CENTRAL AUTOMORPHISMS OF A FINITE p-GROUP[1]

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

$$d_k = a_{k+1}^2 - a_k^2 + (a_k + c_k)\cdot \sum_{x \geqq k} (a_x + b_x) + (a_k + b_k)\cdot \sum_{x > k} (a_x + c_x),$$

and let

$$\begin{aligned} \psi(a_k) &= 1, \qquad a_k = 0, \\ &= (p^{a_k}-1)(p^{a_k}-p)\cdots(p^{a_k}-p^{a_k-1}), \qquad a_k \neq 0. \end{aligned}$$

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 $\stackrel{d}{=}$ 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 $A_c(G)$ 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, $A(P)=A_c(P)$ and, hence, $|A(P)|_p=|A_c(P)|_p$. In the computation of $|A_c(P)|_p$ 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 $k\leqq r$, $d_k=a_{k+1}^2-a_k^2+a_k\cdot\sum_{x\geqq k} a_x+a_k\cdot\sum_{x>k} a_x=a_{k+1}^2+2a_k\cdot\sum_{x>k} a_x$. Thus $|A_c(P)|_p=p^B$, where

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

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 $B\geqq n$. 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 $a_1=n\geqq 3$. So $B=\frac{1}{2}a_1(a_1-1)\geqq a_1=n$.

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

$$\begin{aligned}B&=\sum_{k=1}^{r} ka_{k+1}^2+\sum_{k=1}^{r}\left(ka_k\cdot\sum_{x>k} a_x\right)+\sum_{k=1}^{r}\left(ka_k\cdot\sum_{x>k} a_x\right)+\sum_{k=1}^{r}\tfrac{1}{2}a_k(a_k-1)\\&\geqq\sum_{k=1}^{r-1} ka_{k+1}^2+\sum_{k=1}^{r-1}\left(ka_k\cdot\sum_{x>k} a_x\right)+\sum_{k=1}^{r-1}\left(ka_k\cdot\sum_{x>k} a_x\right)\\&\geqq ra_r+\sum_{k=1}^{r-1} ka_k=\sum_{k=1}^{r} ka_k=n.\end{aligned}$$

Thus $B\geqq n$.

(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 $|P| \neq p^2$. 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^2 in the two remaining cases, we assume $|A(P)|_p = p^{r-1}$. So

$$\begin{aligned} |T \cdot A_c(G)|_p &= (|T|_p \cdot |A_c(G)|_p)/|T \cap A_c(G)|_p \\ &= (|A(P)|_p \cdot |A(B)|_p \cdot |A_c(G)|_p)/(|A(P)|_p \cdot |A_c(B)|_p) \\ &= (p^{r-1} \cdot |A(B)|_p) \cdot (|A_c(G)|_p/(p^{r-1} \cdot |A_c(B)|_p)). \end{aligned}$$

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, $|A_c(G)| = \prod_{k=1}^{\infty} p^{kd_k} \cdot \psi(a_k)$ and $|A_c(B)| = \prod_{k=1}^{\infty} p^{kd'_k}$ where

$$d'_k = c_k \cdot \sum_{x \geqq k} b_x + b_k \cdot \sum_{x > k} c_x.$$

Since P is cyclic, $|A_c(G)|_p = \prod_{k=1}^{\infty} p^{kd_k}$. 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

$$\begin{aligned} \sum_{k=1}^{r} kd_k &= \sum_{k=1}^{r-2} kd_k + (r-1)d_{r-1} + rd_r \\ &= \sum_{k=1}^{r-2} k(d'_k + c_k + b_k) + (r-1)(d'_{r-1} + c_{r-1} + 1 + b_{r-1}) \\ &\quad + r\Big(d'_r + \sum_{x \geqq r} b_x + \sum_{x \geqq r} c_x\Big) \\ &= \sum_{k=1}^{r} kd'_k + (r-1) + \sum_{k=1}^{r-1} k(c_k + b_k) + r\Big(\sum_{x \geqq r} b_x + \sum_{x \geqq r} c_x\Big). \end{aligned}$$

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

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

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

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 $|A_c(G)|_p=p^{1+d_1}\cdot\prod_{k=2}^{\infty}p^{kd_k}$. 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 $d_1=d'_1+2(\sum_{x\geqq 1}(b_x+c_x))>d'_1$. 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 $n\geqq m\geqq 3$.

DEFINITION 2. G is in $ECF(m, n, p) \overset{d}{=} G$ 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 ith member of the descending central series.

THEOREM 2. *Let m and n be positive integers such that $n\geqq m>3$. 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, $d_1=(n+2-m)\cdot\sum_{x\geqq 1}c_x$ and $d_k=0$ for $k\neq 1$. Hence, $|A_c(G)|=p^F$ where $F=(n+2-m)\cdot\sum_{x\geqq 1}c_x$. Since some $c_k>0$, $F\geqq n+2-m$ and, consequently, $|A_c(G)|\geqq p^{n+2-m}$. Let $p^r=|Z|$ and $p^t=|Z_2/Z|$; Z_i is the ith 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 $1\leqq t\leqq(n+2)-(r+m)$. Hence $|Z_2/Z|\leqq p^{(n+2)-(r+m)}$. Then

$$\begin{aligned}|I(G)\cdot A_c(G)| &= (|I(G)|\cdot|A_c(G)|)/|I(G)\cap A_c(G)|\\ &\geqq (|G/Z|\cdot p^{n+2-m})/|Z_2/Z|\\ &\geqq (p^{n-r}\cdot p^{n+2-m})/p^{(n+2)-(r+m)} = p^n.\end{aligned}$$

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

COROLLARY 2.1. *If G is a p-group of maximal class of order $\geqq p^4$, 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.

THEOREM 3. *If G is a PN-group of order p^n where G/G_2 has order p^s, then $p^A \geqq |A_c(G)| \geqq p^C$ where*

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

and

$$C = 2\cdot \sum_{x\geqq 1} c_x, \qquad \textit{when } s = 2,$$

$$= 2c_1 + \sum_{k=2}^{s-2} (k+1)c_k + s\cdot \sum_{x\geqq s-1} c_x, \qquad \textit{when } s > 2.$$

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 $|A_c(H)| = p^A$.

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 $|A_c(K)| = p^C$.

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

$$\begin{aligned} n(1) &= n(2) = \cdots = n(s_1), \\ n(s_1+1) &= n(s_1+2) = \cdots = n(s_2), \qquad \text{where } n(s_1) > n(s_2) \\ &\vdots \\ n(s_{\alpha-1}+1) &= n(s_{\alpha-1}+2) = \cdots = n(s_\alpha) = n(t), \qquad \text{where } n(s_{\alpha-1}) > n(s_\alpha). \end{aligned}$$

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

$$\begin{aligned} B = &\sum_{1\leqq k\leqq n(s_\alpha)} (ks_\alpha)c_k \\ &+ \sum_{i=2}^{\alpha} \sum_{n(s_i)<k<n(s_{i-1})} (ks_{i-1})c_k \\ &+ \sum_{i=1}^{\alpha} \left[s_i c_{n(s_i)} + (s_i - s_{i-1}) \left(\sum_{x>n(s_i)} c_x \right) \right] n(s_i). \end{aligned}$$

Therefore, it remains for us to show that $A \geqq B \geqq C$. 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 $A(k) \geqq B(k) \geqq C(k)$ for each k.

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, $s_\alpha \geqq 2$. The rest of the proof will be divided into parts.

Part (1). Suppose $1 \leqq k \leqq n(s_\alpha)$. Then $B(k)=ks_\alpha$ and $C(k)=1+k$ since $k \leqq n(s_\alpha)<n(s_1) \leqq s-2$. Since $s_\alpha \geqq 2$, $B(k) \geqq C(k)$.

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

Part (3). Suppose $n(s_j)<k<n(s_{j-1})$ where $2 \leqq j \leqq \alpha$. 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), $B(k) \geqq k+1=C(k)$.

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

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

But $k \leqq s-2$ implies $k+1 \leqq s-1<s$. So $B(k) \geqq C(k)$.

Part (5). Suppose $k>s-2$. Then $C(k)=s$ and $B(k)=\sum_{i=1}^{\alpha} n(s_i)(s_i-s_{i-1})=s$. So $B(k) \geqq C(k)$.

We have now shown that $B \geqq C$. It remains for us to show $A \geqq B$, or equivalently, $A(k) \geqq B(k)$ for each k. We note that $A(k)=s$ for each k. Therefore, we must show that $s \geqq B(k)$ for each k. We will again divide the proof into parts.

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 $1 \leqq j \leqq \alpha-1$. Then

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

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

$$\begin{aligned} s_jn(s_j)+\sum_{i=j+1}^{\alpha} n(s_i)(s_i-s_{i-1}) &= \left(\sum_{i=1}^{j}(s_i-s_{i-1})\right)n(s_j)+\sum_{i=j+1}^{\alpha} n(s_i)(s_i-s_{i-1}) \\ &\leqq \sum_{i=1}^{j} n(s_i)(s_i-s_{i-1})+\sum_{i=j+1}^{\alpha} n(s_i)(s_i-s_{i-1}) \\ &= \sum_{i=1}^{\alpha} n(s_i)(s_i-s_{i-1}) = s. \end{aligned}$$

Hence, $s \geqq B(k)$.

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

Part (iv). Suppose $1 \leqq k<n(s_\alpha)$. Then $B(k)=ks_\alpha$. Since $k<n(s_\alpha)$, $ks_\alpha \leqq n(s_\alpha)s_\alpha \leqq s$. So $s \geqq B(k)$.

Part (v). Suppose $n(s_j)<k<n(s_{j-1})$ where $2\leqq j\leqq \alpha$. Then

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

THEOREM 4. *If G is a PN-group of order p^n where Z has order p^r, then*

$$p^A \geqq |A_c(G)| \geqq p^C$$

where

$$A = r\cdot\sum_{x\geqq 1} b_x$$

and

$$C = \sum_{k=1}^{r-1} kb_k+r\cdot\sum_{x\geqq r} b_x.$$

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^r 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^r 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^{rs} central automorphisms where p^s is the order of G/G_2 and p^r 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^r. Then $|G|$ divides $|A(G)|$ under any one of the following conditions*:

(1) $r\geqq n/2$,

(2) $p^r\geqq |Z_2/Z|$,

(3) *If class of* $G=m\geqq 3$, *then* $n+1-2r\leqq m$.

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

Bibliography

1. J. E. Adney, *On the power of a prime dividing the order of a group of automorphisms*, Proc. Amer. Math. Soc. **8** (1957), 627–633.

2. J. E. Adney and T. Yen, *Automorphisms of a p-group*, Illinois J. Math. **9** (1965), 137–143.

3. N. Blackburn, *On a special class of p-groups*, Acta Math. **100** (1958), 45–92.

4. W. Burnside, *Theory of groups of finite order*, 2nd ed., Dover, New York, 1955.

5. H. Fitting, *Die gruppe der zentralen automorphismen einer gruppe mit hauptreihe*, Math. Ann. **114** (1937), 355–372.

6. 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.

7. R. Ree, *The existence of outer automorphisms of some groups*. II, Proc. Amer. Math. Soc. **9** (1958), 105–109.

8. W. R. Scott, *On the order of the automorphism group of a finite group*, Proc. Amer. Math. Soc. **5** (1954), 23–24.

State University of Iowa,
Iowa City, Iowa
Lehigh University
Bethlehem, Pennsylvania