ACADEMIC
PRESS

Journal of Algebra 255 (2002) 392–404

JOURNAL OF
Algebra

www.academicpress.com

On linear just infinite pro-p groups [☆]

Andrei Jaikin-Zapirain

*Departamento de Matemáticas, Facultad de Ciencias, Universidad Autónoma de Madrid,
Cantoblanco Ciudad Universitaria, 28049 Madrid, Spain*

Received 29 October 2001

Communicated by Alex Lubotzky

1. Introduction

Interest on just infinite pro-p groups (i.e. infinite pro-p groups with only finite proper pro-p images) has grown steadily during the last few years, the most ambitious project in this area being the classification of the groups in this family. It is expected that, as in the classification of finite simple groups, except for some 'sporadic' groups, any just infinite pro-p group will lie into one of several well-defined families. However, this theory is still in its first stages and no precise conjectures have been posed by the moment. It is therefore natural to add some extra conditions and the one we choose in this work is linearity. We need first to give a precise meaning to a just infinite pro-p group being linear. According to the classical definition, to be linear means of course to be a subgroup of the full linear group of a given degree defined on a field, however this is not entirely appropriate for our purposes since it is does not take any advantage of the topological nature of a pro-p group. The following two definitions, notably the second one, are better suited in our context.

Definition. Let G be a pro-p group. We shall say that G is *linear* if it is linear over some commutative ring and that G is t*-linear* if it is a closed subgroup of $\mathrm{GL}_n(A)$ for some commutative profinite ring A.

[☆] This work has been supported by a grant of the Government of the Basque Country and by the DGICYT Grant PB97-0604.

E-mail address: andrei.jaikin@uam.es.

PII: S0021-8693(02)00024-8

Recall that if A is a commutative profinite ring then $\mathrm{GL}_n(A)$ is a profinite group, and if G is a finitely generated pro-p group and also a subgroup of $\mathrm{GL}_n(A)$ then G is automatically closed in $\mathrm{GL}_n(A)$ [1, Corollary 1.21]. Note that just infinite pro-p groups are finitely generated.

It seems reasonable that for pro-p groups in general t-linearity should be strictly stronger than linearity but no actual counterexamples are known. In [2] it has been conjectured that a non-abelian free pro-p group is not t-linear. By the moment we only know that it is not t-linear of degree 2 (see [3]) and it is not linear over $\mathbb{F}_p[\![t]\!]$ (see [4]). Yet, I suspect that this group is linear over some field. In this paper our main interest is focused on the following question posed by C.R. Leedham-Green.

Question. Is every linear just infinite pro-p group linear over $\mathbb{Z}_p$ or $\mathbb{F}_p[\![t]\!]$?

We have not been able to settle this question but we have proved that counterexamples, if they exist, must have some interesting properties. Note that soluble just infinite pro-p groups are linear over $\mathbb{Z}_p$. Therefore, our attention is devoted to insoluble just infinite pro-p groups. The following result will be very useful for us and is also of certain interest by itself.

Proposition 1.1. *Let G be a just infinite pro-p group. Then G is insoluble if and only if every non-trivial normal subgroup of G is open.*

So we see that insoluble just infinite pro-p groups are also just infinite as abstract groups. This fact was proved for the Nottingham group by B. Klopsch [5]. Recall that a pro-p group G is called hereditarily just infinite if every open subgroup of G is just infinite. If G is an insoluble pro-p group then every open subgroup is also insoluble and so Proposition 1.1 implies the following corollary.

Corollary 1.2. *Let G be an insoluble hereditarily just infinite pro-p group. Then G is hereditarily just infinite as an abstract group.*

If $x_1, \dots, x_n$ are elements in a ring, we define

$$s_n(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) x_{\sigma(1)} \dots x_{\sigma(n)},$$

where the sum is taken over all permutations of degree n and $\mathrm{sgn}(\sigma)$ is the sign of σ. We say that a ring satisfies the nth standard identity, or s_n for short, if $s_n(x_1, \dots, x_n) = 0$ for any elements $x_1, \dots, x_n$ in the ring. It is easy to prove that, for a commutative ring A, $\mathbb{M}_n(A)$ satisfies s_{n^2+1}. Actually, by the Amitsur–Levitzki Theorem, $\mathbb{M}_n(A)$ satisfies s_{2n}. If R is a ring we set $s_n(R)$ to be the ideal of R generated by $\{s_n(a_1, \dots, a_n) \mid a_1, \dots, a_n \in R\}$. Now we give a criterion for a just infinite pro-p group to be linear.

Theorem 1.3. *Let G be a just infinite pro-p group. Then G is linear if and only if $G \cap (1 + s_{2n}(\mathbb{Z}[G])) = \{1\}$ for some n. Moreover, in this case, G is linear over some field.*

Let Δ be the ideal of $\mathbb{Z}[G]$ generated by p and $\{g - 1 \mid g \in G\}$ and $\overline{s_{2n}(\mathbb{Z}[G])}$ the closure of $s_{2n}(\mathbb{Z}[G])$ in the Δ-adic topology of $\mathbb{Z}[G]$. Hence, $\overline{s_{2n}(\mathbb{Z}[G])} = \bigcap_{i\in\mathbb{N}}(s_{2n}(\mathbb{Z}[G]) + \Delta^i)$.

Theorem 1.4. *Let G be a just infinite pro-p group. Then the following conditions are equivalent*:

(i) *G is linear over $\mathbb{Z}_p$ or $\mathbb{F}_p[\![t]\!]$.*
(ii) *$G \cap (1 + \overline{s_{2n}(\mathbb{Z}[G])}) = \{1\}$ for some n.*

As a corollary of this theorem we obtain that t-linear just infinite pro-p groups are linear over $\mathbb{Z}_p$ or $\mathbb{F}_p[\![t]\!]$.

Corollary 1.5. *Let G be a t-linear just infinite pro-p group. Then G is a closed subgroup of of $\mathrm{GL}_m(\mathbb{Z}_p)$ or of $\mathrm{GL}_m(\mathbb{F}_p[\![t]\!])$ for some m.*

Another proof of this corollary is given in Section 4.

In view of Theorem 1.3 we define the following set $\mathbb{I}_n$ of ideals of $\mathbb{Z}[G]$: an ideal I belongs to $\mathbb{I}_n$ if it is maximal among the ideals J containing $s_{2n}(\mathbb{Z}[G])$ and satisfying $G \cap (1 + J) = \{1\}$. We will see that if G is an insoluble linear just infinite pro-p group and $I \in \mathbb{I}_n$ then $\mathbb{Z}[G]/I$ is a prime Noetherian PI ring. In the case when G is not t-linear we can say a bit more.

Theorem 1.6. *Let G be a just infinite pro-p group. If G is linear but not t-linear (linear over $\mathbb{Z}_p$ or $\mathbb{F}_p[\![t]\!]$), then there exists $n \geqslant 0$ such that for any $m \geqslant n$ the family $\mathbb{I}_m$ is not empty and for any $I \in \mathbb{I}_m$, $\mathbb{Z}[G]/I$ is a simple ring of finite dimension over its centre.*

In [6] the authors consider insoluble just infinite pro-p groups which are linear over $\mathbb{Z}_p$ and they prove that these groups are open compact subgroups of the groups of $\mathbb{Q}_p$-rational points of semisimple algebraic groups. What can we say about just infinite pro-p groups which are linear over $\mathbb{F}_p[\![t]\!]$? The results by Pink in [7] represent a breakthrough in the understanding of these groups. One of the immediate corollaries of this work is an analogue for $\mathbb{F}_p[\![t]\!]$-linear insoluble just infinite pro-p groups: any such group has an open subgroup which is isomorphic to an open compact subgroup of the group of $\mathbb{F}_p((t))$-rational points of a semisimple algebraic group. Here $\mathbb{F}_p((t))$ is the field of quotients of $\mathbb{F}_p[\![t]\!]$. In particular, $\mathbb{F}_p[\![t]\!]$-linear insoluble just infinite pro-p groups are $\mathbb{F}_p[\![t]\!]$-

analytic. The converse implication is proved in Section 5. Actually, assuming that R satisfies some natural conditions, we prove the following theorem.

Theorem 1.7. *Let G be an R-analytic just infinite pro-p group. Then G is linear over R (and so it is linear over $\mathbb{Z}_p$ or $\mathbb{F}_p[[t]]$).*

In Section 3 we consider the question of when a p-adic analytic pro-p group is linear over a field of positive characteristic. In [8, p. 30, Proposition 5.6] A. Shalev proved that a p-adic analytic pro-p group is linear over $\mathbb{F}_p[[t]]$ if and only if it is virtually abelian (it answers a question posed in [9]). The proof is based on Pink's characterization of closed subgroups of $\mathrm{GL}_n(\mathbb{F}_p[[t]])$. In this paper we prove the next result.

Theorem 1.8. *Let G be a p-adic analytic pro-p group. Then G is linear over a field of positive characteristic if and only if G is virtually abelian.*

The proof of this theorem is based on the properties of lattices in semisimple algebraic groups over local fields. This very nice idea, as well as the main steps of the proof, has been suggested to me by A. Lubotzky. I would like to thank him for drawing to my attention to this beautiful world of ideas.

Finally, in Section 4 we prove that a finitely generated t-linear pro-p group is linear over some commutative Noetherian local pro-p ring and we conjecture that two 'minimal' such rings have the same Krull dimension.

If R is a ring then $U(R)$ is the group of units of R. The derived series of a group is denoted by $\{G^{(k)}\}$. The rest of the notation is standard. We refer the reader to [1,6,10] for background on pro-p groups and to [11] for background on PI rings. If G is finite p-subgroup of $\mathrm{GL}_n(K)$, for some field K, then the derived length of G is at most n. We shall use several times these facts, sometimes without mentioning them explicitly.

2. Proofs of the main results

We begin this section with the proof of Proposition 1.1.

Proof of Proposition 1.1. Suppose G is insoluble and let H be a normal subgroup and T its closure in G. Then T is an open subgroup and there exist elements $h_1,\dots,h_d \in H$ such that $T = \overline{\langle h_1,\dots,h_d\rangle}$. Since G is insoluble, $[T,T]$ is open in G. By using the same argument as in the proof of [1, Proposition 1.19], we obtain that $[T,T] = \{[t_1,h_1]\dots[t_d,h_d] \mid t_1,\dots,t_d \in T\}$, whence $[T,T] \leqslant H$ and H is open in G.

Now suppose that G is soluble. Then G has an abelian normal open subgroup A. We pick any non-identity element a in A and take H to be the smallest normal subgroup in G containing a. The $\mathbb{Z}$-rank of H is clearly finite, so H cannot be open. □

Lemma 2.1. *Let R be a ring and G an insoluble just infinite pro-p group contained in $U(R)$. Then for any nilpotent ideal I of R, $G \cap (1 + I) = \{1\}$.*

Proof. Suppose $G \cap (1 + I) \neq \{1\}$. Then by Proposition 1.1, this intersection is an open subgroup of G and since I is nilpotent, it is a nilpotent subgroup. But then G has to be soluble, which is a contradiction. □

We shall need the following two results about PI rings.

Proposition 2.2 [11, Theorem 13.6.4]. *Let R be a semiprime PI ring with centre $Z(R)$ and J a non-trivial ideal of R. Then, $J \cap Z(R) \neq \{0\}$.*

The next proposition is an easy consequence of [11, Theorem 13.4.2].

Proposition 2.3. *Let R be a prime PI ring satisfying a polynomial identity of degree $2n$. Then there exists an embedding, preserving the identity, $R \subseteq \mathbb{M}_{n!}(A)$, where A is a field.*

Now, we are able to prove the next theorem.

Proof of Theorem 1.3. Suppose first that G is linear. Then G is a subgroup of $\mathrm{GL}_n(A)$ for some commutative ring A. Hence we can construct a ring homomorphism $\phi : \mathbb{Z}[G] \to \mathbb{M}_n(A)$, such that $G \cap (1 + \ker\phi) = \{1\}$. Since $s_{2n}(\mathbb{Z}[G]) \subseteq \ker\phi$, the 'only if' part of the theorem is proved.

Now suppose $G \cap (1 + s_{2n}(\mathbb{Z}[G])) = \{1\}$ for some n. If G is soluble then G is linear over $\mathbb{Z}_p$ and we are done, so without loss of generality we can suppose that G is not soluble. By using Zorn's Lemma, we obtain that there exists an ideal I which is maximal with respect to the properties $s_{2n}(\mathbb{Z}[G]) \subseteq I$ and $G \cap (1 + I) = \{1\}$. Put $R = \mathbb{Z}[G]/I$ and identify G with a subgroup of the group of units of R. By Lemma 2.1, R contains no non-trivial nilpotent ideals which implies by [11, Corollary 0.2.7] that R is semiprime. Now, let $J \neq \{0\}$ be an ideal of R. Since $H = G \cap (1 + J) \neq \{1\}$, Proposition 1.1 yields that H is an open subgroup of G and so R/J is Noetherian. It is now clear that R satisfies the ascending chain condition on ideals, which enables us apply [11, Theorem 2.15] and conclude that R has only finitely many minimal prime ideals. By Proposition 1.1 we obtain that $\{0\}$ is the unique minimal prime ideal of R, that is, R is prime. The result follows now from Proposition 2.3. □

Remark 2.4. Note also that the ring R in the last proof not only is prime, but also Noetherian by [11, Theorem 13.6.15].

The proof of Theorem 1.4 requires the following lemma.

Lemma 2.5. *Let G be a just infinite pro-p group and K a closed ideal of $\mathbb{F}_p[\![G]\!]$ such that $G \cap (1+K) = \{1\}$. Then there exists a closed ideal I containing K maximal with respect to the property $G \cap (1+I) = \{1\}$.*

Proof. All we have to do is to explain why Zorn's Lemma can be applied here. We take an ascending chain of closed ideals of $\mathbb{F}_p[\![G]\!]$ containing K, $\{I_k\}$, such that $G \cap (1+I_k) = \{1\}$ for all indices k and claim that the closure J of the union of the ideals in the chain also satisfies the additional condition $G \cap (1+J) = \{1\}$. Indeed, otherwise the ring $\mathbb{F}_p[\![G]\!]/J$ would be finite, whence J would be finitely generated as, say left, $\mathbb{F}_p[\![G]\!]$-module. We take the unique maximal ideal M of $\mathbb{F}_p[\![G]\!]$ and note that $J = I_k + MJ$ for some k. But then, by Nakayama's Lemma, $I_k = J$, which is a contradiction. □

Proof of Theorem 1.4. The proof that (i) follows from (ii) is as in the previous theorem.

We assume now that (ii) holds and, without loss of generality, that G is insoluble. Let Λ be the completion of $\mathbb{Z}[G]/\overline{s_{2n}(\mathbb{Z}[G])}$ in the $\Delta/\overline{s_{2n}(\mathbb{Z}[G])}$-adic topology. If $\overline{\Lambda} = \Lambda/p\Lambda$ is finite then Λ is finitely generated as $\mathbb{Z}_p$-module and so G is linear over $\mathbb{Z}_p$. So, we can suppose that $\overline{\Lambda}$ is infinite. In this case, G is embedded in $U(\overline{\Lambda})$, and by Lemma 2.5, there exists a closed ideal I of $\overline{\Lambda}$ satisfying $G \cap (1+I) = \{1\}$ and maximal with this property. Put $R = \overline{\Lambda}/I$ and let $\overline{\Delta}$ be the unique maximal ideal of R. We regard G as a subgroup of $U(R)$.

The ring R is semiprime because if L is a nilpotent ideal of R, so is its closure, which must be trivial by Lemma 2.1 and the maximality of I. Thus Proposition 2.2 can be applied to pick a non-zero element z in $\overline{\Delta} \cap Z(R)$. We claim that the annihilator of z is trivial. Actually, any non-trivial closed ideal contains a power of z but no power of z annihilates z itself because R is semiprime, hence the only possibility for the annihilator of z is to be trivial. Now, we set K to be the ideal $\bigcap_{i\in\mathbb{N}} z^i R$. If $K \neq \{0\}$ a power of z, say z^k, lies in K and then $z^k = az^{k+1}$ for some $a \in R$. But this is impossible because the annihilator of z is trivial and z is not invertible. Therefore $K = \{0\}$. Now, R/zR is finite so R is a finitely generated free $\mathbb{F}_p[\![z]\!]$-module and this implies that G is linear over $\mathbb{F}_p[\![t]\!]$. □

Proof of Corollary 1.5. As we will see in Section 4 we can suppose that A is a pro-p ring. The inclusion map $G \subseteq \mathbb{M}_n(A)$ can be extended to $\mathbb{Z}[G]$ and this extension is continuous map if $\mathbb{Z}[G]$ is endowed with the Δ-adic topology. This implies that $\overline{s_{2n}(\mathbb{Z}[G])}$ maps to zero, which allows as to appeal to the implication (ii) ⇒ (i) of Theorem 1.4 to obtain the conclusion desired. □

Proof of Theorem 1.6. By way of contradiction, suppose that $R = \mathbb{Z}[G]/I$ is not simple for some $I \in \mathbb{I}_m$. We have seen in the proof of Theorem 1.3, that R

is prime. We consider G as a subgroup of $U(R)$. Since R is not simple, there exists a proper non-zero ideal J of R contained in the ideal of R generated by $\{g-1 \mid g \in G^{(n!+1)}\}$ and by Proposition 2.2, we can take $0 \neq z \in J \cap Z(R)$. The element z enjoys following properties:

(i) For any proper ideal K of R there exists $l \in \mathbb{N}$ such that $z^l \in K$.
(ii) $\bigcap_{i\in\mathbb{N}} z^i R = \{0\}$.

We prove now these claims.

(i) Let K_1/K be the prime radical of R/K. By the construction of R, $H = G \cap (1+K_1)$ is not trivial and is open in G. Since R/K_1 is a semiprime PI ring we obtain, by Proposition 2.3, that R/K_1 can be embedded in $\prod_i \mathbb{M}_{n!}(A_i)$, where each A_i is a field. Hence $(G/H)^{(n!+1)} = \{1\}$, that is, $G^{(n!+1)} \leqslant H$. But this means that $J \subseteq K_1$ and, in particular, $z \in K_1$. Since K_1/K is the prime radical of R/K, there exists $l \in \mathbb{N}$ such that $z^l \in K$.

(ii) Since R is prime, the annihilator of z is trivial. Hence, as in the proof of Theorem 1.4, we obtain that $\bigcap_{i\in\mathbb{N}} z^i R = \{0\}$.

Now we want to show that $L = \bigcap_{i\in\mathbb{N}} p^i R = \{0\}$. Indeed, if this is not the case, each $P_i = G \cap (1+z^i L)$ is an open subgroup of G and not all of them are equal because their intersection reduces in fact to $\{1\}$. So for some j there exists an element $g = 1 + z^j x \in P_j \setminus P_{j+1}$, where $x \in L$. Take l such that $g^{p^l} \in P_{j+1}$. Then $p^l x = zy$ for some $y \in L$. But it is clear from the definition of L that $p^l L = L$ and the annihilator of p^l is trivial, because R is prime, thus multiplication by p^l induces a bijection of L, and the equality $p^l x = zy$ implies that $x \in zL$, which is a contradiction because $g \notin P_{j+1}$. Hence $L = \{0\}$.

We set $H = G \cap (1+Rz)$. Now we reach the final contradiction both in the cases $pR = \{0\}$ and $pR \neq \{0\}$. In the former case, since R/Rz is a quotient of $\mathbb{F}_p[G/H]$, it follows that $\overline{\Delta}^k \subseteq Rz$ for some $k \in \mathbb{N}$. But $\bigcap_{i\in\mathbb{N}} Rz^i = \{0\}$, so I is closed in $\mathbb{Z}[G]$ with respect to the Δ-adic topology. Hence $\overline{s_{2m}(\mathbb{Z}[G])} \subseteq I$ and $G \cap (1+\overline{s_{2m}(\mathbb{Z}[G])}) = \{1\}$ which, by Theorem 1.4, means that G is linear over $\mathbb{Z}_p$ or $\mathbb{F}_p[\![t]\!]$, against the hypothesis. Finally, if $pR \neq \{0\}$, then $\overline{\Delta}^k \subseteq pR$ for some $k \in \mathbb{N}$ and, since $\bigcap_{i\in\mathbb{N}} p^i R = \{0\}$, I is closed which leads to the same contradiction as before. We conclude that R is simple and, since it is a PI ring, it is of finite dimension over its centre. □

3. Linear pro-p groups over fields of characteristic p

Most of results in the previous section can be reformulated considering linearity over rings of characteristic $s > 0$. This is for instance the analogue of Theorem 1.3 in this new context.

Theorem 3.1. *Let G be a just infinite pro-p group. Then G is linear over a ring of characteristic s if and only if $G \cap (1 + s_{2n}(\mathbb{F}_s[G])) = \{1\}$ for some n. Moreover, in this case G is linear over some field of characteristic s.*

Now, we prove Theorem 1.8. The proof uses non-trivial tools related with the Margulis super-rigidity theorem. We refer the reader to [12,13] for the definitions and basic results.

Proof of Theorem 1.8 (A. Lubotzky). The 'if' part of the theorem is clear, because a virtually abelian pro-p group contains $\mathbb{Z}_p^n$ as a subgroup of finite index and $\mathbb{Z}_p^n$ can be embedded in $\mathbb{F}_p[\![t]\!]^*$.

Now, we shall prove the 'only if' part of the theorem by way of contradiction. So, we suppose that G is linear over some field of characteristic $s > 0$ and also that G is not virtually abelian. We split the proof in a number of steps.

Step 1. Every soluble subgroup S of G is virtually abelian.

Obviously, we can assume that S is a closed subgroup of G. From the structure of pro-p groups of finite rank we know that S has a soluble torsion-free subgroup H of finite index which, by the Kolchin–Malcev Theorem [14, Theorem 3.6], is virtually triangular, i.e. it has a subgroup of finite index K conjugated to a subgroup of the group of invertible triangular matrices. The commutator subgroup of this group (the unitriangular group) is an s-group, so K' must be trivial. Hence S is virtually abelian.

Step 2. We may assume that G is an open subgroup of the group of $\mathbb{Q}_p$-rational points of $\mathbf{SL}_1(D)$, where D is a finite-dimensional division $\mathbb{Q}_p$-algebra.

We can embed G in $\mathrm{GL}_n(\mathbb{Z}_p)$ and consider the Zariski closure of G, which we call $\mathbf{G}$. Define by $\mathbf{G}(\mathbb{Q}_p)$ the group of $\mathbb{Q}_p$-rational points of $\mathbf{G}$. Let $\mathbf{G}^0$ be the connected component of $\mathbf{G}$. Since $\mathbf{G}^0(\mathbb{Q}_p) \cap G$ is open in G, without loss of generality we can assume that $\mathbf{G}$ is connected.

Now, $\mathbf{G}$ is defined over $\mathbb{Q}_p$, whence there exists a semisimple $\mathbb{Q}_p$-subgroup $\mathbf{L} \subseteq \mathbf{G}$ such that $\mathbf{G} = \mathbf{L}R(\mathbf{G})$ ($R(\mathbf{G})$ is the radical of $\mathbf{G}$). If $\mathbf{L}$ is trivial, then G is soluble, and so, we obtain a contradiction from Step 1. Therefore, we can assume that $\mathbf{L}$ is not trivial.

The intersection $G \cap \mathbf{L}(\mathbb{Q}_p)$ is an open subgroup of $\mathbf{L}(\mathbb{Q}_p)$. Therefore, we can suppose that $\mathbf{G}$ coincides with $\mathbf{L}$. Next, a minimal connected normal subgroup of $\mathbf{G}$ is almost simple, and $\mathbf{G}$ is an almost direct product of its minimal connected normal subgroups, whence without loss of generality we can assume that $\mathbf{G}$ is almost simple. Changing $\mathbf{G}$ by its universal covering, we may also assume that $\mathbf{G}$ is simply connected.

From the first step we know that every soluble subgroup of G is virtually abelian. Using this and that G is open in $\mathbf{G}(\mathbb{Q}_p)$, we obtain that every connected soluble $\mathbb{Q}_p$-subgroup of $\mathbf{G}$ is abelian. Hence $\mathbf{G}$ is $\mathbb{Q}_p$-anisotropic. But we know (see, for example, [13, Theorem 6.5]) that this implies that $\mathbf{G} = \mathbf{SL}_1(D)$ for some finite-dimensional division $\mathbb{Q}_p$-algebra D.

Step 3. There exists a finite-dimensional division $\mathbb{Q}$-subalgebra E of D, such that $D = E\mathbb{Q}_p$.

Let K be the center of D, R its ring of integers, P the maximal ideal of R and q the order of residue class field $\overline{R} = R/P$. The index m of D is defined by means of $m^2 = |D : K|$. Let W be the unique maximal unramified extension of K of degree m. Then $W = K(w)$, where w is a primitive $(q^m - 1)$th root of unity over K. The Galois group $\mathrm{Gal}(W/K)$ is cyclic of order m, and has a canonical generator, namely, the Frobenius automorphism σ of W/K. Recall that σ is defined by the equation $\sigma(w) = w^q$. There exists a global field $F \subset K$, such that $K = F\mathbb{Q}_p$ (see, for example, [15, Exercise 17.9.2]). Hence we can find a generator π of P lying in F. It is known that W can be embedded in D, and that there exists an element $z \in D^*$ such that

$$D = \sum_{j=0}^{m-1} Wz^j, \quad \text{where } a^z = \sigma^r(a),\ a \in W,\ \text{and } z^m = \pi.$$

Put $E = \sum_{j=0}^{m-1} F(w)z^j$. We have $D = E\mathbb{Q}_p$ and E is a finite-dimensional division $\mathbb{Q}$-algebra.

As a consequence of the last step we obtain that G is an open subgroup of the group of K-rational points of the non-commutative absolutely almost simple F-group $\mathbf{H} = \mathbf{SL}_1(E)$.

Now, let $\mathcal{R}$ be the set of all (inequivalent) valuations of the field F, and let $\mathcal{R}_\infty \subset \mathcal{R}$ be the set of all Archimedean valuations of F. Denote by F_v the completion of the field F with the respect to the valuation $v \in \mathcal{R}$. If $S \subset \mathcal{R}$, then the ring

$$\bigl\{x \in F \bigm| |x|_v \leqslant 1 \text{ for all } v \in \mathcal{R} \setminus (\mathcal{R}_\infty \cup S)\bigr\}$$

of S-integral elements of F will be denoted by $F(S)$. Let $\Gamma = \Gamma(\mathbf{H})$ be the set of valuations v such that $\mathbf{H}$ is anisotropic over F_v (we know that this set is finite) and let $v_1, v_2 \notin \Gamma$.

Step 4. If $S = \{v_1, v_2\} \cup \mathcal{R}_\infty \setminus \Gamma$, then $\mathbf{H}(F(S))$ is not linear over any field of positive characteristic.

This step follows directly from Theorem 3(ii) of [12, p. 4] bearing in mind that $\mathbf{H}(F(S))$ is an irreducible lattice in $H_S = \prod_{v \in S} \mathbf{H}(F_v)$, rank $H_S \geqslant 2$ and for no $v \in S$ the group $\mathbf{H}$ has a nontrivial F_v-anisotropic factor.

Step 5. G is not linear over any field of positive characteristic.

Note that $F(S) \subset R$ and $\mathbf{H}(R)$ is compact and open in $\mathbf{H}(K)$ (moreover, $\mathbf{H}(K)$ is itself compact). Hence $G \cap \mathbf{H}(F(S))$ is of finite index in $\mathbf{H}(F(S))$. From the previous step we conclude that G is not linear over any field of positive characteristic. □

4. Linear dimension of finitely generated t-linear pro-p groups

First of all we prove the result mentioned in the proof of the Corollary 1.5.

Theorem 4.1. *Let G be a finitely generated t-linear pro-p group. Then G is linear over some commutative Noetherian local pro-p ring.*

Proof. Let A be a profinite ring and $G \leqslant \mathrm{GL}_n(A)$. For each prime number q define the subring $A_q = \{x \in A \mid \lim_{n\to\infty} q^n x = 0\}$. Then $A = \prod_q A_q$ and $\mathrm{GL}_n(A) = \prod_q \mathrm{GL}_n(A_q)$. Now let G_q be the image of G in $\mathrm{GL}_n(A_q)$ under the qth projection map and J_q is intersection of all open maximal ideals of A_q. It is easy to see that J_q coincides with the Jacobson radical of A_q. Now suppose that $q \neq p$. If $g \in 1 + \mathbb{M}_n(J_q)$ then $\lim_{n\to\infty} g^{q^n} = 0$ and so $G_q \cap (1 + \mathbb{M}_n(J_q))$ is trivial. Hence G_q can be embedded in $\prod_i \mathrm{GL}_n(K_i)$, where K_i are finite fields of characteristic q. Let F_i be the image of G_q in $\mathrm{GL}_n(K_i)$ under the ith projection map. It is well known that F_i has an abelian subgroup A_i of index at most f, which depends only on n. The rank of A_i is at most n and so A_i has a faithful representation of degree n over $\mathbb{Z}_p[w_i]$, where w_i is an n_ith root of unity for n_i the exponent of group A_i. Therefore F_i has a faithful representation of degree nf over $\mathbb{Z}_p[w_i]$. Hence G_q is linear of degree nf over $\prod_i \mathbb{Z}_p[w_i]$ and so $G \leqslant \prod G_q$ is linear over some pro-p ring.

We are left to deal with the case when A is pro-p ring. Let J be the Jacobson radical of A and put $H = G \cap (1 + \mathbb{M}_n(J))$. Since G/H can be embedded in $\prod_i \mathrm{GL}_n(K_i)$, where K_i are finite fields of characteristic p, G/H is finite.

Since $H \leqslant 1 + \mathbb{M}_n(J)$, $H = \overline{\langle 1 + b_1, \ldots, 1 + b_s\rangle}$, where $b_i \in \mathbb{M}_n(J)$. Let $\{a_j \mid j = 1, \ldots, k\}$ be the set of elements of A which appear in the matrices b_i, R the subring of A generated by $\{a_1, \ldots, a_k\}$ and B the closure of R in A. Define a homomorphism $\phi : \mathbb{Z}[t_1, \ldots, t_k] \to A$ by means of $\phi(t_i) = a_i$. Let M be the ideal of $\mathbb{Z}[t_1, \ldots, t_k]$ generated by $p, t_1, \ldots, t_k$. Then ϕ is a continuous map if $\mathbb{Z}[t_1, \ldots, t_k]$ has the M-adic topology. Therefore we can extend ϕ to $\mathbb{Z}_p[[t_1, \ldots, t_k]]$.

We want to prove that $\phi(\mathbb{Z}_p[[t_1, \ldots, t_k]]) = B$ and, in particular, B is a Noetherian local pro-p ring. Since $\mathbb{Z}_p[[t_1, \ldots, t_k]]$ is compact and ϕ is a continuous map, $\phi(\mathbb{Z}_p[[t_1, \ldots, t_k]])$ is closed. Hence

$$B = \overline{R} = \overline{\phi(\mathbb{Z}[t_1, \ldots, t_k])} \subseteq \phi\big(\mathbb{Z}_p[[t_1, \ldots, t_k]]\big).$$

The converse inclusion is obvious.

Now H is of finite index in G, so G is also linear over B. □

Let A be a commutative Noetherian local pro-p ring and G a pro-p group. We will say that a homomorphism $\phi : G \to \mathrm{GL}_n(A)$ is *minimal* if ϕ is faithful and for every non-trivial ideal I of A the intersection of $\phi(G)$ and $1 + \mathbb{M}_n(I)$ is different from 1. In this case we write $d(\phi)$ for the Krull dimension of A. If $d(\phi)$ is constant for every minimal homomorphism ϕ, we call this constant number the linear dimension of the group G and we denote it simply by $\dim_{\mathrm{l}} G$.

Conjecture 1. Every finitely generated t-linear pro-p group has linear dimension.

At this moment we can prove this conjecture only for insoluble t-linear just infinite pro-p groups.

Theorem 4.2. *Let G be an insoluble t-linear just infinite pro-p group. Then* $\dim_{\mathrm{l}} G = 1$.

Proof. Let $\phi : G \to \mathrm{GL}_n(A)$ be a minimal homomorphism. By Lemma 2.1 A is semiprime. Let Q be an element of $\phi(G^{(n+1)})$ different from the identity matrix I_n and a an element of the matrix $Q - I_n$ different from 0. Consider a maximal ideal J of A which does not intersect $\{a^k \mid k \in \mathbb{N}\}$. It is well known that J is a prime ideal of A. Let $\overline{G}$ be the image of G in $\mathrm{GL}_n(A/J)$. If $\overline{G}$ is finite, then $\overline{G}^{(n+1)} = \{1\}$ which contradicts $a \notin J$. Hence $\overline{G}$ is infinite and so $J = \{0\}$.

The ring A satisfies the following property: every ideal of A contains a power of some fixed element (in our case the element a). Rings with this property are known to have Krull dimension 1 (see [16, Theorem 146]), so our theorem is proved. □

5. Analytic just infinite pro-p groups

Let R be a commutative Noetherian local pro-p ring and $\mathfrak{m}$ its maximal ideal. We assume that the associated graded ring $\mathrm{gr}(R) = \bigoplus_{n=0}^{\infty} \mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an integral domain. The concept of an R-analytic group is defined in [1, Chapter 13], where it is shown that every such group contains an open subgroup which is R-*standard*. To recall what this means, let G be an R-standard group. Then the underlying set of G may be "identified" with the cartesian product $(\mathfrak{m}^l)^{(d)}$ of d copies of $\mathfrak{m}^l$, for some $l \in \mathbb{N}$. The number $d \geqslant 0$ is the *dimension* of G. The group operation is given by a *formal group law*, i.e. a d-tuple $\mathbf{F} = (F_1, \ldots, F_d)$ of power series over R in $2d$ variables, as follows: for all $\mathbf{x}, \mathbf{y} \in G = (\mathfrak{m}^l)^{(d)}$ we have

$$\mathbf{x} \cdot \mathbf{y} = \bigl(F_1(\mathbf{x}, \mathbf{y}), \ldots, F_d(\mathbf{x}, \mathbf{y})\bigr).$$

The neutral element of G is $(0, \ldots, 0)$.

Proposition 5.1. *Let G be an R-standard group. Then $G/Z(G)$ is linear over R.*

Proof. Let d be the dimension of G. Since G is identified with $(\mathfrak{m}^l)^{(d)}$, $A = R[\![x_1,\dots,x_d]\!]$ can be considered as a subring of the ring of functions from G to R. Define on A a structure of $R[G]$-module by putting $(a\cdot\mathbf{y})(\mathbf{x}) = a(\mathbf{yxy}^{-1})$, where $a\in A$ and $\mathbf{x},\mathbf{y}\in G$. For $\alpha=(\alpha_1,\dots,\alpha_d)$, where each α_i is a non-negative integer, put $|\alpha| = \sum\alpha_i$. Since the group operation in G is given by a formal group law, there exist $f_{i,\alpha}\in R[\![y_1,\cdots,y_d]\!]$ such that

$$x_i\cdot\mathbf{y} = x_i + \sum_{|\alpha|\geqslant 1} f_{i,\alpha}(\mathbf{y})x_1^{\alpha_1}\dots x_d^{\alpha_d}.$$

Let K be the ideal of $R[\![y_1,\dots,y_d]\!]$ generated by $W=\{f_{i,\alpha}\}$. Since $R[\![y_1,\dots,y_d]\!]$ is Noetherian, there is a finite subset V of W which generates K. Denote by m the maximum of $|\alpha|$ when $f_{i,\alpha}\in V$. Let $I=\sum x_iA$. Then for any $n\in\mathbb{N}$, I^n is an $R[G]$-submodule of A. If $\mathbf{y}\in G$ acts trivially on I/I^{m+1} then $f(\mathbf{y})=0$ for every $f\in V$ and so $f(\mathbf{y})=0$ for every $f\in K$. Hence $x_i\cdot\mathbf{y}=x_i$ for $i=1,\dots,d$, which means $\mathbf{y}\in Z(G)$. □

Proof of Theorem 1.7. Let $H\leqslant_o G$ be an R-standard group and put $N=\bigcap_{g\in G}H^g$. It is clear that N is also an open subgroup of G. Since N is normal and closed, so is $Z(N)$. If $Z(N)$ is open then G is soluble, and so p-adic analytic, hence R is finite extension of $\mathbb{Z}_p$ (see, for example, [1]), whence G is linear over R. Suppose now that $Z(N)$ is trivial. Then $N\cap Z(H)=\{1\}$ and so by Proposition 5.1, N is linear over R. Since N is of finite index in G, G is also linear over R. □

Note added in proof

Conjecture 1 is not true as the following example shows. Let $G = \mathrm{SL}_2^1(\mathbb{F}_p[\![t_1,t_2,t_3]\!])$. Then the natural embedding $\phi: G\to \mathrm{GL}_2(\mathbb{F}_p[\![t_1,t_2,t_3]\!])$ is minimal. On the other hand, by Remark VII.10.4 of O. Zariski and P. Samuel ("Commutative Algebra," Vol. II), we can embed $\mathbb{F}_p[\![t_1,t_2,t_3]\!]$ into $\mathbb{F}_p[\![s_1,s_2]\!]$. This embedding induces another minimal representation $\psi: G\to\mathrm{GL}_2(\mathbb{F}_p[\![s_1,s_2]\!])$. Hence G does not have linear dimension.

Acknowledgments

I would like to thank C.R. Leedham-Green for suggesting me the study of these groups and for his fruitful conversations. Part of this work was done during my visit to the Queen Mary College and I would like to thank the School of

Mathematical Sciences for its hospitality. I also wish to thank J. Sangroniz and D. Segal for some helpful comments on a preliminary version of this work.

References

[1] J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal, Analytic Pro-p Groups, 2nd ed., Cambridge University Press, Cambridge, UK, 1999.
[2] A. Lubotzky, A. Shalev, On some Λ-analytic pro-p groups, Israel J. Math. 85 (1994) 307–337.
[3] A.N. Zubkov, Non-abelian free pro-p groups cannot be represented by-2-by-2 matrices, Sibirsk. Math. Zh. 28 (1987) 64–69, English translation Siberian Math. J. 28 (1987) 742–747.
[4] Y. Barnea, M. Larsen, A non-abelian free pro-p group is not linear over local field, J. Algebra 214 (1999) 338–341.
[5] B. Klopsch, Normal subgroups in substitution groups of formal power series, J. Algebra 228 (2000) 91–106.
[6] G. Klaas, C.R. Leedham-Green, W. Plesken, Linear Pro-p Groups of Finite Width, Springer-Verlag, Berlin, 1997.
[7] R. Pink, Compact subgroups of linear algebraic groups, J. Algebra 206 (1998) 438–504.
[8] M. du Sautoy, D. Segal, A. Shalev (Eds.), New Horizons in Pro-p Groups, Birkhäuser, Basel, 2000.
[9] A. Shalev, Subgroup structure, fractal dimension, and Kac–Moody algebras, in: Trends in Mathematics, Birkhäuser, Basel, 1998, pp. 163–176.
[10] J.S. Wilson, Profinite Groups, Oxford University Press, Oxford, UK, 1998.
[11] J.C. McConnell, J.C. Robson, Noncommutative Noetherian Rings, Wiley, New York, 1987.
[12] G.A. Margulis, Discrete Subgroups of Semisimple Lie groups, Springer-Verlag, Berlin, 1991.
[13] V. Platonov, A. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, San Diego, 1994.
[14] B.A.F. Wehrfritz, Infinite Linear Groups, Springer-Verlag, Berlin, 1973.
[15] R.S. Pierce, Associative Algebras, Springer-Verlag, Berlin, 1982.
[16] I. Kaplansky, Commutative Rings, Allyan and Bacon, Boston, 1970.