AUTOMORPHISMS OF A p-GROUP[1]

BY

J. E. Adney and Ti Yen

1. Introduction

There have been a number of results on the relationship between the order of a finite group G and the order of its automorphism group $A = A(G)$, for example, see [1], [3], [7], and [10]. It is our purpose in this paper to investigate the relationship between the order of G and the order of A when G is a p-group of class 2, p odd, and G does not have an abelian direct factor (see Theorem 3). Our result is based on a characterization (as a point set) of the group A_c of central automorphisms (Theorem 1) and a construction of non-central automorphisms (Lemma 1). The construction is, perhaps, of some interest in its own right.

It should be pointed out that the main theorem (Theorem 3) is included in a theorem stated in [8]. However that statement depends on a lemma (Lemma 3, [8]) that is invalid [9]. A counterexample to this lemma was announced in [4] and was published in [5].

2. Central automorphisms.

Let G be a finite group, G' its derived group, and Z its center. An automorphism σ of G is called *central* if $x^{-1}x^{\sigma} \in Z$, for every $x \in G$. The set of all central automorphisms of G forms a subgroup A_c of the group A of automorphisms of G. If σ is a central automorphism of G then $f_\sigma : x \rightarrow x^{-1}x^{\sigma}$ is a homomorphism of G into Z. The map $\sigma \rightarrow f_\sigma$ is a one-to-one map of A_c into the group Hom (G, Z) of homomorphisms of G into its center Z. Conversely, if $f \in$ Hom (G, Z) then $\sigma_f : x \rightarrow xf(x)$ defines an endomorphism of G. The endomorphism σ_f is an automorphism if and only if $f(x) \neq x^{-1}$ for every $x \in G$, $x \neq 1$. If G is a direct product with an abelian factor then there exists an $f \in$ Hom (G, Z) such that $f(x) = x^{-1}$ for some $x \in G$, $x \neq 1$. We shall see presently that the converse is also true.

We call a group G *purely non-abelian* if it does not have an abelian direct factor.

Theorem 1. *For a purely non-abelian group G, the correspondence $\sigma \rightarrow f_\sigma$ defined above is a one-to-one map of A_c onto* Hom (G, Z).

Proof. Suppose that there exists a homomorphism $f \in$ Hom (G, Z) such that $f(z) = z^{-1}$ for some $z \in G$, $z \neq 1$. Clearly, $z \in Z$. We can further assume that the order of z, $|z| = p$, is a prime. Write $G/G' = G_p/G' \times G_{p'}/G'$,

Received October 16, 1963.

[1] This work was supported in part by the National Science Foundation.

where G_p/G' is the p-primary component of G/G'. Then $zG' \in G_p/G'$ and $zG' \neq G'$, for G' is contained in the kernel of f. Let the height of zG' in G_p/G' be p^k and let $z = x^{p^k}u$, where $x \in G_p$ and $u \in G'$. Then

$$z^{-1} = f(z) = f(x^{p^k}u) = f(x)^{p^k}.$$

Set $y = f(x)^{-1}$. Then $z = y^{p^k}$, $y \in Z \cap G_p$, and $\{y\} \cap G' = 1$; here $\{X\}$ denotes the subgroup generated by the set X. By [6, Lemma 7, p. 20], yG' generates a direct factor of G_p/G', say $G_p/G' = \{yG'\} \times H_p/G'$. Since $\{y\} \cap G' = 1$, $G = \{y\} \times (H_p\, G_{p'})$ is a direct decomposition of G. Therefore, G has an abelian direct factor if the mapping $\sigma \to f_\sigma$ is not onto.

COROLLARY 1. *A purely non-abelian group G has a non-trivial central automorphism if and only if $(|\,G/G'\,|, |\,Z\,|) \neq 1$, where $|\,X\,|$ denotes the cardinality of the set X.*

COROLLARY 2. *If G is a purely non-abelian p-group then the group A_c of central automorphisms is also a p-group.*

With respect to the existence of non-trivial central automorphisms, we should mention a recent paper of Adney and Deskins [2]. They establish a set of necessary and sufficient conditions in terms of the lattice of subgroups.

3. A construction of non-central automorphism

From now on G will stand for a purely non-abelian p-group of class 2, where p is an odd prime. The numbers p^a, p^b, and p^c stand for the exponents of Z, G', and G/G' respectively.

LEMMA 1. *Suppose*
(i) $G' = \{u\} \times U$, *where* $|\,u\,| = p^b > p^m \geq \exp U$,
(ii) $[g, h] = g^{-1}h^{-1}gh = u$ *and* $h^{p^{b+m}} = 1$.
Let $H = \{g, h\}$ *and* $L = \{x \in G \mid [g, x], [h, x] \in U\}$. *Then* $G = HL$ *and the correspondence*

$$\begin{aligned} g &\to gh^{p^k}, && k \geq m \\ h &\to h, && \\ x &\to x, && \textit{for all } x \in L, \end{aligned}$$

defines an automorphism σ_k which fixes the elements in Z. The index $[\Sigma : \Sigma \cap A_c]$ is p^{b-m}, where Σ is the group generated by the σ_k's.

Proof. For any $x \in G$, we have

$$[g, x] \equiv u^s \pmod{U} \quad \text{and} \quad [h, x] \equiv u^t \pmod{U}.$$

Then

$$[g, h^{-s}g^t x] \equiv 1 \pmod{U} \quad \text{and} \quad [h, h^{-s}g^t x] \equiv 1 \pmod{U}.$$

Hence $h^{-s}g^t x \in L$, $x = (g^{-t}h^s)(h^{-s}g^t x) \in HL$, and $G = HL$.

Since $L \supseteq Z \supseteq G'$ and $|\,gZ\,| = |\,hZ\,| = p^b$, every element $y \in G$ is uniquely expressible as $y = g^s h^t x$, where $0 \leq s, t < p^b$ and $x \in L$. The mapping σ_k

is defined by $y^{\sigma_k} = (gh^{p^k})^s h^t x$. To prove that σ_k is an automorphism fixing Z, we need to show that

$$(hg)^{\sigma_k} = h^{\sigma_k} g^{\sigma_k},$$
$$(xg)^{\sigma_k} = x^{\sigma_k} g^{\sigma_k}, \qquad x \in L,$$

and

$$g^{p^b} = (g^s)^{\sigma_k} (g^{p^b - s})^{\sigma_k}, \qquad 0 \leq s < p^b.$$

We can check these equalities by direct computation, bearing in mind that in a p-group of class 2 the following equalities hold:

$$[x, yz] = [x, y][x, z], \quad \text{and} \quad (xy)^n = x^n y^n [y, x]^{n(n-1)/2}.$$

When p is odd and $p^b = \exp G'$, $(xy)^{p^b} = x^{p^b} y^{p^b}$.

Finally, Σ is cyclic and generated by σ_m. The subgroup $\Sigma \cap A_c$ is generated by σ_b. Hence the index $[\Sigma : \Sigma \cap A_c]$ is p^{b-m}.

THEOREM 2. *A purely non-abelian p-group of class* 2, *p odd, admits an outer automorphism which fixes the elements in the center.*

Proof. Let G be a purely non-abelian p-group of class 2, where p is an odd prime, and let G' and Z be the derived group and center of G respectively. The central automorphisms which fix the elements in Z are in one-to-one correspondence with the elements of Hom $(G/Z, Z)$. Since

$$\exp G/Z = \exp G' \leq \exp Z,$$

Hom $(G/Z, Z)$ contains a subgroup isomorphic with G/Z. If all the central automorphisms that fix the elements in Z are inner, then Hom $(G/Z, Z) \cong G/Z$ and Z is cyclic. In this case, G' is also cyclic. Therefore, we can apply Lemma 1 to produce a non-central outer automorphism which fixes the elements in Z. The hypothesis (i) of Lemma 1 is satisfied. It remains to verify the hypothesis (ii). Let z be a generator of Z. Then $u = z^{p^{a-b}}$ is a generator of G'. Let $[g, h_1] = u$, $g^{p^b} = z^s$, and $h_1^{p^b} = z^t$. We may assume that $t \equiv rs \pmod{p^a}$. Let $h = g^{-r} h_1$. Then $[g, h] = u$ and $h^{p^b} = 1$. This completes the proof.

4. The order of A

THEOREM 3. *The order* $|G|$ *divides* $|A|$ *if* G *is a purely non-abelian p-group of class* 2, *p odd, satisfying one of the following conditions.*

(i) *The center* Z *is cyclic.*

(ii) $a = b$.

(iii) $a \geq c$.

(iv) *The central automorphism group* A_c *is abelian.*

Proof. The proof of all four cases is divided into two steps. First we obtain a lower bound of $|A_c|$ which is $|\text{Hom}(G, Z)|$. Then making use of Lemma 1, we construct enough non-central automorphisms of p-power order to make up the difference.

(i) The center Z is cyclic. We have shown in the proof of Theorem 2 that G satisfies the hypothesis of Lemma 1 with $m = 0$. Therefore, there is a group of non-central automorphisms of order $p^b = |G'|$. Next we show that Hom $(G, Z) \cong G/G'$. Since Z is cyclic of order p^a and G' is the cyclic subgroup of order p^b, $z^{p^{a-b}}$ belongs to G' for every $z \in Z$. It follows that $x^{p^a} = (x^{p^b})^{p^{a-b}}$ belongs to G' for any $x \in G$. Consequently, $\exp G/G' \leq p^a$ and Hom $(G, Z) =$ Hom $(G/G', Z) \cong G/G'$.

(ii) $a = b$. In a cyclic decomposition of G/Z there are two factors $\{gZ\}$ and $\{hZ\}$ of order p^b such that $u = [g, h]$ has order p^b. Then $\{u\}$ is a direct factor of Z: $Z = \{u\} \times Z_1$. Then

Hom $(G/Z, Z)$

$$= \text{Hom } (G/Z, \{u\}) \times \text{Hom } (G/Z, Z_1) \cong G/Z \times \text{Hom } (G/Z, Z_1)$$

and Hom $(G/Z, Z_1)$ contains the subgroup

$$\text{Hom } (\{gZ\}, Z_1) \times \text{Hom } (\{hZ\}, Z_1) \cong Z_1 \times Z_1 .$$

Therefore, Hom (G, Z) contains a subgroup isomorphic with $G/Z \times Z_1 \times Z_1$ whose order is $|G||Z_1|/p^b$. If $|G| > |\text{Hom } (G, Z)|$ then $p^b > |Z_1| = p^m$.

Now we apply Lemma 1 to produce p^{b-m} non-central automorphisms. The hypothesis (i) of Lemma 1 is satisfied for $\{u\}$ is also a direct factor of G'. To establish the hypothesis (ii), let

$$g^{p^b} \equiv u^s \pmod{Z_1} \quad \text{and} \quad h^{p^b} \equiv u^t \pmod{Z_1}.$$

We assume that $t \equiv rs \pmod{p^b}$. Then $(g^{-r}h)^{p^b} \equiv 1 \pmod{Z_1}$. Replacing h by $g^{-r}h$, we have $[g, h] = u$ and $h^{p^{b+m}} = 1$, which is the hypothesis (ii) of Lemma 2.

(iii) $a \geq c$. Let $Z = \prod_{i=1}^{k} \{z_1\} \times Z_1$, where $|z_i| \geq p^c$ and $\exp Z_1 < p^c$. Since $a \geq c$, $k \geq 1$. Then

$$|\text{Hom } (G, Z)| = |G/G'|^k |\text{Hom } (G/G', Z_1)| \geq |G/G'|^k |Z_1|.$$

If $|G| > |\text{Hom } (G, Z)|$ then $|G/G'|^{k-1}|Z_1| < |G'|$ and since $|G/G'| \geq p^{2b}$, $p^{2(k-1)b}|Z_1| < |G'| < p^{kb}|Z_1|$. Thus $2(k - 1) < k$ and so $k = 1$. Now we have $p^m = |Z_1| < |G'| < p^b|Z_1|$ and $Z = \{z_1\} \times Z_1$, where $\exp Z_1 < p^c$. We can improve our estimate of $|\text{Hom } (G/G', Z_1)|$ as follows. Let $G/G' = \{x_1 G'\} \times G_1/G'$ where $|x_1 G'| = p^c$. Then

$$\text{Hom } (G/G', Z_1) \cong Z_1 \times \text{Hom } (G_1/G', Z_1)$$

and

$$|\text{Hom } (G/G', Z_1)| \geq |Z_1| \cdot \min(|G_1/G'|, |Z_1|).$$

Therefore,

$$|\text{Hom } (G, Z)| \geq |G/G'| \cdot |Z_1| \cdot \min(|G_1/G'|, |Z_1|).$$

Since $|G| > |\text{Hom } (G, Z)|$, $|G'| < p^b|Z_1|$ and $\exp G_1/G' \geq p^b$, we must have

$$\min(|G_1/G'|, |Z_1|) = |Z_1|$$

and

$$|\operatorname{Hom}(G, Z)| \geq |G/G'||Z_1|^2 \geq |G|/p^{b-m}.$$

Again we apply Lemma 1 to construct p^{b-m} non-central automorphisms. Choose g, h_1 in G so that $u = [g, h_1]$ has order p^b. Then G' can be decomposed into a direct product $G' = \{u\} \times U$. We have

$$\exp U \leq |U| = |G'|/p^b < p^m.$$

Let $g^{p^b} \equiv z_1^s \pmod{Z_1}$ and $h_1^{p^b} \equiv z_1^t \pmod{Z_1}$. We can assume that $t \equiv rs \pmod{p^a}$. Then, with $h = g^{-r}h_1$, we have $[g, h] = u$ and $h^{p^{b+m}} = 1$.

(iv) A_c is abelian. Let σ, τ be central automorphisms. Then

$$x^{\sigma\tau} = xf_\tau(x)f_\sigma(x)f_\tau(f_\sigma(x)) \quad \text{and} \quad x^{\tau\sigma} = xf_\sigma(x)f_\tau(x)f_\sigma(f_\tau(x)),$$

for any $x \in G$. Hence $\sigma\tau = \tau\sigma$ if and only if $f_\sigma \circ f_\tau = f_\tau \circ f_\sigma$. Thus A_c is abelian if and only if $f_1 \circ f_2 = f_2 \circ f_1$ for any $f_1, f_2 \in \operatorname{Hom}(G, Z)$. It follows that, for any $f \in \operatorname{Hom}(G, Z)$ and $F \in \operatorname{Hom}(G, G')$, $f \circ F = F \circ f = 1$, as G' is contained in the kernel of f. Therefore, $f(G)$ is contained in $F^{-1}(1)$ for any $f \in \operatorname{Hom}(G, Z)$ and $F \in \operatorname{Hom}(G, G')$. The set of all $f(G)$, $f \in \operatorname{Hom}(G, Z)$, generates a subgroup

$$R = \{z \in Z \mid |z| \leq p^d, d = \min(a, c)\}.$$

The intersection of $F^{-1}(1)$ of all $F \in \operatorname{Hom}(G, G')$ is the subgroup

$$K = \{x \in G \mid \text{height } (xG') \geq p^b\}.$$

We have $R \subseteq K$ if A_c is abelian. Conversely, it is always true that $K \subseteq R$. Indeed, since $\exp G/Z = p^b$, $K \subseteq Z$. An element $x \in K$ is of the form $x = y^{p^b}z$, where $z \in G'$. Since $y^{p^c} \in G'$ and $c \geq b$, we have $x^{p^c} = (y^{p^c})^{p^b}z^{p^c} = 1$ and $|x| \leq \min(p^a, p^c) = p^d$. Consequently, $K = R$ if A_c is abelian.

Let $G/G' = \prod_{i=1}^n \{x_i G'\}$ be a direct decomposition of G/G'. Then $R/G' = K/G' = \prod_{i=1}^n \{x_i^{p^b} G'\}$. On account of (ii) and (iii), we assume that $d > b$. Since R is generated by $x_i^{p^b}$, $1 \leq i \leq n$, and G', the $\exp R$ is attained by some $|x_i^{p^b}|$, say $|x_1^{p^b}| = p^d$. We define $f, F_j \in \operatorname{Hom}(G, Z)$, $2 \leq j \leq n$, as follows. Let

$$f(x_1) = x_1^{p^s},$$
$$f(x_i) = 1, \qquad i \geq 2,$$

and

$$F_j(x_i) = 1, \qquad i \neq j,$$
$$F_j(x_j) = x_1^{p^{t(j)}},$$

where

$$s = b + \max(0, d - c_1),$$

$$\text{(1)} \qquad t(j) = b + \max(0, d - c_j), \qquad 2 \leq j \leq n,$$

$$p^{c_i} = |x_i G'|, \qquad 1 \leq i \leq n.$$

Since $F_j \circ f(x_j) = 1$, we have $1 = f \circ F_j(x_j) = x_1^{p^{s+t(j)}}$. Consequently,

$$s + t(j) \geq b + d, \qquad 2 \leq j \leq d. \tag{2}$$

Combining (1) and (2), we get

$$b + \max(0, d - c_1) + \max(0, d - c_j) \geq d, \qquad 2 \leq j \leq n. \tag{3}$$

It follows from $p^d = |x_1^{p^b}|$, $p^{c_1} = |x_1 G'|$, and $p^b = \exp G'$, that $b + c_1 \geq b + d$ and $c_1 \geq d$. Thus $\max(0, d - c_1) = 0$ and $\max(0, d - c_j) = d - c_j > 0$ by (3). Then (3) becomes $b + d - c_j \geq d$ for $2 \leq j \leq n$. Consequently, $b \geq c_j$ for all $j \geq 2$. It follows that R/G' is cyclic generated by $x_1^{p^b} G'$ and $R = \{x_1^{p^b}\} \times R_1$. It is easy to see that $\exp R_1 \leq p^b$.

We have

$$\mathrm{Hom}\,(G, Z) = \mathrm{Hom}\,(G/G', R) = \mathrm{Hom}\,(G/G', \{x_1^{p^b}\}) \times \mathrm{Hom}\,(G/G', R_1).$$

The group $\mathrm{Hom}\,(G/G', R_1)$ contains a subgroup isomorphic with $R_1 \times R_1$ for there are at least two elements $x_i G'$ of order $\geq p^b$. For the group $\mathrm{Hom}\,(G/G', \{x_1^{p^b}\})$, we have

$$\begin{aligned} \mathrm{Hom}\,(G/G', \{x_1^{p^b}\}) &= \textstyle\prod_{i=1}^{n} \mathrm{Hom}\,(\{x_i G'\}, \{x_1^{p^b}\}) \\ &\cong \{x_1^{p^b}\} \times \textstyle\prod_{i=2}^{n} \{x_i G'\}. \end{aligned}$$

Hence $|\mathrm{Hom}\,(G/G', \{x_1^{p^b}\})| = |G/G'|/p^{c-d}$ and $|\mathrm{Hom}\,(G, Z)|$ is divisible by $|G/G'|\,|R_1|^2/p^{c-d}$. Since $\{x_1^{p^b}\} \cap G' = \{x_1^{p^c}\}$ has order p^{d-c+b}, the order of G' is $\leq p^{d-c+b}|R_1|$. Therefore, $|G|\,|R_1|/p^b$ divides $|\mathrm{Hom}\,(G, Z)|$.

If $p^m = |R_1| \geq p^b$ we are done. Suppose $m < b$. Choose g, h_1 in G so that $u = [g, h_1]$ has order p^b. Then $G' = \{u\} \times U$ and

$$|U| = |G'|/p^b \leq p^{d-c+b}|R_1|/p^b \leq p^m.$$

Let $g^{p^b} \equiv z^s \pmod{R_1}$ and $h_1^{p^b} \equiv z^t \pmod{R_1}$, where $z = x_1^{p^b}$. We can assume that $t \equiv rs \pmod{p^d}$. Then, with $h = g^{-r}h_1$, we have $u = [g, h]$ and $h^{p^{b+m}} = 1$. Thus we can apply Lemma 1 to produce p^{b-m} non-central automorphisms.

On the structure of such groups G with abelian A_c we can say the following.

THEOREM 4. *Let G be a purely non-abelian p-group of class 2, p odd, and let $G/G' = \prod_{i=1}^{n} \{x_i G'\}$. Then the group A_c of central automorphisms of G is abelian if and only if*

(i) *$R = K$, and*

(ii) *either $d = b$ or $d > b$ and $R/G' = \{x_1^{p^b} G'\}$,*

where R, K, and d are as defined in Theorem 3.

Proof. The necessity of these conditions is established in the proof of Theorem 3. We suppose that these conditions are satisfied. Since $R = K$, the elements in R are of the form $y^{p^b}z$, where $z \in G'$. If $d = b$ then $f(y^{p^b}z) = 1$ for every $f \in \mathrm{Hom}\,(G, Z)$. Therefore, $f \circ f' = 1$ for any $f, f' \in \mathrm{Hom}\,(G, Z)$.

Suppose that $d > b$ and $R/G' = \{x_1^{p^b} G'\}$. Then $G/G' = \{x_1 G'\} \times G_1/G'$, where $\exp G_1/G' \leq p^b$. Then we have, for any $x \in G_1$ and $f \in \operatorname{Hom}(G_1/G', R)$, $f(x) = x_1^{sp^d} u$, where $u \in G'$. Therefore, $f'(f(x)) = 1$ for any f, $f' \in \operatorname{Hom}(G_1/G', R)$ and $x \in G_1$. Thus the "commutativity" of $\operatorname{Hom}(G, Z) = \operatorname{Hom}(G, R)$ depends on the "commutativity" of $\operatorname{Hom}(\{x_1 G'\}, R)$. The latter is true because R/G' is cyclic.

5. An application

In [1] it was shown that if G was a finite group with abelian Sylow p-subgroup P of order p^n then p^{n-1} divides $| A(G) |$. When G is purely non-abelian we can use our characterization of central automorphisms to simplify his proof and improve the result.

THEOREM 4. *Let G be a purely non-abelian finite group with an abelian Sylow p-subgroup P. Then $| P |$ divides $| A(G) |$.*

Proof. Let G_1 be the kernel of the transfer of G into P and let P_1 be the image. It is known (see e.g. [1, Theorem 2.1]) that $G = G_1 P_1$ and $G_1 \cap P_1 = 1$. Moreover, $P_1 \supseteq P \cap Z$ and $P \cap G_1 = P \cap G'$. Thus $P/P \cap G' \cong P_1$. The group $\operatorname{Hom}(G, Z)$ contains the subgroup

$$\operatorname{Hom}(PG'/G', P \cap Z) \cong \operatorname{Hom}(P/P \cap G', P \cap Z) \cong \operatorname{Hom}(P_1, P \cap Z)$$

whose order is divisible by $| P \cap Z |$. The automorphisms induced by $\operatorname{Hom}(P_1, P \cap Z)$ are distinct from the inner automorphisms induced by P for the latter fix the elements of P. The number of inner automorphisms induced by P is $| P/P \cap Z |$.

REFERENCES

1. J. E. ADNEY, *On the power of a prime dividing the order of a group of automorphisms*, Proc. Amer. Math. Soc., vol. 8 (1957), pp. 627–633.
2. J. E. ADNEY AND W. E. DESKINS, *On automorphisms and subgroups of finite groups, I*, Arch. Math., vol. 13 (1962), pp. 174–178.
3. G. BIRKOFF AND P. HALL, *On the order of groups of automorphisms*, Trans. Amer. Math. Soc., vol. 39 (1936), pp. 489–499.
4. C. GODINO, *The existence of outer automorphisms of certain p-groups*, Notices of Amer. Math. Soc., vol. 8 (August 1961), p. 368.
5. ———, Thesis, University of Notre Dame, 1961.
6. I. KAPLANSKY, *Infinite abelian groups*, Ann Arbor, University of Michigan Press, 1954.
7. W. LEDERMANN AND B. H. NEUMANN, *On the order of the automorphism group of a finite group I*, Proc. Roy. Soc. London Ser. A, vol. 233 (1956), pp. 494–506.
8. E. SCHENKMAN, *Outer automorphisms of some nilpotent groups*, Proc. Amer. Math. Soc., vol. 6 (1955), pp. 6–11.
9. ———, *Errata*, Proc. Amer. Math. Soc., vol. 7 (1956), p. 1160.
10. W. R. SCOTT, *On the order of the automorphism group of a finite group*, Proc. Amer. Math. Soc., vol. 5 (1954), pp. 23–24.

MICHIGAN STATE UNIVERSITY
EAST LANSING, MICHIGAN