THE AUTOMORPHISM GROUP OF FINITE p-ABELIAN p-GROUPS

BY

RICHARD M. DAVITT

If n is an integer, a group G is called n-Abelian if $(xy)^n = x^n y^n$ for all elements x, y of G. It is immediate that, for each integer n, the class of n-Abelian groups forms a variety which contains the variety of Abelian groups as a subvariety. F. Levi [8], O. Grün [5] and R. Baer [2], [3] have developed theory pertaining to n-Abelian groups for arbitrary groups. In this paper we restrict our attention to the class of finite p-Abelian p-groups, where p is a prime number. It should be noted that each p-Abelian p-group is trivially a regular p-group and also that each p-group of exponent p is a p-Abelian p-group.

It is well known that if G is a finite non-cyclic Abelian p-group of order greater than p^2, then the order $o(G)$ of G divides the order of the automorphism group $A(G)$ of G [9, Lemma 1]. It is natural to conjecture that if G is a finite non-cyclic p-group of order greater than p^2, then $o(G)$ divides $o(A(G))$. In recent years this result has proved for certain classes of finite p-groups [4], [9], [10]. Corollary 3 shows that it is also true for the class of finite p-Abelian p-groups.

In the paper the following notation is used. G is a finite p-group; $\exp G$ is the exponent of G; $H \leq G$ means H is a subgroup of G and $H < G$ means H is a proper subgroup of G; $H \triangle G$ means H is normal in G; E denotes the identity subgroup of G. If S is a subset of a group, then $\langle S \rangle$ denotes the subgroup generated by S. $C_G(H)$ is the centralizer of H in G and $N_G(H)$ is the normalizer of H in G. The commutator $h^{-1}k^{-1}hk$ of two elements h, k of G is denoted by (h, k). $G^{(1)}$ is the derived group of G, $Z(G)$ is the center of G

$$\mho_k(G) = \langle \{x^{p^k} : x \in G\} \rangle \quad \text{and} \quad \Omega_k(G) = \langle \{x \in G : o(x) \mid p^k\} \rangle.$$

$I(G)$ denotes the group of inner automorphisms of G and I denotes the identity element of $A(G)$. If $\theta \in A(G)$ and $H \leq G$, then $\theta|_H$ denotes the restriction of θ to H. If H and K are groups, then $H \cong K$ means H is isomorphic to K. When there is no ambiguity, the indexing group G will be omitted in the above notation.

DEFINITION 1. $D(G) = \{\theta \in A(G) : \theta|_{\Omega_1(Z)} = I_{\Omega_1(Z)}\}$.

It is immediate that $I(G) \leq D(G) \leq A(G)$. The principal theorem of the paper, Theorem 3, states that if G is a finite non-Abelian p-Abelian p-group, then $o(G) \mid o(D(G) \mid o(A(G))$. We will prove this theorem through a series of remarks, lemmas and theorems. The first two lemmas are computational in nature.

LEMMA 1. *Let* $k \geq 1$. *If* $r = \sum_{j=1}^{p} (p+1)^{jk}$, *then* $p \mid r$.

Received June 2, 1969.

LEMMA 2. *If $p \neq 2$ and $n \geq 0$ then*

$$(p+1)^{p^n} \equiv 1 \bmod p^{n+1} \quad \textit{and} \quad (p+1)^{p^n} \equiv (1+p^{n+1}) \bmod p^{n+2}.$$

Let G be a p-Abelian p-group. Since G is regular,

$$\mho_k = \{x^{p^k} : x \in G\} \quad \text{and} \quad \Omega_k = \{x \in G : o(x) \mid p^k\}.$$

Furthermore, C. Hobby has shown that $G^{(1)} \leq \Omega_1$ and $\mho_1 \leq Z$ [6, Theorem 1]. Consequently, $\exp I(G) \leq p$.

An extremely useful decomposition of p-Abelian p-groups of exponent greater than p, which was suggested by a construction of J. Adney and T. Yen [1, Lemma 1], is found in

LEMMA 3. *Let G be a p-Abelian p-group of exponent greater than p and let $\mho_1 = \langle a^p \rangle \oplus M$, where $o(a) = p^{n+1}$, $n \geq 1$ and $M \leq G$. If*

$$L = \{x \in G : x^p \in M\},$$

then $\Omega_1 \leq L$, $L \triangle G$, $G = \langle a \rangle L$, $\langle a \rangle \cap L = \langle a^{p^n} \rangle \leq \Omega_1(Z)$ and $G/L = \langle aL \rangle$ is cyclic of order p^n.

Proof. Clearly Ω_1 is a subset of L. Since $G^{(1)} \leq \Omega_1$, $L \triangle G$ and $\langle a \rangle L \leq G$. If $g \in G$, then $g^p = a^{kp}m$ where $0 \leq k < p^n$ and $m \in M$. Thus $m = g^p a^{-kp} = (ga^{-k})^p$, $ga^{-k} \in L$ and $G = \langle a \rangle L$. Clearly $\langle a \rangle \cap L = \langle a^{p^n} \rangle \leq \Omega_1(Z)$. Hence $G/L = \langle aL \rangle$ is cyclic of order p^n. $\|$

LEMMA 4. (i) *The mapping $\sigma : G \to G$ defined by $\sigma(a^k l) = a^{k(p+1)}l$, where $0 \leq k < p^n$ and $l \in L$, is an automorphism of G of order p^n under which L is left elementwise fixed. Hence $\sigma \in D(G)$.*

(ii) *For any $x \in \Omega_n[Z(L)]$, the mapping $\phi_x : G \to G$ defined by*

$$\phi_x(a^k l) = (ax)^k l,$$

where $0 \leq k < p^n$ and $l \in L$, is an automorphism of G under which L is left elementwise fixed. Hence $\phi_x \in D(G)$.

(iii) *If $S = \{\phi_x : x \in \Omega_n[Z(L)]\}$, then $S \leq D(G) \leq A(G)$ and $S \cong \Omega_n[Z(L)]$.*

Proof. (i) To see that σ is a homomorphism let $g, h \in G$. Then $g = a^{k_1}l_1$, $h = a^{k_2}l_2$, where $0 \leq k_1, k_2 < p^n$ and $l_1, l_2 \in L$. Let

$$a^{k_1}l_1 a^{k_2}l_2 = a^{k_1+k_2}l_3 l_2$$

where $l_3 \in L$ and let $k_1 + k_2 = k_3 + rp^n$ where $0 \leq k_3 < p^n$ and $r \geq 0$. Then

$$\sigma(gh) = \sigma(a^{k_3}a^{rp^n}l_3 l_2) = a^{k_3(p+1)}a^{rp^n}l_3 l_2 = a^{k_3(p+1)}a^{rp^n(p+1)}l_3 l_2 = a^{(k_1+k_2)(p+1)}l_3 l_2$$
$$= a^{k_1(p+1)}l_1 a^{k_2(p+1)}l_2 = \sigma(g)\sigma(h).$$

Clearly σ fixes L elementwise and hence $\sigma(L) = L$. Since $\sigma(a) = a^{p+1}$ and $\langle a^{p+1}, L \rangle = G$, $\sigma \in A(G)$. Indeed, since $\Omega_1(Z) \leq L$, $\sigma \in D(G)$.

To determine the order of σ, it suffices to consider the action of the powers of σ on a alone. A routine induction proof shows that if $r \geq 0$, then

$\sigma^r(a) = a^{(p+1)^r}$. By Lemma 2,

$$\sigma^{p^n}(a) = a^{(p+1)^{p^n}} = a^{1+\alpha p^{n+1}} = a$$

while

$$\sigma^{p^{n-1}}(a) = a^{(p+1)^{p^{n-1}}} = a^{1+p^n+\beta p^{n+1}} = aa^{p^n} \neq a.$$

Therefore $o(\sigma) = p^n$.

(ii) Let $x \in \Omega_n[Z(L)]$. Since $(ax)^{p^n} = a^{p^n}x^{p^n} = a^{p^n}$, ϕ_x is an automorphism of G under which L is elementwise fixed [7, p. 174]. Indeed since $\Omega_1(Z) \leq L$, $\phi_x \in D(G)$.

(iii) Let $x, y \in \Omega_n[Z(L)]$. Since $\phi_x \phi_y(a) = \phi_x(ay) = axy = \phi_{xy}(a)$, $S \leq D(G) \leq A(G)$. Indeed the mapping ρ which sends x into ϕ_x is clearly an isomorphism of $\Omega_n[Z(L)]$ onto S. ||

Corollary 1. *If $x \in \Omega_n[Z(L)]$, then $o(\phi_x) = o(x)$ and*

$$\langle\phi_x\rangle = \{\phi_y : y \in \langle x\rangle\}.$$

Corollary 2. *If $M \leq \Omega_n[Z(L)]$ and $T = \{\phi_x : x \in M\}$, then $T \leq S$ and $M \cong T$.*

Lemma 5. *If $R = \langle\sigma\rangle$, then*

$$\sigma \in N_{A(G)}(S), \qquad RS \leq D(G) \leq A(G),$$

$$R \cap S = \langle\phi_{a^{p^n}}\rangle = \langle\sigma^{p^{n-1}}\rangle, \qquad o(RS) = p^{n-1}o(\Omega_n[Z(L)])$$

and $RS/S = \langle S\sigma\rangle$ is cyclic of order p^{n-1}.

Proof. Let $x \in \Omega_n[Z(L)]$ and $l \in L$. Then

$$\sigma^{-1}\phi_x\sigma(l) = l \quad \text{and} \quad \sigma^{-1}\phi_x\sigma(a) = ax^{p+1}.$$

Hence, $\sigma^{-1}\phi_x\sigma = \phi_{x^{p+1}} \in S$, $\sigma \in N_{A(G)}(S)$ and $RS \leq D(G) \leq A(G)$.

In determining $R \cap S$ it suffices to consider the action of the automorphisms under consideration on a alone. Since $a^{p^n} \in \Omega_1(Z) \cap L$,

$$\phi_{a^{p^n}}$$

is defined. As in the proof of Lemma 4, $\sigma^{p^{n-1}}(a) = aa^{p^n}$. Hence,

$$\langle\sigma^{p^{n-1}}\rangle = \langle\phi_{a^{p^n}}\rangle \leq R \cap S.$$

Conversely, let $\theta \in R \cap S$. Then $\theta(a) = ax$ where $x \in \Omega_n[Z(L)]$ and $\theta(a) = aa^k$ where k is an integer. Hence,

$$x = a^k \in \langle a\rangle \cap L = \langle a^{p^n}\rangle.$$

By Corollary 1,

$$\theta \in \langle\phi_{a^{p^n}}\rangle \quad \text{and} \quad R \cap S = \langle\phi_{a^{p^n}}\rangle.$$

Since $o(R \cap S) = p$, $o(RS) = p^{n-1}o(\Omega_n[Z(L)])$ and $RS/S = \langle S\sigma\rangle$ is cyclic of order p^{n-1} · ||

LEMMA 6. *Let $x \in \Omega_n[Z(L)]$ and let $s, k \geq 1$. Then*

$$(\phi_x \sigma^k)^s = \sigma^{sk}\phi_{x^r} \quad \text{where} \quad r = \textstyle\sum_{j=1}^{s} (p+1)^{jk}.$$

Proof. The proof is by induction on s. Since

$$\sigma^{-k}\phi_x \sigma^k(a) = ax^{(p+1)^k},$$

the lemma is true if $s = 1$. Inductively assume that for $s > 1$,

$$(\phi_x \sigma^k)^{s-1} = \sigma^{(s-1)k}\phi_{x^q}$$

where $q = \sum_{j=1}^{s-1} (p+1)^{jk}$. Then

$$(\phi_x \sigma^k)^s = \phi_x \sigma^k \sigma^{(s-1)k}\phi_{x^q} = \sigma^{sk}\phi_{x^{(p+1)^{sk}}}\phi_{x^q} = \sigma^{sk}\phi_{x^r}$$

where $r = (p+1)^{sk} + q = \sum_{j=1}^{s} (p+1)^{jk}$. $\|$

LEMMA 7. *If $\theta \in \Omega_1(RS)$, then $\theta = \phi_x$ where $x \in \Omega_1[Z(L)]$.*

Proof. Let $\theta \in \Omega_1(RS)$. By Lemma 5, $\theta = \phi_x \sigma^k$ where $0 \leq k < p^{n-1}$ and $\phi_x \in S$. Suppose, by way of contradiction, that $k > 0$. Then by Lemma 6,

$$I = \theta^p = (\phi_x \sigma^k)^p = \sigma^{kp}\phi_{x^r}$$

where $r = \sum_{j=1}^{p} (p+1)^{jk}$. By Lemma 1, $p \mid r$. Let $r = \alpha p$. Since $0 < k < p^{n-1}$ and $o(\sigma) = p^n$, $\sigma^{kp} \neq I$. Thus

$$I \neq \sigma^{kp} = \phi_{x^{(-\alpha p)}} \in R \cap S = \langle \phi_{a^{p^n}} \rangle$$

and by Corollary 1, $x^{-\alpha p} \in \langle a^{p^n} \rangle \leq \langle a^p \rangle$. Since $x \in L$,

$$x^{-\alpha p} \in M \cap \langle a^p \rangle = E \quad \text{and} \quad \sigma^{kp} = \phi_e = I$$

which is a contradiction. Thus $\theta = \phi_x$ where $x \in \Omega_n[Z(L)]$. Finally, by Corollary 1, $x \in \Omega_1[Z(L)]$. $\|$

Let G be a non-Abelian p-Abelian p-group of exponent p^{m+1} where $m \geq 1$. Let $\mho_1$ be Abelian of type $(n_1 \geq \cdots \geq n_t)$. Choose $a_1, \cdots, a_t \in G$ such that $\mho_1 = \oplus_{i=1}^{t} \langle a_i^p \rangle$ and $o(a_i) = p^{n_i+1}$. For each i, let

$$M_i = \oplus_{j \neq i} \langle a_j^p \rangle \quad \text{and} \quad L_i = \{x \in G : x^p \in M_i\}.$$

LEMMA 8. *For each i,*

$$\Omega_1 \leq L_i \triangle G, \quad G = \langle a_i \rangle L_i, \quad \langle a_i \rangle \cap L_i = \langle a_i^{p^{n_i}} \rangle \leq \Omega_1(Z),$$

$G/L_i = \langle a_i L_i \rangle$ is cyclic of order p^{n_i} and $\mho_1(L_i) = M_i$. Furthermore if $j \neq i$, then $a_j \in L_i$.

Proof. Fix i. Since $\mho_1 = \langle a_i^p \rangle \oplus M_i$, the first part of lemma follows from Lemma 3. Also, if $j \neq i$, then $a_j^p \in M_i$ and $a_j \in L_i$. Consequently, $a_j^p \in \mho_1(L_i)$ and $M_i \leq \mho_1(L_i)$. Conversely, if $y \in \mho_1(L_i)$, then $y = x^p$ for some $x \in L_i$. Therefore $y = x^p \in M_i$ and $\mho_1(L_i) = M_i$. $\|$

We note that $\mho_1 \leq Z$ and $\exp \mho_1 = p^m$. Hence either $\exp Z = p^m$ or $\exp Z = p^{m+1}$.

LEMMA 9. *Let* $\exp Z = \exp \mho_1 = p^m$ *and let* $n_i = m$ *for some fixed* i. *Then* $C(L_i) = \langle a_i^p \rangle Z(L_i)$ *is an Abelian normal subgroup of* G *and* $\Omega_{n_i}[C(L_i)] = \langle a_i^p \rangle \Omega_{n_i}[Z(L_i)]$.

Proof. Since $L_i \triangle G$, $C(L_i) \triangle G$. Also since $a_i^p \in Z$,

$$\langle a_i^p \rangle Z(L_i) \leq C(L_i).$$

If $x \in C(L_i)$, then $x = a_i^k l$ where $0 \leq k < p^{n_i}$ and $l \in L_i$. If $p \mid k$, then $a_i^k \in \langle a_i^p \rangle \leq Z$ and it follows immediately that $l \in Z(L_i)$. Suppose, by way of contradiction, that $p \nmid k$. Then $o(x) = p^{n_i+1} = p^{m+1} = \exp G$ and $G = \langle x, L_i \rangle$. Since $x \in C(L_i)$, $x \in Z$ which contradicts the fact that $\exp Z = p^m$. Thus $p \mid k$ and $C(L_i) = \langle a_i^p \rangle Z(L_i)$ is an Abelian normal subgroup of G. Finally, since $a_i^p \in \Omega_{n_i}(Z)$,

$$\Omega_{n_i}[C(L_i)] = \langle a_i^p \rangle \Omega_{n_i}[Z(L_i)]. \qquad \|$$

The following lemma which is merely an implementation of Lemma 4 is included for notational purposes.

LEMMA 10. (i) *For each* i, *the mapping* $\sigma_i : G \to G$ *defined by*

$$\sigma_i(a_i^k l) = a_i^{k(p+1)} l,$$

where $0 \leq k < p^{n_i}$ *and* $l \in L_i$, *is an automorphism of* G *of order* p^{n_i}. *If* $R_i = \langle \sigma_i \rangle$, *then* $R_i \leq D(G) \leq A(G)$.

(ii) *For fixed* i, *let* $x \in \Omega_{n_i}[Z(L_i)]$. *Then the mapping* ${}_i\phi_x : G \to G$ *defined by* ${}_i\phi_x(a_i^k l) = (a_i x)^k l$, *where* $0 \leq k < p^{n_i}$ *and* $l \in L_i$, *is an automorphism of* G. *If*

$$S_i = \{ {}_i\phi_x : x \in \Omega_{n_i}[Z(L_i)] \},$$

then $S_i \leq D(G) \leq A(G)$ *and* $S_i \cong \Omega_{n_i}[Z(L_i)]$.

LEMMA 11. $T = \oplus_{i=1}^t R_i$ *exists and* $\sigma_j \in N_{A(G)}(S_i)$, $1 \leq i, j \leq t$.

Proof. Fix i and let $j \neq i$. If $l_i \in L_i$, then $l_i = a_j^k l_j$ where $0 \leq k < p^{n_j}$ and $l_j \in L_i \cap L_j$. Consequently,

$$\sigma_j^{-1} \sigma_i \sigma_j(l_i) = \sigma_j^{-1} \sigma_i \sigma_j(a_j^k l_j) = a_j^k l_j = l_i.$$

Since $\sigma_j^{-1} \sigma_i \sigma_j(a_i) = a_i^{p+1}$ we see that $\sigma_j \in C_{A(G)}(\sigma_i)$. If

$$\theta \in \langle \sigma_i \rangle \cap \langle \sigma_j : j \neq i \rangle,$$

then $\theta(l) = l$ for each $l \in L_i$ and $\theta(a_i) = a_i$. Since $G = \langle a_i, L_i \rangle$, $\theta = I$ and $T = \oplus_{i=1}^t R_i$ exists.

By Lemma 5, $\sigma_i \in N_{A(G)}(S_i)$ for each i. Fix i and let $j \neq i$. Let $x \in \Omega_{n_i}[Z(L_i)]$ and let $l_i \in L_i$. Then $l_i = a_j^k l_j$ where $0 \leq k < p^{n_j}$ and

$l_j \in L_i \cap L_j$. Consequently,

$$\sigma_j^{-1}\,{}_i\phi_x\,\sigma_j(l_i) = a_j^k\,l_j = l_i.$$

Furthermore,

$$\sigma_j^{-1}\,{}_i\phi_x\,\sigma_j(a_i) = a_i\,\sigma_j^{-1}(x).$$

Since $G/L_j = \langle a_j^{p+1}L_j\rangle$, $x = a_j^{r(p+1)}m_j$ where $0 \leq r < p^{n_j}$ and $m_j \in L_j$. Hence

$$\sigma_j^{-1}(x) = \sigma_j^{-1}(a_j^{r(p+1)}m_j) = a_j^r\,m_j.$$

If $y = a_j^r\,m_j$, then $y \in \Omega_{n_i}[Z(L_i)]$ and $\sigma_j^{-1}\,{}_i\phi_x\,\sigma_j = {}_i\phi_y \in S_i$. Hence

$$\sigma_j \in N_{A(G)}(S_i). \qquad \|$$

LEMMA 12. *For each i, let $W_i = \{{}_i\phi_x : x \in \Omega_1(Z)\}$. Then*

$$W_i \leq D(G) \leq A(G) \quad \textit{and} \quad W_i \cong \Omega_1(Z).$$

Furthermore, if $j \neq i$, then $W_j \leq C_{A(G)}(W_i)$.

Proof. The first part of the lemma follows by Corollary 2; the last part follows by a routine computation when we observe that $\Omega_1(Z) \leq \Omega_{n_i}[Z(L_i)]$ for each i. $\|$

Techniques due to R. Ree [10, Theorem 1] are used in the proof of the following.

THEOREM 1. *Let G be a non-Abelian p-Abelian p-group of exponent p^{m+1} where $m \geq 1$. If $\exp Z = \exp \mho_1 = p^m$, then $o(G)\,|\,o(D(G))\,|\,o(A(G))$.*

Proof. Let $\mho_1$ be Abelian of type $(n_1 \geq \cdots \geq n_t)$. Let

$$\mho_1 = \oplus_{i=1}^{t}\langle a_i^p\rangle \quad \text{where} \quad o(a_i) = p^{n_i+1}.$$

The theorem is proved by considering two cases.

Case I. $\exp Z(L_1) \leq \exp Z = p^{n_1}$. By Lemmas 5 and 9,

$$R_1 S_1 \leq D(G) \leq A(G)$$

and

$$o(R_1 S_1) = p^{n_1-1}o(\Omega_{n_i}[Z(L_1)]) = p^{n_1-1}o[Z(L_1)] = o(C(L_1)).$$

Furthermore, the mapping $\rho : C(L_1) \to C(L_1)$ defined by $\rho(x) = (a_1, x)$ is an endomorphism of $C(L_1)$ since $C(L_1)$ is a normal Abelian subgroup of G. Let $K = \operatorname{Ker} \rho$ and $M = \operatorname{Im} \rho$. Then $o(C(L_1)) = o(K)o(M)$. We note that $o(Z)\,|\,o(K)$ since $Z \leq K \leq C(L_1)$. Since $M \leq G^{(1)} \leq \Omega_1 \leq L_1$ and $M \leq C(L_1)$, $M \leq \Omega_1[Z(L_1)]$. Let $T = \{{}_1\phi_y : y \in M\}$. By Corollary 2, $T \leq S_1$ and $T \cong M$.

We shall show that $R_1 S_1 \cap I(G) = T$. Let $\theta \in R_1 S_1 \cap I(G)$. Since $\theta \in I(G)$, $o(\theta) \leq p$ and $\theta \in \Omega_1(R_1 S_1)$. By Lemma 7, $\theta = {}_1\phi_x$ where $x \in \Omega_1[Z(L_1)]$. Let $g \in G$ be such that $\theta = I_g$. If $l \in L_1$, then $\theta(l) = {}_1\phi_x(l) = l = g^{-1}lg$. Hence

$g \in C(L_1)$ and $\rho(g)$ is defined. Also ${}_1\phi_x(a_1) = a_1 x = g^{-1} a_1 g$. Hence $x = (a_1, g) = \rho(g) \in M$ and ${}_1\phi_x \in T$. Conversely, let ${}_1\phi_x \in T$. Then

$$x \in M = \operatorname{Im} \rho.$$

Choose $g \in G$ such that $\rho(g) = (a_1, g) = x$. It follows that

$${}_1\phi_x = I_g \in I(G) \cap R_1 S_1 \quad \text{and} \quad T = R_1 S_1 \cap I(G). \qquad \|$$

Now

$$V = R_1 S_1 I(G) \leq D(G) \leq A(G)$$

and

$$o(V) = o(C(L_1))o(G/Z)/o(M) = o(K)o(G/Z).$$

Since $o(Z) \mid o(K)$, we see that $o(G) \mid o(V) \mid o(D(G)) \mid o(A(G))$.

Case II. $\exp Z(L_1) = \exp G = p^{n_1+1}$. In this case $n_1 = n_2 = m$ and without loss of generality we may assume that $a_2 \in Z(L_1)$. By Lemmas 5 and 9, $R_2 S_2 \leq D(G) \leq A(G)$ and

$$o(R_2 S_2) = p^{n_2-1} o(\Omega_{n_2}[Z(L_2)]) = o(\Omega_{n_2}[C(L_2)].$$

Since $Z \leq \Omega_{n_2}[C(L_2)]$, $o(Z) \mid o(\Omega_{n_2}[C(L_2)])$. Furthermore, the mapping $\rho : C(L_2) \to C(L_2)$ defined by $\rho(x) = (a_2, x)$ is an endomorphism of $C(L_2)$. If $M = \operatorname{Im} \rho$, then $M \leq \Omega_{n_2}[Z(L_2)]$. Let $T = \{{}_2\phi_y : y \in M\}$. By Corollary 2, $T \leq S_2$ and $T \cong M$. As in case I, $T = R_2 S_2 \cap I(G)$.

Let $V = R_2 S_2 I(G) \leq D(G) \leq A(G)$. Then

$$o(V) = o(\Omega_{n_2}[C(L_2)])o(G/Z)/o(M).$$

If $(a_2, x) = e$ for each $x \in C(L_2)$, then $M = E$ and

$$o(V) = o(\Omega_{n_2}[C(L_2)])o(G/Z).$$

Since $o(Z) \mid o(\Omega_{n_2}[C(L_2)])$, $o(G) \mid o(V) \mid o(D(G)) \mid o(A(G))$ and the theorem is true. Hence we may assume that $(a_2, b_1) = y \neq e$ for some $b_1 \in C(L_2)$. Let $b_1 = a_1^k l_1$ where $0 \leq k < p^{n_1}$ and $l_1 \in L_1$. Since $a_2 \in Z(L_1) \triangle G$, $(a_2, a_1^k) \in Z(L_1)$. Thus

$$(a_2, b_1) = (a_2, a_1^k l_1) = (a_2, l_1)(a_2, a_1^k) = (a_2, a_1^k)$$

and hence $p \nmid k$. It now follows that $o(b_1) = p^{n_1+1} = \exp G$ and indeed that $\mho_1 = \langle b_1^p \rangle \oplus M_1$. Without loss of generality, let $a_1 = b_1$. We note that $a_1 \in Z(L_2)$, $(a_2, a_1) = y \neq e$ and y is an element of order p in $M = \operatorname{Im} \rho$. Also since $y \in Z(L_1) \cap Z(L_2)$, $y \in Z$. Let $x \in C(L_2)$. Then $x = a_1^r m_1$ where $0 \leq r < p^{n_1}$ and $m_1 \in L_1$. Thus $\rho(x) = (a_1, x) = (a_2, a_1^r m_1) = (a_2, a_1^r) = y^r$ and $M = \langle y \rangle$. Therefore

$$o(M) = o(T) = p \quad \text{and} \quad o(V) = o(\Omega_{n_2}[C(L_2)])o(G/Z)/p.$$

At this point in the proof of Case II it becomes convenient to turn our attention to two subcases.

Case II (A). $m = 1$. Then $\exp G = p^2$, $Z = \Omega_1(Z)$, $C(L_2) = Z(L_2)$, $\Omega_{n_2}[C(L_2)] = \Omega_1[Z(L_2)]$, and $R_2 S_2 = S_2$.

If $Z < \Omega_1[Z(L_2)]$, then $p^l o(Z) = o(\Omega_1[Z(L_2)])$ where $l \geq 1$. But then $o(V) = p^l o(Z) o(G/Z)/p = p^{l-1} o(G)$ and

$$o(G) \mid o(V) \mid o(D(G)) \mid o(A(G)).$$

Thus we may assume that $Z = \Omega_1[Z(L_2)]$ and hence that

$$S_2 = W_2 = \{{}_2\phi_x : x \in \Omega_1(Z)\}.$$

Let $W_1 = \{{}_1\phi_x : x \in \Omega_1(Z)\}$. By Lemma 12,

$$W_1 \leq S_1, \quad o(W_1) = o[\Omega_1(Z)] \quad \text{and} \quad W_1 \leq C_{A(G)}(W_2).$$

Since $\langle a_1^p \rangle \oplus \langle a_2^p \rangle \leq \Omega_1(Z)$, $o(W_1) \geq p^2$. Let $W = VW_1 = W_2 I(G) W_1$. Then $W \leq D(G) \leq A(G)$ and

$$o(W) = o(G) o(W_1)/p[o(W_2 I(G) \cap W_1)].$$

We recall that $(a_2, a_1) = y$. Let $U = \langle {}_1\phi_y \rangle$. Then $U \leq W_1$ and $o(U) = p$. Indeed, it can be shown by methods analogous to those used earlier in the proof that $U = W_2 I(G) \cap W_1$. Thus

$$o(W) = o(G) o(W_1)/p^2$$

and since $o(W_1) \geq p^2$, $o(G) \mid o(W) \mid o(D(G)) \mid o(A(G))$.

Case II (B). $m \geq 2$. Then $\exp G \geq p^3$ and $m = n_1 = n_2 \geq 2$. Since $\sigma_1 \in C_{A(G)}(R_2)$ and $\sigma_1 \in N_{A(G)}(S_2)$,

$$W = R_2 S_2 I(G) R_1 = VR_1 \leq D(G) \leq A(G).$$

Now $\theta(a_1^p) = a_1^p$ for each $\theta \in V$ while $\sigma_1(a_1^p) = a_1^{p^2} a_1^p \neq a_1^p$ since $o(a_1) = p^{n_1+1} \geq p^3$. Hence $\sigma_1 \notin V$, $V < W = VR_1$ and $o(W) = p^l o(V)$ where $l \geq 1$. Therefore

$$o(W) = p^l o(\Omega_{n_2}[C(L_2)]) o(G/Z)/p = p^{l-1} o(\Omega_{n_2}[C(L_2)]) o(G/Z).$$

Since $o(Z) \mid o(\Omega_{n_2}[C(L_2)])$, $o(G) \mid o(W) \mid o(D(G) \mid o(A(G))$. ||

LEMMA 13. *If G is a non-Abelian p-group of exponent p, then*

$$o(G) \mid o(D(G) \mid o(A(G).$$

Proof. R. Ree actually proved this lemma in [10]. In Theorem 1 of that paper he showed that $o(G) \mid o(A(G))$ when G is a non-Abelian p-group of exponent p by constructing a subgroup of $A(G)$, say W, such that $o(G) \mid o(W) \mid o(A(G))$. A closer investigation of that proof reveals that it is indeed true that $W \leq D(G)$ and hence that

$$o(G) \mid o(W) \mid o(D(G)) \mid o(A(G)). \qquad ||$$

LEMMA 14. *Let G be a p-Abelian p-group of exponent p^{m+1} where $m \geq 1$*

and let $\mho_1 = \oplus_{i=1}^{t} \langle a_i^p \rangle$ *where* $o(a_i) = p^{n_i+1}$. *Suppose* $a \in Z$ *for some fixed* j.

(i) *Let* $\theta \in D(L_j)$. *If we extend* θ *to the mapping* $\bar{\theta} : G \rightarrow G$ *defined by* $\bar{\theta}(a^k l) = a^k \theta(l)$, *where* $0 \leq k < p^{n_j}$ *and* $l \in L_j$, *then* $\bar{\theta} \in A(G)$.

(ii) *If* $V_j = \{\bar{\theta} : \bar{\theta}$ *is an extension of* $\theta \in D(L_j)\}$, *then* $V_j \leq D(G) \leq A(G)$ *and* $o(V_j) = o(D(L_j))$.

(iii) $R_j V_j \leq D(G) \leq A(G)$ *and* $o(R_j V_j) = p^{n_j} o(V_j) = p^{n_j} o(D(L_j))$.

Proof. (i) Let $\theta \in D(L_j)$ and let $\bar{\theta}$ be the extension of θ to G. Since $a_j \in Z$, $\theta(a_j^{p^{n_j}}) = a_j^{p^{n_j}}$ and $G = \langle a_j, L_j \rangle$, it is clear that $\bar{\theta} \in A(G)$.

(ii) Since $D(L_j) \leq A(L_j)$, it follows that $V_j \leq A(G)$ and $o(V_j) = o(D(L_j))$. Then since $\Omega_1(Z) \leq \Omega_1[Z(L_j)]$ and since each $\theta \in D(L_j)$ fixes $\Omega_1[Z(L_j)]$ elementwise, each $\bar{\theta} \in V_j$ fixes $\Omega_1(Z)$ elementwise and $V_j \leq D(G) \leq A(G)$.

(iii) Since $\sigma_j \in C_{A(G)}(V_j)$, $R_j V_j \leq D(G) \leq A(G)$. If $\tau \in R_j \cap V_j$, then $\tau(a_j) = a_j$ and $\tau(l) = l$ for each $l \in L_j$. Hence, $\tau = I$ and

$$o(R_j V_j) = o(R_j) o(V_j) = p^{n_j} o(D(L_j)). \qquad \|$$

THEOREM 2. *Let* G *be a non-Abelian* p*-Abelian* p*-group of exponent* p^{m+1} *where* $m \geq 1$. *If* $\exp Z = \exp G = p^{m+1}$, *then*

$$o(G) \mid o(D(G) \mid o(A(G)).$$

Proof. If G is a p-Abelian p-group satisfying the hypothesis of the theorem, then $\mho_1$ is a non-trivial Abelian p-group of type $(n_1 \geq \cdots \geq n_t)$. The proof is by induction on t.

If $t = 1$, then $\mho_1$ is cyclic of order p^{n_1}. Choose $a_1 \in Z$ such that $o(a_1) = p^{n_1+1}$. Then $\mho_1 = \langle a_1^p \rangle \oplus M_1$ where $M_1 = E$. Hence $L_1 = \Omega_1$ and $G/\Omega_1 = \langle a_1 \Omega_1 \rangle$ is cyclic of order p^{n_1}. Since G is not Abelian and $a_1 \in Z$, Ω_1 is a non-Abelian p-group of exponent p. By Lemma 13,

$$o(\Omega_1) \mid o(D(\Omega_1)) \mid o(A(\Omega_1)).$$

If $V_1 = \{\bar{\theta} : \bar{\theta}$ is an extension of $\theta \in D(\Omega_1)\}$ as defined in Lemma 14, then

$$R_1 V_1 \leq D(G) \leq A(G) \quad \text{and} \quad o(R_1 V_1) = p^{n_1} o(D(\Omega_1)).$$

Since $o(G) = p^{n_1} o(\Omega_1)$ and $o(\Omega_1) \mid o(D(\Omega_1))$,

$$o(G) \mid o(R_1 V_1) \mid o(D(G) \mid o(A(G)).$$

Inductively, assume that the theorem is true for $t - 1$ where $t > 1$. Let G be a p-Abelian p-group satisfying the hypothesis of the theorem such that $\mho_1$ is Abelian of type $(n_1 \geq \cdots \geq n_t)$ where $t \geq 2$. Choose $a_1 \in Z$ such that $o(a_1) = p^{n_1+1}$ and choose $a_2, \cdots, a_t \in G$ such that $\mho_1 = \oplus_{i=1}^{t} \langle a_i^p \rangle$ and $o(a_i) = p^{n_i+1}$. Then $G/L_1 = \langle a_1 L_1 \rangle$ is cyclic of order p^{n_1}. Since $a_1 \in Z$, L_1 is a non-Abelian p-Abelian p-group of exponent at least p^2. But $\mho_1(L_1) = M_1 = \oplus_{i=2}^{t} \langle a_i^p \rangle$ has type $(n_2 \geq \cdots \geq n_t)$. Thus there are $t - 1$ elements in a basis for $\mho_1(L_1)$. If $\exp Z(L_1) = \exp \mho_1(L_1)$, then $o(L_1) \mid o(D(L_1))$ by

Theorem 1. If $\exp Z(L_1) = \exp L_1$, then $o(L_1) \mid o(D(L_1))$ by the induction hypothesis. If $V_1 = \{\bar{\theta} : \bar{\theta}$ is an extension of $\theta \in D(L_1)\}$ as defined in Lemma 14, then

$$R_1 V_1 \leq D(G) \leq A(G) \quad \text{and} \quad o(R_1 V_1) = p^{n_1} o(D(L_1)).$$

Since $o(G) = p^{m_1} o(L_1)$ and $o(L_1) \mid o(D(L_1))$,

$$o(G) \mid o(R_1 V_1) \mid o(D(G)) \mid o(A(G)). \qquad \|$$

Lemma 13, Theorem 1 and Theorem 2 may be consolidated into the following.

THEOREM 3. *If G is a non-Abelian p-Abelian p-group, then*

$$o(G) \mid o(D(G)) \mid o(A(G)).$$

COROLLARY 3. *If G is a non-cyclic p-Abelian p-group of order greater than p^2, then $o(G) \mid o(A(G))$.*

BIBLIOGRAPHY

1. J. E. ADNEY AND T. YEN, *Automorphisms of a p-group*, Illinois J. Math., vol. 9 (1965), pp. 137–143.
2. R. BAER, *Endlichkeitskriterien für Kommutatorgruppen*, Math. Ann., vol. 124 (1952), pp. 161–177.
3. ———, *Factorization of n-soluble and n-nilpotent groups*, Proc. Amer. Math. Soc., vol. 4 (1953), pp. 15–26.
4. R. FAUDREE, *A note on the automorphism group os a p-group*, Proc. Amer. Math. Soc., vol. 19 (1968), pp. 1379–1382.
5. O. GRÜN, *Beiträge zur Gruppentheorie*. IV, Math. Nachr., vol. 3 (1949), pp. 77–94.
6. C. HOBBY, *A characteristic subgroup of a p-group*, Pacific J. Math., vol. 10 (1960), pp. 853–858.
7. O. J. HUVAL, A note on the outer automorphisms of finite nilpotent groups, Amer. Math. Monthly, vol. 73 (1966), pp. 174–175.
8. F. LEVI, *Notes on group theory. I, VII*, J. Indian Math. Soc., vol. 8 (1944), pp. 1–7; vol. 9 (1945), pp. 37–42.
9. A. D. OTTO, *Central automorphisms of a finite p-group*, Trans. Amer. Math. Soc., vol. 125 (1966), pp. 280–287.
10. R. REE, *The existence of outer automorphisms of some groups. II*, Proc. Amer. Math. Soc., vol. 9 (1958), pp. 105–109.

LAFAYETTE COLLEGE
EASTON, PENNSYLVANIA