ON THE POWER OF A PRIME DIVIDING THE ORDER OF THE AUTOMORPHISM GROUP OF A FINITE GROUP

by J. C. HOWARTH

(Received 12 January, 1960)

1. Introduction. The existence of a function g of h having the property that p^h divides the order of the automorphism group of a finite group G whenever p^g divides the order of G was first established by Ledermann and Neumann [4], who showed that the least such function $g(h)$ satisfies the inequality

$$g(h) \leqslant (h-1)^3 p^{h-1} + h.$$

Later Green [2] improved this estimate to

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

In the present paper this will be revised, for sufficiently large h, to

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

The method will follow essentially the argument of Green, but a different lower bound will be used for the order of the group consisting of automorphisms of G which reduce to the identity on the factor group G/Z, where Z is the centre of the finite group G. In order to apply this bound to the problem in question, it was found necessary to treat separately various alternatives for the respective exponents of the groups Z and G/G', G' being the commutator subgroup of G.

2. Some results on finite Abelian groups. Continuing with the notation of Green, we denote by $\Gamma(G)$ the group of automorphisms of any group G, and by $\Gamma(G : H)$ and $\Gamma(G : G/K)$ the subgroups consisting of the automorphisms which reduce to the identity on a subgroup H and a factor group G/K respectively. The order of a group G we denote by $| G |$ and, for any prime p, $| G |_p$ is the highest power of p dividing $| G |$. Also we write G_p for a Sylow p-subgroup of G.

Automorphisms of an Abelian p-group A may readily be constructed by means of the following result (see Ranum [5] and Shoda [7]).

LEMMA 2.1. *For a given basis $a_1, \ldots, a_r$ of A, the mapping γ defined, for each i, by*

$$a_i\gamma = \sum_{j=1}^{r} \gamma_{ij} a_j$$

is an endomorphism of A provided that each element $a_i\gamma$ has order not exceeding that of a_i. An automorphism is obtained if and only if the coefficients γ_{ij} satisfy $\det(\gamma_{ij}) \not\equiv 0 \pmod{p}$.

Suppose that, for $i = 1, \ldots, k$, A has $r_i (\geqslant 1)$ generators of order $p^{n[i]}$, where $n[1] > \ldots > n[k] \geqslant 1$. Thus if there are $p^{N[i]}$ elements of A with order not greater than $p^{n[i]}$, then $N[i] = \sum_{j=1}^{k} r_j \,.\, \mu(n[i], n[j])$, where $\mu(s, t)$ denotes the minimum of any two integers s and t.

It was shown by Ranum [5] that

$$|\Gamma(A)| = \prod_{i=1}^{k}\left(p^{r_i N[i]}\prod_{j=1}^{r_i}(1-p^{-j})\right), \quad \text{.....(2.2)}$$

a fact which we use to construct a Sylow p-subgroup of $\Gamma(A)$.

Suppose now that A has invariants $(p^{n(1)}, \ldots, p^{n(r)})$, where $n(1) \geqslant \ldots \geqslant n(r)$, and let the basis element a_i have order $p^{n(i)}$. For each i, write $V_i = \{pa_1, \ldots, pa_i, a_{i+1}, \ldots, a_r\}$, with the convention that $V_0 = A$, and if A_i is the set of elements of A whose order does not exceed $p^{n(i)}$, let $A_i' = A_i \cap V_i$. Now choose an element b_i from each A_i' and consider the mapping θ of A into itself defined by

$$a_i\theta = a_i + b_i \quad (i = 1, \ldots, r). \quad \text{.....(2.3)}$$

By Lemma 2.1, θ is an automorphism of A. As each b_i ranges over a subgroup A_i', the set of all such automorphisms forms a group, which we denote by $\Delta(A)$.

LEMMA 2.4. *$\Delta(A)$ is a Sylow p-subgroup of $\Gamma(A)$.*

Proof. The order of $\Delta(A)$ is the product of the $|A_i'|$. Now fix i and let the integer $j\,(0 \leqslant j \leqslant i-1)$ be determined by the condition $n(j) > n(j+1) = \ldots = n(i)$ (with $j = 0$ if $n(i) = n(1)$). Since each of the elements $a_{j+1}, \ldots, a_i$ lies in A_i, we have $A_i + V_i = V_j$ and therefore

$$A_i/A_i' = A_i/A_i \cap V_i \cong (A_i + V_i)/V_i = V_j/V_i.$$

Hence, since $|V_j/V_i| = p^{i-j}$, $|A_i'| = p^{j-i}|A_i|$ and comparison with the formula (2.2) yields the result.

Note that, since $A_1 = A$, we have $|A_1'| = p^{-1}.|A|$ and therefore

$$|\Gamma(A)|_p \geqslant p^{-1}.|A|. \quad \text{.....(2.5)}$$

However, provided that the exponent of A is sufficiently small, a closer bound may be derived.

COROLLARY 2.6. *If A has order p^n and exponent $p^{n(1)}$ and if $2n(1) \leqslant n$, then*

$$|\Gamma(A)|_p \geqslant p^{2n-3}.$$

Proof. If $n(2) = n(1)$, then $|\Gamma(A)|_p \geqslant p^{n-1}.p^{n-2} = p^{2n-3}$. If $n(2) < n(1)$, then $n(3) \geqslant 1$ and, since $|A_1| = p^n$, $|A_2| = p^{n(2)+n-n(1)}$ and $|A_3| = p^{2n(3)+n-n(1)-n(2)}$,

$$|\Gamma(A)|_p \geqslant |A_1'|\,|A_2'|\,|A_3'| \geqslant p^{n-1}.p^{n(2)+n-n(1)-1}.p^{2n(3)+n-n(1)-n(2)-2}$$
$$= p^{3n-2n(1)+2n(3)-4} > p^{2n-3}.$$

We now introduce some inequalities concerning the quantity $L(s, t)$ which we define, for $1 \leqslant s \leqslant t \leqslant n$, to be the minimum number of elements of order not exceeding p^s in all Abelian groups of order p^n and exponent p^t. If $n = kt + d$, where $0 \leqslant d \leqslant t-1$, then it is easily verified that

$$L(s, t) = p^{ks+\mu(s,d)}, \quad \text{.....(2.7)}$$

$\mu(s, d)$ denoting the minimum of the integers s and d.

LEMMA 2.8. (i) *If $1 \leqslant s \leqslant t \leqslant t' \leqslant n$, then $L(s, t) \geqslant L(s, t')$.*

(ii) *For $1 \leqslant s \leqslant t \leqslant n-1$, $L(s, t) \leqslant L(s+1, t+1)$.*

Proof. In each case we employ the formula (2.7).

(i) If $n = kt + d = k't' + d'$ where $0 \leqslant d \leqslant t-1$ and $0 \leqslant d' \leqslant t'-1$, then, since $t' \geqslant t$,

we have $k' \leqslant k$. If $k' = k$, then $d' \leqslant d$ and so

$$k's + \mu(s, d') = ks + \mu(s, d') \leqslant ks + \mu(s, d).$$

Alternatively, if $k' < k$, then

$$k's + \mu(s, d') \leqslant (k-1)s + \mu(s, d') = ks + \mu(s, d') - s \leqslant ks + \mu(s, d).$$

(ii) Let $n = kt + d = k_1(t+1) + d_1$, where $0 \leqslant d \leqslant t-1$ and $0 \leqslant d_1 \leqslant t$; then, writing $E = ks + \mu(s, d)$ and $E_1 = k_1(s+1) + \mu(s+1, d_1)$, we establish the inequality $E \leqslant E_1$.

Consider first the case $k_1 = k \geqslant 1$. Then $d_1 = d - k$. Thus, if $d_1 \geqslant s$, then

$$\mu(s, d) \leqslant s \leqslant \mu(s+1, d_1).$$

If $d_1 \leqslant s$, then $E_1 = k(s+1) + d_1 = ks + d \geqslant E$.

On the other hand, if $k_1 < k$, then $t(k - k_1) = k_1 + d_1 - d > 0$; also, since $t \geqslant s$,

$$t(k - k_1) + s \geqslant s(k - k_1) + t.$$

Thus, for $d_1 \geqslant s$,

$$\begin{aligned} E_1 - E &\geqslant k_1(s+1) + s - ks - d = k_1 - s(k - k_1) + s - d \\ &\geqslant k_1 + (t - t(k + k_1) - s) + s - d = k_1 + t - (k_1 + d_1 - d) - d = t - d_1 \geqslant 0. \end{aligned}$$

Finally, if $d_1 \leqslant s$, then

$$\begin{aligned} E_1 - E &\geqslant k_1(s+1) + d_1 - ks - d = k_1 - s(k - k_1) + d_1 - d \\ &\geqslant k_1 + (t - t(k + k_1) - s) + d_1 - d = k_1 + t - (k_1 + d_1 - d) - s + d_1 - d = t - s \geqslant 0. \end{aligned}$$

3. Preliminary results concerning automorphisms. It is known that, for any prime p and finite Abelian group A with subgroups B and C,

$$| \Gamma(A : A/B) \cap \Gamma(A : C) |_p \geqslant | B_p | / p | C_p |, \quad \text{.....(3.1)}$$

(see [2]). In [2] Green also showed that if a finite group G has centre Z and commutator subgroup G', then, writing $\Pi = G/Z$, there exists an Abelian group Q containing Z as a subgroup, with $Q/Z \cong \Pi/\Pi'$, such that

$$\Gamma(G : G/Z) \cong \Gamma(Q : Q/Z) \cap \Gamma(Q : G' \cap Z) \quad \text{.....(3.2)}$$

and hence, by (3.1),

$$| \Gamma(G : G/Z) |_p \geqslant | Z_p | / p \,.\, | G' \cap Z_p |.$$

It will now be shown that

$$| \Gamma(G : G/Z) |_p \geqslant | \Gamma((Z/G' \cap Z)_p) |_p,$$

which, by (2.5), is a stronger result. We first quote a result which may easily be verified (cf. Hughes [3]).

LEMMA 3.3. *Let H and K be subgroups of G for which $G \supseteq H \supseteq G'$ and $Z \supseteq K$ and suppose that $w_1, \ldots, w_t$ are elements of G for which the $\overline{w}_i = w_i H$ form a basis of G/H. If elements k_i of K are chosen so that, for each i, the order of k_i divides the order of $\overline{w}_i$, (or equivalently that k_i is the image of $\overline{w}_i$ under some homomorphism from G/H to K), then the mapping*

$$\phi : \begin{cases} w_i\phi = w_i k_i, \\ h\phi = h \quad \text{for } h \in H \end{cases} \quad \text{.....(3.4)}$$

defines an endomorphism which reduces to the identity on both the groups G/K and H.

Since the endomorphism ϕ is the identity on H, we have

COROLLARY 3.5. *The mapping ϕ of* (3.4) *is an automorphism if and only if its restriction to the factor group G/H is an automorphism.*

Assuming now that both G/H and K are p-groups for some prime p dividing the order of G, automorphisms of G may be obtained by the following construction, similar to that used to obtain the group $\Delta(A)$ of Lemma 2.4.

Let $p^{q(1)}, \ldots, p^{q(t)}$, where $q(1) \geqslant \ldots \geqslant q(t)$, be the invariants of G/H. Choose elements g_i of G for which the cosets $\bar{g}_i = g_i H$ of order $p^{q(i)}$ form a basis of G/H. For each i, write $W_i = \{g_1^p, \ldots, g_i^p, g_{i+1}, \ldots, g_t, H\}$ and, if K_i is the group of all elements of K whose orders do not exceed $p^{q(i)}$, write $K_i' = K_i \cap W_i$. Now choose an element z_i from each K_i' and consider the mapping θ of G into itself defined by

$$\left.\begin{aligned} g_i\theta &= g_i z_i \quad (i = 1, \ldots, t), \\ h\theta &= h \qquad (\text{for } h \in H). \end{aligned}\right\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.6)$$

That θ is an automorphism may be established by observing that, in its restriction $\bar{\theta}$ to G/H (written additively), $\bar{g}_i\bar{\theta}$ takes the form $\theta_{i1}\bar{g}_1 + \ldots + \theta_{ii}\bar{g}_i$, where the coefficients $\theta_{i1}, \ldots, \theta_{i,i-1}$ are each divisible by p and $\theta_{ii} \equiv 1 \pmod{p}$, so that Corollary 3.5 and Lemma 2.1 may be applied.

LEMMA 3.7. *The mapping θ of* (3.6) *defines an automorphism of G which lies in*

$$\Gamma(G : G/K) \cap \Gamma(G : H).$$

Furthermore, the set of all such automorphisms forms a group.

The proof of this last fact amounts to no more than routine verification and is omitted.

COROLLARY 3.8. *If, for $i = 1, \ldots, t$, N_i denotes the number of elements of $K \subseteq Z_p$ which have order less than $p^{q(i)}$, then*

$$|\, \Gamma(G : G/Z) \,|_p \geqslant |\, \Gamma(G : G/K) \,|_p \geqslant N_1 \ldots N_t.$$

LEMMA 3.9. $|\, \Gamma(G : G/K) \cap \Gamma(G : H) \,|_p \geqslant |\, \Gamma(K/K \cap H) \,|_p$.

Proof. Choose a subgroup D of K isomorphic to $K/K \cap H$. If D has invariants $p^{n(1)}, \ldots, p^{n(r)}$, where $n(1) \geqslant \ldots \geqslant n(r)$, then, since D is isomorphic to KH/H, a subgroup of G/H, we have $r \leqslant t$ and, for each i,

$$n(i) \leqslant q(i). \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.10)$$

Also $D \subseteq K$ implies that $\Gamma(G : G/D) \cap \Gamma(G : H) \subseteq \Gamma(G : G/K) \cap \Gamma(G : H)$ and therefore, by Lemma 3.7,

$$|\, \Gamma(G : G/K) \cap \Gamma(G : H) \,|_p \geqslant \prod_{i=1}^{t} |\, E_i' \,|, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.11)$$

where $E_i' = E_i \cap W_i$, E_i being the subgroup consisting of those elements of D of order not exceeding $p^{q(i)}$. We now estimate $|\, E_i' \,|$ in terms of $|\, E_i \,|$. Fixing the suffix i in the range $1 \leqslant i \leqslant t$, let the integer $j\,(0 \leqslant j \leqslant i-1)$, be determined by the condition

$$q(j) > q(j+1) = \ldots = q(i)$$

(with $j = 0$ if $q(i) = q(1)$); then $E_i \subseteq W_j$ and

$$E_i/E_i' = E_i/E_i \cap W_i \cong E_iW_i/W_i \subseteq E_iW_j/W_i = W_j/W_i.$$

Hence, since $|W_j/W_i| = p^{i-j}$, $|E_i'| \geqslant p^{j-i}|E_i|$.

Choose a basis $d_1, \ldots, d_r$ of D, the element d_i having order $p^{n(i)}$. For i in the range $1 \leqslant i \leqslant r$, let D_i be the subgroup consisting of those elements of D whose order does not exceed $p^{n(i)}$. Writing $D_i' = D_i \cap \{d_1^p, \ldots, d_i^p, d_{i+1}, \ldots, d_r\}$, we have, by Lemma 2.4,

$$|\Gamma(D)|_p = \prod_{i=1}^{r} |D_i'|$$

and thus, by (3.11), to prove the lemma it is sufficient to establish that, for $1 \leqslant i \leqslant r$,

$$|E_i'| \leqslant |D_i'|.$$

The integer i remaining fixed, let $d_{k+1}(0 \leqslant k \leqslant i-1)$, be the first of the basis elements $d_1, \ldots, d_r$ to have order $p^{n(i)}$; then $|D_i'| = p^{k-i}|D_i|$. Suppose first that $q(i) = n(i)$. Then the integers k and j satisfy $k \leqslant j$; for if $k > j$, then $n(k) > n(i) = q(i) = q(k)$, contradicting (3.10). Hence, since $D_i = E_i$, $|D_i'| = p^{k-i}|D_i| \leqslant p^{j-i}|E_i| = |E_i'|$. On the other hand, if $q(i) > n(i)$, then $q(i) \geqslant n(i)+1$ and thus, since $|D_i| = p^{kn(i)+n(k+1)+\cdots+n(r)}$, we have $|E_i| \geqslant p^{k(n(i)+1)+n(k+1)+\cdots+n(r)} = p^k|D_i|$ and so

$$|E_i'| \geqslant p^{j-i}|E_i| \geqslant p^{j-i+k}|D_i| = p^j|D_i'| \geqslant |D_i'|.$$

COROLLARY 3.12. $|\Gamma(G : G/Z)|_p \geqslant |\Gamma((Z/G' \cap Z)_p)|_p$.

Proof. In the lemma, choose $K = Z_p$ and $H \supset G'$ such that

$$G/H \ (\cong (G/G')/(H/G')) \cong (G/G')_p.$$

Then $\Gamma(G : G/Z) \supseteq \Gamma(G : G/K) \cap \Gamma(G : H)$ and so $|\Gamma(G : G/Z)|_p$ is divisible by $|\Gamma(K/K \cap H)|_p$. But, since H/G' has order prime to p, $G' \cap K = H \cap K$ and hence

$$(Z/G' \cap Z)_p \cong Z_p/(G' \cap Z)_p = Z_p/G' \cap Z_p = K/G' \cap K = K/H \cap K.$$

Applying the lemma to any two subgroups B and C of a finite Abelian group A, we have, since $B_p/B_p \cap C_p \cong (B/B \cap C)_p$,

COROLLARY 3.13.

$$|\Gamma(A : A/B) \cap \Gamma(A : C)|_p \geqslant |\Gamma(A_p : A_p/B_p) \cap \Gamma(A_p : C_p)|_p \geqslant |\Gamma((B/B \cap C)_p)|_p.$$

It may be noted that, by (2.5), Corollary 3.13 is an improvement on the bound (3.1) and it is clear that, used in conjunction with (3.2), (3.13) would yield (3.12).

4. Schur's multiplicator. The multiplicator $M(\Pi)$ of a finite group Π may be defined as the second cohomology group of Π with coefficients in the additive group of real numbers modulo 1 (see Eilenberg and MacLane [1]). We shall however, in this paper, revert to the original definition of Schur [6] as follows.

Denote the elements of any group Π by $\alpha, \beta, \gamma, \ldots$. By a *factor set* on Π we mean a collection $\{m_{\lambda,\mu}\}$ of complex numbers of unit modulus, defined for each ordered pair (λ, μ) of elements of Π and satisfying, for all $\alpha, \beta, \gamma \in \Pi$, the relation

$$m_{\alpha,\beta}m_{\alpha\beta,\gamma} = m_{\alpha,\beta\gamma}m_{\beta,\gamma}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.1)$$

It is easily verified that if $\{n_{\lambda,\mu}\}$ is a second factor set and if, for each pair (λ, μ) of elements of Π, we define $q_{\lambda,\mu} = m_{\lambda,\mu}n_{\lambda,\mu}$, then $q_{\lambda,\mu}$ is also a factor set. Two factor sets $m_{\lambda,\mu}$ and $m'_{\lambda,\mu}$ are said to be *associated* if there exist complex numbers $y_\alpha, y_\beta, y_\gamma, \ldots$, indexed by elements of Π, such that, for each pair (λ, μ),

$$m'_{\lambda,\mu} = y_\lambda y_\mu y_{\lambda\mu}^{-1} \cdot m_{\lambda,\mu}.$$

It may be shown that associativity in this sense is an equivalence relation and that the product of two equivalence classes is formed unambiguously. Furthermore, the classes can be shown to form an Abelian group under multiplication, and it is this group which is defined to be the multiplicator of Π.

The following are results of Schur [6].

LEMMA 4.2. *If K is a subgroup contained in the centre of a group G, then, putting $\Pi = G/K$, $G' \cap K$ is isomorphic to a subgroup of $M(\Pi)$.*

LEMMA 4.3. *For any group Π, $M(\Pi)_p$ is isomorphic to a subgroup of $M(\Pi_p)$.*

Clearly the multiplicator of the identity is itself the identity group ; hence we have

COROLLARY 4.4. *$M(\Pi_p)$ is a p-group.*

An upper bound for the order of $M(\Pi)$ has been established (see Green [2]).

LEMMA 4.5. *If $|\Pi_p| = p^l$, then $|M(\Pi_p)| \leqslant p^{\frac{1}{2}l(l-1)}$.*

Concerning the exponent of the multiplicator, the next result is inherent in Schur's paper [6].

LEMMA 4.6. *The exponent of $M(\Pi)$ divides $|\Pi|$.*

Proof. In (4.1), let γ range over the whole group Π ; then, writing $|\Pi| = k$, we have

$$m_{\alpha,\beta}^k \prod_\gamma m_{\alpha\beta,\gamma} = \prod_\gamma m_{\alpha,\beta\gamma} \cdot \prod_\gamma m_{\beta,\gamma}.$$

Now, as γ ranges over Π, so also will $\beta\gamma$ and hence, if for any $\lambda \in \Pi$ we write $y_\lambda = \prod_\gamma m_{\lambda,\gamma}$, then

$$m_{\alpha,\beta}^k \cdot y_{\alpha\beta} = y_\alpha \cdot y_\beta.$$

This completes the proof.

COROLLARY 4.7. *Let a group G have centre Z and write $\Pi = G/Z$; then, if exponent is denoted by* exp,

$$\exp Z \text{ divides } |\Pi| \cdot \exp G/G'.$$

Proof. Clearly $\exp G/G'$ is divisible by $\exp Z/G' \cap Z$, which in turn is divisible by $\exp Z/\exp G' \cap Z$. Thus $\exp Z$ divides $\exp G/G' \cdot \exp G' \cap Z$ which, by Lemma 4.2, divides $\exp G/G' \cdot \exp M(\Pi)$. The result now follows on applying Lemma 4.6.

5. The lower bound.

THEOREM 5.1. *For $h \geqslant 12$, write*

$$f(h) = \begin{cases} \frac{1}{2}(h^2+3) & \text{for } h \text{ odd}, \\ \frac{1}{2}(h^2+4) & \text{for } h \text{ even}. \end{cases}$$

Then, if $p^{f(h)}$ divides the order of a group G, p^h divides the order of its automorphism group $\Gamma(G)$.

https://doi.org/10.1017/S2040618500034109 Published online by Cambridge University Press

Proof. Suppose first that for a fixed odd integer $h \geqslant 13$, $p^{\frac{1}{2}(h^2+3)}$ divides the order of a group G. Write $\Pi = G/Z$ and let $|\Pi|_p = p^k$. If $k \geqslant h$, then the order of the group of inner automorphisms is divisible by p^k and there is no more to prove. We therefore assume that $k \leqslant h-1$ or equivalently that $|Z|_p \geqslant p^n$, where $n = \frac{1}{2}(h^2-2h+5)$. Applying, in succession, Lemmas 4.2, 4.3 and 4.5, we have

$$|G' \cap Z|_p \leqslant |M(\Pi)|_p \leqslant |M(\Pi_p)| \leqslant p^{\frac{1}{2}k(k-1)} \leqslant p^{\frac{1}{2}(h-1)(h-2)},$$

and hence, since $|Z|_p \geqslant p^{\frac{1}{2}(h^2-2h+5)}$,

$$|Z/G' \cap Z|_p \geqslant p^{\frac{1}{2}(h+3)}.$$

We denote the exponents of the groups $(Z/G' \cap Z)_p$, Z_p and $(G/G')_p$ by p^s, p^t and p^m respectively.

Suppose first that $h \equiv 1 \pmod 4$. Then $\frac{1}{2}(h+3)$ is even and thus, if

$$\exp(Z/G' \cap Z)_p = p^s \leqslant p^{\frac{1}{2}(h+3)},$$

we have, by Corollaries 3.12 and 2.6,

$$|\Gamma(G : G/Z)|_p \geqslant |\Gamma((Z/G' \cap Z)_p)|_p \geqslant p^h.$$

On the other hand, if $s \geqslant \frac{1}{4}(h+3)+1 = \frac{1}{4}(h+7) = s'$, say, then $\exp Z_p = p^t \geqslant p^{s'}$ and $\exp(G/G')_p = p^m \geqslant p^{s'}$. Let there be p^M elements of Z_p whose orders do not exceed p^{m-1}; then, by Corollary 3.8, $|\Gamma(G : G/Z)|_p \geqslant p^M$.

Consider possible values for the exponent of Z_p. If $t \leqslant s'+h-1 = \frac{1}{4}(5h+3) = t'$, say, then, using the notation of Lemma 2.8 with $n = \frac{1}{2}(h^2-2h+5)$, we have

$$p^M \geqslant L(m-1, t) \geqslant L(s'-1, t').$$

On the other hand, if $t \geqslant t' = s'+h-1$, then, by Corollary 4.7, $m \geqslant t-h+1$ and so, by Lemma 2.8,

$$p^M \geqslant L(m-1, t) \geqslant L(t-h, t) \geqslant L(t'-h, t') \geqslant L(s'-1, t').$$

It is sufficient therefore to establish that $L(s'-1, t') \geqslant p^h$. Now $t' = \frac{1}{4}(5h+3)$ and, for $h \geqslant 13$,

$$4t' = 5h+3 \leqslant \tfrac{1}{2}(h^2-2h+5) = n$$

and hence, by (2.7), $L(s'-1, t') \geqslant p^{4(s'-1)} = p^{h+3}$.

If $h \equiv 3 \pmod 4$, then $\frac{1}{2}(h+1)$ is even and, as before, it follows that if $s \leqslant \frac{1}{4}(h+1)$, then $|\Gamma(G : G/Z)|_p \geqslant p^h$. Assuming therefore that $s \geqslant \frac{1}{4}(h+5) = s'$, then also $t \geqslant s'$ and $m \geqslant s'$. We again investigate the number p^M of elements of Z_p whose orders do not exceed p^{m-1}. Write $t' = s'+h-1$, that is $t' = \frac{1}{4}(5h+1)$. Then if $t \leqslant t'$, $p^M \geqslant L(m-1, t) \geqslant L(s'-1, t')$; and if $t \geqslant t'$, so that $m \geqslant t-h+1$,

$$p^M \geqslant L(m-1, t) \geqslant L(t-h, t) \geqslant L(t'-h, t') = L(s'-1, t').$$

For $h \geqslant 15$, $4t' \leqslant n$ and so, by Lemma 2.8, $p^M \geqslant p^{4(s'-1)} = p^{h+1}$. This completes the proof of the theorem when h is odd.

The proof of the case where h is even is of the same pattern and is omitted.

It may perhaps be remarked here that it is possible to show, by using a more detailed investigation, that the theorem remains valid for $h \geqslant 6$. Also, for large values of h, the bound may be reduced slightly; for example, though $f(12) = 74$, any group G with order divisible by p^{73} may be seen to have an automorphism group with order divisible by p^{12}.

REFERENCES

1. S. Eilenberg and S. MacLane, Cohomology theory in abstract groups I, *Ann. of Math.* **48** (1947), 51.

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

3. N. J. S. Hughes, The structure and order of the group of central automorphisms of a finite group, *Proc. London Math. Soc.* (2) **52** (1951), 377–385.

4. 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.

5. A. Ranum, The group of classes of congruent matrices and group of isomorphisms of any Abelian group, *Trans. Amer. Math. Soc.* **8** (1907), 71–91.

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

7. K. Shoda, Über die Automorphismen einer endlichen Abelschen Gruppe, *Math. Annalen* **100** (1928), 674–686.

THE UNIVERSITY
GLASGOW