Submitted exclusively to the London Mathematical Society
DOI: 10.1112/S0000000000000000

THE NOTTINGHAM GROUP IS FINITELY PRESENTED.

M. V. ERSHOV

Abstract

We prove that the Nottingham group $\mathcal{N}(\mathbb{F}_p)$ is finitely presented as a pro-p group for $p > 2$.

1. *Introduction*

Let $\mathbb{F}_p$ be a finite field of prime order p. The Nottingham group $\mathcal{N}(\mathbb{F}_p)$ is the group of automorphisms of the ring $\mathbb{F}_p[[t]]$ which act trivially on $(t)/(t^2)$ or, equivalently, the group of formal power series $\{t(1+a_1t+a_2t^2+\ldots) \mid a_i \in \mathbb{F}_p\}$ under substitution. The goal of this paper is to show that $\mathcal{N}(\mathbb{F}_p)$ is finitely presented as a pro-p group for $p > 2$.

Given a pro-p group G, let $L(G)$ denote the graded Lie algebra of G with respect to the lower central series. Presentations of G are related to those of $L(G)$; in particular, if $L(G)$ is finitely presented, then so is G. A presentation of $L(\mathcal{N})$, the Lie algebra of the Nottingham group, was computed by Caranti in [**3**]. He showed that $L(\mathcal{N})$ is not finitely presented, but there is a central extension of $L(\mathcal{N})$ which is finitely presented. The latter, together with the results of computer calculations made by E. O'Brien, gave positive evidence of finite presentability of the Nottingham group for $p > 2$.

In [**6**] we constructed a two parametric family $\{\mathcal{Q}^1(s,r)\}$ of subgroups of $\mathcal{N}$, whose Lie algebras with respect to the Zassenhaus filtration (which in this case coincides with the lower central series) are isomorphic to $\mathfrak{sl}_2(\mathbb{F}_p) \otimes t\mathbb{F}_p[t]$ as restricted Lie algebras. We also conjectured that one might be able to prove finite presentability of $\mathcal{N}$ by first showing that its subgroups $\{\mathcal{Q}^1(s,r)\}$ are finitely presented. Although the Lie algebra $\mathfrak{sl}_2(\mathbb{F}_p)\otimes t\mathbb{F}_p[t]$ is not finitely presented, the situation here is slightly better than in the case of the Nottingham group, because there exists a group with the same Lie algebra which is known to be finitely presented, namely $SL_2^1(\mathbb{F}_p[[t]])$, the first congruence subgroup of $SL_2(\mathbb{F}_p[[t]])$. The problem is that the proof of finite presentability of $SL_2^1(\mathbb{F}_p[[t]])$ given in [**9**] relies on deep results about algebraic groups over global fields and clearly cannot be generalized to non-linear groups. In this paper we give a Lie-theoretic proof of finite presentability of $SL_2^1(\mathbb{F}_p[[t]])$ which easily extends to the groups $\{\mathcal{Q}^1(s,r)\}$ and also gives an explicit bound for the number of relators. Combining this result with Caranti's presentation for $L(\mathcal{N})$, we prove the following:

Theorem 1.1. *Let $p > 2$. The Nottingham group $\mathcal{N}(\mathbb{F}_p)$ has a presentation with 2 generators and at most $12p + 32$ relators.*

2000 *Mathematics Subject Classification* 20E18 (primary), 20F05, 20F40 (secondary).

Remarks. 1) By a theorem of Camina [**1**], the Nottingham group is "S-universal", that is, any finitely generated pro-p group can be embedded in $\mathcal{N}(\mathbb{F}_p)$ as a closed subgroup. Thus Theorem 1.1 implies the existence of a finitely presented S-universal pro-p group, answering a question posed in [**5**].

2) Conjecturally (see [**8**]), the minimal number of relators of $\mathcal{N}(\mathbb{F}_p)$ is equal to 5. It is possible to improve the bound given in the theorem using slight variations of our method, but we do not see how to obtain a bound which does not depend on p.

Organization. In section 2 we review basic facts about Lie algebras of pro-p groups. Lie-theoretic methods of proving finite presentability of pro-p groups are discussed in section 3. In section 4 we apply these methods to the groups $\{\mathcal{Q}^1(s,r)\}$. Finally, in section 5 we prove the main theorem.

2. *Preliminaries*

Let G be a pro-p group. Given $u_1,\dots,u_n \in G$, the (left normed) *n-fold commutator* $(u_1,\dots,u_n)$ is defined inductively to be $((u_1,\dots,u_{n-1}),u_n)$, where $(u,v) = u^{-1}v^{-1}uv$. The (closed) normal subgroup of G generated by all n-fold commutators is called the n^{th} term of the lower central series of G and denoted by $\gamma_n G$.

Let $\omega = \{\omega_1 G \supseteq \omega_2 G \supseteq \dots\}$ be a descending chain of closed normal subgroups of a pro-p group G. We will call ω a *filtration* of G if $(\omega_i G, \omega_j G) \subseteq \omega_{i+j} G$ for all $i,j > 0$. Note that our definition does not include standard requirements a) $\omega_1 G = G$, b) $\cap\, \omega_i G = \{1\}$ and c) $\omega_i G$ is open in G. The main example of a filtration is the lower central series (which satisfies a) and b), but not always c)).

The *graded Lie algebra* of G associated with a filtration ω will be denoted by $L^\omega(G)$. As a graded abelian group, $L^\omega(G) = \bigoplus_{n=1}^{\infty} \omega_n G/\omega_{n+1}G$, and the bracket is defined as follows: given $g \in \omega_i G \backslash \omega_{i+1} G$ and $h \in \omega_j G \backslash \omega_{j+1} G$, set $[g\,\omega_{i+1}G, h\,\omega_{j+1}G] = (g,h)\,\omega_{i+j+1}G$. In general $L^\omega(G)$ has the structure of a Lie algebra over $\mathbb{Z}_p$, the ring of p-adic integers, but in many interesting cases one has $pL^\omega(G) = 0$, so that $L^\omega(G)$ becomes a Lie algebra over $\mathbb{F}_p$. If the terms of a filtration satisfy the inclusion $(\omega_i G)^p \subseteq \omega_{pi} G$ for all i, then $L^\omega(G)$ has the structure of a restricted Lie algebra where $(g\omega_{i+1}G)^p = g^p \omega_{pi+1} G$. The basic example of such filtration is the Zassenhaus series $\{\Omega_n G\}$, where $\Omega_n G = \prod_{i\cdot p^j \geq n} (\gamma_i G)^{p^j}$.

Once again, let $\{\omega_n G\}$ be an arbitrary filtration of a pro-p group G. For each $n \geq 1$, the quotient $\omega_n G/\omega_{n+1}G$ has a structure of right G-module with respect to the "conjugation" action. More precisely, given $g \in \omega_n G$ and $h \in G$, we set $(g\omega_{n+1}G)^h := g^h \omega_{n+1} G$ where $g^h = h^{-1}gh$. Extending by linearity, we obtain a grading-preserving action of G on $L^\omega(G) = \bigoplus_{n=1}^{\infty} \omega_n G/\omega_{n+1}G$ which respects the Lie bracket. Note that if $\omega_1 G = G$, this action is necessarily trivial.

If $g \in \omega_n G \backslash \omega_{n+1} G$, the coset $g\,\omega_{n+1}G$ (which can be thought of as an element of $L^\omega(G)$) will be called the *leading term* of g and denoted by $\mathrm{LT}_\omega(g)$. The number n will be referred to as the *degree* of g and denoted by $\deg_\omega(g)$. If $g \in \bigcap_{i\geq 1} \omega_i G$, we set $\mathrm{LT}_\omega(g) = 0$ and $\deg_\omega(g) = \infty$. If $g \notin \omega_1 G$, both the degree and the leading term will be undefined. It is easy to see that $\mathrm{LT}_\omega((g_1,g_2,\dots,g_n)) = [\mathrm{LT}_\omega(g_1),\dots,\mathrm{LT}_\omega(g_n)]$ provided $\deg_\omega((g_1,g_2,\dots,g_n)) = \deg_\omega(g_1)+\dots+\deg_\omega(g_n)$.

The Lie algebra of a pro-p group G with respect to its lower central series will always be denoted by $L(G)$.

3. *Using Lie methods to prove finite presentability*

In this section we will outline the general scheme of studying finite presentability of pro-p groups using Lie theoretic methods. All pro-p groups are assumed to be finitely generated.

Presentations. Let G be a pro-p group. A *presentation* of G is a pair $(P) = (X, \pi)$ where X is a finite set and π is a surjective homomorphism from $F(X)$ to G (where $F(X)$ is the free pro-p group on X). Elements of $\operatorname{Ker}\pi$ are called *relators* of (P). A subset $\mathfrak{R}$ of $\operatorname{Ker}\pi$ will be called a *set of defining relators of* (P) if $\mathfrak{R}$ generates $\operatorname{Ker}\pi$ as a closed normal subgroup. For basic properties of presentations of pro-p groups the reader is referred to [**10**].

If G is a pro-p group, then $L(G)$ is a $\mathbb{Z}_p$-Lie algebra which is graded by positive integers and generated in degree one. Presentations of Lie algebras in this category are defined in a similar way − the role of a free pro-p group is played by a free Lie algebra over p-adic integers, relators are assumed to be homogeneous, and the homomorphisms grading preserving.

Proving finite presentability. Given a presentation of a graded Lie algebra L, the problem of existence of a finite set of defining relators is equivalent to the following question: does there exist an integer N such that for every $n > N$ all relators of degree n are consequences of relators of smaller degree. A similar approach to proving finite presentability of pro-p groups is described below.

DEFINITION. Let G and H be pro-p groups. We say that H is an *n-cover* of G, where n is a non-negative integer, if there is a surjective homomorphism $\varphi : H \to G$ satisfying any of the two equivalent conditions:

1) φ induces an isomorphism between $H/\gamma_{n+1}H$ and $G/\gamma_{n+1}G$,

2) $\operatorname{Ker}\varphi \subseteq \gamma_{n+1}H$.

The map φ will be called an n-covering map.

Remark. It is easy to show that if H is an n-cover of G, then any surjective homomorphism from H to G is n-covering.

Every pro-p group G has a finitely presented n-cover for any n (this follows from part d) of Proposition 3.2 below). Therefore, to prove that G is finitely presented it suffices to show that G has the following property (T_n) for all sufficiently large n.

DEFINITION. A pro-p group G has property (T_n), where n is a positive integer, if every $(n-1)$-cover of G is also an n-cover of G.

Now fix a pro-p group G and a positive integer n, and suppose we are trying to prove that G has (T_n).

Let K be an $(n-1)$-cover of G and let $\varphi : K \to G$ be an $(n-1)$-covering map. Choose presentations $(P_K) = (X, \pi_K)$ of $L(K)$ and $(P_G) = (X, \pi_G)$ of $L(G)$ such that $\pi_G = \varphi_*\pi_K$, where $\varphi_* : L(K) \to L(G)$ is defined by $\varphi_*(k\,\gamma_{i+1}K) = \varphi(k)\gamma_{i+1}G$ for $k \in \gamma_i K$. Let $\mathfrak{R}_G$ be a set of defining relators of (P_G).

Clearly, the map φ is n-covering if and only if φ_* maps $L_n(K)$ isomorphically onto $L_n(G)$, where $L_i(\ )$ is the i^{th} homogeneous component of $L(\ )$. Equivalently, we must show that each relator of (P_G) of degree n is also a relator of (P_K). Since φ is $(n-1)$-covering, (P_G) and (P_K) have the same relators in degrees less than n, and therefore every relator of (P_G) which is a consequence of relators of (P_G) of degrees less than n is automatically a relator of (P_K). In particular, if $\mathfrak{R}_G$ does not contain any relators of degree n, there is nothing to prove. As an immediate consequence we obtain a well-known relation between finite presentability of a pro-p group and its Lie algebra:

PROPOSITION 3.1. *Let G be a pro-p group. If $L(G)$ is finitely presented, then G is finitely presented.*

Unfortunately, in the examples which are of interest to us Lie algebras fail to be finitely presented, so Proposition 3.1 cannot be applied.

Going back to the general case, it remains to show that every element of $\mathfrak{R}_G$ of degree n is a relator of (P_K). Consideration of the Lie algebras $L(G)$ and $L(K)$ alone is insufficient for this purpose and we have to make better use of the fact that K is an $(n-1)$-cover of G. The idea is to choose a filtration ω of K which "descends" faster than the lower central series and study the associated Lie algebra $L^\omega(K)$ using the action of K on it. Below we give a specific example of such filtration and explain how obtained information about $L^\omega(K)$ may be used to solve our problem.

Fix a positive integer t such that $1 < t < n$, and let c be the largest integer such that $tc \le n$. Given a pro-p group H, let $\{\omega_i H\}$ be the following filtration of H: we set $\omega_i H = \gamma_{it} H$ for $i \le c$ and $\omega_i H = \gamma_{n+1} H$ for $i > c$. This is indeed a filtration since $t(c+1) \ge n+1$. Let $L^\omega(H) = \bigoplus_{i=1}^{\infty} L_i^\omega(H)$ be the associated graded Lie algebra, i.e. $L_i^\omega(H) = \omega_i H / \omega_{i+1} H$. Clearly $L_i^\omega(H) = 0$ for $i > c$.

The group K acts on $L^\omega(K)$ (by conjugation) and also on $L^\omega(G)$ (by composition of the action of G on $L^\omega(G)$ with the covering map). Since K is an $(n-1)$-cover of G, the K-modules $L_i^\omega(G)$ and $L_i^\omega(K)$ are isomorphic for $i < c$.

Now suppose that we found $g_1, g_2 \in G$ such that $(g_1, g_2) \in \gamma_n G$ and $\deg_\omega(g_1) + \deg_\omega(g_2) = c$. Choose $k_1, k_2 \in K$ such that $\varphi(k_i) = g_i$ for $i = 1, 2$. Since K is an $(n-1)$-cover of G, we know that $(k_1, k_2) \in \gamma_n K$. Now if k is an arbitrary element of K, we have

$$(k_1^k, k_2^k) = (k_1, k_2)^k \equiv (k_1, k_2) \mod \gamma_{n+1} K \ (= \omega_{c+1} K).$$

Let $u_1 = \mathrm{LT}_\omega(k_1)$ and $u_2 = \mathrm{LT}_\omega(k_2)$. Note that $[u_1, u_2] = (k_1, k_2)\omega_{c+1} K$. Now by definition of the K-action on $L^\omega(K)$ we have $u_1^k = \mathrm{LT}_\omega(k_1^k)$ and $u_2^k = \mathrm{LT}_\omega(k_2^k)$, whence $(k_1^k, k_2^k)\omega_{c+1} K = [u_1^k, u_2^k]$. Thus the above congruence is equivalent to the following relation in $L_c^\omega(K)$:

$$[u_1^k, u_2^k] = [u_1, u_2]. \tag{3.1}$$

By an earlier remark we know how K acts on $L_i^\omega(K)$ for $i < c$, whence both u_1^k and u_2^k can be "evaluated".

If we happen to know that $L^\omega(G)$ is a restricted Lie algebra and there exists $g \in G$ such that $p \cdot \deg_\omega g = c$ but $g^p \equiv 1 \mod \gamma_n G$ (e.g. if $g^p = 1$), we can play the same game with the identity $(g^h)^p = (g^p)^h$, where h is any element of G.

Finally note that $L_n(K) = \gamma_n K/\gamma_{n+1}K$ lies inside $L_c^\omega(K)$. Therefore, by taking appropriate linear combinations of relations of the form (3.1), it is possible to obtain new relations in $L_n(K)$ and hence new relators of the presentation (P_K) of $L(K)$.

The method we just described will be applied in the next section to prove finite presentability of $SL_2^1(\mathbb{F}_p[[t]])$ and the groups $\{\mathcal{Q}^1(s,r)\}$. As a preparation for the proof we are going to state basic properties of covering maps (some of which we already discussed) in a slightly different language which is more technical but is better suited for a formal justification.

DEFINITION. A *pointed* pro-p group is a pair (G,S) where G is a pro-p group and $S = (g_1, g_2, \dots, g_n)$ is a fixed generating n-tuple of G.

Now let (X,π) be a presentation of G, where $X = \{x_1, x_2, \dots, x_n\}$, and let $\mathfrak{R}$ be a set of defining relators. If $\pi(x_i) = g_i$ for $i = 1, 2, \dots, n$, we will say that $\langle X \mid \mathfrak{R}\rangle$ is a presentation of the pointed pro-p group $\Omega = (G, (g_1, g_2, \dots, g_n))$. Any element of $\operatorname{Ker}\pi$ will be called a *relator* of Ω. More generally, given $w \in F(X)$ and $g \in G$, we write $w \underset{\Omega}{=} g$ if $\pi(w) = g$.

Pointed Lie algebras and their presentations are defined in a similar way. Note that with each pointed pro-p group $\Omega = (G, (g_1, g_2, \dots, g_n))$ one can associate the pointed Lie algebra $(L(G), (\operatorname{LT} g_1, \operatorname{LT} g_2, \dots, \operatorname{LT} g_n))$ which will be denoted by $L(\Omega)$.

DEFINITION. Let $\Omega = (G, (g_1, g_2, \dots, g_m))$ and $\Delta = (H, (h_1, h_2, \dots, h_m))$ be pointed pro-p groups. We say that Δ is an *n-cover* of Ω if there exists an n-covering map $\varphi : H \to G$ such that $\varphi(h_i) = g_i$ for $i = 1, 2, \dots, m$ (obviously, such φ is uniquely determined).

PROPOSITION 3.2. *Fix a positive integer n. Let $\Omega = (G, (g_1, g_2, \dots, g_m))$ and $\Delta = (K, (k_1, k_2, \dots, k_m))$ be pointed pro-p groups. Suppose that Δ is an $(n-1)$-cover of Ω and let $\varphi : \Delta \to \Omega$ be the covering map.*

a) *Δ is an l-cover of Ω, where l is some integer, if and only if every relator of $L(\Omega)$ of degree $i \le l$ is also a relator of $L(\Delta)$.*
b) *Let $LF(m)$ be a free $\mathbb{Z}_p$- Lie algebra on m generators. If $w \in LF(m)$ is homogeneous of degree less than n and $k \in K$ is such that $w \underset{L(\Omega)}{=} \operatorname{LT}\varphi(k)$, then $w \underset{L(\Delta)}{=} \operatorname{LT}(k)$.*

Now choose a presentation of $L(\Omega)$ and let $\{w_1, \dots, w_t\}$ be the set of defining relators of degree n.

c) *If each w_i is a relator of $L(\Delta)$, then Δ is an n-cover of Ω.*
d) *If Δ has a presentation with r (defining) relators, then there exists an n-cover $\tilde{\Delta}$ of Ω which has a presentation with $r + t$ relators.*

Proof. Parts a) and b) are straightforward.
Part c) Let $w \in LF(m)$ be a relator of $L(\Omega)$ of degree n. Then w can be written in the form

$$w = \sum \lambda_i w_i + \sum \mu_j [v_j, u_j],$$

where $\lambda_i, \mu_j \in \mathbb{Z}_p$ and each v_j is a relator of $L(\Omega)$ of degree less than n. Now $w_i \underset{L(\Delta)}{=} 0$ for all i by assumption and $v_j \underset{L(\Delta)}{=} 0$ by part a) since Δ is an $(n-1)$-cover of Ω. Therefore, $w \underset{L(\Delta)}{=} 0$.

Part d) Define a homomorphism $\pi : F = F(x_1, x_2, \dots, x_m) \to K$ by setting $\pi(x_1) = k_1, \dots, \pi(x_m) = k_m$. For each $i = 1, \dots, t$ choose $W_i \in F$ such that $\mathrm{LT}(W_i) = w_i$. Since $w_i \underset{L(\overline{\overline{\Omega}})}{=} 0$, there exists $Z_i \in \gamma_{n+1}F$ such that $W_i Z_i^{-1} \underset{\overline{\overline{\Omega}}}{=} 1$. Let $\bar{K}$ be the quotient of K by the closed normal subgroup generated by $\pi(W_1 Z_1^{-1}), \dots, \pi(W_t Z_t^{-1})$ and let $\bar{\Delta} = (\bar{K}, (\bar{k}_1, \dots, \bar{k}_m))$ be the corresponding pointed pro-p group. Clearly, $\bar{\Delta}$ is an $(n-1)$-cover of Ω which can be presented by $r+t$ relators. Moreover, each w_i is a relator of $L(\bar{\Delta})$ by construction. Therefore, by part c) $\bar{\Delta}$ is an n-cover of Ω. □

4. *Finite presentability of the groups* $\{\mathcal{Q}(s,r)\}$

Let r and s be positive integers such that $r < p^s/2$. Let $\mathcal{Q}(s,r)$ be the subgroup of the Nottingham group $\mathcal{N}(\mathbb{F}_p)$ consisting of all elements of the form

$$\sqrt[r]{\frac{at^r + b}{ct^r + d}} \text{ where } a, b, c, d \in \mathbb{F}_p[[t^{p^s}]] \text{ s.t. } a - 1 \equiv d - 1 \equiv b \equiv 0 \mod t\mathbb{F}_p[[t]] \ ,$$

and let $\mathcal{Q}^1(s,r)$ be the subgroup of $\mathcal{Q}(s,r)$ which consists of the elements of the above form with an extra restriction $c \in t\mathbb{F}_p[[t]]$. It is easy to see that the index of $\mathcal{Q}^1(s,r)$ in $\mathcal{Q}(s,r)$ is equal to p.

These groups were introduced and studied in [**6**] where we constructed a bijection from $SL_2^1(\mathbb{F}_p[[t]])$ to $\mathcal{Q}^1(s,r)$ which is *not* a group homomorphism but induces an isomorphism of the Lie algebras with respect to the lower central series (in [**6**], we called such a map an *approximation*). Moreover, for both groups the lower central series coincides with the Zassenhaus filtration, and the associated Lie algebras are isomorphic as restricted Lie algebras. The map $\varepsilon_{s,r} : SL_2^1(\mathbb{F}_p[[t]]) \to \mathcal{Q}^1(s,r)$ defined below is an example of such approximation.

$$\varepsilon_{s,r} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \sqrt[r]{\frac{a^q t^r + b^q}{c^q t^r + d^q}}, \text{ where } q = p^s.$$

The same map establishes a bijection between a Sylow pro-p subgroup of $SL_2(\mathbb{F}_p[[t]])$ and the group $\mathcal{Q}(s,r)$.

The goal of this section is to show that the groups $\{\mathcal{Q}^1(1,r)\}$ are finitely presented. The restriction $s = 1$ is a matter of convenience, and the result is undoubtedly true for all s. We do not know if our argument works for any pro-p group G such that $L(G)$ is isomorphic to $\mathfrak{sl}_2(\mathbb{F}_p) \otimes t\mathbb{F}_p[t]$ as a restricted Lie algebra, but it definitely does for $SL_2^1(\mathbb{F}_p[[t]])$. In fact, we will treat this case explicitly as it requires very few modifications to the proof. For the rest of this section the number $r < p/2$ will be fixed, and $\mathcal{Q}$ will denote the group whose finite presentability we are trying to prove. Thus either $\mathcal{Q} = \mathcal{Q}^1(1,r)$ or $\mathcal{Q} = SL_2^1(\mathbb{F}_p[[t]])$; in the latter case the value of r is irrelevant.

We start by giving a presentation for the Lie algebra $L(\mathcal{Q})$. Define $\bar{E}_n, \bar{F}_n, \bar{H}_n \in \mathcal{Q}$ as follows. If $\mathcal{Q} = SL_2^1(\mathbb{F}_p[[t]])$, we set

$$\bar{E}_n = \begin{pmatrix} 1 & t^n \\ 0 & 1 \end{pmatrix}, \quad \bar{F}_n = \begin{pmatrix} 1 & 0 \\ t^n & 1 \end{pmatrix}, \quad \bar{H}_n = \begin{pmatrix} \frac{1}{\sqrt{1-2t^n}} & 0 \\ 0 & \sqrt{1-2t^n} \end{pmatrix}.$$

If $\mathcal{Q} = \mathcal{Q}^1(1,r)$, we replace the above elements by their images under the map $\varepsilon_{1,r}$.

Thus

$$\bar{E}_n = \sqrt[r]{t^r + t^{pn}}, \quad \bar{F}_n = \frac{t}{\sqrt[r]{1 + t^{pn+r}}}, \quad \bar{H}_n = \frac{t}{\sqrt[r]{1 - 2t^{pn}}}.$$

Note that $\mathcal{Q}$ is generated by $\bar{E}_1, \bar{F}_1$ and $\bar{H}_1$. Finally, we set $\bar{e}_n = \mathrm{LT}(\bar{E}_n), \bar{f}_n = \mathrm{LT}(\bar{F}_n), \bar{h}_n = \mathrm{LT}(\bar{H}_n)$ for $n \geq 1$.

Let $LF = LF(x_1, y_1, z_1)$ be the free $\mathbb{Z}_p$-Lie algebra on 3 generators x_1, y_1 and z_1. Define $x_n, y_n, z_n \in LF$ inductively by setting $x_n = \frac{1}{2}[z_{n-1}, x_1]$, $z_n = [x_{n-1}, y_1]$, $y_n = -\frac{1}{2}[z_{n-1}, y_1]$.

PROPOSITION 4.1. *The following hold:*
1. The Lie algebras $L(\mathcal{Q})$ and $\mathfrak{sl}_2(\mathbb{F}_p) \otimes t\mathbb{F}_p[t]$ are isomorphic via the $\mathbb{F}_p$-linear map defined by $\bar{e}_n \mapsto et^n$, $\bar{f}_n \mapsto ft^n$, $\bar{h}_n \mapsto ht^n$ (here (e, f, h) is the standard $\mathfrak{sl}_2$ triple)

2. Let $\Omega = (\mathcal{Q}, (\bar{E}_1, \bar{F}_1, \bar{H}_1))$. The pointed Lie algebra $L(\Omega) = (L(\mathcal{Q}), (\bar{e}_1, \bar{f}_1, \bar{h}_1))$ admits the following presentation

$$\langle x_1, y_1, z_1 \mid px_1, py_1, pz_1, [x_1, x_2], [y_1, y_2], [z_1, z_2], \\ [x_1, z_2] - [x_2, z_1], [y_1, z_2] - [y_2, z_1], \{[z_{pn-1}, z_1]\}_{n=1}^{\infty} \rangle. \quad (4.1)$$

Moreover, we have $x_n \underset{L(\Omega)}{\equiv} \bar{e}_n$, $y_n \underset{L(\Omega)}{\equiv} \bar{f}_n$, $z_n \underset{L(\Omega)}{\equiv} \bar{h}_n$ for all $n \geq 1$.

Proof. Part 1. The statement is obvious in the case $\mathcal{Q} = SL_2^1(\mathbb{F}_p[[t]])$. In the case $\mathcal{Q} = \mathcal{Q}^1(1, r)$ the proof is analogous to that of [**6**, Theorem 1.1].

Part 2. The assertion can be verified by adapting the argument of [**4**, Theorem 2b)]. □

The main technical result of this section is the following

PROPOSITION 4.2. *If $N > 5p^2 + 5p$, then $\mathcal{Q}$ has property (T_N).*

COROLLARY 4.3. *Each of the groups $\mathcal{Q}^1(1, r)$ and $SL_2^1(\mathbb{F}_p[[t]])$ has a presentation with 3 generators and at most $5p + 13$ relators.*

Proof. The presentation of $L(\Omega)$ given above has three defining relators of degree 1, five defining relators of degree 3 and one defining relator of degree pn for each $n \geq 1$, whence the number of defining relators of $L(\Omega)$ of degree at most $5p^2 + 5p$ is equal to $5p+13$. It follows from Proposition 3.2d) that there exists a $(5p^2+5p)$-cover $\mathcal{G}$ of $\mathcal{Q}$ which has a presentation with 3 generators and $5p + 13$ relators. Applying Proposition 4.2, we see that $\mathcal{G}$ is an n-cover of $\mathcal{Q}$ for any n, whence $\mathcal{G}$ is isomorphic to $\mathcal{Q}$. □

Proof of Proposition 4.2. We only have to consider values of N which are degrees of defining relators of presentation (4.1) of $L(\Omega)$. Therefore we can (and will) assume that $N = pM$, where $M > 5p+5$. Let $\mathcal{G}$ be an $(N-1)$-cover of $\mathcal{Q}$ and let $\varphi : \mathcal{G} \to \mathcal{Q}$ be an $(N-1)$-covering map. For every $n > 0$ choose $E_n, F_n, H_n \in \mathcal{G}$ such that $\varphi(E_n) = \bar{E}_n$, $\varphi(F_n) = \bar{F}_n$ and $\varphi(H_n) = \bar{H}_n$.

CLAIM 4.4. $[\mathrm{LT}\,(H_{N-1}), \mathrm{LT}\,(H_1)] = 0.$

The proof of this claim will occupy the majority of the section. But first we will explain how the assertion of Proposition 4.2 follows from it. Let us apply Proposition 3.2c) to the pointed pro-p groups $\Omega = (\mathcal{Q}, (\bar{E}_1, \bar{F}_1, \bar{H}_1))$ and $\Delta = (\mathcal{G}, (E_1, F_1, H_1))$. Presentation (4.1) of $L(\Omega)$ has exactly one defining relator of degree N, namely $[z_{N-1}, z_1]$, and therefore it is enough to show that $[z_{N-1}, z_1]$ is a relator of $L(\Delta)$. Since Δ is an $(N-1)$-cover of Ω, it follows from Proposition 3.2b) and part 2 of Proposition 4.1 that $x_i \underset{L(\Delta)}{=} \mathrm{LT}\,(E_i)$, $y_i \underset{L(\Delta)}{=} \mathrm{LT}\,(F_i)$, $z_i \underset{L(\Delta)}{=} \mathrm{LT}\,(H_i)$ for $i < N$. Therefore, $[z_{N-1}, z_1] \underset{L(\Delta)}{=} [\mathrm{LT}\,(H_{N-1}), \mathrm{LT}\,(H_1)] = 0$. □

For the rest of the section we write $\mathcal{G}_n = \gamma_n\mathcal{G}$ and $\mathcal{Q}_n = \gamma_n\mathcal{Q}$ for all n.

Proof of Claim 4.4.

LEMMA 4.5. *Let m and n be positive integers. The following relations hold in the group $\mathcal{G}$.*

	case $\mathcal{Q} = \mathcal{Q}^1(1, r)$	case $\mathcal{Q} = SL_2^1(\mathbb{F}_p[[t]])$
1) $(E_n, E_m) \equiv 1$	mod $\mathcal{G}_{n+pm-r}\,\mathcal{G}_{m+pn-r}\,\mathcal{G}_N$	mod $\mathcal{G}_N$
2) $(F_n, F_m) \equiv 1$	mod $\mathcal{G}_{n+pm+r}\,\mathcal{G}_{m+pn+r}\,\mathcal{G}_N$	mod $\mathcal{G}_N$
3) $(H_n, H_m) \equiv 1$	mod $\mathcal{G}_{n+pm}\,\mathcal{G}_{m+pn}\,\mathcal{G}_N$	mod $\mathcal{G}_N$
4) $F_n^{H_m} \equiv F_n F_{n+m}^2$	mod $\mathcal{G}_{2m+n}\,\mathcal{G}_{pn+m+r}\,\mathcal{G}_N$	mod $\mathcal{G}_{2m+n}\,\mathcal{G}_N$
5) $E_n^{H_m} \equiv E_n E_{n+m}^{-2}$	mod $\mathcal{G}_{pm+n}\,\mathcal{G}_{pn+m-r}\,\mathcal{G}_N$	mod $\mathcal{G}_N$
6) $E_n^{F_m} \equiv E_n H_{n+m} \cdot F_{n+2m}^{-1}$	mod $\mathcal{G}_{2n+m}\,\mathcal{G}_{n+pm+r}\,\mathcal{G}_N$	mod $\mathcal{G}_{2n+m}\,\mathcal{G}_N$
7) $E_n^p \equiv 1$	mod $\mathcal{G}_{(p+1)n-r}\,\mathcal{G}_N$	mod $\mathcal{G}_N$
8) $F_n^p \equiv 1$	mod $\mathcal{G}_{(p+1)n+r}\,\mathcal{G}_N$	mod $\mathcal{G}_N$.

Proof. Notice that $\mathcal{G}_N$ appears in each of the above congruences. Since $\mathcal{G}/\mathcal{G}_N \cong \mathcal{Q}/\mathcal{Q}_N$, we can replace all occurrences of E_i, F_i, H_i and $\mathcal{G}_i$ by $\bar{E}_i$, $\bar{F}_i$, $\bar{H}_i$ and $\mathcal{Q}_i$, respectively, and prove the resulting congruence in $\mathcal{Q}$. If $\mathcal{Q} = SL_2^1(\mathbb{F}_p[[t]])$, all congruences can be verified by direct computation. If $\mathcal{Q} = \mathcal{Q}^1(1, r)$, computation is also not very difficult, but it can be avoided as explained in appendix. □

Now we start studying the action of $\mathcal{G}$ on its Lie algebra $L^\omega(\mathcal{G})$ associated with the filtration $\{\omega_i G\}$ where

$$\omega_i\mathcal{G} = \mathcal{G}_{i(M-5)} \text{ for } i \le p \quad \text{and} \quad \omega_i\mathcal{G} = \mathcal{G}_{N+1} \text{ for } i > p.$$

This is indeed a filtration since $(p+1)(M-5) = pM+M-5(p+1) \ge pM+1 = N+1$.

We claim that $L^\omega(\mathcal{G})$ is a restricted Lie algebra, i.e. $(\omega_i\mathcal{G})^p \subseteq \omega_{ip}\mathcal{G}$ for all i. We know that this is true for $i = 1$ since $(\mathcal{Q}_{M-5})^p \subseteq \mathcal{Q}_{p(M-5)}$ and $\mathcal{G}$ is a $(pM-1)$-cover of $\mathcal{Q}$. For $i > 1$, the inclusion is a consequence of a more general result.

LEMMA 4.6. *If $g \in \mathcal{G}_{M+1}$, then $g^p \in \mathcal{G}_{N+1}$.*

Proof. The following group-theoretic identities are well-known (see [**8**]):

(R1) $(xy)^p \equiv x^p y^p \mod K(x,y)$

(R2) $(x^p, y) \equiv (x,y)^p \mod K(x,(x,y))$

where $K(a,b)$ is the normal closure of $\gamma_p\langle a,b\rangle \cdot (\gamma_2\langle a,b\rangle)^p$ in $\langle x,y\rangle$.

We will show that $\mathcal{G}_i^p \subseteq \mathcal{G}_{pM+1}$ for $i \geq M+1$ by downwards induction on i. Fix i, and suppose we already proved the assertion for all $i' > i$. Let $g \in \mathcal{G}_i$.

Case 1. g is a pure commutator, i.e. $g = (h,k)$ where $h \in \mathcal{G}_{i-1}$ and $k \in \mathcal{G}$. We use law (R2) with $x = h$ and $y = k$. The right-hand side is equal to g^p, while the left-hand side is equal to the commutator (h^p, k) which lies in $\mathcal{G}_{pM+1}$ because $h^p \in \mathcal{G}_M^p \subseteq \mathcal{G}_{pM}$. The group $K(h,(h,k)) = K(h,g)$ is generated as a normal subgroup of $\mathcal{G}$ by $(h,g)^p$ and p-fold commutators in $\{h,g\}$ (i.e. commutators $(u_1,\ldots,u_p)$ where each u_i is equal to h or g). All such commutators belong to $\mathcal{G}_{N+1}$ by degree counting, and $(h,g)^p \in \mathcal{G}_{N+1}$ by induction, whence $g^p \in \mathcal{G}_{N+1}$.

General case. There exist finitely many elements $g_1,\ldots,g_n \in \mathcal{G}_i$ such that g_k is a pure commutator for each k, and $g \equiv g_1 g_2 \ldots g_n \mod \langle \mathcal{G}_{N+1}, g_1^p, \ldots, g_n^p\rangle$. Applying law (R1), we have $g^p \equiv g_1^p g_2^p \ldots g_n^p \cdot W_1 W_2 \mod \langle \mathcal{G}_{N+1}, g_1^p, \ldots, g_n^p\rangle$ where $W_1 \in \gamma_p \mathcal{G}_i \subseteq \mathcal{G}_{pi}$ and $W_2 \in (\gamma_2 \mathcal{G}_i)^p \subseteq \mathcal{G}_{2i}^p$. Now $g_k^p \in \mathcal{G}_{N+1}$ by case 1, W_1 lies in $\mathcal{G}_{N+1}$ since $pi \geq pM + p > N$, and $W_2 \in \mathcal{G}_{N+1}$ by induction. □

In what follows, we denote the leading terms of E_i, F_i and H_i (with respect to the filtration ω) by e_i, f_i and h_i. If $g \in \mathcal{G}$, the degrees of g with respect to ω and the lower central series will be denoted by $\deg_\omega(g)$ and $\deg(g)$, respectively. We can also consider two different notions of degree for homogeneous elements of $L^\omega(\mathcal{G})$: if $u = g\ \omega_{i+1}\mathcal{G}$ (where $g \in \omega_i\mathcal{G}\backslash\omega_{i+1}\mathcal{G}$), we set $\deg_\omega(u) := \deg_\omega(g) = i$ and $\deg(u) := \deg(g)$. Clearly, $\deg(u)$ is well defined, and $\deg([u,v]) \geq \deg(u) + \deg(v)$ (for convenience we set $\deg(0) = \infty$).

Now fix a positive integer $k \leq 5$ such that $(p+1)(M-k) - r > N = pM$. By part 1) of Lemma 4.5, $E_{M-k}^p \in \mathcal{G}_N$ and therefore

$$E_{M-k}^p \equiv (E_{M-k}^p)^{F_k} = (E_{M-k}^{F_k})^p \mod \mathcal{G}_{N+1}\,(= \omega_{p+1}\mathcal{G}). \tag{4.2}$$

Notice that both sides of (4.2) lie in $\omega_p\mathcal{G}$. Taking their images in $L_p^\omega(\mathcal{G}) = \omega_p\mathcal{G}/\omega_{p+1}\mathcal{G}$, we obtain

$$e_{M-k}^p = (e_{M-k}^{F_k})^p. \tag{4.3}$$

Indeed, $e_{M-k}^p = (\mathrm{LT}_\omega E_{M-k})^p = E_{M-k}^p \omega_{p+1}\mathcal{G}$, while $(e_{M-k}^{F_k})^p = (E_{M-k}^{F_k})^p \omega_{p+1}\mathcal{G}$.

By part 6) of Lemma 4.5 we know how F_k acts on e_{M-k}:

$$e_{M-k}^{F_k} = e_{M-k} + h_M - f_{M+k} + z \quad \text{where} \quad \deg(z) \geq M + (p-1)k + r.$$

By the restricted Lie algebra axioms, we have

$$(e_{M-k}^{F_k})^p = (e_{M-k} + h_M - f_{M+k} + z)^p = e_{M-k}^p + h_M^p - f_{M+k}^p + z^p + w, \tag{4.4}$$

where w is a sum of p-fold (Lie) commutators in $\{e_{M-k}, h_M, f_{M+k}, z\}$.

By Lemma 4.6, $F_{M+k}^p \in \mathcal{G}_{N+1}$, whence $f_{M+k}^p = 0$, and similarly $z^p = 0$. All commutators which involve z also vanish. Indeed, if u is a p-fold commutator involving z, then $\deg(u) \geq \deg(z) + (p-1)\deg(e_{M-k}) \geq M + (p-1)k + r + (p-1)(M-k) > pM = N$, whence $u = 0$ (since $\mathcal{G}_{N+1} = \omega_{p+1}\mathcal{G}$). The remaining commutators can be "reduced" according to rules 1)-6) below (which follow easily from Lemma 4.5).

Let i and j be positive integers such that $i+j<p$. We have

$$\begin{aligned} &1)[e_{iM-k},e_{jM-k}]=0 && 4)[e_{iM-k},h_{jM}]=-2e_{(i+j)M-k}\\ &2)[f_{iM+k},f_{jM+k}]=0 && 5)[f_{iM+k},h_{jM}]=2f_{(i+j)M+k}\\ &3)[h_{iM},h_{jM}]=0 && 6)[e_{iM-k},f_{jM+k}]=h_{(i+j)M}. \end{aligned} \tag{4.5}$$

Let $[u_1,u_2,\dots,u_{p-1},v]$ be a (p-fold) commutator in $\{e_{M-k},h_M,f_{M+k}\}$, and let $y=[u_1,u_2,\dots,u_{p-1}]$. Suppose that e_{M-k} appeared a times in the sequence $u_1,u_2,\dots,u_{p-1}$, and f_{M+k} appeared b times. Multiple application of rules 1)-6) yields the following:

$$\begin{aligned} &y=0 \text{ if } |a-b|>1, && y\in\mathbb{F}_p\, f_{(p-1)M+k} \text{ if } b-a=1,\\ &y\in\mathbb{F}_p\, h_{(p-1)M} \text{ if } b-a=0, && y\in\mathbb{F}_p\, e_{(p-1)M-k} \text{ if } b-a=-1. \end{aligned}$$

Therefore, up to scalar multiples, we have only three possibilities for y. Combining this observation with (4.3) and (4.4), we conclude the following:

$$h_M^p=\sum_{i=1}^{9}\alpha_i w_i \tag{4.6}$$

where $\alpha_1,\dots,\alpha_9$ are integers (modulo p) and $w_1,\dots,w_9$ are defined below:

$$\begin{aligned} &w_1=[e_{(p-1)M-k},e_{M-k}], && w_2=[h_{(p-1)M},e_{M-k}], && w_3=[f_{(p-1)M+k},e_{M-k}],\\ &w_4=[e_{(p-1)M-k},h_M], && w_5=[h_{(p-1)M},h_M], && w_6=[f_{(p-1)M+k},h_M],\\ &w_7=[e_{(p-1)M-k},f_{M+k}], && w_8=[h_{(p-1)M},f_{M+k}], && w_9=[f_{(p-1)M+k},f_{M+k}]. \end{aligned}$$

Moreover, it is easy to see that each α_i is independent of k.

From now on we will assume that $k=1$ or $k=2$. This will allow us to simplify the right hand side of (4.6).

LEMMA 4.7. *The following equalities hold:*

$$\begin{aligned} &1)w_6=w_8=w_9=0 && 2)w_4=-w_2+w_7+w_3-w_5\\ &3)w_1=0 && 4)w_7=-w_3+\frac{1}{2}[h_{(p-2)M},h_{2M}]. \end{aligned}$$

Proof. *Part 1)* is obvious (degree counting).

Part 2). The elements E_{M-k} and $E_{(p-1)M-k}$ commute modulo $\mathcal{G}_N$ by Lemma 4.5. Therefore, applying formula (3.1) from the previous section we get

$$[e_{M-k}^{F_k},e_{(p-1)M-k}^{F_k}]=[e_{M-k},e_{(p-1)M-k}].$$

As before we have

$$\begin{gathered} e_{M-k}^{F_k}=e_{M-k}+h_M-f_{M+k}+x\\ e_{(p-1)M-k}^{F_k}=e_{(p-1)M-k}+h_{(p-1)M}-f_{(p-1)M+k}+y\\ \text{where } \deg(x)\geq M+(p-1)k+r \text{ and } \deg(y)\geq(p-1)M+(p-1)k+r. \end{gathered}$$

Combining these formulas, we get

$$[e_{M-k}+h_M-f_{M+k}+x, e_{(p-1)M-k}+h_{(p-1)M}-f_{(p-1)M+k}+y] = [e_{M-k}, e_{(p-1)M-k}].$$

Expanding the left-hand side and taking into account that all commutators involving either x or y are equal to zero by degree counting, we obtain an equality which is equivalent to the assertion of Part 2) modulo the results of Part 1).

Part 3) Let $\mathfrak{A}$ be the set of triples (m,n,l) such that $m+pn-r > N$, $n+pm-r > N$, $m+n+pl > N$ and $M-5 \le m,n$. We are going to prove the following two statements by joint induction:

a)$[e_{m+l}, e_n] = -[e_m, e_{n+l}]$ if $(m,n,l) \in \mathfrak{A}$;

b)$[e_m, e_n] = 0$ if there exists l such that
$(m, n-l, l) \in \mathfrak{A}$, $(m-l, n, l) \in \mathfrak{A}$ and $(m-l, n-l, 2l) \in \mathfrak{A}$.

Let $S = m+n$. Both statements are obvious if $S > N$, and we proceed by downwards induction on S.

We start with part a). Let $(m,n,l) \in \mathfrak{A}$. The first two inequalities in the definition of $\mathfrak{A}$ ensure that E_m and E_n commute modulo $\mathcal{G}_N$, and the last inequality implies that E_m and E_n lie in $\omega_1\mathcal{G}$ (so their leading terms are defined). As before we have

$$[e_m^{H_l}, e_n^{H_l}] = [e_m, e_n].$$

Part 5) of Lemma 4.5 yields

$$\begin{aligned} e_m^{H_l} &= e_m - 2e_{m+l} + x && \text{where } \deg(x) \ge m+pl \\ e_n^{H_l} &= e_n - 2e_{n+l} + y && \text{and } \deg(y) \ge n+pl. \end{aligned}$$

Since $m+n+pl > N$, all commutators involving x or y vanish and we get

$$[e_m, e_n] - 2[e_{m+l}, e_n] - 2[e_m, e_{n+l}] + 4[e_{m+l}, e_{n+l}] = [e_m, e_n].$$

Now $[e_{m+l}, e_{n+l}] = 0$ by induction, and the result follows.

To prove part b) apply part a) to the triples $(m-l, n, l)$, $(m-l, n-l, 2l)$ and $(m, n-l, l)$. We have

$$[e_m, e_n] = -[e_{m-l}, e_{n+l}] = [e_{m+l}, e_{n-l}] = -[e_m, e_n],$$

whence $[e_m, e_n] = 0$.

It is easy to check that the triple $(m,n,l) = (M-k, (p-1)M-k, 3)$ satisfies the conditions of part b) for $k = 1, 2$, whence $[e_{M-k}, e_{(p-1)M-k}] = 0$.

Part 4). This is easy – just apply the Jacobi identity to the triple e_{M-k}, f_{M+k}, $h_{(p-2)M}$ and use formulas (4.5). □

Equation (4.6) can now be rewritten in the form

$$h_M^p = \beta_2[h_{(p-1)M}, e_{M-k}] + \beta_3[f_{(p-1)M+k}, e_{M-k}] + \beta_5[h_{(p-1)M}, h_M] + \beta_{10}[h_{(p-2)M}, h_{2M}]$$

where each β_i is independent of k.

The above equality can be translated into group-theoretic language as follows:

$$\begin{aligned} H_M^p \equiv\ & (H_{(p-1)M}, E_{M-k})^{\beta_2} (F_{(p-1)M+k}, E_{M-k})^{\beta_3} \\ & (H_{(p-1)M}, H_M)^{\beta_5} (H_{(p-2)M}, H_{2M})^{\beta_{10}} \mod \mathcal{G}_{N+1}. \end{aligned} \quad (4.7)$$

Applying the covering map $\varphi : \mathcal{G} \to \mathcal{Q}$ to both sides, we see that the following congruence holds in $\mathcal{Q}$:

$$\bar{H}_{pM} \equiv \bar{E}_{pM-k}^{2\beta_2}\, \bar{H}_{pM}^{-\beta_3} \mod \mathcal{Q}_{N+1}.$$

For this to be true, we must have $\beta_3 = -1$, $\beta_2 = 0$, and so the first factor on the right-hand side of (4.7) vanishes. Note that the remaining factors of (4.7) lie in $\mathcal{G}_N$. Now we go back to Lie algebras, but this time we will work with $L(\mathcal{G})$, not $L^\omega(\mathcal{G})$. By abuse of notation we denote the leading terms of E_i, F_i and H_i in $L(\mathcal{G})$ by the same symbols as their leading terms in $L^\omega(\mathcal{G})$, and let $v = \mathrm{LT}\,(H_M^p)$. Congruence (4.7) is equivalent to the following equality in $L_N(\mathcal{G}) = \mathcal{G}_N/\mathcal{G}_{N+1}$:

$$v = [e_{M-k}, f_{(p-1)M+k}] + \beta_5[h_{(p-1)M}, h_M] + \beta_{10}[h_{(p-2)M}, h_{2M}]. \tag{4.8}$$

Since $\mathcal{G}$ is an $(N-1)$-cover of $\mathcal{Q}$, we can evaluate all commutators in $\{e_i, f_i, h_i\}_{i\geq 1}$ of degree less than N using the isomorphism $L(\mathcal{G})/\gamma_N L(\mathcal{G}) \to \mathfrak{sl}_2(\mathbb{F}_p)\otimes t\mathbb{F}_p[t]/(t^N\mathbb{F}_p[t])$ given by $e_i \mapsto et^i$, $f_i \mapsto ft^i$, $h_i \mapsto ht^i$. For any $n > 1$, $m > 1$ with $n + m = N$ we have

$$[e_n, f_m] = \frac{1}{2}[h_1, e_{n-1}, f_m] = -\frac{1}{2}[e_{n-1}, f_m, h_1] - \frac{1}{2}[f_m, h_1, e_{n-1}] = [e_{n-1}, f_{m+1}] - \frac{\theta}{2} \quad \text{where } \theta = [h_{N-1}, h_1].$$

Iterating, we get $[e_n, f_m] = [e_{n-k}, f_{m+k}] - \dfrac{k}{2}\theta$. In particular,

$$[e_{M-k}, f_{(p-1)M+k}] = [e_M, f_{(p-1)M}] + \frac{k}{2}\theta.$$

Combining the last equality and (4.8), we see that $\dfrac{k}{2}\theta$ is equal to something independent of k. Since k can be equal to 1 or 2, we conclude that $\theta = 0$. But $\theta = [\mathrm{LT}\,(H_{N-1}), \mathrm{LT}\,(H_1)]$. The proof of Claim 4.4 is complete. □

We finish this section by giving a bound for the number of relators needed to present the groups $\{\mathcal{Q}(1, r)\}$.

Corollary 4.8. *The group $\mathcal{Q}(1, r)$ has a presentation with 2 generators and at most $5p + 15$ relators.*

Proof. Since $\mathcal{Q}^1(1, r)$ has index p in $\mathcal{Q}(1, r)$, it is easy to deduce from Proposition 4.3 that $\mathcal{Q}(1, r)$ has a presentation with 4 generators and $5p + 17$ relators. In the next section we will show that $\mathcal{Q}(1, r)$ can be generated by two elements. Thus the assertion of the Corollary is a consequence of the following well-known fact (see [**10**]): if a pro-p group G has a presentation with n generators and m relators, then any presentation (X, π) of G has a set of defining relators $\mathfrak{R}$ such that $\mathrm{card}\,(\mathfrak{R}) = \mathrm{card}\,(X) + m - n$. □

To simplify notation, in the next section we set $\mathcal{Q}(r) = \mathcal{Q}(1, r)$.

5. *Finite presentability of the Nottingham group*

In this section we give the proof of the main theorem. But first we need to recall several facts about the structure of the Nottingham group.

The Nottingham group $\mathcal{N} = \mathcal{N}(\mathbb{F}_p)$ has a natural congruence filtration $\{\mathcal{N}_n\}$ where $\mathcal{N}_n = \{t(1 + a_n t^n + a_{n+1}t^{n+1} + \ldots)\}$. The associated graded Lie algebra $L = L^{\mathrm{cong}}(\mathcal{N}) = \bigoplus_{n=1}^{\infty} \mathcal{N}_n/\mathcal{N}_{n+1}$ is known to be isomorphic to the positive part of the Witt algebra $W^+ = \mathrm{Der}^+ \mathbb{F}_p[t] = \bigoplus_{i=1}^{\infty} \mathbb{F}_p\, e_i$, where $e_i = t^{i+1}\partial_t$ and $[e_i, e_j] = (i-j)e_{i+j}$. An isomorphism between the two algebras is given by the map $\mathrm{LT}_{\mathrm{cong}}(t(1+t^n)) \mapsto e_n$.

The lower central series is closely related to but different from the congruence filtration. In fact, one has

$$\gamma_{(p-1)i+j}\mathcal{N} = \begin{cases} \mathcal{N}_{pi+j} & \text{if} \quad 0 \le j \le 1 \\ \mathcal{N}_{pi+j+1} & \text{if} \quad 1 < j < p-1 \end{cases} .$$

Now we will describe $L(\mathcal{N})$, the Lie algebra of $\mathcal{N}$ with respect to the lower central series. For each $n > 0$, set $\bar{U}_n = \frac{t}{1-t^n} \in \mathcal{N}$ and let $\bar{u}_n = \mathrm{LT}(\bar{U}_n)$. The elements $\{\bar{u}_n\}_{n=1}^{\infty}$ form an $\mathbb{F}_p$-basis of $L(\mathcal{N})$ (notice that $\deg(\bar{u}_n) \neq n$ for $n > 1$). The Lie algebra structure on $L(\mathcal{N})$ is determined by the following formulas:

$$[\bar{u}_i, \bar{u}_1] = (i-1)\bar{u}_{i+1}, \quad [\bar{u}_i, \bar{u}_2] = \begin{cases} (i-2)\bar{u}_{i+2} & \text{if } i \equiv 0, 1 \mod p \\ 0 & \text{otherwise} \end{cases} .$$

Caranti [**3**] found a finite presentation for a certain central extension of $L(\mathcal{N})$. As a consequence of his result we can write down a simple presentation for $L(\mathcal{N})$.

Let $LF = LF(u_1, u_2)$ be the free $\mathbb{Z}_p$-Lie algebra on generators u_1 and u_2. Define $u_n, r_n \in LF$ for $n \ge 3$ inductively by setting

$$u_n = \begin{cases} \dfrac{1}{n-2}[u_{n-1}, u_1] & \text{if} \quad n \not\equiv 2 \mod p \\ \\ \dfrac{1}{n-4}[u_{n-2}, u_2] & \text{if} \quad n \equiv 2 \mod p \end{cases}, \quad r_n = [u_{n-1}, u_2].$$

Proposition 5.1. *Assume that $p \ge 5$.*
1) The pointed Lie algebra $\omega = (L(\mathcal{N}), (\bar{u}_1, \bar{u}_2))$ admits the following presentation:

$$\langle u_1, u_2 \mid pu_1, pu_2,\ r_4, r_6, \ldots, r_{p-5}, r_{p-3},\ [u_{p+1}, u_1], r_{2p+2} + u_{2p+3}, \{r_{pn-1}\}_{n=1}^{\infty} \rangle.$$

2) For each $n \ge 1$ we have $u_n \underset{\omega}{=} \bar{u}_n$.

As one can see, the set of defining relators of $L(\mathcal{N})$ consists of an infinite family $\{r_{pn-1}\}$ and a finite number of "exceptional" relators. An easy computation shows that $\deg(r_{pn-1}) = (p-1)n - 1$ and the degrees of exceptional relators are equal to 1 (twice), 3, 5, …, $p-4$, $p+1$ and $2p$. Thus the largest degree of an exceptional relator is equal to $2p$, and the number of defining relators of degree at most $2p$ is equal to $\dfrac{p+7}{2}$.

Next we will discuss the relationship between $\mathcal{N}$ and its subgroups $\{\mathcal{Q}(r)\}$, $1 \le r \le (p-1)/2$. Let $\mathfrak{q}(r)$ be the Lie subalgebra of $L^{\mathrm{cong}}(\mathcal{N})$ corresponding to the

subgroup $\mathcal{Q}(r)$, i.e. $\mathfrak{q}(r) = \bigoplus_{i=1}^{\infty} (\mathcal{Q}(r) \cap \mathcal{N}_i) / (\mathcal{Q}(r) \cap \mathcal{N}_{i+1})$. In [**6**] we showed that

$$\mathfrak{q}(r) = \bigoplus_{n \equiv 0, \pm r \mod p} \mathbb{F}_p e_n.$$

As a consequence, one can prove the following:

a) $\mathfrak{q}(r)$ is generated by e_r and e_{p-r}, whence $\mathcal{Q}(r)$ is generated by any pair of elements $x, y \in \mathcal{Q}(r)$ such that $\mathrm{LT}_{\mathrm{cong}}(x) = \lambda e_r$ and $\mathrm{LT}_{\mathrm{cong}}(y) = \mu e_{p-r}$ with $\lambda, \mu \neq 0$;
b) $\gamma_{2i}\mathcal{Q}(r) = \mathcal{N}_{pi} \cap \mathcal{Q}(r)$ and $\gamma_{2i+1}\mathcal{Q}(r) = \mathcal{N}_{pi+r} \cap \mathcal{Q}(r)$ for all i;
c) $\mathcal{N} = \mathcal{Q}(1)\mathcal{Q}(2)\dots\mathcal{Q}(\frac{p-1}{2})$, i.e. any $g \in \mathcal{N}$ can be written in the form $g_1 g_2 \dots g_{\frac{p-1}{2}}$ where $g_r \in \mathcal{Q}(r)$;
d) if $r \neq r'$, then $\mathcal{Q}(r) \cap \mathcal{Q}(r') = \mathcal{T}$ where $\mathcal{T} = \{t(1 + t^p a) \mid a \in \mathbb{F}_p[[t^p]]\}$. This group was studied by Fesenko in [**7**]. In particular, he showed that $\mathcal{T}$ is finitely generated.

Note that if $p = 3$, the group $\mathcal{Q}(1)$ coincides with $\mathcal{N}$, and the assertion of Theorem 1.1 holds automatically. Thus from now on we assume that $p \geq 5$.

Here is the outline of the proof of the main theorem. We start with choosing a finitely presented $2p$-cover of $\mathcal{N}$. Then after imposing finitely many relations we obtain another cover which contains subgroups $\mathcal{S}_1$ and $\mathcal{S}_2$ isomorphic to the groups $\mathcal{Q}(1)$ and $\mathcal{Q}(2)$, respectively. Now each of these subgroups contains an isomorphic copy of the group $\mathcal{T} := \mathcal{Q}(1) \cap \mathcal{Q}(2)$. Since $\mathcal{T}$ is finitely generated, we can take another quotient (which is still finitely presented) where the two copies of $\mathcal{T}$ will be identified. The latter group turns out to be isomorphic to $\mathcal{N}$; this will follow from the specific form of relators in the family $\{r_{pn-1}\}$. Before proceeding, we introduce an important piece of notation which will be used throughout the proof. The initial cover of $\mathcal{N}$ will be called $\widetilde{\mathcal{G}}$, and the two quotients of $\widetilde{\mathcal{G}}$ mentioned above will be denoted by $\mathcal{G}'$ and $\mathcal{G}$. We will specify certain elements and subgroups of $\widetilde{\mathcal{G}}$ and denote each of them by a symbol of the form $\tilde{a}$ (where a is different in each case). We agree to denote the images of $\tilde{a}$ in $\mathcal{G}'$ and $\mathcal{G}$ by a' and a, respectively.

Proof of Theorem 1.1. Consider the following elements of $\mathcal{N}$: $\bar{A}_1 = \dfrac{t}{1-t}$, $\bar{A}_2 = \dfrac{t}{\sqrt{1-2t^2}}$, $\bar{B}_1 = t - \dfrac{t^p}{2}$, $\bar{B}_2 = \sqrt{t^2 - \dfrac{t^p}{4}}$ and let Ω be the pointed pro-p group $(\mathcal{N}, (\bar{A}_1, \bar{A}_2))$.

Let $(\widetilde{\mathcal{G}}, (\widetilde{A}_1, \widetilde{A}_2))$ be a $2p$-cover of Ω presented by at most $\dfrac{p+7}{2}$ relators (such cover exists by Proposition 3.2d)). Let $\varphi : \Delta \to \Omega$ be the covering map, and choose $\widetilde{B}_1, \widetilde{B}_2 \in \widetilde{\mathcal{G}}$ such that $\varphi(\widetilde{B}_1) = \bar{B}_1$, $\varphi(\widetilde{B}_2) = \bar{B}_2$. Now for $i = 1, 2$, $\bar{A}_i$ and $\bar{B}_i$ generate the group $\mathcal{Q}(i)$. Let $\langle x_i, y_i \mid R_{i1}(x_i, y_i), \dots, R_{ik}(x_i, y_i)\rangle$ be a presentation of the pointed group $(\mathcal{Q}(i), (\bar{A}_i, \bar{B}_i))$ where $k = 5p + 15$ (such a presentation exists by Corollary 4.8), and let $\mathcal{G}' = \widetilde{\mathcal{G}} / \langle \{R_{i1}(\widetilde{A}_i, \widetilde{B}_i), \dots, R_{ik}(\widetilde{A}_i, \widetilde{B}_i)\}_{i=1,2} \rangle^{\widetilde{\mathcal{G}}}$.

Since all the elements R_{ij} $(\bar{A}_i, \bar{B}_i)$ are trivial in $\mathcal{N}$, the surjection $\varphi : \widetilde{\mathcal{G}} \to \mathcal{N}$ factors through $\mathcal{G}'$, whence $(\mathcal{G}', (A'_1, A'_2))$ is also a $2p$-cover of Ω . Moreover, the subgroups $\mathcal{S}'_1 =< A'_1, B'_1 >$ and $\mathcal{S}'_2 =< A'_2, B'_2 >$ of $\mathcal{G}'$ are isomorphic to $\mathcal{Q}(1)$ and $\mathcal{Q}(2)$, respectively.

Finally, we must "glue" $\mathcal{S}'_1$ and $\mathcal{S}'_2$. Let $\mathcal{T} = \mathcal{Q}(1) \cap \mathcal{Q}(2)$. Recall that $\mathcal{T} = \{t(1 + t^p a) \mid a \in \mathbb{F}_p[[t^p]]\}$. It follows from [**7**, Theorem, p.743] that $\mathcal{T}$ is gen-

erated by the elements $\bar{H}_1, \dots, \bar{H}_{p+1}$ where $\bar{H}_i = t(1+t^{pi}) \in \mathcal{N}$. Let $H'_{i,j}$ be the unique element of $\mathcal{S}'_i$ such that $\varphi(H'_{i,j}) = \bar{H}_j$. We claim that the group $\mathcal{G} = \mathcal{G}'/\langle {H'_{1,1}H'_{2,1}}^{-1}, \dots, {H'_{1,p+1}H'_{2,p+1}}^{-1}\rangle^{\mathcal{G}'}$ is isomorphic to $\mathcal{N}$.

Let $\Delta = (\mathcal{G}, (A_1, A_2))$. Obviously, Δ is a $2p$-cover of Ω. By abuse of notation, the covering map from Δ to Ω will also be denoted by φ. Now fix n and suppose we have already shown that Δ is an $(n-1)$-cover of Ω. To show that Δ is an n-cover of Ω we will apply Proposition 3.2c). Note that $\operatorname{LT}\varphi(A_i) = \bar{u}_i$ for $i = 1, 2$, whence the pointed Lie algebra ω, whose presentation was given in Proposition 5.1, coincides with $L(\Omega)$. The above presentation has no defining relators of degree $n > 2p$ unless $n \equiv -1 \mod (p-1)$. Thus we can assume that $n = (p-1)M - 1$ for some M in which case $[u_{pM-2}, u_2]$ is the unique defining relator of degree n. Therefore, it suffices to prove that $[u_{pM-2}, u_2]$ is a relator of $L(\Delta)$.

Let $D = \underbrace{(B_2, A_2, B_2, A_2, \dots, B_2, A_2, B_2)}_{2M-1} \in \mathcal{G}$, and let $\bar{D} = \varphi(D) \in \mathcal{N}$. A direct computation shows that $\bar{D}^{-8} \equiv \bar{U}_{pM-2} \mod \gamma_n\mathcal{N}$ which implies

$$u_{pM-2} \underset{L(\bar{\Omega})}{=} -8\operatorname{LT}(\bar{D}) = -8\operatorname{LT}\varphi(D) \in L_{n-1}(\mathcal{N}).$$

But Δ is an $(n-1)$-cover of Ω, whence $u_{pM-2} \underset{L(\bar{\Delta})}{=} -8\operatorname{LT}(D) \in L_{n-1}(\mathcal{G})$ by Proposition 3.2b). Similarly one shows that $u_2 \underset{L(\bar{\Delta})}{=} \operatorname{LT}(A_2) \in L_1(\mathcal{G})$. Therefore, $[u_{pM-2}, u_2] \underset{L(\bar{\Delta})}{=} 0$ if and only if the commutator $C = (D, A_2)$ lies in $\gamma_{n+1}\mathcal{G}$. We are going to show that $C^2 \equiv H_{2,M} = H_{1,M} \equiv 1 \mod \gamma_{n+1}\mathcal{G}$.

Step 1: $H_{2,M} = H_{1,M}$.
Indeed, let $\mathcal{T}_1 = \langle\{H_{1,i}\}_{i=1}^{\infty}\rangle$ and $\mathcal{T}_2 = \langle\{H_{2,i}\}_{i=1}^{\infty}\rangle$. Since $\operatorname{Ker}\varphi$ intersects $\mathcal{T}_1$ and $\mathcal{T}_2$ trivially, and $\varphi(\mathcal{T}_1) = \varphi(\mathcal{T}_2) = \mathcal{T}$, there is a unique isomorphism $\iota : \mathcal{T}_1 \to \mathcal{T}_2$ such that $\varphi\,\iota|_{\mathcal{T}_1} = \varphi|_{\mathcal{T}_1}$. Clearly, $\iota(H_{1,i}) = H_{2,i}$ for all i. But $H_{1,i} = H_{2,i}$ in $\mathcal{G}$ for $i = 1, 2, \dots, p+1$ by construction, and since $\mathcal{T}_1$ is generated by $H_{1,1}, \dots H_{1,p+1}$, we conclude that ι has to be the identity map. Therefore, $H_{1,i} = H_{2,i}$ for all i.

Step 2: $C^2 \equiv H_{2,M} \mod \gamma_{n+1}\mathcal{G}$.
A computation in $\mathcal{N}$ shows that $\bar{H}_M^{-1}\varphi(C)^2 \in \mathcal{N}_{pM+2} \cap \mathcal{Q}(2) = \gamma_{2M+1}\mathcal{Q}(2)$. Since φ maps $\mathcal{S}_2$ isomorphically onto $\mathcal{Q}(2)$ and $\varphi(H_{2,M}) = \bar{H}_M$, we conclude that $H_{2,M} \equiv C^2 \mod \gamma_{2M+1}\mathcal{S}_2$. But $\gamma_{2M}\mathcal{S}_2 \subseteq \gamma_n G$ since $\varphi(\gamma_{2M}\mathcal{S}_2) = \gamma_{2M}\mathcal{Q}(2) \subset \gamma_{n+1}\mathcal{N}$ and $\operatorname{Ker}\varphi \subseteq \gamma_n\mathcal{G}$. Therefore, $\gamma_{2M+1}\mathcal{S}_2 \subseteq \gamma_{n+1}\mathcal{G}$ and we are done.

Step 3: $H_{1,M} \equiv 1 \mod \gamma_{n+1}\mathcal{G}$.
A similar computation in $\mathcal{S}_1$ yields $H_{1,M} \equiv \underbrace{(B_1, A_1, \dots, B_1, A_1)}_{2M} \mod \gamma_{n+1}\mathcal{G}$. But this time $E := \underbrace{(B_1, A_1, \dots, B_1)}_{2M-1}$ lies in $\gamma_n\mathcal{G}$ (since $\varphi(E) \in \mathcal{N}_{pM-1} = \gamma_n\mathcal{N}$ and $\operatorname{Ker}\varphi \subseteq \gamma_n\mathcal{G}$), so $H_{1,M} \equiv (E, A_1) \equiv 1 \mod \gamma_{n+1}\mathcal{G}$.

To finish the proof we just have to notice that the number of relators needed to present $\mathcal{G}$ does not exceed $\frac{p+7}{2} + 2(5p+15) + p + 1 \le 12p + 32$. □

6. *Appendix*

In this section we outline the proof of the assertions of Lemma 4.5. As we already mentioned, the proof reduces to a certain computation in the group $\mathcal{Q}^1(1, r)$. We fix r and set $\mathcal{Q} = \mathcal{Q}^1(1, r)$, $\mathcal{S} = SL_2^1(\mathbb{F}_p[[t]])$, $\mathcal{Q}_n = \gamma_n\mathcal{Q}$, $\mathcal{S}_n = \gamma_n\mathcal{S}$.

Given $g \in \mathcal{Q}$, let $\deg(g)$ denote the degree of g with respect to the lower central series of $\mathcal{Q}$, and let $d(g)$ be the degree of g with respect to the congruence filtration of $\mathcal{N}$. It follows from the results of [**6**] that for every $g \in \mathcal{Q}$ there exists $e(g) \in \{\pm r, 0\}$ such that $d(g) = p\deg(g) + e(g)$.

Let $\varepsilon = \varepsilon_{1,r} : SL_2^1(\mathbb{F}_p[[t]]) \to \mathcal{Q}$ be the map defined in Section 4, and let ε^{-1} be the inverse map. Given $g_1, g_2 \in \mathcal{Q}$, let $h_1 = \varepsilon^{-1}(g_1)$ and $h_2 = \varepsilon^{-1}(g_2)$. The following formula is the key to proving the assertions of Lemma 4.5.

$$g_1 g_2 = \varepsilon(h_1)\varepsilon(h_2) \equiv \varepsilon(h_1 h_2) \mod \mathcal{Q}_M, \tag{6.1}$$

$$(g_1, g_2) = (\varepsilon(h_1), \varepsilon(h_2)) \equiv \varepsilon((h_1, h_2)) \mod \mathcal{Q}_M, \tag{6.2}$$

$$\text{where } M = \min(d(g_1) + \deg(g_2), d(g_2) + \deg(g_1)).$$

The proofs of (6.1) and (6.2) are analogous to those of [**6**, Proposition 4.3] and [**6**, Proposition 4.2], respectively.

We are forced to change notation of Section 4, since $\bar{E}_i$, $\bar{F}_i$, $\bar{H}_i$ were used to denote elements of different groups. We will keep using these symbols for the elements of $\mathcal{Q}$, and the corresponding elements of $\mathcal{S} = SL_2^1(\mathbb{F}_p[[t]])$ will be denoted by E_i, F_i and H_i. In other words, $\bar{E}_i = \varepsilon(E_i)$, $\bar{F}_i = \varepsilon(F_i)$, $\bar{H}_i = \varepsilon(H_i)$.

The following congruences in $\mathcal{S} = SL_2^1(\mathbb{F}_p[[t]])$ can be verified directly:

$$\begin{array}{ll}
1)(E_n, E_m) = 1 & 2)(F_n, F_m) = 1 \\
3)(H_n, H_m) = 1 & 4)F_n^{H_m} \equiv F_n F_{n+m}^2 \mod \mathcal{S}_{2m+n} \\
5)E_n^{H_m} = E_n E_{n+m}^{-2} & 6)E_n^{F_m} \equiv E_n H_{n+m} \cdot F_{n+2m}^{-1} \mod \mathcal{S}_{2n+m} \\
7)E_n^p = 1 & 8)F_n^p = 1
\end{array}$$

This takes care of Lemma 4.5 for $SL_2^1(\mathbb{F}_p[[t]])$. In the case $\mathcal{Q} = \mathcal{Q}^1(1, r)$ each congruence in the assertion of Lemma 4.5 easily follows from the corresponding congruence in the above list and formulas (6.1) and (6.2). We illustrate this by proving part 6) of Lemma 4.5.

First we compute the degrees of $\bar{E}_n$, $\bar{F}_n$ and $\bar{H}_n$. It is clear that $\deg(\bar{E}_n) = \deg(\bar{F}_n) = \deg(\bar{H}_n) = n$, $d(\bar{E}_n) = pn - r$, $d(\bar{H}_n) = pn$, $d(\bar{F}_n) = pn + r$. Applying (6.2), we have

$$(\bar{E}_n, \bar{F}_m) \equiv \varepsilon((E_n, F_m)) \mod \mathcal{Q}_{n+pm+r}\, \mathcal{Q}_{m+pn-r}$$

We also know that $(E_n, F_m) \equiv H_{n+m} \cdot F_{n+2m}^{-1} \mod \mathcal{S}_{2n+m}$, whence

$$\varepsilon((E_n, F_m)) \equiv \varepsilon(H_{n+m} \cdot F_{n+2m}^{-1}) \mod \mathcal{Q}_{2n+m}.$$

Finally, (6.1) yields

$$\varepsilon(H_{n+m} \cdot F_{n+2m}^{-1}) \equiv \bar{H}_{n+m} \bar{F}_{n+2m}^{-1} \mod \mathcal{Q}_{p(n+m)+n+2m}\, \mathcal{Q}_{p(n+2m)+r+n+m}$$

Combining these congruences and taking into account that $m + pn - r \geq 2n + m$ (since $(p-2)n \geq p - 2 \geq (p-1)/2 \geq r$), we have

$$(\bar{E}_n, \bar{F}_m) \equiv \bar{H}_{n+m} \cdot \bar{F}_{n+2m}^{-1} \mod \mathcal{Q}_{2n+m}\, \mathcal{Q}_{n+pm+r}$$

which is exactly what we wanted.

Remark. The reader may have noticed that the approximation map $\varepsilon_{s,r}$ defined in Section 4 does not coincide with the analogous map $\varphi_{s,r}$ from [**6**]. In [**6**] it was more convenient to think of elements of the Nottingham group as automorphisms

of $\mathbb{F}_p[[t]]$. We adopted the usual convention that automorphisms act on the left; the price we had to pay was that the natural map {power series} $\to$ {automorphisms} given by $f \mapsto (t \mapsto f)$ became an anti-isomorphism instead of an isomorphism.

In this paper we consider elements of $\mathcal{N}$ as power series, and in order to keep computations as simple as possible we use a different approximation map. It is easy to see that all the properties of the old map $\varphi_{s,r}$ asserted in [**6**] hold true for $\varepsilon_{s,r}$, and the proofs are absolutely analogous.

Acknowledgements. The author is grateful to Efim Zelmanov and Alexander Lubotzky for very helpful discussions

References

1. R. Camina, 'Subgroups of the Nottingham group', *J. Algebra* 196 (1997), no. 1, 101–113.
2. R. Camina, 'The Nottingham group', *New horizons in pro-p groups* 205–221, Progr. Math., 184, Birkhuser Boston, Boston, MA, 2000.
3. A. Caranti, 'Presenting the graded Lie algebra associated with the Nottingham group', *J. Algebra* 198 (1997), no. 1, 266-289.
4. A. Caranti, S. Mattarei, M. F. Newman and C.M.Scoppola, 'Thin groups of prime-power order and thin Lie algebras', *Quart. J. Math Oxford Ser.(2)* 47(1996), no. 187, 279-296.
5. M. du Sautoy, D. Segal and A. Shalev, 'New horizons in pro-p groups', Progress in Mathematics, 184, Birkhuser Boston, Boston, MA, 2000.
6. M. Ershov, 'New just-infinite pro-p groups of finite width and subgroups of the Nottinhgam group', *J. Algebra* 275 (2004), no. 1, 419-449.
7. I. Fesenko, 'On just infinite pro-p-groups and arithmetically profinite extensions of local fields', *J. Reine Angew. Math.* 517 (1999), 61–80.
8. C. R. Leedham-Green and S. McKay, 'The structure of groups of prime power order', London Mathematical Society Monographs. New Series, 27. Oxford Science Publications. Oxford University Press, Oxford, 2002.
9. A. Lubotzky and A. Shalev, 'On some Λ-analytic pro-p groups', *Israel J. Math.* 85 (1994), no. 1-3, 307–337.
10. J. Wilson, 'Profinite groups', London Mathematical Society Monographs. New Series, 19. The Clarendon Press, Oxford University Press, New York, 1998

M. V. Ershov
Department of Mathematics
Yale Univeristy
10 Hillhouse Avenue
New Haven, Connecticut 06520
USA

mikhail.erchov@yale.edu