TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 362, Number 12, December 2010, Pages 6663–6678
S 0002-9947(2010)05160-8
Article electronically published on August 3, 2010

ON THE COMMENSURATOR OF THE NOTTINGHAM GROUP

MIKHAIL ERSHOV

Abstract. Let $p \geq 5$ be a prime number. We prove that the abstract commensurator of the Nottingham group $\mathcal{N}(\mathbb{F}_p)$ coincides with its automorphism group, which is known to be a finite extension of $\mathcal{N}(\mathbb{F}_p)$. As a corollary we deduce that the Nottingham group cannot be embedded as an open subgroup of a topologically simple group.

1. Introduction

Let G be a profinite group. Let $\mathrm{VAut}\,(G)$ be the set of virtual automorphisms of G, that is, the set of isomorphisms from an open subgroup of G onto another open subgroup of G. Two elements of $\mathrm{VAut}\,(G)$ are said to be equivalent if they coincide on some open subgroup of G. Equivalence classes of elements of $\mathrm{VAut}\,(G)$ form a group called the *abstract commensurator* of G and denoted by $\mathrm{Comm}(G)$.

The commensurator $\mathrm{Comm}(G)$ contains significantly more information about G than the automorphism group $\mathrm{Aut}\,(G)$. In particular, for any open subgroup U of G, there is a canonical homomorphism $\rho_{U,G} : \mathrm{Aut}\,(U) \to \mathrm{Comm}(G)$. A less obvious and very interesting fact is that $\mathrm{Comm}(G)$ essentially determines possible structures of topological groups containing G as an open subgroup. This relationship is investigated in detail in [BEW], where systematic study of commensurators of profinite groups is initiated. As shown in [BEW], several classical rigidity theorems from the theory of algebraic groups and number theory can be interpreted as results about commensurators for certain classes of profinite groups. In particular, commensurators of open compact subgroups of simple algebraic groups over (non-archimedean) local fields are described by the following theorem, which is a consequence of Pink's structure theory for such groups [Pi] (see [BEW, Section 3] for details):

Theorem 1.1. *Let K be a local field, let $\mathbb{G}$ be an absolutely simple simply connected algebraic group over K, and let G be an open compact subgroup of $\mathbb{G}(K)$. Then* $\mathrm{Comm}(G)$ *is canonically isomorphic to* $(\mathrm{Aut}\,\mathbb{G})(K) \rtimes \mathrm{Aut}\,(K)$.

For instance, if O is the ring of integers of a local field K, then for $n \geq 3$, the group $\mathrm{Comm}(SL_n(O))$ is isomorphic to $PGL_n(K) \rtimes (\langle d \rangle \times \mathrm{Aut}\,(K))$ where d is the Dynkin involution, and $\mathrm{Comm}(SL_2(O))$ is isomorphic to $PGL_2(K) \rtimes \mathrm{Aut}\,(K)$.

Received by the editors October 20, 2008 and, in revised form, May 4, 2009.

2010 *Mathematics Subject Classification.* Primary 20F28; Secondary 20E18, 20F40.

This material is based upon work supported by the National Science Foundation under agreement No. DMS-0111298. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

In this paper we determine the commensurator of the Nottingham group $\mathcal{N}(\mathbb{F}_p)$ for $p \geq 5$ and compare the result with Theorem 1.1. Recall that for a finite field F, the Nottingham group $\mathcal{N}(F)$ is defined as the first congruence subgroup of the group of F-linear automorphisms of the ring $F[[t]]$, that is, $\mathcal{N}(F) = \{\varphi \in \mathrm{Aut}_F(F[[t]]) \mid \varphi(t) \equiv t \mod t^2F[[t]]\}$. The Nottingham group $\mathcal{N}(F)$ behaves similarly to Chevalley groups like $SL_n(F[[t]])$ on the "Lie algebra level", but at the same time $\mathcal{N}(F)$ is very far from being linear and cannot be studied using powerful methods of the theory of algebraic groups. For this reason, $\mathcal{N}(F)$ is an excellent test example for many questions or conjectures in profinite group theory that have been settled for Chevalley groups.

The automorphism group of $\mathcal{N}(F)$ has been determined by Klopsch when char $F \geq 5$. Let $\mathrm{Aut}\,(F[[t]])$ denote the full automorphism group of the ring $F[[t]]$. It is easy to see that $\mathrm{Aut}\,(F[[t]]) \cong \mathcal{N}(F) \rtimes (F^* \times \mathrm{Aut}\,(F))$ where F^* is the subgroup of F-linear automorphisms of $F[[t]]$ of the form $\{t \mapsto \alpha t \mid \alpha \in F^*\}$. In particular, $\mathcal{N}(F)$ is a normal subgroup (of finite index) in $\mathrm{Aut}\,(F[[t]])$, and thus there is a natural homomorphism $i_F : \mathrm{Aut}\,(F[[t]]) \to \mathrm{Aut}\,(\mathcal{N}(F))$. In [K], Klopsch proved that i_F is an isomorphism whenever char $F \geq 5$. In this paper we prove that $\mathrm{Comm}(\mathcal{N}(F))$ coincides with $\mathrm{Aut}\,(\mathcal{N}(F))$ when F is a field of prime order $p \geq 5$.

Theorem 1.2. *Let $p \geq 5$ be a prime and $\mathcal{N} = \mathcal{N}(\mathbb{F}_p)$. Then the natural mapping $\mathrm{Aut}\,(\mathcal{N}) \to \mathrm{Comm}(\mathcal{N})$ is an isomorphism. Hence $\mathrm{Comm}(\mathcal{N}) \cong \mathrm{Aut}\,(\mathbb{F}_p[[t]])$ and $\mathcal{N}$ is a normal subgroup of $\mathrm{Comm}(\mathcal{N})$ of index $p-1$.*

Comparing Theorems 1.2 and 1.1, we see that the commensurator of the Nottingham group $\mathcal{N}(\mathbb{F}_p)$ is much smaller than the commensurator of $SL_n(\mathbb{F}_p[[t]])$. Probably, the most important difference is that $\mathrm{Comm}(\mathcal{N}(\mathbb{F}_p))$ is a compact group while $\mathrm{Comm}(SL_n(\mathbb{F}_p[[t]]))$ is not. By [BEW, Corollary 4.5], if G is a finitely generated profinite group such that $\mathrm{Comm}(G) = \mathrm{Aut}\,(G)$, then no finite index subgroup of G can be embedded as an open subgroup of a topologically simple group. By Theorem 1.2, this result applies to the Nottingham group.

Corollary 1.3. *Let G be a finite index subgroup of the Nottingham group $\mathcal{N}(\mathbb{F}_p)$ for some $p \geq 5$. Then G cannot be embedded as an open subgroup of a topologically simple group.*

On the contrary, each of the groups $SL_n(F[[t]])$ has a finite index subgroup, namely the first congruence subgroup $SL_n^1(F[[t]])$, which is isomorphic to an open subgroup of the simple group $PSL_n(F((t)))$.

Here is yet another interesting consequence of Theorem 1.2.

Corollary 1.4. *Let G and H be finite index subgroups of $\mathcal{N}(\mathbb{F}_p)$ for some $p \geq 5$, with G normal in $\mathcal{N}(\mathbb{F}_p)$ and H non-normal. Then G and H are not isomorphic.*

Once again, the situation is completely different for subgroups $SL_n(F[[t]])$. If g is any element in $SL_n(F((t)))$ lying outside of $SL_n(F[[t]])$ and G is a normal subgroup of $SL_n(F[[t]])$ such that $gGg^{-1} \subseteq SL_n(F[[t]])$, then G and gGg^{-1} are isomorphic finite index subgroups of $SL_n(F[[t]])$, with the first one being normal and the second one non-normal.

We now briefly describe the proof of Theorem 1.2. The main tools in that proof are the correspondence between subgroups of $\mathcal{N}(\mathbb{F}_p)$ and subalgebras of the graded Lie algebra of $\mathcal{N}(\mathbb{F}_p)$ and the notion of Hausdorff dimension. In the discussion below, $\mathcal{N}$ will stand for $\mathcal{N}(\mathbb{F}_p)$ for some $p \geq 5$.

Let G be a profinite group, and let $\{G_n\}_{n\geq 1}$ be a filtration of G such that $[G_i, G_j] \subseteq G_{i+j}$. The corresponding graded Lie algebra $L(G)$ is defined by $L(G) = \bigoplus_{n\geq 1} G_n/G_{n+1}$, and with each subgroup H of G one can associate the Lie subalgebra $L(H) = \bigoplus_{n\geq 1}(H \cap G_n)/(H \cap G_{n+1})$. In general, correspondence between subgroups of G and subalgebras of $L(G)$ is very weak. However, if $G = \mathcal{N}$ and $L(\mathcal{N})$ is the Lie algebra of $\mathcal{N}$ with respect to the congruence filtration, then some subgroups of $\mathcal{N}$ can be recovered from their Lie algebras uniquely up to conjugation – this is the main result of Section 4.

Given an arbitrary profinite group G and a filtration $\{G_n\}$ of G, one can measure the relative sizes of subgroups of G using Hausdorff dimension with respect to suitable metric depending on the filtration $\{G_n\}$ (see [Ab], [BSh] and Section 2). Hausdorff dimension is a particularly useful tool when it is independent of the filtration. The list of known groups with this property is rather short, but it includes the Nottingham group $\mathcal{N}(F)$, with $\operatorname{char} F > 2$. It easily follows that any virtual automorphism φ of $\mathcal{N}$ must preserve Hausdorff dimension of any subgroup of $\mathcal{N}$. For many subgroups H of $\mathcal{N}$ this yields strong restrictions on the Lie subalgebra $L(\varphi(H))$, and in some cases even implies that $L(\varphi(H)) = L(H)$. Thus, if H is one of the subgroups of $\mathcal{N}$ that can be recovered from its Lie algebra, we obtain good control over possible images of H under virtual automorphisms of $\mathcal{N}$. Eventually, we show that for every $\varphi \in \mathrm{VAut}\,(\mathcal{N})$ there is a family of (non-open) subgroups of $\mathcal{N}$, each of which is isomorphic to $\mathcal{N}$ and is mapped by φ to its own conjugate. At this point we can use Klopsch's description of $\mathrm{Aut}\,(\mathcal{N})$ to finish the proof.

We believe that the isomorphism $\mathrm{Comm}(\mathcal{N}(F)) \cong \mathrm{Aut}\,(\mathcal{N}(F))$ holds for any finite field F, with $\operatorname{char} F \geq 5$, and that this result can be proved by adapting the method used in this paper. On the other hand, the restriction $\operatorname{char} F \geq 5$ seems to be essential: in fact, it is used in several different places in the proof.

Basic notation and terminology. Throughout the paper $\mathbb{Z}$ denotes integers, $\mathbb{N}$ positive integers, and $p \geq 5$ is a fixed prime number. A numerical congruence $a \equiv b \mod n$ will be abbreviated as $a \equiv_n b$.

We will mostly work with topological groups, so by a subgroup we mean a closed subgroup unless indicated otherwise. If G is a group and $g, h \in G$, then $g^h = h^{-1}gh$ and $(g, h) = g^{-1}h^{-1}gh$; similarly, if K, L are subgroups of G and $g \in G$, we let (K, L) be the subgroup generated by $\{(k, l) \mid k \in K, l \in L\}$ and $K^g = \{k^g \mid k \in K\}$.

2. Density functions and Hausdorff dimension

Let G be a profinite group. A *filtration* of G is a descending chain $\{G_n\}$ of open normal subgroups of G, with $G_1 = G$, which form a base of neighborhoods of identity. By a *filtered group* we mean a group with chosen filtration.

Fix a filtration $\{G_n\}$ of G. For a subgroup H of G, we define the *density function*[1] $d_{H,G} : \mathbb{N} \to \mathbb{R}$ by

$$d_{H,G}(n) = \frac{\log |HG_n : G_n|}{\log |G : G_n|} = \frac{\log |H : (H \cap G_n)|}{\log |G : G_n|}.$$

The density function $d_{H,G}$ is directly related to the *Hausdorff dimension* of H with respect to certain metric[2] (depending on the filtration $\{G_n\}$). In [BSh], Barnea and Shalev showed that the Hausdorff dimension of a subgroup H of G, which will

[1] This terminology is taken from [AV].

[2] Hausdorff dimension in this context was introduced by Abercrombie in [Ab].

be denoted by $\dim_G H$, is equal to the lower limit of its density function $d_{H,G}(n)$ as $n \to \infty$:

$$\dim_G H = \liminf_{n\to\infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|}.$$

We shall often refer to Hausdorff dimension simply as dimension, since no other notions of dimension will be used.

In general, the Hausdorff dimension and the density function of a subgroup depend heavily on the filtration $\{G_n\}$. In [Er], it was shown that Hausdorff dimension is filtration-independent if G has "rigid" normal subgroup structure and the filtration $\{G_n\}$ is assumed to have finite width. In this paper we shall consider a slight variation of the rigidity condition from [Er].

Definition. Let G be a profinite group.

(a) A filtration $\{G_n\}$ of G is of *finite width* if there exists a constant C such that $|G_n : G_{n+1}| \leq C$ for all n.
(b) Given a filtration $\{G_n\}$ of G and an open subgroup H of G, we define the *stretch* of H with respect to $\{G_n\}$, denoted by $s(H; \{G_n\})$, to be the smallest $C \in \mathbb{N}$ such that $G_i \subseteq H \subseteq G_j$ for some $j < i$ with $|G_j : G_i| \leq C$.
(c) The *stretch* of a filtration $\{G_n\}$ of G is defined to be

$$\sup\{s(H; \{G_n\}) \mid H \text{ is open and normal in } G\}.$$

We will say that a filtration is *narrow* if it has finite stretch.
(d) The group G will be called *narrow* if it has a narrow filtration.

Remark. Note that a narrow filtration is necessarily of finite width. If we assume that $\{G_n\}$ has finite width and no repeated terms ($G_n \neq G_{n+1}$ for all n), then $\{G_n\}$ is narrow if and only if there exists $e \in \mathbb{N}$ such that any open normal subgroup of G lies between G_{m+e} and G_m for some m.

Basic examples of narrow groups include the linear pro-p groups $SL_n^1(\mathbb{Z}_p)$ and $SL_n^1(\mathbb{F}_p[[t]])$, with $p \nmid n$, as well as their open subgroups (see [Er, Lemma 5.4]). Formally, [Er, Lemma 5.4] asserts that these groups have a slightly weaker property, called *rigidity* in [Er], but the proof shows that they are actually narrow. A similar argument shows that open subgroups of the Nottingham group are narrow when $p > 2$. For completeness, we will give a proof of this fact in the next section (see Proposition 3.3)

Proposition 2.1. *Let G be a narrow group. Then any finite width filtration of G is narrow.*

Proof. Let $\{G_n\}$ be a narrow filtration of G and $\{G'_n\}$ any finite width filtration of G. Let D be such that $|G'_n : G'_{n+1}| \leq D$ for all n, and let C be the stretch of $\{G_n\}$.

Now take any open normal subgroup H of G. By definition of D, there exists $m \in \mathbb{N}$ such that $1 \leq \frac{|G:G'_m|}{|G:H|} \leq D$. Similarly, we can choose $u \geq m$ such that $C^2 \leq |G'_m : G'_u| \leq C^2 D$. Finally, choose $v \leq m$ as follows: if $|G : G'_m| \geq C^2 D$, find v such that $C^2 D \leq |G'_v : G'_m| \leq (CD)^2$, and if $|G : G'_m| \leq C^2 D$, set $v = 1$. We claim that $G'_u \subseteq H \subseteq G'_v$. Since $|G'_v : G'_u| \leq C^4 D^3$ by construction, this would imply that the filtration $\{G'_n\}$ is narrow and finish the proof.

Indeed, by definition of C there exist $s_1, t_1, s_2, t_2 \in \mathbb{N}$ such that $G_{s_1} \subseteq G'_u \subseteq G_{t_1}$ and $G_{s_2} \subseteq H \subseteq G_{t_2}$ with $|G_{t_1} : G_{s_1}| \leq C$ and $|G_{t_2} : G_{s_2}| \leq C$. Thus,

$$\frac{|G : G_{t_1}|}{|G : G_{s_2}|} \geq \frac{|G : G'_u|}{C^2 \, |G : H|}.$$

On the other hand, $\frac{|G:G'_u|}{|G:H|} = \frac{|G:G'_m||G'_m:G'_u|}{|G:H|} \geq C^2$ by construction. Therefore, $\frac{|G:G_{t_1}|}{|G:G_{s_2}|} \geq 1$, whence $s_2 \leq t_1$ and we get $G'_u \subseteq G_{t_1} \subseteq G_{s_2} \subseteq H$. Similarly, one shows that $H \subseteq G'_v$. □

Corollary 2.2. *Let G be a narrow group and let $\{G_n\}$, $\{G'_n\}$ be finite width filtrations of G with no repeated terms. Then there exists $e \in \mathbb{N}$ and a function $f : \mathbb{N} \to \mathbb{N}$ such that $G_{f(n)+e} \leq G'_n \leq G_{f(n)}$ for each n.*

Definition. Let H be a subgroup of a profinite group G, and let $\{G_n\}$ be a filtration of G. We will say that

(a) H has *pure dimension* (with respect to $\{G_n\}$) if its density function $d_{H,G}(n)$ has a limit as $n \to \infty$;
(b) H has *strong dimension* α if there exists a constant C such that

$$\left|\log_2 |HG_n : G_n| - \alpha \log_2 |G : G_n|\right| < C$$

for all $n \in \mathbb{N}$.

We now state the main result on filtration-independence of Hausdorff dimension in narrow groups. It easily follows from Corollary 2.2.

Proposition 2.3. *Let G be a narrow group. Then any subgroup H of G has the same Hausdorff dimension with respect to all finite width filtrations of G. Furthermore, if H has strong (resp. pure) dimension α with respect to some finite width filtration of G, then H has strong (resp. pure) dimension α with respect to any finite width filtration of G.*

When we have a chain of three groups $K \subseteq H \subseteq G$, we can talk about the density function of K as a subgroup of H or as a subgroup of G. The following straightforward result describes the relationship between the two functions and the corresponding dimensions.

Proposition 2.4. *Let G be a profinite group and $K \subseteq H$ subgroups of G. Choose a filtration $\{G_n\}$ of G, and consider the induced filtration $\{G_n \cap H\}$ on H. Then the corresponding density functions satisfy the following relation:*

$$d_{K,G}(n) = d_{K,H}(n) \cdot d_{H,G}(n).$$

Furthermore, if H has pure (resp. strong) dimension in G and K has pure (resp. strong) dimension in H, then K has pure (resp. strong) dimension in G, and $\dim_G(K) = \dim_G(H) \cdot \dim_H(K)$.

Now we shall see why the notions introduced in this section are useful for studying commensurators of profinite groups.

Proposition 2.5. *Let G be a profinite group all of whose open subgroups are narrow, and let $\{G_n\}$ be a finite width filtration of G with no repeated terms. Let φ be a virtual automorphism of G, and let $N \in \mathbb{N}$ be such that both the domain and the image of φ contain G_N. Then there exists a constant $e \in \mathbb{N}$ such that $G_{n+e} \subseteq \varphi(G_n) \subseteq G_{n-e}$ for all $n \geq N + e$.*

Proof. Choose $M > N$ such that $G_N \supseteq \varphi(G_M)$. Since G_N is contained in the domain and the image of φ, we know that for any $n \geq M$ both G_n and $\varphi(G_n)$ are normal in G_N. Thus $G_N \supseteq G_M \supseteq G_{M+1} \supseteq G_{M+2} \supseteq \ldots$ and $G_N \supseteq \varphi(G_M) \supseteq \varphi(G_{M+1}) \supseteq \ldots$ are finite width filtrations of G_N. Since G_N is narrow, by Corollary 2.2 there exist $e_1 \in \mathbb{N}$ and a function f such that $G_{f(n)+e_1} \subseteq \varphi(G_n) \subseteq G_{f(n)}$ for all $n \geq M$.

Next we claim that there is $e_2 \in \mathbb{N}$ such that $|f(n) - n| \leq e_2$ for all $n \geq M$. Indeed, for any $n \geq M$ we have

$$\frac{|G : G_{f(n)}|}{|G : G_n|} \leq \frac{|G : \varphi(G_n)|}{|G : G_n|} = \frac{|G : \varphi(G_N)||\varphi(G_N) : \varphi(G_n)|}{|G : G_N||G_N : G_n|} = \frac{|G : \varphi(G_N)|}{|G : G_N|}.$$

On the other hand, if $f(n) \geq n$, then $\frac{|G:G_{f(n)}|}{|G:G_n|} = |G_n : G_{f(n)}| \geq 2^{f(n)-n}$ (the last inequality holds because $\{G_i\}$ has no repeated terms). So, the function $f(n) - n$ is bounded from above. Similarly, we obtain a lower bound.

Taking $e = \max\{e_1 + e_2, M - N\}$, we get $G_{n+e} \subseteq \varphi(G_n) \subseteq G_{n-e}$ for all $n \geq N + e$. □

Corollary 2.6. *Let G be a profinite group all of whose open subgroups are narrow. Let φ be a virtual automorphism of G and H a subgroup of G. Then H and $\varphi(H)$ have the same Hausdorff dimension. Moreover, if H has strong dimension, then so does $\varphi(H)$.*

The concept of narrowness is just one of many similar conditions on a profinite group which yield independence of Hausdorff dimension from the choice of a filtration. A slightly weaker condition is considered in [Er] where a profinite group G is called *rigid* if there exists $C \in \mathbb{N}$ such that for any open normal subgroups H and K of G either $|H : H \cap K| \leq C$ or $|K : H \cap K| \leq C$. It is clear that narrow groups are rigid. The converse is not true in general: for instance, if G is any (infinite) rigid group and A is a non-trivial finite group, then $G \times A$ is rigid, but not narrow; however, we do not know any example of a rigid group which does not contain an open narrow subgroup. It is also easy to see that Proposition 2.3 and Corollary 2.6 still hold if narrowness is replaced by rigidity, but it is not clear whether the same is true for Proposition 2.5.

Finally, we remark that various finiteness conditions on the normal subgroup structure in pro-p groups are investigated in detail in [BGJMS]. In particular, according to [BGJMS, Theorem 20], a pro-p group G is rigid (in the sense of [Er]) if and only if G has constant normal subgroup growth.

3. Some subgroups of $\mathcal{N}(\mathbb{F}_p)$ and their Lie algebras

We start by recalling some basic terminology and facts about the Nottingham group. For details the reader is referred to [Ca] and [Er].

For the rest of the paper we fix a prime $p \geq 5$ and write $\mathcal{N} = \mathcal{N}(\mathbb{F}_p)$. We will think of elements of $\mathcal{N}$ as power series $\{t(1 + a_1 t + a_2 t^2 + \ldots) \mid a_i \in \mathbb{F}_p\}$ under substitution (and not as ring automorphisms of $\mathbb{F}_p[[t]]$). Let $\{\mathcal{N}_n\}$ be the congruence filtration of $\mathcal{N}$, that is, $\mathcal{N}_n = \{t(1 + a_n t^n + a_{n+1} t^{n+1} + \ldots)\}$. Given $g \in \mathcal{N} \backslash \{1\}$, the unique n such that $g \in \mathcal{N}_n \backslash \mathcal{N}_{n+1}$ is called the *degree* of g and denoted by $\deg(g)$. If $\deg(g) = n$, the coset $g\mathcal{N}_{n+1} \in \mathcal{N}_n/\mathcal{N}_{n+1}$ will be called the *leading term of g* and denoted by $\mathrm{LT}(g)$.

We shall use two simple properties of the degree function on $\mathcal{N}$ (see [Ca]):

Lemma 3.1. *The following hold:*

(i) $\deg((f,g)) \geq \deg(f) + \deg(g)$ *for any* $f, g \in \mathcal{N}$*, and equality holds if and only if* $\deg(f) \not\equiv_p \deg(g)$*;*
(ii) $\deg(f^p) \geq p \cdot \deg(f)$ *for any* $f \in \mathcal{N}$*, and equality holds if and only if* $p \mid \deg(f)$*.*

The inequality in Lemma 3.1(i) implies that $(\mathcal{N}_i, \mathcal{N}_j) \subseteq \mathcal{N}_{i+j}$, and thus we can consider the graded Lie algebra of $\mathcal{N}$ with respect to the congruence filtration $L(\mathcal{N}) = \bigoplus_{n=1}^{\infty} \mathcal{N}_n/\mathcal{N}_{n+1}$ with bracket defined by $[g\mathcal{N}_{i+1}, h\mathcal{N}_{j+1}] = (g,h)\mathcal{N}_{i+j+1}$ for $g \in \mathcal{N}_i$ and $h \in \mathcal{N}_j$. It is well known that $L(\mathcal{N}) = \bigoplus_{n=1}^{\infty} \mathbb{F}_p e_n$ where $e_i = \mathrm{LT}(t(1+t^i))$ and $[e_i, e_j] = (j-i)e_{i+j}$. Given a subgroup G of $\mathcal{N}$, we let $L(G)$ be the Lie subalgebra of $L(\mathcal{N})$ corresponding to G, that is, $L(G) = \bigoplus_{n=1}^{\infty} (G \cap \mathcal{N}_n)/(G \cap \mathcal{N}_{n+1})$.

Definition. Let G be a subgroup of $\mathcal{N}$. The set of possible degrees of elements of G will be called the *index set* of G and denoted by $\mathrm{Ind}(G)$.

The following result is straightforward:

Proposition 3.2. *Let* G *be a subgroup of* $\mathcal{N}$*.*

(a) *The density function* $d_{G,\mathcal{N}}(n)$ *(with respect to the congruence filtration) is given by the formula*

$$d_{G,\mathcal{N}}(n) = \frac{\mathrm{card}\,(\mathrm{Ind}\,(G) \cap \{1, 2, \ldots, n-1\})}{n-1}.$$

In particular, the Hausdorff dimension of G *in* $\mathcal{N}$ *is equal to the lower density of its index set.*

(b) $L(G) = \bigoplus_{i \in \mathrm{Ind}\,(G)} \mathbb{F}_p e_i$.

By complete analogy with groups, one can define Hausdorff dimension for subalgebras of any $\mathbb{N}$-graded Lie algebra with finite homogeneous components. We will use this notion for Lie subalgebras of $L(\mathcal{N})$. It is easy to see that any subalgebra $\mathfrak{g}$ of $L(\mathcal{N})$ has the form $\mathfrak{g} = \bigoplus_{i \in I} \mathbb{F}_p e_i$ for some subset I of $\mathcal{N}$, and the Hausdorff dimension of $\mathfrak{g}$ (which we will denote by $\mathrm{Hdim}\,\mathfrak{g}$) is equal to the lower density of I. In particular, $\dim_{\mathcal{N}}(G) = \mathrm{Hdim}\,L(G)$ for any subgroup G of $\mathcal{N}$.

Proposition 3.3. *Open subgroups of* $\mathcal{N}$ *are narrow (provided* $p > 2$*).*

Proof. Fix an open subgroup G of $\mathcal{N}$ and put $G_n = G \cap \mathcal{N}_n$ for $n \in \mathbb{N}$. Clearly, $\{G_n\}$ is a finite width filtration of G. Choose $N \in \mathbb{N}$ such that $\mathcal{N}_N \subseteq G$. We will show that any open normal subgroup H of G lies between G_{m+2N+2} and G_m for some $m \in \mathbb{N}$.

Let H be open and normal in G and let $m \in \mathbb{N}$ be the largest integer such that $H \subseteq G_m$. We claim that $L(H) \supseteq \bigoplus_{n=m+2N+2}^{\infty} \mathbb{F}_p e_n$; this would imply that $H \supseteq \mathcal{N}_{m+2N+2} = G_{m+2N+2}$ and finish the proof.

Since $H \subseteq G_m$ but $H \not\subseteq G_{m+1}$, there exists $h \in H$ with $\deg(h) = m$. Raising h to suitable power, we can assume that $\mathrm{LT}(h) = e_m$. Now take any $n \geq m + 2N + 2$.

If $n \not\equiv_p 2m$, choose $g \in G$ with $\mathrm{LT}(g) = e_{n-m}$ (such g exists since $n - m \geq N$). Then $\deg((g,h)) = \deg(g) + \deg(h) = n$ by Lemma 3.1(i), whence $\mathrm{LT}((g,h)) = [\mathrm{LT}(g), \mathrm{LT}(h)] = (n-2m)e_n$, and thus $e_n \in L(H)$.

If $n \equiv_p 2m$, let $k \in \{N, N+1, N+2\}$ be such that $k \not\equiv_p 0, m$, and choose $g, g_0 \in G$ with $\mathrm{LT}(g_0) = e_k$ and $\mathrm{LT}(g) = e_{n-m-k}$. Similarly to the first case we get $\deg(((h, g_0), g)) = n$ since $k \not\equiv_p m$ and $n - m - k \not\equiv_p (m + k)$. Thus, $e_n \in L(H)$ in this case as well. □

We can now apply Proposition 2.5 and Corollary 2.6 to $G = \mathcal{N}$. We shall reformulate Proposition 2.5 in this case since this result will be particularly useful.

Proposition 3.4. *Let φ be a virtual automorphism of $\mathcal{N}$, and let $N \in \mathbb{N}$ be such that both the domain and the image of φ contain $\mathcal{N}_N$. There exists $e \in \mathbb{N}$ such that $\deg(g) - e \leq \deg(\varphi(g)) \leq \deg(g) + e$ for all $g \in \mathcal{N}_{N+e}$.*

Now we introduce three important families of subgroups of $\mathcal{N}$.

1. Family $\{\mathcal{A}(s), s \in \mathbb{N}\}$.
   Description: $\mathcal{A}(s) := \{t(1 + a_1 t^s + a_2 t^{2s} + \ldots) \mid a_i \in \mathbb{F}_p\}$.
   Index set: $n \in \mathrm{Ind}(\mathcal{A}(s)) \iff s \mid n$.
   Lie algebra: $L(\mathcal{A}(s))$ will be denoted by $\mathfrak{a}(s)$.
2. Family $\{\mathcal{Q}(r), 0 < r < p/2\}$.
   Description:

$$\mathcal{Q}(r) := \left\{ \sqrt[r]{\frac{a^p t^r + b^p}{c^p t^r + d^p}} \;\middle|\; a, b, c, d \in \mathbb{F}_p[[t]]; \right.$$
$$\left. a - 1 \equiv d - 1 \equiv b \equiv 0 \mod t\mathbb{F}_p[[t]] \right\}.$$

   Index set: $n \in \mathrm{Ind}(\mathcal{Q}(r)) \iff n \equiv_p 0, \pm r$.
   Lie algebra: $L(\mathcal{Q}(r))$ will be denoted by $\mathfrak{q}(r)$.
3. Family $\{\mathcal{B}(r), 0 < r < p\}$.
   Description:

$$\mathcal{B}(r) := \left\{ \sqrt[r]{a^p t^r + b^p} \;\middle|\; a, b \in \mathbb{F}_p[[t]]; a - 1 \equiv b \equiv 0 \mod t\mathbb{F}_p[[t]] \right\}.$$

   Index set: $n \in \mathrm{Ind}(\mathcal{B}(r)) \iff n \equiv_p 0, -r$.
   Lie algebra: $L(\mathcal{B}(r))$ will be denoted by $\mathfrak{b}(r)$.

The following facts are easy to show:

(a) (see [Ca]): $\mathcal{A}(n) \cong \mathcal{N}$ when $p \nmid n$, and $\mathcal{A}(n)$ is torsion-free when $p \mid n$.

(b) (see [Er]): For any $0 < r < p/2$ the group $\mathcal{Q}(r)$ contains both $\mathcal{B}(r)$ and $\mathcal{B}(p - r)$; furthermore, $\mathcal{B}(r) \cap \mathcal{B}(p - r) = \mathcal{A}(p)$.

Next we state a series of results which help us control the behavior of the subgroups $\mathcal{A}(s)$, $\mathcal{B}(r)$ and $\mathcal{Q}(r)$ under virtual automorphisms of $\mathcal{N}$.

The first result describes all subgroups H of $\mathcal{N}$ such that $L(H) = \mathfrak{q}(r)$ for some r or $L(H) = \mathfrak{a}(s)$, with $p \nmid s$. In fact, we will need a stronger statement.

Theorem 3.5. *Let $K = \mathcal{Q}(r)$ for some r or $K = \mathcal{A}(s)$, where $p \nmid s$. If H is a subgroup of $\mathcal{N}$ such that $L(H)$ is a finite index subalgebra of $L(K)$, then H is conjugate to a finite index subgroup of K.*

Our statement about the family $\mathcal{B}$ is slightly weaker:

Theorem 3.6. *Let $\mathcal{Q} = \mathcal{Q}(r)$ for some r and let $\mathcal{B}$ be either $\mathcal{B}(r)$ or $\mathcal{B}(p - r)$. If H is a subgroup of $\mathcal{Q}$ such that $L(H)$ is a finite index subalgebra of $L(\mathcal{B})$, then H is conjugate (in $\mathcal{Q}$) to a finite index subgroup of $\mathcal{B}$.*

Theorem 3.6 was already established in the course of the proof of [Er, Proposition 8.1]. Theorem 3.5 will be proved in the next section using the same method.

Another ingredient we will need is a "characterization" of the Lie subalgebras $\{\mathfrak{q}(r)\}$ and $\{\mathfrak{a}(s) \mid s \text{ is a prime}\}$. Such a characterization is an easy consequence of the work of Barnea, Shalev and Zelmanov [BShZ] who classified the so-called weakly maximal graded subalgebras of twisted loop algebras. Following [BShZ], we call a graded subalgebra $\mathfrak{h}$ of an $\mathbb{N}$-graded Lie algebra $\mathfrak{g}$ (over some field) *weakly maximal,* if $\mathfrak{h}$ is of infinite codimension in $\mathfrak{g}$, but any graded subalgebra strictly containing $\mathfrak{h}$ is of finite codimension in $\mathfrak{g}$.

The main theorem of [BShZ] applied to the Lie algebra $L(\mathcal{N})$ asserts the following:

Theorem 3.7. *Let $\mathfrak{g}$ be a weakly maximal subalgebra of $L(\mathcal{N})$. Then either $\mathfrak{g} = \mathfrak{q}(r)$ for some r or $\mathfrak{g} = \mathfrak{a}(s)$ for prime s.*

Slightly more elaborate application of the results of [BShZ] (using an idea from [BSh]) yields a "partial classification" of subalgebras of $L(\mathcal{N})$:

Proposition 3.8. *Let $\mathfrak{h}$ be a graded Lie subalgebra of $L(\mathcal{N})$. Then $\mathfrak{h}$ has one of the following types:*

- (A) *$\mathfrak{h}$ is a finite index subalgebra of $\mathfrak{a}(n)$ for some $n \in \mathbb{N}$, with $p \nmid n$. In this case* $\operatorname{Hdim} \mathfrak{h} = 1/n$.
- (Q) *$\mathfrak{h}$ is a finite index subalgebra of $\mathfrak{q}(r)$ for some r. In this case* $\operatorname{Hdim} \mathfrak{h} = 3/p$.
- (R) *$\mathfrak{h}$ is not solvable, and* $\operatorname{Hdim} \mathfrak{h} = \dfrac{3}{pn}$ *for some $n > 1$.*
- (B) *$\mathfrak{h}$ is solvable, and $\mathfrak{h} \subseteq \mathfrak{b}(r)$ for some r. In this case* $\operatorname{Hdim} \mathfrak{h} \leq 2/p$.

4. Proof of Theorem 3.5

Definition. Let $G \subseteq G_0$ be subgroups of $\mathcal{N}$. We will say that the pair (G_0, G) is *undeformable*, if any subgroup H of G_0 such that $L(H) = L(G)$ is conjugate to G in G_0.

Theorems 3.5 and 3.6 can be reformulated as the statements of undeformability of certain pairs of subgroups (where in Theorem 3.5 we take $G_0 = \mathcal{N}$ and in Theorem 3.6 we take $G_0 = \mathcal{Q}(r)$). We now describe an approach to proving undeformability introduced in [Er, Section 8].

Definition. Let G be a subgroup of $\mathcal{N}$, let $f \in \mathcal{N}$ and $n = \deg(f)$. The largest integer m such that $f \in G\mathcal{N}_{n+m}$ will be called the depth of f with respect to G and denoted by $\operatorname{dep}(f, G)$. If $f \in G\mathcal{N}_{n+m}$ for all m, we set $\operatorname{dep}(f, G) = \infty$.

It is clear that $\operatorname{dep}(f, G) = \infty$ if and only if $f \in G$ and $\operatorname{dep}(f, G) = 0$ if and only if $\operatorname{LT}(f) \notin L(G)$. More generally, we have the following:

Lemma 4.1. *Let G be a subgroup of $\mathcal{N}$, $f \in \mathcal{N}$, let $n = \deg(f)$ and $m = \operatorname{dep}(f, G)$. Assume that $m < \infty$. Then $n + m \notin \operatorname{Ind}(G)$.*

Proof. By assumption, $f = gs$ where $g \in G$ and $s \in \mathcal{N}_{n+m}$. Suppose that $n + m \in \operatorname{Ind}(G)$. Then there exists $g_1 \in G$ such that $g_1^{-1}s \in \mathcal{N}_{n+m+1}$ (since the quotient $\mathcal{N}_{n+m}/\mathcal{N}_{n+m+1}$ is cyclic of prime order). Thus we can write $f = (gg_1)(g_1^{-1}s) \in G\mathcal{N}_{n+m+1}$, which contradicts the definition of m. □

Any element $f \in \mathcal{N}$ can be written in the form $f = g \cdot s$ where $g \in G$ and $\deg(s) = \deg(f) + \operatorname{dep}(f, G)$. Such a factorization will be referred to as a *standard decomposition* of f with respect to G. While it is not unique, the leading term of s is independent of the choice of decomposition. Indeed, suppose that $f = g_1 s_1 = g_2 s_2$ with $g_1, g_2 \in G$ and $\deg(s_i) = \deg(f) + \operatorname{dep}(f, G)$. Since $s_1 s_2^{-1} = g_1^{-1} g_2 \in G$, we have $\deg(s_1 s_2^{-1}) \neq \deg(f) + \operatorname{dep}(f, G)$ by Lemma 4.1. Thus, $\deg(s_1 s_2^{-1}) > \deg(s_1) = \deg(s_2)$, whence $\operatorname{LT}(s_1) = \operatorname{LT}(s_2)$.

Similarly, if $f = gs$ is a standard decomposition of f with respect to G, then $\operatorname{LT}(s) \notin L(G)$ unless $f \in G$ (in which case $s = 1$).

From now on we fix a subgroup G of $\mathcal{N}$ and let $I = \operatorname{Ind}(G)$. Let H be another subgroup of $\mathcal{N}$ such that $\operatorname{Ind}(H) = \operatorname{Ind}(G) = I$, and define

$$m = m(H, G) := \min_{h \in H} \operatorname{dep}(h, G). \tag{4.1}$$

Note that $0 < m < \infty$ since $L(H) = L(G)$ but $H \neq G$.

Given $h \in H$, let gs be its standard decomposition. Let $n = \deg(h) = \deg(g)$. Let $\alpha, \beta \in \mathbb{F}_p$ be such that $g \equiv t(1 + \alpha t^n) \mod \mathcal{N}_{n+1}$ and $s \equiv t(1 + \beta t^{n+m}) \mod \mathcal{N}_{n+m+1}$. Note that either $\operatorname{dep}(h, G) = m$ and $\operatorname{LT}(s) = \beta e_{n+m}$ or $\operatorname{dep}(h, G) > m$ and $\beta = 0$. Since $\operatorname{LT}(h) = \operatorname{LT}(g) = \alpha e_n$, we see that both α and β are independent of the choice of the standard decomposition, so we can write $\alpha = \alpha(h)$, $\beta = \beta(h)$. In [Er, p.446], it is shown that the ratio β/α depends only on $n = \deg(h)$:

Lemma 4.2. *Recall that $I = \operatorname{Ind}(G) = \operatorname{Ind}(H)$. There exists a function $\lambda : I \to \mathbb{F}_p$ such that $\dfrac{\beta(h)}{\alpha(h)} = \lambda(\deg(h))$ for all $h \in H$.*

Note that $\lambda \neq 0$ as a function.

Assume next that G and H both lie in some subgroup G_0 of $\mathcal{N}$, and let $I_0 = \operatorname{Ind}(G_0)$. The following result is [Er, Lemma 9.4].

Lemma 4.3. *Let $i, j \in I$. The following hold:*

(a) *If $i + m \in I$ or $i + m \notin I_0$, then $\lambda(i) = 0$.*
(b) *If $i + j + m \notin I$, then*

$$(j - i)(\lambda(i + j) - \lambda(i) - \lambda(j)) = m(\lambda(j) - \lambda(i)). \tag{4.2}$$

Remark. If $i + j \notin I$, we define $\lambda(i + j)$ to be any number. Note that the assumption $i + j \notin I$ implies that $[e_i, e_j] = 0$, i.e. $j - i \equiv_p 0$, so our choice does not affect the value of the left hand side of (4.2).

Suppose now that we want to prove that H is conjugate to G in G_0. Let $M = \sup_{g \in G_0} m(H^g, G)$ where $m(\cdot, \cdot)$ is defined by (4.1). If $M = \infty$, by compactness of G_0 there is a sequence $\{g_n\}$ in G_0 converging to some $g_\infty \in G_0$ such that $m(H^{g_n}, G) \to \infty$ as $n \to \infty$. Then it is easy to see that $m(H^{g_\infty}, G) = \infty$, and it follows that $H^{g_\infty} = G$, so H is conjugate to G in G_0. If $M < \infty$, then replacing H by a suitable conjugate we can assume that $m(H, G) \geq m(H^g, G)$ for any $g \in G_0$; we will call such H *optimal.*

Lemma 4.4. *Let H be optimal and $m = m(H, G)$. Suppose that $m \in I_0$, and fix $i \in I$ such that $i \not\equiv_p m$. Then after replacing H by a suitable conjugate which is also optimal, we can assume that $\lambda(i) = 0$.*

Proof. We assume that $\lambda(i) \neq 0$ (otherwise there is nothing to prove). Let $h \in H$ be any element of degree i, and let gs be a standard decomposition of h with respect to G. Then $\mathrm{LT}(h) = \mathrm{LT}(g) = \alpha e_i$ and $\mathrm{LT}(s) = \beta e_{i+m}$, where $\beta/\alpha = \lambda(i)$.

Next choose $k \in G_0$ such that $\mathrm{LT}(k) = \frac{\lambda(i)}{m-i} e_m$ (this is possible since $m \in I_0$). Then $\mathrm{LT}((h,k)) = [\mathrm{LT}(h), \mathrm{LT}(k)] = (i-m)\alpha\frac{\lambda(i)}{m-i} e_{i+m} = -\mathrm{LT}(s)$, whence $(h,k) = s^{-1}w$ for some $w \in \mathcal{N}_{i+m+1}$. We have $h^k = h(h,k) = gw \in G\mathcal{N}_{i+m+1}$, so $\mathrm{dep}(h^k, G) \geq m+1$.

We claim that the subgroup H^k has the desired properties. Indeed, $m \geq m(H^k, G) \geq \min\{m(H,G), \deg(k)\} = m$, so H^k is also optimal. Since H^k contains the element h^k, for which $\deg(h^k) = i$ and $\mathrm{dep}(h^k, G) \geq m+1$, the λ-function of H^k vanishes at i. □

One can now try to prove that the pair (G_0, G) is undeformable as follows. Assume the contrary; then, by the above discussion there exists a subgroup $H \subset G_0$ such that $H \neq G$, $L(H) = L(G)$ and H is optimal. The objective is to use Lemmas 4.4 and 4.3 to construct a conjugate of H whose λ-function is identically zero. This will contradict our assumptions and imply that H is in fact conjugate to G in G_0.

Proof of Theorem 3.5. Let K be as in the statement of Theorem 3.5. We claim that to prove the theorem it suffices to show that for any $N \in \mathbb{N}$ the pair $(\mathcal{N}, K \cap \mathcal{N}_N)$ is undeformable. Indeed, suppose the latter is established. Let H be as in the statement of Theorem 3.5, that is, suppose that $L(H)$ is of finite index in $L(K)$. Then there exists $N \in \mathbb{N}$ such that $L(H \cap \mathcal{N}_N) = L(K \cap \mathcal{N}_N)$. Since the pair $(\mathcal{N}, K \cap \mathcal{N}_N)$ is undeformable, $H \cap \mathcal{N}_N$ is conjugate to $K \cap \mathcal{N}_N$. Since H normalizes $H \cap \mathcal{N}_N$, H is conjugate to a subgroup of the normalizer of $K \cap \mathcal{N}_N$. But the normalizer of $K \cap \mathcal{N}_N$ must be equal to K. Indeed, it clearly contains K; on the other hand, any subgroup of $\mathcal{N}$ strictly containing K is open by Theorem 3.7. Thus, it remains to prove that the above mentioned pairs are undeformable.

In both parts below (G_0, G) denotes a pair whose undeformability we are trying to prove. Recall that $I_0 = \mathrm{Ind}(G_0)$ and $I = \mathrm{Ind}(G)$. We show that any function $\lambda : I \to \mathbb{F}_p$ satisfying the conclusions of Lemmas 4.3 and 4.4 must be identically zero.

Part 1: $G_0 = \mathcal{N}$ and $G = \mathcal{A}(s) \cap \mathcal{N}_N$, with $p \nmid s$, $N \in \mathbb{N}$. We have $I_0 = \mathbb{N}$ and $I = \{n \in \mathbb{N} \mid n \geq N \text{ and } s \mid n\}$.

First of all, note that if $s \mid m$, then λ is identically zero by Lemma 4.3(a). So, we can assume that $s \nmid m$, in which case Lemma 4.3(b) implies that (4.2) holds for all $i, j \in I$.

Case 1. $p \mid m$. It follows from (4.2) that $\lambda(i+j) = \lambda(i) + \lambda(j)$ whenever $i \not\equiv_p j$. Since $p \geq 5$, it is easy to deduce that $\lambda(i+j) = \lambda(i) + \lambda(j)$ for all $i, j \in I$ and hence there exists a constant c such that $\lambda(i) = ci$ for all $i \in I$. Now fix any $j \in I$ with $p \nmid j$. By Lemma 4.4, we can assume that $\lambda(j) = 0$, so we must have $c = 0$ and hence $\lambda(i) = 0$ for all i.

Case 2. $p \nmid m$. This time an immediate consequence of (4.2) is that $\lambda(i)$ depends only on i mod p, so we can consider λ as a function from $\mathbb{F}_p$ to $\mathbb{F}_p$.

Applying (4.2) with $p \mid i$ and arbitrary j, we get $-j\lambda(0) = m(\lambda(j) - \lambda(0))$, whence $\lambda(j) = \frac{m-j}{m}\lambda(0)$. Since $p \nmid m$, by Lemma 4.4 we can assume that $\lambda(0) = 0$, whence $\lambda(j) = 0$ for all j.

Part 2: $G_0 = \mathcal{N}$ and $G = \mathcal{Q}(r) \cap \mathcal{N}_N$, with $0 < r < p/2$, $N \in \mathbb{N}$. We have $I_0 = \mathbb{N}$ and $I = \{n \in \mathbb{N} \mid n \geq N \text{ and } n \equiv_p 0, \pm r\}$.

First of all, note that if $p \mid m$, then $\lambda = 0$ by Lemma 4.3(a). So, from now on we assume that $p \nmid m$. By Lemma 4.4, we can also assume that $\lambda(i_0) = 0$ for some fixed $i_0 \in I$ divisible by p (the particular choice of i_0 is not important).

Case 1. $m \not\equiv_p 0, \pm r \pm 2r \pm 3r$. In this case (4.2) holds for all $i, j \in I$, and we can argue exactly as in Case 2 of Part 1.

By symmetry, it suffices to consider the cases $m \equiv_p r, 2r$ or $3r$.

Case 2. $m \equiv_p r$. By Lemma 4.3(a), $\lambda(i) = 0$ for $i \equiv_p 0, -r$. Now take any $i \equiv_p 0$ and $j \equiv_p r$. Since $i + j + m \equiv_p 2r \notin I$, we can apply (4.2) to the pair (i, j). We get $r(\lambda(i + j) - \lambda(j)) = r\lambda(j)$, whence $\lambda(i + j) = 2\lambda(j)$. Applying the same argument to the pairs $(2i, j)$ and $(i, i + j)$, we have $2\lambda(j) = \lambda(2i + j) = 2\lambda(i + j) = 4\lambda(j)$, whence $\lambda(j) = 0$. So, λ is identically zero.

Case 3. $m \equiv_p 2r$. By Lemma 4.3(a), $\lambda(i) = 0$ for $i \equiv_p -r$. Equation (4.2) implies that $\lambda(i)$ is the same for all $i \equiv_p 0$. Since we assume that $\lambda(i_0) = 0$ for some $i_0 \equiv_p 0$, it follows that $\lambda(i) = 0$ for all $i \equiv_p 0$. Finally, applying (4.2) with any $i \equiv_p -r$ and $j \equiv_p r$, we get $-2r\lambda(j) = 2r\lambda(j)$, so $\lambda(j) = 0$.

Case 4. $m \equiv_p 3r$. We can assume that $p \neq 5$, since for $p = 5$ we have $3r \equiv_p -2r$, and the situation is "symmetric" to Case 3.

As before, we conclude that $\lambda(i)$ depends on i modulo p for $i \equiv_p 0, r$ (for $p = 5$ we could not apply (4.2) to the pair (i, j) when $i \equiv j \equiv_p r$). As in Case 3, we can assume that $\lambda(i) = 0$ for all $i \equiv_p 0$. Applying (4.2) with $j \equiv_p r$ and $i \equiv_p 0$, we get $0 = 3r\lambda(j)$, whence $\lambda(j) = 0$. Finally, applying (4.2) with $j \equiv_p r$ and $i \equiv_p -r$ (and taking the last result into account), we get $-2r\lambda(i) = -3r\lambda(i)$, whence $\lambda(i) = 0$. The proof is complete. □

5. Proof of Theorem 1.2

We start by introducing an equivalence relation on the set of virtual automorphisms of $\mathcal{N}$.

Definition. Let ψ_1 and ψ_2 be two virtual automorphisms of $\mathcal{N}$. We will say that ψ_1 and ψ_2 are *tame modifications of each other* if there exist $h, k \in \mathrm{Aut}\,(\mathbb{F}_p[[t]])$ and $n \in \mathbb{N}$ such that $\psi(g) = h^{-1}\varphi(k^{-1}gk)h$ for all $g \in \mathcal{N}_n$.

From now on we fix a virtual automorphism φ of $\mathcal{N}$. We shall show that the set of tame modifications of φ contains the identity automorphism, which is equivalent to the statement of Theorem 1.2. Here is the main technical result of this section:

Proposition 5.1. *There exists a tame modification ψ of φ and $M \in \mathbb{N}$ with the following property: for every prime $s > M$ there exists $h = h(s) \in \mathrm{Aut}\,(\mathbb{F}_p[[t]])$ such that $\psi(g) = g^h$ for all $g \in \mathcal{A}(s)$.*

First we will deduce Theorem 1.2 from Proposition 5.1. Let M be as above and choose primes $s_1, s_2 > M$. Then there exist $h_1, h_2 \in \mathrm{Aut}\,(\mathbb{F}_p[[t]])$ such that $\psi(g) = g^{h_i}$ for all $g \in \mathcal{A}(s_i)$, $i = 1, 2$. Note that $g^{h_1} = g^{h_2}$ for all $g \in \mathcal{A}(s_1) \cap \mathcal{A}(s_2) = \mathcal{A}(s_1 s_2)$. Since the centralizer of $\mathcal{A}(s_1 s_2)$ in $\mathrm{Aut}\,(\mathbb{F}_p[[t]])$ is trivial, it follows that $h_1 = h_2$. Therefore, replacing ψ by a tame modification, we can assume that ψ fixes pointwise both $\mathcal{A}(s_1)$ and $\mathcal{A}(s_2)$. The subgroup $\langle \mathcal{A}(s_1), \mathcal{A}(s_2) \rangle$ generated by $\mathcal{A}(s_1)$

and $\mathcal{A}(s_2)$ is open in $\mathcal{N}$ – if that was not the case, the Lie algebra $L(\langle \mathcal{A}(s_1), \mathcal{A}(s_2)\rangle)$ would have been contained in some weakly maximal subalgebra of $L(\mathcal{N})$, which contradicts Theorem 3.7. Thus, ψ fixes pointwise an open subgroup of $\mathcal{N}$ and hence ψ represents 1 in $\mathrm{Comm}(\mathcal{N})$.

The rest of this section is devoted to the proof of Proposition 5.1.

Let G be the domain of φ. Let N and e be as in the conclusion of Proposition 3.4 applied to φ, and let $M = \max\{N + e, p\}$. Let $s > M$ be any prime number (note that $\mathcal{A}(s) \subseteq G$ since $G \supseteq \mathcal{N}_M$), and let $g \in \mathcal{N}$. Let $A_1(s, g) = \varphi(\mathcal{A}(s)^g)$ and $\mathfrak{a}_1(s, g) = L(A_1(s, g))$. We know that $A_1(s, g)$ has Hausdorff dimension $1/s$ and so does its Lie algebra $\mathfrak{a}_1(s, g)$.

Now recall the classification of Lie subalgebras of $L(\mathcal{N})$ given in Proposition 3.8. Clearly, $\mathfrak{a}_1(s, g)$ cannot be of type (Q) or (R) for any g and s. We shall show (see Claim 5.2 below) that there exists g such that $\mathfrak{a}_1(s, g)$ is of type (A) for any prime $s > M$. Then from Proposition 3.4 it is clear that $\mathfrak{a}_1(s, g) = \mathfrak{a}(s)$, whence $A_1(s, g)$ is conjugate to $\mathcal{A}(s)$ by Theorem 3.5.

So, for each prime $s > M$ we have $\varphi(\mathcal{A}(s)^g) = \mathcal{A}(s)^{h(s)}$ for some $h(s) \in \mathcal{N}$. Now let $\psi : G^{g^{-1}} \to \mathcal{N}$ be defined by $\psi(x) = \varphi(x^g)$. Then ψ is a tame modification of φ, and $\psi(\mathcal{A}(s)) = \mathcal{A}(s)^{h(s)}$. Since $\mathcal{A}(n) \cong \mathcal{N}$ when $p \nmid n$, any automorphism of $\mathcal{A}(s)$ is a conjugation by an element of $\mathrm{Aut}\,(\mathbb{F}_p[[t]])$. The assertion of Proposition 5.1 now follows easily.

Thus, it remains to establish Claim 5.2. Its proof will be based on properties of the groups $\{\mathcal{Q}(r)\}$.

Claim 5.2. There exists $g \in G$ such that for every prime $s > M$, the Lie algebra of $\varphi(\mathcal{A}(s)^g)$ is not of type (B).

The following result announced in [Er] is a direct consequence of Theorem 3.5 and Proposition 3.8.

Theorem 5.3. *Any subgroup of $\mathcal{N}$ of Hausdorff dimension $3/p$ is conjugate to an open subgroup of $\mathcal{Q}(r)$ for some $r = 1, \dots, (p-1)/2$.*

We shall analyze the image of $\mathcal{Q}(1) \cap G$ under φ. Since φ preserves Hausdorff dimension, it follows that $\varphi(\mathcal{Q}(1) \cap G)$ is conjugate to an open subgroup of $\mathcal{Q}(r_0)$ for some r_0. Replacing φ by a tame modification, we can assume that $\varphi(\mathcal{Q}(1) \cap G)$ is equal to an open subgroup of $\mathcal{Q}(r_0)$.

The following is a corrected [3] version of [Er, Proposition 8.1].

Proposition 5.4. *Let $\mathcal{Q} = \mathcal{Q}(r)$ for some $r = 1, \dots, (p-1)/2$. Then any subgroup of $\mathcal{Q}$ of strong Hausdorff dimension $2/3$ (as a subgroup of $\mathcal{Q}$)[4] is conjugate in $\mathcal{Q}$ to an open subgroup of $\mathcal{B}(r)$ or $\mathcal{B}(p-r)$.*

Let us introduce special names for some subgroups of $\mathcal{Q}(1)$. We set $B_+ = \mathcal{B}(1) \cap \mathcal{N}_N$, $B_- = \mathcal{B}(p-1) \cap \mathcal{N}_N$ and $T = \mathcal{A}(p) \cap \mathcal{N}_N = B_+ \cap B_-$.

Given $g \in \mathcal{Q}(1)$, let $K_+(g) = \varphi(B_+^g)$ and $K_-(g) = \varphi(B_-^g)$. Since $K_+(g)$ and $K_-(g)$ are subgroups of $\mathcal{Q}(r_0)$ of strong dimension $2/3$, Proposition 4 implies that there exist $r_+(g), r_-(g) \in \{r_0, p - r_0\}$ such that

$K_+(g)$ is conjugate in $\mathcal{Q}(r_0)$ to an open subgroup of $\mathcal{B}(r_+(g))$;
$K_-(g)$ is conjugate in $\mathcal{Q}(r_0)$ to an open subgroup of $\mathcal{B}(r_-(g))$.

[3] For more on this issue, see Appendix.

[4] Of course, such subgroup has strong Hausdorff dimension $2/p$ in $\mathcal{N}$.

A priori, it is possible that $r_+(g) = r_-(g)$ for some g (or even all g). First we show that if the latter happens for some g, the subgroup T^g has rather "unexpected" image under φ:

Lemma 5.5. *Let $g \in \mathcal{Q}(1)$ be such that $r_+(g) = r_-(g)$. Then for any $h \in T$ we have $\deg(\varphi(h^g)) \equiv_p -r_+(g)$.*

Proof. Let $r = r_+(g) = r_-(g)$ and let $B_0 = \mathcal{B}(r)$. By definition, there exist $x, y \in \mathcal{Q}(r_0)$ such that $\varphi(B_+^g)$ is open in B_0^x and $\varphi(B_-^g)$ is open in B_0^y. Therefore, $\varphi(T^g) = \varphi(B_+^g \cap B_-^g) \subseteq B_0^x \cap B_0^y$. Let $z = yx^{-1}$. Then $B_0^x \cap B_0^y = (B_0 \cap B_0^z)^x$, and it suffices to prove that $\deg(u) \equiv_p -r$ for any $u \in B_0 \cap B_0^z$. In fact, we only need to show that $\deg(u) \not\equiv_p 0$ for any $u \in B_0 \cap B_0^z$ since $\mathrm{Ind}(B_0 \cap B_0^z) \subseteq \mathrm{Ind}(B_0) = \{n \in \mathbb{N} \mid n \equiv_p 0, -r\}$.

First, note that $z \notin B_0$ for otherwise B_0^x would be equal to B_0^y, which is impossible since B_+^g and B_-^g are not commensurable (as subgroups of $\mathcal{N}$). Now let $z_1 w$ be a standard decomposition of z with respect to B_0 so that $z_1 \in B_0$ and $\mathrm{LT}(w) \notin L(B_0) = \mathfrak{b}(r)$. Then $B_0^z = B_0^w$ and $B_0 \cap B_0^w = \{u \in B_0 \mid (u, w) \in B_0\}$. On the other hand, the condition $\mathrm{LT}(w) \notin \mathfrak{b}(r)$ implies that $\deg(w) \not\equiv_p 0, -r$. So, if $\deg(u) \equiv_p 0$, Lemma 3.1(i) yields $\deg((u, w)) = \deg(u) + \deg(w) \equiv_p \deg(w)$ and therefore $(u, w) \notin B_0$. □

Corollary 5.6. *There exists $g \in \mathcal{Q}(1)$ such that $r_+(g) \neq r_-(g)$.*

Proof. Assume the contrary: $r_+(g) = r_-(g)$ for all $g \in \mathcal{Q}(1)$. First we claim that there exist $g_1, g_2 \in \mathcal{Q}(1)$ such that $r_+(g_1) = r_0$ and $r_-(g_2) = p - r_0$.

Indeed, let $\widetilde{G} = \varphi(\mathcal{Q}(1) \cap G)$ which by assumption is an open subgroup of $\mathcal{Q}(r_0)$. Then $\varphi^{-1}(\mathcal{B}(r_0) \cap \widetilde{G})$ is a subgroup of $\mathcal{Q}(1)$ of strong dimension $2/3$, so by Proposition 4 there exists $g_1 \in \mathcal{Q}(1)$ such that $\varphi^{-1}(\mathcal{B}(r_0) \cap \widetilde{G})$ is commensurable with $B_+^{g_1}$ or $B_-^{g_1}$. Since we assume that $r_+(g_1) = r_-(g_1)$, we have $r_+(g_1) = r_0$. Similarly, $p - r_0 = r_+(g_2)$ for some $g_2 \in \mathcal{Q}(1)$.

Take any $h \in T$ and let $h_1 = h^{g_1}$, $h_2 = h^{g_2}$, $x_1 = \varphi(h_1)$ and $x_2 = \varphi(h_2)$. By Lemma 5.5, $\deg(x_1) \equiv_p -r_+(g_1) = -r_0$ and $\deg(x_2) \equiv_p r_0$. Of course, we also have $\deg(h_1) = \deg(h_2) = \deg(h) \equiv_p 0$.

We consider two cases. In the following computations we use Lemma 3.1.

Case 1. $\deg(x_1) < \deg(h)$ and $\deg(x_2) < \deg(h)$. For $n \in \mathbb{N}$, let $h(2n)$ be the left-normed commutator $\underbrace{(h_1, h_2, h_1, h_2, \ldots, h_1, h_2)}_{2n}$ of length $2n$ and let $x(2n) = \varphi(h(2n)) = \underbrace{(x_1, x_2, x_1, x_2, \ldots, x_1, x_2)}_{2n}$.

Since $\deg(x_1) \equiv_p -\deg(x_2) \not\equiv_p 0$, we have $\deg(x(2n)) = n(\deg(x_1) + \deg(x_2))$. On the other hand, $\deg(h(2n)) > 2n \deg(h)$. Hence $\deg(h(2n)) - \deg(\varphi(h(2n))) \to \infty$ as $n \to \infty$, which contradicts Proposition 3.4.

Case 2. $\deg(x_1) > \deg(h)$ or $\deg(x_2) > \deg(h)$. Without loss of generality, we assume that $\deg(x_1) > \deg(h)$. We have $\deg(h_1^{p^n}) = p^n \deg(h_1) = p^n \deg(h)$ since $p \mid \deg(h)$. Since $\deg(x_1^{p^n}) \geq p^n \deg(x_1)$, this time $\deg(h_1^{p^n}) - \deg(\varphi(h_1^{p^n})) \to -\infty$, and we reach a contradiction as above. □

Lemma 5.7. *Let $p \nmid s$ and $0 < r < p$. Then the group $\mathcal{A}(s) \cap \mathcal{B}(r) \cap \mathcal{N}_N$ contains an element of order p.*

Proof. It is easy to see that the element $f_k = \frac{t}{\sqrt[k]{1-t^k}}$ has order p whenever $p \nmid k$. Choose any $k \geq N$ such that $p \mid (k+r)$ and $s \mid k$. Then clearly $f_k \in \mathcal{A}(s) \cap \mathcal{N}_N$; on the other hand, $k = pm - r$ for some $m \geq 1$, whence

$$f_k = \frac{t}{\sqrt[pm-r]{1-t^{pm-r}}} = t\sqrt[r]{(1-t^{pm-r})^{1-\frac{pm}{pm-r}}}$$
$$= \sqrt[r]{(t^r - t^{pm})(1-t^{pm-r})^{-\frac{pm}{pm-r}}} = \sqrt[r]{a^p t^r + b^p},$$

where $a = (1-t^{pm-r})^{-\frac{m}{pm-r}}$ and $b = -t^m a$. Thus, $f_k \in \mathcal{B}(r)$. □

Now we are ready for the final step.

Proof of Claim 5.2. Let $g \in \mathcal{Q}(1)$ be such that $r_+(g) \neq r_-(g)$. Set $r_+ = r_+(g)$ and $r_- = r_-(g)$. We claim that the Lie algebra of the subgroup $\varphi(\mathcal{A}(s)^g)$ cannot be of type (B) for any prime $s > M$.

Recall that $K_+(g) = \varphi(B_+^g)$ and $K_-(g) = \varphi(B_-^g)$. Since $K_+(g)$ is conjugate to a subgroup of $\mathcal{B}(r_+)$, we have $\mathrm{Ind}\,(K_+(g)) \subseteq \mathrm{Ind}\,(\mathcal{B}(r_+))$, and similarly $\mathrm{Ind}\,(K_-(g)) \subseteq \mathrm{Ind}\,(\mathcal{B}(r_-))$. By Lemma 5.7, we can find elements g_- and g_+ of order p such that $g_+ \in \mathcal{A}(s)^g \cap B_+^g$ and $g_- \in \mathcal{A}(s)^g \cap B_-^g$. Let $n_+ = \deg(\varphi(g_+))$ and $n_- = \deg(\varphi(g_-))$. Since $n_+ \in \mathrm{Ind}\,(K_+(g))$, we must have $n_+ \equiv_p 0$ or $-r_+$. But if $n_+ \equiv_p 0$, then $\varphi(g_+)$ is torsion-free, which is impossible. Hence, $n_+ \equiv_p -r_+$ and similarly $n_- \equiv_p -r_-$. Therefore, the Lie algebra of $\varphi(\mathcal{A}(s)^g)$ cannot be contained in $\mathfrak{b}(r)$ for any r. □

6. Appendix

Recall the statement of Proposition 4 which, as we mentioned, is a corrected version of [Er, Proposition 8.1].

Proposition 4. *Let $\mathcal{Q} = \mathcal{Q}(r)$ for some $r = 1, \ldots, (p-1)/2$. Then any subgroup of $\mathcal{Q}$ of strong Hausdorff dimension $2/3$ is conjugate in $\mathcal{Q}$ to an open subgroup of $\mathcal{B}(r)$ or $\mathcal{B}(p-r)$.*

In [Er, Proposition 8.1], a slightly stronger (and probably false) assertion was made – in that paper a subgroup of $\mathcal{Q}$ was only assumed to have Hausdorff dimension $2/3$, not necessarily strong Hausdorff dimension $2/3$. However, looking at the proof, one sees that what is really established there is Proposition 4 above, and Theorem 3.6 is proved along the way. Below we reproduce the argument from [Er] showing how Proposition 4 follows from Theorem 3.6. We also remark that this inaccuracy does not affect the validity of any of the results from [Er] where Proposition 8.1 was used, and the proofs of those results remain virtually unchanged.

Proof of Proposition 4. Let G be a subgroup of $\mathcal{Q}$ of strong Hausdorff dimension $2/3$. Then $L(G)$ is a subalgebra of $L(\mathcal{Q})$ of strong Hausdorff dimension $2/3$. Since $L(\mathcal{Q})$ is commensurable with $\mathfrak{sl}_2(\mathbb{F}_p) \otimes t\mathbb{F}_p[t]$ (see [Er]), the results of [BShZ] imply the following: if $\mathfrak{g}$ is a weakly maximal subalgebra of $L(\mathcal{Q})$, then either $\mathrm{Hdim}_{L(\mathcal{Q})}\mathfrak{g} = 2/3$ and $\mathfrak{g} = \mathfrak{b}(r)$ or $\mathfrak{b}(p-r)$, or $\mathrm{Hdim}_{L(\mathcal{Q})}\mathfrak{g} \leq 1/2$. So, $L(G)$ must be contained in $\mathfrak{b}(r)$ or $\mathfrak{b}(p-r)$. Since $\mathfrak{b}(r)$ and $\mathfrak{b}(p-r)$ have strong dimension $2/3$ and so does $L(G)$, we conclude that $L(G)$ must be a finite index subalgebra of $\mathfrak{b}(r)$ or $\mathfrak{b}(p-r)$. Thus, the result follows from Theorem 3.6. □

Acknowledgements

The author is very grateful to Thomas Weigel for suggesting the problem, and to Yiftach Barnea and the anonymous referee for useful feedback on the earlier version of this paper.

References

[Ab] A. G. Abercrombie, *Subgroups and subrings of profinite rings*, Math. Proc. Cambridge Philos. Soc. 116 (1994), no. 2, 209–222. MR1281541 (95h:11078)

[AV] M. Abert and B. Virag, *Dimension and randomness in groups acting on rooted trees*, J. Amer. Math. Soc. 18 (2005), no. 1, 157–192. MR2114819 (2005m:20058)

[BEW] Y. Barnea, M. Ershov and T. Weigel, *Abstract commensurators of profinite groups*, to appear in Transactions of the AMS.

[BGJMS] Y. Barnea, N. Gavioli, A. Jaikin-Zapirain, V. Monti and C. M. Scoppola, *Pro-p groups with few normal subgroups*, J. Algebra 321 (2009), no. 2, 429–449. MR2483275

[BK] Y. Barnea and B. Klopsch, *Index subgroups of the Nottingham group*, Adv. Math. 180 (2003), 187-221. MR2019222 (2004m:20054)

[BSh] Y. Barnea and A. Shalev, *Hausdorff dimension, pro-p groups, and Kac-Moody algebras*, Trans. Amer. Math. Soc. 349 (1997), no. 12, 5073–5091. MR1422889 (98b:20041)

[BShZ] Y. Barnea, A. Shalev and E. I. Zelmanov, *Graded subalgebras of affine Kac-Moody algebras*, Israel J. Math. 104 (1998), 321–334. MR1622319 (99d:17025)

[Ca] R. Camina, *The Nottingham group*, New horizons in pro-p groups, 205–221, Progr. Math., 184, Birkhäuser Boston, Boston, MA, 2000. MR1765121 (2001f:20054)

[Er] M. Ershov, *New just-infinite pro-p groups of finite width and subgroups of the Nottingham group*, J. Algebra 275 (2004), no. 1, 419–449. MR2047455 (2005b:20052)

[K] B. Klopsch, *Automorphisms of the Nottingham group*, J. Algebra 223 (2000), no. 1, 37–56. MR1738250 (2000j:20047)

[Pi] R. Pink, *Compact subgroups of linear algebraic groups*, J. Algebra 206 (1998), no. 2, 438–504. MR1637068 (99g:20087)

Department of Mathematics, University of Virginia, Charlottesville, Virginia 22904
E-mail address: ershov@virginia.edu