0724

THE ORDER OF THE GROUP OF AUTOMORPHISMS

OF A FINITE P-GROUP

by

THEODOROS EXARCHAKOS

Thesis Submitted
for the Degree of
Doctor of Philosophy
at the University of London

Department of Mathematics
Royal Holloway College
University of London
July 1977

ABSTRACT

In this thesis we are mainly concerned with the order of the group $A(G)$ of automorphisms of a finite p-group G.

First we determine the order of the group of central automorphisms $A_c(G)$ of G in terms of the invariants of its center Z and G/G', when G is a purely non-abelian group (PN-group). For the general case $G = H \times K$, where H is abelian and K is a PN-group we show that

$$|A_c(G)| = |A(H)||A_c(K)||\mathrm{Hom}(K,H)||\mathrm{Hom}(H,Z(K)|$$

so that the general case is reduced to that of PN-groups. By using the class c of G we then get

$$|A(G)| \geq |A_c(G)|.p^{c-1}$$

These results are used in Chapter 3 to study groups for which $|G|$ divides $|A(G)|$ (LA-groups). It is shown that a non-abelian group G is an LA-group if it has any one of the following properties: (i) order p^n, $n \leq 6$, (ii) homocyclic lower central factors and $\exp G/G' \leq |Z|$, (iii) cyclic Frattini subgroup, (iv) certain normal subgroups of maximal class, (v) all two-maximal subgroups abelian, (vi) $|G/Z| \leq p^3$.

In Chapter 4 we find a new bound for the function $g(h)$ for which $|A(G)|_p \geq p^h$ whenever $|G| \geq p^{g(h)}$ We reduce the previous best bound $g(h) = \frac{1}{2}h(h-3) + 3$ obtained by K.H. Hyde in [32] to $g(h) = \frac{1}{6}h^2$.

ACKNOWLEDGEMENTS

I wish to express my deep gratitude to Dr M.V.D. Burmester of Royal Holloway College under whose guidance and supervision this thesis was prepared. His helpful suggestions at every stage of this work were of the greatest value to me. I would like also to thank Professor H.G. Eggleston for his encouragement, especially during the first year of my studies at Royal Holloway College. Finally I owe a special debt to the Greek State Scholarships Foundation for the financial support of this research.

TABLE OF CONTENTS

INTRODUCTION

The number of automorphisms of a finite p-group G has been an interesting subject of research for a long time. Although a large number of papers have appeared on this topic, the size of the order of the automorphism group A(G) of G is a question which still remains open. Part of this interest has been focused upon the role played by the group $A_c(G)$ of central automorphisms of G. Our contribution consists in establishing the size of the order of the group $A_c(G)$. For PN-groups G, that is for purely non-abelian p-groups, we determine the order of $A_c(G)$ in terms of the invariants of G/G' and its center Z. Then, when G = HxK, where H is abelian and K a PN-group, we show that $|A_c(G)| = |A(H)||A_c(K)||\mathrm{Hom}(K,H)||\mathrm{Hom}(H,Z(K))|$ and $|A(G)| \geq |A(H)||A(K)||\mathrm{Hom}(K,H)||\mathrm{Hom}(H,Z(K))|$ Finally we use the class c of G to obtain an even larger number of automorphisms. These results are used to study LA-groups, that is groups for which $|G|$ divides $|A(G)|$, and to obtain a new bound for the function g(h) for which $|A(G)|_p \geq p^h$ whenever $|G| \geq p^{g(h)}$.

It has been conjectured that if G is a non-cyclic finite p-group of order p^n, $n > 2$, then G is an LA-group. This has been established for abelian p-groups and for certain other classes of p-groups [14], [15], [16], [42]. In Chapter 3 we extend this result to p-groups G which have any one of the following conditions: (i) order p^n, $n \leq 5$ or for $p \neq 2$, $n \leq 6$, (ii) homocyclic lower central factors and exp $G/G' \leq |Z|$, (iii) cyclic Frattini subgroup,

(iv) a normal subgroup H of maximal class with G/H either elementary abelian or cyclic of order p^2, (v) a maximal subgroup M which has a homomorphic image of maximal class, (vi) $|G/Z| \leq p^3$, (vii) all two-maximal subgroups abelian.

In Chapter 4 we consider functions g(h) such that if $|G| \geq p^{g(h)}$ then $|A(G)|_p \geq p^h$. The existence of such functions was first conjectured by W.R. Scott [43] who proved that g(2) = 3. Ledermann and Neumann proved that in the general case of finite groups $(h-1)^3p^{h-1} + h$ works [36]. J.A. Green [20] and J.C. Howarth [29] have reduced this bound. The best (least) bound to date for finite p-groups is due to K.H. Hyde [32] and it is $g(h) = \frac{1}{2}h(h-3) + 3$ for $h \geq 5$, $g(h) = h + 1$ for $h \leq 4$. We improve this to $g(h) = \frac{1}{6}h^2$ for $h \geq 12$, $g(h) = 2h - 2$ for $h \leq 11$ and $g(h) = h$ for $h \leq 5$. This is definitely not the best possible. For example, by using a more elaborate technique we can reduce this bound to $g(h) = \frac{1}{7}h^2$ for $h \geq 50$. Finally we consider the case when h is relatively large compared to c. Then we get $g(h) = \frac{1}{2}h(h-c)$ for $h \geq c + \sqrt{3c-6}$. Also we show that if $p^{nc} \geq |G|$, n an integer, then we can take g(h) as a linear expression of h.

CHAPTER ONE

1. Notations and Definitions

Throughout this thesis, G is taken to be a finite p-group, p a prime number. We write $H \leq G$ if H is a subgroup of G, $H < G$ if H is a proper subgroup of G, $H \lhd G$ if H is a normal subgroup of G and H Char G if H is a characteristic subgroup of G. For a subset A of G, $\langle A\rangle$ denotes the subgroup of G generated by A. For abbreviation $\langle\{a_1, a_2, \ldots, a_n\}\rangle = \langle a_1, a_2, \ldots, a_n\rangle$. The commutator $[a, b]$, $a, b \in G$ is $a^{-1} b^{-1} ab$. Also for $H, K \leq G$, $[H, K] = \langle [h, k] \mid h \in H, k \in K\rangle$, and we have $[H, K] \lhd \langle H, K\rangle$. We denote the commutator subgroup $[G, G]$ of G by G' and the center $Z(G)$ of G by Z. For $H \leq G$, $N_G(H)$, $C_G(H)$ is the normalizer, centralizer of H in G respectively. Also $P_i(G) = \langle x^{p^i} \mid x \in G\rangle$ and $E_i(G) = \langle x \in G \mid x^{p^i} = 1\rangle$. Both $P_i(G)$ and $E_i(G)$ are characteristic subgroups of G; we write P(G) for $P_1(G)$ and E(G) for $E_1(G)$. The order of G is denoted by $|G|$ and $|H|_p$ is the greatest power of p which divides $|H|$. We write $[G:H]$ for the index of the subgroup H of G in G. If $x^{p^n} = 1$ for every $x \in G$ we say that G has exponent p^n and we write $\exp G = p^n$. Any finite abelian p-group H of order p^a can be written as a direct product of cyclic groups $H = C(p^{a_1}) \times C(p^{a_2}) \times \ldots \times C(p^{a_r})$, where $C(p^{a_i})$ is cyclic of order p^{a_i}, $a_1 \geq \ldots \geq a_r \geq 1$ and $\sum_{i=1}^{r} a_i = a$.

The numbers $a_1, a_2, \ldots, a_r$ are called the invariants of H. The integer r and the invariants of H are uniquely determined (to within a reordering) and we say that H is of type

$(a_1, a_2, \ldots, a_r)$. A group of type $(a, a, \ldots, a)$ is called homocyclic and a group of type $(1, 1, \ldots, 1)$ is called elementary abelian. Letting $G = L_o(G)$ and defining $L_{i+1}(G) = [L_i(G), G]$ we get the lower central series of G: $G=L_o(G) > \ldots$. Similarly letting $Z_o(G) = 1$ and defining $Z_{i+1}(G) = \{x \in G \mid [x, y] \in Z_i \text{ for all } y \in G\}$ we get the upper central series of G: $1 < Z_1(G) < \ldots$. G is nilpotent of class c if, and only if $L_c(G) = 1$, while $L_{c-1}(G) \neq 1$, or equivalently, if, and only if $Z_c(G) = G$, while $Z_{c-1}(G) \neq G$. Thus for a nilpotent group G the lower and the upper central series of G have the same length c. Finite p-groups are always nilpotent. We take the lower and the upper central series of G to be:

$G = L_o(G) > L_1(G) = G' > \ldots > L_{c-1}(G) \neq 1 > L_c(G) = 1.$

$1 = Z_o(G) < Z_1(G) = Z < \ldots < Z_{c-1}(G) \neq G < Z_c(G) = G.$

It can be shown that $L_i(G) \leq Z_{c-i}(G)$ and $L_i(G) \nleq Z_{c-i-1}(G)$ for all i. When there is no possibility of confusion we write L_i for $L_i(G)$ and Z_i for $Z_i(G)$. If G is abelian, $L_1 = G' = 1$, $Z = G$ so that $c = 1$. If G is non-abelian of order p^n, G has <u>large class</u> c if $2c > n$, and G has maximal class if $c = n-1$. In the second case

$|G/L_1| = |G/Z_{c-1}| = p^2, \quad |L_i/L_{i+1}| = |Z_i/Z_{i-1}| = p$

so that $L_i = Z_{c-i}$ for all i. If G has order p^n and M is a maximal subgroup of G, then M has order p^{n-1} and $M \lhd G$. A maximal subgroup of a maximal subgroup of G is called a <u>two-maximal</u> subgroup of G. The intersection $\Phi(G)$ of all maximal subgroups of G is called the Frattini subgroup of G. $G/\Phi(G)$ is elementary abelian and $\Phi(G)$ contains the elements of G which are not generators of G. For $|G/\Phi(G)| = p^d$, $d = d(G)$ is the minimal number of generators of G. G is called a PN-group (purely non-abelian group) if it has no non-trivial abelian direct factor. G is called metacyclic if it has a normal subgroup H such that both H and G/H are cyclic. G is p-abelian if $(ab)^p = a^p b^p$ for all a, b $\in$ G. It can be shown that G is p-abelian if, and only if, G is regular and exp $G' = p$. G is regular if for every a, b $\in$ G, $(ab)^p = a^p b^p c^p$ for some $c \in \langle a,b\rangle'$. For $p \neq 2$ if G' is cyclic, G is regular. G is called absolutely regular if $|G/P(G)| < p^p$. An absolutely regular p-group is always regular ([23], p. 472). Absolutely regular 2-groups are cyclic and absolutely regular 3-groups are meta-cyclic. For any group H, Hom (G, H) is the set of all homomorphisms of G into H. Finally if H is abelian Hom (G, H) $\cong$ Hom (G/G', H).

2. Elementary Properties

The following properties apply to all finite p-groups. Proofs are not given; they can be found in [21], [22], [31], [44] and [49].

1. Every finite p-group is both nilpotent and soluble.
2. The center Z of G is not trivial and if $|G| = p^2$, G is abelian.
3. If G is non-abelian, both G/G' and G/Z_{c-1} are not cyclic.
4. For $j \geq i$, $[Z_j, L_{i-1}] \leq Z_{j-i}$; in particular $[Z_i, L_{i-1}] = 1$. If G has class c, $[L_i, L_{c-i-1}] = 1$, and if r is the greatest integer with $r \leq \frac{1}{2}c$, then L_r is abelian.

Let H be a normal subgroup of G.

5. G/H is elementary abelian if, and only if, $\Phi(G) \leq H$. Also $\Phi(G/H) = \Phi(G)H/H$ and $G = \Phi(G)H$ implies $G = H$.

6. If G/G' has t invariants, then G can be generated by t elements.

7. If $H \neq 1$, $H \cap Z \neq 1$; if $|H| = p$, $H \leq Z$.

8. $|H| = p^2$ implies that H is contained in the center of some maximal subgroup of G.

9. $|H| = p^i$ implies $H \leq Z_i$.

10. H has a maximal subgroup which is normal in G.

11. $L_i(G/H) = L_i(G)\,H/H$ for all i.

12. If H, K, L are normal subgroups of G, then $[HK, L] = [H,L]\,[K,L]$ and $[H,[K,L]] \leq [[H,K],L]\,[[H,L],K]$.

3. Known Results

Throughout this thesis we use a number of known results on finite p-groups and their automorphisms. Some of these results are used quite frequently and are listed below for the reader's convenience.

Theorem 1.1 [40]. If G is non-cyclic abelian of order p^n, $n > 2$ then $|A(G)|_p \geq |G|$.

Theorem 1.2 [16]. If G is non-abelian of class two then $|A(G)|_p \geq |G|$.

Theorem 1.3 [42]. If $|G| > p^2$ and $x^p = 1$ for every $x \in G$ then $|A(G)|_p \geq |G|$.

Theorem 1.4 [12]. If G is a non-cyclic metacyclic p-group, $p \neq 2$, of order p^n, $n > 2$, then $|A(G)|_p \geq |G|$.

Theorem 1.5 [14]. If G/Z is a non-trivial metacyclic p-group, $p \neq 2$, then $|A(G)|_p \geq |G|$.

Theorem 1.6 [18]. If G is non-abelian, it has an outer automorphism of order p^i for some $i \geq 1$.

Theorem 1.7 [30]. If G is the central product of non-trivial subgroups H and K, where H is abelian and $|A(K)|_p \geq |K|$, then $|A(G)|_p \geq |G|$.

Theorem 1.8 [48]. If $|G/Z| = p^k$, then G' has order at most $p^{\frac{1}{2}k(k-1)}$.

Theorem 1.9 [11]. Let G have order p^n, $p \neq 2$, $n \geq 5$ and r be a fixed integer $3 \leq r \leq n-2$. If all normal subgroups of G of order p^r have two generators, then either G is metacyclic, G is a 3-group of maximal class or $r = 3$ and the elements of G of order at most p form a non-abelian normal subgroup E of G of order p^3 with G/E cyclic and $P(G) \leq C_G(E)$.

Theorem 1.10 [10]. If $m_1 \geq m_2 \geq \ldots \geq m_t \geq 1$ are the invariants of G/G', then $p^{m_2} \geq \exp L_1/L_2 \geq \exp L_2/L_3 \ldots \geq \exp L_{c-1}/L_c$. For $t = 2$, L_1/L_2 is cyclic of order at most p^{m_2}.

Theorem 1.11 [5]. Let G be non-abelian. If $\Phi(G)$ is cyclic and Φ_o is its subgroup of order p, then $G = AB$, where A is the group generated by Φ_o and all normal subgroups of G of type (p, p) containing Φ_o and B is either cyclic or a 2-group of maximal class. If B is cyclic, $\Phi(G) \leq Z$ and G' has order p. If B has maximal class, $G' = \Phi(G)$ and $|B| = 4|\Phi(G)|$.

Theorem 1.12 [39]. If G is a two-generator finite p-group of class c, then $Z_{c-1} \leq \Phi(G)$ and $\exp G/Z_{c-1} = \exp L_{c-1}$.

Theorem 1.13 ([27], [28]). If H is a subgroup of G such that $L_i(H) = L_i(G)$ for some i, then $L_{i+r}(H) = L_{i+r}(G)$ for any positive integer r. If G has two generators and $L_i(G) \neq 1$, then $L_i(H) < L_i(G)$ for any proper subgroup H of G.

Theorem 1.14 [47]. If G has cyclic center and N is an abelian normal subgroup of G such that G/N is cyclic of order p^k, then L_{c-1} is cyclic or order dividing p^k. For $|L_{c-1}| = p^k$, L_i/L_{i+1} is cyclic of order p^k for all $i = 1, \ldots, c-1$. Morover G/L_1Z is abelian of type (p^k, p^k).

Theorem 1.15 [17]. If G has class c and L_i/L_{i+1} is cyclic of fixed order p^r for all $i = 1, \ldots, c-1$, then $L_i \cap Z_{c-i-1} = L_{i+1}$ and $|G/Z_{c-1}| = p^{2r}$.

Theorem 1.16 [37]. If $P(G) \leq Z$, then $P(L_i) \leq L_{ip}$ for $i \geq 1$.

4. Further Basic Results

In this section we prove some theorems on finite p-groups, which shall be needed in the following.

Theorem 1.17. If $Z_2(G)$ is cyclic, then either G is cyclic or G is a 2-group of maximal class.

Proof: G cannot have a normal subgroup H of type (p, p) since then by Property 9, $H \leq Z_2$. So by [4] (Theorem 2.3) G is one of the following groups: a) cyclic, b) dihedral, c) semidihedral, or d) the generalized quaternian group. But the groups b), c), d) are all 2-groups of maximal class ([19], (Theorem 5.4.3).

Theorem 1.18. Let $p \neq 2$. If $Z_3(G)$ is metacyclic, then G is either metacyclic or of maximal class.

Proof: G cannot have a normal subgroup H of order p^3 and exponent p, since then by Property 9, $H \leq Z_3$ and H would be metacyclic. By [11] G is either of maximal class or absolutely regular. In the second case G is regular and so $|G/P(G)| = |E(G)|$. But $\exp E(G) = p$, as G is regular. So $|G/P(G)| = |E(G)| \leq p^2$. Then by [9], G is metacyclic.

Remark 1. Let $H \lhd G$ and $H \cap Z_2$ be cyclic. Then either H is cyclic or H has maximal class. (In fact H contains no normal subgroups of G of type (p, p).)

Theorem 1.19. Let G have class c, L_i/L_{i+1} be cyclic for some i, $1 \leq i \leq c-1$, and all maximal subgroups of L_i be normal in G. Then L_i is cyclic and L_{i+1}/L_{i+2} is cyclic of order at most $|L_i/L_{i+1}|$.

Proof: Since $L_i/\Phi(L_i)$ is elementary abelian and L_i/L_{i+1} is cyclic, $L_i/L_{i+1}\Phi(L_i)$ is both elementary abelian and cyclic. Hence it has order at most p. But $L_i \neq L_{i+1}\Phi(L_i)$, since otherwise $L_i = L_{i+1}$ (Property 5). Hence $L_{i+1}\Phi(G)$ is a maximal subgroup of L_i. If M is another maximal subgroup of L_i, then $L_i/M \leq Z(G/M)$ as $M \lhd G$, so $L_{i+1} = [L_i, G] \leq M$. But $\Phi(L_i) \leq M$, so that $L_{i+1}\Phi(L_i) \leq M$ which gives $L_{i+1}\Phi(L_i) = M$. Hence L_i has only one maximal subgroup and is therefore cyclic. So L_r/L_{r+1} is cyclic, for $r \geq i$ and $\exp L_{i+1}/L_{i+2} \leq \exp L_i/L_{i+1} = |L_i/L_{i+1}|$ (Theorem 1.10).

Corollary 1.19.1. Let G be of order p^n and class c. If G/G' has order p^m and type (p, p^{m-1}) and all maximal subgroups of G' are normal in G, then G' is cyclic and $c = n-m+1$.

Proof: By Theorem 1.10, L_1/L_2 is cyclic of order p and $\exp L_i/L_{i+1} = p$ for $i = 1, \dots , c-1$. By Theorem 1.19, $L_1 = G'$ is cyclic and L_i/L_{i+1} is cyclic of order p. This is true for $i = 1, \dots , c-1$. So $c = n-m+1$.

Corollary 1.19.2. If G/G' has order 4, then G is of maximal class.

Proof: From [9], G has a maximal subgroup which is cyclic. So G' is cyclic and $c=n-1$ (Corollary 1.19.1).

Theorem 1.20. Let $G = HK$, where H and K are both normal in G and $H \cap K$ is contained in either $L_1(H)$ or $L_1(K)$. Then $L_i(G) = L_i(H)L_i(K)$ for all i.

Proof: For $i = 0$, $G = L_0(G) = L_0(H)L_0(K) = HK$. Proceed by induction on i. Then $L_i(G) = L_i(H)L_i(K)$ gives $L_{i+1}(G) = [L_i(G),G] = [L_i(H)L_i(K),HK] = [L_i(H),H][L_i(H),K]$ $[L_i(K),H][L_i(K),K] = L_{i+1}(H)[L_i(H),K][L_i(K),H]L_{i+1}(K)$ (2), as $L_i(H) \lhd G$ and $L_i(K) \lhd G$. Take $H \cap K \leq L_1(H)$. Then $[H,K] = [L_0(H), K] \leq H \cap K \leq L_1(H)$ since both H and K are normal in G. If we assume that $[L_i(H),K] \leq L_{i+1}(H)$, then $[L_{i+1}(H),K] = [[L_i(H),H],K] \leq [[L_i(H),K],H][L_i(H),[H,K]]$ $\leq [L_{i+1}(H),H][L_i(H),L_1(H)] = L_{i+2}(H)[L_i(H),[H,H]] \leq L_{i+2}(H)$ $[[L_i(H),H],H] = L_{i+2}(H)$. Therefore $[L_i(H),K] \leq L_{i+1}(H)$ for all i. Similarly $[L_i(K),H] \leq L_{i+1}(H)$ for all i. So (2) reduces to $L_{i+1}(G) = L_{i+1}(H)L_{i+1}(K)$. On the other hand if $H \cap K \leq L_1(K)$, as above $[L_i(H),K] \leq L_{i+1}(K)$ and

$[L_i(K),H] \leq L_{i+1}(K)$, so (2) reduces again to $L_{i+1}(G) = L_{i+1}(H)L_{i+1}(K)$ and the proof is complete.

Theorem 1.21.

(i) $\exp L_i/L_{i+1} \leq \exp G/Z$ for $i \geq 1$,

(ii) $\exp L_{i+1} \leq [L_i : L_i \cap Z]$ for $i \geq 0$,

(iii) If G is regular, $\exp L_1 = \exp G/Z$.

Proof: (i) For $a, b \in G$, $[[a, b], a] \in L_2$. Hence $[a, b]^a \equiv [a, b] \bmod L_2$ and so $[a^2, b] = [a, b]^a[a,b] \equiv [a,b]^2 \bmod L_2$. Similarly $[a^n, b] \equiv [a, b]^n \bmod L_2$ for any integer n. Therefore if $\exp G/Z = p^t$, $[a, b]^{p^t} \in L_2$ and so $\exp L_1/L_2 \leq p^t$. By Theorem 1.10, $\exp L_i/L_{i+1} \leq \exp L_1/L_2 \leq p^t$ for $i \geq 1$.

(ii) Take $[L_i : L_i \cap Z] = p^a$. For $x \in L_i$, $x^{p^a} \in L_i \cap Z \leq Z$. Let τ be the transfer homomorphism of L_i into $L_i \cap Z$, so that $\tau(x) = \prod_j a_j x^{p^{m_j}} a_j^{-1}$, where $\sum_j p^{m_j} = p^a$ and m_j is minimal such that $a_j x^{p^{m_j}} a_j^{-1} \in L_i \cap Z$. Then $a_j x^{p^{m_j}} a_j^{-1} = x^{p^{m_j}}$ so that $\tau(x) = x^{p^a}$ Since L_i char G, for $y \in G$, $\tau([x, y]) = \tau(x^{-1}y^{-1}xy) = \tau(x^{-1})\tau(y^{-1}xy) = x^{-p^a}(y^{-1}xy)^{p^a} = x^{-p^a}y^{-1}x^{p^a}y = 1$. But $\tau([x,y]) = [x,y]^{p^a}$ and so $[x,y]^{p^a} = 1$ for $x \in L_i$, $y \in G$. Therefore $\exp L_{i+1} \leq p^a$. Observe that for $i = 0$, $\exp L_1 \leq [G : Z]$.

(iii) Since G is regular $[a^n,b] = 1$ if, and only if, $[a,b]^n = 1$ for $a, b \in G$ ([21], Theorem 12.4.3). Take $\exp L_1 = p^r$, $\exp G/Z = p^s$. Since $[a,b]^{p^r} = 1$, $[a^{p^r},b] = 1$ for every $b \in G$, so that $a^{p^r} \in Z$ which give $s \leq r$.

Conversely, since $a^{p^s} \in Z$ for every $a \in G$, $[a^{p^s},b] = 1$ for every $b \in G$. So $[a,b]^{p^s} = 1$ for every a, $b \in G$ and $r \leq s$. Therefore $r = s$.

<u>Theorem 1.22</u>. Let G have two generators. If G has a maximal subgroup M which is of maximal class, then G has maximal class.

<u>Proof</u>: Let $|G| = p^n$ and G have class c. Then M has class n-2, as $|M| = p^{n-1}$. So $c \geq n-2$. We now proceed assuming $c = n-2$ and get a contradiction. Consider the lower central series of G and M, $G = L_o > L_1 > \ldots > L_c = 1$, $M = \bar{L}_o > \bar{L}_1 > \ldots. > \bar{L}_c = 1$, where $c = n-2$. For $i = 0$, $\bar{L}_o = M < G = L_o$. Furthermore $\bar{L}_i \leq L_i$ gives $\bar{L}_{i+1} = [\bar{L}_i,M] \leq [L_i,G] = L_{i+1}$. So $\bar{L}_i \leq L_i$ for all i. Since M has maximal class, $|M/\bar{L}_1| = p^2$ and $|\bar{L}_i/\bar{L}_{i+1}| = p$ for $i = 1, \ldots , c-1$. Also $|G/L_1| \leq p^3$, since G has order p^n and class n-2. For $|G/L_1| = p^3$, $|G/L_1| = p^3 = |G/M|\ |M/\bar{L}_1| = |G/\bar{L}_1|$ so that $|L_1| = |\bar{L}_1|$. Since $\bar{L}_1 \leq L_1$, $\bar{L}_1 = L_1$, a contradiction by Theorem 1.13. As $|G/L_1| > p$, since G/L_1 cannot be cyclic, we have that G/L_1 is elementary abelian of order p^2. Then $|L_1/L_2| = p$ (Th. 1.10) and so $|G/L_2| = p^3 = |G/\bar{L}_1|$, which gives $|L_2| = |\bar{L}_1|$. Since $\bar{L}_1 \lhd G$ and $|L_1/\bar{L}_1| = p$ we have $L_1/\bar{L}_1 \leq Z(G/\bar{L}_1)$ which gives $L_2 = [L_1,G] \leq \bar{L}_1$. Since $|L_2| = |\bar{L}_1|$, $L_2 = \bar{L}_1$. Assume by induction that $L_{i+1} = \bar{L}_i$. Then $L_{i+2} = [L_{i+1},G] \geq [\bar{L}_i,M] = \bar{L}_{i+1}$. Since $\bar{L}_i = L_{i+1} > L_{i+2} \geq \bar{L}_{i+1}$ and $|\bar{L}_i/\bar{L}_{i+1}| = p$, $L_{i+2} = \bar{L}_{i+1}$. So $L_{i+1} = \bar{L}_i$ for all $i \geq 1$. Then $1 = L_c = \bar{L}_{c-1} \neq 1$, a contradiction.

<u>Corollary 1.22.1</u>. If G is not of maximal class but it has a maximal subgroup which is of maximal class, then G/L_1 is elementary abelian of order p^3.

<u>Proof</u>: G has more than two generators and so G/L_1 has more than two invariants. Since $|G/L_1| \leq p^3$, G/L_1 is elementary abelian of order p^3.

<u>Theorem 1.23</u>. Let G have class $c > 2$. If G has a maximal subgroup M which is abelian, then

(i) $M = C_G(G') = C_G(Z_2)$,

(ii) $Z_i < M$ and $M/Z_i \simeq L_i$ for $i \neq 0$, c,

(iii) For $a \in G \setminus M$, $a^p \in Z$,

(iv) $\exp L_i/L_{i+1} = \exp Z_{i+1}/Z_i = p$ for $1 \leq i \leq c-1$.

<u>Proof</u>: (i) Since $|G/M| = p$, $G' \leq M$ and since M is abelian $C_G(G') \geq M$. Hence $C_G(G') = M$, otherwise $G' \leq Z$ and G would have class two. But $[G',Z_2] = [[G,G],Z_2] \leq [[G,Z_2],G] \leq [G,Z] = 1$ and so $Z_2 \leq C_G(G')$. Therefore $C_G(Z_2) = M$ as $Z_2 > Z$.

(ii) For $i = 1, 2$, $Z_i < M$. So we assume $2 < i \leq c-1$. Let $a \in Z_2\setminus Z$, $b \in C_G(Z_i)\setminus Z$. Then $[a,b] = 1$ as $a \in Z_2 < Z_i$ and so $b \in C_G(a) \geq C_G(Z_2) = M$. But $a \notin Z$ and so $C_G(a) = M$. Hence $b \in M$. Since M is abelian and $b \notin Z$, $C_G(b) = M$. This is true for every $b \in C_G(Z_i)\setminus Z$. Hence $M = C_G(b) \geq Z_i$ and $Z_i \neq M$, as G/Z_i cannot be cyclic for $i \neq c$. Thus $Z_i < M$. By [45] $M/Z_i \cap M \simeq L_i$, so $M/Z_i \simeq L_i$.

(iii) For $x \in M$, $x \in C_G(a)$ if and only if $x \in Z$. Since G/M has order p, $a^p \in M$. So $a^p \in Z$.

(iv) Let $a \in G \setminus M$. Then $G = \langle a, M \rangle$ and we claim that $G' = \{ [a,b] \mid b \in M \}$. For $\{ [a,b] \mid b \in M \} = K$ is a group. Since $[a,b]^a = [a,b^a] \in K$, $K \lhd G$. Obviously $\langle a,K\rangle/K \le Z(G/K)$ and since M is abelian, G/K is abelian. Then $G' \le K$ and so $G' = K$, as $K \le G'$. For $x_1, x_2 \in G$ and any positive integer n, we have (cf the Proof of Theorem 1.21(i)) $[x_1, x_2^{\,n}] \equiv [x_1^{\,n}, x_2] \equiv [x_1, x_2]^n \bmod L_2$. Since $a^p \in Z$, $1 = [a^p, b]$ for any $b \in G$. Hence $[a,b]^p \in L_2$ and therefore $\exp L_1/L_2 = p$. But $\exp L_i/L_{i+1} \le \exp L_{i-1}/L_i$ and so $\exp L_i/L_{i+1} = p$ for $1 \le i \le c-1$. Now, let $y \in Z_2 \setminus Z$. Then $[a,y] \in Z$ and so $[a,y]$ commutes with both a and y. Hence $1 = [a^p, y] = [a,y]^p = [a, y^p]$ which implies that $y^p \in Z$ as $a \notin Z$. Therefore $\exp Z_2/Z = p$. But $\exp Z_{i+1}/Z_i \le \exp Z_i/Z_{i-1}$ and so $\exp Z_{i+1}/Z_i = p$ for $1 \le i \le c-1$.

<u>Theorem 1.24</u>. Let G be non-abelian. If G has more than one maximal subgroups which are abelian, then

(i) G has class two and $[G : Z] = p^2$,

(ii) G' has order p, and

(iii) G has two generators if, and only if, all maximal subgroups of G are abelian.

<u>Proof</u>: (i) If H, K are two distinct maximal subgroups of G which are abelian, then $G = HK$. Let $|G| = p^n$. Then $|H| = |K| = p^{n-1}$ and since

$|G| = |H|.|K|/|H \cap K|$, $|H \cap K| = p^{n-2}$. Every maximal subgroup of G which is abelian contains Z, otherwise G would be abelian. So $Z \leq H \cap K$. On the other hand $[G, H \cap K] = [HK, H \cap K] = [H, H \cap K][K, H \cap K] = 1$, as H, K are both abelian and normal in G. Therefore $H \cap K \leq Z$ and so $H \cap K = Z$. Hence Z has index p^2 in G and G/Z is abelian. So $G' \leq Z$ and G has class two.

(ii) Observe that G/H has order p, so $G = \langle a,H \rangle$ for some $a \in G \backslash H$. Then by Theorem 1.23, $G' = \langle [a,b] \mid b \in H \rangle$. Since $G' \leq Z$, G' has order equal to the number of conjugates of a in G. As $a \notin Z$, $C_G(a) = \langle a,Z \rangle$ is a maximal subgroup of G since Z has index p^2 in G and $\langle a,Z \rangle \neq G$ (G is non-abelian). Hence $p = [G : C_G(a)] = |G'|$.

(iii) Since G is non-abelian, G/Z cannot be cyclic and so it is elementary abelian of order p^2. Then G/Z has 1+p subgroups of order p. But every maximal subgroup of G, which is abelian, contains Z. Therefore G has 1+p maximal subgroups which are abelian. If G has two generators, $[G : \Phi(G)] = p^2$ and so G has precisely 1+p maximal subgroups which are therefore all abelian. Conversely, if all maximal subgroups of G are abelian, then Z is contained in every maximal subgroup of G and so $Z \leq \Phi(G)$. But G/Z is elementary abelian, so $\Phi(G) \leq Z$. Hence $\Phi(G) = Z$ and $[G : Z] = p^2 = [G : \Phi(G)]$. Therefore G can be generated by two elements. This proves the theorem.

In the following chapters we investigate the order of A(G), the group of automorphisms of G. It is well known that for cyclic groups $G = C(p^n)$, $|A(G)| = p^{n-1}(p-1)$, and for elementary abelian groups of order p^n, $|A(G)| = p^{\frac{1}{2}n(n-1)}(p^n-1)\ldots(p-1)$. So we restrict our attention to groups which are neither cyclic nor elementary abelian.

To find the order of $A(G)$ we first determine the order of $A_c(G)$, the group of central automorphisms of G (Chapter 2). By using the class c of G we then get $|A(G)|_p \geq |A_c(G)|_p . p^{c-1}$. These results are used in both Chapter 3 and Chapter 4. In Chapter 3 to study groups for which $|G|$ divides $|A(G)|$. In Chapter 4 to find a new bound for the function $g(h)$ such that $|A(G)|_p \geq p^h$ whenever $|G| \geq p^{g(h)}$.

CHAPTER TWO

CENTRAL AUTOMORPHISMS

An isomorphism ϕ of G onto itself is called an automorphism of G. The group of all automorphisms of G is denoted by A(G). For a fixed $c \in G$, the mapping ϕ_c defined by $\phi_c(x) = c^{-1} x c$, $x \in G$ is an automorphism of G called inner automorphism. The group I(G) of all inner automorphisms of G is normal in A(G) and isomorphic to G/Z.

An automorphism θ of G for which $x^{-1}\theta(x) \in Z$ for every $x \in G$ is called central. The set of all central automorphisms of G forms a group $A_c(G)$ which is the centralizer of I(G) in A(G), since $c^{-1}\theta(x)c = \theta(c^{-1})\theta(x)\theta(c)$ if and only if $c^{-1}\theta(c) \in Z$. As $I(G) \lhd G$, $A_c(G) \lhd G$. Also $A_c(G)$ contains I(G) if and only if I(G) is abelian, that is, if and only if G has class $c \leq 2$. If G is non-abelian $I(G) \cap A_c(G) = Z(I(G)) \cong Z(G/Z) \neq 1$. Therefore $A_c(G)$ is non-trivial.

Let $\theta \in A_c(G)$. Since $x^{-1}\theta(x) \in Z$, $\theta(x) = xf(x)$, $f \in \mathrm{Hom}\ (G,Z)$. Consider the mapping $\theta \to f_\theta$. This is a one-to-one mapping of $A_c(G)$ into Hom (G,Z). Furthermore, given $f \in \mathrm{Hom}\ (G,Z)$, $\theta(x) = xf(x)$ is an endomorphism of G which is an automorphism if and only if $f(x) \neq x^{-1}$ for every $x \in G$, $x \neq 1$. Thus $A_c(G)$ is isomorphic to a subgroup of Hom (G,Z). J.E. Adney and T_I. Yen have shown in [1] that if G is a PN-group then for $f \in \mathrm{Hom}\ (G,Z)$ the mapping $\theta(x) = xf(x)$ is always an automorphism of G. So $A_c(G)$ is isomorphic to the whole group of Hom (G,Z). Finally observe that for $f \in \text{Hom}(G,Z)$, $\ker f \geq G' = L_1$ so that $\text{Hom}(G,Z) = \text{Hom}(G/L_1,Z)$.

Throughout this chapter we shall take the invariants of G/L_1 to be $m_1 \geq m_2 \geq \ldots \geq m_t \geq 1$ and $|G/L_1| = p^m$. Similarly we take the invariants of Z to be $k_1 \geq k_2 \geq \ldots \geq k_s \geq 1$ and $|Z| = p^k$. Also a_z, b_z denote the numbers of times z appears among the invariants of G/L_1 and Z respectively.

2.1. General Results

Theorem 2.1. If G is a PN-group, then $|A_c(G)| = p^a$,

$$\text{where} \quad a = \sum_{j,i}^{t,s} \min(m_j,k_i) = m.s - \sum_y b_y \sum_{x>y} a_x(x-y).$$

Proof: Since G is a PN-group $A_c(G) = \text{Hom}(G,Z)$ [1], and so $A_c(G) = \text{Hom}(G/L_1,Z)$. But

$$G/L_1 = \prod_{j=1}^{t} C(p^{m_j}),\ Z = \prod_{i=1}^{s} C(p^{k_i}),\ \text{with} \sum_{x=1}^{m_1} xa_x = m$$

and $\sum_{y=1}^{k_1} y\, b_y = k$. Hence $|A_c(G)| = |\text{Hom}(G/L_1,Z)| =$

$$\left|\text{Hom}\left(\prod_{j=1}^{t} C(p^{m_j}),\ \prod_{i=1}^{s} C(p^{k_i})\right)\right| = \prod_{j,i}^{t,s} |\text{Hom}(C(p^{m_j}),C(p^{k_i}))| = p^a$$

$$\text{where } a = \sum_{j,i}^{t,s} \min(m_j,k_i) \quad (1).$$

Summing powers for $m_j = 1, 2, \ldots$ we get:

$$a = sa_1 + \big(2a_2(s-b_1) + a_2b_1\big) + \big(3a_3(s-b_1-b_2) + a_3(b_1+2b_2)\big) + \ldots =$$

$$s(a_1 + 2a_2 + \ldots) + (b_1 \sum_{x>1} a_x + 2b_2 \sum_{x>2} a_x + \ldots) - b_1(2a_2+3a_3+\ldots)$$

$$b_2(3a_3 + 4a_4 + \ldots) - \ldots = sm + \sum_y y\, b_y \sum_{x>y} a_x - \sum_y b_y \sum_{x>y} xa_x$$

$$= sm - \sum_{y=1}^{k_1} b_y \sum_{x>y}^{m_1} a_x (x - y) \qquad (2).$$

Corollary 2.1.1. $km \geq a \geq 2s$ and $a \geq \min(m,k)$. In fact from (1) we get $a \geq \min(m,k)$ and $a \geq 2s$. Similarly (2) gives $km \geq sm \geq a$, as $k \geq s$. Equality holds if and only if both G/L_1 and Z are elementary abelian.

Theorem 2.2. Let G be as in Theorem 2.1.

(i) If $k \geq m_1$, then $a \geq m + r$, where

$$r = \sum_{i=2}^{s} \left(\sum_{x=1}^{k_i} xa_x + k_i \sum_{x>k_i}^{k_1} a_x \right).$$

(ii) If $m_j \geq k_1$ for some j, $t \geq j \geq 1$, then $a \geq jk + (t-j)s$.

(iii) If $k \geq m_1 \geq k_1 > m_t$, then $a \geq k + m + s - m_1 - 1$.

(iv) If $k_i \geq m_1$ for some i, $s \geq i \geq 1$, then $a \geq im + (s-i)t$. In particular if $k_i \geq m_1 > k_{i+1}$, then $a \geq im + k - (k_1+\ldots+k_i)+(t-1)(s-i)$.

Proof: (i) Summing powers over $m_j = 1, 2, \ldots m_1$ in (1) for $k_i = k_s, \ldots, k_1$ we get:

$$a = \left(\sum_{x=1}^{k_s} xa_x + k_s \sum_{x>k_s}^{m_1} a_x \right) + \ldots + \left(\sum_{x=1}^{k_1} xa_x + k_1 \sum_{x>k_1}^{m_1} a_x \right).$$

Thus, $a = \sum_{i=2}^{s} (\sum_{x=1}^{k_i} xa_x + k_i \sum_{x>k_i}^{k_1} a_x) + \sum_{i=1}^{s} k_i (\sum_{x>k_1}^{m_1} a_x) + \sum_{x=1}^{k_1} xa_x$ (3).

But $k \geq m_1$ and so $\sum_{i=1}^{s} k_i (\sum_{x>k_1}^{m_1} a_x) = k \sum_{x>k_1}^{m_1} a_x \geq \sum_{x>k_1}^{m_1} xa_x$.

Hence $\sum_{i=1}^{s} k_i (\sum_{x>k_1}^{m_1} a_x) + \sum_{x=1}^{k_1} xa_x \geq \sum_{x=1}^{m_1} xa_x = m$. Putting

$r = \sum_{i=2}^{s} (\sum_{x=1}^{k_i} xa_x + k_i \sum_{x>k_i}^{k_1} a_x)$ in (3) we get, $a \geq m + r$.

(ii) Since $m_j \geq k_1$, we have $m_j \geq k_i$ for all i. Then from (1) we get $a \geq jk + \sum_{w=j+1,i=1}^{t,s} \min (m_w,k_i) \geq jk + (t-j)s$.

(iii) Let $\Phi_i = \sum_{x=1}^{k_i} xa_x + k_i \sum_{x>k_i}^{k_1} a_x$ for $i = 2, \ldots, s$.

If $\sum_{x=1}^{k_i} xa_x = 0$, then $m_t > k_i$ so that $k_1 > m_t > k_i$ and $\sum_{x>k_i}^{k_1} a_x \geq 1$. Thus $\Phi_i \geq 1$. On the other hand if $\sum_{x>k_i}^{k_1} a_x = 0$, then $k_i \geq m_t$ so that $\sum_{x=1}^{k_i} xa_x \geq 1$. Again $\Phi_i \geq 1$. For $k = m_1 + b$ ($b \geq 0$), (3) gives

$a \geq \sum_{i=2}^{s} \Phi_i + \sum_{x=1}^{k_1} xa_x + k \sum_{x>k_1}^{m_1} a_x \geq s - 1 + \sum_{x=1}^{k_1} xa_x +$

$m_1 \sum_{x>k_1}^{m_1} a_x + b \sum_{x>k_1}^{m_1} a_x$. Since $m_1 > k_1$, $\sum_{x>k_1}^{m_1} a_x \geq 1$. Also

$\sum_{x=1}^{k_1} xa_x + m_1 \sum_{x>k_1}^{m_1} a_x \geq \sum_{x=1}^{m_1} xa_x = m$. Therefore $a \geq s - 1 + m + b =$

$m + k + s - m_1 - 1$.

(iv) Since $k_i \geq m_1$, $k_i \geq m_j$ for all j and so from (1) we

have $a \geq im + \sum_{j=1,\ell=i+1}^{t,s} \min(m_j,k_\ell) \geq im + (s-i)t$.

Similarly for $k_i \geq m_1 > k_{i+1}$, from (1) we have

$a \geq im + \sum_{\ell=i+1}^{s} k_\ell + \sum_{j=2,\ell=i+1}^{t,s} \min(m_j,k_\ell) \geq im + k - (k_1+\ldots+k_i)+$

$(t-1)(s-i)$. This completes the proof.

We now proceed to determine the order of $A_c(G)$ in the general case in which $G = H \times K$, H abelian, K a PN-group.

<u>Theorem 2.3</u>. Let $G = H \times K$, where H is abelian and K is a PN-group. Then $A_c(G) = ABCD$ and $|A_c(G)| = |A|.|B|.|C|.|D|$, where

$A = \{\hat{\theta} \mid \hat{\theta}(h,k) = (h,\theta(k)),\ h \in H,\ k \in K,\ \theta \in A_c(K)\}$

$B = \{\hat{\psi} \mid \hat{\psi}(h,k) = (h\psi(k),k),\ h \in H,\ k \in K,\ \psi \in \mathrm{Hom}(K,H)\}$

$C = \{\hat{\phi} \mid \hat{\phi}(h,k) = (\phi(h),k),\ h \in H,\ k \in K,\ \phi \in A(H)\}$

$D = \{\hat{x} \mid \hat{x}(h,k) = (h,kx(h)),\ h \in H,\ k \in K,\ x \in \mathrm{Hom}(H,Z(K))\}$.

<u>Proof</u>: Obviously A, B, C, D are groups. Also A,C are subgroups of $A_c(G)$. For $h_1, h_2 \in H$, $k_1, k_2 \in K$ we have $\hat{\psi}((h_1,k_1)(h_2,k_2)) = \hat{\psi}(h_1h_2,k_1k_2) = (h_1h_2\psi(k_1k_2),k_1k_2) = (h_1\psi(k_1),k_1)(h_2\psi(k_2),k_2) = \hat{\psi}(h_1,k_1)\cdot\hat{\psi}(h_2,k_2)$. Also $\hat{\psi}(h,k) = 1$

gives $h\,\psi\,(k) = 1$ and $k = 1$, that is $h = k = 1$. Since $\psi(k) \in H \leq Z$, $\hat{\psi} \in A_c(G)$ and so $B \leq A_c(G)$. Similarly $D \leq A_c(G)$. Therefore $A_c(G) \supseteq ABCD$. Let $\hat{a} \in A_c(G)$. Then $\hat{a}\,(h,k) = (h,k).\ f(h,k)$ for some $f \in \text{Hom}\,(G,Z)$. So $\hat{a}(1,k) = (1,k)(\alpha_1(k),\alpha_2(k)) = (\alpha_1(k),k\alpha_2(k))$, where $\alpha_1 \in \text{Hom}\,(K,H)$ and $\alpha_2 \in \text{Hom}\,(K,Z(K))$. Let $\beta(k) = k\alpha_2(k)$. Since K is a PN-group, $\beta \in A_c(K)$. Therefore if $\hat{\theta}(h,k) = (h,\beta^{-1}(k))$, $\hat{\theta}\hat{a}(1,k) = (\alpha_1(k),k)$. Taking $\hat{\psi}(h,k) = (h\psi(k),k)$, where $\psi(k) = (\alpha_1(k))^{-1}$, $\psi \in \text{Hom}\,(K,H)$, we get $\hat{\gamma}(1,k) = \hat{\psi}\hat{\theta}\hat{a}\,(1,k) = (1,k)$. Let $\hat{\gamma}(h,1) = (g_1(h),g_2(h))$, $g_1 \in \text{Hom}\,(H,H)$, $g_2 \in \text{Hom}\,(H,Z(K))$. Then $\hat{\gamma}(h,k) = (g_1(h),kg_2(h))$. Here $g_1(h)$ is an automorphism of H, since if $g_1(h) = 1$, $h \neq 1$, $\hat{\gamma}\big(h,(g_2(h))^{-1}\big) = (1,1)$. Taking $\hat{\phi}(h,k) = (g_1^{-1}(h),k)$, we finally get $\hat{\phi}\hat{\gamma}(h,k) = (h,kg_2(h)) = \hat{x}(h,k)$ for some $\hat{x} \in D$. Hence $\hat{x} = \hat{\phi}\hat{\gamma} = \hat{\phi}\hat{\psi}\hat{\theta}\hat{a}$, which gives $\hat{a} = \hat{\theta}^{-1}\hat{\psi}^{-1}\hat{\phi}^{-1}\hat{x} \in ABCD$. Therefore $A_c(G) \subseteq ABCD$ and so $A_c(G) = ABCD$.

Since $\hat{\psi}\hat{\theta}(h,k) = \hat{\psi}(h,\theta(k)) = (h\psi(\theta(k)),\theta(k)) = \hat{\theta}\hat{\psi}_1(h,k)$, where $\hat{\psi}_1(h,k) = (h\psi(\theta(k)),k)$, $BA \leq AB$. So $M = AB$ is a group. Similarly $\hat{x}\hat{\phi}(h,k) = \hat{\phi}\hat{x}_1(h,k)$ for a suitable $\hat{x}_1 \in D$. Hence $N = CD$ is also a group. Clearly $A \cap B = C \cap D = 1$. Moreover $M \cap N = 1$. For, let $\hat{\theta}\hat{\psi}(h,k) = (h\psi(k),\theta(k)) = \hat{\phi}\hat{x}(h,k) = (\phi(h),k^{x}(h))$. Setting $k=1$, $\phi(h)=h$ and $x(h)=1$; setting $h = 1$, $\theta(k) = k$ and $\psi(k) = 1$. Therefore $|A_c(G)| = |MN| = |M||N| = |AB|.|CD| = |A||B||C||D|$. This proves the theorem.

Observe that B, C, D, BC, CD are all groups of outer automorphisms. Also, although BCD is not a group in general, all its elements are outer central automorphisms. In particular,

Corollary 2.3.1. $|A_c(G)/A_c(G) \cap I(G)| \geq |B|.|C|.|D|$.

Theorem 2.4. Let G, B, C, D be as in Theorem 2.3 and $\bar{A} = \{\bar{\theta} | \bar{\theta}(h,k) = (h,\theta(k)),\ h \in H,\ k \in K,\ \theta \in A(K)\}$. Then $A(G) \geq \bar{A}BCD$ and $|A(G)| \geq |\bar{A}|.|B|\ |C|\ |D|$.

Proof: Clearly $\bar{A} \leq A(G)$. As $A_c(G) \lhd A(G)$ we have $\bar{A}\ A_c(G) = \bar{A}ABCD = \bar{A}BCD \leq A(G)$ and $|A(G)| \geq |\bar{A}A_c(G)| = |\bar{A}|.|A_c(G)|/|\bar{A} \cap A_c(G)| = |\bar{A}|.|A_c(G)|/|A| = |\bar{A}|\,|B|\,|C|\,|D|$.

Since $I(G) \cong G/Z \cong K/Z(K) \cong I(K)$ and $|A(K)/I(K)| \geq p$ by Theorem 1.6, we have

Corollary 2.4.1. $|A(G)/I(G)| \geq p|B|\,|C|\,|D|$.

Corollary 2.4.2. Let $G = H \times K$, where H is abelian of order p^r and K is a PN-group. Then

(i) $|A_c(G)|_p \geq |A_c(K)|.p^{r+s+t-3} \geq |A_c(K)|.p^{r+s} \geq |A_c(K)|.p^{r+2}$,

and $|A(G)|_p \geq |A(K)|_p.p^{r+s+t-3} \geq |A(K)|_p.p^{r+s} \geq |A(K)|_p.p^{r+2}$,

(ii) For $r \geq \frac{1}{2}k - 1$, $|A(G)|_p \geq |G|$, where $|Z| = p^k$,

(iii) For $\exp H \geq \exp Z(K)$, $|A(G)|_p \geq |G|.|\mathrm{Hom}\ (K,H)|$.

Proof: (i) Let τ, σ, ρ be the numbers of invariants of K/K', $Z(K)$, H respectively. Since $G/G' = H \times K/K'$ and $Z = H \times Z(K)$ we get $t = \rho + \tau$ and $s = \rho + \sigma$. But $\tau \geq 2$, so that $t(\rho-1) \geq \rho^2-1$ and therefore $\rho(t-\rho) \geq t - 1$.

Similarly $\sigma \geq 1$ gives us $\rho(s-\rho) \geq s - 1$. Then $|B| = |\text{Hom }(K,H)| = |\text{Hom }(K/K',H)| \geq p^{(t-\rho)\rho} \geq p^{t-1}$, $|C| = |A(H)| \geq p^{r-1}$ and $|D| = |\text{Hom}(H,Z(K))| \geq p^{\rho(s-\rho)} \geq p^{s-1}$. Applying Theorems 2.3 and 2.4 we get that all inequalities hold, as $t \geq 3$, $s \geq 2$.

(ii) Let $|G| = p^n$, $|A(G)|_p = p^b$. By Theorem 1.6, $|A(K)|_p \geq p^{n-k+1}$ as $|K/Z(K)| = p^{n-k}$. Theorem 2.4 gives $b \geq r - 1 + n - k + 1 + \ell + w$, where $|\text{Hom }(K,H)| = p^{\ell}$ and $|\text{Hom }(H,Z(K)| = p^w$. But $\ell \geq 2$, and since $Z = H \times Z(K)$, $w \geq \min\ (r,\ k-r)$. Hence $b \geq n$. Here $\min\ (r,k-r) \geq k - r - 2$, as $2r \geq k - 2$.

(iii) From $w \geq k - r$ we get $b \geq r - 1 + n - k + 1 + \ell + k - r = n + \ell$. Observe that for groups with homocyclic center $\exp H = \exp Z(K)$.

<u>Theorem 2.5.</u> Let $\exp G/L_1 \leq |Z|$. Then $|A_c(G)|_p \geq p^m = |G/L_1|$.

<u>Proof</u>: If G is a PN-group, the result follows from Theorem 2.2(i). Therefore assume that $G = H \times K$, H abelian of order p^r, K a PN-group. Then $G/L_1 = H \times K/K'$ and $Z = H \times Z(K)$. Hence $|K/K'| = p^{m-r}$ and $|Z(K)| = p^{k-r}$. By Theorem 2.3, $a \geq r - 1 + v + \ell + w$, where $|A_c(G)|_p = p^a$, $|A_c(K)| = p^v$, $|\text{Hom}(K,H)| = p^{\ell}$ and $|\text{Hom }(H,Z(K))| = p^w$. Let $a_1 \geq a_2 \geq \ldots \geq a_\tau \geq 1$ be the invariants of K/K', $\exp Z(K) = p^u$ and $\exp H = p^b$. Here $p^v = |A_c(K)| = |\text{Hom }(K/K',Z(K)|$. By Theorem 2.2 (ii), we get for $u \geq a_1$, $v \geq \Sigma a_i$, and for $a_i > u$ with $a_{i+1} \nmid u$, $v \geq (k-r)i + (a_{i+1}+\ldots+a_\tau)$.

Also $p^{\ell} = |\mathrm{Hom}\ (K,H)| = |\mathrm{Hom}\ (K/K',H)|$. Therefore, as above, for $b \geq a_1$, $\ell \geq \Sigma a_i$ and for $a_j > b$, $a_{j+1} \nmid b$ we get $\ell \geq jr + (a_{j+1} + \ldots + a_\tau)$. But $k \geq a_1$, so $v + \ell \geq \Sigma a_i = m - r$ in all cases. Since $w \geq 1$ we get $a \geq r + m - r = m$.

We proceed to investigate the group of automorphisms $A(G)$ of G. By using the class c of G we now prove the following basic, but extremely useful, result which shall be used frequently in the following Chapters.

Theorem 2.6. Let G have class c. Then $|A_c(G)|.p^{c-1}$ is a factor of $|A(G)|$.

Proof: If G is abelian the result if trivial. Let G be non-abelian. Then G/Z_{c-1} is non-cyclic and $|Z_{i+1}/Z_i| \geq p$ for all $i = 0, 1, \ldots, c-2$. Hence $|G/Z_2| \geq p^{c-1}$ and so $|A(G)| \geq |A_c(G).I(G)| = |A_c(G)||G/Z_2| \geq |A_c(G)|.p^{c-1}$.

Theorem 2.7. Let G have class c and s be the number of invariants of Z. Then $|A(G)|_p \geq p^{2s+c-1}$.

Proof: For PN-groups, by Corollary 2.1.1, $|A_c(G)| \geq p^{2s}$. Using Theorem 2.6 we then get $|A(G)|_p \geq p^{2s+c-1}$. Let $G = H \times K$, H abelian and K a PN-group, and let ρ, σ be the numbers of invariants of H and $Z(K)$ respectively. Then $|\mathrm{Hom}\ (H,Z(K))| \geq p^{\rho}$ and $|A_c(K)| \geq p^{2\sigma}$, as K is a PN-group. By Theorem 2.3, $|A_c(G)|_p \geq p^{r-1}.p^{2\sigma}.p^{\rho}.p^2 > p^{2s}$

since $s = \rho + \sigma$. By Theorem 2.6, $|A(G)|_p \geq p^{2s+c-1}$.

Corollary 2.7.1. Let G have maximal class. Then $|G|$ divides $|A(G)|$.

If $|G| \leq p^4$, then $c = 1, 2, 3$. For $c = 2$ by Theorem 1.2, $|G|$ divides $|A(G)|$. For $c = 3$, G has maximal class so that again $|G|$ divides $|A(G)|$. Thus,

Corollary 2.7.2. Let G be non-abelian of order p^n, $n \leq 4$. Then $|G|$ divides $|A(G)|$.

For $s > 1$, $2s + c - 1 \geq c + 3$. Hence

Corollary 2.7.3. Let G have non-cyclic center, order p^n and class $c \geq n - 3$. Then $|G|$ divides $|A(G)|$.

2.2. Outer Central Automorphisms

Let $G = H \times K$, where H is abelian and K is a PN-group. By Corollary 2.3.1 there exist at least $|B||C||D|$ outer automorphisms in $A_c(G)$. Observe that $|B||C||D| \geq |H|.p^s$, where s is the number of invariants of Z. Also a careful examination of the groups B, C, D, BC, CD of Theorem 2.3 gives us the following information.

(i) If H has order greater than p^2, then $A_c(G)$ has a p-subgroup of outer automorphisms of order at least p^{s+1}.

(ii) If H has order p^2, then either $|G|$ divides $|A(G)|$ or $A_c(G)$ has a p-subgroup of outer automorphisms of order at least p^{s+1}.

(iii) If H has order p, then $A_c(G)$ has a p-subgroup of outer automorphisms of order at least p^{s-1}.

Let G be a PN-group. Then $E(Z) \leq \Phi(G)$, so that $E(Z)$ is contained in every maximal subgroup of G. Below we shall show that if $Z \nleq \Phi(G)$ then $A_c(G)$ has a p-subgroup of outer automorphisms of order p^s. First we prove the following.

Theorem 2.8. Let G be a PN-group and M a maximal subgroup of G. If $a \in G \backslash M$, then the mapping Φ defined by $\Phi_z(a^n m) = (az)^n m$, $0 \leq n < p$, $m \in M$, $z \in E(Z)$ is a central automorphism of G.

Proof: Every element g of G has the form $g = a^n m$, $0 \leq n < p$, $m \in M$. Since $M \lhd G$, $a^n m = m_1 a^n$ for some $m_1 \in M$. Therefore $\Phi_z(a^{n_1} m_1 a^{n_2} m_2) = \Phi_z(a^{n_1} m_1)\Phi_z(a^{n_2} m_2)$ and $(az)^n m = 1$ if and only if $a^n m = 1$. Hence Φ_z is an automorphism of G. Obviously $\Phi_z \in A_c(G)$.

Corollary 2.8.1. Let G be a PN-group. If $Z \nleq \Phi(G)$, then $A_c(G)$ has a subgroup of outer automorphisms which is isomorphic to $E(Z)$.

Proof: Let M be a maximal subgroup of G for which $Z \nleq M$. Since G is a PN-group, $E(Z) \leq M$. Take $a \in Z \backslash M$ and consider the group:

$$L = \{\Phi_z \mid \Phi_z(a^n m) = (az)^n m,\ 0 \leq n < p,\ m \in M,\ z \in E(Z)\}.$$

Obviously $L \cong E(Z)$. If Φ_z were inner, $x^{-1} a^n m x = (az)^n m$ for every $m \in M$ and all n. Taking $m = 1$ we get $z^n = 1$ so that Φ_z is the identity automorphism.

Corollary 2.8.2. Let G be a PN-group. If $E(Z) \nleq G'$, then G has an outer central automorphism of order p.

Proof: $E(Z) \leq M$ for any maximal subgroup M of G. Take $z \in E(Z) \backslash G'$ and consider Φ_z. Here Φ_z is outer since otherwise $x^{-1}a^n m x = (az)^n m$ for every $m \in M$ and all n. Taking $m = 1$, $n = 1$, we get $z = a^{-1}x^{-1}ax \in G'$ which is not so.

CHAPTER THREE

LA-GROUPS

A finite p-group G is called an LA-group if $|G|$ divides $|A(G)|$. All non-cyclic abelian p-groups of order greater than p^2 are LA-groups. Also certain classes of non-abelian p-groups are LA-groups [12], [13], [14], [15], [16], [42]. However cyclic p-groups and groups of order p^2 are not LA-groups. In this chapter we consider some other classes of LA-groups and show that all non-abelian groups of order p^n, $n \leq 5$ or $n \leq 6$ for $p \neq 2$, are LA-groups. Throughout this chapter G will stand for a finite non-abelian p-group.

A.D. Otto in [40] (Theorem 2) has shown that if $|L_i/L_{i+1}| = p$ for $i = 1, \ldots, c-1$ and $\exp G/L_1 = p$, then G is an LA-group. The following is a generalization of this result:

Theorem 3.1. Let L_i/L_{i+1} be cyclic of order p^r, $i = 1, \ldots, c-1$ and $\exp G/L_1 \leq |Z|$. Then G is an LA-group.

Proof: Let $|G/L_1| = p^m$. Since $|L_i/L_{i+1}| = p^r$ for $i = 1, \ldots, c-1$, $|L_1| = p^{(c-1)r}$ so that $n = m + (c-1)r$, where $|G| = p^n$. As $L_i \leq Z_{c-i}$ with $L_i \nleq Z_{c-i-1}$, $Z_{c-i}/L_i \geq L_iZ_{c-i-1}/L_i = Z_{c-i-1}/L_i \cap Z_{c-i-1}$. By Theorem 1.15, $L_i \cap Z_{c-i-1} = L_{i+1}$, and therefore $|Z_{c-i}/L_i| \geq |Z_{c-i-1}/L_{i+1}|$. This gives $|Z_{c-i}/Z_{c-i-1}| \geq |L_i/L_{i+1}| = p^r$ for all $i = 1, \ldots, c-1$.

But $|G/Z_{c-1}| = p^{2r}$ (Theorem 1.15). So $n \geq 2r + (c-3)r + a + k$ where $|Z_2/Z| = p^a$ and $|Z| = p^k$. Then $m + (c-1)r \geq 2r + (c-3)r + a + k$ which gives $m \geq a + k$. By Theorem 2.5, $|A_c(G)|_p \geq p^m$, as $\exp G/L_1 \leq |Z|$. So $|A(G)|_p \geq |A_c(G).I(G)|_p = |A_c(G)|_p.|I(G)|/|Z_2/Z| \geq p^{n+m-k-a} \geq p^n$.

<u>Corollary 3.1.1.</u> Let Z_i/Z_{i-1} be cyclic of order p^r, $i = 1, \ldots, c-1$ and $L_1 = Z_{c-i}$ for some i, $1 \leq i \leq c-1$. Then G is an LA-group.

<u>Proof</u>: By J.A. Gallian [17] (Theorem 3.5) G must have homocyclic lower central factors and $\exp G/L_1 = p^r$. Since $L_{c-1} \leq Z$, $\exp G/L_1 = p^r = |L_{c-1}| \leq |Z|$.

<u>Theorem 3.2</u>. Let G have cyclic center and $|L_{c-1}| = p^r$. Then G is an LA-group if it has a normal abelian subgroup M with G/M cyclic of order p^r.

<u>Proof</u>: By M.N. Vislavskij (Theorem 1.14) L_i/L_{i+1} is cyclic of order p^r, $i = 1, \ldots, c-1$, and G/ZL_1 has type (p^r,p^r). Then by Theorem 1.15, $|G/Z_{c-1}| = p^{2r}$. As $ZL_1 \leq Z_{c-1}$ and $|ZL_1| = |Z_{c-1}|$, $ZL_1 = Z_{c-1}$. Let $\exp Z_{c-1}/L_1 = p^a$. Then $p^r = \exp (G/L_1/Z_{c-1}/L_1) \geq \exp (G/L_1)/\exp (Z_{c-1}/L_1) = \exp (G/L_1)/p^a$. Hence $\exp (G/L_1) \leq p^{r+a}$. By [17] (Theorem 2.1) $Z_1 \cap L_1 = L_{c-1}$. So $p^a = \exp (Z_{c-1}/L_1) = \exp (ZL_1/L_1) = \exp (Z/L_1 \cap Z) \leq |Z/L_1 \cap Z| = |Z|.p^{-r}$. Hence $\exp (G/L_1) \leq p^{r+a} \leq |Z|$ and the result follows from the previous theorem.

Corollary 3.2.1. Let G have cyclic center. Then G is an LA-group if it has a maximal subgroup which is abelian.

Theorem 3.3. If the Frattini subgroup $\Phi(G)$ of G is cyclic, then G is an LA-group.

Proof: By Theorem 1.11 (Ja.G. Berkovic), $G = AB$, where either B is cyclic or B has maximal class. If B is cyclic $Z \geq \Phi(G)$ so that $Z \geq G'$. Then G has class two and is therefore an LA-group. Let B have maximal class. Again by Theorem 1.11, $G' = \Phi(G)$ and so G' is cyclic and $\exp G/G' = p$. By Theorem 1.10 (N. Blackburn) $\exp L_i/L_{i+1} = p$ for $i = 1, \ldots, c-1$, so that L_i/L_{i+1} is both cyclic and elementary abelian. Then $|L_i/L_{i+1}| = p$, and the result follows from Theorem 3.1.

Corollary 3.3.1. G is an LA-group under any one of the following conditions:

(i) G has a maximal subgroup M which is cyclic,

(ii) G has a normal cyclic subgroup H of index p^2 in G, $p \neq 2$,

(iii) The center $\overline{Z}$ of $\Phi(G)$ has no normal subgroups of G of type (p,p),

(iv) G has no non-cyclic abelian characteristic subgroups.

Proof: (i) Since $M \geq \Phi(G)$. For (ii) observe that G/H is either elementary abelian or cyclic. In the first case $H \geq \Phi(G)$, so $\Phi(G)$ is cyclic. In the second case G is metacyclic and the result follows from Theorem 1.4.

(iii) From $\bar{Z}$ char $\Phi(G)$ char G we get $\bar{Z}$ char G. As $\bar{Z}$ is abelian it cannot have maximal class. Then by Ja.G. Berkovic [4] (Theorem 2.3), since $\bar{Z}$ has no normal subgroups of G of type (p,p), $\bar{Z}$ is cyclic. So $\Phi(G)$ is cyclic (Ch. Hobby [25]). Finally, (iv) follows by observing that $\bar{Z}$ is an abelian characteristic subgroup of G.

Any p-group of maximal class is an LA-group (Corollary 2.7.1). Below (Theorems 3.4 - 3.6) we extend this result to p-groups which contain certain normal subgroups of maximal class. First we prove the following:

Lemma 3.1. Let K be a normal subgroup of G and $\Phi(G) \geq K$. Then K cannot be of maximal class.

Proof: Let K have maximal class. Then K contains a normal subgroup H of G of order p^2. By N. Blackburn [8] (Lemma 1) $C_G(H)$ has index at most p in G. So $C_G(H) \geq \Phi(G)$. Then $C_G(H) \geq \Phi(G) \geq K \geq H$ which gives $Z(K) \geq H$. This is a contradiction, since $|Z(K)| = p$.

Theorem 3.4. Let G have a normal subgroup M of maximal class. If G/M is elementary abelian, then G is an LA-group.

Proof: We may assume that G is not of maximal class. Let $|G| = p^n$, $|G/M| = p^a$ and $|G/L_1| = p^m$. Then if c' is the class of M, c' = n-a-1. Obviously G has class $c \geq c'$. Let $G = L_o > L_1 > \ldots > L_c = 1$, $M = \bar{L}_o > \bar{L}_1 > \ldots > \bar{L}_{c'} = 1$, be the lower central series of

G and M respectively. Here $L_i \geq \bar{L}_i$ for all i. Moreover, $|M/\bar{L}_1| = p^2$ and $|\bar{L}_i/\bar{L}_{i+1}| = p$, $i = 1, \ldots, c'-1$, as M is of maximal class. Also $M \geq \Phi(G)$ since G/M is elementary abelian. However $\Phi(G)$ cannot have maximal class by Lemma 3.1. So $M > \Phi(G) \geq G'$ and $m \geq a + 1$. On the other hand $|L_i/L_{i+1}| \geq p$ so that $|L_1| \geq p^{c-1} \geq p^{n-a-2}$, since $c \geq c' = n-a-1$. Hence $|G/L_1| \leq p^{a+2}$ and $m \leq a + 2$. Thus either $m = a + 1$ or $m = a + 2$. Consider

<u>$m = a + 1$.</u> Then $L_1 = \Phi(G)$, so that G/L_1 is elementary abelian. Since $\bar{L}_1$ char $M \lhd G$ we have $\bar{L}_1 \lhd G$. Moreover $|L_1/\bar{L}_1| = p$, as $|M/L_1| = p$, $|M/\bar{L}_1| = p^2$ and $L_1 \geq \bar{L}_1$. Thus $Z(G/\bar{L}_1) \geq L_1/\bar{L}_1$ which implies $\bar{L}_1 \geq [L_1,G] = L_2$. On the other hand by N. Blackburn [10] (Lemma 2.1) since M/L_1 is cyclic $[M,M] = [L_1,M]$. So $L_2 = [L_1,G] \geq [L_1,M] = \bar{L}_1$. Hence $L_2 = \bar{L}_1$. Assume by induction that $L_{i+1} = \bar{L}_i$. Then $\bar{L}_i = L_{i+1} > L_{i+2} = [L_{i+1},G] \geq [\bar{L}_i,M] = \bar{L}_{i+1}$. But $|\bar{L}_i/\bar{L}_{i+1}| = p$. So $L_{i+2} = \bar{L}_{i+1}$ and therefore $L_{i+1} = \bar{L}_i$ for all $i \geq 1$. This gives $L_{c'} = \bar{L}_{c'-1} \neq 1$ and $L_{c'+1} = \bar{L}_{c'} = 1$, so that G has class $c = c' + 1 = n - a$. Since G/L_1 is elementary abelian, $|A_c(G)|_p \geq p^m$ by Theorem 2.5. Now apply Theorem 2.6 to get $|A(G)|_p \geq p^m p^{c-1} = p^{m+c-1} = p^{a+1+n-a-1} = p^n$.

<u>$m = a + 2$.</u> Then $|L_i/L_{i+1}| = p$ for $i = 1, \ldots, c-1$ and $c = c' = n-a-1$. For $|Z| = p$, $|A(G)|_p \geq p|I(G)| = |G|$ (Theorem 1.6). Let $|Z| > p$. Since $p \geq |\Phi(G)/L_1|$ we have

$|Z| \geq p^2 \geq \exp G/L_1$. By Theorem 2.5, $|A_c(G)|_p \geq p^m = p^{a+2}$. Hence $|A(G)|_p \geq p^{a+2}.p^{c-1} = p^{a+2+n-a-2} = p^n$ and so G is an LA-group.

Corollary 3.4.1. Let G have a maximal subgroup which is of maximal class. Then G is an LA-group.

Corollary 3.4.2. Let M be a maximal subgroup of G. Then G is an LA-group under any one of the following conditions:

(i) All maximal subgroups of M have cyclic center,

(ii) $M \cap Z_2$ is cyclic.

Proof: (i) M has no normal subgroups H of G of type (p,p) since otherwise H would be in the center of some maximal subgroup of M (Property 8). By Ja.G. Berkovich[4] (Theorem 23) M is either cyclic or of maximal class. In the first case the result follows from Corollary 3.3.1(i) and in the second case from Corollary 3.4.1. For (ii) observe that again M has no normal subgroup of G of type (p,p).

Theorem 3.5. Let G have a normal subgroup M of maximal class having index p^2 in G. Then G is an LA-group.

Proof: We may assume that G/M is cyclic, otherwise the result follows from above. Then $M > L_1$ since G/L_1 cannot be cyclic. So $|G/L_1| = p^m \geq p^3$. Let $|G| = p^n$ and $L_i, \bar{L}_i$ be the lower central series of G and M as in the previous Theorem. Here $L_i \geq \bar{L}_i$ and $c' = n - 3$, where c' is the class of M. So G has class $c \geq n - 3$ and $|G/L_1| \leq p^4$. Hence $3 \leq m \leq 4$. If $|Z| = p$, $|A(G)|_p \geq p|I(G)| = |G|$ by Theorem 1.6. So, assume $|Z| > p$. Consider:

<u>$m = 3$</u>. Then $|M/L_1| = p$ so that proceeding as in Theorem 3.4 we get $\bar{L}_i = L_{i+1}$ for $i \geq 1$ and $c = n - 2$. Since G/L_1 is not cyclic $|Z| \geq p^2 \geq \exp G/L_1$. By Theorem 2.5, $|A_c(G)|_p \geq p^m = p^3$ and by Theorem 2.6, $|A(G)|_p \geq p^3.p^{c-1} = p^n$.

<u>$m = 4$.</u> Then $|L_i/L_{i+1}| = p$, $i = 1, \ldots, c-1$, and $c = n - 3$. Moreover, $p^4 = |G/L_1| = |G/M|.|M/\bar{L}_1| = |G/\bar{L}_1|$ so that $|L_1| = |\bar{L}_1|$. Since $L_1 \geq \bar{L}_1$, $L_1 = \bar{L}_1$. By Theorem 1.13 (Ch. Hobby and C.R.B. Wright), G has more than two generators. So G/L_1 has more than two invariants. Therefore $|Z| \geq p^2 \geq \exp G/L_1$ so that $|A_c(G)|_p \geq p^m = p^4$ and $|A(G)|_p \geq p^4.p^{c-1} = p^n$.

<u>Theorem 3.6.</u> Let M be a maximal subgroup of G. If M has a normal subgroup H of order p such that M/H has maximal class, then G is an LA-group.

<u>Proof</u>: Let $|G| = p^n$. Then $|M/H| = p^{n-2}$ and M/H has class $n - 3$. Let c' be the class of M. Then $c' \geq n - 3$. For $c' = n - 2$ the result follows from Corollary 3.4.1. Let $c' = n - 3$. Since H is a normal subgroup of M of order p, $Z(M) \geq H$. Let $Z(M)$ be cyclic. As M has order p^{n-1} and class $n - 3$, $p^3 \geq |M/M'| \geq p^2$ and

so M/M' has type (p,p), (p,p^2) or (p,p,p). In all cases $m_2 = 1$, so that by Theorem 1.10 (N. Blackburn) $\exp L_i(M)/L_{i+1}(M) = p$, $i = 1, 2, \ldots, c'-1$. Hence $\exp L_{c'-1}(M) = p$. Also $L_{c'-1}(M) \le Z(M)$ and $Z(M)$ is cyclic. So $L_{c'-1}(M)$ is cyclic of order p. As $Z(M)$ has only one subgroup of order p, $L_{c'-1}(M) = H$. Then $L_{c'-1}(M/H) = L_{c'-1}(M)H/H = 1$, a contradiction ($M/H$ has class $c' = n-3$). So assume that $Z(M)$ is not cyclic. Then it is elementary abelian of order p^2. By Theorem 2.7, $|A(M)|_p \ge p^{c'+3} = |M|$. If $Z \nleq M$, then $G = ZM$ so that $|A(G)|_p \ge |G|$ by Theorem 1.7. Therefore we may assume that $Z \le M$ and so $Z \le Z(M)$. For $|Z| = p$, by Theorem 1.6, $|A(G)|_p \ge p.|I(G)| = |G|$; for $|Z| > p$, $Z = Z(M)$ so that Z is elementary abelian of order p^2 and $|A(G)|_p \ge p^{2s+c-1} = p^{c+3} \ge p^n$, as $c \ge n - 3$.

Theorem 3.7. Let $p \ne 2$. If all normal subgroups of G of order p^3 have two generators, then G is an LA-group.

Proof: We may assume that G is not of maximal class and it is not metacyclic. Also $|G|=p^n$, $n\ge5$. By Theorem 1.9 (N. Blackburn) the elements of G of order at most p form a normal subgroup E of G of order p^3, and G/E is cyclic. So $E \ge L_1$ and since G/L_1 is not cyclic, $|L_1| \le p^2$. If $Z \ge L_1$, G has class two and there is nothing more to show. Therefore assume that $|L_1| = p^2$ and that G has class $c = 3$. Let $G = \langle a,E\rangle$. Then $a^{p^{n-3}} \in E$ while

$a^{p^{n-4}} \notin E$. So $a^{p^{n-3}} \neq 1$. Let $P(G)$ be the subgroup of G generated by all x^p, $x \in G$. By Theorem 1.9, $C_G(E) \geq P(G)$. So $a^p \in Z$. Therefore $|Z| \geq p^{n-3}$. Since $\exp G/L_1 < |G/L_1| = p^{n-2}$ we have $\exp G/L_1 \leq |Z|$. By Theorem 2.5, $|A_c(G)|_p \geq p^{n-2}$. Apply Theorem 2.6 to get $|A(G)|_p \geq p^{n-2}.p^{c-1} = p^n$.

<u>Corollary 3.7.1.</u> Let $p \neq 2$. If Z_3 is metacyclic then G is an LA-group.

<u>Theorem 3.8.</u> If G has order p^n, $n \leq 5$, then G is an LA-group.

<u>Proof</u>: By Theorem 1.2 and Corollary 2.7.2 we may assume that $c = 3$, $n = 5$. If $|Z| = p$, then $|A(G)|_p \geq p.|I(G)| = |G|$ (Theorem 1.6). Therefore take $|Z| > p$. For $|G/L_1| = p^2$, by Theorem 1.10, $|L_1/L_2| = p$ and $\exp L_2 = p$. Since $|L_2| = p^2$ and $Z \geq L_2$, Z is not cyclic. So, by Theorem 2.7, $|A(G)|_p \geq p^{c+3} = p^6$. Next take $|G/L_1| = p^3$. Then $\exp G/L_1 \leq p^2 \leq |Z|$, so that by Theorem 2.5, $|A_c(G)|_p \geq p^3$. Applying Theorem 2.6, $|A(G)|_p \geq p^3.p^{c-1} = p^5$.

<u>Theorem 3.9.</u> If $|G/Z| \leq p^3$, G is an LA-group.

<u>Proof</u>: For $|G/Z| \leq p^2$, G has class two and the result follows from Theorem 1.2. Therefore assume that $|G/Z| = p^3$ and that G has class $c = 3$. By Theorem 1.8, $|L_1| \leq p^3$ so that $p^3 \geq |L_1| \geq p^2$. Let $|L_1| = p^2$. Then

if $|G| = p^n$, exp $G/L_1 \leq p^{n-3} = |Z|$ and by Theorem 2.5, $|A_c(G)|_p \geq p^{n-2}$. Hence $|A(G)|_p \geq p^{n-2}.p^{c-1} = p^n$. So take $|L_1| = p^3$. Since G is non-abelian, G/Z is non-cyclic and exp $G/Z \leq p^2$. Let exp $G/Z = p^2$ and take $a \in G$ such that $a^{p^2} \in Z$, $a^p \notin Z$. Then $M = \langle Z,a\rangle$ is a maximal subgroup of G which is abelian. By Theorem 1.23(ii), $p^2 = |M/Z| = |L_1| = p^3$. This is impossible, so exp $G/Z = p$. Since the class of G is not two, $p \neq 2$. Also $Z \geq P(G)$ and by Theorem 1.16 (I.D. Macdonald), $1 = L_3 \geq L_p \geq P(L_1)$. Hence exp $L_1 = p$. But exp $G/L_1 \geq$ exp $L_1 Z/L_1$ = exp $Z/L_1 \cap Z \geq$ exp Z/exp $L_1 \cap Z$ = exp Z/p. So p.exp $G/L_1 \geq$ exp Z.

Since $|G/L_1| = p^{n-3}$, exp $G/L_1 \leq p^{n-4}$. For exp $G/L_1 = p^{n-4}$, G/L_1 has type (p,p^{n-4}) and by Theorem 1.10, $|L_1/L_2| = p$ and exp $L_2 = p$. Then L_2 is not cyclic and so, as $Z \geq L_2$, Z is not cyclic. Similarly, for exp $G/L_1 \leq p^{n-5}$, $|Z| = p^{n-3} > p^{n-4} \geq p$ exp $G/L_1 \geq$ exp Z and again Z is not cyclic. Therefore we may assume that $s > 1$, where s is the number of invariants of Z. Consider

(a) G is a PN-group. By Theorem 2.2, for $m_1 \geq k_1$, $|A_c(G)| \geq p^{k+s} \geq p^{n-1}$ and for $k_1 > m_1$, $|A_c(G)| \geq p^{m+t(s-1)} \geq p^{n-1}$. Applying Theorem 2.6 we get $|A(G)|_p \geq p^{n-1}.p^{c-1} = p^{n+1}$.

(b) $G = H \times K$, H abelian and K a PN-group. Then $|K/Z(K)| = |G/Z| = p^3$ so that by (a), $|A(K)|_p \geq |K|$. By Corollary 2.4.2.(i), $|A(G)|_p > |G|$.

Corollary 3.9.1. If G has a normal subgroup H of order p^2 and G/H is cyclic, then G is an LA-group.

In fact $G = \langle a,H \rangle$ for some $a \in G \backslash H$ and by N. Blackburn [8] (Lemma 1) $C_G(H)$ has index at most p in G. So $a^p \in C_G(H)$ and therefore $a^p \in Z$. Then $|Z| \geq |\langle a^p \rangle| \geq p^{n-3}$ and $|G/Z| \leq p^3$.

Theorem 3.10. G is an LA-group under any one of the following conditions.

(i) All subgroups of G of order p^2 have the same type,

(ii) $p \neq 2$ and all subgroups of G of order p^3 have the same type,

(iii) $p \neq 2$ and all normal subgroups of G of order p^r, r fixed $3 < r < n-1$ have two generators,

(iv) $p \neq 2$ and all non-cyclic subgroups of G of equal order have the same number of generators.

Proof: (i) If all subgroups of G of order p^2 are cyclic, then G has only one subgroup of order p and so G is the generalized quaternion group [49], which is a 2-group of maximal class. If all subgroups of G of order p^2 are elementary abelian, then $x^p = 1$ for every $x \in G$ and the result follows from Theorem 1.3.

(ii) We may assume that all subgroups of G of order p^3 have either two or three generators, since otherwise G is cyclic [49]. In the first case the result follows from Theorem 3.7 and in the second case from Theorem 1.3.

(iii) By Theorem 3.8 we may assume that $|G| = p^n$, $n \geq 6$. Then G is either metacyclic or a 3-group of maximal class

(N. Blackburn [11]). In the first case the result follows from Theorem 1.4 and in the second case from Corollary 2.7.1.

(iv) By Theorems 1.2, 1.3 and 3.8 we may assume that G has class $c > 2$, $\exp G > p$ and $|G| \geq p^6$. Also we may assume that G is not of maximal class. Then by Ja.G. Berkovic([6], Theorem 9) all proper subgroups of G are metacyclic and the result follows from Theorem 3.7.

<u>Theorem 3.11</u>. If G has order 2^n and class $n - 2$, then G is an LA-group.

<u>Proof</u>: Since G has class $n - 2$, $|G/L_1| \leq 8$. If $|G/L_1| = 4$ by Corollary 1.19.2, G has maximal class. So $|G/L_1| = 8$. For $|Z| = 2$, by Theorem 1.6, $|A(G)|_2 \geq 2.|I(G)| = 2^n$. For $|Z| > 2$, $\exp G/L_1 \leq 4 = |Z|$, and by Theorem 2.5 $|A_c(G)|_2 \geq 8$. Then by Theorem 2.6 $|A(G)|_2 \geq 8.2^{c-1} = 2^n$.

<u>Theorem 3.12</u>. Let G have order p^n and class 3. If $|G/L_1| = p^2$, then $4 \leq n \leq 5$, $\exp Z = p$ and $|A(G)|_p \geq p^{2n-4} \geq p^n$.

<u>Proof</u>: Since $|G/L_1| = p^2$, G is a PN-group. By Theorem 1.10, $|L_1/L_2| = p$ and $\exp L_2 = p$. Hence $|G/L_2| = |G/L_1||L_1/L_2| = p^3$. But $L_2 \leq Z$ and so $|G/Z| \leq p^3$. As G has class 3, $|G/Z| \nleq p^2$. Therefore $|G/Z| = p^3$ and $Z = L_2$. So $\exp Z = \exp L_2 = p$. By Theorem 1.8, $|L_1| \leq p^3$

which gives $|G| = p^2|L_1| \le p^5$. On the other hand $|G| \ge p^4$ as G has class 3. Hence $4 \le n \le 5$. Since Z is elementary abelian, by Theorem 2.2, $|A_c(G)| = p^{2k}$ where $|Z| = p^k$. Then, by Theorem 2.6, $|A(G)|_p \ge p^{2k}.p^{c-1} = p^{2(n-3)+2} = p^{2n-4} \ge p^n$.

Theorem 3.13. Let G be a two generator group of order p^n, class 3 and $|G/L_1| = p^m$ with $m \le \frac{1}{2}n$. Then G is an LA-group if either $\exp G/L_1 = p^{m-1}$ or $\exp G/Z = p$.

Proof: If $\exp G/L_1 = p^{m-1}$, G/L_1 has type (p,p^{m-1}), so that by Theorem 1.10, $|L_1/L_2| = p$ and $\exp L_2 = p$. If $\exp G/Z = p$, by Theorem 1.21(i) $\exp L_1/L_2 = \exp L_2 = p$. Since G has two generators G/L_1 has two invariants and so L_1/L_2 is cyclic. Hence again $|L_1/L_2| = p$. Therefore in both cases $|L_1/L_2| = p$ and $\exp L_2 = p$. Then $|L_2| = p^{n-m-1}$ and since $L_2 \le Z$, $s \ge n - m - 1$ where s is the number of invariants of Z. By Theorem 2.7, $|A(G)|_p \ge p^{2s+c-1} \ge p^{2n-2m} \ge p^n$.

We now proceed to show that if all two-maximal subgroups of G are abelian then G is an LA-group. It is reminded here that a two-maximal subgroup of G is a maximal subgroup of a maximal subgroup of G. We shall require the following result by I.D. Macdonald:

Lemma 3.2. ([38], p. 562). If every maximal subgroup of G has class 2, then G has class at most 3. In particular, if G cannot be generated by two elements then G has class 3 for p = 3 and class 2 otherwise.

Theorem 3.14. Let all two-maximal subgroups of G be abelian and $|G| = p^n$. Then,
(i) If p = 2, either G has maximal class or G has class 2.
(ii) If $p \neq 2$, G has class at most 3. Moreover, if G has two generators and $n \geq 6$ then G is metacyclic. If G has more than two generators then G has class 2 and $4 \leq n \leq 5$.

Proof: Let M be a maximal subgroup of G. Since all maximal subgroups of M are abelian, M has class 2 and two generators (Theorem 1.24). By Lemma 3.2, G has class at most 3. Consider the following cases:

(i) p = 2. If G cannot be generated by 2 elements, by Lemma 3.2, G has class 2. So we may assume that G can be generated by 2 elements. Then G/L_1 has two invariants $m_1 \geq m_2$ and G can be generated by a, b such that $a^{2^{m_1}} \in L_1$, $a^{2^{m_1-1}} \notin L_1$, $b^{2^{m_2}} \in L_1$, $b^{2^{m_2-1}} \notin L_1$. Since G and all its maximal subgroups have two generators, G is metacyclic ([7], Corollary 2). So every subgroup of G is metacyclic. If $m_1 > 1$, $H = \langle a^{2^{m_1-1}}, b^{2^{m_2-1}}, c = [a,b]\rangle$ is an abelian 2-group with more than three elements of order 2. Therefore H is not metacyclic. Hence $m_1 = 1$

and $|G/L_1| = 4$. Then by Corollary 1.19.2, G has maximal class.

(ii) <u>$p \neq 2$</u>. Since all maximal subgroups of G can be generated by 2 elements, G can be generated by 3 elements. If G has 3 generators then by N. Blackburn ([11], Theorem 3.1) G has class 2 (G is non-abelian) and $4 \leq n \leq 5$. If G has 2 generators and $n \geq 6$ then again by N. Blackburn ([11], Theorem 4.2) either G is metacyclic or $|G/L_1| = p^2$. Let $|G/L_1| = p^2$. If G has class 3, then $n = 4, 5$ by Theorem 3.12. If G has class 2, then $L_1 = Z = \Phi(G)$, as G is non-abelian so that all maximal subgroups of G are abelian. Then by Theorem 1.24 $|L_1| = p$ and $n = 3$. Hence for $n \geq 6$, G is metacyclic.

<u>Theorem 3.15</u>. If all two-maximal subgroups of G are abelian, then G is an LA-group.

<u>Proof</u>: Let $|G| = p^n$. For $n \leq 5$, G is an LA-group by Theorem 3.8. For $n \geq 6$, by Theorem 3.14, either a) G has class 2, b) G has maximal class or c) $p \neq 2$ and G is metacyclic. In all three cases by Theorem 1.2, Corollary 2.7.1 and Theorem 1.4 respectively G is an LA-group.

<u>Corollary 3.15.1</u>. Let $p \neq 2$. If all proper non-abelian subgroups of G are metacyclic, then G is an LA-group.

<u>Proof</u>: G is either metacyclic or all two-maximal subgroups of G are abelian ([34], Corollary 1).

Finally we extend Theorem 3.8 to groups of order p^6. However, we have to exclude the case $p = 2$.

Theorem 3.16. Let $p \neq 2$. If G has order p^6, then G is an LA-group.

Proof: We may assume that G has class c with $5 > c > 2$ and by Theorems 2.4 and 3.8 that G is a PN-group. For $|Z| = p$, by Theorem 1.6, $|A(G)|_p \geq p|I(G)| = |G|$. For $|Z| \geq p^3$, $|G/Z| \leq p^3$ and by Theorem 3.9, G is an LA-group. Thus we take $|Z| = p^2$. Finally, let $\Phi(G) \ngeq Z$ so that $G = ZM$ for some maximal subgroup M of G. Then $|A(M)|_p \geq |M| = p^5$ by Theorem 3.8, so that by Theorem 1.7 (K.G. Hummel) G is an LA-group. Therefore we may take $\Phi(G) \geq Z$. Consider the following cases:

c = 4. Then $p^3 \geq |G/L_1| \geq p^2$. Let $|G/L_1| = p^3$. Then $\exp G/L_1 \leq p^2 = |Z|$ and by Theorem 2.5, $|A_c(G)| \geq p^3$. Therefore by Theorem 2.6, $|A(G)|_p \geq p^3.p^{c-1} = p^6$. Next take $|G/L_1| = p^2$. As $L_1 \leq Z_3$ and G/Z_3 is not cyclic we have $|G/Z_3| = p^2$ so that $L_1 = Z_3$. By Theorem 1.10, $|L_1/L_2| = p$. Since $|Z_3/Z_2| \geq p$ and $L_2 \leq Z_2$, $L_2 = Z_2$. Let H be a normal subgroup of G of order p^3 and exponent p. Then $H \leq Z_3 = L_1$ and $|L_1/H| = p$. Hence $L_1/H \leq Z(G/H)$ which implies that $L_2 = [L_1,G] \leq H$. But $|L_2| = p^3 = |H|$ and so $H = L_2 = Z_2$. Then $\exp Z = \exp Z_2 = p$ and so $s = 2$ (s is the number of invariants of Z). By

Theorem 2.7, $|A(G)|_p \geq p^{2s+c-1} = p^{c+3} = p^7$. Therefore we may assume that G has no normal subgroups of order p^3 and exponent p. Then, by N. Blackburn ([11], Theorem 1.1) G is absolutely regular. Hence G is regular and so $|G/P(G)| = |E(G)| \leq p^2$. Then G is metacyclic and by Theorem 1.4, G is an LA-group.

<u>c = 3</u>. Then $p^4 \geq |G/L_1| \geq p^2$. By Theorem 3.12, $|G/L_1| \neq p^2$. Since G has class 3, G/Z has class 2 < p and by P. Hall ([24], p. 137) G/Z has either type (p^2,p^2) or (p,p,p,p). In the first case G/Z is metacyclic and the result follows from Theorem 1.5. In the second case $P(G) \leq Z$ so that by Theorem 1.16 (I.D. Macdonald) $P(L_1) \leq L_p \leq L_3 = 1$. Thus $\exp L_1 = p$. Let $|G/L_1| = p^3$. If G has two generators the result follows from Theorem 3.13. If G/L_1 is elementary abelian, then $Z \leq \Phi(G) = L_1$ so that $\exp Z = p$ and $s = 2$. Applying Theorem 2.7, $|A(G)|_p \geq p^{2s+c-1} = p^{c+3} = p^6$. Therefore we may take $|G/L_1| = p^4$. Since $G/(L_1Z)$ is elementary abelian, $\Phi(G) \leq L_1Z$. Also $L_1Z \leq \Phi(G)$ so that $\Phi(G) = L_1Z$. As $|L_1 \cap Z| \geq p$, $|\Phi(G)| = |L_1Z| \leq p^3$. Hence G/L_1 has more than two invariants and so $\exp G/L_1 \leq p^2 = |Z|$. By Theorem 2.5, $|A_c(G)| \geq p^4$, and by Theorem 2.6, $|A(G)|_p \geq p^4.p^{c-1} = p^6$.

CHAPTER FOUR

A BOUND FOR THE FUNCTION g(h)

In this Chapter a new bound is obtained for the function $g(h)$ for which $|A(G)|_p \geq p^h$ whenever $|G| \geq p^{g(h)}$. W.R. Scott first conjectured the existence of such functions, and proved that $g(2) = 3$ [43]. In 1956 Ledermann and Neumann have shown that in the general case of finite groups $(h-1)^3 p^{h-1} + h$ is such a function [36]. Since then, many papers have appeared on this topic reducing the bound of $g(h)$ considerably [20], [29], [32]. For finite p-groups the best bound known so far was obtained by K.H. Hyde in [32]. He proved that

$$g(h) = \begin{cases} \frac{1}{2}h(h-3) + 3 & \text{for } h \geq 5 \\ h + 1 & \text{for } h \leq 4. \end{cases}$$

The ultimate aim is, of course, to find the least function $\bar{g}(h)$ for which $|A(G)|_p \geq p^h$ whenever $|G| \geq p^{\bar{g}(h)}$. For cyclic p-groups $\bar{g}(h) = h + 1$ and for elementary abelian p-groups of order greater than p, $\bar{g}(h) = \frac{1}{2} + \frac{1}{2}\sqrt{1+8h}$. Also for LA-groups $\bar{g}(h) \leq h$. Since non-cyclic abelian p-groups of order greater than p^2 are LA-groups, we are only concerned with non-abelian p-groups. For such groups we improve K.H. Hyde's result to

$$g(h) = \begin{cases} \frac{1}{6}h^2 & \text{for } h \geq 12 \\ 2h - 2 & \text{for } h \leq 11 \\ h & \text{for } h \leq 5. \end{cases}$$

Also we give other expressions for $g(h)$ when G belongs to certain classes of finite p-groups.

Throughout this chapter, h will be a positive integer and $g(h)$ a function for which $|A(G)|_p \geq p^h$ whenever $|G| \geq p^{g(h)}$. By Theorem 1.2 (R. Faudree), if G has class $c = 2$, then $|A(G)|_p \geq |G|$. Therefore we take G to have class $c > 2$.

We begin by proving the following.

<u>Lemma 4.1.</u> Let $m_1 \geq m_2 \geq \ldots \geq m_t \geq 1$ be the invariants of G/L_1. Then $\exp G \leq p^{m_1+m_2(c-1)}$. For $t = 2$ $\exp Z \leq \exp Z_{c-2} \leq p^{m_1+m_2(c-1)-2}$.

<u>Proof</u>: By Theorem 1.10 (N. Blackburn), $p^{m_2} \geq \exp L_1/L_2 \geq \ldots \geq \exp L_{c-1}/L_c$ so that $\exp L_1 \leq p^{m_2(c-1)}$. Hence $\exp G \leq p^{m_1+m_2(c-1)}$. Let $t = 2$. Then G can be generated by two elements. By Theorem 1.12 (A. Mann) $\exp L_{c-1} = \exp G/Z_{c-1} = p^b$ (say). Since G/Z_{c-1} is not cyclic $|G/Z_{c-1}| \geq p^{b+1}$ and so $|G/Z_{c-2}| \geq p^{b+2}$. By Theorem 1.10, $|L_1/L_2| \leq p^{m_2}$ so that $|G/L_2| = |G/L_1|.|L_1/L_2| \leq p^{m_1+2m_2}$. Then $|G/L_2| = |G/Z_{c-2}|.|Z_{c-2}/L_2|$ gives $|Z_{c-2}/L_2| \leq p^{m_1+2m_2-b-2}$, as $L_2 \leq Z_{c-2}$. But $\exp L_2 \leq p^{m_2(c-3)+b}$, and $Z \leq Z_{c-2}$ as $c > 2$. Hence $\exp Z \leq \exp Z_{c-2} \leq |Z_{c-2}/L_2|.\exp L_2 \leq p^{m_1+m_2(c-1)-2}$.

The following Lemma is an immediate consequence of Lemma 8.5 in [36] (Ledermann and Neumann).

Lemma 4.2. If $|G/Z| = p^b$ and $k_1 \geq k_2 \geq \ldots \geq k_s \geq 1$ are the invariants of Z, then A(G) has a p-subgroup Γ of outer automorphisms which is isomorphic to $\Gamma \simeq \Gamma_1 \times \Gamma_2 \times \ldots \times \Gamma_s$ where $|\Gamma_i| = \sup(1, p^{k_i - b})$ and $|\Gamma| \geq |Z|.p^{-sb}$.

Remark Below we shall be using the invariants m_j, k_i of G/L_1 and Z respectively as given in Lemmas 4.1, 4.2. In this Chapter, we reserve the symbols m_j, k_i for these invariants and use them without further explanation.

Now we proceed with the main result of this Chapter.

Theorem 4.1. Let G be non-cyclic of order greater than p^2. If $|G| \geq p^{g(h)}$, then $|A(G)|_p \geq p^h$,

$$\text{where } g(h) = \begin{cases} h & \text{for } h \leq 5 \\ 2h-2 & \text{for } h \leq 11 \\ \frac{1}{6}h^2 & \text{for } h \geq 12 \end{cases}$$

We prove this Theorem by considering the three branches of g(h) separately. As mentioned earlier we take $c > 2$.

Theorem 4.1a. $g(h) = h$, for $h \leq 5$.

Proof: From Theorem 2.7 we have $|A(G)|_p \geq p^{2s+c-1} \geq p^{c+1}$. Since $c > 2$ the only case to consider is $c = 3$, $h = 5$. By Theorem 2.4 we may assume that G is a PN-group. For $|Z| = p$, by Theorem 1.6, $|A(G)|_p \geq p.|I(G)| = |G| \geq p^h$. So take $|Z| > p$. If $|G/L_1| = p^2$, by Lemma 4.1, exp $Z \leq p^{c-2} = p$ and therefore $s \geq 2$. Then $|A(G)|_p \geq p^{2s+c-1} \geq p^{c+3} = p^6 > p^h$. If $|G/L_1| \geq p^3$, since G/L_1 is non-cyclic, we get $|A_c(G)| = |\mathrm{Hom}\ (G/L_1,Z)| \geq p^3$. Then by Theorem 2.6, $|A(G)|_p \geq p^3.p^{c-1} = p^5 = p^h$.

<u>Theorem 4.1b</u>. $g(h) = 2h - 2$, for $h \leq 11$.

<u>Proof</u>: Let $|G/Z| = p^b$. For $b \geq h - 1$ by Theorem 1.6, $|A(G)|_p \geq p.|I(G)| = p^{b+1} \geq p^h$. Therefore we may assume that $b \leq h - 2$ so that $k \geq g(h) - (h-2) = h$ (1), where $|Z| = p^k$. By Lemma 4.2, $|A(G)|_p \geq |\Gamma|.|I(G)| \geq p^{k-sb+b} \geq p^h$ for $s = 1$. So take $s > 1$. Consider the following cases:

(A) <u>G is a PN-group</u>. By Theorem 2.6 it is enough to show that $a \geq h - c + 1$ where $|A_c(G)| = p^a$. For $m_1 \geq k_1$ by Theorem 2.2(ii) and (1), $a \geq k + s > h$. So take $k_1 > m_1$ and let $k_i \geq m_1 > k_{i+1}$ for some i, $s > i \geq 1$. Then $m_1 > 1$ and $m > 2$. Let $i = 1$. By Theorem 2.2(iv), $a \geq m + k - k_1 + (t-1)(s-1) \geq m + t$. Here $m + t + c \leq h \leq 11$ since otherwise $a \geq m + t \geq h - c + 1$. Apply Lemma 4.1. For $t \geq 3$, $k_1 \leq m_1 + m_2(c-1)$, so that by (1), $a \geq m+h-k_1+1 \geq h-m_2(c-2) + 2 \geq h-c+1$ since $m+c \leq 8$ and $m_2 \leq 2$. For $t =2$, $k_1 \leq m_1 + m_2(c-1) - 2$ and so $a \geq m+h-k_1+1 \geq h-m_2(c-2)+3 \geq h-c+1$ since $m+c \leq 9$ and $m_2 \leq 3$. So take $i>1$. By Theorem 2.2(iv), $a \geq im+t(s-1) \geq 3i+t \geq 8$. Since $h \leq 11$, $a \geq h-c+1$ except when $m=c=3$, $t=2$, $h=11$. In this case, by Lemma 4.1 $\exp Z \leq p^{c-1} = p^2$, so that $2s \geq k \geq h$. Then $a \geq im+t(s-1) \geq i+2s > h$. Finally take $k_s \geq m_1$. By Theorem 2.2(iv), $a = ms$. For $h < ms+c$, $a \geq h-c+1$. So let $h \geq ms+c$. Since $s > 1$ and $h \leq 11$ we get $2 \leq m \leq 4$, $3 \leq c \leq 7$. Consider <u>$m = 2$</u>. Then Lemma 4.1 gives $\exp Z \leq p^{c-2}$ so that $(c-2)s \geq k \geq h$.

By substituting $c = 3, 4, 5, 6, 7$ in this inequality we get $a = 2s \geq h - c + 1$ in all cases since s is an integer.

<u>$m = 3$</u>. Then $a = 3s \geq 6$ so that $c \leq 5$. Lemma 4.1 gives $\exp Z \leq p^{c-1}$ for $t = 2$ and $\exp Z \leq p^c$ for $t = 3$. So $k_1 \leq c$ and $cs \geq k \geq h$. By substituting $c = 3, 4, 5$ in this inequality we get $a = 3s \geq h - c + 1$ in all cases.

<u>$m = 4$</u>. Then $a = 4s \geq 8$ and so $c = 3$. As above Lemma 4.1 gives $\exp Z \leq p^{2c-2} = p^4$ for $t = 2$ and $\exp Z \leq p^{c+1} = p^4$ for $t \geq 3$. Hence $k_1 \leq 4$ and so $a = 4s \geq k \geq h$.

(B) <u>$G = H \times K$, H abelian of order p^r and K a PN-group.</u> Then $|K| = |G|.p^{-r} > p^{2(h-r)-2}$ so that by (A), $|A(K)|_p \geq p^{h-r}$ since $h - r < 11$. By Corollary 2.4.2, $|A(G)|_p \geq |A(K)|_p.p^{r+s} \geq p^{h+s}$.

<u>Remark</u>. It can be shown by a similar method, that if p^7 divides $|G|$ then p^6 divides $|A(G)|$ and if p^9 divides $|G|$ then p^7 divides $|A(G)|$. Also Theorem 4.1b holds for $h = 12$. The proofs are quite elaborate and lengthy and are therefore omitted.

For the proof of the last part of Theorem 4.1 we shall require the use of certain inequalities. We list them with Roman numerals((I) - (VII)). They are proved separately in an Appendix on p. 60.

<u>Theorem 4.1c</u>. $g(h) = \frac{1}{6}h^2$, $h \geq 12$.

<u>Proof:</u> Let $|G/Z| = p^b$. As in Theorem 4.1b we

take $b \le h - 2$ so that $k \ge g(h) - (h-2) = \frac{1}{6}h^2 - h + 2 > h$, as $h \ge 12$. If $k_1 \ge h$, by Lemma 4.2, $|\Gamma_1| \ge p^{k_1-b} \ge p^{h-b}$ so that $|A(G)|_p \ge |\Gamma_1||I(G)| \ge p^h$. If $k_1 = h - 1 = k_2$, then $|A(G)|_p \ge |\Gamma_1||\Gamma_2||I(G)| \ge p^{2h-b-2} \ge p^h$ as $b \le h - 2$. Therefore we may assume that $k_1 \le h - 1$ and $k_i \le h - 2$ for $i \ge 2$. Then $(h-2)(s-1) \ge k - k_1 \ge \frac{1}{6}h^2 - h + 2 - (h-1) = \frac{1}{6}(h-10)(h-2) - \frac{1}{3}$. Since s is an integer we get:

$$s - 1 \ge \tfrac{1}{6}(h-10) \qquad (1).$$

Consider the following cases:

(A) G is a PN-group. By Theorem 2.6 it is enough to show that $a \ge h - c + 1$, where $|A_c(G)| = p^a$. Therefore we may assume that $h \ge a + c$ (2). If $m_1 \ge k_1$, by Theorem 2.2(ii) $a \ge k + s > h$. So take $k_1 > m_1$ and apply Theorem 2.2(iv).

$m \ge 6$. First let $k_i \ge m_1 > k_{i+1}$ for some i, $s > i \ge 1$. By Theorem 2.2(iv), $a \ge im + k - (k_1+\ldots+k_i) + (t-1)(s-i) \ge im + (s-i)t$. Substituting in (2) we get $h \ge im + (s-i)t+c \ge 6i + 5$. As $k_1 \le h - 1$ and $k_i \le h - 2$ for $i \ge 2$, $a \ge 6i + \frac{1}{6}h^2 - h + 2 - (h-1) - (i-1)(h-2) + 1 = \frac{1}{6}h^2 - h(i+1) + 8i + 2 \ge h - 2 \ge h - c + 1$ by (I) since $h \ge 6i + 5$. Next let $k_s \ge m_1$. By Theorem 2.2(iv), $a = ms$. So by (2), $h \ge ms + c$. For $m \ge 7$, by (1), $a = 7s \ge \frac{7}{6}(h-10) + 7 \ge h - 2 \ge h - c + 1$ since $h \ge 7s + c \ge 17$.

Let $m = 6$. Again by (1), $a = 6s \geq h - 10 + 6 = h - 4 \geq h - c + 1$ for $c \geq 5$. Take $c \leq 4$. By Lemma 4.1 $\exp Z \leq p^{3c-2}$ for $t = 2$, and $\exp Z \leq p^{2c+1} \leq p^{3c-2}$ for $t \geq 3$. Hence $k_1 \leq 3c - 2 \leq 10$ and so $10s \geq k$. Then $60s \geq 6k \geq h^2 - 6h + 12 \geq 10(h-2)$ since $h \geq 6s + c \geq 15$ by (2). So $a = 6s \geq h - 2 \geq h - c + 1$. It remains to show that $a \geq h - c + 1$ is valid for $2 \leq m \leq 5$.

<u>$m = 2$</u>. By Lemma 4.1, $\exp Z \leq p^{c-2}$ so that $(c-2)s \geq k \geq \frac{1}{6}h^2 - h + 2$ (3). Then $2(c-2)s \geq 2k \geq \frac{1}{3}h^2 - 2h + 4 \geq (c-2)(h-c+1)$ by (II), except when $c = 7, 8, 9$ and $h \leq 14$. Therefore $a = 2s \geq h - c + 1$, except in the above cases. In the special cases by substituting values of h and c in (3) we get again $2s \geq h - c + 1$ as s is an integer.

<u>$m = 3$</u>. First let $k_i \geq m_1 > k_{i+1}$, for some i, $s > i \geq 1$. Then $m_1 > 1$ and Lemma 4.1 gives $\exp Z \leq p^{c-1}$. So $k_1 \leq c-1$. By Theorem 2.2(iv), $a \geq 3i + k - (k_1+\ldots+k_i) + 1$ so that $h \geq 3i + c + 2$ by (2). Therefore $a \geq 3i + \frac{1}{6}h^2 - h + 2 - i(c-1) + 1 = \frac{1}{6}h^2 - h - ic + 4i + 3 \geq h - c + 1$ by (III). Next let $k_s \geq m_1$. Then $a = 3s$ and $\exp Z \leq p^c$ by Lemma 4.1. So $cs \geq k \geq \frac{1}{6}h^2 - h + 2$, and $3cs \geq \frac{1}{2}h^2 - 3h + 6 \geq c(h-c+1)$ by (IV). Hence $a = 3s \geq h - c + 1$.

<u>$m = 4$</u>. Lemma 4.1 gives $\exp Z \leq p^{2c-2}$ for $t = 2$ and $\exp Z \leq p^{c+1} \leq p^{2c-2}$ for $t \geq 3$. So $k_1 \leq 2c - 2$ and

$2(c-1)s \geq k \geq \frac{1}{6}h^2 - h + 2$ (4). Let $k_i \geq m_1 > k_{i+1}$ for some i, $s > i \geq 1$. Then $a \geq 4i + k - i(2c-2) + 1 = \frac{1}{6}h^2 - h + 6i - 2ci + 3 \geq h - c + 1$ by (V), since $h \geq a + c \geq 4i + c + 2$. Take $k_s \geq m_1$. Then $a = 4s$ and so $h \geq 4s + c$ (5). For $h \geq 17$, (1) gives $s \geq 3$ so that $h \geq 12 + c$. From (4) we get $4(c-1)s \geq 2k \geq \frac{1}{3}h^2 - 2h + 4 \geq (c-1)(h-c+1)$ by (VI) for $h \geq 17$ and for all h if $c \leq 4$. Therefore in these cases $a = 4s \geq h - c + 1$. Assume $h < 17$. Taking into consideration (5) and the fact that $s > 1$ we get $4s \geq h - c + 1$ in all but the following cases: $c=8$, $h = 16$; $c = 7$, $h = 15, 16$; $c = 6$, $h = 14, 15, 16$; $c = 5$, $h \geq 13$. In these cases, (4) gives $s \geq 3$. Therefore $a = 4s \geq 12 \geq h - c + 1$ in all cases.

<u>$m = 5$</u>. As above, for $t = 2$, $\exp Z \leq p^{2c-1}$ and for $t \geq 3$, $\exp Z \leq p^{2c}$. So $k_1 \leq 2c$ and $2cs \geq k \geq \frac{1}{6}h^2 - h + 2$ (6). For $k_i \geq m_1 > k_{i+1}$ for some i, $s > i \geq 1$, $a \geq 5i + k - (k_1 + \ldots + k_i) + 1 \geq 5i + \frac{1}{6}h^2 - h + 2 - 2ci + 1 \geq h - c + 1$ by (V), as $h \geq a + c \geq 5i + c + 2$. Let $k_s \geq m_1$. Then $a = 5s$ and $h \geq a + c = 5s + c$. From (6) we get $10cs \geq 5k \geq \frac{5}{6}h^2 - 5h + 10 \geq 2c(h-c+1)$ by (VII). Hence $a = 5s \geq h - c + 1$.

(B) <u>$G = H \times K$, H abelian of order p^r and K a PN-group</u>. Then $|K| = |G|.p^{-r} \geq p^{g(h)-r}$, and by Corollary 2.4.2 $|A(G)|_p \geq |A(K)|_p.p^{r+s}$. We may assume that $r < h - s$

otherwise there is nothing to show. For $g(h) - r \le 11$, by Theorem 4.1b, $|A(K)|_p \ge p^{h-r}$, as $g(h) - r \ge 2(h-r) - 2$; for $g(h) - r \ge 12$, by part (A), $|A(K)|_p \ge p^{h-r}$, as $g(h) - r \ge \frac{1}{6}(h-r)^2$ for $r < h - s$. Therefore $|A(G)|_p \ge |A(K)|_p . p^{r+s} \ge p^{h+s}$.

Remark. It is possible to show by using a similar technique that for $h \ge 50$ we can take $g(h) = \frac{1}{7}h^2$. Even for smaller values of h, g(h) can be reduced. For example, we can take $g(18) = 52$ instead of $\frac{1}{6}\, 18^2 = 54$ as given above.

Below we consider the case when G belongs to certain classes of finite p-groups and find some other expressions for g(h).

Theorem 4.2. For p odd, if p^6 divides $|G|$ then p^6 divides $|A(G)|$.

Proof: Let $|G| = p^n$. By Theorems 3.8, 3.16 we may assume that $n \ge 7$. Also by Theorem 2.4 we may take G to be a PN-group. Let $|G/Z| = p^b$. For $b \ge 5$, by Theorem 1.6, $|A(G)|_p \ge p|I(G)| \ge p^6$. For $b \le 3$, by Theorem 3.9, $|A(G)| \ge |G| \ge p^7$. Therefore we take $b = 4$ so that $k = n - 4 \ge 3$ (1), where $|Z| = p^k$. Since $|G/Z| \le p^4$, $c \le 4$. Let $|G/L_1| = p^m$. For $m = 2$, by Lemma 4.1, $\exp Z \le p^{c-2} \le p^2$ and Z is not cyclic.

Then by Theorem 2.7, $|A(G)|_p \geq p^{2s+c-1} \geq p^6$. Therefore take $m \geq 3$ and Z cyclic (2). For $\exp G/L_1 \geq |Z|$, by Theorem 2.2, $|A_c(G)| \geq p^{k+1} \geq p^4$ and by Theorem 2.6, $|A(G)|_p \geq p^4.p^{c-1} \geq p^6$. Let $\exp G/L_1 < |Z|$. By Theorem 2.5, $|A_c(G)| \geq p^m$. So we are done if we show that $m \geq 6 - c + 1$ or $m + c \geq 7$. This however always holds unless $m = c = 3$. Then G/L_1 has either type (p,p^2) or (p,p,p). The first case is not possible since then, by Lemma 4.1 $\exp Z \leq p^{c-1} \leq p^2$, and Z would not be cyclic. In the second case $L_1 = \Phi(G)$ and $\exp L_1 \leq p^2$. By Lemma 4.1 $\exp Z \leq p^c = p^3$ so that by (1) and (2) $k = 3$, $n = 7$. As $Z \nleq L_1 = \Phi(G)$, $G = ZM$ for some maximal subgroup M of G. By Theorem 3.16, $|A(M)|_p \geq |M|$ and therefore by Theorem 1.7, $|A(G)|_p \geq |G| \geq p^7$.

Corollary 4.2.1. For p odd we can take $g(h) = h$, $h \leq 6$.

Theorem 4.3. Let n be an integer such that $p^{nc} \geq |G|$, where c is the class of G. For $h \geq 5$ we can take

$$g(h) = nh - 5(n-1).$$

Proof: By Theorem 4.1a we may assume that $h \geq 6$. Let $|Z| = p^k$ and $|G/Z| = p^b$. For $b \geq h - 1$, by Theorem 1.6, $|A(G)|_p \geq p|I(G)| \geq p^h$. So we take $b \leq h - 2$. Then $k \geq g(h) - (h-2) = (h-5)(n-1) + 2 \geq h - 3$, as $n \geq 2$. From $p^{nc} \geq |G|$ we get $c \geq h - 2$

for $n = 2$, $c \geq h - 3$ for $n = 3, 4$ and $c \geq h - 4$ for $n \geq 5$. Also by Theorem 2.7 we may take $c \leq h - 2$, otherwise $|A(G)|_p \geq p^{c+1} \geq p^h$. Let $G = H \times K$, H abelian of order p^r and K a PN-group. Then K has class c and $|A(K)|_p \geq p^{c+1}$ (Theorem 2.7). By Corollary 2.4.2, $|A(G)|_p \geq p^{c+1}.p^{r+s} \geq p^{c+4} \geq p^h$ as $r \geq 1$, $s \geq 2$. Therefore we may further assume that G is a PN-group. By Theorem 2.6, it is enough to show that $a \geq h - c + 1$, where $|A_c(G)| = p^a$. Now apply Theorem 2.2. to get: for $m_1 \geq k_1$, $a \geq k + s \geq h - 2 \geq h - c + 1$ as $k \geq h - 3$, $c > 2$; for $k_1 > m_1$, $a \geq m + t(s-1)$. It remains therefore to show that $m + t(s-1) \geq h - c + 1$ (1). Consider the following cases:

<u>$n = 2$</u>. Then $c = h - 2$ so that (1) holds unless $m = 2$. When $m = 2$, $\exp Z \leq p^{c-2} = p^{h-4}$ (Lemma 4.1) so that Z is not cyclic as $k \geq h - 3$. Therefore $m + t(s-1) \geq m + t = 4 > h - c + 1$.

<u>$n = 3, 4$</u>. Then $h - 2 \geq c \geq h - 3$ so that (1) holds for $m \geq 3$ except when $m = 3$, $c = h - 3$. In this case $k \geq (h-5)(n-1) + 2 \geq h - 2$ as $h \geq 6$. By Lemma 4.1, $\exp Z \leq p^c = p^{h-3}$ and so Z is not cyclic. Hence $m + t(s-1) \geq m + t \geq 5 > h - c + 1$. Let $m = 2$. Then $\exp Z \leq p^{c-2} \leq p^{h-4}$ and again Z is not cyclic. So $m + t(s-1) \geq m + t = 4 \geq h - c + 1$.

<u>$n \geqq 5$</u>. Then $h - 2 \geq c \geq h - 4$ and $k \geq (h-5)(n-1) + 2 \geq h$. By Lemma 4.2, $|A(G)|_p \geq |\Gamma||I(G)| \geq p^{k-sb+b} \geq p^h$ for $s = 1$. So take $s > 1$. Then $m + t(s-1) \geq h - c + 1$ except when

$m = 2$, $c = h - 4$. In this case $\exp Z \leq p^{c-2} = p^{h-6}$, so that $(h-6)s \geq k$. But $k \geq (h-5)(n-1) + 2 > 2(h-6)$ as $h \geq 6$. Hence $s > 2$ and so $m + t(s-1) \geq m + 2t = 6 > h - c + 1$.

Corollary 4.3.1. If G has large class, then we can take $g(h) = 2h - 5$ for $h \geq 5$.

The following Theorem is of some interest in its own right. It covers the case in which the class c of G is small relative to its order. First we prove the following.

Lemma 4.3. Let $h - c \geq \sqrt{3c-6}$. Then
(i) $h(h-c-2) + 4 \geq (c-2)(h-c+1)$,
(ii) $h(h-c-2) + 4 \geq (c-1)(h-c)$, provided h, c are integers with $c \geq 3$ and $h \geq 6$.

Proof: (i) $(h-c)^2 \geq (3c-6)$ is equivalent to $h(h-c-2) + 4 \geq (c-2)(h-c+1)$.
(ii) Observe that for $c = 4$, $h \geq 7$ so that (ii) holds for $c \leq 4$. If $c \geq 5$, $\sqrt{3c-6} \leq c - 2$. So $(h-c)^2 - (h-c) \geq (3c-6) - (c-2) = 2c - 4$. Then $h(h-c-2) + h - c(h-c) + c \geq 2c - 4$, which gives the result.

Theorem 4.5. Let G have class c. Then $g(h) = \frac{1}{2}h(h-c)$ for $h - c \geq \sqrt{3c-6}$.

Proof: By Theorem 4.1a we may assume that for $c = 3$, $h \geq 6$ so that $h - c \geq 3$ (1). As before we take $|G/Z| = p^b$;

$b \le h - 2$. So $k \ge g(h) - (h-2) = \frac{1}{2}h(h-c-2) + 2$, where $|Z| = p^k$. Observe that $\frac{1}{2}h(h-c-2) + 2 \ge h - c + 1$. In fact, for $c \ge 4$ this follows from Lemma 4.3(i). For $c = 3$, $\frac{1}{2}h(h-5) + 2 \ge h - 2$, as $h \ge 6$. Therefore $k \ge h - c + 1$. Let $\frac{1}{2}(h-c-2) \ge s$. Then $k - sb \ge \frac{1}{2}(h-c-2)(h-b) + 2 > h - b$, and by Lemma 4.2, $|A(G)|_p \ge |\Gamma|.|I(G)| \ge p^{k-sb+b} \ge p^h$. Therefore we take $s \ge \frac{1}{2}(h-c-1)$. Consider the following cases:

(A) G is a PN-group. Applying Theorem 2.6 we have to show that $a \ge h - c + 1$, where $|A_c(G)| = p^a$. If $m_1 \ge k_1$, by Theorem 2.2, $a \ge k + s > h - c + 1$, as $k \ge h - c + 1$. Let $k_1 > m_1$. Then $a \ge m + t(s-1) \ge h - c + 1$ for $m \ge 4$, as $s \ge \frac{1}{2}(h-c-1)$. The only cases left are $m = 2, 3$. Consider

$m = 2$. By Lemma 4.1, $\exp Z \le p^{c-2}$ and so $(c-2)s \ge k$. This gives $2(c-2)s \ge 2k \ge h(h-c-2) + 4 \ge (c-2)(h-c+1)$ by Lemma 4.3(i). Hence $a = 2s \ge h - c + 1$.

$m = 3$. For $t = 2$, $\exp Z \le p^{c-1}$ so that $s(c-1) \ge k$. This gives $2s(c-1) \ge 2k \ge h(h-c-2) + 4 \ge (c-1)(h-c)$ by Lemma 4.3(ii). Then $a \ge 1 + 2s \ge h - c + 1$. Let $t = 3$. Then $\exp Z \le p^c$ and so $cs \ge k$. Hence $2cs \ge 2k \ge h(h-c-2) + 4$. By (1), $h - c \ge 3$. For $h - c = 3$, since $h - c \ge \sqrt{3c-6}$, $c \le 5$. Then $2cs \ge h + 4 = c + 7 > 2c$ and so $s > 1$. If $h - c \ge 4$ we have $s \ge \frac{1}{2}(h-c-1) > 1$. Therefore $a = 3s \ge 2 + 2s \ge h - c + 1$.

(B) <u>$G = H \times K$, H abelian of order p^r and K a PN-group</u>.

Then K has class c and by Corollary 2.4.2, $|A(G)|_p \geq |A(K)|_p . p^{r+s}$.
If $|K/Z(K)| \geq p^{h-r-1}$, by Theorem 1.6, $|A(K)|_p \geq p^{h-r}$ so that $|A(G)|_p > p^h$. Therefore we take $|K/Z(K)| \leq p^{h-r-2}$.
Since $|K| = |G|.p^{-r} \geq p^{g(h)-r}$ we get $|Z(K)| \geq p^{\frac{1}{2}h(h-c-2)+2}$.
Let σ be the number of invariants of $Z(K)$. As in (A) we may assume that $\sigma \geq \frac{1}{2}(h-c-1)$. Then by Theorem 2.7, $|A(K)|_p \geq p^{2\sigma+c-1} \geq p^{h-2}$ and so $|A(G)|_p > p^h$.

APPENDIX

In this Appendix we solve the inequalities (I) - (VII) used in Theorem 4.1c. The proofs are trivial and reduce to solving inequalities of the form $x(h) = ah^2+bh+c \geq 0$ where a, b, c are integers and $a > 0$. In the following we assume that $x(h)$ has real roots and require that $h \geq R$, where R is the greatest root of $x(h)$. As in Theorem 4.1c we take $h \geq 12$, $c \geq 3$, $i \geq 1$.

(I) $\frac{1}{6}h^2 - h(i+1) + 8i + 2 \geq h - 2$ for $h \geq 6i + 5$.

This inequality is equivalent to $h^2 - 6h(i+2) + 48i + 24 \geq 0$.

So $R = 3(i+2) + \sqrt{9i^2-12i+12} = 12 \leq h$ for $i = 1$. For $i > 1$,

$R \leq 3(i+2) + \sqrt{9i^2-12i+12+(6i-11)} = 3(i+2) + \sqrt{(3i-1)^2} = 6i+5 \leq h$.

(II) $\frac{1}{3}h^2 - 2h + 4 \geq (c-2)(h-c+1)$ for $h \geq 15$ or for $h \geq 12$ provided either $c \leq 6$ or $c \geq 10$.

This inequality is equivalent to $h^2 - 3ch + 3c^2 - 9c + 18 \geq 0$.

Since $c^2 - 18c + 81 = (c-9)^2 \geq 0$, $R = \frac{3}{2}c + \frac{1}{2}\sqrt{-3c^2+36c-72} \leq$

$\frac{3}{2}c + \frac{1}{2}\sqrt{-3c^2+36c-72+12(c^2-18c+81)} = \frac{3}{2}c + \frac{1}{2}(3(10-c)) = 15 \geq h$.

For $c \leq 6$, $c^2 - 15c + 54 \geq 0$. So

$R \leq \frac{3}{2}c + \frac{1}{2}\sqrt{-3c^2+36c-72+12(c^2-15c+54)} = \frac{3}{2}c + \frac{1}{2}(3(8-c)) = 12 \leq h$.

Observe that for $c \geq 10$ the inequality has complex roots.

(III) $\frac{1}{6}h^2 - h - ic + 4i + 3 \geq h - c + 1$ for $h \geq 3i + c + 2$.

This inequality is equivalent to $h^2 - 12h - 6ic + 24i+6c+12 \geq 0$.

Since $9i^2 + c^2 - 2c - 8 > 0$, $R = 6 + \sqrt{24+6ic-24i-6c} \leq$

$6 + \sqrt{24+6ic-24i-6c+(9i^2+c^2-2c-8)} = 6 + (3i+c-4) \leq h$.

(IV) $\frac{1}{2}h^2 - 3h + 6 \geq c(h-c+1)$.

This inequality is equivalent to $h^2 - 2h(3+c) + 2c^2-2c+12 \geq 0$.

Since $c^2 - 13c + 42 \geq 0$, $R = 3 + c + \sqrt{-c^2+8c-3} \leq 3 + c +$

$\sqrt{-c^2+8c-3+2(c^2-13c+42)} = 3 + c + (9-c) = 12 \leq h$.

(V) $\frac{1}{6}h^2 - h + 5i - 2ci + 3 \geq h - c + 1$ for $h \geq 4i + c + 2$.

This inequality is equivalent to $h^2-12h+30i-12ci+6c+12 \geq 0$.

So $R = 6+\sqrt{24-30i+12ci-6c}$. For $i = 1$, $R = 6+\sqrt{6c-6} \leq 6 + c \leq h$

if $c \geq 5$, and $R \leq 6+\sqrt{24} < 12 \leq h$ if $c \leq 5$. For $i > 1$, since

$16i^2 + c^2 -4ci - 2i - 2c - 8 = (2i-c+1)^2 + 12i^2 - 6i - 9 > 0$,

$R \leq 6 + \sqrt{24-30i+12ci-6c+(16i^2+c^2-4ci-2i-2c-8} = 6 + (4i+c-4) \leq h$.

(VI) $\frac{1}{3}h^2 - 2h + 4 \geq (c-1)(h-c+1)$ for $h \geq 12 + c$ or for $c \leq 4$.

This inequality is equivalent to $h^2-3h(c+1)+3c^2-6c+15 \geq 0$.

Since $c^2 - 21c + 123 \geq 0$, $R = \frac{3}{2}(c+1)+\frac{1}{2}\sqrt{-3c^2+42c-51} \leq$

$\frac{3}{2}(c+1) + \frac{1}{2}\sqrt{-3c^2+42c-51+4(c^2-21c+123)} = \frac{3}{2}(c+1) + \frac{1}{2}(21-c) =$

$c + 12 \leq h$. For $c \leq 4$, $R \leq 12 \leq h$.

(VII) $\frac{5}{6}h^2 - 5h + 10 \geq 2c(h-c+1)$ for $h \geq 10 + c$.

This inequality is equivalent to $5h^2-6h(5+2c)+12c^2-12c+60 \geq 0$.

Since $5c^2-62c+260 \geq 0$, $R = \frac{3}{5}(5+2c) + \frac{1}{5}\sqrt{-24c^2 + 240c-75} \leq$

$\frac{3}{5}(5+2c) + \frac{1}{5}\sqrt{\ \ 24c^2+240c-75+5(5c^2-62c+260)} =$

$\frac{3}{5}(5+2c) + \frac{1}{5}(35-c) = 10 + c \leq h$.

REFERENCES

[1] J.E. Adney and T_I. Yen "Automorphisms of a p-group" Illinois J. Math. 9 (1965), 137-143.

[2] J.L. Alperin "On a special class of regular p-groups" Trans. Amer. Math. Soc. 106 (1963), 77-99.

[3] G. Baumslag and N. Blackburn "Groups with cyclic upper central factors" Proc. London Math. Soc. (3), 10 (1960), 531-544.

[4] Ja.G. Berkovich "On p-groups of finite order" Siberian Math. J. 9 (1968), 963-978.

[5] " "Normal subgroups in a finite group" Dokl. Akad. Nauk. SSSR 182 (1968) No. 2, 1117-1120.

[6] " "Subgroup and normal structure of a finite p-group" Dokl. Akad. Nauk. SSSR 196 (1971), No. 2, 71-75.

[7] " "The structure of a group and the structure of its subgroups" Dokl. Akad. Nauk. SSSR 179 (1968) No. 1, 301-304.

[8] N. Blackburn "On prime-power groups in which the derived group has two generators" Proc. Camb. Phil. Soc. 53 (1957), 19-27.

[9] " "On prime-power groups with two generators" Proc. Camb. Phil. Soc. 54 (1958), 327-337.

[10] " "On a special class of p-groups" Acta Math. 100 (1958), 45-92.

[11] " "Generalizations of certain elementary Theorems on p-groups" Proc. Lond. Math. Soc. (3), 11 (1961), 1-22.

[12] R.M. Davitt "The automorphism group of a finite metacyclic p-group"
Proc. Amer. Math. Soc. 25 (1970), 876-879.

[13] " "The automorphism group of finite p-abelian p-groups"
Illinois J. Math. 16 (1972), 76-85.

[14] R.M. Davitt and A.D. Otto "On the automorphism group of a finite p-group with the central quotient metacyclic"
Proc. Amer. Math. Soc. 30 (1971) No. 3, 467-472.

[15] " "On the automorphism group of a finite modular p-group"
Proc. Amer. Math. Soc. 35 (1972) No. 2, 399-404.

[16] R. Faudree "A note on the automorphism group of a p-group"
Proc. Amer. Math. Soc. 19 (1968), 1379-1382.

[17] J.A. Gallian "Finite p-groups with homocyclic central factors"
Canadian J. Math. 26 (1974), 636-643.

[18] W. Gaschütz "Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen"
Journal of Algebre 4 (1966), 1-2.

[19] D. Gorenstein "Finite groups"
Harper and Row, publishers, New York, 1968.

[20] J.A. Green "On the number of automorphisms of a finite group"
Proc. Roy. Soc. (London) Ser A. 237 (1956), 574-581.

[21] M. Hall, Jr. "The theory of groups"
Macmillan Company, 1959.

[22] P. Hall "A contribution to the theory of groups of prime-power order"
Proc. London Math. Soc. (2), 36 (1933), 29-95.

[23] " "On a theorem of Frobenius"
Proc. London Math. Soc. (3), 40 (1933-35), 468-501.

[24] " "The classification of prime-power groups"
Journal Reine Angew Math. 182 (1940), 130-141.

[25] C. Hobby "The Frattini subgroup of a p-group"
Pac. J. Math. 10 (1960), 209-212.

[26] " "A Characteristic subgroup of a p-group"
Pac. J. Math. 10 (1960), 853-858.

[27] C. Hobby and C.R.B. Wright "A generalization of a theorem of N. Itô on p-groups"
Proc. Amer. Math. Soc. 11 (1960) 707-709.

[28] " "Errata"
Proc. Amer. Math. Soc. 12 (1961), 100.

[29] J.C. Howarth "On the power of a prime dividing the order of the automorphism group of a finite group"
Proc. Glasgow Math. Assoc. 4 (1960), 163-170.

[30] K.G. Hummel "The order of the automorphism group of a central product"
Proc. Amer. Math. Soc. 47 (1975) No. 1, 37-40.

[31] B. Huppert "Endliche Gruppen I"
Springer-Verlag Berlin Heidelberg, 1967.

[32] K.H. Hyde "On the order of the Sylow-subgroups of the automorphism group of a finite group"
Glasgow Math. J. 11 (1970), 88-96.

[33] I. Kaplansky "Infinite abelian groups"
Ann Arbor University of Michigan Press, 1954.

[34] L.S. Kazarin "On some classes of finite groups"
Dokl. Akad. Nauk. SSSR 197 (1971) No. 4, 549-553.

[35] W. Ledermann and B.H. Neumann "On the order of the automorphism group of a finite group I"
Proc. Roy. Soc. Ser A. 233 (1956), 494-506.

[36] " "On the order of the automorphism group of a finite group II"
Proc. Roy. Soc. Ser A. 235 (1956), 235-246.

[37] I.D. Macdonald "The Hughes problem and others"
J. Austral. Math. Soc. 10 (1969), 475-479.

[38] " "Generalizations of a classical theorem about Nilpotent groups"
Illinois J. Math. 8 (1964), 556-570.

[39] A. Mann "Regular p-groups II"
Israel J. Math. 14 (1973), 294-303.

[40] A.D. Otto "Central automorphisms of a finite p-group"
Trans. Amer. Math. Soc. 125 (1966), 280-287.

[41] R. Ree "The existence of outer automorphisms of some groups"
Proc. Amer. Math. Soc. 7 (1956), 962-964.

[42] " "The existence of outer automorphisms of some groups II"
Proc. Amer. Math. Soc. 9 (1958), 105-109.

[43] W.R. Scott "On the order of the automorphism group of a finite group"
Proc. Amer. Math. Soc. 5 (1954), 23-24.

[44] " "Group theory"
Prentice-Hall, 1964.

[45] Tsuboi, Teruo "Note on metabelian groups"
Sci. Rep. Saitama Univer. Ser. A, 2 (1953) 59-68.

[46] R.W. Van Der Waall "On finite p-groups whose commutator subgroups are cyclic"
Nederl. Akad. Wetench. Proc. Ser A. 76 (1973), 342-345.

[47] M.N. Vislavskij "Finite p-groups with an abelian normal divizor whose factor group is cyclic and with cyclic center"
Izv. Vyss. Vcebn Zaned Math. 1967 No. 11 (1966), 11-16.

[48] J. Wiegold "Multiplicators and groups with finite central factor-groups"
Math. Zeit. 89 (1965), 345-347.

[49] H. Zassenhaus "The theory of groups"
Translated from the Cerman, Chelsea Publishing Company, 1949.