AUTOMORPHISMS OF SOLVABLE GROUPS

J. L. ALPERIN[1]

1. **Introduction.** In a recent paper [6], G. Higman has studied the structure of nilpotent groups G which possess fixed-point free automorphisms of prime order. In fact, he showed, if the automorphism has order q, that the group G has class at most some bound which depends only on q. We shall examine a similar situation and prove

THEOREM 1. *To every prime p and integer n there exists an integer $t(p, n)$ such that if G is a finite solvable group and ϕ is an automorphism of G of order p leaving fixed exactly p^n elements of G, then the derived length of G is at most $t(p, n)$.*

From this theorem we shall be able to derive the following interesting application:

COROLLARY. *To every prime p there exists an integer $m(p)$ such that if G is a p-group of maximal class then the derived length of G is at most $m(p)$.*

It is important to note that in both these statements only the *existence* of integers $t(p, n)$ and $m(p)$ is claimed. The only specific information known is that $m(2) = 2$, $m(3) = 2$, and $m(5) = 3$ (see [1]). Even upper bounds for the values of $t(p, n)$ and $m(p)$ are not known to us. Also we note that the corollary is probably far from being a best possible result, in that the derived group G' of G may well have its *class* bounded by a function of p.

The proof of Theorem 1 is accomplished in two stages. First the theorem is proven in the special case that G is a p-group. This is done by examining the factors G_i/G_{i+1} of the lower central series of G. We determine a bound for the number of generators of the groups G_i/G_{i+1} and show the existence of a bound for the exponent of all but finitely many of these factor groups. From these facts the theorem will be proved in the special case. Finally, the general case is proved by use of the upper p-series of G.

2. **Notation. Lie rings.** Before proceeding with the proof we shall describe the notation and recall the definition of the Lie ring associated with a nilpotent group. If x and y are elements of a group G

Presented to the Society, January 24, 1961 under the title *p-automorphisms of solvable groups*; received by the editors February 16, 1961.

[1] National Science Foundation Predoctoral Fellow.

then we denote $(x, y) = x^{-1}y^{-1}xy$ and if H and K are subgroups of G then (H, K) denotes the subgroup of G generated by all elements (h, k) for $h \in H$ and $k \in K$. By recursion we define $(x_1, \cdots, x_n) = ((x_1, \cdots, x_{n-1}), x_n)$ and $(H_1, \cdots, H_n) = ((H_1, \cdots, H_{n-1}), H_n)$ for elements $x_1, \cdots, x_n$ and subgroups $H_1, \cdots, H_n$ of G. The lower central series of G is defined by $G_1 = G$, $G_2 = (G, G)$ and $G_{n+1} = (G_n, G)$; the derived series of G by $G^{(0)} = G$ and $G^{(n+1)} = (G^{(n)}, G^{(n)})$. The upper central series of G is defined inductively by $Z_0 = 1$ and Z_{n+1} as the subgroup of G corresponding to the center of G/Z_n. Finally, the Frattini subgroup of G, which is the intersection of the maximal subgroups of G, is denoted by $\Phi(G)$.

The following commutator identity will be very useful:

$$(xy, z) = (x, z)(x, z, y)(y, z).$$

This may be proven by a direct calculation. We shall need to use the consequence that if $z \in G$ and (w, z) is central in G for all $w \in G$ then the map sending w to (w, z) is a homomorphism.

If G is a nilpotent group then one can construct, in a canonical way, a Lie ring L associated with G (e.g. [2, pp. 328–329]). The additive group of L is the direct sum of the abelian groups $F_i = G_i/G_{i+1}$, $i = 1, 2, \cdots$. An element gG_{i+1} of F_i and an element hG_{j+1} of F_j are multiplied by the rule

$$gG_{i+1}hG_{j+1} = (g, h)G_{i+j+1}$$

which is an element of F_{i+j} and well defined because $(G_i, G_j) \subseteq G_{i+j}$ [3]. This multiplication is extended to L by the distributive laws and makes L into a Lie ring. If ϕ is an automorphism of G then it induces automorphisms on the factors F_i of the lower central series of G. From these automorphisms, in the obvious fashion, an automorphism $\bar{\phi}$ of L may be defined.

3. **Generators.** We now begin the proof of Theorem 1 in the case that G is a p-group. This and the next section will study the factors of the lower central series of G. First we require the following lemmas, the first of which will also be applied elsewhere in this paper.

LEMMA 1. *Let ϕ and G be as in Theorem 1 and let G be a p-group. If K and L are subgroups of G and L is normal in K and K and L are invariant under ϕ then the automorphism induced by ϕ on K/L has at most p^n fixed elements.*

PROOF. To prove this statement we may assume $K = G$ and proceed by induction on the order of L. Let H be the splitting extension of G by ϕ. Suppose first that L has order p so L is normal in H and hence central in H. If ϕ has more than p^n fixed elements in G/L then

choose a subgroup M of G containing L such that M has order p^{n+2} and ϕ leaves fixed each element of M/L. In H, the map of M into L sending $m \in M$ to (m, ϕ) is a homomorphism because L is a central subgroup of H. The kernel M_1 of this map is of order at least p^{n+1} and consists of elements left fixed by ϕ. This is a contradiction and ϕ has at most p^n fixed elements in G/L.

If L has order greater than p then since L is normal in H we can find a ϕ-invariant subgroup L_1 of L normal in G and of index p in L. By induction, ϕ leaves fixed at most p^n elements of G/L_1 and so by the preceding paragraph we are done.

LEMMA 2. *Let X be an elementary abelian p-group and ψ an automorphism of X of order p leaving fixed at most p^n elements of X. Then X is of order at most p^{np}.*

PROOF. Let Y be the splitting extension of X by ψ. Lemma 1 implies that every factor of the upper central series of Y, save the last one, has order at most p^n, and that the last factor has order at most p^{n+1}. To obtain a proof of this lemma it will be enough to show that Y has class at most p. But it is easily shown by induction on m, a positive integer, that if $x \in X$, then

$$(x, \psi^m) = (x, \psi)^{C_{m,1}}(x, \psi, \psi)^{C_{m,2}} \cdots (x, \psi, \cdots, \psi)^{C_{m,m}},$$

where the $C_{m,r}$ are binomial coefficients. If $m = p$ this equation becomes

$$1 = (x, \psi, \cdots, \psi) \quad (\psi \text{ taken } p \text{ times})$$

because each of the binomial coefficients $C_{p,s}$ for $1 \leqq s < p$ is divisible by p. But any other commutator of weight $p+1$ in ψ and elements of X is equal to 1 since X is abelian, so Y has class at most p.

Since the number of generators of a p-group K is d if and only if $K/\Phi(K)$ has order p^d we finally obtain from the previous lemmas

LEMMA 3. *Let ϕ and G be as in Theorem 1 and let G be a p-group. Then any ϕ-invariant subgroup of G has at most np generators. In particular, G_i is ϕ-invariant, $i \geqq 1$, so G_i/G_{i+1} has at most np generators.*

4. Higman's theorem. Exponent. The description of the exponent of the factors G_i/G_{i+1} involves the use of Lie rings. The starting place is the

THEOREM 2 (G. HIGMAN [6]). *To each prime p corresponds an integer $k(p)$ such that if a Lie ring L has an automorphism of order p which leaves fixed no elements except zero, then L is nilpotent of class at most $k(p)-1$.*[2]

[2] For convenience, this $k(p)$ is one less than the $k(p)$ of [6].

However, as we shall argue below, the proof of this theorem, with only entirely trivial changes, gives much more, in fact it gives

THEOREM 3. *To each prime p corresponds an integer $k(p)$ such that if a Lie ring L has an automorphism of order p, all of whose fixed elements lie in an ideal I of L, then $(pL)^{k(p)} \subseteq I$.*

Before discussing the proof of Theorem 3 let us show how this theorem contributes to the proof of Theorem 1. We in fact obtain

LEMMA 4. *Let ϕ and G be as in Theorem 1 and let G be a p-group. Then, if $i \geqq k(p)$, G_i/G_{i+1} has exponent at most $p^{k(p)+n}$.*

PROOF. Let L be the Lie ring of G and $\bar{\phi}$ the automorphism of L corresponding to ϕ. Lemma 1 of the previous section shows that the automorphism ϕ induces on each G_i/G_{i+1} has at most p^n fixed elements, for each $i \geqq 1$. Hence, the fixed elements of $\bar{\phi}$ all lie in the ideal I of elements of L of order at most p^n. We may now apply Theorem 3 and obtain, since $p^n I = 0$, that $p^{k(p)+n} L^{k(p)} = 0$, or $L^{k(p)}$ has exponent at most $p^{k(p)+n}$. But $L^{k(p)}$ is the direct sum of the groups G_i/G_{i+1} for $i \geqq k(p)$ so each of these factor groups has exponent at most $p^{k(p)+n}$ and the lemma is proved.

The first step of the proof of Theorem 3 is to consider the ring L as an algebra over the integers and extend L to an algebra $M = Z(\omega) \otimes L$ over the ring $Z(\omega)$ where $Z(\omega)$ is the ring obtained by adjoining to Z a primitive pth root of unity ω. Let $J = Z(\omega) \otimes I$ be the ideal of M obtained by extension of the ideal I of L. To each element x of L and each integer i, $0 \leqq i \leqq p-1$, is defined

$$x_i = x + \omega^{-i} x\sigma + \cdots + \omega^{-(p-1)} x\sigma^{p-1}$$

where σ is the automorphism mentioned in the theorem. Since $px = x_0 + x_1 + \cdots + x_{p-1}$ the subring S of M generated by all the elements x_i contains pL. Furthermore, S is invariant under σ since $x_i\sigma = (x\sigma)_i$ and the fixed points of S under σ lie in the ideal $J_1 = J \cap S$ of S. We are reduced now to the following situation: σ is an automorphism of order p of a Lie ring S which is generated by elements y such that $y = \omega^i y$ for various integers i. We now wish to prove that $S^{k(p)} \subseteq J_1$. From this will follow $(pL)^{k(p)} \subseteq I$ since $J_1 \cap pL = I \cap pL$. But the remainder of the proof of Theorem 2 [6, p. 328] suffices for this, provided only that the equations of that proof are replaced by congruences modulo the ideal J_1.

5. **Proof of Theorem 1.** If the group G of Theorem 1 is a p-group then Lemmas 3 and 4 tell us that G_i/G_{i+1} has order at most p^s, where

$s=np(k(p)+n)$, provided $i\geqq k(p)$. However $H=G_{s+1}$ and ϕ also satisfy the hypotheses of the theorem; consequently, the factors H_i/H_{i+1} of the lower central series of H, for $i\geqq k(p)$, also have order at most p^s. But a theorem of P. Hall [2, Theorem 2.56] states that the factors of the lower central series of $H=G_{s+1}$, save perhaps the last one, all have order at least p^{s+1}. Hence $H_{k(p)+1}=1$, and this proves Theorem 1 when G is a p-group, because G is an extension of H by G/H and H and G/H each have class at most a certain function of p and n.

We now proceed with the proof of the general case. However, we shall prove the theorem restated in the following form, which is easily seen to be equivalent by use of splitting extensions:

THEOREM 1. *If G is a finite solvable group and x is an element of G of prime order p and the centralizer of x is of order p^n then the derived length of G is bounded by a function of p and n.*

PROOF. Let N be the largest normal p'-subgroup[3] of G. Then the element x induces a fixed-point free automorphism of N so that N is nilpotent and of class at most a bound depending only on p [6]. If P is a p-Sylow subgroup of G containing the centralizer of x then the natural map of P onto PN/N is an isomorphism because N consists of elements of order prime to p. Hence, the centralizer of xN in PN/N is of order p^n, so that if P^*/N is the greatest normal p-subgroup[4] of G/N then xN induces in P^*/N an automorphism of order p which leaves fixed at most p^n elements. Since Theorem 1 has been proved for p-groups we have as a consequence that P^*/N has derived length at most a bound which depends only on p and n.

We shall conclude this proof by demonstrating that G/P^* has order at most a certain function of p and n. Let C/N be a p-complement of G/N [4]. Since P^*/N is self-centralizing in G/N [5], C/N may be regarded as a group of automorphisms of P^*/N. However, since C/N has order prime to p, C/N is faithfully represented by the automorphisms induced on $F=(P^*/N)/\Phi(P^*/N)$ [3]. But Lemma 3 shows that F has order at most p^{np} so the order of C/N is at most $p^{np}!$. Similarly, a p-Sylow subgroup of G/P^* may be considered as a group of automorphisms of the greatest normal p'-subgroup of G/P^* and so has a bounded order. Thus we have described a bound for the order of G/P^*, namely the product of $p^{np}!$ and $(p^{np}!)!$, and the theorem is proved.

---

[3] A p'-subgroup is a subgroup all of whose elements have order prime to p.

[4] A p-subgroup is a subgroup of order a power of p.

6. **Groups of maximal class.** We are now in a position to prove the corollary stated in the first section. Recall [1] that a p-group G is said to be of maximal class if G/G_2 is of order p^2 and all other factors of the lower central series of G are of order p. In such a group $\gamma_1(G)$ is defined to be that subgroup of G consisting of all $g \in G$ such that $(g, G_2) \subseteq G_4$. Then $\gamma_1(G)$ is a characteristic subgroup of G of index p in G. Define $\gamma_i(G) = G_i$ if $i > 1$. G is said to have degree of commutativity $k \geqq 0$ if $(\gamma_i(G), \gamma_j(G)) \subseteq \gamma_{i+j+k}(G)$ for all i and j positive integers. If G has class greater than p then G has a positive degree of commutativity [1, p. 73]. In that case choose $s \in G$, $s \notin \gamma_1(G)$ and $s_1 \in \gamma_1(G)$, $s_1 \notin \gamma_2(G)$. Define, inductively, $s_{i+1} = (s_i, s)$. Then $\gamma_i(G)$ is generated by s_i and $\gamma_{i+1}(G)$, so that every element x of $\gamma_1(G)$ can be uniquely expressed as

$$x = s_1^{a_1} s_2^{a_2} \cdots s_c^{a_c}, \qquad 0 \leqq a_i < p,$$

where G has class c. Therefore

$$s^{-1} x s = s_1^{a_1} s_2^{a_1+a_2} \cdots s_c^{a_{c-1}+a_c}.$$

so s leaves fixed only p elements of $\gamma_1(G)$. In fact s commutes only with central elements of G so s^p is central and the inner automorphism given by s has order p. Theorem 1 now implies that $\gamma_1(G)$ has derived length at most a bound determined by p so the same is true for G since $\gamma_1(G) \supseteq G'$.

In closing, the author should like to express his appreciation for the advice and criticism of Professor G. Higman.

References

1. N. Blackburn, *On a special class of p-groups*, Acta. Math. **100** (1958), 45–92.

2. M. Hall, *The theory of groups*, Macmillan, New York, 1959.

3. P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. **36** (1934), 29–95.

4. ———, *A note on soluble groups*, J. London Math. Soc. **3** (1928), 98–105.

5. P. Hall and G. Higman, *On the p-length of p-soluble groups*, Proc. London Math. Soc. (3) **6** (1956), 1–42.

6. G. Higman, *Groups and rings having automorphisms without non-trivial fixed elements*, J. London Math. Soc. **32** (1957), 321–324.

University of Chicago