A PERMUTATION REPRESENTATION OF THE AUTOMORPHISMS OF A GROUP

Thesis for the Degree of Ph. D.
MICHIGAN STATE UNIVERSITY
MAX GILBERT GRUENDL
1969

This is to certify that the

thesis entitled

A PERMUTATION REPRESENTATION

OF THE AUTOMORPHISMS OF A GROUP

presented by

Max Gilbert Gruendl

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Mathematics

J. E. Adney
Major professor

Date 7/24/69

O-169

ABSTRACT

A PERMUTATION REPRESENTATION
OF THE AUTOMORPHISMS OF A GROUP

By

Max Gilbert Gruendl

This thesis investigates the permutation representation of the automorphisms of a group G on the composition and chief series of G denoted by $(A(G), C_G)$ and $(A(G), D_G)$, respectively. The problem is motivated by the thesis of A. Polimeni, Michigan State University, 1965, in which he considers the group G when $(A(G), C_G)$ is a transitive permutation group. We generalize in two directions: first since every chief series is a composition series, restrictions on the group G are found when $(A(G), D_G)$ is a transitive permutation group (Chapter II), and second we assume that $(A(G), C_G)$ is an intransitive permutation group (Chapter III).

In Chapter II the main results are:

(1) Let G be a nilpotent group. $(A(G), D_G)$ is a transitive permutation group if and only if G is isomorphic to one of the following groups:

(a) cyclic p-group for some prime p,

(b) elementary abelian p-group for some prime p,

(c) the quaternions,

(d) the group generated by a, b, and c where $a^p = b^p = c^p = [a,b] = [a,c] = 1$ and $[b,c] = a$ for some prime p, $p \neq 2$.

(2) If G is a supersolvable group but not nilpotent, and $(A(G), D_G)$ is a transitive permutation group then $G = G'S_q$ where G' is the normal p-Sylow subgroup of G and S_q is a non-normal q-Sylow subgroup of G where $p > q$ and such that

(a) $G' = \mathrm{Fit}(G)$,

(b) S_q is elementary abelian or cyclic,

(c) $\Phi(G)$ is the largest characteristic subgroup of G contained in G',

(d) if, in fact, G' is abelian then $Z(G) = (1)$.

(3) If G is a solvable group and $(A(G), D_G)$ is a transitive permutation group then the following are true:

(a) $\mathrm{Soc}^{n+1}(G)/\mathrm{Soc}^{n}(G)$ is an elementary abelian p-group.

(b) If K is a characteristic subgroup of G then there is an integer n such that $K = \mathrm{Soc}^{n}(G)$.

(c) $G^{(t)}/G^{(t+1)}$ is an abelian p-group and, in particular, G/G' is elementary abelian or cyclic.

(d) Fit(G) is a p-group, and there is an integer n such that $G^{(n)} = \mathrm{Fit}(G)$.

(e) There is no characteristic subgroup between $\Phi(G)$ and $\mathrm{Fit}(G)$ so that $\Phi(\mathrm{Fit}(G)) \leq \Phi(G)$.

(f) If $Z(G) \neq (1)$ then $Z(\mathrm{Fit}(G)) \geq Z(G) \geq \mathrm{Soc}(G)$.

(g) If $L_0 > L_1 > \ldots > L_n = (1)$ is the lower nilpotent series of G then L_i/L_{i+1} is a p-group for some prime p, and L_0/L_1 is isomorphic to one of the four groups of (1).

Chapter III is divided into three sections. The first section contains basic results which are used in the other two sections. In the second section $(A(G), C_G)$ is assumed to be intransitive, that is,

$n(G) \geq 2$ where $n(G)$ is the number of orbits of $(A(G), C_G)$. The results are restricted to p-groups.

(4) If G is a p-group, G/Z_{m-2} is not the quaternions, and $m = d(G)$ then $n(G) \geq d(G)$ where $d(G)$ is the class of G.

(5) If G is a p-group, Q_n is not isomorphic to $H < G$ for $n \geq 3$, and $n(G) \geq 2$ then the exponent of $G \leq p^{n(G)}$.

(6) If G is a p-group such that $Z(G)$ is not cyclic then the exponent of $G \leq p^m$ where m is the largest solution of $n(G) \geq (m + p-1)!/p!(m-1)!$.

(7) If G is a p-group such that $n(G) \geq 2$, $Z(G)$ is cyclic, and if $H \leq G$ then H is not isomorphic to the quaternions or the generalized quaternions then the exponent of $G \leq p^{n(G)-1}$.

The third section considers the case when $n(G) = 2$. Since G must either be a t-group or not a t-group we apply results about t-groups when G is a t-group and (3) when G is not a t-group to obtain the following results.

(8) Let G be a nilpotent group. Then $n(G) = 2$ if and only if G is isomorphic to H where H is the group of (1d) or a cyclic group of order the product of two distinct primes.

(9) If G is solvable, not a t-group, $(A(G), D_G)$ is transitive, and $n(G) = 2$ then G satisfies (3a), (3b), (3d), (3e), and (3f), and (3c) and (3g) are replaced by (c) and (g) below:

(c) $G^{(t)}/G^{(t+1)}$ is an elementary abelian or cyclic p-group,

(g) If $L_0 > L_1 > \ldots > L_n = (1)$ is the lower nilpotent series of G then L_i/L_{i+1} is isomorphic to a cyclic p-group, an elementary abelian p-group, the quaternions, or H where H is the group mentioned in (1d). Also only one of the factors of the lower nilpotent series is isomorphic to H.

(10) Let G be a solvable, non-nilpotent t-group where G/L is the maximal nilpotent factor group of G. $n(G) = 2$ if and only if G has one of the following three sets of properties.

(a) G/L is a cyclic group of order q^m, $m \geq 2$, $|C(L)| = pq$ and $|L| = p$.

(b) G/L is a cyclic group of order qr, L is a cyclic p-group, and $C(L) = L$.

(c) G/L is a cyclic group of order qr, L is an elementary abelian p-group, and $C(L) = L$.

In all cases p, q, and r are distinct primes.

A PERMUTATION REPRESENTATION
OF THE AUTOMORPHISMS OF A GROUP

By

Max Gilbert Gruendl

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1969

G 60302
2-2-70

To Jo Ann, Robert, and Elizabeth

ACKNOWLEDGMENTS

The author is deeply indebted to his major professor, Dr. J.E. Adney for his patience and guidance in the preparation of this thesis. Our discussions about the research leading to this thesis were of immeasurable value to me.

TABLE OF CONTENTS

LIST OF FIGURES

INDEX OF NOTATION

I. <u>Relations</u>:

$H \leq G$	H is a subgroup of G.
$H < G$	H is a proper subgroup of G.
$A \subseteq B$	A is a subset of B.
$A \subset B$	A is a proper subset of B.
$H \triangleleft G$	H is a normal subgroup of G.
$H \triangleleft\triangleleft G$	H is a subnormal subgroup of G.
$H \cong K$	H is isomorphic to K.
$H \cong_{A(G)} K$	H is $A(G)$-isomorphic to K (page 20).
$x \equiv y \bmod z$	x equals y modulo z.
$x \in G$	x is an element of G.

II. <u>Operations</u>:

G^{α}	The image of G under $\alpha \in A(G)$.
g^{α}	The image of g under $\alpha \in A(G)$.
g^{x}	$x^{-1} g x$.
G/H	The factor group of G by H.
$\lvert G:H \rvert$	The index of H in G.
$(a,b,\ldots)$	The group generated by $a,b,\ldots$.
$\{a,b,\ldots\}$	The set containing $a,b,\ldots$.
$\lvert G \rvert$	The order of the group G.
$\lvert g \rvert$	The order of $g \in G$.
(ℓ,k)	The greatest common divisor of ℓ and k.
$n(G)$	page 16.
$\bar{n}(G)$	page 20.

$C_{m,n}$	The number of combinations of m things taken n at a time.
$\ell(G_i,c)$	page 17.
$\mu(G_i,c)$	page 17.

III. <u>Groups</u>: G is a group and $H \leq G$.

$A(G)$	The automorphism group of G.
$I(G)$	The inner automorphism group of G.
$N(H)$	$\{g \in G \mid H^g = H\}$
$C(H)$	$\{g \in G \mid h^g = h$ for all $h \in H\}$
$Z(G)$	$C(G)$
$\Phi(G)$	The intersection of the maximal subgroups of G.
$Fit(G)$	The maximal normal nilpotent subgroup of G.
$Soc(G)$	The subgroup of G generated by the minimal normal subgroups of G.
$Soc^n(G)$	page 11.
$[a,b]$	$a^{-1}b^{-1}a\,b$.
$[H,K]$	$([h,k] \mid h \in H$ and $k \in K)$.
G'	$[G,G]$.
$G^{(n)}$	$G^{(1)} = G'$ and $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$.
C_G	The set of all composition series of G.
D_G	The set of all chief series of G.
$(A(G), C_G)$	page 3.
$(A(G), D_G)$	page 3.
$\begin{pmatrix} m_1 & & m_s \\ t_1 & ,\dots, & t_s \end{pmatrix}$	page 27.
$\left[\begin{pmatrix} m_1 & & m_s \\ t_1 & ,\dots, & t_s \end{pmatrix}\right]$	page 27.
Q_n	page 21.

INTRODUCTION

This thesis is concerned with the problem of describing a group G given the number of orbits of the permutation representation of the automorphisms of G on the composition or chief series. The problem was first considered by A. Polimeni [4] in his thesis where he considered the case when the permutation representation of the automorphisms of G on the composition series is transitive, that is, it has one orbit.

From this starting point we may generalize in two directions. Since the set of chief series is contained in the set of composition series, Chapter II considers G when the permutation representation of the automorphisms on the chief series is transitive from which results similar to Polimeni's are proven. In Chapter III, we take another point of view and investigate G when the permutation representation of the automorphism of G on the composition series is intransitive. The basic definitions of these permutation representations and two examples are contained in Chapter I.

For easy reference the Appendix lists known theorems by capitol Roman letters. Theorem A, Theorem B, etc. which are utilized in the text of the thesis. The Index of Notation should be consulted for the exact meaning of symbolism appearing throughout the thesis.

The results are either called theorems or lemmas and are numbered in the same sequence by chapter, section, and order of appearance. For example, the fourth result in the first section of the third chapter is designated as Theorem 3.1.4. The definitions and examples are numbered similarly.

CHAPTER I

BASIC DEFINITIONS AND SOME EXAMPLES

In this chapter we introduce the definitions of two permutation groups associated with a group G and give some examples to acquaint the reader with the type of problem with which we will be concerned.

Before proceeding further all groups in this thesis are assumed to be finite.

The main idea is to study groups through investigating how their automorphism group acts as permutations on certain sets of objects associated with the group, namely, the set of chief series and composition series of the group. We let

$$s: G = G_0 > G_1 > \dots > G_{n-1} > G_n = (1) \qquad (*)$$

mean that s is a chain of subgroups of the group G which consists of the subgroups $G_0, G_1, \dots, G_n$. It will be convenient to say that a subgroup H is contained in a chain s given by (*) if $G_i = H$ for some i. The first definition shows how an automorphism acts on a chain.

<u>Definition 1.1.1</u>. Let s be a chain of a group G as in (*). Then s^α is defined to be the chain of G given by

$$s^\alpha: G = G_0^\alpha > G_1^\alpha > \dots > G_{n-1}^\alpha > G_n^\alpha = (1).$$

<u>Definition 1.1.2</u>. Let s be a chain of a group G as in (*). Then s is a composition series of G if G_i is a maximal normal subgroup of G_{i-1} for $i = 1, \dots, n$, and s is a chief series of G

if G_i is a maximal subgroup of G_{i-1} which is normal in G.

Note that if G is a group then all composition series of G have the same length [5, page 37].

Let C_G and D_G denote the set of composition and chief series, respectively. Then the facts that $s \in C_G$ implies that $s^\alpha \in C_G$ and $s \in D_G$ implies that $s^\alpha \in D_G$, $\alpha \in A(G)$, allows us to consider the permutation representation of $A(G)$ on C_G and D_G.

Definition 1.1.3. Let $(A(G), C_G)$ be the permutation representation on C_G defined as follows: if $\alpha \in A(G)$ and $s \in C_G$ then s^α is the image of s under the permutation induced by α which is denoted by π_α. $(A(G), D_G)$ is defined as above with D_G substituted for C_G and σ_α denotes the permutation induced by α.

Let K_{C_G} and K_{D_G} be the kernels of the homomorphisms of $A(G)$ onto $(A(G), C_G)$ and $(A(G), D_G)$ defined by α maps to π_α and α maps to σ_α. Clearly

$$K_{C_G} = \{\alpha \in A(G) \mid H^\alpha = H \text{ for all } H \lhd \lhd G\}$$

$$K_{D_G} = \{\alpha \in A(G) \mid H^\alpha = H \text{ for all } H \lhd G\}$$

which implies that

$$K_{C_G} \le K_{D_G} \text{ and } I(G) \le K_{D_G}.$$

The first inclusion implies that $(A(G), D_G)$ is a homomorphic image of $(A(G), C_G)$, and the second inclusion implies that in the case of $(A(G), D_G)$ we are considering in some sense only automorphisms of G which are not inner automorphisms.

The following two examples will be investigated as regards the transitivity of $(A(G), D_G)$ and $(A(G), C_G)$.

Example 1.1.1. $Q_3 = (a,b)$ where $a^4 = b^4 = 1$ and $a^2 = b^2 = [a,b]$. $C_{Q_3} = D_{Q_3} = \{s_1, s_2, s_3\}$ where

$$s_1\colon G > (a) > (a^2) > (1)$$

$$s_2\colon G > (b) > (a^2) > (1)$$

$$s_3\colon G > (ab) > (a^2) > (1).$$

$(A(Q_3), C_{Q_3})$ is a transitive permutation group since if α and β are defined by $a^\alpha = b$, $b^\alpha = a$, $a^\beta = a$, and $b^\beta = ab$ then $\alpha, \beta \in A(Q_3)$, and $s_1^\alpha = s_2$ and $s_2^\beta = s_3$. $(A(Q_3), C_{Q_3})$ is the symmetric group on three symbols.

Q_3, of course, is the quaternions and will be shown to be the "exceptional case" to the results of Chapter III. Another important example for both Chapter II and III is the non-abelian group of order p^3 of exponent p which is exhibited below.

Example 1.1.2. Let $G = (a,b,c)$ where $a^p = b^p = c^p = [a,b] = [a,c] = 1$ and $[b,c] = a$. The center of G is (a), and D_G consists of the $p+1$ composition series containing (a). $(A(G), D_G)$ can be shown to be a transitive permutation group. Now $(A(G), C_G)$ has two orbits, one consisting of the elements of D_G and the other consisting of the other composition series, that is, those not containing (a).

Example 1.1.3. $G = (a,b)$ where $a^4 = b^4 = 1$ and $[a,b] = a^2$. $Z(G) = (a^2)$. The composition series of G are

$$s_1\colon G > (a^2,b) > (b) > (1)$$

$$s_2\colon G > (a^2,b) > (a^2b) > (1)$$

$$s_3\colon G > (a^2,b) > (a^2) > (1)$$

$$s_4\colon G > (a) > (a^2) > (1)$$

$$s_5\colon G > (a^2, ab) > (a^2) > (1)$$

$$s_6\colon G > (a^2, ab) > (ab) > (1)$$

$$s_7\colon G > (a^2, ab) > (a^3 b) > (1)$$

$D_G = \{s_3, s_4, s_5\}$. $(A(G), C_G)$ has the three orbits $\{s_1, s_2, s_6, s_7\}$, $\{s_3, s_5\}$, and $\{s_4\}$ while $(A(G), D_G)$ has the two orbits $\{s_3, s_5\}$ and $\{s_4\}$.

CHAPTER II

THE GROUP $(A(G), D_G)$

On the assumption that $(A(G), D_G)$ is a transitive permutation group we establish restrictions on the group G when G is abelian, nilpotent, supersolvable, and solvable.

<u>Theorem 2.1.1</u>. Let G be an abelian group. Then $(A(G), D_G)$ is a transitive permutation group if and only if G is a cyclic p-group or an elementary abelian p-group for some prime p.

Proof: The theorem follows from Theorem A since $C_G = D_G$ when G is abelian.

In order to consider the case where G is nilpotent we prove the following two lemmas.

<u>Lemma 2.1.2</u>. If G is a group of order p^n, $n \geq 4$, then G contains an abelian subgroup of order p^3.

Proof: It is sufficient to take G to have order p^4 and non-abelian. Assume that G has no abelian subgroup of order p^3. By considering a refinement of the upper central series we see that there is a normal abelian subgroup X of G such that $|X| = p^2$. $C(X) = X$ since X is abelian, and if $C(X) > X$ then for any $y \in C(X)$ but $y \notin X$ (X,y) would be abelian of order greater than p^2. Therefore $G/X = N(X)/C(X)$ is isomorphic to a subgroup of $A(X)$. But $p^2 = |G/X|$ does not divide $|A(X)|$ since if X is elementary abelian then $|A(X)|$ divides $(p^2 - p)(p^2 - 1)$, if X is cyclic and $p = 2$ then $|A(X)| = 2$, and if X is cyclic and $p \neq 2$ then $|A(X)| = p(p-1)$. (See Scott [5, pages 120 and 161]). Therefore we have reached a contradiction and the lemma is proven.

Lemma 2.1.3. Let G be a p-group. Then all normal subgroups of the same order are isomorphic if and only if G is isomorphic to one of the following groups:

1. cyclic p-group for some prime p,
2. elementary abelian p-group for some prime p,
3. the quaternions, that is, (a,b) such that $a^4 = b^4 = 1$ and $a^2 = b^2 = [a,b]$,
4. (a,b,c) where $a^p = b^p = c^p = [a,b] = [a,c] = 1$ and $[b,c] = a$ for some prime p, $p \neq 2$.

Proof: Clearly the four groups listed in the lemma have all normal subgroups of the same order isomorphic.

Now let G be a p-group such that all normal subgroups of the same order are isomorphic. If G is abelian then it is clear that G is elementary abelian or cyclic, so we assume that G is not abelian. This implies that $|G| \geq p^3$.

Case 1. If $|G| = p^3$ then since the non-abelian p-groups of order p^3 are well-known [1, pages 145-146], we see that the two groups mentioned in 3 and 4 are the only groups satisfying the hypothesis.

Case 2. $|G| > p^3$. We now show that there are no non-abelian p-groups of order p^n, $n > 3$, satisfying the hypothesis of the lemma by induction on n. If $n = 4$, the non-abelian groups of order p^4 are well-known [1, pages 145-146], and it is easily checked that none of them satisfy the hypothesis. Assume $n > 4$ and that no non-abelian group of order p^{n-1} satisfies the hypothesis. Let K be a non-abelian group of order p^n satisfying the hypothesis. Since K is a p-group $Z(K) \neq (1)$, so there is a normal subgroup H of K such that $H \leq Z(K)$

and $|H| = p$. Consider K/H. $|K/H| = p^{n-1}$ and all normal subgroups of the same order of K/H are isomorphic. Therefore K/H is abelian by the induction hypothesis, and so K/H is cyclic or elementary abelian since K/H satisfies the hypothesis of the lemma. Since $H \leq Z(K)$, K/H cannot be cyclic or $K/Z(K)$ would be cyclic. Therefore K/H is elementary abelian and $H = K'$. All subgroups of K/H are normal so that all subgroups of K containing H are normal in K. By Lemma 2.1.2 there is an abelian subgroup A of K of order p^3. Let $A^* = (A,H)$. Clearly A^* is a normal abelian subgroup of K with $|A^*| \geq p^3$ since $H \leq A^*$ and $H \leq Z(K)$. Now we proceed to find a normal non-abelian subgroup of K with the same order as A^*. There are two elements k_1 and k_2 of K such that $[k_1,k_2] \neq 1$ since K is not abelian. $|(k_1,k_2)| = p^3$ since $(k_1,k_2) \geq H = K'$ and $|(k_1,k_2)/H| = |(k_1H,k_2H)| = p^2$. Let B^* be a subgroup of K of the same order as A^* which contains (k_1,k_2). B^* is normal non-abelian since $B^* \geq (k_1,k_2) > H$. Therefore all groups K of order p^n, $n > 3$, must be abelian in order to satisfy the hypothesis, and so the group G of Case 2 cannot exist.

<u>Theorem 2.1.4</u>. Let G be a nilpotent group. $(A(G), D_G)$ is a transitive permutation group if and only if G is isomorphic to one of the four groups of Lemma 2.1.3.

Proof: The groups mentioned in Lemma 2.1.3 are all p-groups so that they are all nilpotent. By Theorem 2.1.1 $(A(G), D_G)$ is a transitive permutation group if G is a cyclic or elementary abelian p-group. In Example 1.1.1 we have shown that $(A(G), D_G)$ is a transitive permutation group if G is the quaternions. Now suppose that G is the group of 4, that is, $G = (a,b,c)$ where

$a^p = b^p = c^p = [a,b] = [a,c] = 1$, and $[b,c] = a$. There are $p+1$ chief series of G, namely,

$$s : G > (a,b) > (a) > (1)$$

$$s_n : G > (a,b^n c) > (a) > (1) \quad \text{for} \quad n = 0,1,\ldots,p-1.$$

Let α_n, $n = 0,1,\ldots,p-1$ be the automorphism defined as follows:

$$\alpha_0 \begin{cases} a \to a^{-1} \\ b \to c \\ c \to b \end{cases}, \quad \alpha_n \begin{cases} a \to a^n \\ b \to b^n c \\ c \to c \end{cases} \quad \text{for} \quad n = 1,\ldots,p-1.$$

Now $s^{\alpha_n} = s_n$ for $n = 0,1,\ldots,p-1$, and this shows that $(A(G),\ D_G)$ is a transitive permutation group.

To show the converse we assume that G is nilpotent, and $(A(G),\ D_G)$ is a transitive permutation group. G is a p-group because if P and Q are a p-Sylow and a q-Sylow subgroup of G, respectively, then P and Q are characteristic subgroups of the nilpotent group G, but this contradicts the transitivity of $(A(G),\ D_G)$. $(A(G),\ D_G)$ being a transitive permutation group implies that all normal subgroups of the same order are isomorphic, and this allows us to apply Lemma 2.1.3 to finish the proof.

In order to consider the situation where G is supersolvable it is easier to first look at G solvable. The following lemmas help us to reach this end.

<u>Lemma 2.1.5</u>. If G is a group such that $(A(G),\ D_G)$ is a transitive permutation group then $H \lhd G$, $K \lhd G$, $H < K$, and K/H nilpotent implies that K/H is a p-group for some prime p.

Proof: Suppose that $|K/H|$ is divisible by two primes p and q, and let $\overline{P} = P/H$ and $\overline{Q} = Q/H$ be the p-Sylow and q-Sylow subgroups of K/H, respectively. Since K/H is nilpotent P/H and Q/H are characteristic subgroups of K/H. Since $K/H < G/H$, P/H and Q/H are normal in G/H and we have that P and Q are normal subgroups of G. $(A(G), D_G)$ cannot be a transitive permutation group since there are two chief series which are refinements of the normal series $G > P > H > (1)$ and $G > Q > H > (1)$. So we must have that K/H is a p-group for some prime p.

<u>Lemma 2.1.6</u>. Let G be a group such that $(A(G), D_G)$ is a transitive permutation group. Then the following are true:

1. If H is a characteristic subgroup of G, then every chief series is a refinement of the normal series $G > H > (1)$.
2. If H is a characteristic subgroup of G and $K \lhd G$ then either $K \leq H$ or $K \geq H$.
3. If $(1) = H_0, H_1, H_2, \ldots, H_n = G$ are all the characteristic subgroups of G, then every chief series is a refinement of the normal series

$$G = H_n > H_{n-1} > \ldots > H_1 > H_0 = (1).$$

The H's may need to be renumbered.

Proof: 1. Let s be a chief series of G not containing H. Then by the transitivity of $(A(G), D_G)$ there is an $\alpha \in A(G)$ such that s^{α} contains H. Now $s = s^{\alpha\alpha^{-1}}$ and $s^{\alpha\alpha^{-1}}$ contains H since $H^{\alpha^{-1}} = H$. This contradiction proves 1.

2. $K \lhd G$ and H characteristic in G implies there is a chief series containing K, and by part 1 all chief series contain H so that $K \leq H$ or $K \geq H$.

3. Part 2 implies that

$$G = H_n > H_{n-1} > \dots > H_1 > H_0 = (1).$$

(The H's will probably have to be renumbered.) Part 1 implies that every H_i must be contained in every chief series which gives us that every chief series is a refinement of the normal series containing all characteristic subgroups of G.

<u>Lemma 2.1.7</u>. Let H be a characteristic subgroup of G. If $(A(G), D_G)$ is a transitive permutation group then $(A(G/H), D_{G/H})$ is also.

Proof: Let $\bar{s}$ and $\bar{s}^*$ be two chief series of G/H. We must produce an automorphism of G/H that maps $\bar{s}$ to $\bar{s}^*$. Let s and s^* be chief series of G which are refinements of the normal series consisting of the preimages of the groups of $\bar{s}$ and $\bar{s}^*$ respectively. Since $(A(G), D_G)$ is transitive then there is an $\alpha \in A(G)$ such that $s^\alpha = s^*$. $\bar{\alpha}$ defined by $(xH)^{\bar{\alpha}} = x^\alpha H$ is an automorphism of G/H, and $\bar{s}^{\bar{\alpha}} = \bar{s}^*$ which proves the theorem.

The converse of Lemma 2.1.7 is not true because an automorphism of G/H cannot, in general, be extended to an automorphism of G.

<u>Definition 2.1.1</u>. The sockel, $Soc(G)$, of a group G is the subgroup generated by all its non-trivial minimal normal subgroups. Also, let $Soc^n(G)$ be defined recursively as $Soc^0(G) = (1)$ and

$$Soc^{n+1}(G)/Soc^n(G) = Soc(G/Soc^n(G)).$$

From its definition the sockel of G is a characteristic subgroup of G. It can be shown that $Soc(G)$ is a direct product of some of the non-trivial minimal normal subgroups of G [5, page 168]. This, in the case where G is a solvable group, gives us that the $Soc(G)$ is a direct product of elementary abelian p-groups since the minimal normal subgroups of a solvable group are elementary abelian [5, page 74].

Lemma 2.1.8. $Soc^{n+1}(G) = (H|H$ is minimal with respect to being normal and properly containing $Soc^{n}(G))$.

Proof: The proof follows since if H is minimal with respect to being normal and properly containing $Soc^{n}(G)$, then $H/Soc^{n}(G)$ is a non-trivial minimal normal subgroup of $G/Soc^{n}(G)$, and conversely.

Theorem 2.1.4 assumes that G is nilpotent so in our investigation of G solvable the importance of the next definition is apparent.

Definition 2.1.2. Let G be a solvable group. Let L_i be defined recursively as $L_0 = G$, and L_i is the smallest normal subgroup of L_{i-1} such that L_{i-1}/L_i is nilpotent. The normal series

$$G = L_0 > L_1 > \ldots > L_n = (1)$$

is called the lower nilpotent series.

Theorem 2.1.9. If G is a solvable group and $(A(G), D_G)$ is a transitive permutation group then the following are true:

1. $Soc^{n+1}(G)/Soc^{n}(G)$ is an elementary abelian p-group.

2. If K is a characteristic subgroup of G then there is an integer n such that $K = Soc^{n}(G)$.

3. $G^{(t)}/G^{(t+1)}$ is an abelian p-group, and, in particular, G/G' is elementary abelian or cyclic.

4. The $Fit(G)$ is a p-group, and there is an integer n such that $G^{(n)} = Fit(G)$.

5. There are no characteristic subgroups between $\Phi(G)$ and $Fit(G)$ so that $\Phi(Fit(G)) \leq \Phi(G)$.

6. If $Z(G) \neq (1)$ then $Z(Fit(G)) \geq Z(G) \geq Soc(G)$.

7. If $L_0 > L_1 > \ldots > L_n = (1)$ is the lower nilpotent series of G, then L_i/L_{i+1} is a p-group for some prime p, and L_0/L_1 is isomorphic to one of the four groups of Lemma 2.1.3.

Proof: 1. Since G is a solvable group $G/\mathrm{Soc}^n(G)$ is a solvable group, and $\mathrm{Soc}(G/\mathrm{Soc}^n(G)) = \mathrm{Soc}^{n+1}(G)/\mathrm{Soc}^n(G)$ is the direct product of elementary abelian groups and therefore $\mathrm{Soc}^{n+1}(G)/\mathrm{Soc}^n(G)$ is abelian. By Lemma 2.1.5 $\mathrm{Soc}^{n+1}(G)/\mathrm{Soc}^n(G)$ is a p-group so that it is an elementary abelian p-group.

2. Let K be a characteristic subgroup of G. By Lemma 2.1.6 there is an integer n such that $\mathrm{Soc}^{n-1}(G) < K \leq \mathrm{Soc}^n(G)$. By Lemma 2.1.6 K contains all subgroups of G that are minimal with respect to being normal in G and properly containing $\mathrm{Soc}^{n-1}(G)$. But Lemma 2.1.8 implies that $K \geq \mathrm{Soc}^n(G)$ so that $K = \mathrm{Soc}^n(G)$.

3. $G^{(t)}/G^{(t+1)}$ is an abelian p-group by Lemma 2.1.5, and G/G' is elementary abelian or cyclic by Theorem 2.1.1 and Lemma 2.1.7.

4. Since $\mathrm{Fit}(G)$ is the maximal normal nilpotent subgroup of G, Lemma 2.1.5 implies that $\mathrm{Fit}(G)$ is a p-group. There is an integer n such that $G^{(n)} \leq \mathrm{Fit}(G) < G^{(n-1)}$ by Lemma 2.1.6. If $G^{(n)} < \mathrm{Fit}(G)$, since $|G^{(n-1)}/G^{(n)}|$ is a power of a prime, then $|G^{(n-1)}|$ is a p-group and is therefore nilpotent. This contradicts the definition of $\mathrm{Fit}(G)$. Therefore $G^{(n)} = \mathrm{Fit}(G)$.

5. Let $\Phi(G) = \mathrm{Soc}^n(G)$ which is possible by 2. By Theorem E, $\mathrm{Fit}(G) \geq \Phi(G)$. Theorem F gives us that $\mathrm{Fit}(G)/\Phi(G) = \mathrm{Soc}(G/\Phi(G))$. Therefore $\mathrm{Fit}(G)/\mathrm{Soc}^n(G) = \mathrm{Fit}(G)/\Phi(G) = \mathrm{Soc}(G/\Phi(G)) = \mathrm{Soc}(G/\mathrm{Soc}^n(G))$

$= \mathrm{Soc}^{n+1}(G)/\mathrm{Soc}^n(G)$, and so we have that

$\mathrm{Fit}(G) = \mathrm{Soc}^{n+1}(G)$. This along with 2 implies that there are no characteristic subgroups of G between $\mathrm{Fit}(G)$ and $\Phi(G)$. $\Phi(\mathrm{Fit}(G))$

is a characteristic subgroup of G properly contained in $Fit(G)$ so that $\Phi(Fit(G)) \leq \Phi(G) < Fit(G)$.

6. Let $Z(G) \neq (1)$. $Z(G) \geq Soc(G)$ since 2 implies that $Soc(G)$ is the smallest non-trivial characteristic subgroup of G: $Z(G) \leq Fit(G)$ since $Z(G)$ is abelian. Also $Z(G) = Fit(G) \cap Z(G) \leq Z(Fit(G))$ which gives us that $Z(Fit(G) \geq Z(G) \geq Soc(G)$.

7. L_i/L_{i+1} is nilpotent so that Lemma 2.1.5 implies that L_i/L_{i+1} is a p-group for some prime p. Lemma 2.1.7 implies that $(A(L_0/L_1), C_{L_0/L_1})$ is a transitive permutation group, and this along with Theorem 2.1.4 implies that L_0/L_1 is isomorphic to one of the four groups mentioned in Lemma 2.1.3.

Next we consider the case where G is supersolvable. Since supersolvable implies solvable, Theorem 2.1.9 will play a major role in the proof of Theorem 2.1.10.

Theorem 2.1.10. If G is a supersolvable group but not nilpotent, and $(A(G), D_G)$ is a transitive permutation group, then $G = G'S_q$ where G' is the normal p-Sylow subgroup of G, and S_q is a non-normal q-Sylow subgroup of G where $p > q$ and such that

1. $G' = Fit(G)$,
2. S_q is elementary abelian or cyclic,
3. $\Phi(G)$ is the largest characteristic subgroup of G contained in G',
4. if, in fact, G' is abelian then $Z(G) = (1)$.

Proof: 1. Theorem G implies that G' is nilpotent so that $G' \leq Fit(G)$. Theorem 2.1.9 says that there is an integer n such that $G^{(n)} = Fit(G)$. But $Fit(G)$ is not G since G is not nilpotent, and this gives us that $G' = Fit(G)$. $G' = Fit(G)$ must be a p-group for some prime p

by Theorem 2.1.9. G/G' is an elementary abelian or cyclic q-group by Theorem 2.1.9 where $q \neq p$ for otherwise G would be nilpotent. $p > q$ for by Theorem I, G has a normal Sylow subgroup for the largest prime, and if $q > p$ then G would be a direct product of two nilpotent groups which is nilpotent. Let S_q be a q-Sylow subgroup of G. Then $G = G'S_q$ and G/G' is isomorphic to S_q and this proves 2.

3. This follows directly from part 5 of Theorem 2.1.9.

4. G' abelian implies that all of G's Sylow subgroups are abelian, and so G is an A-group. (An A-group is a group whose Sylow subgroups are abelian. A-groups have been extensively studied by D.R. Taunt [6]). By Theorem J in an A-group $G' \cap Z(G) = (1)$. But this along with the facts that $G' = Fit(G)$ and $Z(G) \leq Fit(G)$ gives us that $Z(G) = G' \cap Z(G) = (1)$. This completes the proof.

The following example shows that the conclusions of Theorem 2.1.10 are not sufficient to imply that $(A(G), D_G)$ is a transitive permutation group. Polimeni [4] shows that the converse of Theorem C is true under very limited circumstances, and we could do the same here, but no new knowledge would be gained.

<u>Example 2.1.1</u>. Let $G = (a,b,c,d)$ where $a^9 = b^3 = c^3 = d^2 = [b,c] = 1$, $[a,b] = a^3$, $[a,c] = b$, $[a,d] = a^7$, $[b,d] = a^3$, and $[c,d] = c$. It may be seen that $(a,b) \lhd G$, $(a^3,b,c) \lhd G$, and $|(a,b)| = |(a^3,b,c)|$ but clearly this implies that $(A(G), D_G)$ is not a transitive permutation group.

CHAPTER III

$(A(G),\ C_G)$ INTRANSITIVE

In his thesis [4], Polimeni investigated a group G where $(A(G),\ C_G)$ was assumed to be a transitive permutation group, and in Chapter II we have looked at G when $(A(G),\ D_G)$ is a transitive permutation group. Chapter III's purpose is to consider G where $(A(G),\ C_G)$ is not a transitive permutation group. Of course, this is a much more difficult problem and in order to attack this problem the hypothesis had to be further restricted.

Chapter III is divided into three sections: Basic Properties of $n(G)$, $n(G)$ for G a p-group, and $n(G) = 2$. Here $n(G)$ denotes the number of orbits of $(A(G),\ C_G)$.

3.1. Basic Properties of $n(G)$.

Definition 3.1.1. An orbit of $(A(G),\ C_G)$ is $\{s^{\alpha} \mid \alpha \in A(G) \text{ and } s \in C_G (s \text{ fixed})\}$.

It is well-known that the set of orbits of a permutation group form a partition so that the set of orbits of $(A(G),\ C_G)$ form a partition of C_G.

Definition 3.1.2. Let $n(G)$ denote the number of orbits of $(A(G),\ C_G)$.

If $n(G) = 1$ then $(A(G),\ C_G)$ is a transitive permutation group and conversely.

The following results are lower bounds on the number of orbits of $(A(G),\ C_G)$ depending on the structure of the lattice of subnormal subgroups of G. To do this we need the following definition.

Definition 3.1.3. If $c: G = G_m > G_{m-1} > \dots > G_1 > G_0 = (1)$ is a chain of characteristic subgroups of G, then let $\ell(G_i,c)$ ($\mu(G_i,c)$) be the number of subnormal subgroups K_{ij} of G such that $K_{ij} \neq G_i$, $|K_{ij}| = |G_i|$, $K_{ij} > G_{i-1}$ ($K_{ij} < G_{i+1}$), and there does not exist $\alpha \in A(G)$ such that $K_{ij}^{\alpha} = K_{ik}$ for $j \neq k$, $j,k = 1,2,\dots,\ell(G_i,c)$ ($\mu(G_i,c)$) and $i = 1,2,\dots,m-1$. In particular, if H is a proper characteristic subgroup of G and $c: G > H > (1)$ then $\ell(H,c) = \mu(H,c)$ and is called $\ell(H)$ or $\mu(H)$.

Theorem 3.1.1. Let H be a proper characteristic subgroup of G. Then

1. $n(G) \geq n(H) + \mu(H)$,
2. $n(G) \geq n(G/H) + \ell(H)$.

Proof: 1. Let s_i' be a representative composition series of C_i' where C_i' is an orbit of $(A(H), C_H)$ where $i = 1,2,\dots,n(H)$. Let s_i be a composition series of G which is a refinement of s_i' in G (s_i exists since H is a subnormal subgroup of G). There does not exist $\alpha \in A(G)$ such that $s_i^{\alpha} = s_j$ where $i \neq j$, since if $s_i^{\alpha} = s_j$ where $i \neq j$ then $s_i'^{\alpha'} = s_j'$ where α' is α restricted to H and $\alpha' \in A(H)$ since H is a characteristic subgroup of G. Therefore s_i and s_j belong to different orbits of $(A(G), C_G)$ if $i \neq j$. Note that each s_i contains H. Since there are $\mu(H)$ subnormal subgroups K_j of G with the same order as H, such that there does not exist $\alpha \in A(G)$ where $K_j^{\alpha} = K_k$, $j \neq k$, then there are at least $\mu(H)$ orbits of $(A(G), C_G)$ whose composition series do not contain H. Therefore $n(G) \geq n(H) + \mu(H)$.

2. Let $\bar{s}_i$ be a representative composition series of $\bar{C}_i$ where $\bar{C}_i$

is an orbit of $(A(G/H), C_{G/H})$ with $i = 1,\ldots,n(G/H)$. Let s_i be a composition series of G which is a refinement of the subnormal series consisting of all the preimages of the subgroups of $\bar{s}_i$ in G. Again there does not exist $\alpha \in A(G)$ such that $s_i^{\alpha} = s_j$ for $i \neq j$, since if $s_i^{\alpha} = s_j$ then $\bar{s}_i^{\bar{\alpha}} = \bar{s}_j$ where $\bar{\alpha}$ is the automorphism of G/H induced by α (that is, $\bar{\alpha}$ is defined by $(gH)^{\bar{\alpha}} = g^{\alpha}H$, and $\bar{\alpha} \in A(G/H)$ since H is a characteristic subgroup of G). Note that each s_i contains H. Since there are $\ell(H)$ subnormal subgroups K_i of G with the same order as H where there does not exist $\alpha \in A(G)$ such that $K_j^{\alpha} = K_k$, $j \neq k$, then there are at least $\ell(H)$ orbits of $(A(G), C_G)$ whose composition series do not contain H. Therefore $n(G) \geq n(G/H) + \ell(H)$.

Corollary 3.1.2. If H is a characteristic subgroup of G then

1. $n(G) \geq n(H)$ where, in particular, there are $n(H)$ orbits of $(A(G), C_G)$ whose composition series contain H,
2. $n(G) \geq n(G/H)$ where, in particular, there are $n(G/H)$ orbits of $(A(G), C_G)$ whose composition series contain H.

Proof: See proof of Theorem 3.1.1.

Corollary 3.1.2 is stated here to clarify the proof of the next theorem.

Theorem 3.1.3. If $c\colon G = G_m > G_{m-1} > \ldots > G_1 > G_0 = (1)$ where G_i is a characteristic subgroup of G for $i = 1,\ldots,m-1$, then

1. $n(G) \geq n(G_1) + \Sigma_{i=1}^{m-1} \mu(G_i, c)$,
2. $n(G) \geq n(G/G_{m-1}) + \Sigma_{i=1}^{m-1} \ell(G_i, c)$.

Proof: 1. Consider G_1. By Corollary 3.1.2 there are at least

$n(G_1)$ orbits of $(A(G), C_G)$ whose composition series contain G_1. Also there are at least $\mu(G_1,c)$ orbits of $(A(G), C_G)$ whose composition series do not contain G_1 but do contain G_2 (Definition 3.1.3). $G_1 < G_2$, and G_1 characteristic in G implies that there are at least $n(G_1) + \mu(G_1,c)$ orbits of $(A(G), C_G)$ whose composition series contain G_2. Now repeating this argument for G_i, $i = 2,3,\ldots,m-1$, we obtain part 1 of the theorem.

2. Consider G_{m-1}. By Corollary 3.1.2 there are at least $n(G/G_{m-1})$ orbits of $(A(G), C_G)$ whose composition series contain G_{m-1}. Also by Definition 3.1.3 there are at least $\ell(G_{m-1},c)$ orbits of $(A(G), C_G)$ whose composition series contain G_{m-2} but do not contain G_{m-1}. $G_{m-2} < G_{m-1}$, and G_{m-1} characteristic subgroup of G implies that there are at least $n(G/G_{m-1}) + \ell(G_{m-1},c)$ orbits of $(A(G), C_G)$ whose composition series contain G_{m-2}. Repeat this argument for G_i, $i = m-2,\ldots,2,1$, and we obtain the result of the theorem.

Another lower bound for $n(G)$ is given in the next theorem by considering the number of orbits of the factor groups of a chain of characteristic subgroups of G.

<u>Theorem 3.1.4</u>. If $c\colon G = G_m > G_{m-1} > \ldots > G_1 > G_0 = (1)$ is a chain of characteristic subgroups of G then

$$n(G) \geq \Pi_{i=1}^{m} n(G_i/G_{i-1}).$$

Proof: Let $s_{i,j}$ be a representative composition series of $C_{i,j}$ where $C_{i,j}$ is an orbit of $(A(G_i/G_{i-1}), C_{G_i/G_{i-1}})$ with $i = 1,\ldots,m$ and $j = 1,\ldots,n(G_i/G_{i-1})$. Let $s_{j(i)}$ be the composition series of G obtained by combining all subgroups of G that are preimages in G_i of the subgroups in the composition series $s_{i,j(i)}$ $i = 1,2,\ldots,m$.

If $s^{\alpha}_{j(i)} = s_{k(i)}$ where $\alpha \in A(G)$ then $s^{\alpha_i}_{i,j(i)} = s_{i,k(i)}$ where α_i is the automorphism of G_i/G_{i-1} induced by α (that is, $(g_iG_{i-1})^{\alpha_i} = g_i^{\alpha}G_{i-1})$ which, in turn, implies that $s_{i,j(i)}$ and $s_{i,k(i)}$ are in the same orbit of $(A(G_i/G_{i-1}), C_{G_i/G_{i-1}})$, so that $j(i) = k(i)$, $i = 1,\ldots,m$. Therefore we have proven this theorem.

Definition 3.1.4. If G is a group and $s_1, s_2 \in C_G$ then s_1 is isomorphic to s_2, denoted by $s_1 \cong s_2$, if every subgroup of s_1 is isomorphic to a subgroup of s_2. s_1 is $A(G)$-isomorphic to s_2, denoted by $s_1 \cong_{A(G)} s_2$ if there exists $\alpha \in A(G)$ such that every subgroup of s_2 is an image of a subgroup of s_1 under α.

Clearly $s_1 \cong_{A(G)} s_2$ implies $s_1 \cong s_2$. $\cong_{A(G)}$ and $\cong$ are equivalence relations on C_G, and the equivalence classes of $\cong_{A(G)}$ are the orbits of $(A(G), C_G)$. $n(G)$ is the number of equivalence classes of C_G under $\cong_{A(G)}$, and so we similarly define $\bar{n}(G)$ to be the number of equivalence classes of C_G under $\cong$. Trivially $n(G) \geq \bar{n}(G)$. This new equivalence relation allows us to prove two theorems similar to Corollary 3.1.2 where $H \triangleleft \triangleleft G$ or $H \triangleleft G$ instead of H is characteristic in G.

Theorem 3.1.5. Let $H \triangleleft \triangleleft G$ where G is a group, then $\bar{n}(H) \leq n(G)$ and, in particular, there are at least $\bar{n}(H)$ orbits of $(A(G), C_G)$ each of which contain a composition series containing H.

Proof: Let s_i' be a representative composition series of C_i' where C_i' is an orbit of $(A(H), C_H)$ (not necessarily all the orbits of $(A(H), C_H)$ are included) where $s_i' \not\cong s_j'$, if $i \neq j$, $i,j = 1,\ldots,\bar{n}(H)$. Let s_i be a composition series which is a refinement of s_i' in G (s_i exists since $H \triangleleft \triangleleft G$). $s_i \not\cong_{A(G)} s_j$, for $i \neq j$, since $s_i \cong_{A(G)} s_j$ implies $s_i \cong s_j$ and this implies $s_i' \cong s_j'$. Therefore there are at least $\bar{n}(H)$ orbits of $(A(G), C_G)$ each of which contains a composition series containing H.

Theorem 3.1.6. Let $H \lhd G$ where G is a group, then $\bar{n}(G/H) \leq n(G)$, and, in particular, there are at least $\bar{n}(G/H)$ orbits of $(A(G), C_G)$ each of which contains a composition series containing H.

Proof: Let $\bar{s}_i$ be a representative composition series of $\bar{C}_i$ where $\bar{C}_i$ are orbits of $(A(G/H), C_{G/H})$ (not necessarily all the orbtis of $(A(G/H), C_{G/H})$ are included) where $\bar{s}_i \not\cong \bar{s}_j$, if $i \neq j$, $i,j = 1,\ldots,\bar{n}(G/H)$. Let s_i be a composition series of G which is a refinement of the subnormal series of all the preimages in G of the subgroups of $\bar{s}_i$. $s_i \not\cong_{A(G)} s_j$, for $i \neq j$, for if $s_i \cong_{A(G)} s_j$ then $s_i \cong s_j$, and so $\bar{s}_i \cong \bar{s}_j$ which is a contradiction. Therefore there are at least $\bar{n}(G/H)$ orbits of $(A(G), C_G)$ each of which contains a composition series containing H.

3.2 $n(G)$ for G a p-group.

Next we restrict our attention to p-groups, and show that in most cases $n(G) \geq$ the class of G. Also we will find upper bounds on the exponent of G. The generalized quaternions, because of the fact that there is only one subgroup of order 2, is very crucial in this chapter so the next two lemmas investigate this important group.

Definition 3.2.1. The group $Q_n = (a,b)$ where $a^{2^{n-1}} = 1$, $b^2 = a^{2^{n-2}}$, $b^{-1}a\,b = a^{-1}$ is called the generalized quaternions for $n = 4,5,\ldots$. Q_3 is the quaternions.

Lemma 3.2.1. $n \neq 3$.

1. Every element of Q_n can be written in the form $a^m b^\ell$ where $m = 0,1,\ldots,2^{n-1} - 1$, $\ell = 0,1$, and therefore $|Q_n| = 2^n$.
2. $|a^m b| = 4$ for all m.

3. If $x \in Q_n$ and $|x| = 2^k$, $k \geq 3$ then $x \in (a^{2^{n-k-1}})$.

4. $a^{2^{n-2}}$ is the only element of order 2.

5. (a^{2^k}) is a characteristic subgroup of Q_n for $k = 0,1,\ldots,n-2$.

6. If $K \leq Q_n$ and $|K| = 2^k$ then $K = (a^{2^{n-k-1}})$ or $K = (a^{2^{n-k}}, a^m b)$ for some m.

7. If $s \in C_{Q_n}$ then s must be of the form

$s\colon Q_n > (a^2, a^m b) >\ldots> (a^{2^t}, a^m b) > (a^{2^t}) > (a^{2^{t+1}}) >\ldots> (a^{2^{n-2}}) > (1)$

where $t = 0,1,2,\ldots,n-2$.

Proof: 1. Every element can be written in the form $a^m b^\ell$ since $(a) \triangleleft Q_n$ where m ranges from 0 to $2^{n-1} - 1$ since $|a| = 2^{n-1}$ and ℓ ranges from 0 to 1 since $|b| = 4$ and $b^2 = a^{2^{n-2}}$.

2. $$\begin{aligned}(a^m b)(a^m b) &= a^m a^{-1} b\ a^{m-1} b \quad \text{since } b^{-1} a\, b = a^{-1}\\ &= a^m a^{-2} b\ a^{m-2} b\\ &\ldots\\ &= a^m a^{-m} b\ b\\ &= b^2,\end{aligned}$$

and so $|a^m b| = 4$ since $|b| = 4$.

3. Let $x \in Q_n$ and $|x| = 2^k$, $k \geq 3$, then $x \in (a)$ by 2.

4. By 2 any element of order 2 must also belong to (a) and so it is $a^{2^{n-2}}$.

5. (a) is characteristic in Q_n since it is the only cyclic subgroup of order 2^{n-1}. (a^{2^k}) is characteristic in Q_n since (a) is a cyclic 2-group.

6. If $K \leq Q_n$ and $|K| = 2^k$ then K contains only one subgroup of order 2 and Theorem K implies that K is cyclic or K is a generalized quaternion group or quaternion group of order 2^k. If $k \geq 3$, in the former case, by 3, $K = (a^{2^{n-k-1}})$, and, in the latter case, K must be

generated by an element of order 4 which, by 2, must have the form $a^m b$ for some m, and by an element of order 2^{k-1} which, by 3, is in $(a^{2^{n-k}})$. Therefore $K = (a^{2^{n-k}}, a^m b)$. If $k = 2$, then $(a^{2^{n-k}}, a^m b) = (a^m b)$ and so K is either $(a^m b)$ for some m or $(a^{2^{n-k-1}})$.

7. Let $s \in C_{Q_n}$ and let t be the smallest integer such that (a^{2^t}) is contained in s (t exists because $(a^{2^{n-2}})$ is the only subgroup of order 2). The next largest subgroup of s must be of the form $(a^{2^t}, a^m b)$ by 6. Any other subgroup K of s of order 2^k containing $(a^{2^t}, a^m b)$ must be of the form $(a^{2^{n-k}}, a^{m'} b)$ by 6, but $a^m b \in K$. Therefore $K = (a^{2^{n-k}}, a^m b)$. Therefore s is of the form shown in 7.

<u>Definition 3.2.2</u>. If G is a group then $Z_n(G)$ is defined recursively as $Z_0(G) = (1)$ and $Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G))$. We will let $Z_i = Z_i(G)$ when there is no chance of confusion. $Z_0 \leq Z_1 \leq \ldots \leq Z_n \leq \ldots$ is called the upper central series of G. If $Z_m = G$ for some m then the class of G, denoted by $d(G)$ is the smallest such m.

<u>Lemma 3.2.2</u>. If $n \neq 3$, then $n(Q_n) = n-1$ so that the exponent of $Q_n = 2^{n(Q_n)}$.

Proof: Let $s_t \in C_{Q_n}$ be of the form

s: $Q_n > (a^2, b) > \ldots > (a^{2^t}, b) > (a^{2^t}) > \ldots > (a^{2^{n-2}}) > (1)$. Any other composition series s with t being the smallest number such that s contains (a^{2^t}) is of the form

s_t: $Q_n > (a^2, a^m b) > \ldots > (a^{2^t}, a^m b) > (a^{2^t}) > \ldots > (a^{2^{n-2}}) > (1)$ by Lemma 3.2.1. Now $\alpha \in A(Q_n)$ defined by $a^\alpha = a$ and $b^\alpha = a^m b$ maps s_t to s. Therefore the orbits of $(A(Q_n), C_{Q_n})$ which contains s_t must contain all s such that t is the smallest integer such that s contains (a^{2^t}). Since all composition series have such a t by Lemma 3.1.2, and $s_t \not\approx_{A(G)} s_r$, for $r \neq t$ since $s_t \not\approx s_r$, the number of such s_t's is equal to $n(Q_n)$. t ranges from 0 to $n-2$ so we have $n(Q_n) = n-1$. Clearly the exponent of Q_n is 2^{n-1} so that the exponent of Q_n is $2^{n(Q_n)}$.

In considering the relationship of the class of a p-group G and the number of orbits of $(A(G), C_G)$, we use Theorem 3.1.3, which leads to the necessity of proving the next two results.

Lemma 3.2.3. If G is a p-group and $c\colon G = G_m > G_{m-1} > \ldots > G_1 > G_0 = (1)$ is a chain of characteristic subgroups of G such that G/G_i is not the quaternions, the generalized quaternions, or cyclic for $i = 0,1,\ldots,m-2$, then $\ell(G_i,c) \geq 1$.

Proof: To show $\ell(G_i,c) \geq 1$ we need to show that there is at least one subgroup of G with the same order as G_i and containing G_{i-1}, $i = 0,1,\ldots,m-2$. G/G_{i-1} is not cyclic, the quaternions, or the generalized quaternions so from Theorems K and L there is at least one other subgroup of G/G_{i-1} of the same order as G_i/G_{i-1} and this subgroup's preimage in G is a subgroup with the same order as G_i and containing G_{i-1}.

Theorem 3.2.4. If G is a p-group and $c\colon G = G_m > G_{m-1} > \ldots > G_1 > G_0 = (1)$ is a chain of characteristic subgroups of G such that G/G_i is not the quaternions or cyclic for $i = 0,1,\ldots,m-1$ then $n(G) \geq m$.

Proof: Case 1. If G/G_i, $i = 0,1,\ldots,m-2$ is not the generalized quaternions then, by Lemma 3.2.3, $\ell(G_i,c) \geq 1$ for $i = 1,\ldots,m-1$. Theorem 3.1.3 implies that

$$n(G) \geq n(G/G_{m-1}) + \Sigma_{i=1}^{m-1} \ell(G_{i,} c) \geq 1 + m-1 = m.$$

Case 2. If G/G_i is the generalized quaternions for $i = 0,1,\ldots,$ or $m-2$ let n be the smallest integer such that G/G_n is the generalized quaternions. Since G/G_{m-1} is not cyclic $|G/G_{m-1}| \geq 2^2$ so that

$$|G/G_n| = |G/G_{m-1}|\prod_{i=n+1}^{m-1}|G_i/G_{i-1}| \geq 2^2 \cdot 2^{m-1-n-1+1} = 2^{m-n+1}.$$

This implies that if G/G_n is isomorphic to Q_k, $k \geq 4$, then $k \geq m-n+1$ by Lemma 3.2.1. It now follows that if $n \neq m-2$ then

$$n(G/G_n) = n(Q_k) \geq n(Q_{m-n+1}) = m-n+1-1 = m-n,$$

and if $n = m-2$ then

$$n(G/G_n) = n(Q_k) \geq n(Q_4) = 3 \geq m-n$$

by Lemma 3.2.2. Consider the chain of characteristic subgroups $c'\colon G > G_n > G_{n-1} > \ldots > G_1 > G_0 = (1)$. $\ell(G_i,c') \geq 1$ for $i = 1,\ldots,n$ by the minimality of n. Applying Theorem 3.1.3 to c' we obtain

$$n(G) \geq (G/G_n) + \Sigma_{i=1}^{n} \ell(G_i,c') \geq m-n+n = m.$$

<u>Theorem 3.2.5</u>. If G is a p-group, G/Z_{m-2} is not the quaternions, and $m = d(G)$, then $n(G) \geq d(G)$.

Proof: If G is abelian then $d(G) = 1$, and clearly $n(G) \geq d(G)$. Assume G is not abelian, that is, $d(G) \geq 2$. It is well-known that G/Z_i is not cyclic for $i = 0,1,\ldots,m-1$. G/Z_i cannot be isomorphic to the quaternions for $i = 0,1,\ldots,m-3$, and $m-1$ since $d(Q_3) = 2$ and $d(G/Z_i) = m-i$. G/Z_{m-2} cannot be isomorphic to the quaternions by hypothesis. Therefore the upper central series is a chain of characteristic subgroups of G as in Theorem 3.2.4, and this implies that $d(G) \leq n(G)$.

The quaternions Q_3, Example 1.1.1, have $d(Q_3) = 2$ and $n(Q_3) = 1$, which points out the necessity of the hypothesis of the last theorem. $n(G)$ can be equal to $d(G)$ for this is the case when G is the group of Example 1.1.2. The next theorem investigates a p-group G when $n(G) = d(G)$.

Theorem 3.2.6. If G is a p-group and there does not exist a characteristic subgroup H of G such that G/H is the quaternions, then $m = d(G) = n(G)$ implies that if K is a proper characteristic subgroup of G where G/K is not cyclic then $K = Z_i$ for some $i = 0,1,\ldots,m-1$.

Proof: Let K be a characteristic subgroup of G where G/K is not cyclic and $K \neq Z_i$ for all $i = 0,1,\ldots,m-1$. There is a largest integer n $(n < m)$ such that $Z_n < K$. Now $K \cap Z_{n+1} > Z_n$, since $K/Z_n \lhd G/Z_n$, and $Z_{n+1}/Z_n = Z(G/Z_n)$, K/Z_n intersects Z_{n+1}/Z_n non-trivially. If $K \cap Z_{n+1} < Z_{n+1}$ then the series of characteristic subgroups c: $G = Z_m > \ldots > Z_{n+1} > K \cap Z_{n+1} > Z_n > \ldots > (1)$ has length $m+1$, but c also satisfies the conditions of Theorem 3.2.4 since $G/K \cap Z_{n+1}$ is not the quaternions by the hypothesis, and $G/K \cap Z_{n+1}$ is not cyclic since if $n < m-1$ then G/Z_{m-1} is not cyclic, and if $n = m-1$ then $K \cap Z_{n+1} = K \cap G = K$ and G/K is not cyclic by assumption. However if $K \cap Z_{n+1} = Z_{n+1}$ then $K \geq Z_{n+1}$ which contradicts the maximality of n. This proves the theorem.

This completes our discussion of the length of chains of characteristic subgroups in relation to $n(G)$. The exponent of a p-group G is the next parameter to be considered in relation to $n(G)$. The exponent of a group G is the smallest positive integer

m such that $g^m = 1$ for all $g \in G$. We show that if G is a p-group then the exponent of G is less than or equal to $p^{n(G)}$ without any difficulties, and then proceed to lower this upper bound for most p-groups G. In order to do this we must build up some notation to handle the case when G is an abelian p-group.

Definition 3.2.3. Let $\begin{pmatrix} m_1 & & m_s \\ t_1 & ,\ldots, & t_s \end{pmatrix}$ denote an abelian p-group which is the direct product of the direct product of t_i cyclic p-groups of order p^{m_i}, $i = 1,\ldots,s$. Let $m_i \geq m_j \geq 0$ for $i \leq j$ and $i,j = 1,\ldots,s$.

Definition 3.2.4. If $\begin{pmatrix} n_1 & & n_r \\ \mu_1 & ,\ldots, & \mu_r \end{pmatrix}$ is such that $n_i > n_j > 0$ for $i < j$ and $\mu_i > 0$ for $i,j = 1,\ldots,r$ then it is said to be in reduced form.

Lemma 3.2.7. All abelian p-groups are isomorphic to an abelian p-group of the form $\begin{pmatrix} n_1 & & n_r \\ \mu_1 & ,\ldots, & \mu_r \end{pmatrix}$ which is in reduced form. In fact, if G is isomorphic to an abelian p-group of the form $\begin{pmatrix} m_1 & & m_s \\ t_1 & ,\ldots, & t_s \end{pmatrix}$ then G is isomorphic to a group of the form

1. $\begin{pmatrix} m_1 & & m_i & & m_{i+2} & & m_s \\ t_1 & ,\ldots, & t_i+t_{i+1} & , & t_{i+2} & ,\ldots, & t_s \end{pmatrix}$ if $m_i = m_{i+1}$,

2. $\begin{pmatrix} m_1 & & m_{s-1} \\ t_1 & ,\ldots, & t_{s-1} \end{pmatrix}$ if $m_s = 0$,

3. $\begin{pmatrix} m_1 & & m_{i-1} & & m_{i+1} & & m_s \\ t_1 & ,\ldots, & t_{i-1} & , & t_{i+1} & ,\ldots, & t_s \end{pmatrix}$ if $t_i = 0$.

Using these three types of reductions $\begin{pmatrix} m_1 & & m_s \\ t_1 & ,\ldots, & t_s \end{pmatrix}$ can always be changed to reduced form.

Proof: This follows directly from Definitions 3.2.3 and 3.2.4.

Definition 3.2.5. Let $\left[\begin{pmatrix} m_1 & & m_s \\ t_1 & ,\ldots, & t_s \end{pmatrix}\right]$ denote the reduced form of $\begin{pmatrix} m_1 & & m_s \\ t_1 & ,\ldots, & t_s \end{pmatrix}$.

Lemma 3.2.8. If G is an abelian p-group isomorphic to $\begin{pmatrix} m_1 & & m_s \\ t_1, & \ldots, & t_s \end{pmatrix}$ then $|G| = p^{\Sigma_{i=1}^{s} m_i t_i}$.

Proof: The proof is clear because of Definition 3.2.3.

Definition 3.2.6. Let $\bar{n}$ be defined recursively as $\bar{n}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1$ and

$$\bar{n}\begin{pmatrix} n_1 & & n_r \\ \mu_1, & \ldots, & \mu_r \end{pmatrix} = \Sigma_{i=1}^{s} \bar{n}\left[\begin{pmatrix} n_1 & & n_i & n_i-1 & n_{i+1} & & n_r \\ \mu_1, & \ldots, & \mu_i-1, & 1, & \mu_{i+1}, & \ldots, & \mu_r \end{pmatrix}\right]$$

where $\begin{pmatrix} n_1 & & n_r \\ \mu_1, & \ldots, & \mu_r \end{pmatrix}$ is in reduced form.

Lemma 3.2.9. If G is an abelian p-group isomorphic to $\begin{pmatrix} n_1 & & n_r \\ \mu_1, & \ldots, & \mu_r \end{pmatrix}$, in reduced form, then

$$\bar{n}(G) = \bar{n}\begin{pmatrix} n_1 & & n_r \\ \mu_1, & \ldots, & \mu_r \end{pmatrix}.$$

Proof: The proof is by induction on $\Sigma_{i=1}^{r} n_i \mu_i$. If $\Sigma_{i=1}^{r} n_i \mu_i = 1$ then $n_1 = \mu_1 = s = 1$. Therefore G is a cyclic p-group of order p so that $\bar{n}(G) = 1$ and $\bar{n}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1$. Now assume that all abelian p-groups of order less than $p^{\Sigma_{i=1}^{r} n_i \mu_i}$ the theorem is true. Let G be a group isomorphic to $\begin{pmatrix} n_1 & & n_r \\ \mu_1, & \ldots, & \mu_r \end{pmatrix}$ in reduced form. There are r subgroups of G of the order $p^{(\Sigma_{i=1}^{r} n_i \mu_i)-1}$ none of which are isomorphic to any other. Call them H_i, $i = 1,\ldots,r$, where H_i is isomorphic to $\begin{pmatrix} n_1 & & n_i & n_i-1 & & n_r \\ \mu_1, & \ldots, & \mu_i-1, & 1, & \ldots, & \mu_r \end{pmatrix}$.

$$\bar{n}(G) = \Sigma_{i=1}^{r} \bar{n}(H_i) = \Sigma_{i=1}^{r} \bar{n}\left[\begin{pmatrix} n_1 & & n_i & n_i-1 & & n_r \\ \mu_1, & \ldots, & \mu_i-1, & 1, & \ldots, & \mu_r \end{pmatrix}\right] = \bar{n}\begin{pmatrix} n_1 & & n_r \\ \mu_1, & \ldots, & \mu_r \end{pmatrix}$$

by the induction hypothesis which proves the lemma.

<u>Lemma 3.2.10</u>. $\bar{n}\binom{1}{m} = 1$, $\bar{n}\binom{m}{1} = 1$ for $m \geq 1$.

Proof: Lemma 3.2.9 allows us to write

$$\bar{n}\binom{1}{m} = \bar{n}\left[\begin{pmatrix}1\\m-1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right] = \bar{n}\binom{1}{m-1} = \ldots = \bar{n}\binom{1}{1} = 1,$$

and

$$\bar{n}\binom{m}{1} = \bar{n}\left[\begin{pmatrix}m\\0\end{pmatrix}, \begin{pmatrix}m-1\\1\end{pmatrix}\right] = \bar{n}\binom{m-1}{1} = \ldots = \bar{n}\binom{1}{1} = 1.$$

The need for the next lemma and thus all the preceding lemmas will be seen in Theorem 3.2.14 where we obtain upper bounds on the exponent of a p-group G.

<u>Lemma 3.2.11</u>. $\bar{n}\left[\begin{pmatrix}n\\1\end{pmatrix}, \begin{pmatrix}1\\m\end{pmatrix}\right] = C_{n+m-1,m}$ $n \geq 1$, $m \geq 1$ where $C_{\ell,k} = \ell!/(\ell-k)!k!$.

Proof: Case 1. $n = 1$. $\bar{n}\left[\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\m\end{pmatrix}\right] = \bar{n}\binom{1}{m+1} = 1$ by Lemma 3.2.10, and $C_{1+m-1,m} = C_{m,m} = 1$.

Case 2. $n > 1$. The proof is by induction on $n+m$. The smallest value of $n+m$ is 3 which means that $m = 1$ and $n = 2$.

$$\bar{n}\left[\begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right] = \bar{n}\left(\begin{matrix}2\\1\end{matrix}, \begin{matrix}1\\1\end{matrix}\right) = \bar{n}\left[\begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right] + \bar{n}\left[\begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right]$$

$$= \bar{n}\binom{1}{2} + \bar{n}\binom{2}{1} = 1+1 = 2,$$

and $C_{2+1-1,1} = C_{2,1} = 2$. Now assume the lemma is true for $n+m < k$. If $n+m = k$ then

$$\bar{n}\left[\begin{pmatrix}n\\1\end{pmatrix}, \begin{pmatrix}1\\m\end{pmatrix}\right] = \bar{n}\left(\begin{matrix}n\\1\end{matrix}, \begin{matrix}1\\m\end{matrix}\right) = \bar{n}\left[\begin{pmatrix}n\\0\end{pmatrix}, \begin{pmatrix}n-1\\1\end{pmatrix}, \begin{pmatrix}1\\m\end{pmatrix}\right] + \bar{n}\left[\begin{pmatrix}n\\1\end{pmatrix}, \begin{pmatrix}1\\m-1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right]$$

$$= \bar{n}\left(\begin{matrix}n-1\\1\end{matrix}, \begin{matrix}1\\m\end{matrix}\right) + \bar{n}\left(\begin{matrix}n\\1\end{matrix}, \begin{matrix}1\\m-1\end{matrix}\right) = C_{n-1+m-1,m} + C_{n+m-1-1,m-1}$$

$$= C_{n+m-2,m} + C_{n+m-2,m-1} = C_{n+m-1,m}.$$

In order to prove that for G a p-group the exponent of $G \le p^{n(G)}$ we need the following.

<u>Lemma 3.2.12</u>. If $H_1 = (a,b)$ such that $a^{p^{\ell}} = b^p = 1$, and $[a,b] = a^p$, or $H_2 = (a,b)$ such that $a^{p^{\ell}} = b^p = 1$ and $[a,b] = 1$, then $\bar{n}(H_i) \ge \ell$ and $n(H_i) \ge \ell+1$ for $i = 1,2$.

Proof: Consider Figure 1.

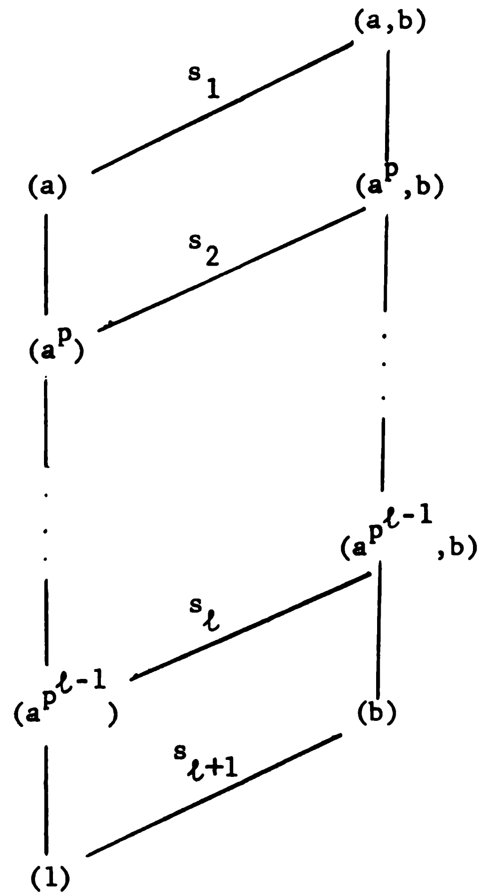

Figure 1.

Clearly $s_i \cong s_j$ for $i \ne j$ and $i,j = 1,\ldots,\ell$ which proves that $\bar{n}(H_i) \ge \ell$. $(a^p) = \Phi(H_i)$ for $i = 1,2$, since $\Phi(H_i)$ is the smallest normal subgroup of H_i such that its factor group is elementary abelian, and $H_i/(a^p)$ is elementary abelian so that $(a^p) \ge \Phi(H_i)$. Since $H_i/(a^{p^2})$ is not elementary abelian $\Phi(H_i) = (a^p)$. There does not exist $\alpha \in A(G)$ such that $(a^{p^{\ell-1}})^{\alpha} = (b)$ since $(a^{p^{\ell-1}}) \le \Phi(H_i)$

and $\Phi(H_i)$ is a characteristic subgroup of H_i. This gives us that $s_i \not\approx_{A(H_i)} s_j$ for $i,j = 1,2,\ldots,\ell+1$ which implies that $n(H_i) \geq \ell+1$.

Theorem 3.2.13. If G is a p-group, Q_n is not isomorphic to $H < G$ for $n \geq 3$, and $n(G) \geq 2$ then the exponent of $G \leq p^{n(G)}$.

Proof: Since $n(G) \geq 2$ Theorem B implies that G is not cyclic. Assume there is an $a \in G$ such that $|a| = p^{\ell}$ where $\ell > n(G)$ and that (a) is not contained in a cyclic subgroup of G $((a) \neq G)$. Let $b \in N((a))$ but $b \notin (a)$ such that $b^p \in (a)$. $|(a,b)| = p^{\ell+1}$ since $b^p \in (a)$. If $b \notin C(a)$ then (a,b) is a group isomorphic to the group H_1 of Lemma 3.2.12. On the other hand if $b \in C(a)$ then (a,b) is a group isomorphic to the group H_2 of Lemma 3.2.12. In either case (a,b) is subnormal in G, and by Lemma 3.2.12 $\bar{n}((a,b)) \geq \ell > n(G)$ which contradicts Theorem 3.1.5 and this proves the theorem.

So far we have shown that exponent of $G \leq p^{n(G)}$. The following example gives us some hope that this upper bound can be made smaller.

Example 3.2.1. Let $G = H \times (d)$ where $|d| = p$, and $H = (a,b,c)$ with $a^p = b^p = c^p = [a,b] = [a,c] = 1$, and $[b,c] = a$. $Z(G) = (a,d)$. $n(G) \geq 3$ since the three composition series

$$s_1\colon G > (a,b,c) > (a,b) > (a) > (1)$$

$$s_2\colon G > (a,b,d) > (a,d) > (a) > (1)$$

$$s_3\colon G > (a,b,d) > (a,b) > (a) > (1)$$

are in different orbits of $(A(G), C_G)$ since (a,b,d) is abelian and (a,b,c) is not abelian and $Z(G) = (a,d)$. Even though $n(G) \geq 3$ the exponent of G is p. The fact that $Z(G)$ in this example is not cyclic leads us to the following theorem.

Theorem 3.2.14. If G is a p-group such that $Z(G)$ is not cyclic and the exponent of G is p^k then $n(G) \geq C_{k+p-1,p}$.

Proof: Let $g \in G$ such that $|g| = p^k$. It is well-known that the number of subgroups of a particular order in a p-group is equal to 1 modulo p [1, page 129]. Since $Z(G)$ is not cyclic and abelian, Theorems K and L imply that $Z(G)$ has at least $1+p$ subgroups of order p. Since $(g^{p^{k-1}})$ may or may not be contained in $Z(G)$ we can construct a subgroup H of G isomorphic to $\begin{pmatrix} k & , & 1 \\ 1 & & p \end{pmatrix}$ where H is the direct product of (g) with p subgroups of $Z(G)$ of order p. By Theorem 3.1.5, Lemma 3.2.9, and Lemma 3.2.11 we have

$$n(G) \geq \bar{n}(H) = \bar{n}\begin{pmatrix} k & , & 1 \\ 1 & & p \end{pmatrix} = C_{k+p-1,p}.$$

Corollary 3.2.15. If G is a p-group such that $Z(G)$ is not cyclic, then the exponent of $G \leq p^m$ where m is the largest solution of $n(G) \geq C_{m+p-1,p}$.

Proof: By Theorem 3.2.14, $n(G) \geq C_{k+p-1,p}$ where the exponent of G is p^k. If m is the largest solution of $n(G) \geq C_{m+p-1,p}$ then $k \leq m$ and the exponent of $G \leq p^m$.

Corollary 3.2.16. If G is an abelian p-group such that $n(G) \geq 2$ then the exponent of $G \leq p^m$ where m is the largest solution of $n(G) \geq C_{m+p-1,p}$.

Proof: Since $n(G) \geq 2$ and $G = Z(G)$, $Z(G)$ is not cyclic by Theorem A, and we apply Corollary 3.2.15 to prove the theorem.

The next corollary gives an easy method for finding an upper bound for the exponent of G, but it does not give as sharp a bound.

Corollary 3.2.17. If G is a p-group and $Z(G)$ is not cyclic then the exponent of $G \le p^m$ where m is the smallest integer such that $\Sigma_{i=1}^{m} i \ge n(G)$.

Proof: Let the exponent of G be p^k. In the proof of Theorem 3.2.14 replace H by direct product of (g) with just 2 subgroups of $Z(G)$ of order p which can be done since $p \ge 2$. Then we have

$$n(G) \ge \bar{n}(H) = \bar{n}\left[\begin{pmatrix} k \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}\right] = C_{k+2-1,2} = \frac{(k+1)!}{2!(k-1)!} = \frac{k(k+1)}{2} = \Sigma_{i=1}^{k} i.$$

If m is the smallest integer such that $\Sigma_{i=1}^{m} i \ge n(G)$ then

$$\Sigma_{i=1}^{m} i \ge n(G) \ge \Sigma_{i=1}^{k} i.$$

Therefore $m \ge k$, and so the exponent of $G \le p^m$.

Note that if G is a p-group with $Z(G)$ not cyclic, this corollary implies that when $n(G) \ge 3$ then the exponent of $G \le p^{n(G)-1}$. If $n(G) = 2$, Corollary 3.2.15 implies that the exponent of $G = p = p^{n(G)-1}$. Of course, Corollary 3.2.15 gives much better bounds for the exponent of G in most cases. When $Z(G)$ is cyclic we can only give the upper bound $p^{n(G)-1}$ which is the content of the next theorem.

Theorem 3.2.18. If G is a p-group such that $n(G) \ge 2$, $Z(G)$ is cyclic, and if $H \le G$ then H is not isomorphic to the quaternions or the generalized quaternions, then the exponent of $G \le p^{n(G)-1}$.

Proof: Suppose that $a \in G$ such that $|a| = p^{\ell}$ where $\ell = n(G)$. Let $Z(G) = (z)$ where $|z| = p^m$. Then $m \le \ell$ because of Theorem 3.2.13.

Case 1. $(a) \not\le Z(G)$ and $(a) \cap Z(G) \ne (1)$. Suppose that $(a) \cap Z(G) = (a^{p^{\ell-k}})$ where $k = 1,\ldots,m-1$. Let $H = (a, z^{p^{m-k-1}})$.

H is abelian and

$$|H| = \frac{|(a)||(z^{p^{m-k-1}})|}{|(a) \cap (z^{p^{m-k-1}})|} = \frac{p^{\ell} \cdot p^{k+1}}{p^{k}} = p^{\ell+1} .$$

Since $z^{p^{m-k}} \in (a^{p^{\ell-k}})$, $z^{p^{m-k}} = a^{sp^{\ell-k}}$. Let $b = a^{-sp^{\ell-k-1}} z^{m-k-1}$. Then $b \notin Z(G)$ and $|b| = p$ since

$$(a^{-sp^{\ell-k-1}} z^{m-k-1})^{p} = a^{-sp^{\ell-k}} z^{p^{m-k}} = a^{-sp^{\ell-k}} a^{sp^{\ell-k}} = 1.$$

Therefore $H = (a,b)$ where $b \notin Z(G)$ and $a^{p^{\ell-1}} \in Z(G)$.

Case 2. $(a) \geq Z(G)$. By hypothesis $N((a))$ is not the quaternions or the generalized quaternions so that there is a $b \in N((a))$ such that $|b| = p$ and $b \notin Z(G)$. Let $H = (a,b)$ where $b \notin Z(G)$ and $a^{p^{\ell-1}} \in Z(G)$.

Case 3. $(a) \cap Z(G) = (1)$. Let $b \in Z(G)$ and $|b| = p$. Let $H = (a,b)$ where $b \in Z(G)$ and $a^{p^{\ell-1}} \notin Z(G)$.

In all cases we consider the $\ell+1$ composition series s_i, $i = 1,\ldots,\ell+1$ defined in Figure 1, page 30. Again $s_i \not\approx s_j$, for $i \neq j$, $i,j = 1,2,\ldots,\ell$. Also $s_{\ell+1} \not\approx s_i$ for $i = 1,2,\ldots,\ell-1$. $s_{\ell+1} \not\approx_{A(G)} s_{\ell}$ since either $a^{p^{\ell-1}} \notin Z(G)$ and $b \in Z(G)$, or $a^{p^{\ell-1}} \in Z(G)$ and $b \notin Z(G)$ in all three cases which proves that $n(G) \geq \ell+1 = n(G) + 1$ which is a contradiction so that no such a exists and we have proven the theorem.

3.3. $n(G) = 2$.

This section is included in this thesis as an application of the results of Chapter II to show that $(A(G), D_G)$ and $(A(G), C_G)$ are intimately related. The assumption that $n(G) = 2$ can be broken down into two cases: G has a subnormal subgroup which is not normal in G, and all subnormal subgroups are normal. The former case implies that $(A(G), D_G)$ is a transitive permutation group, so we can apply the results of Chapter II. On the other hand, the latter case implies that G is a t-group, in which case we use the result of Gaschütz [2]. We recall some definitions before we state the results.

Definition 3.3.1. A group G is called a t-group if every subnormal subgroup of G is normal in G.

Definition 3.3.2. A group G is a Dedekind group if all of its subgroups are normal. A non-abelian Dedekind group is called a Hamiltonian group.

A Dedekind group is a t-group, and every nilpotent t-group is a Dedekind group. The Hamiltonian groups have been characterized, and this is the content of Theorem M of the Appendix which we will use in Theorem 3.3.2.

The following lemma will make the proof of the other theorems easier.

Lemma 3.3.1. If G is a p-group and $n(G) = 2$ then G is not abelian.

Proof: Assume G is abelian. Theorem 3.2.13 says that the exponent of G is less than or equal to p^2. G is not elementary abelian or cyclic by Theorem A, and therefore G contains a subgroup H isomorphic to $\begin{pmatrix} 2 & , & 1 \\ 1 & & 1 \end{pmatrix}$.

Case 1. $G = H$. H is isomorphic to H_2 of Lemma 3.2.12 where $\ell = 2$, and so we have $n(G) \geq 3$ which is a contradiction.

Case 2. $G > H$ and G is isomorphic (c,d) where $c^{p^2} = d^{p^2} = [c,d] = 1$.

Consider the three composition series

$$s_1\colon G > (c,d^p) > (c) > (c^p) > (1),$$

$$s_2\colon G > (c,d^p) > (c^p,d^p) > (c^p) > (1),$$

$$s_3\colon G > (c,d^p) > (c^p,d^p) > (d^p) > (1).$$

$s_1 \not\approx s_2$ and $s_1 \not\approx s_3$ since $(c) \not\approx (c^p,d^p)$. $s_2 \not\approx_{A(G)} s_3$ for if $s_2 \approx_{A(G)} s_3$ then there is an $\alpha \in A(G)$ such that $(c,d^p)^\alpha = (c,d^p)$ and $(c^p)^\alpha = (d^p)$. Therefore $[c^p]^\alpha = d^{pn}$ where $(p,n) = 1$ and $c^\alpha = c^\ell d^{pk}$ where $(\ell,p) = 1$. $d^{pn} = [c^p]^\alpha = [c^\alpha]^p = [c^\ell d^{kp}]^p = c^{\ell p}$, and it follows that $(d^p) = (c^p)$ and this contradiction implies that $n(G) \geq 3$, which eliminates this case.

Case 3. $G > H$ and there is a subgroup K of G isomorphic to $\begin{pmatrix} 2 & , & 1 \\ 1 & & 2 \end{pmatrix}$. Lemma 3.2.9 implies that $n(G) \geq \bar{n}(K) = \bar{n}\begin{pmatrix} 2 & , & 1 \\ 1 & & 2 \end{pmatrix} = C_{2+2-1,2} = C_{3,2} = 3$, and we have reached another contradiction. So G is not abelian where G is a p-group and $n(G) = 2$.

Let $H = (a,b,c)$ where $a^p = b^p = c^p = [a,b] = [a,c] = 1$ and $[b,c] = a$. In the next result we will prove that H is one of the two nilpotent groups such that $n(G) = 2$.

<u>Theorem 3.3.2</u>. Let G be a nilpotent group. Then $n(G) = 2$ if and only if G is isomorphic to H as defined above or a cyclic group of order the product of two distinct primes.

Proof: Assume $n(G) = 2$ and G is nilpotent.

Case 1. G has a subgroup which is subnormal but not normal in G. In this case all the chief series are in one orbit of $(A(G), C_G)$ and the composition series which are not chief series are in the other orbit. This implies that $(A(G), D_G)$ is a transitive permutation group. Applying Theorem 2.1.4 we see that G is isomorphic to H.

(G is not isomorphic to a cyclic p-group, an elementary abelian p-group, or the quaternions because all of the composition series of these groups are chief series.)

Case 2. All subnormal subgroups of G are normal in G, that is, G is a t-group. Since G is nilpotent G is a Dedekind group. If, in fact, G is a Hamiltonian group then G is isomorphic to the direct product of Q_3, A, and B where Q_3 is the quaternions, A is an elementary abelian 2-group, and B is an abelian group in which every element is of odd order by Theorem M. $n(Q_3) = 1$ by Theorem B, so not both A and B are trivial. Let $Q_3 = (a,b)$ where $a^4 = b^4 = 1$ and $a^2 = b^2 = [a,b]$. Let $c \in A$ or B with $|c| = p$, p a prime. Three chief series that are in different orbits of $(A(G), C_G)$ can be constructed using the facts that (a,b) is the quaternions and (a,c) is not the quaternions, and (a) is cyclic of order 4, and (a^2,c) is elementary abelian of order 4 if $p = 2$ or it is of order 2p if p is not 2. This contradicts $n(G) = 2$ so that no Hamiltonian group has $n(G) = 2$. If G is an abelian group (Dedekind but not Hamiltonian), then clearly $|G|$ is not divisible by 3 distinct primes and Lemma 3.3.1 eliminates the possibility that G is a p-group so that $|G|$ is divisible by two primes. If $|G|$ is divisible by p^2 then G contains a cyclic subgroup of order p^2 or an elementary abelian subgroup of order p^2. Taking another element of G of order q (the other prime dividing $|G|$) three non-isomorphic chief series of G may be constructed which contradicts $n(G) = 2$. Therefore G is a cyclic group of order pq where p and q are distinct primes.

To complete the proof of the theorem we show that H and a cyclic group of order pq has two orbits. The cyclic group of order pq clearly has 2 orbits. We now consider H. In Theorem 2.1.4 we have shown that $(A(H), D_H)$ is a transitive permutation group. Therefore to show that $(A(H), C_H)$ has two orbits we show that $A(H)$ acts transitively on the composition series of H which are not chief series. There are p^2+p non-chief series of H which are exhibited below:

$$s_x: H > (a,x) > (x) > (1) \quad \text{where} \quad x = b,c,bc,\ldots,b^{p-1}c;$$

$$s_{x,n}: H > (a,x) > (ax^n) > (1) \quad \text{where} \quad n = 1,\ldots,p-1.$$

Since all elements of H have order p and $Z(H) = (a)$ an automorphism α of H may be constructed by letting a^α, b^α and c^α be such that $[b^\alpha,c^\alpha] \in Z(H)$, $(b^\alpha,c^\alpha) = H$, and $a^\alpha = [b^\alpha,c^\alpha]$.

For $x = c,bc,\ldots,b^{p-1}c$, $s_b \cong_{A(G)} s_x$ by the automorphism α_x defined by

$$\alpha_x \begin{cases} a \to [x,c] \\ b \to x \\ c \to c \end{cases} \quad \text{for} \quad x \neq c, \ \alpha_c \begin{cases} a \to [c,b] \\ b \to c \\ c \to b \end{cases}$$

Now again for $x = b,c,bc,\ldots,b^{p-1}c$, $s_x \cong_{A(G)} s_{x,n}$ by the automorphism $\alpha_{x,n}$ defined by

$$\alpha_{x,n} \begin{cases} a \to [ax^n,y] \\ x \to ax^n \\ y \to y \end{cases}$$

where y is an element of H such that $(x,y) = H$, and $[x,y] = a$.

Therefore s_b is A(H)-isomorphic to every other non-chief series of H, and this proves that $n(H) = 2$.

If G is assumed to be a solvable group and $n(G) = 2$, G is either a t-group or not a t-group. These two possibilities lead to the last two theorems of this thesis.

Theorem 3.3.3. If G is solvable, not a t-group, $(A(G), D_G)$ is transitive, and $n(G) = 2$, then G satisfies:

1. $\mathrm{Soc}^{n+1}(G)/\mathrm{Soc}^{n}(G)$ is an elementary abelian p-group.
2. If K is a characteristic subgroup of G then there is an integer n such that $K = \mathrm{Soc}^{n}(G)$.
3. $G^{(t)}/G^{(t+1)}$ is an elementary abelian or cyclic p-group.
4. There is an integer n such that $G^{(n)} = \mathrm{Fit}(G)$.
5. There are no characteristic subgroups between $\Phi(G)$ and $\mathrm{Fit}(G)$ so that $\Phi(\mathrm{Fit}(G)) \leq \Phi(G)$.
6. If $Z(G) \neq (1)$ then $Z(\mathrm{Fit}(G)) \geq Z(G) \geq \mathrm{Soc}(G)$.
7. If $L_0 > L_1 > \ldots > L_n = (1)$ is the lower nilpotent series of G, then L_i/L_{i+1} is isomorphic to a cyclic p-group, an elementary abelian p-group, the quaternions, or H where H is the group mentioned before Theorem 3.3.2. Also only one of the factors of the lower nilpotent series is isomorphic to H.

Proof: Assume $n(G) = 2$, and G is a solvable group which is not a t-group. Since $(A(G), D_G)$ is a transitive permutation group, we apply Theorem 2.1.9 to prove 1 to 7. 1,2,4,5 and 6 are the same as 1,2,4,5 and 6 in Theorem 2.1.9. Theorem 2.1.9 part 3 says that $G^{(t)}/G^{(t+1)}$ is an abelian p-group, and Theorem 3.1.2 gives us that $2 = n(G) \geq n(G^{(t)}) \geq n(G^{(t)}/G^{(t+1)})$. $n(G^{(t)}/G^{(t+1)}) = 1$ by Lemma 3.3.1, and then Theorem A implies that $G^{(t)}/G^{(t+1)}$ is a cyclic p-group or an elementary abelian p-group which proves part 3. Theorem 2.1.9 part 7 says that L_i/L_{i+1} is a p-group and Theorem 3.1.2 gives us that $2 = n(G) \geq n(L_i) \geq n(L_i/L_{i+1})$. Therefore $n(L_i/L_{i+1}) = 1$ or 2, and Theorem 3.3.2 and Theorem B implies that L_i/L_{i+1} is isomorphic to a cyclic p-group, an elementary abelian p-group, the quaternions, or H. Since H is the only one of the four groups just mentioned such that $n(H) = 2$, Theorem 3.1.4 implies that only one of the factors of the lower nilpotent series is isomorphic to H which proves 7 and the theorem.

It is doubtful that the converse of this theorem is true, but I do not know of a counter-example.

Before proving a similar theorem when G is a t-group, we prove several lemmas. The following depends heavily on Theorems N and P which are taken from Gaschütz's paper on t-groups [2]. In these lemmas, G will be assumed to be a solvable, non-nilpotent, t-group and G/L will be the maximal nilpotent factor group of G. Under these assumptions Theorem N implies that $C(L) \geq L$ and $L \neq (1)$.

<u>Lemma 3.3.4</u>. If $H \triangleleft G$ with the property that to each prime p dividing $|L|$ there is an $h \in H$ such that $\ell^h = \ell^n$ for all $\ell \in L$ where $n \not\equiv 1 \bmod p$, then $H \geq L$.

Proof: Let G be a minimal counter-example, that is, G contains a normal subgroup $H (\neq G)$ such that to each p dividing $|L|$ there is an $h \in H$ such that $\ell^h = \ell^n$ for all $\ell \in L$ where $n \not\equiv 1 \bmod p$, and $H \not\geq L$. This implies that $HL > L > H \cap L$.

Case 1. $HL < G$. Theorem N implies that (1) HL/L is Dedekind, (2) $(|HL: L|, |L|) = 1$, and (5) the inner automorphisms of HL induce power automorphisms on L with power n in such a way that to each p dividing the $|L|$ there is an $h \in H < HL$ with $\ell^h = \ell^n$ for all $\ell \in L$ where $n \not\equiv 1 \bmod p$. Theorem P implies that HL is a solvable t-group and HL/L is the maximal nilpotent factor group of HL. But $H \triangleleft HL$ implies by the minimality of G that $H \geq L$ which is a contradiction.

Case 2. $G = HL$. $H/H \cap L \cong HL/L$ which is nilpotent since G/L is Dedekind. Now $G/H \cap L = HL/H \cap L = (H/H \cap L)(L/H \cap L)$ so that Theorem Q implies that $G/H \cap L$ is nilpotent. Therefore $L = H \cap L$ so that $H \geq L$, which again is a contradiction.

<u>Lemma 3.3.5</u>. $C(L) < G$.

Proof: If $C(L) = G$ then $Z(G) \geq L$. Since G/L is nilpotent, then G is nilpotent which is a contradiction.

<u>Lemma 3.3.6</u>. If G/L is abelian or the quaternions, then $C(L)$ is abelian and so $H \leq C(L)$ or $H \geq L$ implies $H \triangleleft G$.

Proof: L is a Hall subgroup of G by Theorem N which implies that L is also a Hall subgroup of $C(L)$. Theorem R implies that L has a complement K in $C(L)$. $C(L)/L = LK/L \cong K/L \cap K = K$. Since G/L is abelian or the quaternions, and $C(L) < G$, $K \cong C(L)/L$ is abelian. Therefore since L is abelian and $K \leq C(L)$, $LK = C(L)$ is abelian. The remainder of this lemma follows because G is a t-group and $C(L) \triangleleft G$. If $H \leq C(L)$ then $H \triangleleft C(L)$. $C(L) \triangleleft G$ since $L \triangleleft G$. Therefore $H \triangleleft G$. If $H \geq L$ then $H \triangleleft G$ since G/L is Dedekind.

<u>Lemma 3.3.7</u>. If L is a p-group, then $H \triangleleft G$ implies that $H \leq C(L)$ or $H \geq L$.

Proof: Suppose $H \not\geq L$ and $H \triangleleft G$, then Lemma 3.3.4 implies that for all $h \in H$ such that $\ell^h = \ell^n$ for all $\ell \in L$ where $n \equiv 1 \bmod p$. We would like to show that $H \leq C(L)$. If $L \cap H = H$ then

$H \leq L \leq C(L)$. If $L \cap H < H$ then $L \cap H$ is a Hall subgroup of H so that, by Theorem R, $L \cap H$ has a complement K in H. Let $k \in K$ and ℓ be an element of L of maximal order. Then $\ell^k = \ell^n$ where $n \equiv 1 \bmod p$. Therefore $\ell = \ell^{k^{|k|}} = \ell^{n^{|k|}}$ implies that $n^{|k|} \equiv 1 \bmod p$. Let t be the largest integer such that $n \equiv 1 \bmod p^t$. If $|\ell|$ divides p^t then $k \in C(L)$. If $|\ell|$ does not divide p^t then we know that $n = 1+s\ p^t$, and

$$n^{|k|} = (1 + s\ p^t)^{|k|} = 1 + |k| s\ p^t + \frac{|k|(|k|-1)}{2} s^2 p^{2t} +$$

(terms in higher powers of p),

also

$$n^{|k|} = 1 + r|\ell|.$$

Therefore

$$|k|s\ p^t = r|\ell| - (\frac{|k|(|k|-1)}{2} s^2 p^{2t} + \ldots).$$

Since $(|k|,p) = 1$, and p^t divides $|\ell|$ but $p^t \neq |\ell|$, then p divides s which contradicts the maximality of t. This gives us that $k \in C(L)$ for all $k \in K$. Clearly $L \cap K \leq C(L)$, so $H \leq C(L)$ which proves the theorem since all subgroups H such that $H \geq L$ are normal in G.

<u>Lemma 3.3.8</u>. If L is an elementary abelian p-group or a cyclic p-group, then $G/C(L)$ is a cyclic group whose order divides $p-1$.

Proof: Case 1. L is a cyclic p-group. Let $|L| = p^r$. Then $A(L)$ is a cyclic group of order $p^{r-1}(p-1)$ [5, page 120]. $G/C(L)$ is isomorphic to a subgroup of $A(L)$ and since $(|G:L|, |L|) = 1$, $G/C(L)$ is a cyclic group whose order divides $p-1$.

Case 2. L is an elementary abelian p-group. Let n_g be defined by $\ell^g = \ell^{n_g}$ where $\ell \in L$. (This is well-defined by Theorem N). Let F_p^* be the multiplicative group of the integers modulo p. Let $\varphi(g) = n_g$ so that φ is a map from G into F_p^*. φ is a homomorphism since $x^{n_{gh}} = x^{gh} = (x^g)^{n_h} = x^{n_g n_h}$ which implies $n_{gh} \equiv n_g n_h \bmod p$. The kernel of φ is $\{g \in G | n_g \equiv 1 \bmod p\}$. Since L is elementary abelian, the kernel of φ also equals $\{g \in G | \ell^g = \ell$ for all $\ell \in L\} = C(L)$. Therefore $G/C(L)$ is isomorphic to a subgroup of F_p^*. F_p^* is a cyclic group of order $p-1$, so that again we have the conclusion of the lemma.

Combining the results of these Lemmas with the condition that $n(G) = 2$ provides the proof of the final theorem of this thesis.

Theorem 3.3.9. Let G be a solvable, non-nilpotent, t-group where G/L is the maximal nilpotent factor group of G. $n(G) = 2$ if and only if G has one of the following three sets of properties:

1. G/L is a cyclic group of order q^m, $m \geq 2$, $|C(L)| = pq$ and $|L| = p$.
2. G/L is a cyclic group of order qr, L is a cyclic p-group, and $C(L) = L$.
3. G/L is a cyclic group of order qr, L is an elementary abelian p-group, and $C(L) = L$.

In all three cases p, q, and r are distinct primes.

Proof: Assume $n(G) = 2$. Theorem N says that G/L is Dedekind and L is abelian. By Theorem 3.1.2, $2 = n(G) \geq n(G/L)$ so that $n(G/L) = 1$ or 2. Theorem B, Theorem 3.3.2, and the fact that G/L is Dedekind implies that G/L is isomorphic to a cyclic q-group, an elementary abelian q-group, the quaternions, or a cyclic group of order the product of two primes q and r. ($G/L \not\cong H$ since H is not Dedekind). Again Theorem 3.1.2 implies that $2 = n(G) \geq n(L)$. L abelian together with Theorem 3.3.1 gives that $n(L) = 1$ so that L is isomorphic to a cyclic p-group or an elementary abelian p-group by Theorem A. Because of Lemma 3.3.8 $G/C(L)$ is cyclic so that in the two cases where G/L is an elementary abelian q-group or the quaternions, $|G/C(L)| = q$ or 2. Under these same conditions Lemma 3.3.6 implies that $C(L)$ is abelian. By Theorem N there is also a non-abelian normal subgroup of G containing L of the same order as $C(L)$. This accounts for at least two orbits. Since $|C(L)|$ is divisible by two primes, and $C(L)$ is abelian, clearly at least one more orbit exists which is a contradiction. Therefore G/L cannot be an elementary abelian q-group or the quaternions. In the remaining possibilities G/L is cyclic so that $C(L)$ may be L. In the case where G/L is a cyclic q-group and L is a cyclic p-group, if $C(L) = L$, Lemma 3.3.7 implies that G has only one chief series which contradicts $n(G) = 2$. If G/L is a cyclic q-group, L is an elementary abelian p-group, and $C(L) = L$, then Lemma 3.3.7 implies that all chief series contain L, so that if $s_1, s_2 \in C_G$ then they can be written in the form

$$s_1\colon G = (g,L) > (g^q,L) >\ldots> (L) > (a_1,\ldots,a_{m-1}) >\ldots> (a_1) > (1)$$

$$s_2\colon G = (g,L) > (g^q,L) >\ldots> (L) > (b_1,\ldots,b_{m-1}) >\ldots> (b_1) > (1)$$

where $(gL) = G/L$ and $L = (a_1,\ldots,a_m) = (b_1,\ldots,b_m)$, and $a_i^g = a_i^n$ and $b_i^g = b_i^n$ by Theorem N. (Note that n does not depend on which element of L is conjugated by g). Let α be defined by $a_i^\alpha = b_i$ and $g^\alpha = g$. $\alpha \in A(G)$ since it preserves the relations of G. Since

$s_1^\alpha = s_2$, $n(G) = 1$ and this eliminates this possibility. If G/L is a cyclic q-group and $C(L) > L$, then $C(L)$ is divisible by both p and q. If $C(L)$ is divisible by p^2 or q^2 then $C(L)$ contains at least three non-isomorphic chief series, and since G is a t-group and $C(L) \lhd G$ they can be extended to non-isomorphic chief series of G which implies that $|C(L)| = pq$. This group where G/L is a cyclic q-group, $|C(L)| = pq$, and $|L| = p$ is the group mentioned in 1. In the case of a group as in 1, $C(L)$ is cyclic so by Lemma 3.3.7 G has exactly two non-isomorphic chief series: one containing $C(L)$ and L, and the other containing $C(L)$ and the q-Sylow subgroup of $C(L)$. This proves that such a group does have $n(G) = 2$. The only possibilities left are where G/L is a cyclic group of order qr where q and r are primes. If $C(L) > L$, then there are at least three non-isomorphic chief series in G in the same way as in the case when G/L was elementary abelian q-group or the quaternions, so that $C(L) = L$. With $C(L) = L$ and G/L cyclic of order qr we have the two groups of 2 and 3. If L is a cyclic p-group as in 2, then clearly G has $n(G) = 2$ when $|G/L| = qr$, L is an elementary abelian p-group, and $C(L) = L$. There are, by Lemma 3.3.7, two kinds of chief series: those containing the normal subgroup of index r and those containing the normal subgroup of index q. In either case, all chief series of that kind can be shown to be in the same orbit in the same way as we proved that if G/L is a cyclic q-group, L is an elementary abelian p-group, and $C(L) = L$, then $n(G) = 1$. This completes the proof of the theorem.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Burnside, W., Theory of Groups of Finite Order (New York: Dover Publications, Inc., 1955).

2. Gaschütz, W., "Gruppen, in denen das Normalteilersein transitiv ist," Journal für die Reine und Angewandte Mathematik, 198 (1957), 87-92.

3. Hall, M., The Theory of Groups (New York: Macmillian, 1959).

4. Polimeni, A., A Study of the Automorphisms and Chains of a Finite Group, Thesis for the Degree of Ph.D., Michigan State University, 1965.

5. Scott, W.R., Group Theory (Englewood Cliffs, New Jersey: Prentice Hall, 1964).

6. Taunt, D.R., "On A-groups," Proceedings of the Cambridge Philosophical Society, 45 (1949), 24-42.

APPENDIX

APPENDIX

Theorem A [4, page 11]. Let G be an abelian group. Then $(A(G), C_G)$ is transitive if and only if G is an elementary abelian p-group or a cyclic p-group, for some prime p.

Theorem B [4, page 14]. Let G be a nilpotent group. Then $(A(G), C_G)$ is transitive if and only if G is one of the following:

1. G is an elementary abelian p-group for some prime p,
2. G is a cyclic p-group for some prime p,
3. G is isomorphic to the quaternion group of order 8.

Theorem C [4, page 17]. If G is a supersolvable, non-nilpotent group and $A(G), C_G)$ is transitive then $G = S_p \cdot S_q$, p and q primes, where S_p is a p-Sylow subgroup of G and S_q is a q-Sylow subgroup of G. Furthermore if $q < p$ it follows that

1. $S_p = G'$,
2. Every subgroup of S_p is normal in G,
3. S_p is either cyclic or elementary abelian,
4. S_q is elementary abelian or cyclic,
5. $Z(G) = (1)$.

Theorem D [4, page 26]. If $(A(G), C_G)$ is transitive and 2 does not divide $|G|$ then the following are true:

1. The lower nilpotent series of G coincides with the derived series of G,
2. Each term $G^{(k)}$ of the derived series for G is complemented in G by the relative system normalizer of $G^{(k-1)}$ in G,

3. There exists r subgroups $H_1, H_2, \ldots, H_r$, r the length of the derived series for G, such that

a. Each H_i is either a cyclic p_i-group or an elementary abelian p_i-group for some prime p_i,

b. $G^{(k)} = H_r H_{r-1} \cdots H_{k+1}$ for $k = 0,1,\ldots,r-1$,

c. $H_i H_j = H_j H_i$ for all i,j and $H_i \cap H_j = (1)$ if $i \neq j$,

4. $Z(G) = (1)$,

5. $\Phi(G) = (1)$ if $r > 2$,

6. $G^{(k)}/G^{(k+1)}$ is an elementary abelian group for $k = 2,3,\ldots,r-1$.

Theorem E [5, page 167]. If G is a finite group then $\mathrm{Fit}(G) \geq \Phi(G)$.

Theorem F [5, page 170]. If G is a finite solvable group then $\mathrm{Fit}(G)/\Phi(G) = \mathrm{Soc}(G/\Phi(G))$.

Theorem G [5, page 157]. If G is a supersolvable group then G' is nilpotent.

Theorem H [3, page 159]. A supersolvable group G has a normal series $G = C_0 > C_1 > \ldots > C_k = (1)$ in which every C_{i-1}/C_i is either infinite cyclic or cyclic of prime order, and if C_{i-1}/C_i and C_i/C_{i+1} are of prime orders p_i and p_{i+1} we have $p_i \leq p_{i+1}$.

Theorem I. A finite supersolvable group G has a normal p-Sylow subgroup if p is the largest prime divisor of $|G|$.

Proof: The proof follows from Theorem H.

Theorem J [6]. If G is an A-group then $G' \cap Z(G) = (1)$.

Theorem K [1, page 132]. If a group G, of order 2^m, has a single subgroup of order 2^s $(s > 1)$, it must be cyclic; if it has a single subgroup of order 2, it is cyclic or isomorphic to Q_m.

Theorem L [1, page 131]. If G, of order p^m, where p is an odd prime, contains only one subgroup of order p^s, $s = 1,\ldots,m-1$, then G is cyclic.

Theorem M [3, page 190]. A Hamiltonian group is the direct product of a quaternion group with an abelian group in which every element is of finite odd order and an elementary abelian 2-group.

Theorem N [2, page 88]. Let G be a solvable t-group, G/L be the maximal nilpotent factor group of G. Then

1. G/L is Dedekind,
2. $|L|$ is odd,
3. L is abelian,
4. $(|G/L|, |L|) = 1$,
5. The inner automorphisms of G induce power automorphisms on L with power n, $(n, |L|) = 1$, in such a way that to each prime divisor p of $|L|$ there exists an n such that $n \not\equiv 1 \bmod p$.

Theorem P [2, page 89]. If G is a group, L a normal subgroup of G, and 1 and 4 of Theorem N hold along with (5^*) the inner automorphisms of G induce power automorphisms on L, then G is a solvable t-group. If (5) of Theorem M replaces (5^*), then G/L is the maximal nilpotent factor group of G.

Theorem Q [5, page 166]. If A and B are normal nilpotent subgroups of a group G, then AB is also a normal, nilpotent subgroup of G.

Theorem R [5, page 224]. If H is a normal Hall subgroup of a finite group G, then H has a complement.