THE AUTOMORPHISM GROUP OF A FINITE METACYCLIC p-GROUP

RICHARD M. DAVITT

ABSTRACT. In this paper it is shown that if G is a finite non-Abelian metacyclic p-group, $p \neq 2$, then the order of G divides the order of the automorphism group of G.

It is well known that if G is a finite noncyclic Abelian p-group of order greater than p^2, then the order $|G|$ of G divides the order of the automorphism group $A(G)$ of G. This result has recently been extended to other classes of finite p-groups [1], [6]. We recall that a group G is said to be *metacyclic* if G possesses a cyclic normal subgroup K such that G/K is also cyclic. The purpose of this paper is to show that $|G|$ divides $|A(G)|$ if G is a finite noncyclic metacyclic p-group of order greater than p^2, $p \neq 2$.

The following notation is used: G is a finite p-group where p is a prime; class G denotes the nilpotency class of G; G_n is the nth element in the descending central series of G; $Z(G)$ denotes the center of G (or Z, if no ambiguity is possible); $H \leqq G$ means H is a subgroup of G, $[G:H]$ denotes the index of H in G and $H \lhd G$ means that H is normal in G. If $x, y \in G$, then $|x|$ denotes the order of x, $(x, y) = x^{-1}y^{-1}xy$ and $\langle x, y\rangle$ is the subgroup generated by x and y; more generally, if S is a subset of G, then $\langle S\rangle$ is the subgroup generated by S; $P(G) = \langle x^p : x \in G\rangle$ and $\Omega_m(G) = \langle x \in G : |x| \leqq p^m\rangle$. $I(G)$ denotes the group of inner automorphisms of G; I is the identity subgroup of $A(G)$; if $S \leqq A(G)$, $C(S)$ is the centralizer of S in $A(G)$ and $N(S)$ is the normalizer of S in $A(G)$.

Before proving the main theorem of the paper, we will establish a number of preliminary results.

LEMMA 1. *Let m and n be positive integers. If $p \neq 2$, then*
(i) $(1+p^m)^{p^n} \equiv 1 \bmod p^{n+m}$ *and*
(ii) $(1+p^m)^{p^{n-1}} \equiv (1+p^{n+m-1}) \bmod p^{n+m}$.

PROOF. (i) Since $1+p^m \equiv 1 \bmod p^m$, $(1+p^m)^{p^n} \equiv 1^{p^n} \bmod p^{n+m}$ [4, Lemma 3.2 (iv)].

(ii) Part (ii) is proved by induction on n. The straightforward but

Received by the editors November 24, 1969.

AMS Subject Classifications. Primary 20XX; Secondary 2022, 2025, 2040.

Key Words and Phrases. Finite p-groups, regular, metacyclic, automorphism group.

computational induction proof also uses [4, Lemma 3.2 (iv)], the binomial theorem and the fact that $p\neq 2$. □

LEMMA 2. *Let $K \lhd G$ and let $a\in G$ be such that $G/K=\langle aK\rangle$ is cyclic of order p^n. If $e\neq a^{p^m}\in\Omega_n(Z)$, then the mapping $\theta(a, K, a^{p^m})$ defined by $a^jk\theta(a, K, a^{p^m})=a^{j(p^m+1)}k$, where $0\leqq j<p^n$ and $k\in K$, is an automorphism of G of order $|a|/p^m$ which fixes K elementwise.*

PROOF. Let $\theta(a, K, a^{p^m})=\theta$. If $g, h\in G$, then $g=a^{j_1}k_1$ and $h=a^{j_2}k_2$, where $0\leqq j_1, j_2<p^n$ and $k_1, k_2\in K$. If $k_1a^{j_2}=a^{j_2}k_3$, where $k_3\in K$, then $gh=a^{j_1+j_2}k_3k_2=a^{j_3+rp^n}k_3k_2$, with $j_1+j_2=j_3+rp^n$, $0\leqq j_3<p^n$ and $r=0, 1$. Consequently,

$$\begin{aligned} gh\theta &= a^{j_3(p^m+1)}a^{rp^n}a^{r(p^{m+n})}k_3k_2 \\ &= a^{(j_3+rp^n)(p^m+1)}k_3k_2 \\ &= a^{j_1(p^m+1)}a^{j_2p^m}a^{j_2}k_3k_2. \end{aligned}$$

Since $a^{p^m}\in Z$, we see that

$$gh\theta = a^{j_1(p^m+1)}k_1a^{j_2(p^m+1)}k_2 = g\theta h\theta.$$

Hence θ is an endomorphism of G.

Clearly θ fixes K elementwise and since $a\theta=a^{1+p^m}$, θ is onto and hence an automorphism. Let $|a|=p^s$. Since $a\theta^t=a^{(1+p^m)^t}$ for each positive integer t, we see by Lemma 1 that $a\theta^{p^{s-m}}=a$ while $a\theta^{p^{s-m-1}}\neq a$. Hence $|\theta|=p^{s-m}$. □

The definition of a regular p-group and the basic properties of such groups are well known and may be found in any standard group theory text (see for example [2]); these will be used without reference throughout the rest of the paper. The next preliminary result that we will establish is that metacyclic p-groups, $p\neq 2$, are regular.

LEMMA 3. *Let G be a p-group, $p\neq 2$. If G_2 is cyclic, then G is regular.*

PROOF. If $g,h\in G$, let $H=\langle g, h\rangle$. Then $(gh)^p=g^ph^pcd$ where $c\in P(H_2)$ and $d\in H_p$ [3]. Since H_2 is cyclic and H_p is a proper subgroup of H_2, it follows that $cd=f^p$ where $f\in H_2$. Hence G is regular. □

COROLLARY 1. *If G is a metacyclic p-group, $p\neq 2$, then G is regular.*

Let G be a regular p-group. An extremely useful class of automorphisms of G is constructed in

LEMMA 4. *Let $K\lhd G$ and let $a\in G$ be such that $G/K=\langle aK\rangle$ is cyclic of order p^n. If $x\in\Omega_n(Z(K))$, then the mapping $\phi(a, K, x)$ defined by $a^jk\phi(a, K, x)=(ax)^jk$, where $0\leqq j<p^n$ and $k\in K$, is an automorphism*

of G under which K is elementwise fixed. Furthermore, $|\phi(a, K, x)| = |x|$.

PROOF. Since G is regular and $x \in \Omega_n(Z(K))$, $(ax)^{p^n} = a^{p^n}$. Hence $\phi(a, K, x) = \phi$ is an automorphism of G which leaves K elementwise fixed [5]. Since $a\phi^s = ax^s$, it follows that $|\phi| = |x|$. $\square$

THEOREM. *If $p \neq 2$ and G is a noncyclic metacyclic p-group of order greater than p^2, then $|G|$ divides $|A(G)|$.*

PROOF. We may assume that G is non-Abelian; indeed by R. Faudree's result [1], we may assume that class $G > 2$. Choose $a, b \in G$ such that $H = \langle b \rangle$ and $G/H = \langle aH \rangle$ is cyclic of order k. Let $G_2 = \langle b^l \rangle$ where l is a power of p. We may assume that $(a, b) = b^l$. Furthermore, $|bG_2| = l$ and since class $G > 2$, $|aG_2| = k$. Let $|b^l| = m$. Then $x^m \in Z$ for each $x \in G$ and since $(b^l)^k = (a^k, b) = e$, we see that $m \leqq k$. Furthermore, since class $G > 2$, it is also true that $l < m$. Let $k = rl$ and let $a^k = (b^l)^s$ where $1 < s \leqq m$.

We note that $I(G) = \langle I_a, I_b \rangle$ and hence that $|I(G)| = m^2$. Also if $\sigma \in I(G)$ and $g, h \in G$ are such that $g\sigma = gh$, then $h \in \langle b^l \rangle = G_2$.

To complete the proof we will consider four cases; in each case we will construct a subgroup S of $A(G)$ such that $|S| = klm = |G|$.

Case I. $s \geqq r$.
Let $c = b^{-sl/r}a$. Then $(c, b) = b^l$, $|c| = k$, $G = \langle b, c \rangle$ and $H \cap \langle c \rangle = E$. Let $K = \langle c, b^l \rangle$. Then $K \lhd G$ and $G/K = \langle bK \rangle$ is cyclic of order l. Also $c^{m/l} \in Z(K)$ and $|c^{m/l}| = kl/m \geqq l$. Choose t such that $|c^{mt/l}| = l$ and let $x = c^{mt/l}$. Then $\phi(b, K, x) = \phi \in A(G)$, $|\phi| = l$. Furthermore, $G/H = \langle cH \rangle$ is cyclic of order k and $\theta(c, H, c^m) = \theta \in A(G)$ with order k/m. Since $m > l$, it follows that $\phi \in C(\langle \theta \rangle)$. Hence, if $S = \langle \phi, \theta, I(G) \rangle$, then $|S| = klm$.

Case II. $1 < s < r$, $k/s \leqq m$.
Let $d = a^{-r/s}b$. Then $(a, d) = b^l$, $|d| = ls \geqq m$, $G = \langle a, d \rangle$ and $H \cap \langle d \rangle = E$. Let $L = \langle a, b^l \rangle$. Then $L \lhd G$ and $G/L = \langle bL \rangle = \langle dL \rangle$ is cyclic of order l. Finally, if $M = \langle d, b^l \rangle$, then $M \lhd G$ and $G/M = \langle aM \rangle$ is cyclic of order k/s. We note that $(d^{ms/k}, b^l) = e$ and that $|d^{ms/k}| = kl/m \geqq k/s$. If we choose u such that $|d^{msu/l}| = k/s$ and let $y = d^{msu/l}$, then $\phi(a, M, y) = \phi \in A(G)$ and $|\phi| = k/s$. Furthermore, since $ls \leqq lm$, $\theta(d, L, d^m) = \theta \in A(G)$ with order ls/m. Since $k/s \leqq m$, it follows that $\phi \in C(\langle \theta \rangle)$. Thus if $S = \langle \phi, \theta, I(G) \rangle$, $|S| = klm$.

Case III. $1 < s < r$, $k/s > m$, $ls \leqq k/s$.
Since $k/s > m$, $(d, b^l) = e$. Thus $d \in \Omega_{k/s}(Z(M))$ and $\phi(a, M, d) = \phi \in A(G)$ with order ls. If $R = \langle \phi, I(G) \rangle$, then $|R| = lsm^2$. Furthermore, since $|a| = km/s$, $\theta(a, M, a^m) = \theta \in A(G)$ and $|\theta| = k/s$. Since

$\theta \in N(\langle\phi\rangle)$, if $S=\langle\theta, R\rangle$, then $|S|=|R|\cdot[S:R]$. By Lemma 1, $[S:R]=|a^m M|=k/ms$. Hence $|S|=klm$.

Case IV. $1<s<r$, $k/s>m$, $ls>k/s$.

Choose v such that $ls=kv/s$. Then $d^v \in \Omega_{k/s}(Z(M))$ and $\phi(a, M, d^v)=\phi \in A(G)$ with order k/s. Also $\theta(d, L, d^m)=\theta \in A(G)$, $|\theta|=ls/m$ and $\theta \in N(\langle\phi\rangle)$. Finally, letting $S=\langle\phi, \theta, I(G)\rangle$, we see that $|S|=klm$ and the proof of the theorem is complete. □

References

1. R. Faudree, *A note on the automorphism group of a p-group*, Proc. Amer. Math. Soc. **19** (1968), 1379–1382.

2. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959. MR **21** #1996.

3. P. Hall, *A contribution to the theory of groups of prime-power orders*, Proc. London Math. Soc. (2) **36** (1933), 29–95.

4. J. C. Howarth, *Some automorphisms of finite nilpotent groups*, Proc. Glasgow Math. Assoc. **4** (1960), 204–207. MR **22** #9537.

5. O. J. Huval, *A note on the outer automorphisms of finite nilpotent groups*, Amer. Math. Monthly **73** (1966), 174–175.

6. A. D. Otto, *Central automorphisms of a finite p-group*, Trans. Amer. Math. Soc. **125** (1966), 280–287. MR **34** #4362.

Lafayette College, Easton, Pennsylvania 18042