ON THE AUTOMORPHISM GROUP OF A FINITE MODULAR $p$-GROUP

RICHARD M. DAVITT AND ALBERT D. OTTO

Abstract. In this paper it is shown that if $G$ is a finite non-Abelian modular $p$-group ($p > 2$), then the order of $G$ divides the order of the automorphism group of $G$.

In recent years there have been a number of papers exploring the relationships between the order of a finite $p$-group and the order of its automorphism group. In particular many of these have shown that for a certain class of finite $p$-groups, the order of the group divides the order of the automorphism group ([1], [2], [3], [4], [8]). We recall that a group $G$ is modular if the lattice of subgroups of $G$ is modular. It is the purpose of this paper to show that if $G$ is a non-Abelian modular $p$-group ($p > 2$), then the order of $G$ divides the order of the automorphism group of $G$.

The following notation is used: $G$ is a finite $p$-group where $p$ is an odd prime; $A(G)$ is the group of automorphisms of $G$; $A_n(G)$ and $\text{Inn}(G)$ are the normal subgroups of $A(G)$ of central automorphisms and inner automorphisms, respectively; $G_n$ is the $n$th member of the lower central series of $G$ and so $G_2$ is the derived group; $Z(G)$ and $Z_2(G)$ are the center and second center of $G$, respectively (or $Z$ and $Z_2$ if no ambiguity is possible); $\exp G$ is the exponent of $G$; $|G|$ is the order of the group $G$; for $x$ and $y$ in $G$, $o(x)$ is the order of the element $x$, $(x, y)$ is the commutator $x^{-1}y^{-1}xy$, and $(x)$ is the cyclic subgroup generated by $x$; $\Omega_1(G) = \{x \in G : o(x) \leq p^n\}$; and $\cup_n(G) = \{x^{p^n} : x \in G\}$. In addition, $H \leq G$ means $H$ is a subgroup of $G$ and $\oplus$ is used to denote the direct sum of subgroups. Finally, for groups $A$ and $B$, $\text{Hom}(A, B)$ is the set of all homomorphisms from $A$ into $B$.

There are certain results which we often need and shall use throughout the paper without further reference. Their proofs may be found in [5]. If $a$, $b$, and $c$ are elements of a group $G$, then $(a, bc) = (a, c)(a, b)c$ and $(ab, c) = (a, c)^{(b, c)}$. Also $|\text{Hom}(\bigoplus A_n, \bigoplus B_n)| = \prod_{i,j} |\text{Hom}(A_i, B_j)|$ where $A_i$ and $B_i$ are Abelian $p$-groups. In addition, $\text{Hom}(C(p^n), C(p^m))$ is isomorphic to $C(p^{\min(n,m)})$ where $C(n)$ is the cyclic group of order $n$. Finally,
it is assumed that the definition of a regular $p$-group and the basic properties of such groups are known.

We now state our theorem.

**Theorem.** If $G$ is a finite non-Abelian modular $p$-group ($p > 2$), then $|G|$ divides $|A(G)|$.

We may assume that the nilpotency class of $G$ is greater than 2 [4] and also that $G/Z$ is not metacyclic [3]. Furthermore, we may assume $G$ is purely non-Abelian [8] and consequently $|A(G)| = |\text{Hom}(G, Z)|$ [1] which is then a power of $p$.

For purposes of notation we shall let $R$ be the normal subgroup $\text{Inn}(G)A_0(G)$ of $A(G)$. We note that $R$ is a $p$-group and our goal is to show that $|R| \geq |G|$.

We begin by examining in greater detail the structure of $G$. By [6] and [7] or [9] we know that $G$ contains a normal Abelian subgroup $A$ and an element $b$ such that $G/A = \langle bA \rangle$ and $G_2 = A$ for some fixed nonnegative integer $\alpha$, $\langle a, b \rangle = a^{\alpha}$ for each $a$ in $A$. Since $G/A$ is Abelian, $G_3$ is contained in $A$. Also $\alpha > 0$. For if $\alpha = 0$, $\langle a, b \rangle = a$ for each $a$ in $A$ and so $G_3 = A$ which is a contradiction since $G/A$ is Abelian. Since $\langle a, b \rangle = a^{\alpha}$ for each $a$ in $A$, $G_3 = G_3$. We next note that $\langle a, b \rangle = a^{\alpha}$ for each $a$ in $A$, $G_3 = G_3$. We can now prove the following important and useful lemma.

**Lemma 1.** $G$ is regular.

Suppose $x$ and $y$ are in $G$ and $H = \langle x, y \rangle$. For convenience we may assume $H$ is not Abelian. Then $(xy)^p = x^p y^p c^p d$ where $c$ is in $H_2$ and $d$ is in $H_3$. Since $G$ is modular, $H$ is also modular. Thus we have $H_3 \leq H_3 = \bigcup_{x_1} (H_2) \leq \bigcup_{x} (H_2)$, where $x_1$ is the "$x$" for $H$. Thus $d = d' \in H_3$. Since $G_3 = G_3$ which is Abelian $c^p d = (cd)^p$ with $cd$ in $H_3$. So $(xy)^p = x^p y^p z^p$ with $z$ in $H_3$ and $G$ is regular.

For purposes of notation we let $p^k = |G/A|$ and $p^m = \exp G_2$. Since $G$ is not Abelian, $G_3 = \bigcup_{x} (A) > E$ and so $A = p^{m+2}$. Also since for each $a$ in $A$, $e = (a, b)^p = (a, b^p) = (a^{p^m}, b)$, we see that $a^{p^m}$ and $b^{p^m}$ are in $Z$ and hence that $\bigcup_m (G) \leq Z$. Consequently, $m > \alpha$. For if $m \leq \alpha$, then $G_3 = \bigcup_{x} (A) \leq \bigcup_{x} (G) \leq \bigcup_m (G) \leq Z$, which means $G$ has nilpotency class 2.

We also observe that since for each $a$ in $A$, $(a, b)^p = a^{p^m}$, we have $a^{p^m} = e$ if and only if $a$ is in $Z$. Thus $\bigcup_{x} (A) = A \cap Z$.

In order to find a suitable lower bound on $|R|$, we begin by determining $Z$ and $Z_3$ and consequently their orders.
First of all we recall that $b^{p^n}$ is in $Z$ and thus $\langle b^{p^n} \rangle (A \cap Z) \leq Z$. Conversely suppose $x = b'a$ with $a$ in $A$ is in $Z$. Then $e = (x, b) = (b'a, b) = (a, b)$ is in $\Omega_2(A)$. For $\bar{a}$ in $A$, $e = (b'a, \bar{a}) = (b', \bar{a}) = (\bar{a}, b')$ and so $p^{m_1}$. Thus $Z = \langle b^{p^n} \rangle (A \cap Z) = \langle b^{p^n} \rangle \Omega_2(A)$. We note that, since $o(bA) = p^k$, $o(bA \cap Z) = p^k$. Furthermore $o(bZ) = p^m$. For if $o(bZ) \leq p^{m-1}$, then, by the regularity of $G$, each commutator in $G$ has order $\leq p^{m-1}$ and so $\exp G \leq p^{m-1}$. Thus in addition we have $k \geq m$ and $|Z| = p^{k-m} |\Omega_2(A)|$.

Next we investigate $Z_2$ and find its order. First of all it is easily seen that $Z_2$ can be characterized as the set of all $x$ in $G$ such that $(x, b) \in Z$ and $(x, a) \in Z$ for all $a$ in $A$. For $a$ in $\Omega_2(A)$, $(a, b)^p = a^{p^2}$ is in $\Omega_2(A)$. Thus $\langle b^{p^n} \rangle \Omega_2(A) \leq Z_2$. Also for $a$ in $A$, $(a, b^{p^n-1})$ is in $\langle b^{p^n} \rangle \subseteq Z$. Conversely suppose $x = b'a$ is in $Z_2$ with $a$ in $A$. Then $(x, b) = (b'a, b) = (a, b) = a^{p^2}$ is in $Z \cap A = \Omega_2(A)$ and so $a$ is in $\Omega_2(A)$. So now $b'$ is in $Z_2$ and so for $\bar{a}$ in $A$, $(b', \bar{a})$ is in $A \cap Z = \Omega_2(A)$. Thus $e = (b', \bar{a}) = (b'^p, \bar{a})$. So $b'^p$ is in $Z$ and $p^{m_2} |ip^p|$. Hence $p^{m_2-1}$. So now $Z_2 = (b^{p^n} \cap \Omega_2(A))$. Since $o(bA) = o(b\Omega_2(A)) = p^k$, we have $o(b\Omega_2(A)) = p^k$. Thus $|Z_2| = p^{k-m_2} |\Omega_2(A)|$.

We can now give our first estimate on $|R|$. 

\[ |R| = |\text{Inn}(G)A_2(G)| = |\text{Inn}(G)| |A_2(G)| |Z_2/Z| \]

\[ = (|G|/|Z|) |A_2(G)|(|Z_2/Z|) = p^k |A| |A_2(G)|/ |\Omega_2(A)| \]

\[ = p^{m_2-1} |A_2(G)| (|A|/|\Omega_2(A)|) = p^{m_2-1} |A_2(G)| (|\Omega_2(A)|) \]

We now turn our attention to finding a suitable lower bound for $|A_2(G)|$. To do this we look at $|\text{Hom}(G, Z)|$ which is the same as $|\text{Hom}(G, \Omega_2, Z)|$. For this purpose we shall examine $A$ as well as $G/G_2$ and $Z$.

Since $A = b^{p^{m_2}}$, $A$ may be written in the form $\langle a_1 \rangle \oplus S$ where $o(a_1) = p^{m_2}$ and $S$ is a subgroup. We observe that $\exp S > p^2$. For if not, then $S \leq \Omega_2(A) = A \cap Z \leq Z$ and so $G/Z$ would be metacyclic with generators $a_1Z$ and $bZ$. Consequently $S = (a_2) \oplus T$ where $T$ is a subgroup of order $p^r$, $r \geq 0$, and $o(a_2) = p^{m_2-1}$ with $m_2 > 0$. Hence, $A = \langle a_1 \rangle \oplus (a_2) \oplus T$.

We next turn our attention to $G/G_2$. Let us suppose $G/G_2 = \langle b_1 \rangle \oplus \cdots \oplus \langle b_r \rangle$ where $b_i = b_iG_2$ with $b_i$ in $G$ and $o(b_i) = p^{k_i}$ with $k_1 \geq k_2 \geq \cdots \geq k_r$. First of all we observe that $r \geq 3$. For otherwise $G$ can be generated by the two elements $b$ and $a_1$ and hence would be metacyclic. We now prove a sequence of three lemmas each of which will establish an important relationship to be used in estimating $|A_2(G)|$.

**Lemma 2.** $o(bG_2) = p^{k_1}$ and so $k + x \geq k_1$.

Since $\exp G/G_2 = p^{k_1}$, $o(bG_2) \leq p^{k_1}$. Furthermore, there is $g = b'a$ with
0 ≤ i < p^k and a in A such that o(gG2) = p^{k1}. Because G2 ≤ A, p^k = o(bA) ≤ o(bG2) ≤ p^{k1} and so k1 ≥ k > x. So e ≠ (gG2)^{p^k} = (b^i aG2)^{p^k} = (b^{p^k a^x}) G2 = b^{p^k a^x} G2 = (b^i bG2)^{p^k} since a^xG2 ∈ O(A) = G2. From (b^i G2)^{p^k} = (gG2)^{p^k} ≠ e, we can conclude that o(bG2) ≥ p^{k1} and thus o(bG2) = p^{k1}. Since o(bOmega(A)) = p^k, o(b) ≤ p^{k1}. Now with o(bG2) = p^{k1}, we see that k1 ≥ k + α.

Thus we may now assume without loss of generality that b = b1. Furthermore, we observe that k1 ≥ k.

**Lemma 3.** p^{k1} ≥ exp Z.

For the purpose of notation in this lemma let exp Z = p^l. We recall that Omega(A) ≤ Z and thus l ≥ x. If α = l, then since α < k ≤ k1, we have that k1 ≥ l. Thus we may assume that l > x. We now recall that Z = (b^{p^m}) O(A) and since exp Z > exp O(A), we have that o(b^{p^m}) = p^l and so o(b) = p^{m+l}. Since exp G2 = p^m and o(bG2) = p^{k1}, we have b^{p^{m+k1}} = e. Hence m + k1 ≥ m + l and so k1 ≥ l.

**Lemma 4.** k2 = a.

Let b_2 = b_1 a where b_1 = b, 0 ≤ i < p^k, and a is in A. Then

(b_2 G2)^{p^k} = (b_1 a G2)^{p^k} = (b_1^{p^k} a^x G2) = b_1^{p^k} a^x = (b_1 G2)^{p^k}

since a^{p^k} is in Omega(A) = G2. Because of the direct sum in G/G2, we have (b_2 G2)^{p^k} = e and so a ≥ k_2. Now by way of contradiction suppose k_2 < x. Since b_1, ..., b_n generate G/G2, b_1, b_2, ..., b_n generate G and hence G is the normal closure of {((b_i, b_j), 1 ≤ i < j ≤ n)}. For i ≥ 2, we have o(b_i G2) = p^{ki} ≤ p^{ki} ≤ p^{k1} and thus b_i^{p^k} = 1 is in G2 ≤ A. For i ≥ 2, (b_i^{p^k})^{p^k} = e since exp G2 = p^m. Consequently, for i ≥ 2, (b_i^{p^k})^{p^k} = b_i^{p^k} is in Omega(A) ≤ Z and hence o(b_i G2) ≤ p^{m+i}. So o(b_1, b_2) ≤ p^{m+i} when 1 ≤ i < j ≤ n. This means exp G2 ≤ p^{m+i} since G is regular. This is a contradiction. Thus we now have k_2 = a.

For convenience we now let H = \langle b_3 \rangle ⊕ ... ⊕ \langle b_n \rangle and let |H| = p^s. We note that s > 0 since v ≥ 3. Also we can now calculate |G/G_3| in two ways. Since G/G_2 = \langle b_1 \rangle ⊕ (b_2) ⊕ H, we have

\begin{equation}
|G/G_2| = p^{k1 + p^x + s}.
\end{equation}

Furthermore, |G/G_2| = |G/Omega(A)| = |G/A| |A/Omega(A)| and thus we have

\begin{equation}
|G/G_2| = p^k |Omega(A)|.
\end{equation}

Taking a careful look at A_e(G), we have

|A_e(G)| = |Hom(G/G_2, Z)| = |Hom(b_1, Z)| |Hom(b_2, Z)| |Hom(H, Z)|.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
By Lemma 3, $|\text{Hom}(\langle b_1 \rangle, Z)| = |Z|$. By Lemma 4, $|\text{Hom}(\langle b_2 \rangle, Z)| = |\Omega_2(Z)| \geq |\Omega_2(A)|$. Since exp $Z \geq p^s = p^{s_1} \geq p^{s_2} \geq \cdots \geq p^{s_k}$, we have

$$|\text{Hom}(H, Z)| \geq p^s.$$

Hence we now see that $|A_c(G)| \geq |Z| \cdot |\Omega_2(A)| \geq p^{k-m} \cdot |\Omega_2(A)|^2 \cdot p^s$.

This combined with our earlier calculation of $|R|$ yields

$$|R| \geq p^{m-3} \cdot |\Omega_2(A)| \cdot p^{k-m} \cdot |\Omega_2(A)|^2 \cdot p^s \geq p^{k-s} \cdot |\Omega_2(A)| \cdot |\Omega_2(A)|^2 \geq p^{k-3s} \cdot |\Omega_2(A)|^2.$$

(3) $\geq p^{k-s} \cdot |\Omega_2(A)|^2$.

(4) $\geq p^{k-s} \cdot |\Omega_2(A)|^2$.

First of all let us suppose that $r > \alpha$ where we recall that $a(T) = p^r$. If exp $T \geq p^s$, then $|\Omega_2(A)| \geq p^{k+s} = p^{3s}$. If exp $T < p^s$, then $T \leq \Omega_2(A)$ and so $|\Omega_2(A)| = p^{k+s} |T| = p^{k+s} \geq p^{3s}$. In either case $|\Omega_2(A)| \geq p^{3s}$. Then using (2) we see that $|G|^{G_2} \geq p^{k+3s}$. Consequently, we have $k + \alpha + s \geq k + 3\alpha$ from (1). Then Lemma 2 implies that $k + \alpha + \alpha + s \geq k + 3\alpha$ or that $s \geq \alpha$. Since $|G| = p^k |A|$ we now have $|R| \geq |G|$ by (4). Thus we may assume $r < \alpha$ and hence just as important we now have $T \leq \Omega_2(A)$.

We recall that $A = \langle a_1 \rangle \otimes \langle a_2 \rangle \otimes T$ where $o(a_1) = p^{u+\alpha}$ and $o(a_2) = p^{m_2+\alpha}$ with $m_2 > 0$. Thus $\Omega_2(A) = \langle a_1^{m_1} \rangle \otimes \langle a_2^{m_2} \rangle \otimes T$. Since $o(b\Omega_2(A)) = p^k$, $b \cdot a = (a_1^{m_1}) \cdot (a_2^{m_2}) \cdot a$ where $w_1, w_2 \geq 0$ and $a$ is in $T$. Furthermore $|\Omega_2(A)| = p^{k+3s}$. We now divide the proof into two major cases.

Case (i). $m_2 \geq \alpha$. Then $b^{k+s} = a_1^{w_1} \cdot a_2^{w_2} \cdot a$ since exp $T \leq p^r$. Since $m_2 \geq \alpha$, we have $b^{k+s}$ is in $\Omega_2(A) = G_2$. Thus $k + r \geq k$, because $o(bG_2) = p^k$. Hence, by (1) and (2), $k_1 + \alpha + s = k + 2\alpha + r$ and so $k + r + \alpha + s \geq k + 2\alpha + r$ which means $s \geq \alpha$. Again by (4) we have $|R| \geq |G|$.

Case (ii). $m_2 < \alpha$. To finish this case we consider two possibilities.

Subcase (a). $\alpha - m_2 \leq r$. Let $r = \alpha - m_2 + \beta$ where $\beta \geq 0$. Then $b^{k+s} = a_1^{w_1} \cdot a_2^{w_2} \cdot a$ since $a^{w} = e$. Because $\beta \geq 0$ and $\alpha > m_2$, $b^{k+s}$ is in $\Omega_2(A) = G_2$ and as in Case (i), $k + r \geq k_1$ and again as in Case (i), $|R| \geq |G|$.

Subcase (b). $\alpha - m_2 > r$. Then $b^{k-r} \cdot a = a_1^{w_1} \cdot a_2^{w_2} \cdot a_3^{w_3}$ where $a^{w_3} = e$ since $\alpha - m_2 > r$. Again we have $b^{k+r} \cdot a$ is in $\Omega_2(A) = G_2$ and so $k + \alpha - m_2 \geq k_1$. From (1) and (2) we see that $k_1 + \alpha + s = k + 2\alpha + r$ and thus $k + \alpha - m_2 + \alpha + s \geq k + 2\alpha + r$. So now $s \geq m_2 + r$. Since $m_2 < \alpha$ we have that $\Omega_2(A) = \langle a_1^{w_1} \rangle$ and so $|\Omega_2(A)| = p^{m_2}$ and (3) yields

$$|R| \geq p^{k-3s} \cdot p^{m_2} \cdot (p^{2s+r})^2 \geq p^{k + m + 2s + 3r + s} \geq p^{k + m + 2s + 3r + s}.$$

At the same time

$$|G| = p^k |A| = p^k \cdot p^{m_2} \cdot p^r = p^{k + m + 2s + 3r + s}.$$

Hence $|R| \geq |G|$ and the proof is now complete.
References


Department of Mathematics, University of Louisville, Louisville, Kentucky 40208

Department of Mathematics, Illinois State University, Normal, Illinois 61761