangle \times \ldots \times \langle x_r \rangle$ with x_i of order n_i and that $n_{i+1} \mid n_i$ $(i = 1, \ldots, r-1)$. If $n_1/n_2 > 1$, write $y_1 = x_1$ and $y_i = x_1 x_i$, $i > 1$, and let $u = y_1^{n_2}$. Then $G = \langle y_1, \ldots, y_r \rangle$ with $u \neq e$ and $u = y_i^{n_2}$ for each i. Therefore G is incapable. Conversely, if G is capable, then its two largest invariants must be identical.

Q.E.D.

Proof of Theorem 11.4. This follows directly from corollary 11.5.

Q.E.D.

The smallest elementary Abelian 2-group is of course the cyclic group of order 2. This group is also the Sylow 2-group of S_3. The elementary Abelian 2-group of order 4 is the four-group, also called the quadratic group, and is denoted by V_4. This group is a Sylow 2-subgroup of A_4 and A_5. With regard to A_4, V_4 is the only Sylow 2-subgroup since it is invariant in A_4. With regard to A_5, it has five conjugate subgroups. The four-group functions as the group of inner automorphisms of those class 2 groups which have at least one Abelian subgroup of index 2 and whose commutator subgroups are of order 2 (see M. Hall and Senior [1]).

We next discuss the dihedral and generalized quaternion groups. We recall the dihedral group of order $2m$ ($m > 1$) is generated by two elements a and b with defining relations

$$a^{m} = e, \quad b^2 = e, \quad bab^{-1} = a^{-1}.$$

For each $m > 1$, there is only one dihedral group of order $2m$. All dihedral groups, except the four-group, are non-Abelian.

We also recall the generalized quaternion group of order 2^m ($m \geq 3$) is generated by two elements a and b with defining relations

$$a^{2^{m-1}} = e, \quad b^2 = a^{2^{m-2}}, \quad bab^{-1} = a^{-1}.$$

When $m = 3$, we have the quaternion group of order 8.

The dihedral and quaternion groups of order 8 possess several properties in common as well as properties which are not. When we consider their structure, we find

(1) Both are non-Abelian groups all of whose subgroups are Abelian.

(2) Both contain at least one cyclic subgroup of order 4.

(3) In each of these groups, the center and the commutator subgroup are identical.

(4) Every subgroup of the quaternion group is normal (such a group is called Hamiltonian). On the other hand, not every subgroup of the dihedral group is normal.

We quote Schenkman ([1] , p 91) for the definition of split extension.

Definition 11.1. A group is called a split extension of its subgroup H by its subgroup K if (i) $H \lhd G$, (ii) $HK = G$; (iii) $H \cap K = E$.

(5) The dihedral group contains five elements of order 2, and is a split extension of a cyclic group of order 4 by a cyclic group of order 2. It is the Sylow subgroup of S_4, S_5, A_6, and A_7. On the other hand, the quaternion group contains only one element of order 2 (Theorem 8.2); this element is expressed as a power of some other element of order 4, hence the quaternion group is not a split extension of any

of its subgroups.

We proceed to give more properties of these two groups.

Theorem 11.6. The dihedral and quaternion groups cannot function as the Frattini subgroup of any p-group.

Proof. This follows directly from Theorem 5.13.

Q.E.D.

Theorem 11.7. The quaternion group Q is incapable.

Proof. Since Q contains element $b^2 = a^2 \neq e$, hence by the lemma of Theorem 11.4, Q is incapable.

Q.E.D.

From this theorem, it follows that every Hamiltonian group is incapable, while every dihedral group is capable.

For 2-groups of higher orders, the dihedral, generalized quaternion, and semi-dihedral groups are of special interest owing to their unusual properties which have already been discussed in various sections. In addition to these, we finally note that the semi-dihedral group of order 2^m $(m > 3)$ is the Sylow subgroup of the automorphism group of the Abelian group of order p^2 and type (1,1), where $p \equiv 2^{m-2} - 1 \pmod{2^{m-1}}$; moreover, every normal subgroup is characteristic.

I2. Summary.

In year 1872, Sylow first showed that for every natural prime p dividing the order of a finite group G, there is contained in G at least one Sylow p-subgroup; all Sylow p-subgroups are conjugate and the number of such subgroups is $\equiv 1 \pmod{p}$. The study of groups of arbitrary order is thus focus to those groups whose orders are powers of prime numbers, also called p-groups.

The most fundamental property of a p-group is that it has a non-trivial center and that its central quotient group possesses the same property. This is in contrast with the symmetric group S_n which is centerless. In studying the properties of p-groups more closely, two important central series possessed by a p-group were derived, namely: the upper and the lower central series. The relation between these two series was shown by Theorem 5.15.

The importance of the Frattini subgroup of a p-group is reflected in determining the nilpotency of a group. It has been shown (Theorem 5.4) that the Frattini subgroup of a nilpotent group contains the commutator subgroup. Conversely, if the Frattini subgroup of a finite group contains the commutator subgroup, then the group is nilpotent.

The usefulness of the Burnside's basis theorem is

made clear by its application in obtaining a limitation for the order of the automorphism group of a p-group.

Of all classes of p-groups, the 2-groups are of special interest owing to their structure which is different from other classes of p-groups. These 2-groups are classified by a method suggested by Burnside [1] . The class provides an excellent method in classifying groups of order 16. As a result, there are just three groups of order 2^m ($m > 3$) and maximal class with commutator subgroup of type (m-2), and contain cyclic subgroups of type (m-1); these are the dihedral, generalized quaternion, and semi-dihedral groups.

The relation between the orders of 2-groups and their class numbers were discussed. In particular, the class numbers of the dihedral, generalized quaternion, and semi-dihedral groups were obtained.

The importance of the elementary Abelian 2-group of order 2^m is reflected in its automorphism group. It has been shown (Burnside [1] , p 116) that this automorphism group is isomorphic with the lenear homogeneous group which is of great importance in many branches of analysis. The dihedral and quaternion groups of order 8 were discussed.

Although most of the theorems and styles of proofs come from the authors listed in the bibliography, I note in particular that the proofs of Theorems 5.7; 5.8; 5.9; 5.11; 5.12; 11.1; 11.2; and Theorem 11.6 are my own work.

BIBLIOGRAPHY

Blackburn, N.

[1] " On Prime-Power Groups ", Proc. Camb. Phil. Soc. 53 (1957), 19-27.

Burnside

[1] Theory of Groups of Finite Order, 2nd ed., Dover, N.Y. (1955)

Dlab, V.

[1] " The Frattini Subgroups of Abelian Groups ", Czech. Math. J. 10 (1960), 1-16.

Gaschutz.

[1] " Uber die Φ-Untergruppe endlicher Gruppen ", Mat. Z. 58 (1953), 160-170.

Hall, P.

[1] " A Contribution to the Theory of Groups of Prime-Power Orders ", Proc. Lond. Math. Soc. 11 36 (1933), 29-95.

[2] " The Classification of Prime- Power Groups ", J. fur die reine u. ang. Math. 182 (1940), 130-141.

Hall, M.

[1] The Theory of Groups, N. Y., Macmillan, (1959).

Hall, M. and Senior, J.

[1] The Groups of Order 2^n ($n \leq 6$), N. Y., Macmillan, (1964).

Herstein, I. N. and Adney, J. E.

[1] " A Note on the Automorphism Group of a Finite Group ", Am. Math. Monthly, 59 (1952), 309-310.

Hirsch, K. A.

[1] " On a Theorem of Burnside ", Quart. J. Math., 1 (1950), 97-99.

Hobby C.

[1] " The Frattini Subgroup of a p-Group ", Pac. J. Math., 10 (1960), 209-212.

Ledermann.

[1] The Theory of Finite Groups, N. Y., Oliver and Boud, (1964).

Miller, G., Blichfeldt, Dickson.

[1] Finite Groups, N. Y., John Wiley and Sons, (1916).

Miller, G. and Moreno, H.

[1] " Non-Abelian Groups in Which Every Subgroup Is Abelian ", Trans. Am. Math. Soc. 4 (1903), 398-404.

Miller, G.

[1] " Determination of All the Groups of Order 64 ", Am. J. of Math. 52 (1930), 617-634.

Poland.

[1] On The Group Class Equation, Ph. D. 's thesis, McGill University, Math. Dept. (1966).

Rotman.

[1] The Theory of Group: An Introduction, Boston, Allyn and Bacon, (1965).

Schenkman.

[1] Group Theory, N. Y., D. Van Nostrand, (1965).

[2] " The Existence of Outer Automorphisms of Some Nilpotent Groups of Class 2 ", Proc. Amer. Math. Soc. 6 (1955), 6-11.

Scott.

[1] Group Theory, N. J., Prentice-Hall, (1964).

[2] " On the Order of the Automorphism Group of a Finite Group ", Proc. Amer. Math. Soc. 5 (1954), 23-24.

Zassenhaus.

[1] The Theory of Groups, N. Y., Chealsea, (1958), 2nd ed.