On subgroups of the Nottingham group of positive Hausdorff dimension.

Mikhail Ershov

October 29, 2004

Abstract

By a Theorem of Camina, the Nottingham group $\mathcal{N}(\mathbb{F}_p)$ contains an isomorphic copy of every finitely generated pro-p group. In this paper we obtain several restrictions on the structure of subgroups of $\mathcal{N}(\mathbb{F}_p)$ which have positive Hausdorff dimension and show that such groups, if finitely generated, cannot be linear over a local field. This implies that just-infinite subgroups of $\mathcal{N}(\mathbb{F}_p)$ studied in [F] and [BK] are not linear over any profinite ring.

1   Introduction

Let F be a finite field and let $\mathcal{N}(F)$ be the group of wild automorphisms of the field $F((t))$, traditionally called the Nottingham group. One of the remarkable properties of the Nottingham group $\mathcal{N} = \mathcal{N}(\mathbb{F}_p)$ is the fact that any finitely generated pro-p group can be embedded as a closed subgroup of $\mathcal{N}$. The original proof of this result is due to Camina [Ca1]; later a different argument was given by Fesenko [F]. Both Camina's and Fesenko's proofs provide a certain algorithm for constructing a subgroup of $\mathcal{N}$ isomorphic to a given pro-p group G. However, the subgroups of $\mathcal{N}$ constructed in such a way have rather special form. For example, they always lie in the closure of the torsion of the Nottingham group and are small in the sense of Hausdorff dimension. As noted in [BK], Fesenko's construction always gives subgroups of dimension zero, and in Camina's construction dimensions cannot exceed $1/p$; moreover, it is not clear whether positive dimensional subgroups can occur at all. Thus one may hope that positive dimensional subgroups of the Nottingham group have more restricted structure. In this note we prove the following theorem.

Theorem 1.1. *Let G be a finitely generated subgroup of $\mathcal{N}(\mathbb{F}_p)$ of positive Hausdorff dimension. Then G is not linear over a local field (as a topological group).*

A stronger statement can be made about just-infinite subgroups of $\mathcal{N}(\mathbb{F}_p)$. This is because of a Theorem of Jaikin-Zapirain [JZ] which says that a just-infinite pro-p group which is linear over some profinite ring must be linear over a local field.

Corollary 1.2. *Let G be a just-infinite subgroup of $\mathcal{N}(\mathbb{F}_p)$ of positive Hausdorff dimension. Then G is not linear over any profinite ring.*

This result is important in connection with the problem of classification of hereditarily just-infinite pro-p groups of finite width (HJIFW groups)— see [LM] and [Sh]. The majority of the known examples of such groups are compact open subgroups of linear algebraic groups over local fields. The only other known examples of HJIFW groups are the Nottingham groups $\mathcal{N}(\mathbb{F}_q)$, where $q = p^n$, and three infinite families $\mathcal{B}, \mathcal{Q}$ and $\mathcal{T}$ of subgroups of $\mathcal{N}(\mathbb{F}_p)$ constructed in [BK], [Er] and [F], respectively (see also [Grif1] and [Grif2]). All groups in the above families are easily seen to have positive Hausdorff dimension, and thus Theorem 1.1 confirms that these groups are not commensurable to any of the previously known HJIFW groups.

The proof of Theorem 1.1 consists of two parts. In the first part (Section 3) we use the structure of the Nottingham group to show that the centralizers and the normalizers of certain subgroups of $\mathcal{N}(\mathbb{F}_p)$ must have dimension zero (in particular, any nilpotent subgroup of $\mathcal{N}(\mathbb{F}_p)$ is zero dimensional). In the second part (Sections 4 and 5) we use Pink's Theorem [P] to show that every finitely generated pro-p group G which is linear over a local field can be written as a product of finitely many subgroups $G_1 G_2 \ldots G_n$ such that each G_i cannot be embedded in $\mathcal{N}(\mathbb{F}_p)$ as a positive dimensional subgroup because of the above restrictions (Theorem 4.1). The latter implies the assertion of Theorem 1.1 according to Proposition 2.1.

Remark. Recently, M. Abert and B.Virag [AV] obtained several interesting results about the structure of positive dimensional subgroups of $\Gamma(p)$, the group of p-adic automorphisms of the infinite rooted p-ary tree (see [Grig] for background). In particular, they showed that such subgroups cannot be solvable (and, more generally, cannot be abstractly generated by countably many solvable subgroups). They also established a special case of their conjecture (related to earlier conjectures of Boston [Bo] and Wilson [Wil]) that a positive dimensional subgroup of $\Gamma(p)$ must contain a nonabelian free pro-p group. It would be interesting to answer the analogous questions about positive dimensional subgroups of $\mathcal{N}(\mathbb{F}_p)$.

2 Preliminaries

Throughout the paper, groups are assumed to be topological unless indicated otherwise; by a subgroup of a topological group we always mean a closed subgroup. As usual, $(g, h) = g^{-1}h^{-1}gh$ will stand for the commutator of g and h. The nth term of the lower central series of a group G will be denoted by $\gamma_n G$.

Filtrations and Lie algebras of pro-p groups. By a filtration of a profinite group G we mean a descending chain of open normal subgroups $G = G_1 \supseteq G_2 \supseteq \ldots$ which form a base of neighborhoods of identity. A filtration is called central if $[G_i, G_j] \subseteq G_{i+j}$ for all $i, j \geq 1$. If in addition G is pro-p and all quotients G_i/G_{i+1} have exponent p, the filtration is called p-central.

Now let $\{G_n\}$ be a central filtration of a pro-p group G. The associated graded Lie ring $\text{Lie}(G)$ is defined as follows. As a graded abelian group, $\text{Lie}(G) = \bigoplus_{n=1}^{\infty} L_n$, where $L_n = G_n/G_{n+1}$, and Lie bracket is defined by $[aG_{n+1}, bG_{m+1}] = (a, b)G_{n+m+1}$. With each subgroup H of G we associate a Lie subring $\text{Lie}_G(H) = \bigoplus_{n=1}^{\infty} (H \cap G_n)G_{n+1}/G_{n+1} \subseteq \text{Lie}(G)$. If the filtration $\{G_n\}$ is p-central, $\text{Lie}(G)$ becomes a Lie algebra over $\mathbb{F}_p$.

For every $g \in G \backslash \{1\}$ there exists a unique number n such that $g \in G_n \backslash G_{n+1}$. This number will be called the *degree* of g and denoted by $\deg(g)$. The coset $g G_{n+1}$ will be called the *leading term* of g and denoted by $\text{LT}(g)$. Note that if H is a subgroup of G, then $\{\text{LT}(h) \mid h \in H\}$ coincides with the set of homogeneous elements of $\text{Lie}_G(H)$.

Hausdorff dimension. Let G be a profinite group with fixed filtration $\{G_n\}$. One can define an invariant metric on G by setting $d(x, y) = \inf\{|G : G_n|^{-1} \mid xy^{-1} \in G_n\}$ and use the associated Hausdorff dimension function to measure the sizes of subgroups of G. This concept was studied in detail by Barnea and Shalev [BSh] who showed that the Hausdorff dimension of a subgroup H of G coincides with its lower box (Minkowski) dimension $\underline{\dim}_G H$ and is given by the following formula:

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

The upper box dimension, which is given by the formula

$$\overline{\dim}_G H = \limsup_{n \to \infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|},$$

will also be considered.

Here are some basic properties of these dimension functions:

1) If H is open in G then $\overline{\dim}_G H = \underline{\dim}_G H = 1$.

2) Let $K \subseteq H \subseteq G$. Choose some filtration of G and consider the induced filtrations on K and H. The associated dimension functions satisfy the following inequalities:

$$\underline{\dim}_H K \cdot \overline{\dim}_G H \geq \underline{\dim}_G K \geq \underline{\dim}_H K \cdot \underline{\dim}_G H$$

$$\overline{\dim}_H K \cdot \underline{\dim}_G H \leq \overline{\dim}_G K \leq \overline{\dim}_H K \cdot \overline{\dim}_G H.$$

(2.1)

3) If G has subgroups $\{G_i\}_{i=1}^n$ such that $G = G_1 G_2 \ldots G_n$, then

$$\sum_{i=1}^n \overline{\dim}_G G_i \geq 1.$$

(2.2)

The following consequence of (2.1) and (2.2) will be one of our main tools [1].

Proposition 2.1. *Let G be a pro-p group with fixed filtration and let H be a subgroup of G of positive Hausdorff dimension. If $H = H_1 H_2 \ldots H_n$ (where each H_i is a subgroup), then $\overline{\dim}_G H_i > 0$ for some i.*

The Nottingham group $\mathcal{N} = \mathcal{N}(\mathbb{F}_p)$ can be defined as the group of automorphisms of the ring $\mathbb{F}_p[[t]]$ which act trivially on $(t)/(t^2)$ or, equivalently, as the group of automorphisms of the local field $\mathbb{F}_p((t))$ which act trivially on the residue field (such automorphisms are called wild). A natural filtration of $\mathcal{N}$ consists of congruence subgroups $\{\mathcal{N}_n\}$ where $\mathcal{N}_n = \{f \in \mathcal{N} \mid f(t) \equiv t$ mod $t^{n+1}\mathbb{F}_p[[t]]\}$. For a detailed account of the structure of $\mathcal{N}$ the reader is referred to [Ca2]; some related concepts and properties will be introduced throughout the paper as they are needed.

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

It is easy to see that the upper (lower) box dimension of a subgroup G of $\mathcal{N}$ (with respect to the congruence filtration) is equal to the upper (lower) density of its index set. More precisely, we have

$$\overline{\dim}_{\mathcal{N}} G = \limsup_{n \to \infty} \frac{\text{card}\,(\text{Ind}\,(G) \cap \{1, 2, \ldots, n\})}{n}$$

$$\underline{\dim}_{\mathcal{N}} G = \liminf_{n \to \infty} \frac{\text{card}\,(\text{Ind}\,(G) \cap \{1, 2, \ldots, n\})}{n}.$$

---

[1] The same idea is used in the proof of [AV, Corollary 8.3]

3 Nottingham-small groups

For convenience we introduce the following definition.

Definition. a) A subgroup G of $\mathcal{N}$ will be called small, if G has upper box dimension zero (with respect to the congruence filtration).

b) A pro-p group G will be called *Nottingham-small* (or $\mathcal{N}$-small), if for every embedding of G in $\mathcal{N}$, the image of G is a small subgroup of $\mathcal{N}$.

The goal of this section is to find sufficient conditions for a pro-p group to be $\mathcal{N}$-small.

The following theorem of Wintenberger [Win] implies that all abelian pro-p groups are $\mathcal{N}$-small.

Theorem 3.1 (Wintenberger). *Let H be an abelian subgroup of $\mathcal{N}(\mathbb{F}_p)$, and let I be the index set of H. Let $i_1 < i_2 < \ldots$ be the elements of I listed in increasing order. Then $i_{n+1} \equiv i_n \mod p^n$ for each $n \in \mathbb{N}$.*

In [Er] we used Wintenberger's theorem to prove the following.

Theorem 3.2. *Let H be an infinite subgroup of $\mathcal{N}(\mathbb{F}_p)$. Then the centralizer of H in $\mathcal{N}$ is small.*

It follows immediately that every nilpotent group is $\mathcal{N}$-small. We conjecture that every solvable group is $\mathcal{N}$-small. The latter would be established if one could show that the normalizer of an infinite abelian subgroup of $\mathcal{N}$ is always small. We will address this problem in the special case of abelian groups of exponent p which is sufficient for our purposes. In other words, we will prove the following.

Proposition 3.3. *Let A be a subgroup of $\mathcal{N}$ which is isomorphic to the additive group of the ring $\mathbb{F}_p[[t]]$. Then the normalizer of A in $\mathcal{N}$ is small.*

Remark. In what follows, the additive group of $\mathbb{F}_p[[t]]$ will be denoted by $\mathbb{F}_p^\infty$. In fact, it is the unique infinite countably based abelian pro-p group of exponent p.

The normalizers of abelian subgroups of exponent p are very easy to study because we possess an exhaustive description of the centralizers of elements of order p in $\mathcal{N}$. Here we state only basic facts which will be used in the proof; for more details the reader is referred to [K] and [Er].

Let $f \in \mathcal{N}$ be an element of order p. Consider $\mathcal{N}$ as the group of wild automorphisms of a local field $F \cong \mathbb{F}_p((t))$. Denote the fixed field of f by K and the centralizer of f in $\mathcal{N}$ by C. It is easy to see that $K \cong \mathbb{F}_p((t))$.

Every element of C leaves K invariant, and the induced automorphism of K is always wild. Therefore, we obtain a homomorphism $\varphi_f : C \to \mathcal{N}$. Clearly, $\operatorname{Ker} \varphi_f = \langle f \rangle$ (in fact, the image of φ_f is an open subgroup of $\mathcal{N}$, as shown in [Er], whence C is commensurable to $\mathcal{N}$). Note that our definition of φ_f depends on the choice of an isomorphism between K and $\mathbb{F}_p((t))$. However, φ_f is well defined up to conjugation.

Now given $h \in C$, there exists a simple relation between the numbers $\deg h$ and $\deg \varphi_f(h)$:

$$\deg \varphi_f(h) = \begin{cases} \deg h & \text{if} \quad \deg h < \deg f \\ \deg f + \frac{\deg h - \deg f}{p} & \text{if} \quad \deg h > \deg f \end{cases} \tag{3.1}$$

The proof of this formula is analogous to that of [dSF, Lemma 4.2]. Finally, we note that the index set of C is equal to $\{i \in \mathbb{N} \mid i \equiv \deg f \mod p\}$ (see [BK, Proposition A.1]).

The proof of Proposition 3.3 will be based on the following lemma which is similar to Wintenberger's theorem.

Lemma 3.4. *Let B be a subgroup of $\mathcal{N}$ isomorphic to $\mathbb{F}_{p^s}$ for some $s < \infty$. Let $\{j_1 < j_2 < \ldots < j_s\}$ be the index set of B. Let g be any element of $\mathcal{N}$ such that $d := \deg(g) > j_s$. Suppose that for any $b \in B$ we have $(b, g) \in \mathcal{N}_{p^s d}$. Then $d \equiv j_s \mod p^s$.*

Proof. The case $s = 1$ is obvious. Indeed, choose any $b \in B \backslash \{1\}$. If $d \not\equiv j_1 \mod p$, then by [Ca2, Proposition 1] we have $\deg(b, g) = \deg b + \deg g = d + j_1 < pd$, contrary to our assumption.

We proceed by induction on s. Choose an element $b \in B$ such that $\deg(b) = j_1$. Let C be the centralizer of b in $\mathcal{N}$, and let $\varphi_b : C \to \mathcal{N}$ be an associated homomorphism as described above.

First assume that $g \in C$. Let $B' = \varphi_b(B)$ and let $g' = \varphi_b(g)$. We claim that the pair (B', g') satisfies the conditions of the Lemma. Since $\operatorname{Ker} \varphi_b = \langle b \rangle$, B' has order p^{s-1}. It follows from formula (3.1) that the largest element of $\operatorname{Ind}(B')$ is equal to $j_1 + \dfrac{j_s - j_1}{p}$ which is less than $\deg g' = j_1 + \dfrac{d - j_1}{p}$. Now given $h' \in B'$, let h be any element of $\varphi_b^{-1}(h')$. By our assumption $\deg(g, h) \geq p^s d$, whence

$$\deg(g', h') = \deg \varphi_b((g, h)) \geq j_1 + \frac{p^s d - j_1}{p} \geq$$

$$p^{s-1}(j_1 + \frac{d - j_1}{p}) + (p^{s-1} - p^{s-2})(d - j_1) \geq p^{s-1} \deg g'.$$

By induction we have $\deg g' \equiv j_1 + \dfrac{j_s - j_1}{p} \mod p^{s-1}$, whence $d \equiv j_s$ $\mod p^s$.

Now we treat the general case. Since b is an element of order p and $\deg b = j_1$, we know that the set $\mathrm{Ind}\,(C)$ consists of all integers n congruent to j_1 modulo p. Note also that all quotients $\mathcal{N}_i / \mathcal{N}_{i+1}$ are cyclic of order p, whence $(C \cap \mathcal{N}_n) \mathcal{N}_{n+1} = \mathcal{N}_n$ for every $n \in \mathrm{Ind}\,(C)$. It follows that g can be written in the form cu where $c \in C$ and $\deg u \not\equiv j_1 \mod p$.

Since $(b, c) = 1$, we have $(b, u) = (b, cu) = (b, g) \in \mathcal{N}_{p^s d}$ by assumption. On the other hand, $\deg u \not\equiv_p \deg b$, whence $\deg (u, b) = j_1 + \deg u$. We conclude that $\deg u \geq p^s d - j_1$. We claim that the pair (B, c) satisfies the conditions of the Lemma, and therefore we are reduced to the previous case.

Indeed, $\deg u > d = \deg g$, whence $\deg c = \deg (gu^{-1}) = d$. For any $h \in B$, we have $(h, g) = (h, cu) \equiv (h, c) \mod \mathcal{N}_{\deg h + \deg u}$. Now $(h, g) \in \mathcal{N}_{p^s d}$ by assumption. Finally, $\deg h + \deg u \geq p^s d - j_1 + \deg h \geq p^s d$, whence $(h, c) \in \mathcal{N}_{p^s d}$. The proof is complete. $\qquad\square$

Proof of Proposition 3.3. Let G be the normalizer of A in $\mathcal{N}$. Set $\alpha_n = \dfrac{\log_p |G : G_n|}{\log_p |\mathcal{N} : \mathcal{N}_n|}$. It will be enough to show that $\limsup \alpha_n \leq 1/p^s$ for every positive integer s. From now on s will be fixed.

Let $I = \{i_1 < i_2 < i_3 \ldots\}$ be the index set of A. Define the integer-valued function $j(n)$ by $j(n) = \mathrm{card}\,\{i \in I \mid i \leq n\}$. It follows easily from Theorem 3.1 that $j(n) \leq C \log_p n$ for some constant C. Set $m = i_s$, and choose a subgroup B of A whose index set is equal to $\{i_1 < i_2 < \cdots < i_s\}$.

Let n be any integer larger than m, and set $Q(n) := A / A \cap \mathcal{N}_{p^s n}$. This is a finite abelian group of exponent p which can be thought of as a vector space over $\mathbb{F}_p$. Its dimension d_n does not exceed $i(p^s n) \leq C(\log_p n + s)$. Now G acts by conjugation on both A and $A \cap \mathcal{N}_{p^s n}$, hence also on $Q(n)$. Let $K(n)$ be the kernel of this action. Clearly, we have

$$\log_p |G : K(n)| \leq \log_p |GL_{d_n}(\mathbb{F}_p)| < C^2 (\log_p n + s)^2.$$

On the other hand, if g is any element of $K(n)$ whose degree d satisfies the inequality $m < d \leq n$, then applying Lemma 3.4 to the pair (B, g), we conclude that $d \equiv i_s \mod p^s$. Now we can estimate the numbers $\{\alpha_n\}$ from above. We have

$$\alpha_n \leq \frac{\log_p |G : G_{m+1}| + \log_p |G_{m+1} \cap K(n) : G_n \cap K(n)| + \log_p |G : K(n)|}{\log_p |\mathcal{N} : \mathcal{N}_n|}.$$

The denominator of this fraction is equal to $n-1$. In the numerator the first term is independent of n, the third term is bounded from above by $C^2(\log_p n + s)^2$, and the second term does not exceed card $\{d \in \operatorname{Ind} K(n) \mid m < d \le n\} \le \frac{n-m}{p^s} + 1$. Therefore, $\limsup \alpha_n \le 1/p^s$, and we are done. $\quad\square$

Now we are ready to explain how Theorem 1.1 follows from Theorem 4.1.

Proof of Theorem 1.1. It is enough to show that G does not satisfy either condition in the conclusion of Theorem 4.1. Condition b) cannot hold for G by Proposition 3.3. Proposition 2.1 and Theorem 3.2 imply that G does not satisfy a). $\quad\square$

4 Linear pro-p groups

In this section we will prove the following.

Theorem 4.1. *Let G be a finitely generated pro-p group which is linear over a local field. Then G has a finite index subgroup H satisfying at LEAST one of the following conditions:*

a) H is a product of finitely many subgroups $H_1, \ldots, H_k$ such that each H_i has infinite centralizer in H;

b) H has a normal subgroup isomorphic to the additive group of the ring $\mathbb{F}_p[[t]]$.

Our main tool is the famous theorem of Pink [P], which is stated below:

Theorem 4.2. *Let G be a compact subgroup of $GL_n(E)$ where E is a local field of characteristic p. Then there exist normal subgroups $\Gamma_3 \subseteq \Gamma_2 \subseteq \Gamma_1$ of G such that*

G/Γ_1 is finite;

Γ_1/Γ_2 is abelian of finite exponent;

there exists a local field F of characteristic p, a connected semisimple adjoint algebraic group $\mathbb{H}_{\mathrm{ad}}$ over F with a universal cover $\pi : \mathbb{H} \to \mathbb{H}_{\mathrm{ad}}$ and an open compact subgroup L of $\mathbb{H}(F)$ such that Γ_2/Γ_3 is isomorphic to $\pi(L)$ as a topological group;

Γ_3 is solvable.

Proof of Theorem 4.1. If G is linear in characteristic zero, it is p-adic analytic. In this case G is a product of finitely many procyclic subgroups, and the assertion of the Theorem is obvious. Thus we can assume that G is a closed subgroup of $GL_n(E)$ where E is a local field of characteristic p.

Let Γ_1, Γ_2 and Γ_3 be as in Pink's theorem. First we consider the case when Γ_3 is infinite.

Case 1: Γ_3 is infinite.

By Lie-Kolchin-Maltsev theorem, Γ_3 has an open subgroup Γ_4 which is triangularizable over some finite extension E' of E (which is also a local field). Choose an open subgroup H of G such that $R := \Gamma_3 \cap H \subseteq \Gamma_4$. Note that $\gamma_2 R$ is unipotent. Moreover, we can assume that either R is abelian or $\gamma_2 R$ is infinite (if $\gamma_2 R$ is finite, replace H by an open subgroup H_1 such that $H_1 \cap \gamma_2 R = \{1\}$ and replace R by $R \cap H_1$). If $\gamma_2 R$ is infinite, let C be the last infinite term of the derived series of R. Once again replacing H by an open subgroup we can assume that C is abelian. Now C is unipotent, whence has finite exponent. Therefore, $C(p) := \{g \in C \mid g^p = 1\}$ is a closed normal subgroup of H isomorphic to $\mathbb{F}_p{}^\infty$.

Suppose now that R is abelian. Since R is a pro-p group, every torsion element of R has order p^k for some k and therefore is unipotent. If every element of R is unipotent, we can argue as before. Otherwise, consider the set $C = \{g^{p^n} \mid g \in R\}$. Since R is abelian, C is a subgroup; moreover, C is normal in H. It is easy to see that every element of C is diagonalizable over E', whence we can assume that C lies inside $D_n(E')$, the diagonal subgroup of $GL_n(E')$.

An easy computation shows that given $c \in C$ and $g \in GL_n(E')$ with nonzero diagonal entries, g commutes with c whenever $g^{-1}cg \in D_n(E')$. Obviously, H has a finite index subgroup whose elements have nonzero diagonal entries. Since H normalizes C, we conclude that H has a finite index subgroup with infinite center.

Case 2: Γ_3 is finite.

Since G is finitely generated, Γ_2 has finite index in G. We also know that the kernel of the map π in Pink's theorem is finite. Therefore, G has a finite index subgroup H which is isomorphic to an open compact subgroup of $\mathbb{H}(F)$ (where F is a local field of characteristic p and $\mathbb{H}$ is a semisimple simply-connected algebraic group over F).

We use [Sp] as a reference for the theory of algebraic groups. Throughout the proof we will identify an algebraic group defined over F with the set of its $\bar{F}$-points (where $\bar{F}$ is the algebraic closure of F). We consider two subcases:

Subcase 1: $\mathbb{H}$ *is isotropic (over F).*

We start by choosing an F-embedding of $\mathbb{H}$ into $\mathbb{G} = \mathbb{GL}_n$. Since $\mathbb{H}$ is isotropic, there exists an F-homomorphism λ from the multiplicative group of F to $\mathbb{H}$ such that Im λ is non-central in $\mathbb{H}$. After conjugating by an element of $GL_n(F)$ we may assume that there exist integers $m_1 \geq m_2 \geq \ldots \geq m_n$ such that $\lambda(a)$ is the diagonal matrix with entries $a^{m_1}, a^{m_2}, \ldots, a^{m_n}$ for any

$a \in \bar{F}$.

Consider the following subgroups of $\mathbb{G} = \mathbb{GL}_n$:

$\mathbb{U}_\mathbb{G}{}^+ = \{x \in \mathbb{G} \mid \lim_{a \to 0} \lambda(a) x \lambda(a)^{-1} = 1\}$,

$\mathbb{U}_\mathbb{G}{}^- = \{x \in \mathbb{G} \mid \lim_{a \to 0} \lambda(a)^{-1} x \lambda(a) = 1\}$ and

$\mathbb{C}_\mathbb{G} = \mathrm{Cent}_\mathbb{G}(\mathrm{Im}\,\lambda)$, the centralizer of $\mathrm{Im}\,\lambda$ in $\mathbb{G}$.

In fact, these subgroups can be described explicitly. In the simplest case when all m_i are distinct, $\mathbb{U}_\mathbb{G}{}^\pm$ are the subgroups of strictly upper (lower) triangular matrices, and $\mathbb{C}_\mathbb{G}$ is the diagonal subgroup of $\mathbb{GL}_n$.

Now if $\mathbb{K}$ is any reductive F-subgroup of $\mathbb{GL}_n$, we set $\mathbb{U}_\mathbb{K}{}^\pm = \mathbb{U}_\mathbb{G}{}^\pm \cap \mathbb{K}$, $\mathbb{C}_\mathbb{K} = \mathbb{C}_\mathbb{G} \cap \mathbb{K}$. By [Sp, Theorem 13.4.2] $\mathbb{U}_\mathbb{K}{}^\pm$ and $\mathbb{C}_\mathbb{K}$ are connected F-subgroups of $\mathbb{K}$; $\mathbb{C}_\mathbb{K}$ is reductive, $\mathbb{U}_\mathbb{K}{}^\pm$ are unipotent, and the product morphism $\pi_\mathbb{K} : \mathbb{U}_\mathbb{K}{}^- \times \mathbb{C}_\mathbb{K} \times \mathbb{U}_\mathbb{K}{}^+ \to \mathbb{K}$ is a bijection onto a Zariski open subset of $\mathbb{K}$.

Let $\{G_i\}$ be the congruence filtration of $\mathbb{G}(F) = GL_n(F)$ and let $H_i = \mathbb{H} \cap G_i$. If i is sufficiently large, $H_i \subseteq H$ since H is open in $\mathbb{H}(F)$. We also know that $\mathrm{Im}\,\pi_\mathbb{H}$ is Zariski open in $\mathbb{H}$, whence $H_k \subseteq H \cap \mathrm{Im}\,\pi_\mathbb{H}$ for some k. Thus for any $h \in H_k$ there exist $u^- \in \mathbb{U}_\mathbb{H}{}^-$, $u^+ \in \mathbb{U}_\mathbb{H}{}^+$ and $c \in \mathbb{C}_\mathbb{H}$ such that $h = u^- c u^+$. We claim that $u^-, c, u^+ \in G_k$.

Indeed, as an element of $\mathbb{G}$, h has a unique decomposition of the form $h = v^- t v^+$ where $v^- \in \mathbb{U}_\mathbb{G}{}^-$, $v^+ \in \mathbb{U}_\mathbb{G}{}^+$ and $t \in \mathbb{C}_\mathbb{G}$. But we already have one such decomposition: $h = u^- c u^+$. Therefore, $u^+ = v^+$, $u^- = v^-$ and $c = t$. On the other hand, one can compute v^+, v^- and t directly. For simplicity assume that all integers $\{m_i\}$ are distinct. In this case we must find a strictly lower triangular matrix v^-, a diagonal matrix t and a strictly upper triangular matrix v^+ such that $h = v^- t v^+$. This problem can be solved by Gaussian elimination, and the inclusions $v^-, t, v^+ \in G_k$ easily follow from the fact that the entries $\{h_{ij}\}$ of h satisfy the congruence $h_{ij} \equiv \delta_{ij} \mod \mathfrak{m}^k$, where $\mathfrak{m}$ is the maximal ideal of the valuation ring of F.

Therefore, we have shown that

$$H_k = (\mathbb{U}_\mathbb{H}{}^- \cap G_k)(\mathbb{C}_\mathbb{H} \cap G_k)(\mathbb{U}_\mathbb{H}{}^+ \cap G_k)$$

Using the fact that the groups $\mathbb{U}_\mathbb{H}{}^\pm$ are connected and unipotent, it is easy to show that their subgroups $\mathbb{U}_\mathbb{H}{}^\pm \cap G_k$ have infinite centers. The group $\mathbb{C}_\mathbb{H} \cap G_k$ centralizes an infinite subgroup of H_k by construction. Therefore, we managed to write H_k as a product of three subgroups with infinite centralizers.

Case 2: $\mathbb{H}$ is anisotropic.

Since $\mathbb{H}$ is simply connected, it is a direct product of finitely many almost simple groups $\mathbb{H}_1, \ldots, \mathbb{H}_k$. Each $\mathbb{H}_i$ is obtained by restriction of scalars from

an absolutely almost simple group $\mathbb{B}_i$ defined and anisotropic over some finite extension F_i of F, and $\mathbb{H}_i(F) \cong \mathbb{B}_i(F_i)$ as a topological group. By the classification of absolutely almost simple algebraic groups over local fields (see [Ti]), $\mathbb{B}_i(F_i)$ is isomorphic to the group $SL_1(D_i)$ of reduced norm 1 elements of a finite-dimensional division algebra D_i over F_i.

For each $i = 1, \ldots, k$, set $H_i = \mathbb{H}_i(F) \cap H$. Since $\mathbb{H}$ is anisotropic, $\mathbb{H}(F)$ is compact. Therefore, H has finite index in $\mathbb{H}(F) = \mathbb{H}_1(F) \times \ldots \times \mathbb{H}_k(F)$, whence $H_1 \times \ldots \times H_k$ is a finite index subgroup of H. In the next section we will use the structure of division algebras over local fields to show that each H_i is a product of finitely many abelian subgroups. $\square$

5 The group $SL_1(D)$

Let D be a finite-dimensional central division algebra over a local field F of characteristic p. Our goal in this section is to prove the following

Proposition 5.1. *Let H be a finite index pro-p subgroup of $SL_1(D)$. Then H is a product of finitely many abelian subgroups.*

Remark. In the terminology of [Ab], a group which is a product of finitely many abelian subgroups is said to have *finite abelian width.* [2]

We start by reviewing some basic facts about the structure of division algebras over local fields (see [Ri] for more details). First of all, D is always a cyclic algebra. More precisely, there exists an unramified extension W of F of degree $n = \deg(D)$ and an element $\pi \in D$ such that

a) $D = W \oplus W\pi \oplus W\pi^2 \oplus \cdots \oplus W\pi^{n-1}$ as a left vector space over W;

b) $\pi w \pi^{-1} = \sigma(w)$ for all $w \in W$, where σ is a generator of the Galois group $\mathrm{Gal}(W/F)$;

c) $\tau := \pi^n$ is a uniformizer of F, i.e. τ is a generator of the maximal ideal of the valuation ring of F.

We denote by O_F, O_W and O_D the valuation rings of F, W and D, and by $\mathfrak{m}_F$, $\mathfrak{m}_W$, $\mathfrak{m}_D$ the corresponding maximal ideals. Note that $\mathfrak{m}_D = \pi O_D$, $\mathfrak{m}_F = \tau O_F$ and $\mathfrak{m}_W = \tau O_W$. Let κ_F and κ_W be the residue fields of F and W. Since W/F is unramified, the natural map $\mathrm{Gal}(W/F) \to \mathrm{Gal}(\kappa_W/\kappa_F)$ is an isomorphism. Thus $\mathrm{Gal}(\kappa_W/\kappa_F)$ is generated by the element $\bar{\sigma}$ defined by $\bar{\sigma}(w + \mathfrak{m}_W) := \sigma(w) + \mathfrak{m}_W = \pi w \pi^{-1} + \mathfrak{m}_W$.

---

[2] I am extremely grateful to Laci Pyber who pointed out the relevance of such factorizations to linearity questions

The reduced norm map from D to F will be denoted by $\mathrm{N_{red}}$. Recall that if $a \in D$, then $\mathrm{N_{red}}(a)$ is the determinant of the endomorphism of the left W-vector space D given by $d \mapsto da$.

Let $U = \{x \in D^* \mid x \equiv 1 \mod \mathfrak{m}_D\}$ and let $G = U \cap SL_1(D)$, where $SL_1(D)$ is the group of elements of D of reduced norm one. The groups U and G have natural congruence filtrations $\{U_i\}$ and $\{G_i\}$, respectively, where $U_i = \{x \in U \mid x \equiv 1 \mod \mathfrak{m}_D^i\}$ and $G_i = G \cap U_i$. It is clear that U is an open pro-p subgroup of D^* and G is a finite index pro-p subgroup of $SL_1(D)$ (since $SL_1(D)$ is compact). In what follows, $\mathrm{Lie}(U)$ and $\mathrm{Lie}(G)$ will denote the Lie algebras of U and G with respect to the above filtrations. Obviously, $\mathrm{Lie}(G)$ can be identified with the subalgebra $\mathrm{Lie}_U(G)$ of $\mathrm{Lie}(U)$.

The additive group of the Lie algebra $\mathrm{Lie}(U)$ is isomorphic to $\bigoplus_{i=1}^{\infty} \kappa_W\, t^i$ such that $\mathrm{LT}\,(1 + w\pi^i) \mapsto (w + \mathfrak{m}_W)t^i$ for all $i \geq 1$ and all $w \in O_W \backslash \mathfrak{m}_W$. The Lie bracket is now given by the following simple formula:

$$[\lambda t^i, \mu t^j] = (\lambda \bar{\sigma}^i(\mu) - \mu \bar{\sigma}^j(\lambda))t^{i+j}, \text{ where } \bar{\sigma} \text{ is as above.}$$

The subalgebra $\mathrm{Lie}_U(G)$ has the form $\bigoplus_{i=1}^{\infty} M_i$, where $M_i = \kappa_W t^i$ if $n \nmid i$, and $M_i = \{\lambda t^i \mid \mathrm{tr}\,(\lambda) = 0\}$ if $n \mid i$ (here tr is the trace of the extension κ_W / κ_F).

Proof of Proposition 5.1. Clearly, it is sufficient to show that some open subgroup of H has finite abelian width. Thus we can assume that H is one of the congruence subgroups $\{G_i\}$. To keep notation simple we will present the proof in the case $H = G = G_1$; the reader is assured that the same argument works in the general case (alternatively, one could show that the property of having finite abelian width is a commensurability invariant).

The first step of the proof is to construct a "large" abelian subgroup of G. Let A be the group generated by the set $\{\sigma(w)w^{-1} \mid w \in W^* \cap U\}$ (recall that $\sigma(w) = \pi w \pi^{-1}$). Since $\sigma \in \mathrm{Gal}\,(W/F)$, $A \subset W^* \cap U$, whence A is abelian. Moreover, $A \subset G$ since $\mathrm{N_{red}}\,(\sigma(w)w^{-1}) = \mathrm{N_{red}}\,(\pi w \pi^{-1} w^{-1}) = 1$ for every $w \in W^*$. We claim that the Lie algebra $\mathrm{Lie}_U(A) = \mathrm{Lie}_G(A)$ contains every homogeneous element of $\mathrm{Lie}(G)$ whose degree is a multiple of n. Indeed, any such element is of the form λt^{ni}, where $\lambda \in \kappa_W$ and $\mathrm{tr}\,(\lambda) = 0$. The last condition implies that there exists $\alpha \in \kappa_W$ such that $\lambda = \alpha - \bar{\sigma}(\alpha)$. Choose $a \in W$ such that $\alpha = a + \mathfrak{m}_W$ and let $w = 1 + a\pi^{ni}$. Clearly, $\mathrm{LT}\,(w) = \alpha t^{ni}$ and $\mathrm{LT}\,(\sigma(w)) = \mathrm{LT}\,(1 + \sigma(a)\pi^{ni}) = \bar{\sigma}(\alpha)t^{ni}$, whence $\mathrm{LT}\,(\sigma(w)w^{-1}) = \mathrm{LT}\,(\sigma(w)) - \mathrm{LT}\,(w) = \lambda t^{ni}$.

To prove that G has finite abelian width we use the following criterion which will be established in Appendix.

Lemma 5.2. *Let G be a pro-p group. Let $\{G_n\}$ be a p-central filtration of G, and denote by $\mathrm{Lie}(G)$ the associated Lie algebra. Assume we are given*

a) an abelian subgroup A of G,

b) a finite subset S of G,

c) an integer N such that

any homogeneous element of $\mathrm{Lie}(G)$ of degree $n \geq N$ either lies in $\mathrm{Lie}_G(A)$ or has the form $\mathrm{LT}((a,s))$ for some $s \in S$ and $a \in A$.

Then the product of finitely many conjugates of A contains G_N. Therefore, G has finite abelian width.

We resume the proof of Proposition 5.1. First assume that either $n > 2$ or $p > 2$. Let S be any subset of G such that the set $V = \{\mathrm{LT}(s) \mid s \in S\}$ consists of all homogeneous elements of $\mathrm{Lie}_U(G) = \mathrm{Lie}(G)$ of degree at most $n - 1$. Now pick an integer $k \geq n$ and let $u \in \mathrm{Lie}(G)$ be a homogeneous element of degree k. We already know that $u \in \mathrm{Lie}_G(A)$ if $n \mid k$. We claim that if $n \nmid k$, then u lies in the set $B := \{[a,v] \mid a \in \mathrm{Lie}_G(A), v \in V\}$. This will finish the proof by Lemma 5.2, since any element of B has the form $\mathrm{LT}((g,s))$ for some $s \in S$ and $g \in A$.

Write k in the form $ni + j$ where $1 \leq j \leq n - 1$. Since $p > 2$ or $n > 2$, the field extension κ_W/κ_F can be generated by an element η of trace zero (see [Ri, Lemma 4]). Since $\eta t^{ni} \in \mathrm{Lie}_G(A)$, for any $\nu \in \kappa_W$ we have $B \ni [\eta t^{ni}, \nu t^j] = (\eta \bar{\sigma}^{ni}(\nu) - \bar{\sigma}^j(\eta)\nu)t^{ni+j} = (\eta - \bar{\sigma}^j(\eta))\nu\, t^{ni+j}$. Now $\eta \neq \bar{\sigma}^j(\eta)$ since $j < n = [\kappa_W : \kappa_F]$. Therefore, $B \ni \mu t^k$ for any $\mu \in \kappa_W$.

Now we treat the case $n = p = 2$. By Artin-Schreier theory, there exists $x \in W$ such that $\sigma(x) = x + 1$. Recall that $\tau = \pi^2$ is a uniformizer of O_F. Given $k \geq 1$, let $g_k = (1+\tau^k(x+1))(1+\tau^k x)^{-1} \in A$. Choose a finite subset R of $O_W \backslash \mathfrak{m}_W$ such that $R + \mathfrak{m}_W = O_W$ and let $S = \{1 + r\tau^i \pi \mid r \in R, i = 0, 1\}$. We claim that the set $B := \{\mathrm{LT}((g_k, s)) \mid k \in \mathbb{N}, s \in S\}$ contains all homogeneous elements of $\mathrm{Lie}(G)$ of odd degree $d \geq 5$ (elements of $\mathrm{Lie}(G)$ of even degree lie in $\mathrm{Lie}_G(A)$ as before).

Fix $r \in R$, $i, k \in \mathbb{N}$, and let us compute the group commutator of the elements $h_{r,i} := 1 + r\tau^i \pi$ and g_k. Let $w = g_k - 1$ and $v = r\tau^i$. We have

$$(h_{r,i}, g_k) = (1 + v\pi)^{-1}(1 + w)^{-1}(1 + v\pi)(1 + w) =$$
$$1 + h_{r,i}^{-1}g_k^{-1}(v\pi\, w - wv\pi) = 1 + h_{r,i}^{-1}g_k^{-1} \cdot v(\sigma(w) - w)\pi.$$

Now $w = \dfrac{\tau^k}{1 + \tau^k x}$, whence

$$\sigma(w) - w = \frac{\tau^k}{1 + \tau^k x} - \frac{\tau^k}{1 + \tau^k(x + 1)} = \frac{\tau^{2k}}{(1 + \tau^k x)(1 + \tau^k(x + 1))}.$$

13

It is clear now that

$$\text{LT}\left((h_{r,i}, g_k)\right) = \text{LT}\left(1 + r\tau^{i+2k}\pi\right) = \bar{r}t^{2i+4k+1} \text{ where } \bar{r} = r + \mathfrak{m}_W.$$

Since every odd integer $d \geq 5$ is of the form $4k + 2i + 1$ with $i = 0$ or 1, we are done. $\qquad\square$

6   Appendix

Proof of Lemma 5.2. Let $s_1, \ldots, s_l$ be the elements of S listed on some order. For $i = 1, \ldots, l$ set $A_i = s_i^{-1} A s_i$.

Claim 6.1. *For every $g \in G$ of degree at least N and any $n \geq 1$ there exist elements $a_1 = a_1(g, n), \ldots, a_l = a_l(g, n), b_1 = b_1(g, n), \ldots, b_l = b_l(g, n)$ and $r = r(g, n)$ such that $g = b_1 a_1 b_2 a_2 \ldots b_l a_l r$, $a_i \in A_i$, $b_i \in A$ for $i = 1, \ldots, l$, and $r \in G_{n+1}$.*

Proof. Fix $g \in G$ with $\deg g \geq N$. We will prove the assertion by induction on n. If $n < N$, the claim is obvious (just set $a_i = b_i = 1$ for all i and $r = g$).

Now let n be arbitrary and suppose we constructed elements $a_1 = a_1(g, n - 1), \ldots, a_l = a_l(g, n - 1), b_1 = b_1(g, n - 1), \ldots, b_l = b_l(g, n - 1)$, and $r = r(g, n - 1)$ satisfying the required conditions. If $r \in G_{n+1}$, there is nothing to prove. Otherwise, let $w = \text{LT}(r)$. By assumption, either $w \in \text{Lie}_G(A)$ or $w = \text{LT}\left((a, s_i)\right)$ for some $a \in A$ and $i \leq l$. We treat the second case, the first one being even easier. There exists $r_1 \in G_{n+1}$ such that $r = a^{-1} s_i^{-1} a s_i r_1$. Let $q = b_1 a_1 \ldots b_{i-1} a_{i-1} b_i (r r_1^{-1}) a_i \ldots b_l a_l$. Since $g = b_1 a_1 b_2 a_2 \ldots b_l a_l r$ and $r \in G_n$, it is clear that $q \equiv g \mod G_{n+1}$. On the other hand, q can written as follows: $q = b_1' a_1' \ldots b_l' a_l'$, where $b_j' = b_j$, $a_j' = a_j$ for $j \neq i$; $b_i' = b_i a^{-1}$, $a_i' = s_i^{-1} a s_i a_i$. Clearly, $a_j' \in A_j$ and $b_j' \in A$ for $j = 1, \ldots, l$. The proof is complete. $\qquad\square$

It is now easy to finish the proof of Lemma 5.2. Apply the above claim with $g \in G_N$ fixed and $n \to \infty$. Since G is compact, there exists a sequence of integers $n_1 < n_2 < \ldots$ such that $a_i := \lim_{k \to \infty} a_i(g, n_k)$ and $b_i := \lim_{k \to \infty} b_i(g, n_k)$ exist for every i. Clearly, $a_i \in A_i, b_i \in A$, whence $G_N \subseteq A A_1 A A_2 \ldots A A_l$. Hence G is a product of $2l$ abelian subgroups and finitely many cyclic subgroups (generated by representatives of the cosets of G/G_N). $\qquad\square$

References

[Ab]   M. Abert, *Symmetric groups as products of abelian subgroups.* Bull. London Math Soc. 34 (2002), no. 4, 451–456.

[AV]   M. Abert and B. Virag, *Dimension and randomness in groups acting on rooted trees,* preprint.

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

[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.

[Bo]   N. Boston, *p-adic Galois representations and pro-p Galois groups.* New horizons in pro-p groups, 329-348, Progr. Math., 184, Birkhuser Boston, Boston, MA, 2000.

[Ca1]   R. Camina, *Subgroups of the Nottingham group.* J. Algebra 196 (1997), no. 1, 101–113.

[Ca2]   R. Camina, *The Nottingham group.* New horizons in pro-p groups, 205–221, Progr. Math., 184, Birkhuser Boston, Boston, MA, 2000.

[dSF]   M. P. F. du Sautoy, I. Fesenko, *Ramification groups and the Nottingham group.* New horizons in pro-p groups, 287–328, Progr. Math., 184, Birkhuser Boston, Boston, MA, 2000.

[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.

[F]   I. Fesenko, *On just infinite pro-p-groups and arithmetically profinite extensions of local fields.* J. Reine Angew. Math. 517 (1999), 61–80.

[Grif1]   C. Griffin, *Some hereditarily just infinite subgroups of the Nottingham Group,* to appear in J. Algebra.

[Grif2]   C. Griffin, *The Fesenko Groups have finite width,* preprint

[Grig]   R. Grigorchuk, *Just-infinite branch groups,* New horizons in pro-p groups, 125–185, Progr. Math., 184, Birkhuser Boston, Boston, MA, 2000.

[JZ]   A. Jaikin-Zapirain, *On linear just infinite pro-p groups.* J. Algebra 255 (2002), no. 2, 392–404.

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

[LM]   C. R. Leedham-Green and S. McKay, *On the classification of p-groups and pro-p groups.* New horizons in pro-p groups, 55–74, Progr. Math., 184, Birkhuser Boston, Boston, MA, 2000.

[P]   R. Pink, *Compact subgroups of linear algebraic groups.* J. Algebra 206 (1998), no. 2, 438–504.

[Ri]   C. Riehm, *The norm 1 group of $\mathfrak{p}$-adic division algebra.* Amer. J. of Math. 92 (1970), no. 2, 499-523.

[Sp]   T. A. Springer, *Linear algebraic groups.* Second edition. Progress in Mathematics, 9. Birkhuser Boston, Inc., Boston, MA, 1998.

[Sh]   A. Shalev, *Lie methods in the theory of pro-p groups.* New horizons in pro-p groups, 1–54, Progr. Math., 184, Birkhuser Boston, Boston, MA, 2000.

[Ti]   J. Tits, *Reductive groups over local fields.* Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1, pp. 29–69, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.

[Wil]   J. Wilson, *On just-infinite abstract and profinite groups.* New horizons in pro-p groups, 181-203, Progr. Math., 184, Birkhuser Boston, Boston, MA, 2000.

[Win]   J.- P. Wintenberger, *Extensions abeliennes et groupes d'automorphismes de corps locaux.* (French) C. R. Acad. Sci. Paris Sr. A-B 290 (1980), no. 5, A201–A203.