ISRAEL JOURNAL OF MATHEMATICS **129** (2002), 209–220

FINITE GROUPS OF BOUNDED RANK WITH AN ALMOST REGULAR AUTOMORPHISM*

BY

A. JAIKIN-ZAPIRAIN

Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid, Cantoblanco Ciudad Universitaria
28049 Madrid, Spain
e-mail: andrei.jaikin@uam.es

ABSTRACT

In this paper we prove that any finite group of rank r, with an automorphism whose centralizer has m points, has a characteristic soluble subgroup of (m,r)-bounded index and r-bounded derived length. This result gives a positive answer to a problem raised by E. I. Khukhro and A. Shalev (see also Problem 13.56 from the "Kourovka Notebook" [Kou]).

1. Introduction

There has been certain interest on the study of finite groups with an automorphism of some fixed type over the last years. The classical restrictions on an automorphism consist in fixing the order of the automorphism and the order of the centralizer. We refer the interested reader to [Kh2] for background on this subject.

In [Sh1] A. Shalev began a new approach in this area. The **rank** of a group G (denoted by $\operatorname{rk} G$) is the minimal integer r such that every subgroup of G is r-generated, and the **rank** of a $\mathbb{Z}_p$-Lie ring L is the minimal number of generators of L as $\mathbb{Z}_p$-module. In his work Shalev proved that if a finite group of rank r has an automorphism whose centralizer has m elements, then it has a soluble

* This work has been supported by a grant of the Government of the Basque Country and by the DGICYT Grant PB97-0604.
Received May 1, 2000 and in revised form April 16, 2001

subgroup of (m,r)-bounded index. (In this paper we say that a certain invariant is $(a,b,\ldots)$-bounded if it is bounded above by some function of $(a,b,\ldots)$.) If, in addition, the orders of the automorphism and the group are coprime, then the derived length of the subgroup can also be bounded by some function of (m,r). The key to Shalev's proof is the reduction of the problem to the analogue for **uniform** p-Lie rings of bounded rank (i.e., a finitely generated free $\mathbb{Z}/p^i\mathbb{Z}$-module for some i), which is valid without any hypotheses on the orders. In [Kh1] E. I. Khukhro, assuming also that the order of the group and the order of the automorphism are coprime, improved Shalev's result, showing that the derived length of some soluble subgroup of (m,r)-bounded index is r-bounded.

In this paper we consider the general case and we prove the following result.

THEOREM 1.1: *Let G be a finite group of rank r admitting an automorphism with m fixed points. Then G has a characteristic soluble subgroup H, whose index is (m,r)-bounded and whose derived length is r-bounded.*

In Section 2 we prove the Lie ring analogue of our result and in Section 3, using the Shalev–Khukhro consruction of a Lie ring associated with a uniform powerful p-group, we give the proof of Theorem 1.1 in the case of p-groups. In Section 4 we finish the proof of Theorem 1.1, following the lines of [Sh1, Kh1], and we also pose some conjectures. The notation is standard. The derived series of a group is denoted by $\{G^{(k)}\}$ and a similar notation will be used for Lie rings. We will denote by G^n the subgroup of a group G generated by all nth powers of elements in G. $[r]$ denotes the upper integral part of a real number r.

2. The Lie ring case

Let $\mathbb{Z}_p$ be the ring of p-adic integers and $\mathbb{Q}_p$ its field of quotients. Set $S = \mathbb{Z}_p[x,x^{-1}]$. For every finitely generated S-module M such that $M/(x-1)M$ is finite, define the **x-rank** of M, $\mathrm{rx}\, M = \log_p(|M:(x-1)M|)$. Note that if M is finite then $|C_M(x)| = p^{\mathrm{rx}\, M}$. Throughout this paper we shall call Lie $\mathbb{Z}_p$-(sub)algebras simply **Lie (sub)rings** for brevity and then Lie automorphism will mean Lie $\mathbb{Z}_p$-algebra automorphism. The following theorem is the main result of this section.

THEOREM 2.1: *There is a function $f = f(p^m, r)$ such that if G is a Lie ring of rank r and also a finitely generated S-module of x-rank m with x operating on it as a Lie automorphism, then G has a soluble subring H of index less than f and derived length at most 1 if $r = 1$ and at most $2^r - 2$ if $r > 1$. Moreover, if G is a uniform Lie ring then the derived length of H is at most 2^{r-1}.*

In order to prove this theorem we need some preliminary work. In this paper all the tensor and exterior products are taken over $\mathbb{Z}_p$. Let L be an S-module. Then we can define in $L \wedge L$ an S-module structure by setting

$$x(a \wedge b) = (xa) \wedge (xb),\ x^{-1}(a \wedge b) = (x^{-1}a) \wedge (x^{-1}b),\ \text{where } a \wedge b \in L \wedge L.$$

We define the category $\mathbb{K}$, whose objects are the triples $(L, +, \cdot)$ where

(i) $(L, +)$ is an S-module,

(ii) $\cdot$ is a $\mathbb{Z}_p$-bilinear and alternating operation in L (i.e., $\cdot$ defines an element of $\operatorname{Hom}_{\mathbb{Z}_p}(L \wedge L, L)$).

The morphisms of $\mathbb{K}$ are the S-homomorphisms preserving multiplication. In the sequel the elements of $\mathbb{K}$ will be called **rings** and we shall write (L, α) instead of L when we want to emphasize that the multiplication $\cdot$ in a ring L is given by $\alpha \in \operatorname{Hom}_{\mathbb{Z}_p}(L \wedge L, L)$. For any $L_1, L_2 \in \mathbb{K}$ we shall write $L_1 < L_2$ if L_1 is a proper subring of L_2, i.e., L_1 is a proper subset of L_2 and the inclusion of L_1 into L_2 is a morphism in $\mathbb{K}$. We shall use $\cong$ for isomorphisms of $\mathbb{Z}_p$-modules and $\cong_{\mathbb{K}}$ for isomorphisms in the category $\mathbb{K}$.

If $L \in \mathbb{K}$ and $A, B \subseteq L$ let $A \cdot B$ be the S-submodule generated by $a \cdot b$, where $a \in A$ and $b \in B$. Let $\Gamma_1(L)$ be the S-submodule of L generated by the elements

$$(a \cdot b) \cdot c + (c \cdot a) \cdot b + (b \cdot c) \cdot a,\ x(a \cdot b) - (xa) \cdot (xb),\ a, b, c \in L,$$

and, for $i > 1$, let $\Gamma_i(L) = \Gamma_{i-1}(L) \cdot L$. Set $\Gamma(L) = \sum_i \Gamma_i(L)$ (so $\Gamma(L)$ is the ideal of L generated by $\Gamma_1(L)$). It is clear that $\bar{L} = L/\Gamma(L)$ becomes a Lie ring if for $\bar{a}, \bar{b} \in \bar{L}$ we define its Lie bracket by $[\bar{a}, \bar{b}] = (a \cdot b) + \Gamma(L)$, and x acts on $\bar{L}$ as a Lie automorphism. We call $L \in \mathbb{K}$ a **lattice** if $L \cong (\mathbb{Z}_p)^s$ for some s. The key to the proof of Theorem 2.1 is to prove it for the Lie rings $L/\Gamma(L)$ when L is lattice (see Theorem 2.4). Recall the following lemma proved in [Ja].

LEMMA 2.2: *Let L be an S-module and suppose that it is finitely generated as a $\mathbb{Z}_p$-module. If the x-rank of $L/p^{m+1}L$ is $\leq m$ then the x-rank of L is also at most m.*

LEMMA 2.3: *Let A be an S-module of x-rank m, finitely generated as a $\mathbb{Z}_p$-module, and let B be an S-submodule of A. Then $\operatorname{rx} B \leq m$.*

Proof: Remember that the case when B is of finite index in A was proved in [Ja, Lemma 3.6]. Let $\bar{B} = \{a \in A |\ p^k a \in B \text{ for some } k \geq 0\}$. Then, by [Ja, Lemma 3.6], $\operatorname{rx} B \leq \operatorname{rx} \bar{B}$ and $\operatorname{rx}(\bar{B} + p^{m+1}A)/p^{m+1}A \leq \operatorname{rx} A/p^{m+1}A \leq m$.

It follows directly from the definition of $\bar{B}$ that $\bar{B} \cap p^{m+1}A = p^{m+1}\bar{B}$. Hence $\mathrm{rx}\,\bar{B}/p^{m+1}\bar{B} \leq m$ and, by Lemma 2.2, $\mathrm{rx}\,\bar{B} \leq m$. ∎

Recall that if D is an associative ring, then a D-module P is called projective if, given a surjective homomorphism of D-modules $\beta\colon B \to A$, each D-module homomorphism $\psi\colon P \to A$ can be lifted to an homomorpism $\phi\colon P \to B$ such that $\beta\phi = \psi$. It is well known that a free D-module is projective. We will use this fact in the next theorem for $D = \mathbb{Z}_p$.

THEOREM 2.4: *Let G be a Lie ring of rank r and suppose that it is also a finitely generated S-module of x-rank m with x operating on it as a Lie automorphism. If $\mathrm{rk}\,p^m G = r$, then there exists a lattice $L \in \mathbb{K}$ of rank r and x-rank m, such that G is an epimorphic image (as an element of $\mathbb{K}$) of $\bar{L} = L/\Gamma(L)$.*

Proof: Let $L = (\mathbb{Z}_p)^r$, β a surjective homomorphism from L onto G and $\psi\colon L \to G$ given by $\psi(l) = x\beta(l)$. Using the fact that L is a free $\mathbb{Z}_p$-module, we obtain that there exists $\phi \in \mathrm{End}_{\mathbb{Z}_p}(L)$ such that $\psi(l) = x\beta(l) = \beta(\phi(l))$ for every $l \in L$. Now, we will see that ϕ has an inverse. Since x induces a bijection on G/pG, ϕ induces a bijection on L/pL. We conclude that $\phi(L) + pL = L$, which implies $\phi(L) = L$. Since any $\mathbb{Z}_p$-epimorphism of $\mathbb{Z}_p^r$ onto $\mathbb{Z}_p^r$ is always an automorphism, we obtain that ϕ has an inverse.

Define on L a structure of S-module by means of $xl = \phi(l)$, $x^{-1}l = \phi^{-1}(l)$ for every $l \in L$. Hence $\beta(xl) = x\beta(l)$. Since $x\beta(x^{-1}l) = \beta(l)$, we also have that $\beta(x^{-1}l) = x^{-1}\beta(l)$. We conclude that β is an S-homomorphism. The condition $\mathrm{rk}\,p^m G = r$ implies that $\mathrm{Ker}\,\beta \subseteq p^{m+1}L$ and so $|L : ((x-1)L + p^{m+1}L)| \leq p^m$. According to Lemma 2.2, the x-rank of L is at most m.

Since $L \wedge L$ is $\mathbb{Z}_p$-free, there exists $\alpha \in \mathrm{Hom}_{\mathbb{Z}_p}(L \wedge L, L)$ such that $\beta(\alpha(l \wedge m)) = [\beta(l), \beta(m)]$ for every $l, m \in L$. Define $a \cdot b = \alpha(a \wedge b)$, for $a, b \in L$. Hence $\beta(a \cdot b) = [\beta(a), \beta(b)]$. Recall that $\Gamma_1(L)$ is generated by

$$(a \cdot b) \cdot c + (c \cdot a) \cdot b + (b \cdot c) \cdot a,\ x(a \cdot b) - (xa) \cdot (xb),\ a, b, c \in L.$$

Applying β, we have

$$\begin{aligned}\beta((a \cdot b) \cdot c + (c \cdot a) \cdot b + (b \cdot c) \cdot a) =& [[\beta(a), \beta(b)], \beta(c)] + [[\beta(c), \beta(a)], \beta(b)] \\ &+ [[\beta(b), \beta(c)], \beta(a)] = 0\end{aligned}$$

and

$$\beta(x(a \cdot b) - (xa) \cdot (xb)) = x[\beta(a), \beta(b)] - [x\beta(a), x\beta(b)] = 0.$$

We see that the images of the S-generators of $\Gamma_1(L)$ are 0, and so $\beta(\Gamma_1(L)) = 0$. By an inductive argument, we obtain that $\beta(\Gamma_i(L)) = 0$, which implies $\beta(\Gamma(L)) = 0$. Hence G is an epimorphic image of $\bar{L} = L/\Gamma(L)$. ∎

Thus, we see that in order to prove Theorem 2.1 there is no loss of generality if we take G to be a Lie ring of the type $\bar{L} = L/\Gamma(L)$ where L is a lattice.

Define $\mathbb{E} = \mathbb{E}_{p,m,r} = \{L \in \mathbb{K} | \ L \cong (\mathbb{Z}_p)^r, \mathrm{rx}\, L = m\}$. If $L \in \mathbb{E}$, the tensor product $\mathbb{L} = \mathbb{Q}_p \otimes L$ belongs to the category $\mathbb{K}$. We call $\mathbb{L}$ **simple** if $\mathbb{L}^2 \neq 0$ and there is no proper $\mathbb{Q}_p[x, x^{-1}]$-submodule A of $\mathbb{L}$ such that $\mathbb{L} \cdot A \subseteq A$. Also a lattice M is called **maximal** if there are no lattice $N \in \mathbb{E}$ and injective morphism ϕ: $M \to N$ in $\mathbb{K}$ such that $\phi(M) < N$.

The proof of the following result is the same as the one of [Ja, Corollary 4.6]. We include the main steps of it for the sake of completeness.

LEMMA 2.5: *Let $L \in \mathbb{E}$ and suppose that $\mathbb{L}$ is simple. Then there exists a maximal lattice $M \in \mathbb{E}$, such that $L \leq M < \mathbb{L}$.*

Proof: We split the proof into a number of steps.

STEP 1: Let N be a lattice and $L < N < \mathbb{L}$. Define $t(L) = \min\{t | \ p^t L \subseteq L^2\}$ and $k = \max\{l | \ L \subseteq p^l N\}$. Then $t(L)$ and k are finite and $k \leq t(L)$.

Since $\mathbb{L}$ is simple, $\mathbb{L}^2 = \mathbb{L}$ and so $\mathbb{Q}_p L^2 = \mathbb{L}^2 = \mathbb{L}$. Hence $|L : L^2|$ is finite and so $t(L)$ is also finite. Using that N/L is a torsion finitely generated $\mathbb{Z}_p$-module, we also obtain that k is finite. By the definitions of $t(L)$ and k, we have

$$p^{t(L)} L \subseteq L^2 \subseteq p^{2k} N^2 \subseteq p^{2k} N.$$

Therefore by the maximality of k it follows that $2k - t(L) \leq k$, whence $k \leq t(L)$.

STEP 2: There is no proper ascending series of lattices $L < L_1 < L_2 < \cdots < \mathbb{L}$.

Otherwise, put $N = \bigcup_{i \geq 1} L_i$ and define

$$A = \{a \in N | \ p^{-k} a \in N \text{ for every } k \in \mathbb{N}\}.$$

Then A is a $\mathbb{Q}_p[x, x^{-1}]$-submodule of $\mathbb{L}$. For any $l \in N$, $a \in A$ and $k \in \mathbb{N}$ we have

$$p^{-k}(l \cdot a) = l \cdot (p^{-k} a) \in N.$$

Hence $N \cdot A \subseteq A$. Since $\mathbb{L} = \mathbb{Q}_p N$, $\mathbb{L} \cdot A \subseteq A$ and either $A = 0$ or $\mathbb{L}$.

In the former case, by [Ja, Lemma 4.3], N is a finitely generated $\mathbb{Z}_p$-module and so $|N : L|$ is finite, which is a contradiction.

If $A = \mathbb{L}$ fix $a_1, \ldots, a_m$, a $\mathbb{Z}_p$-system of generators of L. Since $p^{-t(L)-1}a_i \in N$, there exists $k \geq 1$ such that $p^{-t(L)-1}a_i \in L_k$ for all i. Hence $L \subseteq p^{t(L)+1}L_k$, which contradicts Step 1.

STEP 3: There exists a maximal lattice M such that $L \leq M < \mathbb{L}$.

By the previous step, there exists a lattice M such that $L \leq M < \mathbb{L}$ and M is maximal with this property. We shall prove that M is a maximal lattice. Suppose by way of contradiction that there exist a lattice $N \in \mathbb{E}$ and an injective morphism ϕ such that $\phi(M) < N$. Since N and $\phi(M)$ have the same rank, $N/\phi(M)$ is finite and so for every $n \in N$ there exists $k \in \mathbb{N}$ such that $p^k n = \phi(m)$ for some $m \in M$. We define $\psi\colon N \to \mathbb{L}$ by means of $\psi(n) = p^{-k}m \in \mathbb{L}$. This map is well defined and it is an injective morphism in the category $\mathbb{K}$. Hence $L \leq M < \psi(N) < \mathbb{L}$, against the choice of M. ∎

We shall need the following result on finite dimensional Lie algebras from [Kr].

PROPOSITION 2.6: *Let $\mathbb{F}$ be a field, L a finite dimensional Lie $\mathbb{F}$-algebra and ϕ an automorphism of L. If the centralizer $C_L(\phi)$ is trivial, then L is soluble of derived length at most* $\dim_{\mathbb{F}} L$.

Let $L \in \mathbb{E}$. Define $\gamma(L) = \sup\{k \mid \Gamma_1(L) \subseteq p^k L\}$. Put $L^{(0)} = L$ and, for $i > 0$, $L^{(i)} = L^{(i-1)} \cdot L^{(i-1)}$.

LEMMA 2.7: *There exists $a = a(p, m, r) \geq 0$ such that, for every maximal lattice $M \in \mathbb{E}$ and for every $s \geq 0$, $\gamma(p^s M) \leq 2s + a$.*

Proof: Suppose that for every j there exists a maximal lattice $M \in \mathbb{E}$ such that $\gamma(M) > j$. Then the set of Lie rings $T_0 = \{M/p^{\gamma(M)}M \mid M \in \mathbb{E} \text{ is maximal}\}$ is infinite. Put $N_0 = \{0\}$. Now, suppose that we have constructed a Lie ring $N_k \in \mathbb{K}$ such that $N_k \cong (C_{p^k})^r$ and the subset $T_k = \{N \in T_0 \mid N/p^k N \cong_{\mathbb{K}} N_k\}$ of T_0 is infinite. Since there is a finite number of non-isomorphic rings (as elements of $\mathbb{K}$) of type $N/p^{k+1}N$, where $N \in T_k$, we can find a Lie ring $N_{k+1} \in \mathbb{K}$ such that $N_{k+1} \cong (C_{p^{k+1}})^r$ and the subset $T_{k+1} = \{N \in T_k \mid N/p^{k+1}N \cong_{\mathbb{K}} N_{k+1}\}$ of T_0 is infinite. Following these constructions we obtain a series of Lie rings $\{N_i\}$ such that $N_i \cong_{\mathbb{K}} N_{i+1}/p^i N_{i+1}$. Let L be the inverse limit of the series $\{N_i\}$. Then L is a Lie ring and is also an S-module, where x acts as a Lie automorphism. As a $\mathbb{Z}_p$-module, L is isomorphic to $\mathbb{Z}_p^r$.

Since $\mathrm{rx}\, L/p^{m+1}L = \mathrm{rx}\, N_{m+1} = \mathrm{rx}\, N/p^{m+1}N$ for any $N \in T_{m+1}$, by Lemma 2.2, $\mathrm{rx}\, L = m$ and so x acts without fixed points on L. By Proposition 2.6, $\mathbb{L} = \mathbb{Q}_p \otimes L$ is soluble, whence there is an abelian ideal $A \neq 0$ of $\mathbb{L}$ which is also a $\mathbb{Q}_p[x, x^{-1}]$-submodule (for example, $A = \mathbb{L}^{(d-1)}$, where d is the derived length of $\mathbb{L}$). Put $B = A \cap L$. It is clear that B is an abelian ideal of L, also an S-submodule of L and that $p^{-1}B \not\subseteq L$. Take any maximal lattice M such that $M/p^{\gamma(L)}M$ belongs to T_2. Hence $M/p^2M \cong_{\mathbb{K}} N_2$. Let C be the image of B in $N_2 \cong_{\mathbb{K}} L/p^2L$ and let D be the inverse image of C under the natural morphism from M onto $N_2 \cong_{\mathbb{K}} M/p^2M$. By the construction, D is an S-submodule of M, $D \cdot D \subseteq p^2M$, $M \cdot D \subseteq D + p^2M$ and $p^{-1}D \not\subseteq M$. Put $P = M + p^{-1}D$. Then $P \cdot P \subseteq P$ and $M < P$, a contradiction to the maximality of M.

Hence there exists $a = a(p, m, r)$ such that $\gamma(M) \leq a$ for every maximal lattice $M \in \mathbb{E}$. If $a, b, c \in M$, then

$$\begin{aligned} p^{3s}((a \cdot b) \cdot c + (c \cdot a) \cdot b + (b \cdot c) \cdot a) =&(p^s a \cdot p^s b) \cdot p^s c + (p^s c \cdot p^s a) \cdot p^s b \\ &+ (p^s b \cdot p^s c) \cdot p^s a \in \Gamma_1(p^s M) \end{aligned}$$

and $p^{2s}(x(a \cdot b) - (xa) \cdot (xb)) = x(p^s a \cdot p^s b) - (x(p^s a)) \cdot (x(p^s b)) \in \Gamma_1(p^s M)$. Therefore $p^{3s}\Gamma_1(M) \subseteq \Gamma_1(p^sM) \subseteq p^{\gamma(p^sM)+s}M$ and we obtain that $\gamma(p^sM) \leq 2s + \gamma(M) \leq 2s + a$. ∎

Now we complete the proof of Theorem 2.1.

Proof of Theorem 2.1: We shall argue by induction on r. It is obvious that the result is true for $r = 1$ and $r = 2$. Suppose now that $r > 2$.

Consider first the case $m = 0$. Since G is residually finite (p^sG is an ideal of G for any $s \in \mathbb{N}$ and $\bigcap_{s\in\mathbb{N}} p^sG = \{0\}$), we can suppose that G is finite. Let $n = n_1p^k$, where n_1 and p are coprime and x^n acts trivially on G. Note that the condition $m = 0$ implies $C_G(x) = \{0\}$. Now, $(G, +)$ is a finite p-group and $C_G(x) = C_{C_G(x^{p^k})}(x)$. It implies that $C_G(x^{p^k}) = 0$ and Theorem 2.1 follows from [Sh3, Proposition 6.8].

Now suppose that $m > 0$. If $\operatorname{rk} p^mG$ is less than r, then the theorem follows from the inductive hypothesis because the index of p^mG in G is (p^m, r)-bounded. So we suppose that $\operatorname{rk} p^mG = r$. By Theorem 2.4, we have that G is an epimorphic image of some $\bar{L} = L/\Gamma(L)$, where $L \cong \mathbb{Z}_p^r$ is a lattice of x-rank m. Moreover, if G is uniform then G is an epimorphic image of $L/p^{\gamma(L)}L$.

First, suppose that $\mathbb{L} = \mathbb{Q}_p \otimes L$ is simple. By Lemma 2.5, there exists a maximal lattice M such that $L \leq M < \mathbb{L}$. We define $s = \min\{k \mid p^kM \subseteq L\}$. Hence the rank of $L/((p^{s-1}M \cap L) + \Gamma(L))$ is less than r and so, by the inductive hypothesis, we obtain that there is a function $h = h(p, m, r)$ such that

$$(1) \qquad (p^hL)^{(2^{r-1}-2)} \subseteq p^sM + \Gamma(L).$$

If $\Gamma_1(L) \subseteq p^{\gamma(p^sM)+s+1}L$, then

$$\Gamma_1(p^sM) \subseteq \Gamma_1(L) \subseteq p^{\gamma(p^sM)+s+1}L \subseteq p^{\gamma(p^sM)+1}p^sM.$$

But this is impossible, so $\gamma(L) \leq \gamma(p^s M) + s$. Applying Lemma 2.7, we obtain that $\gamma(L) \leq 3s + a$. In particular, $p^a(p^sM)^{(2)} \subseteq p^{a+3s}(p^sM) \subseteq p^{\gamma(L)}L$ and, consequently, by (1), $(p^gL)^{(2^{r-1})} \subseteq p^{\gamma(L)}L$ for some $g = g(p,m,r)$. If G is uniform then we are done. The general case follows from the inductive hypothesis, because the rank of $p^{\gamma(L)}L/\Gamma(L)$ is less than r.

Suppose now that $\mathbb{L}$ is not simple. Then there exists a $\mathbb{Q}_p[x,x^{-1}]$-submodule $0 \neq A \neq \mathbb{L}$ such that $A \cdot \mathbb{L} \subseteq A$. Let $B = A \cap L$. Note that $\bar{B} = (B + \Gamma(L))/\Gamma(L)$ is an ideal of $\bar{L}$ and also an S-submodule. Hence we can apply the inductive hypothesis to $\bar{B}$ and $\bar{L}/\bar{B}$. Indeed, from the construction of B we see that the ranks of B and L/B are less than r and the x-ranks of B (by Lemma 2.3) and L/B (as a quotient of L) are at most m. ∎

3. The p-group case

We will begin this section with the construction of a certain Lie ring associated with a uniform powerful group. The idea of this construction is taken from [Sh1], but in the present form it was suggested by E. Khukhro [Kh3]. Recall that a finite p-group Q is called **powerful** if $Q/Q^{\mathbf{p}}$ is abelian, where $\mathbf{p} = 4$ if $p = 2$ and $\mathbf{p} = p$ if p is odd, and that a powerful p-group P is called **uniform** if the rank of P^{p^i} does not depend on i, as long as $P^{p^i} \neq 1$. We suggest to the reader the books [DDMS, Kh2] for a detailed account of the properties of these groups. In the sequel we will write $[\ ,\ ]$ for group commutators and $[\ ,\ ]_L$ for Lie brackets.

In this section we use the following notation. Let G be a uniform powerful p-group and p^n its exponent. Set $G_i = G^{p^i}$. We write n in the form $n = 4e + f$, where $0 \leq f \leq 3$, and put $L = G_e/G_{2e}$. For each integer $0 \leq k \leq 2$ let $\pi_k\colon G_{ke}/G_{(k+1)e} \to G_{(k+1)e}/G_{(k+2)e}$ be the map defined in the following way: if $t \in G_{ke}$ then $\pi_k(tG_{(k+1)e}) = t^{p^e}G_{(k+2)e}$. It is known that these maps are well defined and, moreover, that π_1 and π_2 are group isomorphisms.

The group L is abelian and we will use additive notation in it. If $a, b \in G_e$ define

$$[aG_{2e}, bG_{2e}]_L = \pi_1^{-1}([a,b]G_{3e}).$$

LEMMA 3.1: *With these operations L becomes a Lie ring.*

Proof: We will prove that the Jacobi condition holds. The rest of the axioms for a Lie ring can be proved in the same way. Let $a, b, c \in G_e$. Bearing in mind that $[G_e, G_{3e}] \leq G_{4e}$ and using the Hall–Witt identity, we obtain that

$$[a,b,c][b,c,a][c,a,b] \in G_{4e}.$$

Note that if $d \in G_{2e}$ and $c \in G_e$, then

$$\pi_2([\pi_1^{-1}(dG_{3e}), c]G_{3e}) = [d, c]G_{4e}.$$

Hence

$$[\pi_1^{-1}([a,b]G_{3e}), c][\pi_1^{-1}([b,c]G_{3e}), a][\pi_1^{-1}([c,a]G_{3e}), b] \subseteq G_{3e}$$

and, applying π_1^{-1} here, we obtain the Jacobi identity in L. ∎

Remark 3.2: If ϕ is a group automorphism of G, then ϕ acts in the natural way on L and, from the definition of the Lie brackets on L, it follows that ϕ is a Lie ring automorphism of L.

We will say that a subgroup N of a finite p-group Q is **powerfully embedded in** Q if $[N, Q] \leq N^{\mathbf{p}}$. It is known that if M and N are powerfully embedded in Q, then so are MN, M^p and $[M, N]$. The next lemma which was proved in [Sh2] is very important for the future applications of our construction.

LEMMA 3.3: *If M and N are powerfully embedded subgroups in a finite p-group Q, then $[M^{p^i}, N^{p^j}] = [M, N]^{p^{i+j}}$.*

LEMMA 3.4: *If T is powerfully embedded subgroup in G, then $\bar{T} = \pi_0(TG_e/G_e)$ is an ideal of L and $[\bar{T}, \bar{T}]_L = \pi_0([T,T]G_e/G_e)$.*

Proof: Since TG_e is powerful, $\bar{T} = (TG_e)^{p^e}/G_{2e}$ and so it is a subgroup of L. Let us prove that it is also an ideal of L. Using that $(TG_e)^{p^e}$ is powerfully embedded in G, we obtain that $[(TG_e)^{p^e}, G_e] = [TG_e, G]^{p^{2e}}$. Hence $[\bar{T}, L]_L = [TG_e, G]^{p^e} G_{2e}/G_{2e} \subseteq \bar{T}$.

Now, we will prove the second part of the lemma. We have that

$$[(TG_e)^{p^e}, (TG_e)^{p^e}]G_{3e} = [(TG_e), (TG_e)]^{p^{2e}} G_{3e} = ([T,T]G_e)^{p^{2e}}.$$

Therefore $[\bar{T}, \bar{T}]_L = ([T,T]G_e)^{p^e}/G_{2e} = \pi_0([T,T]G_e/G_e)$. ∎

COROLLARY 3.5: *Let T be a powerfully embedded subgroup in G and consider $\bar{T} = \pi_0(TG_e/G_e)$ as an ideal of L. Then $\bar{T}^{(d)} = \pi_0(T^{(d)}G_e/G_e)$.*

For each nonnegative integer i, we define $L_i = \pi_0(G_i/G_e) = G_{i+e}G_{2e}/G_{2e}$. Then by Lemma 3.4 we know that L_i is an ideal of L.

LEMMA 3.6: *Let d be the derived length of L_i (as a Lie ring). Then the derived length of G_i is $\leq d+2$.*

Proof: By the previous corollary, $G_i^{(d)} \leq G_e$. Now it is easy to see that $G_i^{(d+2)} = \{1\}$. ∎

Proof of Theorem 1.1 for finite p-groups: Let G be a finite p-group of rank r admitting an automorphism ϕ with m fixed points. The case $m = 1$ was considered in [Sh1, Chapter 4], so we may assume that $m \neq 1$ $(m \geq p)$. By [LM] there exists a characteristic powerful subgroup Q such that $|G : Q| \leq p^{r[\log_2 r]}$. Hence we can suppose that G is powerful. Since the rank of G is r, there exists a series of characteristic subgroups $\{1\} = T_0 \subset T_1 \subset \cdots \subset T_k = G$ with $k \leq r$ and such that the factors $H_i = T_i/T_{i-1}, 1 \leq i \leq k$, are uniform powerful p-groups. Note that $|C_{H_i}(\phi)| \leq m$ (see, for example, [Kh2, Lemma 2.12]). By the above construction we can associate with each group H_i a Lie ring $L = L(i)$. Moreover, ϕ can be considered as a Lie automorphism of L and we have that $|C_L(\phi)| \leq m$. By Theorem 2.1 there are functions $t_i = t_i(r,m)$ and $s_i = s_i(r)$ such that $L_{t_i}^{(s_i)} = (p^{t_i}L)^{(s_i)} = \{0\}$. Hence, by Lemma 3.6, we obtain that $(H_i^{p^{t_i}})^{(s_i+2)} = \{1\}$ and so $(T_i^{p^{t_i}})^{(s_i+2)} \subseteq T_{i-1}$. Hence, by Lemma 3.3 we can find $f = f(m,r)$ and $g = g(r)$ such that $(G^{p^f})^{(g)} = \{1\}$. Since G is powerful, the index of G^{p^f} in G is at most p^{fr}. ∎

4. Final remarks

We now extend Theorem 1.1 to arbitrary finite groups.

Proof of Theorem 1.1: First suppose that G is a nilpotent group. Then G is the direct product of its Sylow p_i-subgroups G_i. Decompose m as $m = \prod p_i^{m_i}$. If $m_i = 0$ then, by [Sh1], the derived length of G_i is bounded by some function which depends only on r. In this case we put $H_i = G_i$. If $m_i \neq 0$, then by the previous section there exists a characteristic subgroup H_i of G_i of $(p_i^{m_i}, r)$-bounded index and r-bounded derived length. Then $H = \prod H_i$ is a characteristic subgroup of G of (m,r)-bounded index and r-bounded derived length.

Suppose now that G is a soluble group. We follow the same argument as in [Kh1]. Let $\pi(G)$ be the set of prime divisors of $|G|$ and $q \in \pi(G)$. Denote by $O_{q'}(G)$ the maximal normal q'-subgroup of G and by $O_{qq'}(G)$ the inverse image of the maximal normal q-subgroup Q of the quotient $G/O_{q'}(G)$. It is well-known that the action of $G/O_{qq'}(G)$ by conjugation on $Q/\Phi(Q)$ is faithful. Then the group $G/O_{qq'}(G)$ is isomorphic to a soluble subgroup of $\mathrm{GL}_d(q)$, where d is the number of generators of Q. Since $d \leq r$, using the Kolchin–Malcev theorem [We, Theorem 3.6], we obtain that the derived length of $G/O_{qq'}(G)$ is r-bounded. Hence G/F, where $F = \bigcap_{q\in\pi(G)} O_{qq'}(G)$ is the Fitting subgroup of G, is soluble of r-bounded derived length. Since F is nilpotent, there exists a characteristic subgroup N of F of (m,r)-bounded index and r-bounded derived length. Put $H = C_G(F/N)$. The index of H is (m,r)-bounded, because G/H acts as a group of automorphisms of F/N and the order of F/N is (m,r)-bounded. Also, the derived length of H is r-bounded, because the derived lengths of $H/(H\bigcap F) \cong HF/F$ and $H \cap N$ are r-bounded and $[H\cap F, H\cap F] \leq (H\cap N)$. Hence H satisfies the desired conditions.

Now, if G is an arbitrary finite group of rank r admitting an automorphism with m fixed points, then, using the classification of the finite simple groups, Shalev proved in [Sh1, Proposition 3.2] that G has a characteristic soluble subgroup of (r,m)-bounded index. Therefore this case follows from the previous paragraph. ∎

From [Sh1, Section 5] we can deduce that if G is a finite p-group of rank r admitting a p'-automorphism ϕ with p^m fixed points, then the derived length of G is (m,r)-bounded. This result suggests to us the following conjecture:

Conjecture 1: Let G be a finite p-group of rank r admitting an automorphism ϕ with p^m fixed points. Then the derived length of G is (m,r)-bounded. Moreover, there are functions $f = f(m,r)$ and $d = d(r)$ such that G has a subgroup of index at most p^f and derived length at most d.

In [Ja], it was proved that there are functions $f(p,m,n)$ and $h(m)$ such that any finite p-group G with an automorphism of order p^n, whose centralizer has p^m points, has a subgroup of derived length $\leq h(m)$ and index $\leq f(p,m,n)$. Note that in this situation the rank of G is also (p,m,n)-bounded. Therefore, we pose the following problem:

Conjecture 2: Let G be a finite p-group of rank r admitting a p-automorphism ϕ with p^m fixed points. Then there are functions $f = f(p,m,r)$ and $d = d(m)$ such that G has a subgroup of index at most f and derived length at most d.

References

[DDMS] J. Dixon, M. du Sautoy, A. Mann and D. Segal, *Analytic Pro-p Groups*, 2nd edn., Cambridge University Press, Cambridge, 1999.

[Ja] A. Jaikin-Zapirain, *On the almost regular automorphisms of finite p-groups*, Advances in Mathematics **153** (2000), 391–402.

[Kh1] E. I. Khukhro, *Almost regular automorphisms of finite groups of bounded rank*, Sibirskii Matematicheskii Zhurnal **37** (1996), no. 6, 1407–1412; English transl.: Siberian Mathematical Journal, **37** (1996), no. 6, 1237–1241.

[Kh2] E. I. Khukhro, *p-Automorphisms of Finite p-Groups*, Cambridge University Press, 1998.

[Kh3] E. I. Khukhro, private communication.

[Kou] E. I. Khukhro and V. D. Mazurov (eds.), *The Kourovka Notebook: Unsolved Problems in Group Theory*, 14th edn., Novosibirsk, 1999.

[Kr] V. A. Kreknin, *The solubility of the Lie algebras with a regular automorphism*, Sibirskii Matematicheskii Zhurnal **8** (1967), 715–716; English. transl.: Siberian Mathematical Journal **8** (1968), 536–537.

[LM] A. Lubotzky and A. Mann, *Powerful p-groups. I. Finite groups*, Journal of Algebra **105** (1987), 484–505.

[Sh1] A. Shalev, *Automorphisms of finite groups of bounded rank*, Israel Journal of Mathematics **82** (1993), 395–404.

[Sh2] A. Shalev, *On almost fixed point free automorphisms*, Journal of Algebra **157** (1993), 271–282.

[Sh3] A. Shalev, *Finite p-groups*, in *Collection: Finite and Locally Finite Groups (Istanbul, 1994)*, NATO Advanced Science Institutes Series C: Mathematical and Physical Sciences **471** (1995), 401–450.

[We] B. A. F. Wehrfritz, *Infinite Linear Groups*, Springer-Verlag, Berlin, 1973.