ON THE ORDER OF THE SYLOW SUBGROUPS OF THE AUTOMORPHISM GROUP OF A FINITE GROUP

by K. H. HYDE

(Received 30 September, 1968; revised 26 September, 1969)

1. Introduction. Given any finite group G, we wish to determine a relationship between the highest power of a prime p dividing the order of G, denoted by $|G|_p$, and $|A(G)|_p$, where $A(G)$ is the automorphism group of G. It was shown by Herstein and Adney [8] that $|A(G)|_p \geqq p$ whenever $|G|_p \geqq p^2$. Later Scott [16] showed that $|A(G)|_p \geqq p^2$ whenever $|G|_p \geqq p^3$. For the special case where G is abelian, Hilton [9] proved that $|A(G)|_p \geqq p^{n-1}$ whenever $|G|_p \geqq p^n$. Adney [1] showed that this result holds if a Sylow p-subgroup of G is abelian, and gave an example where $|G|_p = p^4$ and $|A(G)|_p = p^2$. We are able to show in Theorem 4.5 that, if $|G|_p \geqq p^5$, then $|A(G)|_p \geqq p^3$.

In the general case, Ledermann and Neumann [11] showed that there exists a function $g(h)$ having the property that $|A(G)|_p \geqq p^h$ whenever $|G|_p \geqq p^{g(h)}$, and gave an upper bound for $g(h)$. Later, Green [6] improved their result by showing that

$$g(h) \leqq \tfrac{1}{2}(h^2+3h+2).$$

Howarth [10] then proved that, for $h \geqq 12$,†

$$g(h) \leqq \begin{cases} \tfrac{1}{2}(h^2+3) & \text{for } h \text{ odd,} \\ \tfrac{1}{2}(h^2+4) & \text{for } h \text{ even.} \end{cases}$$

We are able to improve this result by showing that, for all h,

$$g(h) \leqq \tfrac{1}{2}(h^2-h+6).$$

We shall also consider the special case where G is a p-group, and show that in this case $|A(G)|_p \geqq p^h$ whenever $|G| \geqq p^A$, where

$$A = \begin{cases} \tfrac{1}{2}(h^2-3h+6) & \text{for } h \geqq 5, \\ h+1 & \text{for } h \leqq 4. \end{cases}$$

We point out that all groups considered in this paper are finite. Also, the letter p will always stand for a prime.

2. Central automorphisms. An automorphism σ such that $g^{-1}g^{\sigma}$ is in the center of G, for all g in G, is called *central*. The set of all central automorphisms of G forms a subgroup of $A(G)$, which we denote by $A_c(G)$. It is easy to show that $A_c(G)$ is the centralizer of the inner automorphism group $I(G)$ in $A(G)$. From this it follows that $A_c(G)$ is normal in $A(G)$, and that

† Howarth remarks that the result can be shown to be valid for $h \geqq 6$.

https://doi.org/10.1017/S0017089500000902 Published online by Cambridge University Press

$A_c(G)$ contains $I(G)$ if and only if $I(G)$ is abelian. If G' is the derived group of G, then G' is left fixed elementwise by any σ in $A_c(G)$, and σ induces the identity on G/Z.

The mapping f_σ defined by $gf_\sigma = g^{-1}g^\sigma$ is a homomorphism of G into Z. The map $\sigma \to f_\sigma$ is a one-one map of $A_c(G)$ into the group $\mathrm{Hom}(G,Z)$ of homomorphisms of G into Z. On the other hand, if f is in $\mathrm{Hom}(G,Z)$, then $\sigma: g \to g(gf)$ defines an endomorphism of G. It has been shown by Adney and Yen [2] that, if G has no abelian direct factor, then the endomorphism $\sigma: g \to g(gf)$ is an automorphism of G. If G is a group which does not have an abelian direct factor, we say that G is *purely non-abelian*. We shall for brevity call such a group a *PN-group*.

We note that, for any f in $\mathrm{Hom}(G,Z)$, the kernel of f contains G' so that $\mathrm{Hom}(G,Z) = \mathrm{Hom}(G/G',Z)$. We now state the result of Adney and Yen as a lemma for future reference.

LEMMA 2.1. *If G is a PN-group, then the order of* $\mathrm{Hom}(G/G',Z)$ *is equal to the order of* $A_c(G)$.

For a prime p we shall denote the cyclic group of order p^a by $C(p^a)$. We shall denote the minimum of two real numbers x and y by $\min(x,y)$. The proofs of the following two lemmas are straightforward.

LEMMA 2.2. *If* $H = C(p^a) \times C(p^{b+x})$, $K = C(p^d)$ *and* $H_1 = C(p^{a+x}) \times C(p^b)$, *where* $a \geqq b$, *then* $|\mathrm{Hom}(H_1,K)| \leqq |\mathrm{Hom}(H,K)|$. *We also have* $|\mathrm{Hom}(K,H_1)| \leqq |\mathrm{Hom}(K,H)|$.

LEMMA 2.3. *If H and K are abelian p-groups, then* $|\mathrm{Hom}(H,K)| \geqq \min(|H|,|K|)$.

The following result will reduce our problem to the case of a p-group.

LEMMA 2.4. *If* $|A_c(G)|_p = |A(G)|_p$, *then* $G = G_p \times G_{p'}$, *where* G_p *is a Sylow p-subgroup of G.*

Proof. Let x be an element of a Sylow p-subgroup G_p. If T_x is the inner automorphism induced by x, then $o(T_x) = p^a$ for some a. Let A_p be a Sylow p-subgroup of $A(G)$ which contains T_x. Since $|A_c(G)|_p = |A(G)|_p$ and since $A_c(G)$ is normal in $A(G)$, by Sylow's Theorem, $A_p \subseteq A_c(G)$. Therefore T_x is central and, for any $g \in G$, $(gZ)T_x = g^xZ = gZ$. Hence $[g,x] \in Z$ for all $x \in G_p$, and so $[G,G_p]$ is contained in the center of G. Now let H be any subgroup of G_p and x an element of order prime to p which normalizes H. For any h in H we have $hT_x = h[h,x]$ and $[h,x]$ is in $H \cap [G,G_p] \subseteq H \cap Z(G)$. Let $n = o(T_x)$; then $hT_x^n = h[h,x]^n = h$. But n divides the order of x, which is prime to p, and $[h,x]$ is in G_p. Therefore $[h,x] = e$ and x centralizes H. From Theorem 14.4.7 of Hall [7], G_p has a normal complement $G_{p'}$. Since $[G_p,G]$ is contained in the center, G_pZ is normal in G. Also G_p is characteristic in G_pZ and therefore normal in G. We now have that $G = G_p \times G_{p'}$.

3. Automorphisms of p-groups. We shall make use of the following results. The first is due to Gaschütz [5].

LEMMA 3.1. *If G is a non-abelian p-group, then there exists an outer automorphism of G which has order a power of p.*

The proof of the following result is given in a paper by Otto [**12**].

LEMMA 3.2. *If the p-group G is a direct product of an abelian group H and a PN-group K, then*

$$\text{(i) } |A(G)|_p \geqq |H|\,|A(K)|_p \quad \textit{and}$$

$$\text{(ii) } |A_c(G)|_p \geqq |H|\,|A_c(K)|_p.$$

The next lemma is due to Wiegold [**17**].

LEMMA 3.3. *Let p be a prime and G a group with $|G/Z| = p^r$. Then G′ is a p-group of order at most $p^{r(r-1)/2}$.*

It is known that, if $|G/Z|_p = p^r$, then $|G' \cap Z|_p \leqq p^{r(r-1)/2}$.

This result can be found in a paper of Howarth [**10**, Lemmas 4.2 to 4.5].

From this we get the following result.

LEMMA 3.4. *If G is a group with $|G/Z|_p = p^r$, then $|G'|_p \leqq p^{r(r+1)/2}$.*

THEOREM 3.5. *If G is a p-group of order at least p^{h+1} and $h \leqq 4$, then $|A(G)|_p \geqq p^h$.*

Proof. The result holds for abelian groups, so we shall assume that G is non-abelian. Hence $|I(G)| = |G/Z| \geqq p^2$. Since there also exists an outer automorphism of p-power order, we have $|A(G)|_p \geqq p^3$. This leaves only the case where $h = 4$. In this case, if $|G/Z| \geqq p^3$, then, as in the preceding argument, $|A(G)|_p \geqq p^4$. It will now be sufficient to consider the case where $|G| \geqq p^5$ and $|G/Z| = p^2$. From Lemma 3.3, $|G'| = p$ and $|G/G'| \geqq p^4$. Now G/Z is elementary abelian and is isomorphic to a subgroup of G/G'. Therefore G/G' has at least two cyclic factors. We have $|Z| \geqq p^3$ and so, by Lemma 2.2, $|\mathrm{Hom}(G/G', Z)| \geqq |\mathrm{Hom}(H, K)|$, where $H \cong C(p^3) \times C(p)$ and $K \cong C(p^3)$. If G is purely non-abelian, then, from Lemma 2.1,

$$|A_c(G)| = |\mathrm{Hom}(G/G', Z)| \geqq |\mathrm{Hom}(H, K)| = p^4.$$

If G has an abelian direct factor, we write $G = H \times K$ with H abelian and K a PN-group and apply the previous results to get

$$|A(G)|_p \geqq |H|\,|A(K)|_p \geqq |H|\,|K|/p = |G|/p \geqq p^4.$$

THEOREM 3.6. *If G is a p-group of order at least $p^{g(h)}$ with $g(h) = \frac{1}{2}(h^2 - 3h + 6)$ and $h \geqq 5$, then $|A(G)|_p \geqq p^h$.*

Proof. The result holds if G is abelian. We therefore consider the case where G is non-abelian. If $|G/Z| \geqq p^{h-1}$, then $|I(G)| \geqq p^{h-1}$. By Lemma 3.1 there exists an outer automorphism α which has order a power of p, and α along with $I(G)$ will generate a subgroup whose order is divisible by p^h.

We now consider the case where $|G/Z| \leqq p^{h-2}$, and G is purely non-abelian. From Lemma 3.3,

$$|G'| \leqq p^{(h^2 - 5h + 6)/2}$$

and so $|G/G'| \geqq p^h$. Also

$$|Z| \geqq p^{(h^2-5h+10)/2}$$

and, for $h \geqq 5$, $\frac{1}{2}(h^2-5h+10) \geqq h$. We apply Lemma 2.1 and Lemma 2.3 to get

$$|A_c(G)| = |\text{Hom}(G/G', Z)| \geqq p^h.$$

If $|G/Z| \leqq p^{h-2}$ and G has an abelian direct factor, then we write $G = H \times K$, where H is abelian and K is a PN-group. From Lemma 3.2,

$$|A(G)|_p \geqq |H| \; |A(K)|_p.$$

Let $|H| = p^r$ so that $|K| \geqq p^{g(h)-r}$. If $r \geqq h$, we have the result. We therefore take $h \geqq r$, and show that $|A(K)|_p \geqq p^{h-r}$. If $h-r \geqq 5$, then $2rh \geqq r^2+5r$, which implies that $g(h)-r \geqq g(h-r)$. From the first part of the proof for PN-groups, we have $|A(K)|_p \geqq p^{h-r}$. In the case in which $h-r \leqq 4$, we have $h^2-5h+4 \geqq 0$ for $h \geqq 5$, which implies that $g(h)-r \geqq h-r+1$. From Theorem 3.5, we get $|A(K)|_p \geqq p^{h-r}$. This completes the proof.

4. The main results. We shall now find a bound for the least function $g(h)$ such that $|A(G)|_p \geqq p^h$ whenever $|G|_p \geqq p^{g(h)}$. It was conjectured that $g(h) = h+1$, but it was pointed out by Adney **[1]** that this is not true. Let G be the general linear group $GL(2, 19)$. The order of G is $(19^2-1)(19^2-19)$, and so $|G|_3 = 3^4$. The order of the automorphism group of G is $2|I(G)|$ and so

$$|A(G)|_3 = |G/Z|_3 = 3^2.$$

This example can be extended to show that $g(h) \geqq 2h-1$.† It is known that, if a and d are integers which are relatively prime, then the set $\{a+nd \mid n = 0, 1, 2, \ldots\}$ contains an infinite number of primes. Let $a = 1+p^n$ and $d = p^{n+1}$; then a and d are relatively prime and, for some k, $1+p^n+kp^{n+1} (= q \text{ say})$ is a prime. Now let $G = GL(2, q)$; then the order of G is $(q+1)q(q-1)^2$. For an odd prime p, p^n divides $q-1$, p^{n+1} does not divide $q-1$, and p does not divide q or $q+1$. Hence the highest power of p dividing the order of G is p^{2n}. Now $|Z(G)| = q-1$ and so $|I(G)| = (q+1)q(q-1)$. Since q is a prime, $|A(G)| = 2|I(G)|$, and the highest power of p dividing $|A(G)|$ is p^n. Therefore in seeking a bound for the least function $g(h)$ such that $p^h \leqq |A(G)|_p$ whenever $|G|_p \geqq p^{g(h)}$, we must have $g(h) \geqq 2h-1$, where $h \geqq 2$. We have thus proved the following theorem.

THEOREM 4.1. *For $h \geqq 2$, the least function $g(h)$ such that $|A(G)|_p \geqq p^h$ whenever $|G|_p \geqq p^{g(h)}$, satisfies the inequality $g(h) \geqq 2h-1$.*

Our main problem in this section will be to find an upper bound for $g(h)$, and we shall show that $g(h) \leqq \frac{1}{2}(h^2-h+6)$. We shall be mainly concerned with central automorphisms, and shall repeatedly use the fact that, for PN-groups, $|A_c(G)| = |\text{Hom}(G/G', Z)|$. We are interested in finding the highest order of a prime p which divides $|A_c(G)|_p$. We note that $|\text{Hom}(G/G', Z)|_p = |\text{Hom}((G/G')_p, Z_p)|$, so that we can apply the lemmas in Section 2 as they apply to p-groups.

† The author is indebted to W. R. Scott for the proof of this result.

https://doi.org/10.1017/S0017089500000902 Published online by Cambridge University Press

LEMMA 4.2. *If $G = H \times K$, where H is abelian with order divisible by p and K is a group with $|Z(K) \cap K'|$ divisible by p, then $|A(G)|_p > |A(K)|_p$.*

Proof. If $|H|_p > p$, then $|A(H)|_p \geqq p$ and we have $|A(G)|_p \geqq |A(H)|_p > |A(K)|_p$. If $|H|_p = p$, it will be sufficient to consider the case in which $H \cong C(p)$. Since $A_c(G)$ is normal in $A(G)$, we have

$$|A(G)|_p \geqq |A_c(G)A(K)|_p = \frac{|A_c(G)|_p |A(K)|_p}{|A_c(G) \cap A(K)|_p} = \frac{|A_c(G)|_p}{|A_c(K)|_p} |A(K)|_p.$$

Therefore it will be sufficient to show that $|A_c(G)|_p > |A_c(K)|_p$. We shall now construct a central automorphism of order p which is not induced by a central automorphism of K. First, we define a homomorphism of G/G' into $Z(G)$. We note that $G/G' \cong H \times K/K'$, and let h be a generator of H. Since p divides $|Z(K) \cap K'|$, we can pick an element z in $Z(K) \cap K'$ of order p. The mapping defined by

$$h \to z,$$

$$\bar{k} \to e, \quad \text{for all} \quad \bar{k} \text{ in } K/K',$$

defines a homomorphism f of G/G' into Z. As described in Section 2, there exists a corresponding central endomorphism σ of G defined by $g\sigma = g(gG'f)$. Each g in G can be written in the form $g = (h^n, k)$, where k is in K, and so $g\sigma = (h^n, kz^n)$ with kz^n in K. We claim that σ is an automorphism. Since G is finite, it will be sufficient to show that $\ker(\sigma) = 0$. Suppose there exists $(h^n, k) \neq e$ such that $(h^n, k)\sigma = (h^n, kz^n) = e$. Then $h^n = e$ and $n \equiv 0 \pmod{p}$. Since z is of order p, $z^n = e$ and $(h^n, k) = (h^n, kz^n) = e$, a contradiction. It is clear that the central automorphism σ is of order p. Also $h\sigma = hz$, so that σ is not an automorphism induced by an automorphism of K.

We shall now show that σ centralizes $A_c(K)$. Let α be any element of $A_c(K)$; then

$$(h^n, k)\sigma^{-1}\alpha\sigma = (h^n, kz^{-n})\alpha\sigma = (h^n, (k\alpha)(z^{-n}\alpha))\sigma$$

$$= (h^n, (k\alpha)(z^{-n}\alpha)z^n).$$

Since z^{-n} is in K' and α is central, we have $z^{-n}\alpha = z^{-n}$. Therefore $(h^n, k)\alpha^\sigma = (h^n, k)\alpha$ and σ centralizes $A_c(K)$. We can form the subgroup $A_c(K)\langle\sigma\rangle$ and we have

$$|A_c(G)|_p \geqq |A_c(K)\langle\sigma\rangle|_p > |A_c(K)|_p,$$

which is what we wanted to show.

LEMMA 4.3. *If G is a PN-group such that $|G|_p \geqq p^{(h^2-h+2)/2}$, where $h \geqq 3$ and $|G' \cap Z|_p = 1$, then $|A(G)|_p \geqq p^h$.*

https://doi.org/10.1017/S0017089500000902 Published online by Cambridge University Press

Proof. If $|G/Z|_p \geqq p^h$, the results holds. If $|G/Z|_p \leqq p^{h-2}$, then, by Lemma 3.4,

$$|G'|_p \leqq p^{(h-2)(h-1)/2} = p^{(h^2-3h+2)/2}$$

and $|G/G'|_p \geqq p^h$. Also

$$|Z|_p \geqq p^{(h^2-h+2)/2-(h-2)} = p^{(h^2-3h+6)/2} \geqq p^h$$

for integral values of h. Therefore

$$|A_c(G)|_p \geqq \min(|G/G'|_p, |Z|_p) \geqq p^h.$$

Finally, if $|G/Z|_p = p^{h-1}$, then, using the fact that $|G' \cap Z|_p = 1$, we obtain

$$|G'|_p = |G'/G' \cap Z|_p \leqq |GG'/Z|_p = |G/Z|_p = p^{h-1}.$$

Therefore

$$|G/G'|_p \geqq p^{(h^2-h+2)/2-(h-1)} = p^{(h^2-3h+4)/2} \geqq p^{h-1}$$

for integral values of h. Since $|G/Z|_p = p^{h-1}$, a similar argument shows that $|Z|_p \geqq p^{h-1}$, and we have

$$|A_c(G)|_p \geqq \min(|Z|_p, |G/G'|_p) \geqq p^{h-1}.$$

If $|A(G)|_p > |A_c(G)|_p$, we have the desired result. If $|A(G)|_p = |A_c(G)|_p$, we apply Lemma 2.4 and obtain $G = G_p \times G_{p'}$. If G_p is abelian, then the result follows, since $\frac{1}{2}(h^2-h) \geqq h$ for $h \geqq 3$. If G_p is non-abelian, then, by Lemma 3.1, there exists an outer automorphism of order a power of p which together with $I(G)$ generates a group with order divisible by p^h.

LEMMA 4.4. *Let H and K be abelian p-groups with $|H| = p^a$, $\exp(H) \leqq p^b$, $|K| = p^t$, and $t \leqq b$. Then $|\mathrm{Hom}(H,K)| \geqq p^B$, where $B = at/b$.*

Proof. Let $a = bq + r$, where $0 \leqq r < b$, let H_1 be a p-group of type $(p^{b(1)}, \ldots, p^{b(q)}, p^r)$ with $b(1) = \ldots = b(q) = b$, and let K_1 be cyclic of order p^t. Repeated application of Lemma 2.2 gives $|\mathrm{Hom}(H_1, K_1)| \leqq |\mathrm{Hom}(H,K)|$ but $|\mathrm{Hom}(H_1, K_1)| = p^A$, where $A = qt + \min(t, r)$. Now

$$at/b = (bq+r)t/b = qt + (rt)/b,$$

but neither r nor t exceeds b, so that $rt/b \leqq \min(t,r)$ and $A \geqq at/b$, which proves the result.

We are now prepared to prove our main result. We shall show that the least function $g(h)$, such that $|A(G)|_p \geqq p^h$ whenever $|G|_p \geqq p^{g(h)}$, satisfies the inequality $g(h) \leqq \frac{1}{2}(h^2-h+6)$. We know from previous results ([8] and [16]) that $g(1) = 2$ and $g(2) = 3$. We begin by showing that $g(3) = 5$. From Theorem 4.1, we know that $g(3) \geqq 5$. We must show that, if $|G|_p \geqq p^5$, then $|A(G)|_p \geqq p^3$. It will be sufficient to consider the case in which $|G/Z|_p \leqq p^2$. By Lemma 3.4, $|G'|_p \leqq p^3$ and so $|G/G'| \geqq p^2$. If G is purely non-abelian, then

$$|A_c(G)|_p = |\mathrm{Hom}(G/G', Z)|_p \geqq \min(|G/G'|_p, |Z|_p) \geqq p^2.$$

If the strict inequality holds, then we are done. Otherwise, we can apply Lemma 2.4 and write $G = G_p \times G_{p'}$, where G_p is a Sylow p-subgroup of G. This reduces the problem to the case of a p-group and, by Theorem 3.5, the result holds. If G is not PN, then we write $G = H \times K$, where H is abelian and K is PN. We now look at the different possibilities for

https://doi.org/10.1017/S0017089500000902 Published online by Cambridge University Press

$|H|_p$. The result follows immediately in each case except when $|H|_p = p$ and $|K|_p = p^4$. If $|K' \cap Z(K)|$ is divisible by p, then, by Lemma 4.2, we obtain

$$|A(G)|_p > |A(K)|_p \geqq p^2.$$

If $|K' \cap Z(K)|_p = 1$, then, applying Lemma 4.3, we have $|A(K)|_p \geqq p^3$. We now have the desired result, which is significant since it is best possible, and we state it as a theorem.

THEOREM 4.5. *If* $|G|_p \geqq p^5$, *then* $|A(G)|_p \geqq p^3$.

We note that this is in agreement with our general result, since $5 = g(3) \leqq \frac{1}{2}(3^2 - 3 + 6)$.

We now proceed to the general case. We shall need the following result, due to Howarth [**10**, Corollary 4.7, p. 168].

$$\exp(Z) \quad \text{divides} \quad |G/Z| \exp(G/G'). \tag{4.6}$$

We want to show that $|A(G)|_p \geqq p^h$ whenever

$$|G|_p \geqq p^{(h^2 - h + 6)/2}.$$

It is sufficient to consider the case in which $|G/Z|_p \leqq p^{h-1}$. In this case, $|Z|_p \geqq p^{(h^2 - 3h + 8)/2}$, and, by Lemma 3.4, $|G'|_p \leqq p^{(h^2 - h)/2}$, which implies that $|G/G'|_p \geqq p^3$. Let $|G/G'|_p = p^t \geqq p^3$; then, by (4.6),

$$\begin{aligned} \exp(Z)_p &\leqq |G/Z|_p \exp(G/G')_p \\ &\leqq p^{h-1} |G/G'|_p = p^{h-1+t}. \end{aligned}$$

Suppose now that G is purely non-abelian. If $t \geqq h$, then, since $|Z|_p \geqq p^h$, we have

$$|A_c(G)|_p = |\mathrm{Hom}(G/G', Z)|_p \geqq p^h.$$

Therefore we consider the case in which $t \leqq h - 1$. In this case we can apply Lemma 4.4 and get $|\mathrm{Hom}(G/G', Z)|_p \geqq p^B$ with

$$B \geqq \tfrac{1}{2}(h^2 - 3h + 8)t/(h - 1 + t) \quad (= C \text{ say}).$$

We can now show that $C \geqq h - 1$. This is equivalent to showing that

$$(t-2)h^2 + (4 - 5t)h + 10t - 2 \geqq 0.$$

The discriminant of the quadratic in h is $-15t^2 + 48t$, which is negative for $t \geqq 4$. Hence, for $t \geqq 4$, the above inequality holds. For $t = 3$, we have $h^2 - 11h + 28 \geqq 0$, which holds for $h > 6$ and $h = 4$. We must now examine separately the cases in which $5 \leqq h \leqq 6$ and $|G/G'|_p = p^3$. We wish to show that $|A_c(G)|_p \geqq p^{h-1}$. For $h = 5$, $|Z|_p \geqq p^9$ and, by (4.6),

$$\exp(Z)_p \leqq p^4 p^3 = p^7.$$

By Lemma 2.2,

$$|\mathrm{Hom}(G/G', Z)|_p \geqq |\mathrm{Hom}(C(p^7) \times C(p^2), C(p^3))| \geqq p^4.$$

For $h = 6$, $|Z|_p \geqq p^{13}$ and, by (4.6), $\exp(Z)_p \leqq p^5 p^3 = p^8$. By Lemma 2.2,

$$|\mathrm{Hom}(G/G', Z)|_p \geqq |\mathrm{Hom}(C(p^8) \times C(p^5), C(p^3))| \geqq p^5.$$

We now have $|A_c(G)|_p \geqq p^{h-1}$. If $|A(G)|_p > |A_c(G)|_p$, the desired result follows. Otherwise, we may apply Lemma 2.4, so that $G = G_p \times G_{p'}$. Since $|A(G)|_p \geqq |A(G_p)|_p$, we can apply Theorem 3.5 and Theorem 3.6, obtaining $|A(G)|_p \geqq p^h$, since $\frac{1}{2}(h^2-h+6)$ is greater than both $\frac{1}{2}(h^2-3h+6)$ and $h+1$.

Now suppose G has an abelian direct factor, and write $G = H \times K$, where H is abelian and K is purely non-abelian. Let $|H|_p = p^r$ and

$$|K|_p \geqq p^{(h^2-h+6)/2-r}.$$

If $r = 0$, then the problem reduces to the case previously considered. Also, if $r \geqq h+1$, then $|A(H)|_p \geqq p^h$, which gives the desired result. For $1 \leqq r \leqq h$, we shall consider two cases, $2 \leqq r \leqq h$ and $1 = r \leqq h$. Since the theorem is known to hold for $h \leqq 3$, we shall assume that $h > 3$. We know that $|A(H)|_p \geqq p^{r-1}$, and so we shall show that $|A(K)|_p \geqq p^{h-r+1}$. For $r > 2$ and $h \geqq r$, we can show that

$$2hr \geqq r^2+2h+r.$$

For $r = 2$ this inequality reduces to $h \geqq 3$. Therefore, for $2 \leqq r \leqq h$, the inequality holds, and from it we get

$$\tfrac{1}{2}(h^2-h+6)-r \geqq \tfrac{1}{2}\{(h-r+1)^2-(h-r+1)+6\},$$

which implies that

$$|K|_p \geqq p^{((h-r+1)^2-(h-r+1)+6)/2}.$$

From the proof of the first part of the theorem, we obtain

$$|A(K)|_p \geqq p^{h-r+1}.$$

Now suppose that $h \geqq r = 1$; then

$$|K|_p \geqq p^{\frac{1}{2}(h^2-h+6)-1} = p^{\frac{1}{2}(h^2-h+4)}.$$

Since $h \geqq 3$, we have

$$\tfrac{1}{2}(h^2-h+4) \geqq \tfrac{1}{2}\{(h-1)^2-(h-1)+6\}.$$

This gives $|A(K)|_p \geqq p^{h-1}$. If p divides $|Z(K) \cap K'|$, then, by Lemma 4.2, we get $|A(G)|_p > |A(K)|_p$, which gives the desired result. If $|Z(K) \cap K'|_p = 1$, then we apply Lemma 4.3 to obtain $|A(K)|_p \geqq p^h$. We have now considered all possible cases and have our main result.

THEOREM 4.7. *If* $|G|_p \geqq p^{(h^2-h+6)/2}$, *then* $|A(G)|_p \geqq p^h$.

REFERENCES

1. J. E. Adney, On the power of a prime dividing the order of a group of automorphisms, *Proc. Amer. Math. Soc.* **8** (1957), 627–633.

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

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

4. H. Fitting, Die Gruppe der zentralen Automorphismen einer Gruppe mit Hauptreihe, *Math. Ann.* **114** (1937), 355–372.

5. W. Gaschütz, Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen, *Journal of Algebra* **4** (1966), 1–2.

6. J. A. Green, On the number of automorphisms of a finite group, *Proc. Roy. Soc.* (A) **237** (1956), 574–581.

7. M. Hall, *The theory of groups* (New York, 1959).

8. I. N. Herstein and J. E. Adney, A note on the automorphism group of a finite group, *Amer. Math. Monthly* **59** (1952), 309–310.

9. H. Hilton, On the order of the group of automorphisms of an abelian group, *Messenger of Mathematics* II **38** (1909), 132–134.

10. J. C. Howarth, On the power of a prime dividing the order of the automorphism group of a finite group, *Proc. Glasgow Math. Assoc.* **4** (1960), 163–170.

11. W. Ledermann and B. H. Neumann, On the order of the automorphism group of a finite group II, *Proc. Roy. Soc.* (A) **235** (1956), 235–246.

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

13. A. Ranum, The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group, *Trans. Amer. Math. Soc.* **8** (1907), 71–91.

14. E. Schenkman, The existence of outer automorphisms of some nilpotent groups of class 2, *Proc. Amer. Math. Soc.* **6** (1955), 6–11.

15. I. Schur, Über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. reine angew. Math.* **127** (1904), 20–50.

16. W. R. Scott, On the order of the automorphism group of a finite group, *Proc. Amer. Math. Soc.* **5** (1954), 23–24.

17. J. Wiegold, Multiplicators and groups with finite central factor-groups, *Math. Zeit.* **89** (1965), 345–347.

WEBER STATE COLLEGE
OGDEN, UTAH, U.S.A.

https://doi.org/10.1017/S0017089500000902 Published online by Cambridge University Press