

Author: Theodoros Exarchakos

Title: Automorphisms of a Finite P-Group

Creator: HDML

AUTOMORPHISMS OF A FINITE P-GROUP

By
Theodoros Exarchakos

The existence of functions $g(h)$ for which $|A(G)| \geq p^h$ whenever $|G| \geq p^{g(h)}$, G any finite group, has been the subject of research for some time. Ledermann and Neumann have shown that in the general case $(h-1)^3 p^{h-1} + h$ is one such a function [7]. For non-abelian p -groups K.H. HYDE reduced this to $\frac{1}{2} h(h-3)+3$ for $h \geq 5$ and $h+1$ for $h \leq 4$ [6]. In this paper we shall improve this result by showing that $g(h) = \frac{1}{2} h(h-8)$ for $h \geq 12$, $g(h) = 2h-2$ for $h \leq 11$ and $g(h) = h$ for $h \leq 5$ is such a function. The same technique can be used to reduce this even further and get $g(h) = \frac{1}{2} h(h-b)$ for $8 \leq b \leq 13$ and $h \geq 2b-4$. There is no reason why this method should not extend for all $b \geq 14$, except that for large values of b the number of subcases increases considerably. Finally we prove that if G has class c , then we can take $g(h) = \frac{1}{2} h(h-c)$, where $h \geq c + \sqrt{3c-6}$.

Notation: G is always a finite p -group, $|G|$ denotes the order of G , $|K|_p$ is the greatest power of p which divides $|K|$, $G' = [G, G]$ is the commutator subgroup of G , $Z = Z(G)$ is the center of G . Also we shall take $\left| \frac{G}{G'} \right| = p^m$ and $|Z| = p^k$. Since $\frac{G}{G'}$ and Z are both finite abelian p -groups,

$\frac{G}{G'} \cong C_{p^{m_1}} \times \dots \times C_{p^{m_t}}$ and $Z \cong C_{p^{k_1}} \times C_{p^{k_2}} \times \dots \times C_{p^{k_s}}$, where C_{p^x} is cyclic group of order p^x , $m_1 \geq m_2 \geq \dots \geq m_t$ with $\sum_{j=1}^t m_j = m$ and $k_1 \geq k_2 \geq \dots \geq k_s$ with $\sum_{i=1}^s k_i = k$. The numbers $p^{m_1}, p^{m_2}, \dots, p^{m_t}$ are the invariants of $\frac{G}{G'}$ and the numbers $p^{k_1}, p^{k_2}, \dots, p^{k_s}$ are the invariants of Z . Here t and s are the numbers of invariants of $\frac{G}{G'}$ and Z respectively. Since G is a finite p -group, G is nilpotent. Let G be of class c and $G = L_0 \supset L_1 \supset L_2 \supset \dots \supset L_c = 1$, $1 = Z_0 \subset Z_1 \subset Z_2 \subset \dots \subset Z_c = G$ be the lower and the upper central series of G where $L_1 = G' = [G, G]$ and $Z_1 = Z(G) = Z$. If G is non-abelian then both $\frac{G}{G'}$ and $\frac{G}{Z_{c-1}}$ are non-cyclic and $L_i \cong Z_{c-i}$ for all i [5]. Denote $A(G)$, $I(G)$, $A_c(G)$ the groups of automorphisms, inner automorphisms and central automorphisms of G respectively. Let $\text{Hom}(G, H)$ be the homomorphisms of G into H ; if H is abelian then $\text{Hom}(G, H) = \text{Hom}(\frac{G}{G'}, H)$. G is called a pN -group if it has no non-trivial abelian direct factor. G is of maximal class if $|G| = p^n$ and $c = n-1$.

The following two theorems will give us a general expression for the order of the group of central automorphisms $A_c(G)$ of a pN -group G in terms of the invariants of $\frac{G}{G'}$ and Z . In theorem 3 we show that $|A_c(G)| \cdot p^{c-1}$ is a factor of the order of the automorphism group $A(G)$ of G (c is the class of G). We then use these results to find the bounding function $g(h)$ (Theorem 4).

Theorem 1: *Let G be a pN -group. If a_2, b_2 is the number of times p^2 appears in the invariants of $\frac{G}{G'}$ and Z respectively, then $|A_c(G)| = p^A$ where*

$$A = m \cdot s - \sum_{y=1}^{k_1} b_y \sum_{x>y}^{m_1} a_x (x-y).$$

Proof: Let $Z = \prod_{i=1}^s C_p^{k_i}$ with $\sum_{i=1}^s k_i = k$ then $\sum_{y=1}^{k_1} y b_y = k$.

Similarly if $\frac{G}{G^r} = \prod_{j=1}^t C_p^{m_j}$ with $\sum_{j=1}^t m_j = m$ then $\sum_{x=1}^{m_1} x a_x = m$.

Since G is a pN -group $|A_c(G)| = |\text{Hom}(G, Z)|$ [1]. But Z is abelian

and so $|\text{Hom}(G, Z)| = |\text{Hom}(\frac{G}{G^r}, Z)|$. Then $|A_c(G)| = |\text{Hom}(\frac{G}{G^r}, Z)| =$

$$\begin{aligned} &= |\text{Hom}(\prod_{j=1}^t C_p^{m_j}, \prod_{i=1}^s C_p^{k_i})| = \prod_{j,i}^{t,s} |\text{Hom}(C_p^{m_j}, C_p^{k_i})| = \\ &= \prod_{j,i}^{t,s} |C_p^{\min(m_j, k_i)}| = \prod_{j,i}^{t,s} p^{\min(m_j, k_i)} = p^A \quad \text{for some } A \quad (1). \end{aligned}$$

Summing powers over $m_j = 1, 2, \dots, m_1$ we get:

$$\begin{aligned} A &= s a_1 + (2a_2(s-b_1) + a_2 b_1) + (3a_3(s-b_1-b_2) + a_3(b_1+2b_2)) + \dots = \\ &= s(a_1 + 2a_2 + 3a_3 + \dots) + (b_1 \sum_{x=2}^{m_1} a_x + 2b_2 \sum_{x=3}^{m_1} a_x + \dots) - b_1(2a_2 + 3a_3 + \dots) \\ &- b_2(3a_3 + 4a_4 + \dots) - \dots = s \sum_{x=1}^{m_1} x a_x + \sum_{y=1}^{k_1} y b_y \sum_{x>y}^{m_1} a_x - \\ &- \sum_{y=1}^{k_1} b_y \sum_{x>y}^{m_1} x a_x = m \cdot s - \sum_{y=1}^{k_1} b_y \sum_{x>y}^{m_1} a_x (x-y). \end{aligned}$$

Theorem 2: Let G be as in Theorem 1.

(i) If $m_1 \leq k$, then $A \geq m+r$, where $r = \sum_{i=2}^s (\sum_{x=1}^{k_i} x a_x + k_i \sum_{x>k_i} a_x)$.

(ii) If $m_1 \leq k_s$, then $A = m \cdot s$.

(iii) If $k_1 \leq m_t$, then $A = kt$.

(iv) If $m_t < k_1 < m_1 \leq k$, then $A \geq m+k+s-(m_1+1) \geq k+s$.

(v) If $k_i \geq m_1$ for some i with $1 \leq i \leq s$, then $A \geq im + t(s-i) \equiv B_i$.

Proof: Summing power over $m_j = 1, 2, \dots, m_1$ in (1) for $k_i = k_s, \dots, k_1$ we get.

$$A = \left(\sum_{x \geq 1}^k x a_x + k_s \sum_{x > k_s}^{m_1} a_x \right) + \dots + \left(\sum_{x \geq 1}^{k_1} x a_x + k_1 \sum_{x > k_1}^{m_1} a_x \right). \text{ Thus}$$

$$A = \sum_{i=2}^s \left(\sum_{x \geq i}^{k_i} x a_x + k_i \sum_{x > k_i}^{m_1} a_x \right) + \sum_{i=1}^s k_i \left(\sum_{x > k_1}^{m_1} a_x \right) + \sum_{x \geq 1}^{k_1} x a_x =$$

$$\sum_{i=2}^s \left(\sum_{x \geq i}^{k_i} x a_x + k_i \sum_{x > k_i}^{m_1} a_x \right) + k \sum_{x > k_1}^{m_1} a_x + \sum_{x \geq 1}^{k_1} x a_x \quad (2). \quad \text{But}$$

$k \geq m_1$ and so $k \sum_{x > k_1}^{m_1} a_x \geq \sum_{x > k_1}^{m_1} x a_x$. Hence $k \sum_{x > k_1}^{m_1} a_x + \sum_{x \geq 1}^{k_1} x a_x \geq$

$$\sum_{x \geq 1}^{m_1} x a_x = m.$$

Putting $r = \sum_{i=2}^s \left(\sum_{x \geq i}^{k_i} x a_x + k_i \sum_{x > k_i}^{m_1} a_x \right)$ we get $A \geq m+r$.

(ii) Since $m_1 \leq k_s$ we have $m_j \leq k_s$ for all $j=1, 2, \dots, t$.

Moreover $\sum_{x > k_i}^{m_1} a_x = 0$ while $\sum_{x \geq 1}^{k_i} x a_x = \sum_{x \geq 1}^{m_1} x a_x = m$. Let $\partial_i =$

$$= \sum_{x \geq 1}^{k_i} x a_x + k_i \sum_{x > k_i}^{m_1} a_x \quad \text{for all } i=1, 2, \dots, s. \text{ Then } \partial_i = m \quad \text{and}$$

$$\text{so } A = \sum_{i=1}^s \partial_i = \sum_{i=1}^s m = ms.$$

(iii) Since $k_1 \leq m_t$ we have $k_i \leq m_t$ for all $i=1,2,\dots,s$.

$$\begin{aligned} \text{Moreover } a_x &= 0 \text{ for } x < m_t. \text{ Hence } \partial_i = k_i \sum_{x \geq k_i}^{m_1} a_x = \\ &= k_i \sum_{x \geq m_t}^{m_1} a_x = k_i t. \end{aligned}$$

$$\text{Thus } A = \sum_{i=1}^s \partial_i = \sum_{i=1}^s k_i t = kt.$$

(iv) Let $\phi_i = \sum_{x>1}^{k_i} xa_x + k_i \sum_{x>k_i}^{k_1} a_x$ for $i=2,3,\dots,s$. From

$$(2) \text{ we get } A = \sum_{i=2}^s \phi_i + k \sum_{x>k_1}^{m_1} a_x + \sum_{x \geq 1}^{k_1} xa_x. \text{ If } \sum_{x \geq 1}^{k_1} xa_x = 0,$$

then $k_i < m_t$ and since $m_t < k$, $\sum_{x>k_i}^{k_1} a_x \geq 1$, so $\phi_i \geq 1$. On

the other hand if $\sum_{x>k_i}^{k_1} a_x = 0$, then $k_i \geq m_t$ and so $\sum_{x \geq 1}^{k_i} xa_x \geq 1$

Therefore $\phi_i \geq 1$ for all $i=2,3,\dots,s$. Since $k \geq m_1$ we have $k =$

$$= m_1 + b \text{ for some } b \geq 0 \text{ and so } A \geq s-1 + \sum_{x \geq 1}^{k_1} xa_x + m_1 \sum_{x>k_1}^{m_1} a_x +$$

$$+ b \sum_{x>k_1}^{m_1} a_x. \text{ Since } \sum_{x>k_1}^{m_1} a_x \geq 1 \text{ as } k_1 < m_1 \text{ and } \sum_{x \geq 1}^{k_1} xa_x +$$

$$+ m_1 \sum_{x>k_1}^{m_1} a_x \geq \sum_{x \geq 1}^{m_1} xa_x = m \text{ we have } A \geq s-1+m+b = s-1+m+k-$$

$-m_1 = m+k+s-(m_1+1)$. Since $\frac{G}{G'}$ cannot be cyclic, we have m

$\geq m_1+1$ and so $A \geq m+k+s-(m_1+1) \geq k+s$.

(v) Let $k_i \geq m_1$ and $k_{i+1} < m_1$ for some i . If ∂_ℓ is as defined in (ii) then $A = \sum_{i=1}^s \partial_\ell$. For $\ell \leq i$ we have

$k_\ell \sum_{x > k_\ell}^{m_1} a_x = 0$, while $\sum_{x \geq 1}^{k_\ell} xa_x = \sum_{x \geq 1}^{m_1} xa_x = m$, so that $\theta_\ell = m$.

On the other hand if $\ell \geq i+1$, then we have

$$\theta_\ell = \sum_{x \geq 1}^{k_\ell} xa_x + k \sum_{x > k_\ell}^{m_1} a_x \geq \sum_{x \geq 1}^{k_\ell} a_x + \sum_{x > k_\ell}^{m_1} a_x = \sum_{x \geq 1}^{m_1} a_x = t.$$

$$\begin{aligned} \text{Therefore } A &= \sum_{\ell=1}^s \theta_\ell = \sum_{\ell=1}^i \theta_\ell + \sum_{\ell=i+1}^s \theta_\ell = \sum_{\ell=1}^i m + \sum_{\ell=i+1}^s t = \\ &= im + t(s-i) \equiv B_i. \end{aligned}$$

Theorem 3: If G is a finite p -group of class $c \neq 2$, then $|A_c(G)| \cdot p^{c-1}$ is a factor of $|A(G)|$.

Proof: If G is abelian the result is trivial. Assume that G is non-abelian, then $\left| \frac{G}{Z_{c-1}} \right|$ is not cyclic and so

$$\left| \frac{G}{Z_{c-1}} \right| \geq p^2 \text{ and } \left| \frac{Z_{i+1}}{Z_i} \right| \geq p \text{ for all } i=1,2,\dots,c-2, \text{ Where}$$

$1 = Z_0 \subset Z_1 \subset Z_2 \subset \dots \subset Z_c = G$ is the upper central series of G .

$$\text{Hence } \left| \frac{G}{Z_2} \right| \geq p^{c-1} \quad (1).$$

$$\text{Since } |A_c(G) \cap I(G)| = |Z(I(G))| = \left| Z\left(\frac{G}{Z}\right) \right| = \left| \frac{Z_2}{Z} \right| \quad \text{we}$$

$$\text{have } |A(G)|_p \geq |A_c(G) \cdot I(G)| = \frac{|A_c(G)| \cdot |I(G)|}{|A_c(G) \cap I(G)|} = \frac{|A_c(G)| \cdot \left| \frac{G}{Z} \right|}{\left| \frac{Z_2}{Z} \right|} =$$

$$= |A_c(G)| \cdot \left| \frac{G}{Z_2} \right| \geq |A_c(G)| \cdot p^{c-1} \text{ by (1).}$$

Remarks: From theorems 2 and 3 we easily get the following

(a) If $k_1 \geq m_1$, but $k_i < m_1$ for all $i=2,3,\dots,s$, then $A \geq B_1 = m + t(s-1)$ and $(m_1-1)(s-1) \geq k-k_1$.

(b) Since $m \geq t$ we have $im+t(s-i) \geq (i-1)m+t(s-i+1)$ for
all i with $i=2,3,\dots,s$ and so $B_i \geq B_{i-1}$.

(c) If G is a pN -group, then $|A_c(G)| \geq p^{2s}$

(d) If G is any non-abelian p -group of class c , then
 $|A(G)|_p \geq p^{c+1}$ and if G is of maximal class then $|A(G)|_p \geq |G|_p$
If G is a pN -group then $|A(G)|_p \geq p^{2s+c-1}$

(e) If G is a pN -group and $c \geq n-3$, then $|A(G)|_p \geq |G|_p$
for $s \geq 2$.

Lemma 1: Let G be a non-abelian finite p -group. If
 $\left| \frac{G}{Z} \right| = p^d$ and s is the number of invariants of Z , then $A(G)$
has a subgroup A of outer automorphisms and $|A| \geq |Z| \cdot p^{-ds}$.

This lemma is an immediate consequence of lemma 8.5 in [7].

Lemma 2: Let G be a finite p -group of class $c \geq 3$, If
 $p^{m_1} \geq p^{m_2} \geq \dots \geq p^{m_t}$ are the invariants of $\frac{G}{G'}$, then $\exp G$
 $\leq p^{m_1+m_2(c-1)}$. In particular if $\frac{G}{G'}$ has two invariants p^{m_1}
 $\geq p^{m_2}$, then $\exp Z \leq \exp Z_{c-2} \leq p^{m_1+m_2(c-1)-2}$.

Proof: Let $G = L_0 \supset L_1 \supset L_2 \supset \dots \supset L_c = 1$ be the lower central series of G . Then $p^{m_2} \geq \exp \frac{L_1}{L_2} \geq \exp \frac{L_2}{L_3} \geq \dots \geq \exp \frac{L_{c-1}}{L_c}$ [2]. Hence $\exp L_1 \leq p^{m_2(c-1)}$. But $\exp \frac{G}{L_1} = p^{m_1}$ and so $\exp G \leq p^{m_1+m_2(c-1)}$. Let $\frac{G}{G'}$ has two invariants $p^{m_1} \geq p^{m_2}$. Then $\frac{L_1}{L_2}$ is cyclic of order at most p^{m_2} [2]. Hence $\left| \frac{G}{L_2} \right| = \left| \frac{G}{L_1} \right| \left| \frac{L_1}{L_2} \right| \leq p^{m_1+2m_2}$. Since G has two generators $\exp \frac{G}{Z_{c-1}} = \exp L_{c-1}$. If $\exp L_{c-1} = p^k$, then $\exp \frac{G}{Z_{c-1}} = p^k \leq p^{m_2}$ and since $\frac{G}{Z_{c-1}}$ can-

not be cyclic we get $\left| \frac{G}{Z_{c-1}} \right| \geq p^{k+1}$ and so $\left| \frac{G}{Z_{c-2}} \right| \geq p^{k+2}$.

From $p^{m_2} \geq \exp \frac{L_1}{L_2} \geq \dots \geq \exp \frac{L_{c-1}}{L_c} = p^k$ we get $\exp L_2 \leq p^{m_2(c-3)+k}$.

But $L_2 \subseteq Z_{c-2}$ and $\left| \frac{Z_{c-2}}{L_2} \right| = \left| \frac{G}{L_2} \right| : \left| \frac{G}{Z_{c-2}} \right| \leq p^{m_1+2m_2-k-2}$.

Since $c \geq 3$ we have $Z \subseteq Z_{c-2}$ and so $\exp Z \leq \exp Z_{c-2} \leq \left| \frac{Z_{c-2}}{L_2} \right| \exp L_2 \leq p^{m_1+m_2(c-1)-2}$.

Lemma 3: ([4]) *W. Gaschütz*. A finite non-abelian p-group has a non-trivial outer automorphism of order a power of p.

Theorem 4: Let G be a finite non-abelian p-group .
If $|G| \geq p^{g(h)}$ then $|A(G)|_p \geq p^h$, where

$$\begin{aligned} & h \text{ for } h \leq 5, \\ & g(h) = 2h-2 \text{ for } h \leq 11, \\ & \frac{1}{2} h (h-8) \text{ for } h \geq 12, h \text{ an integer} \end{aligned}$$

We divide this theorem into 3 parts.

Theorem 4a: $g(h) = h$ for $h \leq 5$.

Proof: If G is of class two then $|A(G)|_p \geq |G| \geq p^h$ [3]. We assume therefore that $c \geq 3$. By remark d, $|A(G)|_p \geq p^{c+1}$, so the only case to consider is $c=3, h=5$. Also we may assume that G is a PN-group [9]. If $|Z|=p$, then by Lemma 3, $|A(G)|_p \geq p \cdot |I(G)| \geq |G| \geq p^h$. So we assume, $|Z| \geq p^2$. If $\left| \frac{G}{Z} \right| = p^2$, by Lemma 2, $\exp Z \leq p^{c-2} = p$ and by Theorem 2, $|A_c(G)| = p^{m \cdot s} \geq p^4$. Then by Theorem 3, $|A(G)|_p \geq$

$|A_c(G)| \cdot p^{c-1} \geq p^6$. If $\left|\frac{G}{G^c}\right| \geq p^3$, since $|Z| \geq p^2$ and $|A_c(G)| = |\text{Hom}(\frac{G}{G^c}, Z)|$ we get $|A_c(G)| \geq p^3$, so that $|A(G)|_p \geq p^3 \cdot p^{c-1} = p^5 = p^h$. This proves the theorem.

Theorem 4.b: $g(h) = 2h-2$ for $h \leq 11$.

Proof: Again we may assume that $c \geq 3$. Let $\left|\frac{G}{Z}\right| = p^d$, $|Z| = p^k$. If $d \geq h-1$ then $|A(G)|_p \geq |I(G)| \cdot p = \left|\frac{G}{Z}\right| \cdot p \geq p^h$ by Lemma 3. Hence we may assume that $3 \leq d \leq h-2$ so that $k \geq g(h) - (h-2) = h$. By Lemma 1, $|A(G)|_p \geq |A| \cdot |I(G)| \geq p^{k-sd+d} \geq p^h$ for $s = 1$. So we take $s > 1$. Consider the following cases.

A: G is a pN-group: We may assume that $\exp \frac{G}{G^c} \leq |Z|$ since otherwise $\left|\frac{G}{G^c}\right| > |Z|$ which implies $|A_c(G)| = |\text{Hom}(\frac{G}{G^c}, Z)| \geq |Z| \geq p^h$. By Theorem 2, if $k_i < m_i$ then $|A_c(G)| \geq p^k \geq p^h$. If $k_i \geq m_i$ for some i then $|A_c(G)| \geq p^{B_i}$, where $B_i = im + t(s-i) \geq B_{i-1}$ (Remark b). By Theorem 3 it is enough to show that $B_i \geq h-c+1$. Since $B_i \geq B_1 = m+t(s-1) \geq m+t$, as $s \geq 2$, we may assume that $m+t+c \leq B_1+c-1 \leq h \leq 11$, otherwise we have nothing to show. But $t \geq 2$ so that $2 \leq m \leq 6$, $3 \leq c \leq 7$. Consider

m = 2. By Lemma 2 we get $\exp Z \leq p^{c-2}$. Hence $s(c-2) \geq k \geq h$. By substituting $c = 3, 4, 5, 6, 7$ we get $B_i \geq h-c+1$ in all cases.

m = 3. Let $t = 2$. By Lemma 2, $\exp Z \leq p^{c-1}$ so that $s(c-1) \geq h$. Substituting values of c as before we get $B_i \geq h-c+1$ in all cases. If $t = 3$ then $\exp Z \leq p^c$ (Lemma 2), so that $cs \geq h$.

By substituting values of c we have $B_1 = 3s \geq h-c+1$ in all cases.

$m = 4$. If $t = 2$ then $2 \leq m_1 \leq 3$, $m_2 \leq 2$ so that by Lemma 2 $\exp Z \leq p^{2c-2}$. If $t \geq 3$ then $m_1 \leq 2$, $m_2 = 1$ and so again $\exp Z \leq p^{c+1} \leq p^{2c-2}$. If $k_i < m_1$ for all $i = 2, 3, \dots, s$ then $(m_1-1)(s-1) \geq k-k_1$ (Remark a) and so $2(s-1) \geq h-(2c-2)$, as $m_1 \leq 3$. Hence $B_1 \geq 4+2(s-1) \geq h-c+1$. On the other hand if $k_i \geq m_1$ for some $i \geq 2$ then $B_i \geq B_2 = 2m+t(s-2) \geq 4+2s$. Hence $B_i \geq h-c+1$ for $c \geq 4$. If $c = 3$ then $\exp Z \leq p^{2c-2} = p^4$ so that $4s \geq h \geq m+t+c \geq 9$. Therefore $s \geq 3$ and so $B_i \geq 4+2s \geq 10 > h-c+1$.

$m = 5$. If $t = 2$ then $3 \leq m_1 \leq 4$, $m_2 \leq 2$ and by Lemma 2, $\exp Z \leq p^{2c-1}$. If $t \geq 3$ then $m_1 \leq 3$, $m_2 \leq 2$ so that $\exp Z \leq p^{2c}$. For $k_i \geq m_1$ for some $i \geq 2$ we have $B_i \geq B_2 = 2m+t(s-2) \geq 10 > h-c+1$ and there is nothing more to show. Otherwise for $k_i < m_1$ for all $i = 2, 3, \dots, s$ we get $(m_1-1)(s-1) \geq k-k_1$. For $m_1 = 4$, $m_2 = 1$ and $\exp Z \leq p^{c+1}$ (Lemma 2) so that $3(s-1) \geq h-(c+1)$ which implies that $B_i \geq B_1 \geq h-c+1$ since $h \leq 11$. For $m_1 \leq 3$ we have $2(s-1) \geq (m_1-1)(s-1) \geq h-2c$ and again $B_1 \geq 5+h-2c \geq h-c+1$ as $c \leq 4$.

$m = 6$. Then $c = 3$, $t = 2$, $h = 11$, $m_2 \leq 3$. Hence $\frac{L_1}{L_2}$ is cyclic of order at most p^3 and $\exp L_2 \leq p^3$ [2]. Then $|L_2| \geq p^{2h-2-9} = p^{11}$. Since $L_2 \leq Z$ we have $s \geq$ number of invariants of $L_2 \geq \frac{1}{3}$. $11 > 3$ so that $B_1 = m+t(s-1) \geq 6+2(s-1) \geq 12 > h$.

B: $G = H \times K$, where H is abelian of order p^r and K is

a pN-group. By [9], $|A(G)|_p \geq p^r \cdot |A(K)|_p$. Since $|K| = |G| \cdot p^{-r} \geq p^{2h-2-r} > p^{2(h-r)-2}$ and $h-r < 11$, by A: we get $|A(K)|_p \geq p^{h-r}$ and so $|A(G)|_p \geq p^r \cdot p^{h-r} = p^h$. This completes the proof of part 4b.

For the last part we shall need,

Lemma 4: Let s, c, h be positive integers with $h \geq 12$

- (i) $sc \geq \frac{1}{2} h(h-10)+2$ implies $2s \geq h-c-1$.
- (ii) $2sc \geq \frac{1}{2} h(h-10)+2$ implies $2s \geq h-c-4$.
- (iii) $3s \geq \frac{1}{2} h(h-10)-2c$ implies $2s \geq h-c-6$. This also holds for $s = 0$.
- (iv) $4s \geq \frac{1}{2} h(h-10)+2-3c$ implies $2s \geq h-c-6$.
- (v) $5s \geq \frac{1}{2} h(h-10)-3c$ implies $2s \geq h-c-7$.
- (vi) $5s \geq \frac{1}{2} h(h-10)-c-1$ implies $2s \geq h-c-6$.

Proof: (i) It is enough to show that $h(h-10)+4 \geq c(h-c-1)$. This is equivalent to $h^2-h(c+10)+c^2+c+4 \geq 0$ which holds for all $h \geq 12$ except when $h = 12, 5 \leq c \leq 7$. For $h = 12, 5 \leq c \leq 7$ we get $sc \geq 14$ which gives $2s \geq h-c-1$, as s is an integer.

(ii) As in (i) it is enough to show that $h(h-10)+4 \geq 2c(h-c-4)$ or equivalently $h^2-h(2c+10)+2c^2+8c+4 \geq 0$. This holds for all $h \geq 13$ and for $h = 12$ if $c \geq 6$. For $h = 12, c \leq 5$, we get $c \cdot s \geq 7$ so that again since s is an integer, $2s \geq h-c-4$.

(iii), (iv), (v) and (vi) can be shown in a similar manner.

Claim 4c: $g(h) = \frac{1}{2} h(h-8), h \geq 12,$

Proof: G is a pN-group: As in Theorem 4b we may assume that $c \geq 3$, $3 \leq d \leq h-2$, $k \geq \frac{1}{2} h(h-8)-(h-2) = \frac{1}{2} h(h-10)+2 > h$. If $s \leq \frac{1}{2} (h-10)$, $k-sd \geq \frac{1}{2} (h-10)(h-d)+2 > h-d$ so that by Lemma 1, $|A| \geq p^{h-d}$. Then $|A(G)|_p \geq |A| \cdot |I(G)| \geq p^{h-d} \cdot p^d = p^h$. Hence we take $s > \frac{1}{2} (h-10) \geq 1$. Also we may assume $\exp \frac{G}{G'} \leq |Z|$, since otherwise $|\frac{G}{G'}| > |Z|$ so that $|A_c(G)| = |\text{Hom}(\frac{G}{G'}, Z)| \geq |Z| \geq p^h$. Now apply Theorem 2. For $k_i < m_i$ we get $|A_c(G)| \geq p^{k+s} > p^h$. For $k_i \geq m_i$ for some i we get $|A_c(G)| \geq p^{B_i}$, $B_i = im+t(s-i) \geq B_{i-1}$ (remark b), so that by Theorem 3, it is enough to show $B_i \geq h-c+1$. If $m+c > 11$, $B_{i+c-1} \geq B_{i+c-1} \geq m+c-1+2s-2 \geq m+c-3+2s > h-1$ so that $B_i \geq h-c+1$. Hence take $m+c \leq 11$. For $m=2$, $\exp Z \leq p^{c-2}$ (Lemma 2), so that $s(c-2) \geq k \geq \frac{1}{2} h(h-10)+2$. Then $B_1 = 2s \geq h-(c-2)-1 = h-c+1$ by Lemma 4(i). For $m \geq 3$, $m_1 = 1$, we get $m_2 = 1$ which gives $\exp Z \leq p^c$ (Lemma 2), so that $c \cdot s \geq k \geq \frac{1}{2} h(h-10)+2$. Then $B_1 \geq 3s \geq 2s+2 \geq h-c-1+2 = h-c+1$ by Lemma 4(i). Below we consider the remaining cases with $m+c \leq 11$, $3 \leq c \leq 8$, $k_1 \geq m_1 \geq 2$, $3 \leq m \leq 8$.

$m=3$. Then $m_1 = 2$, $m_2 = 1$, which gives $\exp Z \leq p^{c-1}$ (Lemma 2), so that $s(c-1) \geq \frac{1}{2} h(h-10)+2$. By Lemma 4(i) (replacing c by $c-1$) we get $2s \geq h-(c-1)-1 = h-c$. Then $B_1 \geq 1+2s \geq h-c+1$.

$m=4$. Then $c \leq 7$. For $t=2$, $\exp Z \leq p^{2c-2}$ (Lemma 2) and for $t=3$, $\exp Z \leq p^{c+1} \leq p^{2c-2}$. So $s(2c-2) \geq k \geq \frac{1}{2} h(h-10)+2$ and by Lemma 4(ii) $2s \geq h-(c-1)-4 = h-c-3$. If $k_i \geq m_i$ for some $i \geq 2$, then $B_i \geq B_2 = 2m+t(s-2) \geq 4+2s \geq$

$\geq h-c+1$. On the other hand if $k_i < m_1$ for all $i \geq 2$, by remark a, $(m_1-1)(s-1) \geq k-k_1$. Since $m_1 \leq 3$, $2(s-1) \geq k-k_1 \geq \frac{1}{2} h(h-10)+2-(2c-2) = \frac{1}{2} h(h-10)+4-2c \geq h+4-2c$. So $B_1 \geq 4+2(s-1) \geq h+8-2c \geq h-c+1$ as $c \leq 7$.

$m = 5$. Then $c \leq 6$. For $t = 2$, $\exp Z \leq p^{2c-1}$ and for $t \geq 3$, $\exp Z \leq p^{2c}$ (Lemma 2). So $2cs \geq \frac{1}{2} h(h-10)+2$ and by Lemma 4(ii), $2s \geq h-c-4$. If $k_i \geq m_1$ for some $i \geq 2$ then $B_i \geq B_2 = 2m+t(s-2) \geq 6+2s > h-c+1$. On the other hand if $k_i < m_1$ for all $i \geq 2$, $(m_1-1)(s-1) \geq k-k_1$ (Remark a). Let $m_1=4$ Then $\exp Z \leq p^{c+1}$ so that $3(s-1) = (m_1-1)(s-1) \geq k-k_1 \geq \frac{1}{2} h(h-10)+2-(c+1)$. Hence $3(s-2) \geq \frac{1}{2} h(h-10)-2-c \geq \frac{1}{2} h(h-10)+1-2c$ as $c \geq 3$ and $s \geq 2$. Then by Lemma 4(iii), $2(s-2) \geq h-c-6$ or $2(s-1) \geq h-c-4$ and so $B_1 \geq 5+2(s-1) \geq h-c+1$. For $m_1 \leq 3$, $2(s-1) \geq \frac{1}{2} h(h-10)+2-2c \geq h+2-2c$ so that $B_1 \geq 5+2(s-1) \geq h+7-2c \geq h-c+1$ as $c \leq 6$. Observe that for $m \geq 6$ if $k_i \geq m_1$ for some $i \geq 2$, then $B_i \geq B_2 = 2m+t(s-2) \geq 2m+2s-4 > 2m-4 + (h-10) \geq h-c+1$. Therefore, in the remaining cases we shall make the further assumption $k_i < m_1$ for all $i \geq 2$. This by remark a, gives $(m_1-1)(s-1) \geq k-k_1$.

$m = 6$. Then $c \leq 5$. For $t \geq 3$, $m_1 \leq 4$ so $\exp Z \leq p^{2c+1}$ (Lemma 2) or $k_1 \leq 2c+1$. Hence $3(s-1) \geq (m_1-1)(s-1) \geq \frac{1}{2} h(h-10)+2-(2c+1) \geq h+1-2c$ and therefore $B_1 = m+t(s-1) \geq 6+3(s-1) \geq h+7-2c \geq h-c+1$ as $c \leq 5$. Next take $t = 2$. For $m_1 = 5$, $\exp Z \leq p^{c+2}$, $k_1 \leq c+2$ and we get $4(s-1) \geq \frac{1}{2} h(h-10)+2-(c+2) = \frac{1}{2} h(h-10)-c$. So $B_1 \geq 6+2(s-1) \geq 6 + \frac{1}{4} h(h-10) - \frac{c}{2} \geq h-c+1$. For $m_1 = 4$, $\exp Z \leq p^{2c}$ (Lemma 2), $k_1 \leq 2c$ so $3(s-1) \geq (m_1-1)$.

$(s-1) \geq \frac{1}{2} h(h-10)+2-2c$. Then $B_1 \geq 6+2(s-1) \geq 6 + \frac{1}{3} h(h-10) + \frac{4}{3} - \frac{4}{3} c \geq h-c+1$ as $c \leq 5$. For $m_1 = 3$, $\exp Z \leq p^{3c-2}$, $k_1 \leq 3c-2$ so $2(s-1) \geq \frac{1}{2} h(h-10)+2-(3c-2) = \frac{1}{2} h(h-10)+4-3c$. Then $B_1 \geq 6+2(s-1) \geq h-c+1$ except the case $h = 12, c = 5$. In this case, since $s \geq 2$ we get $B_1 = m+t(s-1) \geq 4+2s \geq 8 = h-c+1$.

$m = 7$. Then $c \leq 4$. For $t \geq 3$, $m_1 \leq 5$ and $\exp Z \leq p^{3c}$ (Lemma 2), so that $k_1 \leq 3c$. This gives $4(s-1) \geq (m_1-1)(s-1) \geq k-k_1 \geq \frac{1}{2} h(h-10)+2-3c$ and by Lemma 4(iv), $2(s-1) \geq h-c-6$. Then $B_1 \geq m+3(s-1) \geq 7+h-c-6 = h-c+1$. Next let $t = 2$. For $m_1 = 6$, $\exp Z \leq p^{c+3}$, $k_1 \leq c+3$ and so $5(s-1) = (m-1)(s-1) \geq \frac{1}{2} h(h-10)+2-(c+3) = \frac{1}{2} h(h-10)-1$. Then by Lemma 4(vi), $2(s-1) \geq h-c-6$ and so $B_1 \geq 7+2(s-1) \geq h-c+1$. For $m_1 \leq 5$, $\exp Z \leq p^{3c-1}$, $k_1 \leq 3c-1$ so that $4(s-1) \geq \frac{1}{2} h(h-10) + 3-3c$ and by Lemma 4(iv), $2(s-1) \geq h-c-6$. Then $B_1 \geq 7+2(s-1) \geq h-c+1$.

$m = 8$. Then $c = 3$. For $t \geq 3$, $\exp Z \leq p^{3c+1}$, $k_1 \leq 3c+1$ so that since $m_1 \leq 6$ we get $5(s-1) \geq (m_1-1)(s-1) \geq \frac{1}{2} h(h-10)+2-(3c+1) = \frac{1}{2} h(h-10)+1-3c$ and by Lemma 4(v), $2(s-1) \geq h-c-7$ which gives $B_1 \geq 8+2(s-1) \geq h-c+1$. Next take $t = 2$. Since $c = 3$ we have $L_2 \subseteq Z$. But $m_2 \leq 4$ so $\frac{L_1}{L_2}$ is cyclic of order at most $p^{m_2} \leq p^4$ and $\exp L_2 \leq p^{m_2}$ [2]. Then $|L_2| \geq p^{\frac{1}{2}h(h-8)-12}$ and so $s \geq$ number of invariants of $L_2 \geq \frac{1}{4} (\frac{1}{2} h(h-8)-12) = \frac{1}{8} h(h-8)-3$. Hence $B_1 \geq 6+2s \geq$

$\geq 6 + \frac{1}{4} h(h-8) - 6 = \frac{1}{4} h(h-8) \geq h > h-c+1$. This proves the first part.

$G = H \times K$, where H is abelian of order p^r and K is a pN -group. Then K has the same class as G and $|A(G)|_p \geq p^r \cdot |A(K)|_p$ [9]. If we replace $g(h)$ and h by $g(h)-r$ and $h-r$ ($r =$ positive integer) respectively in the first part, the proof remains the same. Applying this to K , since $|K| = |G| \cdot p^{-r} \geq p^{g(h)-r}$ we get $|A(K)|_p \geq p^{h-r}$ and so $|A(G)|_p \geq p^r \cdot p^{h-r} = p^h$. This completes the proof.

By exactly the same method one can prove the following extension.

Theorem 4c'. $g(h) = \frac{1}{2} h(h-b)$ for h, b integers with $0 \leq b \leq 13$, $h \geq 2b-4$.

There is no reason why this method should not work for all $b \geq 14$, except that for large values of b the number of subcases increases considerable.

The special case $b = c$ is covered by Theorem 5 for which we need the following.

Lemma 5. *Let $h \geq c + \sqrt{3c-6}$. 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 and $c \geq 3, h \geq 6$.

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 $c = 3, h \geq 6$ and for $c = 4, h \geq 7$, so that (ii) holds for $c \leq 4$. For $c \geq 5, \sqrt{3c-6} < c-2$, so that $(h-c)^2 - (h-c) > (3c-6) - (c-2) = 2c-4$. Then $h(h-c-2) +$

+ $h-c(h-c)+c \geq 2c-4$, which gives the result.

Theorem 5: Let G be a finite non-abelian p -group of class c . If $|G| \geq p^{g(h)}$ then $|A(G)|_p \geq p^h$, where $g(h) = \frac{1}{2} h(h-c)$ for any integer h with $h \geq c + \sqrt{3c-6}$.

Proof: G is a pN -group: As in Theorem 4 we assume $c \geq 3$, $3 \leq d \leq h-2$, $k \geq \frac{1}{2} h(h-c)-(h-2) = \frac{1}{2} h(h-c-2)+2$. Also if $c = 3$ we take $h \geq 6$, otherwise the result follows Theorem 4a. Observe that $\frac{1}{2} h(h-c-s)+2 \geq h-c+1$. In fact for $c \geq 4$ this follows from Lemma 5(i). For $c = 3$, $\frac{1}{2} h(h-c-2)+2 = \frac{1}{2} h(h-5)+2 \geq h-2$ since $h \geq 6$. Hence $k \geq h-c+1$. Let $\frac{1}{2} (h-c-2) \geq s \geq 1$. Then $k-sd \geq \frac{1}{2} (h-c-2)(h-d)+2 \geq h-d$, so that by Lemma 1, $|A| \geq p^{h-d}$. Therefore $|A(G)|_p \geq |A| \cdot |I(G)| \geq p^{h-d} \cdot p^d = p^h$. So, take $s \geq \frac{1}{2} (h-c-1)$. For $\exp \frac{G}{G^s} > |Z|$, $\left| \frac{G}{G^s} \right| > |Z|$ and so $|A_c(G)| = \left| \text{Hom} \left(\frac{G}{G^s}, Z \right) \right| \geq |Z| \geq p^{h-c+1}$. Then by Theorem 3, $|A(G)|_p \geq p^{h-c+1} p^{c-1} = p^h$. Next take $\exp \frac{G}{G^s} \leq |Z|$ and apply Theorem 2. For $k_1 < m_1$, $|A_c(G)| \geq p^{k+s} > p^{h-c+1}$ and so $|A(G)|_p \geq p^h$ (Theorem 3). For $k_1 \geq m_1$, $|A_c(G)| \geq p^{B_1}$ (Theorem 2), where $B_1 = m+t(s-1)$. By Theorem 3, it is enough to show that $B_1 \geq h-c+1$. For $m \geq 4$, $B_1 = m+t(s-1) \geq 2+2s \geq h-c+1$, the only cases left are $m=2, m=3$. For $m=2$, $\exp Z \leq p^{c-2}$ (Lemma 2), so that $s(c-2) \geq k$. Then $2s(c-2) \geq h(h-c-2)+4 \geq (c-2)(h-c+1)$, by Lemma 5(i). Hence $B_1 = 2s \geq h-c+1$. Next $m=3$. If $t=2$ then $\exp Z \leq p^{c-1}$ (Lemma 2) and so $s(c-1) \geq k$, which gives $2s(c-1) \geq h(h-c-2)+h \geq$

$\geq (c-1)(h-c)$ by Lemma 5(ii). Then $B_1 \geq 1+2s \geq h-c+1$. If $t=3$ then $\exp Z \leq p^c$ (Lemma 2) so that $2cs \geq h(h-c-2)+4$. From $h-c \geq \sqrt{3c-6}$ and $h \geq 6$ for $c=3$ we get $h-c \geq 3$. For $h-c=3$, $3 \geq \sqrt{3c-6}$ gives $c \leq 5$. Then $2cs \geq h(h-c-2)+4 = h+4 = c+7 > 2c$ forces $s > 1$. For $h-c > 3$ we get $s > 1$ as $s \geq \frac{1}{2}(h-c-1)$. Therefore $B_1 = 3s \geq 2+2s \geq h-c+1$.

$G = H \times K$, where H is abelian of order p^r and K is a pN -group. Then K has class c and $|A(G)|_p \geq p^r \cdot |A(K)|_p$ [9]. Observe that we can replace $g(h)$ and h by $g(h)-r$ and $h-r$ respectively in the first part, and the proof will remain the same. So applying this to K , since $|K| = |G| \cdot p^{-r} \geq p^{g(h)-r}$, $|A(K)|_p \geq p^{h-r}$. Thus $|A(G)|_p \geq p^r \cdot p^{h-r} = p^h$ and the proof is complete.

References

- [1] J.E. Adney and T. Yen "Automorphisms of p -groups" Illinois J. Math. 9(1965), 137-143.
- [2] N. Blackburn "On a special class of p -groups" Acta Math. 100 (1958), 45-95.
- [3] R. Faudree "A note on the automorphism group of a p -group" Proc. Amer. Math. Soc. 19 (1968), 1379 - 1382.
- [4] W. Gaschütz "Nichtabelsche p -gruppen" Journal Algebra 4 (1966), 1-2.
- [5] P. Hall "A contribution to the theory of p -groups" Proc. London Math. Soc. (2) 36 (1933), 29-95.