PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 35, Number 2, October 1972

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; $A_c(G)$ and $\mathrm{Inn}(G)$ are the normal subgroups of $A(G)$ of central automorphisms and inner automorphisms, respectively; G_n is the nth 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 $\langle x\rangle$ is the cyclic subgroup generated by x; $\Omega_n(G)=\{x \in G: o(x)\leqq p^n\}$; and $\mho_n(G)=\{x^{p^n}: x \text{ in } G\}$. In addition, $H\leqq G$ means H is a subgroup of G and $\oplus$ is used to denote the direct sum of subgroups. Finally, for groups A and B, $\mathrm{Hom}(A, B)$ 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 $(ab, c)=(a, c)^b(b, c)$. Also $|\mathrm{Hom}(\bigoplus A_i, \bigoplus B_j)|=\prod_{i,j} |\mathrm{Hom}(A_i, B_j)|$ where A_i and B_j are Abelian p-groups. In addition, $\mathrm{Hom}(C(p^\alpha), C(p^\beta))$ is isomorphic to $C(p^{\min(\alpha,\beta)})$ where $C(n)$ is the cyclic group of order n. Finally,

Presented to the Society, January 18, 1972; received by the editors October 11, 1971.

AMS 1970 *subject classifications*. Primary 20D15, 20D45; Secondary 20F55.

Key words and phrases. Finite p-groups, regular, modular, inner automorphisms, central automorphisms.

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 $|A_c(G)|=|\mathrm{Hom}(G,Z)|$ [**1**] which is then a power of p.

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

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 for some fixed nonnegative integer α, $(a, b)=a^{p^\alpha}$ for each a in A. Since G/A is Abelian, G_2 is contained in A. Also $\alpha>0$. For if $\alpha=0$, $(a, b)=a$ for each a in A and so $G_2=A$ which is a contradiction since G/A is cyclic. Since $(a, b)=a^{p^\alpha}$ for each a in A, $\mho_\alpha(A)\leqq G_2$. We next note that $(a, b^i)=a^{(1+p^\alpha)^i-1}$ is in $\mho_\alpha(A)$ for each a in A and integer $i\geqq 0$. Thus by using commutator identities we have that each commutator is of the form a^{p^α} for some a in A. Thus $\mho_\alpha(A)=G_2$. In a similar fashion we see that $\mho_{2\alpha}(A)=G_3$. 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 $(xy)^p=x^py^pc^pd$ where c is in H_2 and d is in H_p. Since G is modular, H is also modular. Thus we have $H_p\leqq H_3=\mho_{\alpha_1}(H_2)\leqq \mho_1(H_2)$, where α_1 is the "α" for H. Thus $\bar{d}=\bar{d}^p$ where $\bar{d}$ is in H_2. Since $H_2\leqq G_2$ which is Abelian $c^pd=(c\bar{d})^p$ with $c\bar{d}$ in H_2. So $(xy)^p=x^py^pz^p$ with z in H_2 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, $G_2=\mho_\alpha(A)>E$ and so $\exp A=p^{m+\alpha}$. Also since for each a in A, $e=(a, b)^{p^m}=(a, b^{p^m})=(a^{p^m}, b)$, we see that a^{p^m} and b^{p^m} are in Z and hence that $\mho_m(G)\leqq Z$. Consequently, $m>\alpha$. For if $m\leqq\alpha$, then $G_2=\mho_\alpha(A)\leqq\mho_\alpha(G)\leqq\mho_m(G)\leqq Z$, which means G has nilpotency class 2. We also observe that since for each a in A, $(a, b)=a^{p^\alpha}$, we have $a^{p^\alpha}=e$ if and only if a is in Z. Thus $\Omega_\alpha(A)=A\cap Z$.

In order to find a suitable lower bound on $|R|$, we begin by determining Z and Z_2 and consequently their orders.

First of all we recall that b^{p^m} is in Z and thus $\langle b^{p^m}\rangle(A\cap Z)\leqq Z$. Conversely suppose $x=b^ia$ with a in A is in Z. Then $e=(x,b)=(b^ia,b)=(a,b)=a^{p^\alpha}$ and so a is in $\Omega_\alpha(A)$. For $\bar{a}$ in A, $e=(b^ia,\bar{a})=(b^i,\bar{a})=(b,\bar{a})^i$ and so $p^m|i$. Thus $Z=\langle b^{p^m}\rangle(A\cap Z)=\langle b^{p^m}\rangle\Omega_\alpha(A)$. We note that, since $o(bA)=p^k$, $o(b(A\cap Z))=p^k$. Furthermore $o(bZ)=p^m$. For if $o(bZ)\leqq p^{m-1}$, then, by the regularity of G, each commutator in G has order $\leqq p^{m-1}$ and so $\exp G_2\leqq p^{m-1}$. Thus in addition we have $k\geqq m$ and $|Z|=p^{k-m}|\Omega_\alpha(A)|$.

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 $\Omega_{2\alpha}(A)$, $(a,b)=a^{p^\alpha}$ is in $\Omega_\alpha(A)\leqq Z$. Thus, $\Omega_{2\alpha}(A)\leqq Z_2$. Also for a in A, $(a,b^{p^{m-\alpha}})$ is in $\langle a^{p^m}\rangle\leqq Z$. Thus $\langle b^{p^{m-\alpha}}\rangle\Omega_{2\alpha}(A)\leqq Z_2$. Conversely suppose $x=b^ia$ is in Z_2 with a in A. Then $(x,b)=(b^ia,b)=(a,b)=a^{p^\alpha}$ is in $Z\cap A=\Omega_\alpha(A)$ and so a is in $\Omega_{2\alpha}(A)$. So now b^i is in Z_2 and so for $\bar{a}$ in A, $(b^i,\bar{a})$ is in $A\cap Z=\Omega_\alpha(A)$. Thus $e=(b^i,\bar{a})^{p^\alpha}=(b^{ip^\alpha},\bar{a})$. So b^{ip^α} is in Z and $p^m|ip^\alpha$. Hence $p^{m-\alpha}|i$. So now $Z_2=\langle b^{p^{m-\alpha}}\rangle\Omega_{2\alpha}(A)$. Since $o(bA)=o(b\Omega_\alpha(A))=p^k$, we have $o(b\Omega_{2\alpha}(A))=p^k$. Thus $|Z_2|=p^{k-m+\alpha}|\Omega_{2\alpha}(A)|$.

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

$$\begin{aligned}|R| &= |\mathrm{Inn}(G)A_c(G)| = |\mathrm{Inn}(G)|\,|A_c(G)|/|Z_2/Z|\\ &= ([|G|/|Z|]\,|A_c(G)|)/(|Z_2|/|Z|) = p^k|A|\,|A_c(G)|/p^{k-m+\alpha}|\Omega_{2\alpha}(A)|\\ &= p^{m-\alpha}|A_c(G)|(|A|/|\Omega_{2\alpha}(A)|) = p^{m-\alpha}|A_c(G)|\,|\mho_{2\alpha}(A)|.\end{aligned}$$

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

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

We next turn our attention to G/G_2. Let us suppose $G/G_2=\langle\bar{b}_1\rangle\oplus\cdots\oplus\langle\bar{b}_v\rangle$ where $\bar{b}_i=b_iG_2$ with b_i in G and $o(\bar{b}_i)=p^{k_i}$ with $k_1\geqq k_2\geqq\cdots\geqq k_v$. First of all we observe that $v\geqq 3$. 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 $|A_c(G)|$.

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

Since $\exp G/G_2=p^{k_1}$, $o(bG_2)\leqq p^{k_1}$. Furthermore, there is $g=b^ia$ with

$0 \leqq i < p^k$ and a in A such that $o(gG_2) = p^{k_1}$. Because $G_2 \leqq A$, $p^k = o(bA) \leqq o(bG_2) \leqq p^{k_1}$ and so $k_1 \geqq k > \alpha$. So $e \neq (gG_2)^{p^\alpha} = (b^i a G_2)^{p^\alpha} = (b^{ip^\alpha} a^{p^\alpha}) G_2 = b^{ip^\alpha} G_2 = (b^i G_2)^{p^\alpha}$ since $a^{p^\alpha} \in \mho_\alpha(A) = G_2$. From $(b^i G_2)^{p^\alpha} = (gG_2)^{p^\alpha} \neq e$, we can conclude that $o(bG_2) \geqq p^{k_1}$ and thus $o(bG_2) = p^{k_1}$. Since $o(b\Omega_\alpha(A)) = p^k$, $o(b) \leqq p^{k+\alpha}$. Now with $o(bG_2) = p^{k_1}$, we see that $k_1 \leqq k + \alpha$.

Thus we may now assume without loss of generality that $b = b_1$. Furthermore we observe that $k_1 \geqq k$.

LEMMA 3. $p^{k_1} \geqq \exp Z$.

For the purpose of notation in this lemma let $\exp Z = p^l$. We recall that $\Omega_\alpha(A) \leqq Z$ and thus $l \geqq \alpha$. If $\alpha = l$, then since $\alpha < k \leqq k_1$, we have that $k_1 \geqq l$. Thus we may assume that $l > \alpha$. We now recall that $Z = \langle b^{p^m} \rangle \Omega_\alpha(A)$ and since $\exp Z > \exp \Omega_\alpha(A)$, we have that $o(b^{p^m}) = p^l$ and so $o(b) = p^{m+l}$. Since $\exp G_2 = p^m$ and $o(bG_2) = p^{k_1}$, we have $b^{p^{m+k_1}} = e$. Hence $m + k_1 \geqq m + l$ and so $k_1 \geqq l$.

LEMMA 4. $k_2 = \alpha$.

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

$$(b_2 G_2)^{p^\alpha} = (b_1^i a G_2)^{p^\alpha} = (b_1^{ip^\alpha} a^{p^\alpha}) G_2 = b_1^{ip^\alpha} G_2 = (b_1 G_2)^{ip^\alpha}$$

since a^{p^α} is in $\mho_\alpha(A) = G_2$. Because of the direct sum in G/G_2, we have $(b_2 G_2)^{p^\alpha} = e$ and so $\alpha \geqq k_2$. Now by way of contradiction suppose $k_2 < \alpha$. Since $\bar{b}_1, \cdots, \bar{b}_v$ generate G/G_2, $b_1, b_2, \cdots, b_v$ generate G and hence G_2 is the normal closure of $\{(b_i, b_j) : 1 \leqq i < j \leqq v\}$. For $i \geqq 2$, we have $o(b_i G_2) = p^{k_i} \leqq p^{k_2} \leqq p^{\alpha-1}$ and thus $b_i^{p^{\alpha-1}}$ is in $G_2 \leqq A$. So when $i \geqq 2$ $(b_i^{p^{\alpha-1}})^{p^m} = e$ since $\exp G_2 = p^m$. Consequently, for $i \geqq 2$, $(b_i^{p^{\alpha-1}})^{p^{m-\alpha}} = b_i^{p^{m-1}}$ is in $\Omega_\alpha(A) \leqq Z$ and hence $o(b_i Z) \leqq p^{m-1}$. So $o(b_i, b_j) \leqq p^{m-1}$ when $1 \leqq i < j \leqq v$. This means $\exp G_2 \leqq p^{m-1}$ since G is regular. This is a contradiction. Thus we now have $k_2 = \alpha$.

For convenience we now let $H = \langle \bar{b}_3 \rangle \oplus \cdots \oplus \langle \bar{b}_v \rangle$ and let $|H| = p^s$. We note that $s > 0$ since $v \geqq 3$. Also we can now calculate $|G/G_2|$ in two ways. Since $G/G_2 = \langle \bar{b}_1 \rangle \oplus \langle \bar{b}_2 \rangle \oplus H$, we have

$$|G/G_2| = p^{k_1+\alpha+s}. \tag{1}$$

Furthermore, $|G/G_2| = |G/\mho_\alpha(A)| = |G/A|\,|A/\mho_\alpha(A)|$ and thus we have

$$|G/G_2| = p^k\,|\Omega_\alpha(A)|. \tag{2}$$

Taking a careful look at $|A_c(G)|$, we have

$$|A_c(G)| = |\mathrm{Hom}(G/G_2, Z)| = |\mathrm{Hom}(\langle \bar{b}_1 \rangle, Z)|\,|\mathrm{Hom}(\langle \bar{b}_2 \rangle, Z)|\,|\mathrm{Hom}(H, Z)|.$$

By Lemma 3, $|\mathrm{Hom}(\langle \bar{b}_1\rangle, Z)|=|Z|$. By Lemma 4, $|\mathrm{Hom}(\langle \bar{b}_2\rangle, Z)|=|\Omega_\alpha(Z)|\geqq|\Omega_\alpha(A)|$. Since $\exp Z\geqq p^\alpha=p^{k_2}\geqq p^{k_3}\geqq\cdots\geqq p^{k_v}$, we have

$$|\mathrm{Hom}(H, Z)| \geqq p^s.$$

Hence we now see that $|A_c(G)|\geqq|Z|\,|\Omega_\alpha(A)|\,p^s\geqq p^{k-m}\,|\Omega_\alpha(A)|^2\,p^s$.

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

$$|R| \geqq p^{m-\alpha}\,|\mho_{2\alpha}(A)|\,p^{k-m}\,|\Omega_\alpha(A)|^2\,p^s$$

$$\geqq p^{k-\alpha+s}\,|\mho_{2\alpha}(A)|\,|\Omega_\alpha(A)|^2 \tag{3}$$

$$\geqq p^{k-\alpha+s}\,|A|. \tag{4}$$

First of all let us suppose that $r\geqq\alpha$ where we recall that $o(T)=p^r$. If $\exp T\geqq p^\alpha$, then $|\Omega_\alpha(A)|\geqq p^{\alpha+\alpha+\alpha}=p^{3\alpha}$. If $\exp T<p^\alpha$, then $T\leqq\Omega_\alpha(A)$ and so $|\Omega_\alpha(A)|=p^{\alpha+\alpha}\,|T|=p^{\alpha+\alpha+r}\geqq p^{3\alpha}$. In either case $|\Omega_\alpha(A)|\geqq p^{3\alpha}$. Then using (2) we see that $|G/G_2|\geqq p^{k+3\alpha}$. Consequently, we have $k_1+\alpha+s\geqq k+3\alpha$ from (1). Then Lemma 2 implies that $k+\alpha+\alpha+s\geqq k+3\alpha$ or that $s\geqq\alpha$. Since $|G|=p^k\,|A|$ we now have $|R|\geqq|G|$ by (4). Thus we may assume $r<\alpha$ and hence just as important we now have $T\leqq\Omega_\alpha(A)$.

We recall that $A=\langle a_1\rangle\oplus\langle a_2\rangle\oplus T$ where $o(a_1)=p^{m+\alpha}$ and $o(a_2)=p^{m_2+\alpha}$ with $m_2>0$. Thus $\Omega_\alpha(A)=\langle a_1^{p^m}\rangle\oplus\langle a_2^{p^{m_2}}\rangle\oplus T$. Since $o(b\Omega_\alpha(A))=p^k$, $b^{p^k}=(a_1^{p^m})^{w_1}(a_2^{p^{m_2}})^{w_2}a$ where w_1, $w_2\geqq 0$ and a is in T. Furthermore $|\Omega_\alpha(A)|=p^{2\alpha+r}$. We now divide the proof into two major cases.

Case (i). $m_2\geqq\alpha$. Then $b^{p^{k+r}}=a_1^{w_1p^{m+r}}a_2^{w_2p^{m_2+r}}$ since $\exp T\leqq p^r$. Since m, $m_2\geqq\alpha$, we have $b^{p^{k+r}}$ is in $\mho_\alpha(A)=G_2$. Thus $k+r\geqq k_1$ because $o(bG_2)=p^{k_1}$. Hence, by (1) and (2), $k_1+\alpha+s=k+2\alpha+r$ and so $k+r+\alpha+s\geqq k+2\alpha+r$ which means $s\geqq\alpha$. Again by (4) we have $|R|\geqq|G|$.

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

Subcase (a). $\alpha-m_2\leqq r$. Let $r=\alpha-m_2+\beta$ where $\beta\geqq 0$. Then $b^{p^{k+r}}=a_1^{w_1p^{m+\alpha-m_2+\beta}}a_2^{w_2p^{\alpha+\beta}}$ since $a^{p^r}=e$. Because $\beta\geqq 0$ and $\alpha>m_2$, $b^{p^{k+r}}$ is in $\mho_\alpha(A)=G_2$ and as in Case (i), $k+r\geqq k_1$ and again as in Case (i), $|R|\geqq|G|$.

Subcase (b). $\alpha-m_2>r$. Then $b^{p^{k+\alpha-m_2}}=a_1^{w_1p^{m+\alpha-m_2}}a_2^{w_2p^\alpha}$ where $a^{p^{\alpha-m_2}}=e$ since $\alpha-m_2>r$. Again we have $b^{p^{k+\alpha-m_2}}$ is in $\mho_\alpha(A)=G_2$ and so $k+\alpha-m_2\geqq k_1$. From (1) and (2) we see that $k_1+\alpha+s=k+2\alpha+r$ and thus $k+\alpha-m_2+\alpha+s\geqq k+2\alpha+r$. So now $s\geqq m_2+r$. Since $m_2<\alpha$ we have that $\mho_{2\alpha}(A)=\langle a_1^{p^{2\alpha}}\rangle$ and so $|\mho_{2\alpha}(A)|=p^{m-\alpha}$. Thus (3) yields

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

At the same time

$$|G| = p^k\,|A| = p^k p^{m+\alpha} p^{m_2+\alpha} p^r = p^{k+m+2\alpha+m_2+r}.$$

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

References

1. J. E. Adney and T. Yen, *Automorphisms of a p-group*, Illinois J. Math. **9** (1965), 137–143. MR **30** #2072.

2. R. M. Davitt, *The automorphism group of finite p-Abelian p-groups*, Illinois J. Math. **16** (1972), 76–85.

3. R. M. Davitt and A. D. Otto, *On the automorphism group of a finite p-group with the central quotient metacyclic*, Proc. Amer. Math. Soc. **30** (1971), 467–472.

4. R. Faudree, *A note on the automorphism group of a p-group*, Proc. Amer. Math. Soc. **19** (1968), 1379–1382. MR **40** #1476.

5. B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin and New York, 1967. MR **37** #302.

6. K. Iwasawa, *Über die endlichen und die Verbände ihrer Untergruppen*, J. Fac. Sci. Imp. Univ. Tokyo Sect. I **4** (1941), 171–199. MR **3**, 193.

7. F. Napolitani, *Sui p-gruppi modulari finiti*, Rend. Sem. Mat. Univ. Padova **39** (1967), 296–303. MR **36** #6509.

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

9. G. Seitz, *On the structure of modular p-groups*, unpublished paper.

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

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