ISRAEL JOURNAL OF MATHEMATICS 82 (1993), 395–404

AUTOMORPHISMS OF FINITE GROUPS OF BOUNDED RANK

BY

ANER SHALEV

Department of Mathematics
The Hebrew University of Jerusalem, Jerusalem 91904, Israel

To Professor John Thompson, in honor of his outstanding achievements

ABSTRACT

Let G be a finite group admitting an automorphism α with m fixed points. Suppose every subgroup of G is r-generated. It is shown that (1) G has a characteristic soluble subgroup H whose index is bounded in terms of m and r, and (2) if the orders of α and G are coprime, then the derived length of H is also bounded in terms of m and r.

1. Introduction

This paper is devoted to the study of certain finite groups admitting automorphisms with few fixed points. Some of the group-theoretic problems will be reduced to Lie-theoretic ones, which in turn may be tackled using "linear" methods. There is extensive literature on the subject, originating with Higman's and Thompson's fundamental papers [H], [Th]. The reader is referred to Hartley's survey paper [H1] and its reference list. See also [Kh],[M],[Sh]. In contrast with classical results, which deal with automorphisms α of a given (often prime) order, we shall try (not always successfully) to avoid any reference to the order of α in our results. Instead, the rank of the finite group G — or the Lie ring L — will play a key role. Here the rank of G (denoted by $rk(G)$) is defined to be the minimal integer r such that every subgroup of G is r-generated, and the rank of L is the rank of its additive group. Our aim is to show that, if a finite group G of

Received June 1, 1992

bounded rank admits an automorphism with boundedly many fixed points, then it possesses a soluble subgroup H whose index and derived length are bounded.

An automorphism is called **fixed-point-free** if it does not have a non-trivial fixed point. An automorphism of a Lie ring of finite rank is called **semisimple** if it can be represented by a diagonal matrix (over a suitable integral extension of the integers $\mathbb{Z}$). The derived length of a soluble group (or Lie ring) G is denoted by $dl(G)$.

PROPOSITION: *Let L be a Lie ring of finite rank admitting a semisimple fixed-point-free automorphism α with d distinct eigenvalues. Then L is soluble of derived length at most $2^{d-1}-1$. In particular $dl(L) \leq 2^{r-1}-1$, where $r = rk(L)$.*

This result is closely related to Kreknin's Theorem [Kr], showing that a Lie ring with a fixed-point-free automorphism of order n is soluble of derived length at most $2^n - 2$.

Our main result (part of which applies to the above Proposition) deals with finite groups of bounded rank admitting an automorphism with few fixed points. Throughout this paper we say that a certain invariant is $m, n \ldots$-bounded if it is bounded above by some function of $m, n, \ldots$.

THEOREM: *Let G be a finite group of rank r admitting an automorphism α with m fixed points. Then G has a characteristic soluble subgroup H whose index is m, r-bounded. Moreover, if $(|\alpha|, |G|) = 1$ then the derived length of H is also m, r-bounded.*

It has been shown in [Sh, Corollary D] that the derived length of a finite soluble group of rank r admitting an automorphism α of order n with m fixed points is n, m, r-bounded. We see that, in a coprime situation, our Theorem provides a bound which is independent of n. I have not been able to decide whether the coprimeness assumption in the Theorem is really essential.

The proof of the above result applies the classification of finite simple groups, the theory of powerful p-groups [LM], as well as some Lie-theoretic arguments. There are two ingredients which deserve particular attention. The first is a recent theorem of Hartley [H2], generalizing the classical Brauer–Fowler Theorem. It states that there are only finitely many simple groups admitting an automorphism α of a given order with a given number of fixed points. The second is the use of a Lie ring, constructed from certain p-groups P, which may be regarded as a finite analog of Lazard's Lie algebra of a p-adic Lie group [L]. As shown in [Sh],

this Lie ring reflects the structure of P more closely than the graded Lie ring used by Higman and others, and may therefore give rise to some new reductions of group-theoretic problems to Lie-theoretic ones. I am grateful to Brian Hartley for stimulating conversations and for his proof of Lemma 3.1 below.

Some words on the structure of this paper.

The Proposition is proved in section 2. Section 3 deals with solubility results, and contains the proof of the first part of the Theorem. In section 4 we briefly discuss the construction of a "p-adic" Lie ring associated with a "uniform" p-group, and apply it in the proof of the second part of the Theorem, starting with the fixed-point-free case. The proof is then completed in section 5.

Notation is standard. The derived series of a group G is denoted by $\{G^{(i)}\}_{i\geq 0}$ and G' stands for the commutator subgroup $G^{(1)}$. A similar notation will be used for Lie rings. Lie products of length greater than 2 will be interpreted using the left-normed convention. $\phi(G)$ denotes the Frattini subgroup of a group G, and G^p stands for the subgroup generated by all pth powers in G. A simple group will be understood to be non-abelian. $[x]$ and $\lceil x \rceil$ denote the lower and upper integral parts of a real number x.

2. Lie ring automorphisms

Definition 2.1: Let S be a set of complex numbers. A linear ordering $<$ on S will be called **good** if there are no $x, y \in S$ such that $xy \in S$ and $x < xy < y$.

LEMMA 2.2: *The complex numbers admit a good ordering.*

Proof: We first claim that the unit circle $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ admits a good ordering. Indeed, given $z = e^{\theta i}, z' = e^{\theta' i}$ $(0 \leq \theta, \theta' < 2\pi)$, define $z < z'$ if $\theta < \theta'$. Then $zz' > z, z'$ if $\theta + \theta' < 2\pi$, and $zz' < z, z'$ otherwise, so $<$ is a good ordering.

Now, it is easy to see that the multiplicative group $\mathbb{C}^*$ is isomorphic to S^1 (as an abstract group). Hence $\mathbb{C}^*$ — and therefore $\mathbb{C}$ as well — admits a good ordering. ∎

Remark: Most groups do not admit a good ordering. A typical example is the elementary abelian p-group $C_p \times C_p$. However, if G is an abelian group whose cardinality is at most the continuum and whose torsion part is locally cyclic, then G admits a good ordering. This is because it can be embedded in $\mathbb{C}^*$.

Definition 2.3: Let S be a finite set of complex numbers. We say that a Lie ring L is S-**graded** if its additive group can be decomposed as $L = \bigoplus_{x \in S} L_x$, and, for $x, y \in S$ we have $[L_x, L_y] \leq L_{xy}$. It is understood that $L_x = 0$ whenever x is not in S.

The following result is proved using a slight modification of Kreknin's method [Kr].

PROPOSITION 2.4: *Let L be an S-graded Lie ring, where S is a finite set of complex numbers not including* 1. *Then L is soluble. Moreover, if $|S| = d$ then $dl(L) \leq 2^{d-1} - 1$.*

Proof: Choose a good ordering on S, and label the elements of S such that $x_1 < x_2 < \ldots < x_d$. Then $L = \bigoplus_{i=1}^{d} L_{x_i}$. For simplicity, define $L_i = L_{x_i}$. For $1 \leq k \leq d$ let H_k be the subring generated by $L_{k+1}, \ldots, L_d$. Note that $H_d = 0$.

Claim:

(1) $L^{(2^{k-1})} \cap L_k \subseteq H_k \quad (1 \leq k \leq d)$.

(2) $L^{(2^k-1)} \subseteq H_k \qquad (1 \leq k \leq d)$.

We prove (1) and (2) simultaneously, by induction on k. Suppose $k = 1$. We have to show that $L' \subseteq H_1$. It suffices to prove that $[L_i, L_j] \subseteq H_1$ for all i, j. This is obvious if $x_i x_j \neq x_1$, so suppose $x_i x_j = x_1$. Since $1 \notin S$ it follows that $x_i, x_j \neq x_1$, so that $i, j \geq 2$, and $[L_i, L_j] \subseteq H_1$.

Suppose now that $k > 1$. The induction hypothesis for (2) yields

$$L^{(2^{k-1}-1)} \subseteq H_{k-1}$$

so that

$$L^{(2^{k-1})} \subseteq (H_{k-1})'.$$

To prove (1) it therefore suffices to show that

$$(H_{k-1})' \cap L_k \subseteq H_k.$$

Let $a, b \in H_{k-1}$ be homogeneous elements with $h := [a, b] \in L_k$. We have to show that $h \in H_k$. We may assume that $b = [b_1, \ldots, b_m]$ where $m \geq 1$ and $b_i \in L_{n_i}$ for some $n_1, \ldots, n_m \geq k$. Then h is a linear combination of elements of the form $[a, b_{\sigma(1)}, \ldots, b_{\sigma(m)}]$ for permutations $\sigma \in Sym(m)$. It therefore suffices to show that all these elements lie in H_k. Clearly, we may assume that σ is the

identity permutation, and consider the element $g := [a, b_1, \ldots, b_m] = [c, b_m]$ where $c := [a, b_1, \ldots, b_{m-1}]$. Suppose $c \in L_i$ and $b_m \in L_j$ (so that $j = n_m$). Recall that $h \in L_k$, so that $g \in L_k$ as well. Thus $x_i x_j = x_k$. We know that $j \geq k$, and since $x_i \neq 1$ we have $j > k$. It is also clear that $i \neq k$. We claim that $i > k$. For otherwise $i < k$, so $x_i < x_k = x_i x_j < x_j$, contradicting the assumption that $<$ is a good ordering. We conclude that $g = [c, b_m] \in [L_i, L_j] \subseteq H_k$. This proves (1).

To prove (2), consider $M := L^{(2^{k-1})}$ as an S-graded Lie ring. Apply (2) for M with $k-1$ to obtain

$$M^{(2^{k-1}-1)} \subseteq \langle M \cap L_k, \ldots, M \cap L_d \rangle \subseteq \langle M \cap L_k, H_k \rangle.$$

Now, condition (1) for L and k yields $M \cap L_k \subseteq H_k$. Therefore

$$M^{(2^{k-1}-1)} \subseteq H_k.$$

Since $L^{(2^k-1)} = M^{(2^{k-1}-1)}$ the result follows. ∎

Now, given a fixed-point-free semisimple automorphism of a Lie ring L, let $x_1, \ldots, x_d$ be its eigenvalues in a suitable integral extension R of $\mathbb{Z}$. Then $x_i \neq 1$ for all i. We see that $L \otimes_{\mathbb{Z}} R$ is S-graded where $S = \{x_1, \ldots, x_d\}$, which may be considered as a subset of $\mathbb{C}$. Proposition 2.4 may therefore be applied. It follows that $L (\subseteq L \otimes R)$ is soluble of derived length $\leq 2^{d-1} - 1$. This proves the Proposition.

3. The existence of a large soluble subgroup

The following result, whose proof is due to Brian Hartley, is rather useful for our purpose.

LEMMA 3.1: *Let $S = L(n, F)$ be a simple group of Lie type, where $F = F_{p^b}$ and n is the Lie rank. Suppose S admits an automorphism α with m fixed points. Then the order of S is b, m, n-bounded.*

Proof: By the structure of the automorphism group of S (see, e.g., [C]) we see that the order of $Out(S)$ is b, n-bounded. In particular $\alpha^e \in S$ (which we identify with $Inn(S)$) for some e which is b, n-bounded. It follows that $\langle \alpha^e \rangle \subseteq C_S(\alpha)$, so $\alpha^{em} = 1$ (as $|C_S(\alpha)| = m$). Hence the order of α is b, m, n-bounded. By a recent result of Hartley [H2, Theorem A′] there is a bound to the order of a simple

group admitting an automorphism of a given order with a given number of fixed points. It therefore follows that the order of G is b, m, n-bounded. ∎

We can now prove:

PROPOSITION 3.2: *Let G be a finite group of rank r admitting an automorphism α with m fixed points. Then G has a soluble characteristic subgroup H whose index is m, r-bounded.*

Proof: Let M be a characteristic section of G which is characteristically simple. Suppose M is non-abelian. Then it is the direct product of isomorphic simple groups $S_i (1 \leq i \leq k)$. Since $rk(G) = r$ we have $k \leq r$. Now, the automorphism α acts on the section M with at most m fixed points; this follows from [HB, p.361]. Let $i \geq 1$ be the minimal integer such that $S_1^{\alpha^i} = S_1$. Then $K := S_1 \times S_1^{\alpha} \times \cdots \times S_1^{\alpha^{i-1}}$ is an α-invariant subgroup of M. Note that, if $s \in C_{S_1}(\alpha^i)$, then $ss^{\alpha} \cdots s^{\alpha^{i-1}} \in C_K(\alpha)$. Hence $|C_{S_1}(\alpha^i)| \leq |C_K(\alpha)| \leq m$. We conclude that S_1 is a simple group of rank at most r admitting an automorphism with at most m fixed points. Applying the classification we see that, either $|S_1|$ is bounded, or S_1 is of Lie type, say $S_1 = L(n, F)$ where $F = F_{p^b}$ for some b. Since $rk(S_1) \leq r$ we easily see that b and n are r-bounded. But $|S_1|$ is b, m, n-bounded, by Lemma 3.1. We conclude that, in either case, $|S_1|$ is m, r-bounded. It follows that $|M|$ is m, r-bounded, for any non-abelian characteristic section M which is characteristically simple.

Given such a section M, consider $C_G(M)$. Then $G/C_G(M) \leq Aut(M)$, so the index of $C_G(M)$ is m, r-bounded. Since G is r-generated, its number of subgroups of index $\leq i$ is r, i-bounded. Therefore the number of possibilities for $C_G(M)$ is m, r-bounded. Let $H := \cap C_G(M)$ where M ranges over all (characteristic) non-abelian characteristically simple sections of G. The above discussion shows that $(G : H)$ is m, r-bounded. Finally, since every characteristic section of H which is characteristically simple is abelian, H must be soluble. ∎

This proves the first part of the Theorem.

4. A bound on the derived length: the fixed-point-free case

Let G be a finite soluble group of rank r admitting an automorphism α with m fixed points. Our goal is to show that the derived length of G is bounded, provided that the order of α is coprime to the order of G. In this section we focus on the case $m = 1$, leaving the general case to the next section.

The main idea behind the proof is a reduction to a Lie-theoretic problem, which is then solved by applying the Proposition. The reduction is based on a construction of a Lie ring from a certain type of p-group, which is called **uniform**. A detailed account of this process is given in [Sh, Sec. 3] (see also [DDMS, Chapter 4]). Here we briefly discuss the major points, for the benefit of the reader.

Let p be a fixed prime. For simplicity we assume that p is odd.

Definition 4.1:

(1) A finite p-group P is called **powerful** if P/P^p is abelian.

(2) A powerful p-group G is called **uniform** if the order of $P^{p^i}/P^{p^{i+1}}$ does not depend on i, as long as $P^{p^i} \neq 1$.

For an extensive study of powerful p-groups and their important role in the theory of p-adic Lie groups, see Chapters 2–4 of the recent book [DDMS].

Now let P be a uniform p-group of rank r and exponent p^e, and let $i \leq e/4$. Then $L_i := P^{p^i}/P^{p^{2i}}$ and $M_i := P^{p^{2i}}/P^{p^{3i}}$ are homocyclic abelian groups of rank r. The map $x \mapsto x^{p^i}$ induces an isomorphism $q : L_i \xrightarrow{\sim} M_i$. The commutator operation $x, y \mapsto x^{-1}y^{-1}xy$ induces a well-defined bilinear map $c : L_i \times L_i \longrightarrow M_i$. Pulling the values of this map back to L_i we obtain a bilinear map $[\ ,\ ] : L_i \times L_i \longrightarrow L_i$ defined by $[x, y] = q^{-1}(c(x, y))$. This product, together with the natural additive structure, turns L_i into a Lie ring.

Definition 4.2: A Lie ring L will be called **uniform** if it is a finitely generated free $\mathbb{Z}/p^i\mathbb{Z}$-module for some i, and L/pL is a commutative Lie algebra.

The Lie ring L_i just constructed turns out to be uniform. Its rank coincides with that of P. It is clear that any automorphism α of P induces a Lie automorphism on L_i in such a way that $|C_{L_i}(\alpha)| \leq |C_P(\alpha)|$. Not obvious, but still true, is the following fact.

PROPOSITION 4.3 ([Sh, Theorem 3.6]): *Let P be a uniform p-group, and suppose that the derived length of each of the Lie rings L_i associated with P is at most k. Then the derived length of P is at most $2k + 1$.*

Now, let P and L_i be as in 4.3, and let α be a p'-automorphism of P which is fixed-point-free. Since L_i is a $\mathbb{Z}/p^i\mathbb{Z}$-module and the order of α is prime to p, we see that α induces on L_i a semisimple automorphism which is fixed-point-free. Setting $rk(P) = rk(L_i) = r$ and applying the Proposition, we obtain

$dl(L_i) \leq 2^{r-1} - 1$. But this holds for every Lie ring L_i associated with P. Applying Proposition 4.3 we obtain:

LEMMA 4.4: *Let P be a uniform p-group of rank r admitting a fixed-point-free p'-automorphism. Then $dl(P) \leq 2^r - 1$.*

Now, a powerful p-group P of rank r and exponent p^e splits into $k \leq r$ uniform sections of the form $P^{p^{i_1}}/P^{p^{i_2}}, \ldots, P^{p^{i_k}}/P^{p^{i_{k+1}}} (0 = i_1 < \cdots < i_{k+1} = e)$ of ranks $r = r_1 > \cdots > r_k$ respectively (see [Sh, Sec. 2] for details). If P admits a fixed-point-free p'-automorphism, then, applying 4.4 for each of these uniform sections, we see that

$$dl(P) \leq 2^{r_1} - 1 + \cdots + 2^{r_k} - 1$$

$$\leq 2^r - 1 + 2^{r-1} - 1 + \cdots + 2^1 - 1 = 2^{r+1} - r - 2.$$

However, since powerful p-groups of rank 2 are metacyclic, we may replace the two last summands (corresponding to uniform sections of ranks 2 and 1 respectively) by 2. We have proved:

LEMMA 4.5: *Let P be a powerful p-group of rank $r > 1$ admitting a fixed-point-free p'-automorphism. Then $dl(P) \leq 2^{r+1} - r - 4$.*

To pass from the powerful case to the case of an arbitrary p-group, an important result of Lubotzky and Mann should be applied [LM, Theorem 1.13]. It shows that every p-group P of rank r has a characteristic powerful subgroup Q such that $(P : Q) \leq p^{r\lceil \log_2 r \rceil}$ and $dl(P/Q) \leq \lceil \log_2 r \rceil$. This gives rise to:

PROPOSITION 4.6: *The derived length of a p-group of rank $r > 1$ admitting a fixed-point-free p'-automorphism cannot exceed $2^{r+1} - r - 4 + \lceil \log_2 r \rceil$.*

Now, let G be a finite group of rank r, admitting a fixed-point-free automorphism α. Then G is soluble (this is a well-known consequence of the classification). Suppose further that $(|\alpha|, |G|) = 1$. Fix p dividing the order of G, and set $P := O_{p'p}(G)/O_{p'}(G)$.

Then P is a p-group, say, of rank $d \leq r$, and by the Hall–Higman theory $G/O_{p'p}(G)$ may be identified with a completely reducible subgroup of $Aut(P/\phi(P)) = GL(d,p)$. By a result of M.F. Newman [N], it follows that $dl(G/O_{p'p}(G)) \leq 5\log_9(d/8) + 8 \leq 5\log_9(r/8) + 8$. By Proposition 4.6, $dl(P)) \leq 2^{r+1} - r - 4 + \lceil \log_2 r \rceil$. Hence the derived length of $G/O_p(G)$ is at most $2^{r+1} -$

$r-4+\lceil \log_2 r\rceil + 5\log_9(r/8)+8$. Since p is arbitrary, and $\bigcap_p O_p(G)=1$ we have established the following result.

THEOREM 4.7: *Let G be a finite group of rank r admitting a fixed-point-free automorphism whose order is coprime to $|G|$. Then $dl(G) \leq 2^{r+1}-r+\lceil \log_2 r\rceil + 5\log_9(r/8)+4$.*

5. A bound on the derived length: the general case

Let L be a uniform Lie ring of rank r and additive exponent p^i, and let A be an abelian p'-group of automorphisms of L having exactly m fixed points. We assume that $m>1$. Then the additive group of L may be written as a direct product $L=C_L(A)\times[L,A]$ (see [G, Theorem 5.2.3]). This implies that $C_L(A)$ has order at least p^i, so that $p^i \leq m$.

Now, an easy computation based on the fact that L/pL is commutative (see [Sh,4.2]) shows that $dl(L)\leq \lceil \log_2(i+1)\rceil$. We therefore obtain:

LEMMA 5.1: *Let L be a uniform Lie ring admitting an abelian p'-group of automorphisms A with $m>1$ fixed points. Then $dl(P)\leq \lceil \log_2(\lceil \log_p m\rceil+1)\rceil$.*

Now, let P be a uniform p-group of rank r admitting a p'-automorphism α with at most m fixed points, and let L_i be a (uniform) Lie ring associated with P. The combination of the Proposition and Lemma 5.1 yields

$$dl(L_i)\leq \max\{2^{r-1}-1, \lceil \log_2(\lceil \log_p m\rceil)\rceil\}.$$

Applying 4.3 we obtain

LEMMA 5.2: *Let P be a uniform p-group of rank r admitting a p'-automorphism with at most m fixed points. Then $dl(P)\leq \max\{2^r-1, 2\lceil \log_2(\lceil \log_p m\rceil+1)\rceil+1\}$.*

Keeping track of the arguments applied in the preceding section we readily have:

PROPOSITION 5.3: *Let P be a p-group of rank r admitting a p'-automorphism with at most m fixed points. Then the derived length of P is m,r-bounded.*

We leave the computation of the concrete bound obtained to the reader. As in the proof of 4.7, this gives rise to:

THEOREM 5.4: *Let G be a finite soluble group of rank r admitting an automorphism α with m fixed points. Suppose that the order of α is coprime to $|G|$. Then the derived length of G is r,m-bounded.*

This result completes the proof of the Theorem.

References

[A] J.L. Alperin, *Automorphisms of solvable groups*, Proc. Amer. Math. Soc. **13** (1962), 175–180.

[C] R.W. Carter, *Simple Groups of Lie Type*, Wiley, New York, 1972.

[DDMS] J. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, London Math. Society Lecture Notes Series 157, Cambridge, 1991.

[G] D. Gornstein, *Finite Groups*, Harper and Row, New York, 1968.

[H1] B. Hartley, *Centralizers in locally finite groups*, in Proc. of Group Theory—Bressanone 1986, Lecture Notes in Math. 1281, Springer, Berlin, 1987.

[H2] B. Hartley, *A general Brauer–Fowler Theorem and centralizers in locally finite groups*, Pac. J. Math. **152** (1992), 101–117.

[H] G. Higman, *Groups and rings having automorphisms without non-trivial fixed points*, J. London Math. Soc. **32** (1957), 321–334.

[HB] B. Huppert and N. Blackburn, *Finite Groups II*, Springer, Berlin, 1982.

[Kh] E.I. Khukhro, *Groups and Lie rings admitting almost regular automorphisms of prime order*, in Proc. of Group Theory—Bressanone 1989, Palermo, 1990.

[Kr] V.A. Kreknin, *Solvability of Lie algebras with a regular automorphism of finite period*, Soviet Mat. Dokl. **4** (1963), 683–685.

[L] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. I.H.E.S. **26** (1965), 389–603.

[LM] A. Lubotzky and A. Mann, *Powerful p-groups. I: finite groups*, J. Algebra **105** (1987), 484–505.

[M] Yu.A. Medvedev, *Groups and Lie algebras with almost regular automorphisms*, J. Algebra, to appear.

[N] M.F. Newman, *The soluble length of soluble linear groups*, Math. Z. **126** (1972), 59–70.

[Sh] A. Shalev, *On almost fixed point free automorphisms*, J. Algebra, to appear.

[Th] J.G. Thompson, *Finite groups with fixed-point-free automorphisms of prime order*, Proc. Natl. Acad. Sci. U.S.A. **45** (1959), 578–581.