Can. J. Math., Vol. XXXII, No. 5, 1980, pp. 1168–1176

ON THE AUTOMORPHISM GROUP OF A FINITE p-GROUP WITH A SMALL CENTRAL QUOTIENT

RICHARD M. DAVITT

In recent years there has been considerable interest in the conjecture that $|G|$ divides $|\text{Aut } G|$ for all finite non-cyclic p-groups G of order greater than p^2. In particular, the conjecture has been established for a considerable number of (not necessarily distinct) classes of finite p-groups ([**6**], [**7**], [**8**], [**9**], [**15**], [**16**]); additionally, results have been obtained, often using homological methods, which permit reductions in any attempt to establish the overall conjecture ([**5**], [**10**], [**13**], [**15**]). In the former case, the p-groups G have generally been regular p-groups (see, for example, [**6**]) and the prime $p = 2$ has either been excluded (see, for example, [**8**]) or treated as a special case (as in [**9**]). It is the purpose of this paper to establish the conjecture for the class of all p-groups G where $|G: Z(G)| \leqq p^4$ with no restrictions on the prime p.

Most of the notational conventions and terminology used in the paper are standard (see, for example, [**14**]). For the sake of convenience, G will always be assumed to be a finite p-group where p is a prime, $G = G_1 \geqq G_2 \geqq \ldots \geqq G_i \geqq \ldots$ will denote the lower central series of G and the argument G will be omitted in any notation where no ambiguity is possible. Special purpose notation will be introduced as needed.

There are certain results which we often need and shall use throughout the paper without further reference. Their statements and proofs may be found in [**4**] and [**14**]. First,

$$|\text{Hom}(\oplus A_i, \oplus B_j)| = \textstyle\prod_{i,j}|\text{Hom } A_i, B_j|$$

where A_i and B_j are abelian p-groups. Secondly, $\text{Hom}(C(p^\alpha), C(p^\beta))$ is isomorphic to $C(p^{\min(\alpha,\beta)})$ where $C(n)$ is the cyclic group of order n. Thirdly, it is assumed that the definitions of a regular p-group, a metacyclic group and a metabelian group and the basic properties of such groups are known. We will not need all of the standard commutator identities for the variety of metabelian groups. The three identities which we will use the most are:

(1) $\quad [x^n, y] = \prod_{i=1}^{n} [x, y, (i-1)x]^{\binom{n}{i}}$,

(2) $\quad [x, y^n] = \prod_{i=1}^{n} [x, iy]^{\binom{n}{i}}$, and

(3) $\quad [c^m, x] = [c, x]^m$,

Received December 21, 1978 and in revised form October 31, 1979.

https://doi.org/10.4153/CJM-1980-088-3 Published online by Cambridge University Press

where x and y are elements of a metabelian group G, c is in G_2, m and n are positive integers, $\binom{n}{i}$ denotes the usual binomial coefficient with the convention that $\binom{n}{i} = 0$ when $n < i$, and the commutator notation is standard left-normed.

We now state our theorem.

THEOREM. *If G is a finite non-cyclic p-group of order greater than p^2 such that $|G: Z| \leqq p^4$, then $|G|$ divides $|\mathrm{Aut}\, G|$.*

We may assume that the nilpotency class of G is greater than 2 [**9**] and hence that $p^3 \leqq |G: Z| \leqq p^4$. This same assumption in combination with the reduction obtained in [**5**] and [**13**] also allows us to assume that $Z < \Phi(G)$ and consequently that G is purely non-abelian. From this we know that $|A_c(G)| = |\mathrm{Hom}(G, Z)|$ [**15**], where $A_c(G)$ is the p-group of central automorphisms of G. Finally, we may assume that G is not p-abelian [**6**] and that $|Z| > p$ [**10**]. Throughout the rest of the paper G will be taken to be a p-group which satisfies the hypotheses of the theorem and the assumptions noted in this paragraph.

1. General p-groups.

LEMMA 1. *If G is a regular p-group, then the theorem is true.*

Let G be a regular p-group. Since regular 2-groups are abelian, $p \neq 2$. Also since G is not p-abelian, there are elements a and b in G with $[a, b]^p \neq e$. It follows from regularity that $[a^p, b]$ and $[a, b^p]$ are not e. Thus a^p and b^p are not in $Z(G)$. Indeed, $\langle a^p \rangle Z/Z$ and $\langle b^p \rangle Z/Z$ have trivial intersection since otherwise $a^p y \in \langle b \rangle$ for some y in Z and consequently $[a^p y, b] = [a^p, b] = e$. If we let $H = \langle a, b \rangle Z/Z$, it is clear that $|H| = p^4$ and we have that $H = G/Z$. Furthermore, the above work shows that $|\mho_1(H)| = p^2$ and that $|H: \mho_1(H)| = p^2$. Thus $H = G/Z$ is metacyclic [**14**, K.III, S.11.4] and the lemma follows by [**8**].

Since the nilpotency class of G ($\mathrm{cl}(G)$) is necessarily either 3 or 4, Lemma 1 establishes that the theorem is true for all primes p, $p \geqq 5$, and that we need only concern ourselves with the classes of irregular 2-groups and irregular 3-groups to complete the proof of the theorem. We note that a finite 2-group is irregular if, and only if, it is non-abelian and that a finite 3-group is irregular if, and only if, for some 2-generator subgroup K of G, $K_3 \nsubseteq \mho_1(K_2)$ [**2**, Theorem 4]. Thus it is clear that there do exist 2- and 3-groups G which are not covered by Lemma 1.

Even if G is an irregular p-group, it is still true that G is metabelian, a fact which we establish in

LEMMA 2. *G is metabelian.*

From our previous assumptions it follows that G possesses the following chain of subgroups: $Z < G_2Z \leqq \Phi(G) < G$. But now either $|G_2Z: Z| = p$

and the result follows immediately or $|G_2Z: Z| = p^2$ and $G_2Z = \Phi$. If G_2Z/Z is cyclic, the result again follows immediately; so we assume that $G_2Z/Z = \langle aZ\rangle \oplus \langle bZ\rangle$ for a and b in G. If $\mathrm{cl}(G) = 3$, we can choose a and b to be in G_2 so that $[a, b]$ is in $G_4 = E$ [**14**, K.III, H.2.11, b] and if $\mathrm{cl}(G) = 4$, we can choose a to be in G_2 and b to be in G_3 so that $[a, b]$ is in $G_5 = E$. Since $G_2Z = \langle a, b, Z\rangle$, G_2Z is abelian and consequently G is seen to be metabelian.

Before turning our attention to the remaining cases of $p = 3$ and $p = 2$, respectively, it remains appropriate to do additional work in the general setting primarily to avoid repetition of analogous arguments later in the paper and to establish additional convenient notation. In the latter vein let $d(G)$ be the minimal number of generators of G, let the exponent of G ($\exp G$) be p^m, where $m \geqq 2$ since G is not p-abelian, and let $H = G/Z$. Also let R be the p-subgroup of Aut G defined by $R = \mathrm{Inn}\, G\, A_c(G)$. It should also be noted that the restriction $Z < \Phi(G)$ implies that we are dealing with either 2 or 3 generator groups. To see this, observe that $\Phi(H) = \Phi(G)/Z$ and conclude that $|H: \Phi(H)| = |G: \Phi(G)|$ is p^2 or p^3. From the preceding work we can also see that $d(G) = d(H)$. Finally, we note that

$$|R| = |A_c(G)||G: Z_2| = |\mathrm{Hom}(G/G_2, Z)||G: Z_2|$$

as in [**8**] and that whenever $|R| \geqq |G|$, the theorem follows.

The last items in this section are a sequence of simple but useful lemmas.

LEMMA 3. *If* $\exp H_2 = p$, *then* $\mathcal{V}_1(G_2) \leqq Z$ *and* $\exp G_3 = p$.

This lemma follows from (3) and the fact that $H_2 = (G/Z)_2 = G_2Z/Z$.

LEMMA 4. *If* $\exp H \leqq p^2$, *then* $\exp G_2 \leqq p^2$.

We note that $\mathrm{cl}(G) \leqq 4$. So for elements x and y in G,

$$e = [x^{p^2}, y] = [x, y]^{p^2}[x, y, x]^{\binom{p^2}{2}}[x, y, x, x]^{\binom{p^2}{3}}$$

by (1). Clearly, $e = [x, y]^{p^2}$ if $p > 3$. If $p = 3$, then $\exp H_3 \leqq 3$ and again $[x, y]^{p^2} = e$. Finally, if $p = 2$, it is true that $\exp H_2 \leqq 2$ ([**11**], p. 39) so that we still obtain $[x, y]^{p^2} = e$. Since in all cases G_2 is abelian, generated by elements of order less than or equal to p^2, $\exp G_2 \leqq p^2$.

LEMMA 5. *If* $\exp G_2 = p$ *and* $\Phi(G)$ *is regular, then* $\exp G/G_2 \geqq \exp Z$.

If $\exp G_2 = p$, then clearly $\exp G/G_2 \geqq p^{m-1}$. Since Z is a subgroup of the regular group $\Phi(G) = \mathcal{V}_1 G_2$,

$$\exp Z \leqq \max\{\exp \mathcal{V}_1, \exp G_2\} = p^{m-1}$$

and the lemma follows.

A similar argument yields

LEMMA 6. *If* $\exp G_2 = p^2$ *and* $\Phi(G)$ *is regular, then* $\exp G/G_2 \geqq \exp Z/p$.

Finally, for future reference we list two additional lemmas.

LEMMA 7 [**14**, Aufgabe 2a) and b), S.259]. *If A is an abelian normal subgroup of G with cyclic factor group $G/A = \langle xA \rangle$, then the map $a \to [a, x]$ is an epimorphism from A to G_2 and consequently $|A| = |G_2|\,|A \cap Z|$.*

LEMMA 8 [**17**, 3.2.10]. *If H is a group containing a non-identity element w and a generating subset S such that some power of each element in S equals w, then there is no group G such that $G/Z \cong H$.*

2. G **is an irregular 3-group.** We may assume that H is not metacylic [**8**]. Consequently, $\exp H \leqq 9$, $\exp G_2 \leqq 9$ (Lemma 4) and $\exp G/G_2 \geqq 3^{m-2}$. Clearly $|H_2| \leqq 9$. But if we suppose that H_2 is cyclic of order 9, then H would be regular [**2**, Theorem 4] and $d(H) = 2$. Letting $H = \langle x, y\rangle$, the regularity of H implies that $H_2 = \langle [x, y]\rangle$ and consequently that $\mho_1(H) = \langle x^3, y^3\rangle$ has order 9. But then $|H : \mho_1(H)| = 3^2$ and H would be metacyclic contradicting the assumption just made. Thus $\exp H_2 = 3$ and by Lemma 3, $\mho_1(G_2) \leqq Z(G)$ and $\exp G_3 = 3$. Furthermore, since $|\Phi(G) : Z| \leqq 9$, $\Phi(G)$ is regular.

a. $|H| = 3^3$.

Since H is neither metacyclic nor abelian, precisely one of the well-known groups H of order 3^3 remains under consideration. For this group it is true that $d(H) = 2$, $\text{cl}(H) = 2$ and $\exp H = 3$. Let $G = \langle a, b\rangle$. Since $\text{cl}(G) = 3$, and $\exp G_3 = 3$, using (1) we conclude that

$$e = [a^3, b] = [a, b]^3[a, b, a]^3[a, b, a, a] = [a, b]^3.$$

Since $G_2 = \langle [a, b], G_3\rangle$ [**12**, Theorem 2.81], we see that $\exp G_2 = 3$. Thus $\exp G/G_2 \geqq \exp Z$ (Lemma 5) and consequently, $|R| \geqq |Z|\cdot 3\cdot 3^2 = |G|$.

b. $|H| = 3^4$.

Suppose first that $d(G) = 3$. If $|G : Z_2| = 3^3$, then since $\exp G/G_2 \geqq \exp Z/3$ (Lemma 6),

$$|R| \geqq |\Omega_1(Z)|^2\cdot 3\cdot 3^3 \geqq 3^4\cdot|Z| = |G| \text{ if } m = 2 \text{ and}$$
$$|R| \geqq \Omega_{m-2}(Z)|\,|\Omega_1(Z)|\cdot 3\cdot 3^3 \geqq |G| \text{ if } m > 2,$$

given that $\exp Z \leqq 3^{m-1}$ in the latter case. If $|G : Z_2| = 9$, we turn our attention to H which is regular. Indeed, since $|H_2| = 3$, H is 3-abelian. If $\exp H = 3$, $G = \langle a, b, c\rangle$ where

$$o(aZ) = o(bZ) = o(cZ) = 3 \text{ and}$$
$$G_2 = \langle [a, b], [a, c], [b, c], G_3\rangle \text{ [3, Lemma 1.1].}$$

Using (1) and the fact that $\mathrm{cl}(G) = 3$, it follows that $\exp G_2 = 3$. Thus $\exp G/G_2 \geqq \exp Z$ (Lemma 5) and $|R| \geqq |Z|\cdot 3\cdot 3\cdot 3^2 = |G|$. If $\exp H = 9$, let $H = \langle x, y, w\rangle$ where $o(x) = 9$ and $\mathcal{V}_1(H) = \langle x^3\rangle$. Because H is 3-abelian, we may assume, without loss of generality, that $o(y) = o(w) = 9$ so that H has a generating subset S such that some power of each element in S equals x^3. By Lemma 8 there is no group G such that $G/Z \cong H$ and we conclude that the theorem holds when $d(G) = 3$.

Suppose then that $d(G) = 2$ and let $G = \langle a, b\rangle$. Also let $|G: Z_2| = 3^3$. If $\exp G/G_2 \geqq \exp Z$ or if Z is not cyclic, then it readily follows that $|R| \geqq |G|$. Thus we assume that Z is cyclic, $\exp G/G_2 < \exp Z$ and $\exp G_2 = 9$ (Lemma 5). Since $G_2 = \langle [a, b], G_3\rangle$, $\mathcal{V}_1(G_2) \leqq Z$ and $\exp G_3 = 3$, $\langle [a, b]^3\rangle$ is the unique subgroup of Z of order 3 and $|G_2| = 3\cdot|G_3|$. If $\mathrm{cl}(G) = 3$, it would follow that $|G_2| = 9$ or that G_2 is cyclic of order 9, an impossibility since G is irregular. If $\mathrm{cl}(G) = 4$, then

$$|G_2| = 3\cdot|G_3Z: Z||G_3 \cap Z| = 27$$

and $|G_2 \cap Z| = 3$. If $m = 2$ it would be the case that $\exp G/G_2 = 3$ while $\exp Z = 9$. This is impossible, for on the one hand,

$$|G| = |G/G_2||G_2| = 3^5$$

while on the other,

$$|G| = |G/Z||Z| = 3^6.$$

If $m > 2$, then given x in G of order 3^m, x^9 is in Z and hence $x^{3^{m-2}}$ is in $Z \cap G_2$ implying that $\exp G/G_2 \geqq 3^{m-2}$. But $Z \leqq \mathcal{V}_1 G_2$ which has exponent 3^{m-1} which leaves the subcase $\exp G/G_2 = 3^{m-2}$ and Z cyclic of order 3^{m-1} for our consideration. If G/G_2 is abelian of type $(3^{m-2}, 3)$, we again get a contradiction, namely, $|G| = |G/G_2||G_2| = 3^{m+2}$ which does not coincide with $|G| = |G/Z||Z| = 3^{m+3}$. But if G/G_2 is abelian of type $(3^{m-2}, 3^s)$ with $s \geqq 2$, we obtain $|R| \geqq 3^3\cdot 3^{m-2}\cdot 3^2 = |G|$ once again. Letting $|G: Z_2| = 9$, we obtain a group $H = G/Z$ which is regular and indeed 3-abelian since $|\mathcal{V}_1(H)| \leqq 3$. The assumption that $\exp H = 3$ yields the immediate contradiction that $Z(H) = H_2 = \langle [x, y]\rangle$ is cyclic of order 9. On the other hand if $|\mathcal{V}_1(H)| = 3$, we can use the arguments of the preceding paragraph to apply Lemma 8 thereby discovering that there is no group G such that $G/Z \cong H$ in this last subcase too. Thus the proof of the theorem is complete for the prime $p = 3$.

3. *G* is an irregular 2-group. In dealing with the generally exceptional prime 2, it is convenient to use information obtained from the Hall-Senior tables [**11**]. For example, a quick check of these tables establishes that the theorem is indeed true for all 2-groups G where $|G| \leqq 64$.

a. $|H| = 2^3$.

The two non-abelian 2-groups H of order 8 are both 2-generator metacyclic groups containing as they do elements of order 4. Thus we may assume that $G = \langle a, b \rangle$ where $\circ(aZ) = 4$, $\circ(bZ) = 2$ and $\langle aZ \rangle$ is a normal subgroup of G/Z of index 2. If we let $A = \langle a, Z \rangle$,

$$|A| = |G_2||Z| = 4 \cdot |Z| \text{ (Lemma 7).}$$

Thus $|G_2| = 4$ and $|G/G_2| = 2 \cdot |Z|$. If $\exp G/G_2 \geqq \exp Z$, then $|R| \geqq |Z| \cdot 2 \cdot 2^2 = |G|$, while if $\exp G/G_2 < \exp Z$, it follows that $|R| \geqq |G/G_2| \cdot 2^2 = |G|$.

b. $|H| = 2^4$.

Defining relations and other information for the nine isomorphism classes of non-abelian groups H of order 16 are listed in the Hall-Senior tables on pages 39 and 45. These are the groups labeled 6 through 14 on these two pages.

It is convenient to list the defining relations and other facts about these groups in terms of generators x, y (and w where needed). When considering these groups as $H = G/Z$, the identifications $x = aZ$, $y = bZ$, and $w = cZ$ will be used.

Group 6: $H = \langle x, y, w \rangle$, $x^4 = e$, $y^2 = w^2 = e$, $[x, y] = x^2$, $H_2 = \langle x^2 \rangle$, $Z(H) = \langle x^2 \rangle \oplus \langle w \rangle$.

Group 7: $H = \langle x, y, w \rangle$, $x^4 = y^4 = e$, $w^2 = e$, $[x, y] = x^2 = y^2$, $H_2 = \langle x^2 \rangle$, $Z(H) = \langle x^2 \rangle \oplus \langle w \rangle$.

Group 8: $H = \langle x, y, w \rangle$, $x^2 = y^2 = e$, $w^4 = e$, $[x, y] = w^2$, $H_2 = \langle w^2 \rangle$, $Z(H) = \langle w \rangle$.

Group 9: $H = \langle x, y \rangle$, $x^2 = e$, $y^4 = e$, $[x, y]^2 = e$, $H_2 = \langle [x, y] \rangle$, $Z(H) = \langle [x, y] \rangle \oplus \langle y^2 \rangle$.

Group 10: $H = \langle x, y \rangle$, $x^4 = y^4 = e$, $[x, y] = x^2$, $H_2 = \langle x^2 \rangle$, $Z(H) = \langle x^2 \rangle \oplus \langle y^2 \rangle$.

Group 11: $H = \langle x, y \rangle$, $x^2 = e$, $y^8 = e$, $[x, y] = y^4$, $H_2 = \langle y^4 \rangle$, $Z(H) = \langle y^2 \rangle$.

Group 12: $H = \langle x, y \rangle$, $x^8 = e$, $y^2 = e$, $[x, y]^{-1} = x^2$, $H_2 = \langle [x, y] = Z_2(H)$, $Z(H) = \langle [x, y]^2 \rangle = H_3$.

Group 13: $H = \langle x, y \rangle$, $x^8 = e$, $y^2 = e$, $[x, y] = x^2$, $H_2 = \langle [x, y] = Z_2(H)$, $Z(H) = \langle [x, y]^2 \rangle = H_3$.

Group 14: $H = \langle x, y \rangle$, $x^8 = e$, $y^4 = e$, $[x, y]^{-1} = x^2$, $[x, y]^2 = y^2$, $H_2 = \langle [x, y] \rangle = Z_2(H)$, $Z(H) = \langle [x, y]^2 \rangle = H_3$.

LEMMA 9. *Groups* 7, 8, 10, 11, 13 *and* 14 *are groups H for which there is no group G such that $G/Z \cong H$.*

This lemma follows an application of G. A. Miller's result (Lemma 8) to an appropriate generating set S for each of these groups. For example, in Group 7, if we let $\bar{w} = xw$, then $\bar{w}^2 = x^2$ and $S = \langle x, y, \bar{w} \rangle$. Thus $x^2 \in \langle x \rangle \cap \langle y \rangle \cap \langle \bar{w} \rangle$ and the lemma holds for Group 7 by Lemma 8.

The application of Lemma 8 to the other five groups listed is equally routine and is omitted.

To complete the proof of the theorem, we consider the three cases involving Groups 6, 9 and 12.

Case (i). Let H be the group labeled "6".

Using the list we see that $\exp G_3 = 2$, $\mathscr{V}_1(G_2) \leqq Z$ (Lemma 3), $|G: Z_2| = 4$, $\mathrm{cl}(G) = 3$, $|G_2Z: Z| = 2$ and consequently that $\Phi(G)$ is abelian. By Lemmas 4, 5 and 6, it follows that $\exp G_2 \leqq 4$, $\exp G/G_2 \geqq \exp Z/2$ and $\exp G/G_2 \geqq \exp Z$ when $\exp G_2 = 2$. If Z is not cyclic or if $\exp G/G_2 \geqq \exp Z$, then $|R| \geqq |G|$ by the familiar arguments of this paper. Thus we assume that Z is cyclic, $\exp G/G_2 < \exp Z$, and $\exp G_2 = 4$. According to our notation, $G = \langle a, b, c\rangle$ where $o(cZ) = 2$ and c is in Z_2 so that $[a, c]$ and $[b, c]$ are elements of $\Omega_1(Z)$ by (2). Since $G_2 = \langle [a, b], [a, c], [a, c], G_3\rangle$, it necessarily follows that $[a, b]$ is an element of order 4 in G_2. Indeed it is clear that $\Omega_1(Z) = \langle [a, b]^2\rangle$ so that $G_2 = \langle [a, b]\rangle$ is cyclic of order 4. Consequently, $|R| \geqq 4\cdot|G/G_2| = |G|$ and the theorem holds in this case.

Case (ii). Let H be the group labeled "9".

Using the list we see that $\exp G_3 = 2$, $\mathscr{V}_1(G_2) \leqq Z$, $|G: Z_2| = 4$, $\mathrm{cl}(G) = 3$, $|G_2Z: Z| = 2$ and $\Phi(G) = \langle [a, b], b^2, Z\rangle$. Now $\Phi(G)$ is abelian since $[a, b] \in G_2$ and $b^2 \in Z_2$ [**14**, 2.11c, S.265] and it follows by Lemmas 4 and 6 that $\exp G_2 \leqq 4$ and $\exp G/G_2 \geqq \exp Z/2$. Now $G_2 = \langle [a, b], [a, b, a], [a, b, b]\rangle$ [**3**, Lemma 1.1] where only $[a, b]$ could possibly have order as large as 4. Since $o(aZ) = 2$, $e = [a^2, b] = [a, b]^2[a, b, a]$ so that $[a, b, a] \in \langle [a, b]^2\rangle$ which means that $|G_2| \leqq 8$. If Z is not cyclic, then $|R| \geqq 4\cdot|Z|\cdot 4 = |G|$ when $\exp G/G_2 \geqq \exp Z$ and $|R| \geqq 4\cdot|G/G_2|\cdot 2 \geqq |G|$ when $\exp G/G_2 = \exp Z/2$. Thus we assume that Z is cyclic. Since $G_2 = \langle [a, b], [a, b, b]\rangle$, it is now true that $|G_2| = 4$.

If we assume that $o([a, b]) = 4$, it then follows that $[a, b, b] = e$. To see this, suppose $[a, b, b] \neq e$. Then $[a, b, b] = [a, b]^2$, the unique element of order 2 in G_2. But then by (2),

$$[a, b^2] = [a, b]^2[a, b, b] = [a, b]^2[a, b]^2 = e$$

and b^2 is in Z which is a contradiction. If we now let $B = \langle [a, b], b, Z\rangle$, B is an abelian normal subgroup of G of index 2. Thus on the one hand, $|B| = 8\cdot|Z|$ while on the other hand, by Lemma 7, $|B| = |G_2||B \cap Z| = 4\cdot|Z|$. This final contradiction shows that $o([a, b]) = 2$ and consequently that $\exp G_2 = 2$ and $[a, b, a] = e$.

Because $|Z| > 2$ and $Z \leqq \mathscr{V}_1 G_2$, an abelian group of exponent 2^{m-1}, we see that $m > 2$. If g is an element of G of maximal order 2^m, g^4 is in Z and hence $g^{2^{m-1}}$ is in $Z \cap G_2$, the unique subgroup of Z of order 2. Thus $\exp G/G_2 = 2^{m-1}$. Similarly, $\exp Z = |Z| \geqq 2^{m-2}$. If $|Z| = 2^{m-1}$ then

https://doi.org/10.4153/CJM-1980-088-3 Published online by Cambridge University Press

$|R| = |G/G_2| \cdot 4 = |G|$. Thus we assume that Z is cyclic of order 2^{m-2} and consequently that $Z \leqq \mathcal{V}_2 G_2$. Let $Z = \langle vw^4 \rangle$ where $v \in G_2$ and $w \in G$. Then

$$a^2 = v^i w^{4j} = v^i (w^2)^{2j}$$

since a^2 is in Z. If we let $\bar{a} = a(w^2)^{-j}$, then we have that $\bar{a}^4 = e$. But $G = \langle \bar{a}, b \rangle$ since $(w^2)^{-j}$ is in $\Phi(G)$ and we see that, without loss of generality, we may assume that $G = \langle a, b \rangle$ where $2 \leqq \circ(a) \leqq 4$. If $A = \langle [a, b], a, Z \rangle$, then A is a normal abelian subgroup of G such that $G/A = \langle bA \rangle$ is cyclic of order 4. It follows that the mapping $\phi: G \rightarrow G$ defined by $b^k c \rightarrow (ba)^k c$, where $0 \leqq k < 4$ and c is in A is an automorphism of G under which A is elementwise fixed and such that $\circ(\phi) = \circ(a)$ [**8**, Lemma 3]. Since $\phi(b) = ba$ where a is not in $G_2 Z$, ϕ is a non-trivial 2-power automorphism which is not in R. Hence, if $S = \langle R, \phi \rangle$, then

$$|S| \geqq 2 \cdot |R| = 2 \cdot (|Z| \cdot 2) \cdot 4 = |G|$$

and the theorem holds in this case.

Case (iii). Let H be the group labeled "12".

Using the list we see that $G = \langle a, b \rangle$ where $\circ(aZ) = 8$ and that $|G: Z_2| = 8$. Thus $A = \langle a, Z \rangle$ is a normal abelian subgroup of index 2. Since $|A| = 8 \cdot |Z| = |G_2||Z|$ by Lemma 7, we have that $|G_2| = 8$. Consequently, $|R| \geqq 8 \cdot |Z| \cdot 2 = |G|$ when $\exp G/G_2 \geqq \exp Z$ and $|R| \geqq 8 \cdot |G/G_2| = |G|$ when $\exp G/G_2 < \exp Z$. Thus the theorem holds in this last case when $p = 2$.

The proof of the entire theorem is now complete.

COROLLARY. *If G is a finite non-cyclic p-group where $p^3 \leqq |G| \leqq p^6$, then $|G|$ divides $|\mathrm{Aut}\, G|$.*

REFERENCES

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

2. D. E. Arganbright, *The power-commutator structure of finite p-groups*, Pacific J. Math. *29* (1969), 11–17.

3. N. Blackburn, *On prime power groups with two generators*, Proc. Cambridge Phil. Soc *54* (1958), 327–337.

4. W. Brisley and I. D. Macdonald, *Two classes of metabelian p-groups*, Math. Z. *112* (1969), 5–12.

5. J. Buckley, *Automorphism groups of isoclinic p-groups*, J. Lond. Math. Soc. *12* (1975), 37–44.

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

7. R. M. Davitt and A. D. Otto, *On the automorphism group of a finite modular p-group*, Proc. Amer. Math. Soc. *35* (1972), 399–404.

8. ——— *On the automorphism group of a finite p-group with the central quotient metacyclic*, Proc. Amer. Math. Soc. *30* (1971), 467–472.

9. R. Faudree, *A note on the automorphism group of a p-group*, Proc. Amer. Math. Soc. *19* (1968), 1379–1382.
10. W. Gaschütz, *Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen*, J. Alg. *4* (1966), 1–2.
11. M. Hall, Jr. and J. K. Senior, *The groups of order* 2^n ($n \leqq 6$) (The Macmillan Company, New York, 1964).
12. P. Hall, *A contribution to the theory of groups of prime-power orders*, Proc. London Math. Soc. *36* (1933), 29–95.
13. K. Hummel, *The order of the automorphism group of a central product*, Proc. Amer. Math Soc. *47* (1975), 37–40.
14. B. Huppert, *Endliche Gruppen*, I, Die Grundlehren der math. Wissenschaften, Band *134* (Springer-Verlag, Berlin and New York, 1967).
15. A. D. Otto, *Central automorphisms of a finite p-group*, Trans. Amer. Math. Soc. *125* (1966), 280–287.
16. R. Ree, *The existence of outer automorphisms of some groups*, II, Proc. Amer. Math. Soc. *9* (1958), 105–109.
17. W. R. Scott, *Group theory* (Prentice-Hall, Inc., Englewood Cliffs, NJ, 1964).

University of Louisville,
Louisville, Kentucky