On Almost Regular Automorphisms of Finite $p$-Groups

A. Jaikin-Zapirain

Departamento de Matemáticas-Matematika Saila, Facultad de Ciencias-Zientzi Fakultatea, Universidad del País Vasco-Euskal Herriko Unibertsitatea, Apdo. 644, 48080 Bilbao, Spain
E-mail: mtbjaza@ehu.es

Received December 7, 1999; accepted December 14, 1999

In this paper we prove that there are functions $f(p, m, n)$ and $h(m)$ such that any finite $p$-group with an automorphism of order $p^n$, whose centralizer has $p^m$ points, has a subgroup of derived length $h(m)$ and index $f(p, m, n)$. This result gives a positive answer to a problem raised by E. I. Khukhro (see also Problem 14.96 from the "Kourovka Notebook" (1999, E. I. Khukhro and V. D. Mazurov (Eds.), "The Kourovka Notebook: Unsolved Problems in Group Theory," 14th ed., Novosibirsk)).

2000 Academic Press

1. INTRODUCTION

By a classical result of J. Thompson and G. Higman a finite group with a regular (without non-trivial fixed points) automorphism of prime order $p$ is nilpotent of nilpotency class bounded by a function depending only on $p$, $h(p)$, known as Higman’s function. J. Thompson (see [21]) established the nilpotency and G. Higman (see [2]) showed the existence of such function $h(p)$. Later in [11] V. A. Kreknin proved that a $\mathbb{Z}/n\mathbb{Z}$-graded Lie ring $L$ with $L_0 = 0$ is soluble of derived length at most $k(n)$, giving an explicit upper bound for $k(n)$. Applying this theorem he showed that an arbitrary Lie ring admitting a regular automorphism of order $n$ is soluble of derived length at most $2k(n)$. Also in [12] A. I. Kostrikin and V. A. Kreknin gave an upper bound for Higman’s function. The analog of Kreknin’s Theorem for finite groups remains unsettled: although a finite group with a regular automorphism of order $n$ is known to be soluble, no bound for its derived length in terms of $n$ only has been found at the moment for $n$ composite, except for the particular case $n = 4$ (see [10]).

1 This work has been supported by a grant of the Government of the Basque Country and by the DGICYT Grant PB97-0684.
2 I thank Professor E. I. Khukhro for introducing me to this subject.
In a different direction, using Higman’s method, J. L. Alperin (see [1]) showed that if $G$ is a finite $p$-group admitting an automorphism of order $p$ with $p^m$ fixed points, then the derived length of $G$ is $(p, m)$-bounded (in this paper we say that a certain invariant is $(a, b, ...)$-bounded if it is bounded above by some function of $(a, b, ...)$). In [5, 14] this result was improved by E. I. Khukhro and N. Yu. Makarenko and it was shown that $G$ has a subgroup $H$ of $(p, m)$-bounded index and nilpotency class at most $h(p)$.

In [18] A. Shalev considers a finite $p$-group $G$ admitting an automorphism of order $p^n$ with $p^m$ fixed points and proves that its derived length is $(p, m, n)$-bounded. E. I. Khukhro [6] makes this information precise and shows that $G$ has a subgroup $N$ of $(p, m, n)$-bounded index and derived length at most $2k(p^n)$. He also asked if the derived length of $N$ can be bounded by some function depending only on $m$. Yu. Medvedev showed in [16] that this problem can be reduced to the analog question about finite Lie rings with an additive $p$-group and, in [17], he gave a positive answer to it for the particular case $n = 1$. In fact, he proved a bit more than this by showing that a subgroup of $(p, m)$-bounded index and $m$-bounded nilpotency class exists. Actually, R. Shepherd [20] and C. R. Leedham-Green and S. McKay [13] had proved that for $n = 1$ and $m = 1$, $G$ has a subgroup of $p$-bounded index and nilpotency class at most 2. Also for $m = 1$, S. McKay [15] and I. Kiming [8] proved that $G$ has a subgroup of $(p, n)$-bounded index and nilpotency class at most 2. In this paper we answer Khukhro’s question in the positive for arbitrary $m$ and $n$. We refer the interested reader to [4] for more background on this subject.

Let $\mathbb{Z}_p$ be the ring of $p$-adic integers and $\mathbb{Q}_p$ its field of quotients. Set $S = \mathbb{Z}_p[x]$ and $R = S/(1 + \cdots + x^{p^n - 1})$. Let $M$ be a finitely generated $R$-module (or $S$-module). It is clear that if $|M: (x-1)M|$ is finite then it is a power of $p$. In this case we define the $x$-rank of $M$ by $r_x M = \log_p(|M: (x-1)M|)$. Put $m = r_x M$. Since $(x - 1)M$ is contained in the Jacobson radical of $M$, $M$ can be generated by $m$ elements. Hence, $M$ is an epimorphic image of $R^m$ and the rank of $M$ as $\mathbb{Z}_p$-module is $(m, n)$-bounded. In particular, if $u$ is a $(p, m, n)$-bounded number then both the index of $p^u M$ in $M$ and the order of $\{ t \in M | p^u t = 0 \}$ are $(p, m, n)$-bounded as well. In the next sections, we shall use several times these facts, sometimes without mentioning them explicitly. Note also that if $M$ is finite then $|C_M(x)| = p^{r_x M}$.

Throughout this paper we shall call Lie $\mathbb{Z}_p$-(sub)algebras simply Lie (sub)algebras or Lie rings for brevity. The main result of this paper is the following theorem.

**THEOREM 1.1.** There is a function $f = f(p, m, n)$ such that if $M$ is a Lie ring and also a finitely generated $R$-module of $x$-rank $m$ with $x$ operating on it as a Lie automorphism, then $M$ has a soluble subring $N$ of index less than $f$ and derived length at most $2^{m+1} - 2$. 

Suppose now that $M$ is a Lie ring whose additive group is a finite $p$-group and $M$ has an automorphism $\phi$ of order $p^n$ with $p^m$ fixed points. It is clear that $p^n(1 + \cdots + \phi^{p^n-1}) M = 0$, and so $p^n M$ can be viewed as an $R$-module of $x$-rank $\leq m$. On the other hand, by [4, Corollary 2.7], the rank of $M$ is $(p, m, n)$-bounded and so the index of $p^n M$ is $(p, m, n)$-bounded. Hence, Theorem 1.1 yields the following corollary.

**Theorem 1.2.** Let $M$ be a Lie ring whose additive group is a finite $p$-group and suppose that $M$ has an automorphism $\phi$ of order $p^n$ with $p^m$ fixed points. Then there is a subring $N$ of $(p, m, n)$-bounded index and derived length $\leq 2^{m+1} - 2$.

Using the reduction theorem from [16] we obtain the following result.

**Corollary 1.3.** There are functions $f(p, m, n)$ and $g(m)$ such that any finite $p$-group with an automorphism of order $p^n$ and $p^m$ fixed points has a subgroup of derived length $\leq g(m)$ and index $\leq f(p, m, n)$.

2. PRELIMINARIES

In this paper all the exterior and tensor products are taken over $\mathbb{Z}_p$. Let $M$ be an $R$-module. Then we can define in $M \otimes M$ an $S$-module structure by setting

$$x(a \otimes b) = (xa) \otimes (xb), \quad \text{where} \quad a, b \in M \otimes M.$$  

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

(i) $(M, +)$ is an $R$-module.

(ii) $\cdot$ is an antisymmetric and bilinear form on $M$ and if we put $x(m_1 \cdot m_2) = m_1 \cdot x(m_2)$, then $x \in \text{Hom}_S(M \otimes M, M)$.

The morphisms of $\mathcal{K}$ are defined in the natural way. Hence $\mathcal{K}$ is the category of (nonassociative) rings with an additional compatible structure of $R$-modules. In the sequel we shall write $(M, \cdot)$ instead of $M$ when we want to emphasize that the operation $\cdot$ in $M \in \mathcal{K}$ is given by $x \in \text{Hom}_S(M \otimes M, M)$. For any $M_1, M_2 \in \mathcal{K}$ we shall write $M_1 < M_2$ if $M_1$ is a proper subring of $M_2$ in the category $\mathcal{K}$, i.e., $M_1$ is a proper subset of $M_2$ and the inclusion of $M_1$ into $M_2$ is a morphism in $\mathcal{K}$. We use $\cong$ for isomorphism of $R$-modules and $\cong_K$ for isomorphism in the category $\mathcal{K}$. 

393 ALMOST REGULAR AUTOMORPHISMS
If \( M \in \mathbb{K} \) and \( A, B \subseteq M \) let \( A \cdot B \) be the \( R \)-submodule generated by \( a \cdot b \), where \( a \in A \) and \( b \in B \). Let \( \Gamma_i(M) \) be the \( R \)-submodule of \( M \) generated by the elements
\[
a \cdot (b \cdot c) + c \cdot (a \cdot b) + b \cdot (c \cdot a), \quad a, b, c \in M,
\]
and, for \( i > 1 \), let \( \Gamma_i(M) = \Gamma_{i-1}(M) \cdot \Gamma(M) \). Set \( \Gamma(M) = \sum_i \Gamma_i(M) \) (so \( \Gamma(M) \) is the ideal of \( M \) generated by \( \Gamma_i(M) \)). It is clear that \( M = M/\Gamma(M) \) becomes a Lie ring if for \( a, b \in M \) we define its Lie bracket by
\[
[a, b] = (a \cdot b) + \Gamma(M).
\]

The polynomial \( 1 + \cdots + x^{p^n-1} \) can be decomposed in \( \mathbb{Z}_p[x] \) as the product of the cyclotomic polynomials
\[
f_i = \prod_{j} (x - \omega_{i,j}), \quad i = 1, \ldots, n,
\]
where \( \{ \omega_{i,j} \} \) is the set of \( p^i \)th primitive roots of 1. Then \( R_i = \mathbb{Z}_p[x]/(f_i) \) is a discrete valuation ring whose maximal ideal is generated by \( (x - 1) \). We call \( L \subseteq K \) a lattice if \( L \subseteq \bigoplus_i R_i^k \) for some \( k_1, \ldots, k_n \). The key of the proof of Theorem 1.1 is to prove it for the Lie rings \( L/\Gamma(L) \) when \( L \) is a lattice.

We shall deal with this case in Section 4. First, in Section 3, we show how the general case follows from this particular one.

### 3. THE REDUCTION THEOREM

The goal of this section is to show that in order to prove Theorem 1.1 there is no loss of generality if we take \( M \) to be a Lie ring of the type \( L = L_1/\Gamma(L) \) where \( L \) is a lattice. This reduction is a consequence of the following theorem.

**Theorem 3.1.** There are functions \( g_1 = g_1(p, m, n) \) and \( g_2 = g_2(p, m, n) \) satisfying the following property: if \( M \) is a Lie ring and a finitely generated \( R \)-module of \( x \)-rank \( m \) with the element \( x \) acting as a Lie automorphism, then there exists a subring \( N_1 \), an ideal \( N_2 \) of \( N_1 \) and a lattice \( L \) of \( x \)-rank at most \( m \) such that

(i) \( |M : N_1| \leq g_1 \) and \( |N_2| \leq g_2 \).

(ii) The ring \( N_1/N_2 \) is an epimorphic image of \( L = L/\Gamma(L) \).

In order to prove this theorem we need some preliminary work. We introduce first some additional notation. Let \( f_i = \prod_{j \neq i} f_j \). The polynomials \( f_i \) and \( f_j \) are coprime in \( \mathbb{Q}_p[x] \), so there exist \( r_i, q_i \in \mathbb{Z}_p[x] \) and \( t_i \geq 0 \) such that \( r_i f_i + q_i f_j = p^i t_i \). Define \( z_i = z_i(p, n) = \max_i t_i \).

Let \( L \) be an \( R \)-module and suppose that \( L = \bigoplus_{i=1}^n L_i \), with \( L_i \cong R_i^{k_i} \). The following lemma is an easy consequence of the definition of \( z_i \).

**Lemma 3.2.** Let \( A \) be an \( R \)-submodule of \( L \), and \( a = \sum a_i \in A \), \( a_i \in L_i \). Then \( p^{z_i} a_i \in A \).
Proof. We have \( q_i f_i a = q_i f_i a_i = p^s a_i \in A \). Since \( z_1 \geq t \), then \( p^s a_i \in A \).

**Corollary 3.3.** Let \( A \) be an \( R \)-submodule of \( L \) such that \( \{ l \in L \mid p^k l \in A \) for some \( k \in \mathbb{N} \} = A \). Then \( A \cong \sum R_i^k \) for some \( 0 \leq s_i \leq k \), and there exists \( B \cong \sum R_i^k \) such that \( L = A \oplus B \).

Consider now the ideal \( \bar{R} = \sum_i R_i^k \) of \( R \). Note that this sum is direct and \( R_i^k \cong R_i \). It is easy to see that there exists \( z_2 \geq 0 \) such that \( p^z R \subseteq \bar{R} \). We can prove now the following lemma.

**Lemma 3.4.** Let \( M \) be a finitely generated \( R \)-module which is \( \mathbb{Z}_p \)-torsion free. Then there exists a submodule \( N \) of finite index such that \( N \cong \bigoplus_{i=1}^r R_i^k \) for some \( s_i \geq 0 \) and \( p^s M \subseteq N \).

Proof. Set \( N = R M \). Then \( N = \sum N_i \), where \( N_i = R_i^k M \). Since \( N_i \) is \( \mathbb{Z}_p \)-torsion free, then \( N_i \cong R_i^k \) for some \( s_i \geq 0 \). Suppose \( \sum a_i = 0 \), where \( a_i \in N_i \). By using the same argument as in the proof of Lemma 3.2 we deduce that \( p^s a_i = 0 \) for every \( i \), whence \( a_i = 0 \). Hence, \( N = \bigoplus_i N_i \cong \bigoplus_i R_i^k \).

**Lemma 3.5.** Let \( M \) be an \( S \)-module and finitely generated as \( \mathbb{Z}_p \)-module. If \( \text{rx}(M/p^{m+1}M) \leq m \) then \( \text{rx} M \leq m \).

Proof. Since \( \text{rx}(M/p^{m+1}M) \leq m \) then \( p^s M \subseteq (x - 1) M + p^{m+1}M \). Hence, by Nakayama’s Lemma, \( p^s M \subseteq (x - 1) M \). Then we have
\[
|M : (x - 1) M| = |M : (p^s M + (x - 1) M)| \\
\leq |M : (p^{m+1} M + (x - 1) M)| \leq p^m,
\]
and so \( \text{rx} M \leq m \).

**Lemma 3.6.** Let \( M \) be an \( S \)-module of \( x \)-rank \( m \), finitely generated as \( \mathbb{Z}_p \)-module and \( N \) an \( S \)-submodule of \( M \) of finite index. Then \( \text{rx} N \leq m \).

Proof. Since the index of \( N \) in \( M \) is finite, there exists \( u \) such that \( p^u M \subseteq N \). Set \( \bar{M} = M/p^{u+1}M \) and \( \bar{N} = N/p^{u+1}M \). Then we have
\[
\text{rx}(N/p^{u+1}N) = \text{rx} \bar{N} = \log_p |C_{\bar{M}}(x)| \leq \log_p |C_{\bar{M}}(x)| = \text{rx} \bar{M} \leq m,
\]
and so, by Lemma 3.5, \( \text{rx} N \leq m \).

**Lemma 3.7.** Let \( M \) be a finitely generated \( R \)-module of \( x \)-rank \( m \). Then there exists a submodule \( N \) of \( (p, m, n) \)-bounded index which is an epimorphic image of \( \bigoplus_i R_i^k \) for some \( k_i \geq 0 \) with \( \sum k_i \leq m \).
Proof. Since \((x-1)M\) is contained in the Jacobson radical of \(M\), \(M\) can be generated by \(m\) elements. Hence, \(M\) is an epimorphic image of \(R^m\) and the index of \(K = RM\) in \(M\) is \((p, m, n)\)-bounded. Using Lemma 3.6 we obtain that \(rxK \leq m\).

From the definition of \(K\) there is an \(R\)-submodule \(T\) of \(R^m = \bigoplus_i R^{n_i}\) such that \(K \cong R^m/T\). Let \(T_i\) be the image of the projection of \(T\) to \((R^i)^m\). Put \(\overline{T} = \bigoplus_i T_i\). Then \(T \subseteq \overline{T}\). Set \(D = R^m/\overline{T} = \bigoplus_i D_i\), where \(D_i \cong R^{n_i}/T_i\) and denote the \(x\)-rank of \(D_i\) by \(k_i\). It is clear that \(D_i\) is an epimorphic image of \(R^{n_i}\). Since \(D\) is a quotient of \(K\) we have

\[
\sum_i k_i = \sum_i \text{rx} D_i = \text{rx} D \leq m.
\]

Set \(N = p^i K\). By Lemma 3.2, \(p^i \overline{T} \subseteq T\) and so \(N\) is an epimorphic image of \(D\), whence it is also a quotient of \(\bigoplus_l R^{k_l}\). Finally, we have that \(p^{i+1}M \leq N\) and so the index of \(N\) in \(M\) is \((p, m, n)\)-bounded.

**Corollary 3.8.** There is a function \(f = f(p, m, n)\) such that for every Lie ring \(M\) which is a finitely generated \(R\)-module of \(x\)-rank \(m\), there exists a subring \(N\) of index \(\leq f\) which is, as \(R\)-module, an epimorphic image of \(\bigoplus_l R^{k_l}\) for some \(k_i \geq 0\) with \(\sum k_i \leq m\).

**Proof.** From Lemma 3.7 there exists a submodule \(K\) of \((p, m, n)\)-bounded index which is a quotient of \(\bigoplus_l R^{k_l}\) for some \(k_i \geq 0\) with \(\sum k_i \leq m\). Let \(p^m\) be the index of \(K\) in \(M\). Then the Lie subring \(N = p^m K\) satisfies the desired conditions.

**Proof of Theorem 3.1.** By Corollary 3.8 we can suppose that there exist \(L = \bigoplus L_i, L_i \cong R^{k_i}, \sum_i k_i \leq m, \text{ and } T \subseteq L\), such that \(M \cong L/T\). Let \(\beta\) be the natural projection from \(L\) onto \(M\) and define \(\beta(a) = [\beta(a), \beta(b)]\). Consider \(H = (L \wedge L)/(1 + \cdots + x^{p^{i-1}})(L \wedge L)\). Since \((1 + \cdots + x^{p^{i-1}})M = 0\), \(\beta(1 + \cdots + x^{p^{i-1}})(L \wedge L) = 0\) and so we can view \(\beta\) as an \(R\)-homomorphism from \(H\) to \(M\). Let \(U\) be the \(R\)-submodule of \(H\) of \(Z_{p^i}\)-torsion elements. Since \(H\) is \(Z_{p^i}\)-finitely generated, \(U\) is finite. Its order depends on the numbers \(k_i\) and \(p\), so it is \((p, m, n)\)-bounded. Hence, without loss of generality, we can suppose that \(\beta(U) = 0\) and \(\beta\) can be regarded as an \(R\)-homomorphism from \(H = H/U\) to \(M\).

Since \(H\) is \(Z_{p^i}\)-torsion free, by Lemma 3.4, there exists a submodule \(D\) of \(H\), such that \(D = \bigoplus D_i\), and \(D_i \cong R^{k_i}\). Let \(d \in D_k\) for some \(k\) and \(a = \beta(d)\). There exist \(l_j \in L_i\), such that \(a = \beta(\sum_j l_j)\). By the definition of \(z_{p^i}\), there exist \(q, r \in Z_{p^i}[x]\) such that \(p^{i+1} = q f_k + r f_k\), whence

\[
p^{i+1} a(d) = r f_k \beta(a(d)) = r f_k \beta \left( \sum_i l_j \right) = r f_k \beta (l_k) = p^{i+1} \beta (l_k).
\]
We fix now a set of free $R_k$-generators $\{d_{k,i} \in D_k\}$ of $D_k$. We have that $p^i(\beta(d_{k,i})) = p^n(\beta)(d_{k,i})$, where $\beta$ is an $R$-module homomorphism. Therefore if we define the $R$-module homomorphism $\gamma: p^n D \rightarrow p^n L$ by setting $\gamma(p^i d_{k,i}) = p^n(\beta)(d_{k,i})$, we obtain that $\gamma$ is well-defined and $\beta \circ \gamma = \beta$ on $p^n D$. Let $u = z_1 + z_2$, so that $p^n(\beta) \subseteq p^n D$. Set $N = p^n M$ and let $\pi$ be the natural projection from $p^n L \wedge p^n L$ onto $p^{2n} L$ and $\alpha = \gamma \circ \tau$. Then $\beta: p^n L \rightarrow N, \quad p^n L \wedge p^n L \rightarrow p^n L, \quad \alpha: p^n L \wedge p^n L \rightarrow N$ and $\beta \circ \alpha = \beta \circ \tau$. Hence $\beta([p^n L, \alpha]) = 0$ and so $N$ is a (Lie ring) quotient of $p^n L/\langle p^n L, \alpha \rangle$.

4. THE PROOF OF THE MAIN RESULT

If $L$ is a lattice, the tensor product $L = \mathbb{Q}_p \otimes L$ belongs to the category $\mathbb{K}$. We call $L$ simple if $L^2 \neq 0$ and there is no proper $\mathbb{Q}_p[x]$-submodule $A$ of $L$ such that $L : A \simeq A$. Also $L$ is called maximal if there are no lattice $N$ and injective morphism $\phi: L \rightarrow N$ in $\mathbb{K}$ such that $\phi(L) < N$ and $L \cong N$. The first step in the proof of our main result is to show that if $L$ is a lattice and $L$ is simple then there exists a maximal lattice $M$ such that $L \leq M < L$.

First we need some preliminary lemmas.

**Lemma 4.1.** Let $M, N$ be $R$-submodules of $L$ such that $\mathbb{Q}_p M = L$, $M \leq N$ and $N$ is finitely generated. Then $|N : M|$ is finite.

**Proof.** Since $\mathbb{Q}_p M = L$, $N/M$ is a $\mathbb{Z}_p$-torsion module. By using that $N$ is finitely generated, we obtain that $|N : M|$ is finite.

**Lemma 4.2.** Suppose $M \leq N$ are lattices. Then $|N : M|$ is finite if and only if $M \cong N$.

**Proof.** We can decompose $M$ and $N$ as follows: $M = \bigoplus_i M_i$ and $N = \bigoplus_i N_i$, where $M_i \cong R^j_i$ and $N_i \cong R^j_i$ for some non-negative integers $s_i$ and $t_i$. It is clear from the hypothesis $M \leq N$ that $M_i \subseteq N_i$, whence $s_i \leq t_i$. Moreover $s_i = t_i$ if and only if $N_i/M_i$ is finite. Now the result is clear bearing in mind that the condition $M \cong N$ amounts to the equalities $s_i = t_i$ for all $i$.

Now we give a criterion for a $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p$ to be finitely generated.

**Lemma 4.3.** Let $N$ be a $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p$ and suppose that $\{n \in N \mid p^{-n} n \in N \text{ for every } k \in \mathbb{N}\} = 0$. Then $N$ is finitely generated.

**Proof.** We prove it by induction on $k$. For $k = 1$ it is trivial. Suppose that we have proved the result for $k - 1$. Then
Of course we can suppose $N \not= 0$. We choose an element $x \in N$ with $p^{-1}x \not\in N$ and define

$$\bar{N} = N/\mathbb{Z}_p x = N/(Q_p x \cap N) \cong (N + Q_p x)/Q_p x.$$  

Suppose there exists $n \in N \setminus \mathbb{Z}_p x$ such that $p^{-k}(n + Q_p x) \subseteq N + Q_p x$ for every $k \in \mathbb{N}$. Then for every $k \geq 0$ there exists $a_k \in Q_p$ such that $p^{-k}(n + a_k x) \in N$. Since $p^{-1}x \not\in N$, $a_k \in \mathbb{Z}_p$ and $a_{k+1} - a_k \in p^k \mathbb{Z}_p$. Let $a = \lim_{k \to \infty} a_k$. Then $p^{-k}(n + ax) \in N$ for every $k \in \mathbb{N}$, which is impossible because $n + ax \not= 0$. Thus, no such an element $n$ exists and this allows us to apply the inductive hypothesis on $N$. Then $\bar{N}$ is finitely generated and so is $N$.

**Lemma 4.4.** Suppose $L$ is simple, $M$ is a lattice, and $L < M < L$. Define $\tau(L) = \min \{ t | p^{t}L \subseteq L^2 \}$ and $k = \max \{ t | L \subseteq p^{t}M \}$. Then $\tau(L)$ is finite and $k \leq \tau(L)$.

**Proof.** Since $L$ is simple, $L^2 = L$ and $Q_p L^2 = \mathbb{Z}_p L$. By Lemma 4.1, $|L : L^2|$ is finite and so $\tau(L)$ is also finite. By the definitions of $\tau(L)$ and $k$, we obtain

$$p^{\tau(L)}L \subseteq L^2 \subseteq p^{k+1}M \subseteq p^k M.$$  

By Lemma 4.1, $k$ is finite, so by the maximality of $k$ it follows that $2k - \tau(L) \leq k$, whence $k \leq \tau(L)$.

**Proposition 4.5.** Suppose $L$ is simple. Then there is no proper ascending series of lattices $L < L_1 < L_2 \cdots < L$.

**Proof.** Suppose there exists an infinite series of lattices $L < L_1 < L_2 \cdots < L$ and $K \subseteq \bigcup_{i \geq 1} L_i$. Then it is clear that $K \in \mathcal{L}$. Define $A = \{ a \in K | p^{-k}a \in K \text{ for every } k \in \mathbb{N} \}$. Then $A$ is a $Q_p[x]$-submodule of $L$. For any $l \in K, a \in A$ and $k \in \mathbb{N}$ we have

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

Hence $K \cdot A \subseteq A$. Since $L = Q_p K, L \cdot A \subseteq A$ and either $A = 0$ or $L$.

In the former case, by Lemma 4.3, $K$ is a finitely generated $R$-module and so, by Lemma 4.1, $|K : L|$ is finite, which is a contradiction.

If $A = L$ fix $a_1, \ldots, a_m$ an $R$-system of generators of $L$. Since $p^{-n(L)-1}a_i \in K$, there exists $k \geq 1$ such that $p^{-n(L)-1}a_i \in L_k$ for all $i$. Hence $L \subseteq p^{n(L)+1}L_k$, which contradicts Lemma 4.4.

**Corollary 4.6.** Suppose $L$ is simple. Then there exists a maximal lattice $M$ such that $L \leq M < L$.
Proof. By Proposition 4.5 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 $N$ and an injective morphism $\phi$ such that $\phi(M) < N$ and $M \cong N$. By Lemma 4.2, $N(\phi(M))$ 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 $\psi: N \to \mathbb{L}$ by means of $\psi(n) = p^{-k} m \in \mathbb{L}$. This map is well defined and it is a morphism in the category $\mathbb{L}$. Hence $L \leq N < \psi(N) < \mathbb{L}$, against the choice of $M$.

For $k = (k_1, \ldots, k_n)$, with the number $k_j$ non-negative integer and $\sum k_j = m$, we set $T^{(k)} = \bigoplus_i R_j^k$, $\mathcal{E}^{(k)} = \{(T^{(k)}, \alpha) \in \mathcal{E} | \alpha \in \mathcal{E}(T^{(k)} \wedge T^{(k)})\}$ and $\mathbb{E}^{(k)} = \{(T^{(k)}, \alpha) \in \mathbb{E} | \alpha(T^{(k)} \wedge T^{(k)}) \leq p^{n-1} T^{(k)}\}$. We can define a structure of compact metric space on $\mathbb{E}^{(k)}$ by putting $\rho((T^{(k)}, x), (T^{(k)}, x_j)) = 1/n$ if $(T^{(k)}, x_1 - x_2)$ is in $\mathbb{E}^{(k)}$ but not in $\mathbb{E}^{(k+1)}$.

Let $L \in \mathbb{E}$ and define $\gamma(L) = \max\{n | T^{(k)}(L) \leq p^n L\}$. Put $L^{(0)} = L$ and, for $i > 0$, $L^{(i)} = L^{(i-1)} \setminus L^{(i-1)}$.

**Proposition 4.7.** There exists $a = a(p, m, n) \geq 0$ such that for every maximal lattice $L$ of $x$-rank $m$ and for every integer $s \geq 0$, $p^{a + s} L / \Gamma(p^n L)$ has $x$-rank less than $m$.

**Proof.** Suppose for every $j$ there exists a maximal lattice $L_j$ of $x$-rank $m$ such that $\gamma(L_j) > j$. Since the number of possible choices for the numbers $k_j$ is finite, we can suppose that for all $j$, $L_j \cong T^{(k_j)}$ for some $k_j = (k_{j1}, \ldots, k_{jn})$, whence $L_j \cong \mathcal{E}(T^{(k_j)})$ for some $x_j \in \mathcal{E}(T^{(k_j)} \wedge T^{(k_j)}, T^{(k_j)})$. Since $\mathcal{E}^{(k)}$ is compact, for some $\{j_i\}$ there exists $\lim_{i \to \infty} x_j = x = (T^{(k)}, x)$. It is clear that $\gamma(L) = 0$ and so $L$ is a Lie ring. By Kreknin’s Theorem $L$ is solvable. Hence, there exists an abelian ideal $A \neq \{0\}$ (for example, $A = L^{(1)}$), where $d$ is the derived length of $L$ which is also an $R$-submodule. Let $\bar{A} = \{t \in L | p^d t \in A \text{ for some } k \in \mathbb{N}\}$. It is clear that $\bar{A}$ is an abelian ideal of $L$ and satisfies the conditions of Corollary 3.3. Thus, $A \cong \bigoplus_i R_j^k$ and there exists $B \cong \bigoplus_i R_j^k$ such that $T^{(k)} = A \oplus B$. Since $(\bar{A}, x - x_j) \in \mathcal{E}(n)$ for some $j$, we have $x_j(T^{(k)} \wedge \bar{A}) \leq A + p^n T^{(k)}$ and $x_j(T^{(k)} \wedge A) \leq p^n T^{(k)}$. Let $M = (1/p) A \oplus B \cong T^{(k)}$ and denote by $\beta$ the natural extension of $x_j$ to $M \times M$. Then $(T^{(k)}, x_j) < (M, \beta)$, against the maximality of $(T^{(k)}, x_j)$. We conclude that there exists $a = a(p, m, n)$ such that $\gamma(L) \leq a_1$ for every maximal lattice $L$ of $x$-rank $m$.

Let $L \in \Gamma(L)$ \setminus $p^n L$. Write $L$ as $\bigoplus_i L_i$, where $L_i \cong R_j^k$ and let $l = \sum_i l_i$, where $l_i \in L_i$. Since $l \notin p^n L$, there is an index $i$ such that $l_i \notin p^n L$. By Lemma 3.2, $i = p^{l_1} \in \Gamma(L) \setminus p^{a_1 + m} L$. Put $a = a_1 + 3$. Then $p^{a_1} \notin \bigcup L_i \cap \Gamma_L(p^n L)$ and $p^{a_1} \notin \bigcup L_i \cap \Gamma_L(p^n L)$. Hence, the $x$-rank of $p^{a_1 + m} L / \Gamma(p^n L)$ is less than $m$. \[\square\]
Theorem 4.8. Theorem 1.1 is true for \( m = 1 \).

Proof. By Theorem 3.1 we can suppose that \( M \cong L / \Gamma(L) \), where \( L \cong R_k \) for some \( 1 \leq k \leq n \). If \( L^2 = 0 \) then we are done. If \( L^2 \neq 0 \) then \( \mathbb{K} \) is simple, and by Corollary 4.6, there exists a maximal lattice \( N \) such that \( L \leq N < \mathbb{K} \). Since \( N \cong R_k \), we have \( L = (x - 1)^t N \) for some \( t \geq 0 \). Let \( s = \min \{ k \mid p^k N \subseteq L \} \). (Actually, \( s = \left\lceil \frac{(t - 1)}{p^k - 1} (p - 1) \right\rceil + 1 \)). Since \( |L : p^k N| \leq p^n \), we can suppose \( L = p^k N \). Hence, from Proposition 4.7 there is \( f = f(p, n) \) such that \( p^{q_3(M)} = 0 \).

Now we prove Theorem 1.1 by induction on \( m \). The case \( m = 1 \) has proved in the previous theorem. Suppose now that \( m > 1 \) and also that Theorem 1.1 is true for \( m - 1 \).

Proposition 4.9. Suppose \( \mathbb{K} \) is simple, \( M \in \mathbb{K} \) is maximal, and \( L \leq M < \mathbb{K} \). We define \( s = \min \{ k \mid p^k M \subseteq L \} \). Then there are functions \( f_1 = f_1(p, n, m) \) and \( f_2 = f_2(p, m, n) \) such that \( p^f L^{(2^n - 2)} \subseteq p^f M + \Gamma(L) \) and \( (p^{3^f} + s(M))^{(2^n - 2)} \subseteq \Gamma(L) \).

Proof. We can decompose \( L \) and \( M \) as follows: \( L = \bigoplus_{i=1}^n L_i \) and \( M = \bigoplus_{i=1}^n M_i \), where \( L_i \cong M_i \cong R_k \). It is clear that \( L_i \subseteq M_i \) and \( s = \max \{ k \mid p^k M_i \subseteq L_i \} \). From this observation it follows that if we define \( \bar{L} = L / ((p^{k-1} M) \cap L) + \Gamma(L) \) then the \( x \)-rank of \( \bar{L} \) is less than \( m \). By the inductive hypothesis, there exists a function \( f_1 = f_1(p, n, m) \) such that \( p^f \bar{L}^{(2^n - 2)} \subseteq p^f M + \Gamma(L) \).

Now, by Proposition 4.7, there exists \( a = a(p, m, n) \) such that the Lie ring \( p^{3^f} + s(M) / \Gamma(p^f M) \) has \( x \)-rank less than \( m \). Since \( p^f M \subseteq L \), we have that \( \text{rk}(p^{3^f} + s(M) / \Gamma(p^f M)) \) and the proof is finished by applying again the inductive hypothesis.

Proof of Theorem 1.1. By Theorem 3.1 we can suppose that \( M \cong L / \Gamma(L) \), where \( L \) is a lattice of \( x \)-rank \( m \). If \( \mathbb{K} \) is simple then, by Proposition 4.9, there exists \( f = f(p, m, n) \) such that \( (p^{3^f} + s(M))^{(2^n - 2)} = 0 \).

Suppose now that \( \mathbb{K} \) is not simple. Then there exists a \( \mathbb{K}[x] \)-submodule \( 0 \neq A \neq \mathbb{K} \) such that \( A \cdot L \leq A \). Let \( B = A \cap L \). From Corollary 3.3 there exists \( C \) such that \( L = B \oplus C \). Note that the \( x \)-rank of \( B \) and \( C \) is less than \( m \) and \( B = (B + \Gamma(L)) / \Gamma(L) \) is an ideal of \( L / \Gamma(L) \), so the theorem follows from the inductive hypothesis.

5. FINAL REMARKS

In fact, the proof of Theorem 1.1 gives us the following result.
Theorem 5.1. Under the hypothesis of Theorem 1.1, there exists a subring $\mathcal{N}$ of $(p, m, n)$-bounded index such that $\gamma_3(\gamma_3(...\gamma_3(N)...)) = 0$, where $\gamma_3$ appears $2^m - 1$ times.

We expect that this result can be improved and pose the next conjecture.

Conjecture. The number of times that $\gamma_3$ appears in Theorem 5.1 can be reduced to $m$.

We think that the method of this paper will be useful in other situations. For example, in [3] a similar argument is used to prove that a finite $p$-group of rank $r$ admitting an automorphism with $p^m$ fixed points has a subgroup $H$ of $(p^m, r)$-bounded index and $r$-bounded derived length. For background on this problem see [7; 9, Problem 13.56; 19].

REFERENCES


