CENTRAL AUTOMORPHISMS OF A FINITE $p$-GROUP

BY

ALBERT D. OTTO

1. Introduction. In recent years there has been an increased interest in the relationship between the order of a finite group $G$ and the order of the automorphism group $A(G)$ of $G$ [1], [6], [7], [8]. Some of the interest has been focused on the role played by the group $A_c(G)$ of central automorphisms for a finite $p$-group $G$; in particular, when $G$ is a $p$-group of class 2 with no abelian direct factors [2]. The purpose of this paper is (1) to use $A_c(G)$ to show that the order $|G|$ of $G$ divides $|A(G)|$ for certain $p$-groups $G$ and (2) to determine bounds on $|A_c(G)|$ for a $p$-group $G$ with no abelian direct factors.

All groups will be finite groups. $p$ will denote a prime. If $G$ is a group, then $G_2$ denotes the derived group, $I(G)$ denotes the group of inner automorphisms, $Z(G)$ denotes the center (or $Z$, if no ambiguity is possible), and, in addition, $|G|_p$ denotes the highest power of $p$ dividing $|G|$.

2. PN-groups. H. Fitting [5] developed a procedure for determining the number of central automorphisms for a group with a chief series. Throughout the rest of this paper this procedure and the associated notation will be used for the case of a $p$-group. Suppose $G$ is a $p$-group. Decompose $G$ into the direct product of two subgroups $P$ and $B$ where $P$ is abelian and $B$ has no nontrivial abelian direct factors and is nonabelian. For each positive integer $k$, let $a_k$ (resp. $b_k$, resp. $c_k$) denote the number of times the number $p^k$ appears in the invariants of $P$ (resp. $B/B_2$, resp. $Z(B)$), let

$$d_k = a_k^2 + b_k^2 + (a_k + c_k) \cdot \sum_{x \leq k} (a_x + b_x) + (a_k + b_k) \cdot \sum_{x > k} (a_x + c_x),$$

and let

$$\psi(a_k) = 1, \quad a_k = 0,$$

$$= (p^{a_k} - 1)(p^{a_k} - p) \cdots (p^{a_k} - p^{a_k - 1}), \quad a_k \neq 0.$$

Fitting then showed that $|A_c(G)| = \prod_{k=1}^{\infty} p^{kd_k} \cdot \psi(a_k)$. We note that if nonabelian $p$-groups without abelian direct factors are considered, then this equation is greatly simplified. Thus, the following definition for $p$-groups is made.

Received by the editors February 14, 1966.

(1) This research was supported in part by the National Science Foundation under Grant NSF GP-1652.
Definition 1. G is a PN-group if G is a nonabelian p-group and has no nontrivial abelian direct factors.

An immediate consequence which has already been demonstrated [2] is that if G is a PN-group, then AC(G) is a p-group. Since our major objective is to determine when |G| divides |A(G)| for a p-group G, Theorem 1 shows that we may restrict our attention to PN-groups. But first a lemma is needed.

Lemma 1(2). Suppose P is an abelian p-group of order \( p^n \), \( n \neq 2 \). Then \( p^n \) divides \(|A(P)|\) if and only if P is not cyclic.

Proof. Since P is abelian, \( A(P) = \mathcal{A}_c(P) \) and, hence, \( |A(P)|_p = |\mathcal{A}_c(P)|_p \). In the computation of \(|\mathcal{A}_c(P)|_p \) we shall use the prescribed notation. Let \( p^r \) be the exponent of P. Since P is abelian, \( b_k = c_k = 0 \) for all \( k \). Also \( d_k = 0 \) and \( \psi(a_k) = 1 \) for \( k > r \) whereas for \( k \leq r \), \( d_k = a_k^2 + a_k \cdot \sum_{x \geq k} a_x + a_k \cdot \sum_{x > k} a_x = a_k^2 + 2a_k \cdot \sum_{x > k} a_x \).

Thus \(|\mathcal{A}_c(P)|_p = p^n \), where

\[
B = \sum_{k=1}^{r} \left\{ k \left[ a_k^2 + 2a_k \cdot \sum_{x > k} a_x \right] + \frac{1}{2}a_k(a_k - 1) \right\}.
\]

Since it is known [4] that if P is cyclic then \( p^n \) does not divide \(|A(P)|\), we assume P is not cyclic. To show that \( p^n \) divides \(|A(P)|\) it is sufficient to show that \( B \geq n \).

It is necessary to consider two cases.

Case (a). Suppose \( r = 1 \). Then \( a_1 = n \) and \( a_k = 0 \) for all \( k > 1 \). Since P is not cyclic and \( n \neq 2 \), we have \( a_1 = n \leq 3 \). So \( B = \frac{1}{2}a_1(a_1 - 1) \geq a_1 = n \).

Case (b). Suppose \( r > 1 \). Since \( \sum_{x > k} a_x > 0 \) for \( k \) where \( 1 \leq k \leq r - 1 \), we have \( \sum_{k=1}^{r-1} (ka_k \cdot \sum_{x > k} a_x) \geq \sum_{k=1}^{r-1} ka_k \). In addition because \( \sum_{k=1}^{r-1} ka_k \geq (r - 1)a_k^2 \), \( \sum_{k=1}^{r-1} ka_k^2 + \sum_{k=1}^{r-1} (ka_k \cdot \sum_{x \geq k} a_x) \geq (r - 1)a_k^2 + \sum_{k=1}^{r-1} (ka_k \cdot \sum_{x > k} a_x) \). Then since P is not cyclic, either \( a_r > 1 \) or there exists \( k, 1 \leq k \leq r - 1 \), such that \( a_k > 0 \). Thus in either case we have \( (r - 1)a_k^2 + \sum_{k=1}^{r-1} (ka_k \cdot \sum_{x > k} a_x) \geq ra_r \). So

\[
B \geq \sum_{k=1}^{r} ka_k^2 + \sum_{k=1}^{r-1} \left( ka_k \cdot \sum_{x > k} a_x \right) + \sum_{k=1}^{r-1} \left( ka_k \cdot \sum_{x \geq k} a_x \right) + \sum_{k=1}^{r-1} \frac{1}{2}a_k(a_k - 1)
\]

\[
\geq ra_r + \sum_{k=1}^{r-1} ka_k = \sum_{k=1}^{r-1} ka_k = n.
\]

Thus \( B \geq n \).

(2) The author is indebted to the referee for a shorter, more elegant proof of Lemma 1.
Theorem 1. If the $p$-group $G$ is the direct product $P \otimes B$ of the two subgroups $P$ and $B$ where $P$ is abelian of order $p^r$ and $B$ is a PN-group, then $p^r \cdot |A(B)|_p$ divides $|A(G)|$.

Proof. Let $T = A(P) \otimes A(B)$. Then $|T|_p = |A(P)|_p \cdot |A(B)|_p$. At this point we consider three cases.

Case (a). Suppose $P$ is not cyclic and $|P| \neq p^3$. Then by Lemma 1 $p^r$ divides $|A(P)|$. Thus, $p^r \cdot |A(B)|_p$ divides $|T|_p$ which divides $|A(G)|$.

In considering the two remaining cases we look at $[T \cdot A_c(G)]_p$. Since $A(P)$ is a subgroup of $A_c(G)$, $T \cap A_c(G) = A(P) \otimes (A(B) \cap A_c(G)) = A(P) \otimes A_c(B)$. Because $A$ will be either cyclic or of order $p^3$ in the two remaining cases, we assume $|A(P)|_p = p^{r+1}$. So

$$|T \cdot A_c(G)|_p = \frac{|T|_p \cdot |A_c(G)|_p}{|T \cap A_c(G)|_p} = \frac{|A(P)|_p \cdot |A(B)|_p \cdot |A_c(G)|_p}{|A(P)|_p \cdot |A_c(B)|_p} = (p^{r-1} \cdot |A(B)|_p \cdot |A_c(G)|_p/(p^{r-1} \cdot |A_c(B)|_p))$$

Since $|T \cdot A_c(G)|$ divides $|A(G)|$, it is sufficient to prove

$$|A_c(G)|_p > |A_c(B)|_p \cdot p^{r-1} = |A_c(B)| \cdot p^{r-1}.$$ 

Case (b). Suppose $P$ is cyclic of order $p^r$. Using the notation described before, $|A_c(G)| = \prod_{k=1}^{r} p^{kd_k} \cdot \psi(a_k)$ and $|A_c(B)| = \prod_{k=1}^{r} p^{kd'_k}$ where

$$d_k = c_k \cdot \sum_{x \in \mathbb{Z}_p} b_x + b_k \cdot \sum_{x \geq k} c_x.$$ 

Since $P$ is cyclic, $|A_c(G)|_p = \prod_{k=1}^{r} p^{kd_k}$. Because $d_k = d'_k$ for $k > r$ to compare $|A_c(G)|_p$ and $|A_c(B)|$, it is sufficient to compare $\sum_{k=1}^{r} kd_k$ and $\sum_{k=1}^{r} kd'_k$. It is easy to see that

$$\sum_{k=1}^{r} kd_k = \sum_{k=1}^{r-2} kd_k + (r-1)d_{r-1} + rd_r,$$

$$= \sum_{k=1}^{r-2} k(d'_k + c_k + b_k) + (r-1)(d'_{r-1} + c_{r-1} + 1 + b_{r-1})$$

$$+ r\left(d'_r + \sum_{x \geq r} b_x + \sum_{x \geq r} c_x\right)$$

$$= \sum_{k=1}^{r-1} kd'_k + (r-1) + \sum_{k=1}^{r-1} k(c_k + b_k) + r\left(\sum_{x \geq r} b_x + \sum_{x \geq r} c_x\right).$$

Since $c_k \geq 0$ and $b_k \geq 0$ for all $k$ and since some $b_k > 0$,

$$\sum_{k=1}^{r-1} k(c_k + b_k) + r\left(\sum_{x \geq r} b_x + \sum_{x \geq r} c_x\right) > 0.$$ 

Consequently, $\sum_{k=1}^{r-1} kd'_k + (r-1) > \sum_{k=1}^{r-1} kd_k + r - 1$. Thus, $|A_c(G)|_p > |A_c(B)| \cdot p^{r-1}$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Case (c). Suppose $P$ is of order $p^2$. By Case (b) we assume that $P$ is elementary abelian of order $p^2$. Now we have $\psi(a_1) = (p^2 - 1)(p^2 - p)$ and $\psi(a_x) = 1$ for $x \neq 1$. Hence $|A_c(G)|_p = p^{1+d_1} \prod_{k=2}^{x} p^{kd_k}$. Because $d_k = d_k'$ for $k > 1$ to compare $|A_c(G)|_p$ and $|A_c(B)|$, it is sufficient to compare $1+d_1$ and $d_1'$. It is easily checked that $d_1 = d_1' + 2(\sum_{x \geq 1} (b_x + c_x)) > d_1'$. Thus $d_1 + 1 > d_1' + 1$. Hence,

$$|A_c(G)|_p > |A_c(B)|_p \cdot p = |A_c(B)| \cdot p^{r-1}.$$ 

**Corollary 1.1.** Suppose $G$ is a $PN$-group and $P$ is an abelian $p$-group of order $p^r$. If $p^n$ divides $|A(G)|$, then $p^{n+r}$ divides $|A(G \otimes P)|$.

We now use $A_c(G)$ to show that $|G|$ divides $|A(G)|$ for certain $PN$-groups $G$. For this we make the following definition, which was first introduced by Blackburn [3]. Let $n$ and $m$ be positive integers where $n \geq m \geq 3$.

**Definition 2.** $G$ is in $ECF(m, n, p) \triangleq G$ is a $p$-group of order $p^n$ and class $m-1$, $G/G_2$ is elementary abelian, and $|G_i/G_{i+1}| = p$ for $i = 2, 3, \ldots, m-1$; $G_i$ is the $i$th member of the descending central series.

**Theorem 2.** Let $m$ and $n$ be positive integers such that $n \geq m > 3$. If $G$ is a $PN$-group in $ECF(m, n, p)$, then $p^n$ divides $|A(G)|$.

**Proof.** Since $|G_i/G_{i+1}| = p$ for $i = 2, 3, \ldots, m-1$ and $|G| = p^n$, $|G/G_2| = p^{n+2-m}$. Using the notation described before, we have $b_1 = n+2-m$ and $b_x = 0$ for $x \neq 1$. Thus, $d_1 = (n+2-m) \cdot \sum_{x \geq 1} c_x$ and $d_k = 0$ for $k \neq 1$. Hence, $|A_c(G)| = |F|$ where $F = (n+2-m) \cdot \sum_{x \geq 1} c_x$. Since some $c_x > 0$, $F \geq n+2-m$ and, consequently, $|A_c(G)| \leq p^{n+2-m}$. Let $p' = |Z|$ and $p'' = |Z_2/Z|$; $Z_i$ is the $i$th member of the ascending central series of $G$ where $Z_1 = Z$. Since $G/Z_{m-2}$ has order at least $p^2$ and $Z_i/Z_{i-1}$ has order at least $p$ for $i = 1, 2, \ldots, m-2$, we have $1 \leq t \leq (n+2) - (r+m)$. Hence $|Z_2/Z| \leq p^{(n+2) - (r+m)}$. Then

$$|I(G) \cdot A_c(G)| = (|I(G)| \cdot |A_c(G)|)/|I(G) \cap A_c(G)| \geq \frac{(|G| \cdot p^{n+2-m})/|Z_2/Z|}{p^n} \geq \frac{(p^{n-r} \cdot p^{n+2-m})/p^{(n+2) - (r+m)}}{p^n} = p^n.$$ 

Hence, $|G|$ divides $|A(G)|$.

**Corollary 2.1.** If $G$ is a $p$-group of maximal class of order $\geq p^s$, then $|G|$ divides $|A(G)|$.

3. **Bounds on $|A_c(G)|$ for a $PN$-group $G$.** We will now prove two theorems which show the influence of the center and commutator factor group in determining the number of central automorphisms for a $PN$-group. These two theorems will then yield bounds on $|A_c(G)|$ for a $PN$-group $G$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Theorem 3. If $G$ is a PN-group of order $p^n$ where $G/G_2$ has order $p^s$, then $p^A \geq |A_\varepsilon(G)| \geq p^C$ where

$$A = s \cdot \sum_{x \equiv 1} c_x$$

and

$$C = 2 \cdot \sum_{x \equiv 1} c_x,$$  

when $s = 2$,

$$= 2c_1 + \sum_{k=2}^{s-2} (k+1)c_k + s \cdot \sum_{x \equiv s-1} c_x,$$  

when $s > 2$.

Note 1. It should be noted that if there exists a PN-group $H$ of order $p^n$ where $H/H_2$ is elementary abelian of order $p^s$ and $Z(G)$ is isomorphic to $Z(H)$, then $|A_\varepsilon(H)| = p^A$.

Note 2. In addition it should be noted that if there exists a PN-group $K$ of order $p^n$ where $K/K_2$ is of type $(s-1, 1)$ and $Z(G)$ is isomorphic to $Z(K)$, then $|A_\varepsilon(K)| = p^C$.

Proof. We observe first that if $s=2$, then $G/G_2$ is elementary abelian of order $p^2$ and, hence, $|A_\varepsilon(G)| = p^A = p^C$. Thus, we assume $s>2$. To help in the calculation of $|A_\varepsilon(G)|$ the following notation is introduced. Suppose $G/G_2$ is of type $(n(1), n(2), \ldots, n(t))$, where $n(1) \geq n(2) \geq \cdots \geq n(t)$. In addition suppose

$$n(1) = n(2) = \cdots = n(s_1),$$

$$n(s_1+1) = n(s_1+2) = \cdots = n(s_2), \quad \text{where } n(s_1) > n(s_2)$$

$$\vdots$$

$$n(s_{a-1}+1) = n(s_{a-1}+2) = \cdots = n(s_a) = n(t), \quad \text{where } n(s_{a-1}) > n(s_a).$$

For convenience we set $s_0 = 0$. Then $\sum_{i=1}^s n(i) = s$, $\sum_{i=1}^s (s_i - s_{i-1})n(s_i) = s$, and $n(s_1) > n(s_2) > \cdots > n(s_a)$. Extended calculations then show that $|A_\varepsilon(G)| = p^B$ where

$$B = \sum_{i \equiv 0}^{s_a} (ks_a)c_k$$

$$+ \sum_{i=2}^{s_a} \sum_{n(s_i) < k < n(s_i-1)} (ks_{i-1})c_k$$

$$+ \sum_{i=1}^{s_a} \left[ s_i c_{n(s_i)} + (s_i - s_{i-1}) \left( \sum_{x \equiv n(s_i)} c_x \right) \right] n(s_i).$$

Therefore, it remains for us to show that $A \geq B \geq C$. To facilitate this comparison, we let $A(k)$ (resp. $B(k)$, resp. $C(k)$) be the coefficient of the element $c_k$ in the term $A$ (resp. $B$, resp. $C$) for each $k$. Consequently, it is sufficient to show that $A(k) \geq B(k) \geq C(k)$ for each $k$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
We shall first compare \( B(k) \) and \( C(k) \). If \( n(1) = s - 1 \), then \( n(2) = 1 \) and, hence, \( B(k) = C(k) \) for all \( k \). Thus, we assume \( n(1) < s - 1 \). Also since \( G/G_2 \) is not cyclic, \( s_a \geq 2 \). The rest of the proof will be divided into parts.

**Part (1).** Suppose \( 1 \leq k \leq n(s_a) \). Then \( B(k) = ks_a \) and \( C(k) = 1 + k \) since \( k \leq n(s_a) < n(s_1) \leq s - 2 \). Since \( s_a \geq 2 \), \( B(k) \geq C(k) \).

**Part (2).** Suppose \( k = n(s_j) \) where \( 1 \leq j \leq \alpha - 1 \). Then \( C(n(s_j)) = n(s_j) + 1 \) and \( B(n(s_j)) = s_j n(s_j) + \sum_{i=j+1}^{\alpha} n(s_i)(s_i - s_{i-1}) \). Since \( n(s_i) \geq 1 \) and \( s_i - s_{i-1} \geq 1 \) for \( i = j + 1, \ldots, \alpha \) and \( s_j \geq 1 \), \( B(n(s_j)) \geq n(s_j) + 1 = C(n(s_j)) \).

**Part (3).** Suppose \( n(s_j) < k < n(s_{j-1}) \) where \( 2 \leq j \leq \alpha \). Then \( C(k) = k + 1 \) and

\[
B(k) = ks_{j-1} + \sum_{i=j}^{\alpha} (s_i - s_{i-1})n(s_i).
\]

As in Part (2), \( B(k) \geq k + 1 = C(k) \).

**Part (4).** Suppose \( n(s_1) < k \leq s - 2 \). Then \( C(k) = k + 1 \) and

\[
B(k) = \sum_{i=1}^{\alpha} n(s_i)(s_i - s_{i-1}) = s.
\]

But \( k \leq s - 2 \) implies \( k + 1 \leq s - 1 < s \). So \( B(k) \geq C(k) \).

**Part (5).** Suppose \( k > n(s_1) \). Then \( C(k) = \sum_{i=1}^{\alpha} (s_i - s_{i-1})n(s_i) = s \).

**Part (i).** Suppose \( k > n(s_1) \). Then \( B(k) = \sum_{i=1}^{\alpha} (s_i - s_{i-1})n(s_i) = s \).

**Part (ii).** Suppose \( k = n(s_j) \) where \( 1 \leq j \leq \alpha - 1 \). Then

\[
B(n(s_j)) = s_j n(s_j) + \sum_{i=j+1}^{\alpha} n(s_i)(s_i - s_{i-1}) = s.
\]

Since \( n(s_1) > n(s_2) > \cdots > n(s_{j-1}) > n(s_j) \), we have that

\[
s_j n(s_j) + \sum_{i=j+1}^{\alpha} n(s_i)(s_i - s_{i-1}) = \left( \sum_{i=1}^{j} (s_i - s_{i-1}) \right) n(s_j) + \sum_{i=j+1}^{\alpha} n(s_i)(s_i - s_{i-1})
\]

\[
\leq \sum_{i=1}^{j} n(s_i)(s_i - s_{i-1}) + \sum_{i=j+1}^{\alpha} n(s_i)(s_i - s_{i-1})
\]

\[
= \sum_{i=1}^{\alpha} n(s_i)(s_i - s_{i-1}) = s.
\]

Hence, \( s \geq B(k) \).

**Part (iii).** Suppose \( k = n(s_a) \). Then \( B(k) = s_a n(s_a) \). As before we have that \( n(s_a) s_a = n(s_a) \sum_{i=1}^{\alpha} (s_i - s_{i-1}) \leq \sum_{i=1}^{\alpha} n(s_i)(s_i - s_{i-1}) = s \). Hence, \( s \geq B(k) \).

**Part (iv).** Suppose \( 1 \leq k < n(s_a) \). Then \( B(k) = ks_a \). Since \( k < n(s_a) \), \( ks_a \leq n(s_a) s_a \leq s \). So \( s \geq B(k) \).
Part (v). Suppose \( n(s_j) < k < n(s_{j-1}) \) where \( 2 \leq j \leq \alpha \). Then

\[
B(k) = k s_{j-1} + \sum_{i=1}^{\alpha} (s_i - s_{i-1}) n(s_i) \leq n(s_{j-1}) s_{j-1} + \sum_{i=1}^{\alpha} (s_i - s_{i-1}) n(s_i) \leq s.
\]

**Theorem 4.** If \( G \) is a PN-group of order \( p^n \) where \( Z \) has order \( p' \), then

\[
p^A \geq |A_c(G)| \geq p^C
\]

where

\[
A = r \cdot \sum_{x \geq 1} b_x
\]

and

\[
C = \sum_{k=1}^{r-1} k b_k + r \cdot \sum_{x \geq r} b_x.
\]

**Note 3.** It should be observed that if there exists a PN-group \( H \) of order \( p^n \) where \( Z \) is elementary abelian of order \( p' \) and \( G/G_2 \) is isomorphic to \( H/H_2 \), then \( |A_c(H)| = p^A \).

**Note 4.** Also if there exists a PN-group \( K \) of order \( p^n \) where \( Z \) is cyclic of order \( p' \) and \( G/G_2 \) is isomorphic to \( K/K_2 \), then \( |A_c(K)| = p^C \).

**Proof.** The proof of Theorem 4 corresponds very closely to the proof of Theorem 3 and is, consequently, omitted.

From Theorems 3 and 4 we are able to derive bounds on \( |A_c(G)| \).

**Corollary 4.1.** If \( G \) is a PN-group, then \( G \) has at least \( p^2 \) and at most \( p^{n^2} \) central automorphisms where \( p^2 \) is the order of \( G/G_2 \) and \( p' \) is the order of \( Z \).

**Corollary 4.2.** If \( G \) is a nonabelian \( p \)-group, then \( p^2 \) divides \( |A_c(G)| \).

In addition Theorems 3 and 4 lead to some immediate results on when the order of a PN-group will divide the order of its automorphism group. Some of these are as follows.

**Corollary 4.3.** Suppose \( G \) is a PN-group of order \( p^n \). Suppose \( Z \) is elementary abelian of order \( p' \). Then \( |G| \) divides \( |A(G)| \) under any one of the following conditions:

1. \( r \geq n/2 \),
2. \( p' \mid |Z_2/Z| \),
3. If class of \( G = m \geq 3 \), then \( n + 1 - 2r \leq m \).

**Proof.** By direct calculation (see Note 3) we have \( |A_c(G)| = p^A \) where \( A = r \cdot \sum_{x \geq 1} c_x \). Since \( G/G_2 \) is not cyclic, \( \sum_{x \geq 1} c_x \geq 2 \). Thus, \( |A_c(G)| \geq p^{2r} \). Next we observe that \( |A_c(G) \cdot I(G)| \geq p^{n+r}/|Z_2/Z| \). The proofs of these three statements now follow.


