# Ellipticity of words

Consuelo Martínez*
Departamento de Matemáticas, Universidad de Oviedo,
C/ Calvo Sotelo, s/n, 33007 Oviedo SPAIN

*Dedicated to Efim Zelmanov on his 60th birthday*

**Abstract**

We prove that an arbitrary word $v$ of the free pro-$p$-group is elliptic on a pro-$p$-completion of a discrete finitely generated torsion residually-$p$ group.

## 1 Introduction

Let $p$ be a prime number. We say that a group $G$ is residually-$p$ if

$$\bigcap\{H \triangleleft G \mid |G:H| = p^k,\ k \geq 1\} = (1).$$

In this case the subgroups $H$ of the above intersection can be viewed as a basis of neighborhoods of 1, thus making $G$ a topological group. If the topology is complete, then we say that $G$ is a pro-$p$-group. If not, then the completion $G_{\hat{p}}$ of the group $G$ is called the pro-$p$-completion of $G$.

Let $F(\infty)$ be the free group on the countable set of generators $x_1, x_2, \ldots$. The pro-$p$-completion $F = F(\infty)_{\hat{p}}$ is called a free pro-$p$-group on $x_1, x_2, \ldots,$. We call an element $w \in F$ a word if it involves finitely many generators.

*Partially supported by MTM 2013-45588-C3-1-P and GRUPIN 14-142

Let $G$ be a pro-$p$-group and let $w = w(x_1, \ldots, x_n) \in F$. Consider

$$w(G) = \{w(g_1, \ldots, g_n) \,|\, g_i \in G,\ 1 \leq i \leq n\}$$

the set of values of the word $w$ in $G$ and let $\langle \overline{w(G)} \rangle$ denote the closed subgroup of $G$ generated by the set $w(G)$.

We say (see [S ]) that the word $w$ is *elliptic* (or has finite verbal width) on $G$ if there exists $N \geq 1$ such that $\langle \overline{w(G)} \rangle = \underbrace{w(G)^{\pm 1} \cdots w(G)^{\pm 1}}_{N}$. This is equivalent to say that the discrete subgroup of $G$ generated by $w(G)$ is closed in $G$.

It is known that on some important classes of pro-$p$-groups ($p$-adic analytic pro-$p$-groups [JZ], the Nottingham group [Kl]) all words are elliptic.

In the first chapter we prove the following theorem

**Theorem 1.1** *Let $\Gamma$ be a finitely generated residually-$p$ torsion group. Then an arbitrary word $w \in F$ is elliptic on $G = \Gamma_{\hat{p}}$.*

We remark that the celebrated groups of Golod-Shafarevich, Grigorchuk or Gupta-Sidki are residually-$p$ torsion groups.

In the second chapter we prove a stronger statement for the so called *multilinear words.*

Let $w = w(x_1, \ldots, x_n) \in F$. Let $G$ be a pro-$p$-group. Choose elements $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in G$ and fix all variables $x_j = a_j$ except one $x_i$. Denote $\alpha = (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ and consider the set $w(G, i, \alpha) = \{w(a_1, \ldots, a_{i-1}, g, a_{i+1}, \ldots, a_n) \mid g \in G\}$.

**Definition 1.1** *We say that the element $w$ is strongly elliptic on $G$ if there exist finite subsets $M_i \subseteq \underbrace{G \times \cdots \times G}_{n-1}$, $1 \leq i \leq n$, and an order on $\cup_{i=1}^{n} M_i = \{\alpha_1 < \alpha_2 < \cdots < \alpha_q\}$, $\alpha_k \in M_{i_k}$, $1 \leq k \leq q$, $1 \leq i_k \leq n$, such that the verbal subgroup $\langle \overline{w(G)} \rangle$ is equal to*

$$w(G, i_1, \alpha_1)^{\pm 1} \cdots w(G, i_q, \alpha_q)^{\pm 1}.$$

Clearly, if a word is strongly elliptic on $G$ then it is elliptic.

By the result of J. P. Serre [Se] the commutator is strongly elliptic on finitely generated pro-$p$-groups.

Consider the lower central series of $F$, $F = F_1 \geq F_2 \geq \cdots$, and the Zassenhaus series $F = F_{(1)} \geq F_{(2)} \geq \cdots \geq F_{(n)} \geq \cdots$, where $F_{(n)}$ is the subgroup of $F$ generated by all powers $g^{p^j}$, $g \in F_i$, $ip^j \geq n$. Both series (central series) lead to Lie algebras $L(F) = \bigoplus_{i \geq 1} F_i/F_{i+1}$ and $L_p(F) = \bigoplus F_{(i)}/F_{(i+1)}$.

**Definition 1.2** *Let $w \in F$ be a word. Suppose that $w \in F_n \setminus F_{n+1}$. We call the word $w$* **multilinear** *if $w = \bar{w}w'$, where*

*(i) $\bar{w}$ is a product of powers of left-normed commutators,*

$$\bar{w} = \prod_{\sigma \in S_n} [\cdots [x_{\sigma(1)}, x_{\sigma(2)}], \cdots, x_{\sigma(n)}]^{k_\sigma},$$

*where $k_\sigma \in \mathbb{Z}_p$ are $p$-adic integers such that the element $\bar{w}F_{n+1}$ does not belong to $pL(F)$,*

*(ii) the element $w' \in F_{n+1}$ is a (converging) product of commutators in $x_1, \ldots, x_n$ of length $\geq n+1$, each commutator involves all $n$ generators $x_1, \ldots, x_n$.*

**Theorem 1.2** *Let $\Gamma$ be a finitely generated residually-$p$ torsion group. Then an arbitrary multilinear word is strongly elliptic on the pro-$p$-group $G = \Gamma_{\hat{p}}$, the pro-$p$-completion of $\Gamma$.*

A linearization process leads to

**Theorem 1.3** *For an arbitrary nonidentical word $w \in F$ there exist a multilinear element $\tilde{w} \in \overline{\langle w(F) \rangle}$.*

# 2 Verbally just infinite pro-$p$-groups

We say that a pro-$p$-group $G$ is verbally just infinite if $G$ is infinite and for an arbitrary word $w \in F$ either $w(G) = 1$ or $|G : \overline{\langle w(G) \rangle}| < \infty$.

**Lemma 2.1** *Let $G$ be a finitely generated verbally just infinite pro-$p$-group. Then an arbitrary word $w \in F$ is elliptic on $G$ or $G$ is virtually abelian.*

**Proof.** Let $G$ be a finitely generated pro-$p$-group that is not virtually abelian. Let $w \in F$, $H = \langle \overline{w(G)} \rangle$. If $H = (1)$, then the word $w$ is clearly elliptic on $G$. If $H \neq (1)$ then the subgroup $H$ has finite index in $G$ and, therefore, is a finitely generated pro-$p$-group.

Since the group $G$ is not virtually abelian it follows that $[H, H] \neq (1)$. By the result of J. P. Serre [Se], the subgroup $[H, H]$ is closed in $G$.

Consider the word

$$v(x_1, \ldots, x_m, y_1, \ldots, y_m) = [w(x_1, \ldots, x_m), w(y_1, \ldots, y_m)].$$

Clearly, $[H, H] = \langle \overline{v(G)} \rangle$. By the assumption of the lemma, $|G : [H, H]| < \infty$.

Let $h_1, \ldots, h_r \in w(G)^{\pm 1}$ be a maximal system of elements that are distinct module $[H, H]$. Then $h_1, \ldots, h_r$ generate $H$. By the result of J. P. Serre [Se] we have

$$[H, H] = [H, h_1] \cdots [H, h_r].$$

Every element of $H$ can be represented as $h_{i_1} \cdots h_{i_t}$, $t \leq |H : [H, H]|$, modulo $[H, H]$. Hence

$$H = \bigcup h_{i_1} \cdots h_{i_t} [H, h_1] \cdots [H, h_r].$$

Now the verbal width of $w$ is $\leq |H : [H, H]| + 2r$ since $[x, h_i] = (h_i^x)^{-1} h_i \in w(G)^{\pm 1} \cdot w(G)^{\pm 1}$. This completes the proof of the lemma.

**Remark.** A finitely generated virtually abelian pro-$p$-group $G$ is $p$-adic analytic. If $w \in F(\infty)$ then $w$ is elliptic on $G$ by the result of A. Jaikin-Zapirain [JZ]. Most likely this is also the case when $w \in F \setminus F(\infty)$, but there are no references.

Let $G$ be a pro-$p$-group and let $1 \neq w \in F$. We say that the group $G$ satisfies the pro-$p$- identity $w = 1$ if $w(G) = (1)$.

The following theorem was proved by E. Zelmanov ( [Z3]).

**Theorem 2.1** *Let $G$ be a pro-$p$-group satisfying a nontrivial pro-$p$-identity and having a dense finitely generated torsion discrete subgroup. Then $|G| < \infty$.*

**Lemma 2.2** *Let $\Gamma$ be a finitely generated residually-p torsion group, $G = \Gamma_{\hat{p}}$. Then either $|\Gamma| < \infty$ or $G$ is a verbally just infinite group.*

**Proof.** Suppose that the groups $\Gamma$ and $G$ are infinite. Let $1 \neq w = w(x_1, \ldots, x_n) \in F$ be a word. We need to show that the subgroup $H = \overline{\langle w(G) \rangle}$ has finite index in $G$.

Consider the pro-$p$-group $G^\sharp = G/H$ and the discret subgroup $\Gamma^\sharp = \Gamma H/H$. The group $\Gamma^\sharp$ is finitely generated, torsion and dense in $G^\sharp$. The pro-$p$-group $G^\sharp$ satisfies a non trivial pro-$p$-identity. Then, by Zelmanov's theorem , $|G^\sharp| < \infty$, what finishes the proof of the lemma.

**Proof of Theorem 1.1**

Let $\Gamma$ be a finitely generated residually-$p$ torsion group and let $G = \Gamma_{\hat{p}}$ be its pro-$p$-completion. Let $w \in F$ be a word. If $|\Gamma| < \infty$ then the result is obvious. Suppose therefore that $\Gamma$ is infinite. By Lemma 2.2 the pro-$p$-group $G$ is verbally just infinite. We remark that the group $G$ is not virtually abelian since then a finitely generated torsion virtually abelian group $\Gamma$ would be finite. Now Lemma 2.1 implies the word $w$ is elliptic on $G$.

# 3 Multilinear words

Let's recall the construction of a Lie ring associated to a pro-p-group $G$.

Consider the lower central series $G = G_1 > G_2 > \cdots$ of the group $G$, $G_{n+1} = [G_n, G]$. Clearly $[G_i, G_j] \subseteq G_{i+j}$, the abelian group $G_i/G_{i+1}$ is a module over the ring of p-adic integers $\mathbb{Z}_p$.

Consider the direct sum

$$L(G) = \oplus_{i \geq 1} G_i/G_{i+1}.$$

The Lie ring multiplication is defined on homogeneous elements by

$$[aG_{i+1}, bG_{j+1}] = [a, b]G_{i+j+1}$$

and extended to arbitrary elements by linearity. This makes $L(G)$ a Lie algebra over $\mathbb{Z}_p$.

For the free pro-p-group $F$ the Lie algebra $L(F)$ is known to be the free Lie $\mathbb{Z}_p$-algebra on the set of free generators $\bar{X} = \{\bar{x}_i = x_i F_2 \,|\, i \geq 1\}$

Along with the lower central series of $F$, $F = F_1 \geq F_2 \geq \cdots$, we consider the Zassenhaus series $F = F_{(1)} \geq F_{(2)} \geq \cdots \geq F_{(n)} \geq \cdots$, where $F_{(n)}$ is the subgroup of $F$ generated by all powers $g^{p^j}$, $g \in F_i$, $ip^j \geq n$, $[F_{(i)}, F_{(j)}] \subseteq F_{(i+j)}$, $\cap_{i\geq 1} F_{(i)} = (1)$, each factor $F_{(i)}/F_{(i+1)}$ is an elementary abelian p-group. The Zassenhaus series gives rise to the Lie algebra $L_p(F) = \bigoplus F_{(i)}/F_{(i+1)}$ over the field $\mathbb{Z}/p\mathbb{Z}$.

**Proof of Theorem 1.3**

The proof of this result imitates the well known linearization process in algebras (see [SSSZ]) or, equivalently, Higman's collection process in groups [H ].

As always we consider the free group $F(\infty)$ and the free pro-$p$-group $F$ on the set $X = \{x_i \,|\, i \geq 1\}$ of free generators.

Let $w \in F_{(n)} \setminus F_{(n+1)}$. Replacing $w$ by a group commutator $[w, x_i]$, if necessary, we may assume that $n$ is coprime to $p$. The element $w$ can be represented as $w = \bar{w}w'$, where $\bar{w}$ is a product of $\rho^{p^j}$, $\rho$ is a commutator in $X$ of length $i$, $ip^j = n$, $w' \in F_{(n+1)}$.

Since $n$ is coprime to $p$ it follows that all $j = 0$, that is, $\bar{w}$ is a product of commutators of length $n$ in $X$. If $\bar{w}F_{n+1} \in p(F_n/F_{n+1})$ then $\bar{w} \in F_{(n+1)}$, a contradiction.

Let $Lie\langle X\rangle$ denote the free Lie $\mathbb{Z}_p$-algebra on the same set of free generators $X$ and $\bar{X} = \{\bar{x}_1, \bar{x}_2, \ldots\}$, where $\bar{x}_i = x_i F_2$. Consider the element $f(\bar{x}_1, \ldots, \bar{x}_m) = \bar{w}F_{n+1}$ of the free Lie $\mathbb{Z}_p$-algebra $Lie\langle \bar{X}\rangle$. The element $f(\bar{x}_1, \ldots, \bar{x}_m)$ is homogeneous of total degree $n$ and $f \notin pLie\langle \bar{X}\rangle_n$. The element $f$ does not, though, have to be homogeneous in each variable $\bar{x}_i$.

For a multiindex $d = (d_1, \ldots, d_m)$, $d_i \geq 0$, $\sum_{i=1}^m d_i = n$ let $f_d$ be the homogeneous component of $f$ having degree $d_i$ in $\bar{x}_i$, $1 \leq i \leq m$.

For a fixed index $i$, $1 \leq i \leq m$, let $f_i' = \sum_{d_i \neq 0} f_d$, $f_i'' = \sum_{d_i = 0} f_d$. Then $f = f_i' + f_i''$.

If $f_i'' \notin pLie\langle \bar{X}\rangle_n$, then considering $w(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_m)$ (that lies in $\langle w(F)\rangle$) instead of $w$ we cut the number of variables.

If $f_i' \notin pLie\langle \bar{X}\rangle_n$, then considering $w := ww(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_m)^{-1}$ instead of $w$ we can assume that $f = \sum_{d_i \neq 0} f_d$.

Arguing in this way with all generators $x_1, \dots, x_m$ we will assume that $f(\bar{x}_1, \dots \bar{x}_m) = \sum f_d(\bar{x}_1, \dots \bar{x}_m)$, where for each multiindex $d$ on the right hand side we have $d_1 \geq 1, \dots, d_m \geq 1$.

Fix a multiindex $d = (d_1, \dots, d_m)$, $d_i \geq 1$ such that $f_d \notin pLie\langle \bar{X}\rangle_n$. For each $i, 1 \leq i \leq r$, choose a set of $d_i$ elements $X_i = \{x_{i1}, \dots, x_{id_i}\} \subset X$ such that the subsets $X_1, \dots, X_m$ do not intersect. (If $d_i = 1$ then we choose $X_i = \{x_i\}$).

For a nonempty subset $S \subseteq [1, d_i]$ let $\bar{X}_i(S) = \sum_{j \in S} \bar{x}_{ij}$.

For a nonnegative integer $a$, let us define $sgn(a) = (-1)^a$. The element

$$\tilde{f} = \sum_{\emptyset \neq S_i \subseteq [1,d_i]} sgn(\sum_{i=1}^{r}(d_i - |S_i|)) f(\bar{X}_1(S_1), \dots, \bar{X}_m(S_m)) =$$

$$\sum_{\emptyset \neq S_i \subseteq [1,d_i]} sgn(\sum_{i=1}^{r}(d_i - |S_i|)) f_d(\bar{X}_1(S_1), \dots, \bar{X}_m(S_m))$$

is multilinear in all variables $\bar{x}_{ij}$, $1 \leq i \leq m$, $1 \leq j \leq d_i$.

We call $\tilde{f}$ the complete linearization of $f$, that corresponds to the multiindex $d$. Of course, it depends on the choice of $d$.

We use two facts about complete linearizations over a field (see [SSSZ]):

(1) If $h(x_1, \dots, x_m)$ is a homogeneous (in all variables) element of degree multiindex $d' = (d_1', \dots, d_m')$, $d_i' \geq 1$, $\sum_{i=1}^m d_i' = \sum_{i=1}^m d_i$ and $d' \neq d$, then the complete linearization corresponding to the multiindex $d$ turns $h$ into 0,

(2) let $h$ be a nonzero element of a free Lie (associative) algebra over a field which is homogeneous in all variables. Then the complete linearization of $h$ is $\neq 0$.

The assertions (1), (2) imply that $\tilde{f} \neq 0 \bmod p$.

Now let us imitate the above process in the free pro-$p$-group. For a nonempty subset $S \subseteq [1, d_i]$ let $X_i(S)$ be a product of generators $x_{ij}$, $j \in S$, in an arbitrary order.

Let $v$ be a product of elements of the form

$$w(X_1(S_1), \dots, X_m(S_m))^{sgn(\sum_{i=1}^m (d_i - |S_i|))}$$

in an arbitrary order, where $S_i$ run over all nonempty subsets of $[1, d_i]$.

It is straightforward that $v \in F_{(n)}$ and $vF_{(n+1)} = \tilde{f}(x_{ij}F_{(2)}) \neq 0$.

Changing names of free generators, if needed, we can say that we found a nonidentical element $v \in \langle w(F)\rangle$ such that $v = \bar{v}v'$, the element $\bar{v}$ is a product of multilinear commutators $[\dots[x_{\sigma(1)}, x_{\sigma(2)}], \dots, x_{\sigma(n)}]$, $\sigma \in S_n$, $\bar{v} \notin F_{(n+1)}$, $v' \in F_{(n+1)}$.

Collecting at the right end all commutators not involving $x_1$, then collecting again, among all those commutators that include $x_1$, those that do not involve $x_2$ (again at the right end) and so on, finally we can represent $v'$ as $v' = v''v_n \cdots v_2v_1$, where $v''$, $v_i \in F_{(n+1)}$, the element $v_i$ is a product of commutators (of length $\geq n+1$ ) that involve $x_1, \dots, x_{i-1}$ and do not involve $x_i$. The element $v''$ is a product of commutators that involve $x_1, x_2, \dots, x_n$.

Let us show, by induction on $i$, that $v_i \in \langle v(F)\rangle$. Substituting $x_1 = 1$ we get $v|_{x_1=1} = v_1$. Hence $v_1 \in \langle v(F)\rangle$. Now substituting $x_i = 1$ we get $v|_{x_i=1} = v_i(v_{i-1}|_{x_i=1}) \cdots (v_1|_{x_i=1})$. Hence $v_i \in \langle v(F)\rangle$.

It implies that $\bar{v}v'' \in \langle v(F)\rangle$, $v''$ is product of commutators of length $\geq n+1$, involving $x_1, \dots, x_n$ and of $p$-powers $[\dots[x_{\sigma(1)}, x_{\sigma(2)}], \dots, x_{\sigma(n)}]^{p^k}$, $k \geq 1$, $\sigma \in S_n$. Moving all these p-powers to the left we get

$$\bar{v}v'' = (\prod_{\sigma \in S_n} [\dots[x_{\sigma(1)}, x_{\sigma(2)}], \dots, x_{\sigma(n)}]^{k_\sigma})v''',\ k_\sigma \in \mathbb{Z}_p,$$

and $v'''$ is a (converging) product of commutators of length $\geq n+1$ involving all $x_1, \dots, x_n$. Substituting 1 for all generators that do not belong to $\{x_1, \dots, x_n\}$ we can assume that all factor commutators in $v'''$ involve only $x_1, \dots, x_n$. This finishes the proof of Theorem 1.3.

In order to prove Theorem 1.2 we will have to adapt the above definitions to Lie algebras.

As above, let $X = \{x_i \,|\, i \geq 1\}$ and let $Lie\langle X\rangle$ denote the free Lie $\mathbb{Z}_p$-algebra on the set of free generators $X$. Let $f(x_1, \dots, x_n)$ be a multilinear element from $Lie\langle X\rangle$ and let $L$ be a Lie algebra over $\mathbb{Z}_p$.

Consider the set $f(L) = \{f(a_1, \dots, a_n) \,|\, a_i \in L\}$ of values of the element $f$ on $L$.

**Definition 3.1** *We say that the element $f$ is* **elliptic** *on $L$ if there exists $N \geq 1$ such that the $\mathbb{Z}_p$-linear span of $f(L)$, $Spanf(L)$, is*

$$Span(f(L)) = \underbrace{f(L) + \cdots + f(L)}_{N}.$$

**Definition 3.2** *We say that the element $f$ is* **strongly elliptic** *on $L$ if there exist finite sets $M_i \subseteq \underbrace{L \times \cdots \times L}_{n-1}$, $1 \leq i \leq n$, such that $Spanf(L)$ is a sum of additive subgroups $f(a_1, \ldots, a_{i-1}, L, a_{i+1}, \ldots, a_n)$, where $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in M_i$, $1 \leq i \leq n$.*

Clearly a strongly elliptic multilinear element is elliptic.

An element $a$ of a Lie algebra is said to be ad-nilpotent if the linear transformation $ad(a)$ is nilpotent.

**Lemma 3.1** *Let $L$ be a Lie $\mathbb{Z}/p^k\mathbb{Z}$-algebra generated by a finite subset $X \subseteq L$ such that an arbitrary commutator in $X$ is ad-nilpotent (we consider elements of $X$ as commutators of length 1). Let $f(x_1, \ldots, x_n) \in Lie\langle X\rangle$ be a multilinear element of the free Lie $\mathbb{Z}_p$- algebra such that $f \notin pLie\langle X\rangle$. Then*
*(i) $I = Spanf(L)$ is a Lie ideal in $L$, $|L : Spanf(L)| < \infty$;*
*(ii) $f$ is strongly elliptic on $L$*

**Proof:** To see that $I = Spanf(L)$ is an ideal in $L$ choose arbitrary elements $b, b_1, \ldots, b_n \in L$. Then

$$[b, f(b_1, \ldots, b_n)] = f([b, b_1], b_2, \ldots b_n) + \ldots + f(b_1, b_2, \ldots, [b, b_n]),$$

which implies the claim.

The Lie algebra $L/I + pL$ (1) is generated by a finite set ( = image of $X$) and every commutator in these generators is ad-nilpotent and (2) satisfies a nontrivial polynomial identity.

By [ Z3] the $\mathbb{Z}/p\mathbb{Z}$-algebra $L/I + pL$ is nilpotent. Hence there exists $s \geq 1$ such that $L^s \subseteq I + pL$.

Since $p^k L = (0)$ this implies $(L^s)^k \subseteq I$.

In [K, P ] it is shown that in a finitely generated solvable Lie algebra $L$ if all commutators in generators are ad-nilpotent, then the algebra is nilpotent.

Hence there exists $d \geq 1$ such that $L^d \subseteq (L^s)^k \subseteq I$. It implies that $|L : I| < \infty$, which finishes the proof of (i).

Again in [K, P] it is shown that in a finitely generated Lie algebra $L$ if all commutators in generators are ad-nilpotent, then each power of $L$ is a finitely generated subalgebra (this result is even valid in rings). Since the algebra $L^d$ is finitely generated and $|I : L^d| < \infty$, it follows that the algebra $I$ is finitely generated.

Suppose that $I$ is generated as a Lie algebra by a finite collection of elements $f(a_{i_1}, \ldots, a_{i_n})$, $1 \leq i \leq r$, $a_{ij}$ are commutators in generators. We have

$$I \subseteq \sum_i (\mathbb{Z}/p^k\mathbb{Z}) f(a_{i_1}, \ldots, a_{i_n}) + \sum_i [L, f(a_{i_1}, \ldots, a_{i_n})] \subseteq$$
$$\sum f(a_{i_1}, \ldots, a_{i_{t-1}}, L, a_{i_{t+1}}, \ldots, a_{i_n}),$$

which means that the element $f$ is strongly elliptic on $L$. This finishes the proof of the lemma.

Let $w = \bar{w}w'$ be a multilinear word from $F$,

$$\bar{w} = \prod_{\sigma \in S_n} [\cdots [x_{\sigma(1)}, x_{\sigma(2)}], \cdots x_{\sigma(n)}]^{k_\sigma}, \ k_\sigma \in \mathbb{Z}_p, \ w' \in F_{n+1}.$$

As we have mentioned earlier, the Lie ring $L(F) = \oplus_{i \geq 1} F_i/F_{i+1}$ is a free Lie $\mathbb{Z}_p$ algebra on the free generators $\bar{x}_i = x_i F_2$, $i \geq 1$.

Let $f(\bar{x}_1, \ldots, \bar{x}_n) = \sum k_\sigma [\bar{x}_{\sigma(1)}, \ldots, \bar{x}_{\sigma(n)}] = wF_{n+1}$ be a multilinear element from $L(F) = Lie\langle \bar{X} \rangle$ that corresponds to $w$.

Let $G$ be a pro-$p$-group, let $G = G_1 > G_2 > \cdots$ be its lower central series. Let $L = L(G) = \oplus_{i \geq 1} G_i/G_{i+1}$ be the Lie algebra linked to the lower central series. As above, $Span f(L)$ denotes the $\mathbb{Z}_p$-linear span of the set $f(L)$. Since $f$ is multilinear it follows (as in Lemma 3.1) that $Span f(L)$ is an ideal of $L$.

**Lemma 3.2** *If $|L : Span f(L)| < \infty$ and $f$ is strongly elliptic on $L$, then $|G : \langle w(G) \rangle| < \infty$ and $w$ is strongly elliptic on $G$.*

**Proof.** Since $|L : Span f(L)| < \infty$, it follows that there is $k \geq 1$ such that $p^k L \subseteq Span f(L)$. Hence $L/Span f(L)$ becomes a $\mathbb{Z}/p^k\mathbb{Z}$-module.

Since the element $f$ is strongly elliptic, there exist finite sets $\bar{M}_i \subseteq \underbrace{L \times \cdots \times L}_{n-1}$, $1 \leq i \leq n$, $\bar{M}_i = \{(a_{j,1}^{(i)}, \ldots, a_{j,i-1}^{(i)}, a_{j,i+1}^{(i)}, \ldots, a_{j,n}^{(i)}) \mid 1 \leq j \leq m_i = |\bar{M}_i|\}$ such that

$$Spanf(L) = \sum f(a_{j,1}^{(i)}, \ldots, a_{j,i-1}^{(i)}, L, a_{j,i+1}^{(i)}, \ldots, a_{j,n}^{(i)}).$$

Without loss of generality we will assume all elements $a_{j,k}^{(i)}$ to be homogenoeus, $a_{j,k}^{(i)} \in L_{d(i,j,k)}$.

Choose elements $g_{jk}^{(i)} \in G_{d(i,j,k)}$ such that $a_{j,k}^{(i)} = g_{jk}^{(i)} G_{d(i,j,k)+1}$.

Let $M_i = \{(g_{j1}^{(i)}, \ldots, g_{jn}^{(i)}),\ 1 \leq j \leq m_i\}$, $1 \leq i \leq n$.

Choose an arbitrary order in $\bigcup_{i=1}^n M_i$.

Let $S$ denote the ordered product $S = \prod_u w(G, i, u)$, $u \in \bigcup_{i=1}^n M_i$. For an $(n-1)$-tuple, $u = (g_{j1}^{(i)}, \ldots, g_{jn}^{(i)}) \in M_i$, denote $d(u) = \sum_{i \neq k=1}^n d(i,j,k)$.

Let $g \in G_r$. Suppose that the element $gG_{r+1} \in L_r$ lies in $Spanf(L)$. Then $gG_{r+1} = \sum f(a_{j,1}^{(i)}, \ldots, a_{j,i-1}^{(i)}, b_{ji}^{(i)}, a_{j,i+1}^{(i)}, \ldots, a_{j,n}^{(i)})$, where $b_{ji}^{(i)}$ are homogeneous elements of degrees $r - \sum_{i \neq k=1}^n d(i,j,k)$.

Choose elements $g_u \in G_{r-d(u)}$, $u = (g_{j1}^{(i)}, \ldots, g_{j,n}^{(i)})$ such that $g_u G_{r-d(u)+1} = b_{ji}^{(i)}$. Then $g = \prod_u w(g_u, i, u)$ modulo $G_{r+1}$, $u \in \bigcup_{i=1}^n M_i$.

From $|L : Spanf(L)| < \infty$ it follows that there exist $t \geq 1$ and $k \geq 1$ such that $p^k L + \sum_{i \geq t} L_i \subseteq Spanf(L)$.

We have $p^k L_1 \subseteq Spanf(L) \subseteq L_2 + L_3 + \cdots$. Hence $p^k L_1 = (0)$.

Let us show that $G_t \subseteq S$. Since the set $S$ is closed (because it is the continous image of a compact set) it is sufficient to show that for any $r \geq t$ we have that $G_t \subseteq SG_r$ (what would imply that $G_t \subseteq \bar{S} = S$.)

Let us use induction on $r$. It is clear if $r = t$ (since $G_t \subseteq SG_t$). Choose $g \in G_t$ and suppose that there exists $s \in S$ such that $gs^{-1} \in G_r$. Then the element $gs^{-1}G_{r+1}$ lies in the $Spanf(L)$. Hence, there exist elements $g_u \in G_{r-d(u)}$ such that $gs^{-1} = \prod_u w(g_u, i, u)$ mod $G_{r+1}$.

Let $s = \prod_u w(g'_u, i, u)$. Then

$$g = s.gs^{-1} \quad mod\ G_{r+1} = \prod_u w(g'_u, i, u) \prod_u w(g_u, i, u) \quad mod\ G_{r+1} =$$

$$= \prod_u w(g'_u g_u, i, u) \quad mod\ G_{r+1}.$$

Indeed, the elements $w(g_u, i, u)$ lie in $G_r$ and therefore they are central modulo $G_{r+1}$. For an arbitrary $u \in \cup_{i=1}^n M_i$, Hall identity $[xy, z] = [x, z][[x, z], y][y, z]$ and multilineariy of $w$ imply that

$$w(g'_u, i, u)w(g_u, i, u) = w(g'_u g_u, i, u) \quad mod\ G_{r+1}.$$

That is, we have proved that if $G_t \subseteq SG_r$ for some $r \geq t$ , then an arbitrary element $g \in G_t$ lies in $SG_{r+1}$, what proves our claim.

All $\mathbb{Z}_p$-modules $G_i/G_{i+1}$ are finitely generated and $p^k(G_i/G_{i+1}) = (0)$. This implies that each term $G_i$ of the lower central series has finite index in $G$. In particular, $|G : G_t| < \infty$.

Hence there exists a finite collection of elements $a_1, \ldots, a_r \in w(G)$ such that

$$\langle\overline{w(G)}\rangle = \bigcup a_{i_1} \cdots a_{i_\mu} G_t \subseteq \bigcup a_{i_1} \cdots a_{i_\mu} S,\ 1 \leq \mu \leq |G : G_t|\ 1 \leq i_1, \ldots, i_\mu \leq r.$$

Let $r' = r|G : G_t|$ and let us repeat $|G : G_t|$ times the sequence $a_1, \ldots, a_r$ :

$$a'_1, \ldots, a'_{r'} = a_1, a_2, \ldots, a_r, a_1, a_2, \ldots, a_r, a_1, a_2, \ldots, a_r.$$

Then

$$\langle\overline{w(G)}\rangle = \bigcup a'_{j_1} \cdots a'_{j_\mu} S,$$

where $1 \leq j_1 < j_2 \cdots < j_\mu \leq r'$; $1 \leq \mu \leq |G : G_t|$.

Since each $a'_i \in w(G)$, let $a'_i = w(a_{i,1}, \ldots a_{i,n})$, $1 \leq i \leq r'$ and $\alpha'_i = (a_{i,2}, \ldots, a_{i,n})$.

Then

$$\langle\overline{w(G)}\rangle = w(G, 1, \alpha'_1) \cdots w(G, 1, \alpha'_r)S$$

which implies that the word $w$ is strongly elliptic on $G$ and completes the proof of the lemma.

**Proof of Theorem 1.2**

Let $x_1, \ldots, x_m$ be generators of the group $\Gamma$. Then the Lie $\mathbb{Z}_p$- algebra $L = L(G)$ is generated by elements $x_i G_2$, $1 \leq i \leq m$. There exists $k \geq 1$

such that $x_i^{p^k} = 1$, $1 \leq i \leq m$. This implies $p^k x_i G_2 = 0$, $1 \leq i \leq m$ and therefore $p^k L = (0)$. Hence $L$ can be viewed as a $\mathbb{Z}/p^k\mathbb{Z}$- algebra.

The following result was proved in [MZ]. Let $\Gamma$ be a finitely generated residually-$p$ torsion group. Let $\Gamma = \Gamma_1 > \Gamma_2 > \cdots$ be its lower central series. Then an arbitrary homogenous element of the Lie ring $L(\Gamma) = \oplus_{i \geq 1} \Gamma_i / \Gamma_{i+1}$ is ad-nilpotent. This result implies that the Lie algebra $L = L(G)$ satisfies the assumptions of Lemma 3.1. Hence $|L : Span f(L)| < \infty$ and $f$ is strongly elliptic on $L$. Now, by Lemma 3.2 the word $w$ is strongly elliptic on the group $G$, which finishes the proof of Theorem 1.2.

# References


[Go] E. S. Golod, On nil algebras and finitely approximable- p- groups, *Izv. Akad. SSSR, Ser. Mat.* 28, (1964), 273–276.

[Gr] R. Grigorchuk, Degrees of growth of finitely generated groups and the theory of invariant means. *Izv. Akad. Nauk SSSR, Ser. Mat.* 48 n. 5, (1984), 939–985.

[GuS] N. Gupta and S. Sidki, On the Burnside problem for periodic groups. *Math. Z.* 182 n. 3, (1983), 385-388.

[H] G. Higman, Lie rings methods in the theory of finite nilpotent groups, Cambridge Univ. Press, New York. 1958 Proc. Internat. Congress Math. (1960), 307-312.

[JZ] A. Jaikin-Zapirain, On the verbal witdth of finiteley generated pro-p-groups. *Rev. Mat. Iberoam.* 24, (2008), 617-630.

[Kl] B. Klopsch, Normal subgroups of Substitutions Groups of Formal Power Series, *J. of Algebra* 228, (2000), 91-106.

[K] A. I. Kostrikin, On local nilpotency of Lie rings that satisfy Engel's condition, *Dokl. Akad. Nauk. SSSR* 118, 1958 1074-1077.

[MZ] C. Martínez and E. Zelmanov, On Lie rings of torsion groups, *Bull. Math. Sci* 6, (2016), 371-377.

[P] B. J. Plotkin, Algebraic sets of elements in groups and Lie algebras, *Uspehi Math. Nauk* 13, no. 6, (1958), 133-138.

[S] D. Seagal, Words: Notes on Verbal Width in Groups. London Math. Soc. Lecture Note Series 361, pp.121, 2009.

[Se] J. P. Serre, Cohomologie galoisienne. Springer Verlag 1964.

[Z1] E. Zelmanov, On the restricted Burnside problem. Proceedings of the International Congress of Mathematicians Kyoto 1990. Math. Soc. Japan, Tokyo 1991, 395-402.

[Z.2] E. Zelmanov, Nil rings and periodic groups. With a preface by Jongsik Kim. KMS Lecture Notes in Mathematics, Korean Math. Soc. Seoul 1992, x + 79 pp.

[Z.3] E. Zelmanov, Lie algebras and torsion groups with identity, Submitted. Arxiv 160405678.

[ZSSS] K. A. Zhevlakov, A. M. Slinko, I. P. Shestakov and A. I. Shirshov, Rings that are nearly associative. Academic Press, ING. 1982.