Invent. math. 104, 521–533 (1991)

Inventiones mathematicae

On groups of polynomial subgroup growth

Alexander Lubotzky and Avinoam Mann
Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel

Oblatum 1-VII-1989 & 7-VI-1990

Summary. Let Γ be a finitely generated group and $a_n(\Gamma)$ = the number of its subgroups of index n. We prove that, assuming Γ is residually nilpotent (e.g., Γ linear), then $a_n(\Gamma)$ grows polynomially if and only if Γ is solvable of finite rank. This answers a question of Segal. The proof uses a new characterization of p-adic analytic groups, the theory of algebraic groups and the Prime Number Theorem. The method can be applied also to groups of polynomial word growth.

Introduction

Given a group Γ, let $a_n(\Gamma)$ be the number of subgroups of index n in Γ. If Γ is finitely generated, which we shall always assume, then $a_n(\Gamma) < \infty$ for every n. In recent years there has been a fair amount of interest in the properties of the number theoretic function $n \to a_n(\Gamma)$. Most notably, the work of Grunewald et al. [GSS], who associated a Dirichlet series $\zeta_\Gamma(s) = \sum_{n=1}^{\infty} a_n(\Gamma) n^{-s}$ with Γ and studied its properties when Γ is nilpotent.

A basic problem, raised explicitly by Segal [Sg], is to determine for what groups Γ, the sequence $a_n(\Gamma)$ has polynomial growth. This is equivalent to $\zeta_\Gamma(s)$ having a non-trivial domain of convergence. Or equivalently, $\alpha(\Gamma) < \infty$ when $\alpha(\Gamma)$ is defined as:

$$\alpha(\Gamma) = \limsup_n \frac{\log a_n(\Gamma)}{\log n}$$

If this is the case we say that Γ is a *group of polynomial subgroup growth* (a *PSG*-group, for short).

The problem to determine the *PSG*-groups makes sense, of course, only under the assumption that Γ is residually finite, i.e., the intersection of its finite index (normal) subgroups is trivial. In this paper we answer this problem under a somewhat stronger assumption:

Theorem A *Let Γ be a residually nilpotent finitely generated group. Then Γ has polynomial subgroup growth if and only if Γ is solvable of finite rank.*

In a forthcoming paper [LMS] we solve the general problem by showing that the words "residually nilpotent" in Theorem A can be replaced by "residually finite". This proof is based on the results of the present paper and of [MS].

The unexplained notions in the theorem are explained in the text. Theorem A was proved by Segal [Sg] under the additional assumption that Γ is solvable. We actually prove the difficult part of Theorem A by reducing it to Segal's case, the other part is included in Segal's. This is done in several stages: We give a new characterization of p-adic compact Lie groups:

Theorem B *A pro-p group G is a p-adic Lie group if and only if it has polynomial subgroup growth.*

Theorem B enables us, along the lines of [Lu1] to prove that a residually-p *PSG*-group is linear over $\mathbf{C}$, i.e., a subgroup of $GL_n(\mathbf{C})$ for some n.

We then prove:

Theorem C *A finitely generated linear group of polynomial subgroup growth is virtually solvable (of finite rank).*

Of course, Theorem C follows easily from Theorem A, since every linear group (in every characteristic) is virtually residually-p for some prime p (and hence virtually residually nilpotent). We isolated it for its importance and since the case of a linear group over a field of characteristic zero plays a central role: We prove this case first and then Theorem A is deduced from it (and Segal's Theorem) using Theorem B. It then follows that Theorem C holds for fields of any characteristic.

The proof of Theorem C uses first some basic results about algebraic groups to make a reduction to subgroups of $\mathrm{GL}_n(\mathbf{Q})$. Then, strong approximation results (of Nori [N] or Mathews et al. [MVW]) are applied with a counting argument to deduce the theorem. In this counting argument the prime number theorem (in a weak form) is used in an essential way.

Our main result (Theorem A) recalls the celebrated result of Gromov [Gr] on groups of polynomial growth in the sense of counting words. It is interesting to observe that while Gromov uses a variant of Hilbert's 5th problem (the characterization of real Lie groups) we are using the p-adic analogue. In both instances this is used to reduce the problem to the case of linear groups. Moreover, our method can be used to reprove Gromov's result for the special case of residually nilpotent groups.

Theorem D *Let Γ be a finitely generated residually nilpotent group generated by a finite set B. Let $b_n(\Gamma)$ be the number of elements of Γ which can be written as words of length at most n on the generators in B. Assume $b_n(\Gamma)$ grows polynomially. Then Γ is virtually nilpotent.*

In §1 we prove Theorems B and D. From Theorem B we deduce that a residually nilpotent group of polynomial subgroup growth is linear. This corollary, together with Theorem C, which is proved in §2, imply Theorem A (with the help of Segal's Theorem 0.3).

Acknowledgements. The authors are grateful to J. Bernstein, D. Segal and T. Tamagawa for several useful conversations and especially to A. Borel for detailed comments which greatly improved the exposition of this paper.

0 Notations, conventions and some preliminaries

Unless otherwise said, Γ is always a finitely generated (f.g.) group. Let $\mathscr{C}$ be a family of finite groups. Then Γ is residually $\mathscr{C}$ if

$$\cap\{H \lhd \Gamma \mid \Gamma/H \simeq C \in \mathscr{C}\} = \{e\} .$$

So Γ is residually-finite (resp. nilpotent, solvable, p) if it is residually $\mathscr{C}$ and $\mathscr{C}$ is the family of all finite groups (resp. nilpotent, solvable, p-groups).

A group is said to be *virtually-X* if it has a finite index subgroup with property X. We recall that if F is a field of characteristic p then every finitely generated linear group Γ over F (i.e., a f.g. subgroup of $\mathrm{GL}_n(F)$) is virtually residually p. If $\mathrm{char}(F) = 0$ then Γ is virtually residually p for almost every prime p (cf. [We, Di]).

We denote $a_n(\Gamma) = |\{H \leqq \Gamma \mid [\Gamma : H] = n\}|$ and $S_n(\Gamma) = \sum_{i=1}^{n} a_i(\Gamma)$. We say that Γ has polynomial subgroup growth (*PSG*) if $a_n(\Gamma)$ (or equivalently $S_n(\Gamma)$) grows polynomially, i.e., there exists $\alpha \in \mathbf{R}$ such that $a_n(\Gamma) \leqq n^{\alpha}$ for every n. This is equivalent to $\limsup_n \dfrac{\log a_n(\Gamma)}{\log n} < \infty$.

For a (topological) group H, $d(H)$ denotes the number of (topological) generators while $\mathrm{rank}(H) = \sup\{d(H) \mid H \text{ a finitely generated (closed) subgroup of } H\}$. If $\mathrm{rank}(H) < \infty$, H is said to be of finite rank. H^p(resp: $[H, H]$) denotes the (closed) subgroup generated by the p-th powers (resp: commutators). For a pro-p group H, $d(H) = d(H/[H, H]H^p)$.

The following lemmas seem to be known. Still for the sake of reference we bring them here:

Lemma 0.1 *Let H be a finite index subgroup of Γ. Then Γ has polynomial subgroup growth if and only if H does.*

Proof. One direction ($\Rightarrow$) is trivial. Assume, therefore, that H has polynomial subgroup growth. We may assume that H is normal. Let $[\Gamma : K] \leqq n$. Then $[H : H \cap K] \leqq n$. Thus, the number of possibilities for $H \cap K$ is bounded by some polynomial, say $f(n)$, while the number of possibilities for HK is bounded by the number of subgroups of Γ/H, C say. Let $r = \mathrm{rank}(\Gamma/H)$ and let HK be generated by H and by the elements $a_1, \ldots, a_r$. Then K is generated by $H \cap K$ and elements $b_i = a_i h_i$ where $h_i \in H$ and h_i is determined only mod $H \cap K$. Therefore, given HK and $H \cap K$, the number of possibilities for K is at most n^r and so the number of subgroups of Γ of index at most n is bounded by $Cn^r f(n)$. □

Remark. The polynomials associated to Γ and H may have different degrees. A simple example is provided by the infinite dihedral group and its infinite cyclic subgroup of index 2. It may be interesting to check this phenomenon somewhat closer.

Lemma 0.2 *Let $\pi: \Gamma \to \Delta$ be an epimorphism with* $\mathrm{Ker}\pi$ *finite. Then Γ is a PSG-group if and only if Δ is.*

Proof. For a group G, we denote $P(G)$ the intersection of all finite index subgroups of G. So $G/P(G)$ is residually finite and G is a *PSG*-group iff $G/P(G)$ is. We can therefore in the lemma replace Γ (resp. Δ) by $\Gamma/P(\Gamma)$ (resp. $\Delta/P(\Delta)$) and assume therefore that Γ and Δ are residually finite. The kernel of π is still finite.

Now, as Γ is residually finite it has a finite index subgroup H such that $H \cap \mathrm{Ker}(\pi) = \{1\}$. Thus H is also isomorphic to a finite index subgroup of Δ. By Lemma 0.1, Γ is *PSG* iff H is iff Δ is. □

Segal studied *PSG*-groups and proved the following theorem, which was the main motivation for the present work:

Theorem 0.3 (Segal [Sg]). *A finitely generated, residually nilpotent, solvable group is PSG if and only if it is of finite rank.*

A lot is known about solvable groups of finite rank (cf. [Ro1, 2]) so such a characterization is satisfactory.

Finally we mention the following easy lemma:

Lemma 0.4 *If G is a residually solvable, virtually solvable group, then G is solvable.*

Proof. G has a normal solvable subgroup H of index m and derived length l, for some integers m and l. Every solvable quotient of G is therefore solvable of derived length at most $m + l$. Since G is residually solvable, we can deduce that G is solvable of derived length at most $m + l$. □

1 PSG-pro-p groups are p-adic analytic

Let p be a prime and G a pro-p group. G is said to be *analytic* (or a p-adic Lie group) if it has a structure of a p-adic analytic manifold compatible with the group operations (see [Se1, Lz, LM1]). Every compact p-adic Lie group is virtually pro-p, but not every pro-p group is analytic. The problem of determining which pro-p groups are analytic ("the Hilbert 5th problem for p-adic Lie groups") was solved for the first time by Lazard [Lz]. In [LM1] we gave a different characterization. Here we shall use it to give an additional one.

Before stating the result, we observe that if G is a finitely generated (in the topological sense) pro-p group then $a_n(G) = \#\{H \mid H \text{ an open subgroup of } G \text{ of index } n\}$ is finite for every n. (In fact $a_n(G) = 0$ if n is not a power of p.) So the notion of pro-p (or pro-finite) *PSG*-group is defined in the obvious way.

Theorem 1.1 *Let G be a finitely generated pro-p group. The following conditions are equivalent:*

(*i*) *G is analytic.*
(*ii*) *G is a group of polynomial subgroup growth.*
(*iii*) *There exists an integer m such that $d(H) \leqq m$ for every open subgroup H of G. ($d(H)$ denotes the number of topological generators of H).*
(*iv*) *There exists an integer m' such that $d(H) \leqq m'$ for every normal open subgroup H of G.*

Proof. The equivalence of (i), (iii) and (iv) is proved in [LM1]. To prove the theorem it suffices to prove (*iii*) ⇒ (*ii*) ⇒ (*iv*).

(*iii*) $\Rightarrow$ (*ii*). Every open subgroup of G is subnormal of p-power index. Thus every subgroup K of index p^{l+1} lies in some subgroup H of index p^l. By assumption $d(H) \leqq m$ and hence the Frattini subgroup $\Phi(H) = H^p[H, H]$ is of index at most p^m in H. Every subgroup of index p of H contains $\Phi(H)$, hence H has at most $M = \dfrac{p^m - 1}{p - 1}$ subgroups of index p. This shows that $a_{p^{l+1}}(G) \leqq M a_{p^l}(G)$ and by induction $a_{p^l}(G) \leqq M^l$. Thus $\limsup_l \dfrac{\log a_{p^l}(G)}{\log(p^l)} \leqq \dfrac{\log M}{\log p} \leqq m < \infty$ and G is a *PSG*-group.

To prove (*ii*) $\Rightarrow$ (*iv*) we need the following lemma:

Lemma 1.2 *Let G be a pro-p group and k a positive integer. If there exists an open normal subgroup K of G with $d(K) \geqq k$, then such K exists with $[G:K] \leqq p^{k(\log_2 k + 1)}$. Moreover, K can be chosen so that G/K has a normal sequence $\{1\} = T_r \leqq T_{r-1} \leqq \cdots \leqq T_0 = G/K$ where $r \leqq \log_2 k + 1$ and T_i/T_{i+1} is an elementary abelian p-group of rank at most k.*

Proof. Let K be a normal subgroup of G maximal with respect to the property $d(K) \geqq k$ and $\Phi(K)$ its Frattini subgroup. Then $[K:\Phi(K)] \geqq p^k$, and we can choose a subgroup $\Phi(K) \subseteq L \subseteq K$ such that $[K:L] = p^k$ and L is normal in G. Let $C = C_G(K/L)$. Then C contains K. We claim that $C = K$. If not, then there exists a group M, $K \subset M \subseteq C$ with $[M:K] = p$ and $M \lhd G$ (since G/K is a finite p-group). Now $K/L \subseteq Z(M/L)$ (Z denotes center), and hence M/L is a central by cyclic group, whence abelian. This yields $d(M/L) \geqq d(K/L) \geqq k$ which contradicts the maximality of K.

We conclude that $C = K$ and that G/K can be embedded as a subgroup of $\mathrm{Aut}(K/L) \simeq \mathrm{GL}_k(\mathbf{F}_p)$. In fact G/K can be identified with a subgroup of S, the p-Sylow subgroup of $\mathrm{GL}_k(\mathbf{F}_p)$. In S, there is a sequence

$$\{1\} = S_r \leqq S_{r-1} \leqq \cdots \leqq S_0 = S$$

such that $S_i \lhd S$, S_i/S_{i+1} is elementary abelian and $r \leqq \log_2(k) + 1$ (cf. [Hu, III.16]). The embedding of $T = G/K$ in S induces a sequence

$$\{1\} = T_r \leqq T_{r-1} \leqq \cdots \leqq T_0 = T$$

by taking $T_i = S_i \cap T$. Then $T_i \lhd T$ and T_i/T_{i+1} is elementary abelian. By our maximality condition on K, we deduce that $|T_i/T_{i+1}| \leqq p^k$ and thus

$$|T| = [G:K] \leqq p^{k(\log_2 k + 1)}.$$

This proves Lemma 1.2.

Back to Theorem 1.1 (*ii*) $\Rightarrow$ (*iv*): by assumption we know that there exists $\alpha \in \mathbf{R}$ such that the number of subgroups of index at most p^l is at most $p^{l\alpha}$. We want to prove that for sufficiently large k, there is no normal open subgroup K with $d(K) \geqq k$. Assume for convenience that k is even, $k = 2s$ and let K and L be as in Lemma 1.2 (and its proof). Since K/L is an elementary abelian group of order p^k, it has at least $p^{k^2/4}$ subgroups of index $p^{k/2}$. Hence G has at least $p^{k^2/4}$ subgroups of index at most $p^{k\log_2 k + \frac{3k}{2}}$. Our assumption implies now that $\dfrac{k^2}{4} \leqq \alpha\left(k \log k + \dfrac{3k}{2}\right)$ which implies that k is bounded and the theorem is proved. □

Corollary 1.3 *For every $\alpha \in \mathbf{N}$, there is $f(\alpha) \in \mathbf{N}$ such that if G is a pro-p-group for which $a_n(G) \leqq n^\alpha$ for every n, then G is a p-adic Lie group of dimension $\leqq f(\alpha)$.*

Proof. The proof of (1.2) shows that there exists $f(\alpha)$ such that $d(H) \leqq f(\alpha)$ for every open normal subgroup of G. By [LM1], this implies that G is of dimension at most $f(\alpha)$. □

Remark 1.4 The function $\alpha \mapsto f(\alpha)$ is independent of p!

Corollary 1.5 *Let Γ be a residually nilpotent finitely generated PSG-group. Then Γ is linear over $\mathbf{C}$.*

Proof. Assume first that Γ is residually-p for some prime p. Let G be the pro-p completion of Γ, i.e., $G = \varprojlim \Gamma/N$ when N runs over the normal subgroups of Γ of p-power index. Since Γ is residually p the canonical map $\Gamma \to G$ is injective. Now, for every subgroup H of G of index n, $H \cap \Gamma$ is a subgroup of Γ of index at most n and $\overline{H \cap \Gamma} = H$. This yields that if Γ is *PSG*-group then G is a *PSG*-pro-p group. So, G is *PSG*-group and by Theorem 1.1 it is therefore a p-adic Lie group. Proposition 4 of [Lu1] says that a compact p-adic Lie group can be embedded in $\mathrm{GL}_n(\mathbf{Q}_p)$ for some n. Hence our G is embedded in $\mathrm{GL}_n(\mathbf{Q}_p)$, and thus so is Γ. Since $\mathbf{Q}_p$ as an abstract field can be embedded in $\mathbf{C}$, we conclude that Γ is linear over $\mathbf{C}$.

To prove (1.5) for residually nilpotent groups we need some lemmas:

Lemma 1.6 *Let D be a finitely generated nilpotent group. Then, for every prime p, the pro-p completion $D_{\hat{p}}$ of D is a p-adic Lie group of dimension exactly $h(D)$ — the Hirsch rank of D.*

Proof. The elements of finite order in D form a finite normal subgroup, so we can assume D is torsion free. Every finite index subgroup of D is generated by at most $h(D)$ elements and hence the same holds for $D_{\hat{p}}$, which implies $\dim D_{\hat{p}} \leqq h(D)$ [LM1]. The converse is proved by induction on $h(\Gamma)$, by proving that if $N = \mathrm{Ker}(D \to \mathbf{Z})$ then the pro-p topology of D induces the pro-p topology of N. □

Lemma 1.7 *Let Γ be a finitely generated residually nilpotent group. Assume that for every prime p, $\Gamma_{\hat{p}}$ analytic. Then Γ is linear.*

Proof. Let G be the pro-nilpotent completion of Γ, i.e., $G = \varprojlim \Gamma/N$ when N runs over the finite index normal subgroups of Γ with Γ/N nilpotent. Let $\gamma_n(\Gamma)$ (resp. $\gamma_n(G)$) be the n-th term of the lower central series of Γ (resp. G), $\Gamma(n) = \Gamma/\gamma_n(\Gamma)$ and $G(n) = G/\gamma_n(G)$. Then $G(n)$ is the pro-nilpotent completion of $\Gamma(n)$, and $\gamma_n(\Gamma)$ is dense in $\gamma_n(G)$.

G, being a pro-nilpotent group, is the product of its p-Sylow subgroups $G = \prod_p G_p$. In fact G_p is the pro-p completion of Γ. Similarly $G(n) = \prod_p G(n)_p$ where $G(n)_p$ is the pro-p completion of $\Gamma(n)$. We claim that the Hirsch rank of $\Gamma(n)$ is bounded. Indeed fix some p. Then $h(\Gamma(n)) = \dim(\Gamma(n)_{\hat{p}}) \leqq \dim \Gamma_{\hat{p}}$ (the equality is by (1.6)).

Fix n for which $h(\Gamma(n))$ is maximal. Then $\gamma_n(\Gamma)/\gamma_{n+1}(\Gamma)$ is a finite group. Its order is therefore divisible only by primes from a finite set S. But $\gamma_n(\Gamma)/\gamma_{n+1}(\Gamma)$ is dense in $\gamma_n(G)/\gamma_{n+1}(G)$ which proves that for $p \notin S$, G_p is nilpotent of class $\leqq n$.

Let $H_1 = \prod_{p \notin S} G_p$, $H_2 = \prod_{p \in S} G_p$ and Γ_i be the image of Γ in H_i $(i = 1, 2)$. Then Γ is embedded in $\Gamma_1 \times \Gamma_2$ and each Γ_i is a quotient of Γ. Now, H_1 is nilpotent and so is Γ_1. On the other hand, for every $p \in S$ (in fact, for every p), G_p is a linear group (since it is analytic and by [Lu1, Prop. 4] is linear) so H_2 is linear over $\mathbf{C}$, and so is Γ_2. Thus both Γ_1 and Γ_2 are linear, hence so are $\Gamma_1 \times \Gamma_2$ and Γ. This concludes the proof of (1.7).

Corollary (1.5) is now also proved since the beginning of the proof shows that the pro-p completion of Γ is analytic. □

The rest of this section will be devoted to prove Theorem D, whose proof will use some of the arguments used above.

Theorem 1.8 *Let Γ be a finitely generated residually nilpotent group generated by a finite set B. Let $b_n(\Gamma)$ be the number of elements of Γ which can be written as words of length at most n on the generators in B. Assume there exist C such that $b_n(\Gamma) \leqq C \cdot n^C$. Then Γ is virtually nilpotent.*

Proof. Fix some prime p and let $G = \Gamma_{\hat{p}}$ be the pro-p completion of Γ. The canonical map $i: \Gamma \to G$ may not be injective, but anyway $i(\Gamma) = \Gamma_1$ is a dense subgroup of G. Let $B = \{b_1, \ldots, b_d\}$ be the set of generators of Γ (and hence for Γ_1 and G by abuse of the language). Consider a p-elementary abelian factor group Γ/Δ of Γ of order $\leqq p^k$, say, and let $H = \overline{i(\Delta)}$. We can then choose a basis for $\Gamma/\Delta \simeq G/H$ consisting of some of the cosets $b_i H$. Each element of G/H can be written as a product of powers with exponents at most $p/2$ of these basis elements (and their inverses) and it lies in the coset of H determined by the corresponding product of the $a_i's$ themselves. This shows that each coset has a representative of length $\leqq kp/2$. But the subgroup Δ is generated by elements of the form xay^{-1}, where x and y are two such coset representatives and a is one of the given generators (see [H, 7.2.2]). Thus Δ has a finite set of generators of length at most kp. Now, let $\Delta/\Delta_1 \simeq H/H_1$ (where $H_1 = \overline{i(\Delta_1)}$) be a p-elementary abelian factor group of H, again of order $\leqq p^k$. Then repeating the above argument shows that Δ_1 (and H_1) can be generated by elements of length at most $(kp)^2$ etc.

Now assume there exists a normal open subgroup K with $d(K) \geqq k$, let K be as in Lemma 1.2 and L a subgroup of K such K/L is elementary abelian p-group of order p^k. By the above argument each coset of K/L has a representative of length at most $(kp)^{\log_2 k + 1}$. Thus

$$p^k \leqq C \cdot (kp)^{c(\log_2 k + 1)}$$

As p is fixed this shows that k is bounded. From Theorem 1.1 it follows now that G is analytic.

Now, Lemma 1.7 implies that Γ is linear. Linear groups have either exponential or polynomial growth and in the second case they are virtually nilpotent [Ti]. This finishes the proof of Theor. 1.8.

Remark. It was observed by I. Ilani that our proof in fact yields the same conclusion under the weaker assumption that $b_n(\Gamma) = O(2^{2\sqrt{\log n}})$. But, Grigorchuk [Gr] proved it under the even weaker assumption that $b_n(\Gamma) = O(2^{\sqrt{n}})$. Grigorchuk also applied the theory of p-adic analytic groups. (In [Gr] the assumption is that Γ is

residually p, but our Lemma 1.7 shows that also there the assumption of residual nilpotence suffices).

2 Linear groups of polynomial subgroups growth

The main goal of this section is to prove Theorem C for linear groups over $\mathbf{C}$. We begin with reduction to groups over Q.

Lemma 2.1 *If there exists a f.g. PSG-group Γ_1 in $GL_n(\mathbf{C})$ which is not virtually solvable then such a group, say Γ_2, also exists in $GL_m(\mathbf{Q})$ for some m. (Γ_2 can even be taken to be a quotient of Γ_1.)*

Proposition 2.2 *Let Γ be a f.g. subgroup of $GL_n(\mathbf{C})$ which is not virtually solvable. Then Γ has a specialization $\varphi\colon \Gamma \to GL_n(\bar{\mathbf{Q}})$ such that $\varphi(\Gamma)$ is not virtually solvable ($\bar{\mathbf{Q}}$ denotes the algebraic closure of $\mathbf{Q}$.)*

Proposition 2.2 implies Lemma 2.1. Indeed, in this case $\Gamma_2 = \varphi(\Gamma_1)$ would be a f.g., non-virtually solvable, *PSG*-group embedded in $GL_n(\bar{\mathbf{Q}})$. But, as $\varphi(\Gamma_1)$ is f.g., it is inside $GL_n(k)$ for some number field k, $[k:Q] = l$. Hence $\Gamma_2 = \varphi(\Gamma_1) \leqq GL_n(k) \leqq GL_{n \cdot l}(\mathbf{Q})$.

To prove Proposition 2.2, we need the following nice result (due to Platonov). It is proved by combining the Lie–Kolchin Theorem with Jordan's Theorem on finite linear groups ([We, 10.11]).

Proposition 2.3 *Given a positive integer n, there exist two integers $j(n)$ and $l(n)$ such that every virtually solvable subgroup G of $GL_n(\mathbf{C})$ has a normal subgroup H of index at most $j(n)$ which is solvable of derived length at most $l(n)$.*

Proposition 2.3 implies Proposition 2.2. Indeed, since Γ is finitely generated it is contained in $GL_n(A)$ where A is a finitely generated $\mathbf{Q}$-algebra. By Hilbert's Nullstellensatz, the homomorphisms from A to $\bar{\mathbf{Q}}$ separate the points of A. Every such homomorphism φ induces a homomorphism, denoted also φ from $GL_n(A)$ to $GL_n(\bar{\mathbf{Q}})$, called a specialization. The specializations separate the points of $GL_n(A)$ and of Γ, i.e., for every $1 \neq \gamma \in \Gamma$ there exists such a φ with $\varphi(\gamma) \neq 1$.

Assume now that for all specializations φ, $\varphi(\Gamma)$ is virtually solvable. Let H be the intersection of all subgroups of Γ of index less than or equal to $j(n)$. Since there are only finitely many such subgroups, $[\Gamma:H] < \infty$. Let K be the $l(n)$-th term in the derived series of H. By Propos. 2.3, $\varphi(K) = \{e\}$ for every specialization. Hence $K = \{e\}$ and Γ is solvable by finite. Propos. 2.2 is thus proven and hence also Lemma 2.1.

To prove Theorem C for groups over $\mathbf{C}$ it suffices now to prove it for subgroups of $GL_n(\mathbf{Q})$. Namely:

Theorem 2.4 *Let Γ be a finitely generated PSG subgroup of $GL_n(\mathbf{Q})$. Then Γ is virtually solvable.*

To prove this theorem, we bring first a few results needed later on in the proof. The first one is a special case of [BT2, 3.17]. Since our case is so simple we include a proof.

Lemma 2.5 *Let G be a semi-simple algebraic group defined over $\mathbf{Q}$, and $\pi\colon \tilde{G} \to G$ its universal covering (cf. [BT1, 2.24 (ii)]). Then*

$$\frac{G(\mathbf{Q})}{\pi(\tilde{G}(\mathbf{Q}))}$$

is an abelian torsion group whose exponent divides the order of the center of $\tilde{G}(\bar{Q})$.

Example. A typical example is $G = \mathrm{PGL}_2$, $\tilde{G} = \mathrm{SL}_2$ and

$$\frac{G(\mathbf{Q})}{\pi(\tilde{G}(\mathbf{Q}))} \simeq \frac{\mathbf{Q}^*}{(\mathbf{Q}^*)^2} \simeq \bigoplus_{i=1}^{\infty} \frac{\mathbf{Z}}{2\mathbf{Z}}.$$

Proof. The map $\pi\colon \tilde{G}(\bar{\mathbf{Q}}) \to G(\bar{\mathbf{Q}})$ is surjective with a finite central kernel Z of order m, say. Let $L = \pi^{-1}(G(\mathbf{Q}))$ and $M = \tilde{G}(\mathbf{Q})$. The Galois group $\mathrm{Gal} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts on L and M is precisely the set of the fixed points. Moreover, for every $x \in L$ and $\sigma \in \mathrm{Gal}$, $x^{-1}\sigma(x) \in Z$. This implies that for every $\sigma \in \mathrm{Gal}$ and every $x, y \in L$, $\sigma[x, y] = [x, y]$ (where $[x, y] = x^{-1}y^{-1}xy$). Hence $[x, y] \in M$ which means that M is a normal subgroup of L containing $[L, L]$. Furthermore, for $x \in L$, $\sigma(x) = xz$ for some $z = z(\sigma, x)$ in Z. Whence $\sigma(x^m) = (xz)^m = x^m z^m = x^m$ since $z \in Z$. This shows that $x^m \in M$, whence L/M is an abelian torsion group. The group

$$\frac{G(\mathbf{Q})}{\pi(\tilde{G}(\mathbf{Q}))}$$

is a quotient of L/M, and the lemma is proven.

The next result, which is crucial to our proof, needs some preparation. Let Γ be a finitely generated subgroup of $\mathrm{GL}_n(\mathbf{Q})$. Then there exists a finite set of primes S such that all the entries of the elements of Γ are in the ring $R = \mathbf{Z}_S$ of S-integers (i.e., the denominators are divisible only by primes from S). Let G be the Zariski closure of Γ. On $\Delta = G(R)$ we have the *congruence topology* defined by declaring $\Delta(m) = \mathrm{Ker}(G(R) \to G(R/mR))$, for all non-zero integers m, to be a basis of open neighborhoods of the identity of Δ. This makes Δ a topological group. It is not complete. Its completion is the closure of Δ in $G(\hat{R})$ where $\hat{R}$ is the pro-finite completion of R. In fact $\hat{R} = \prod_{p \notin S} \mathbf{Z}_p$, where $\mathbf{Z}_p$ is the ring of p-adic integers. Classical strong approximation results assure that under suitable conditions Δ is indeed dense in $G(\hat{R})$. In the last few years, some generalizations of it were proved by several authors. Most suitable for our needs is the following:

Theorem 2.6 *In the notations above, assume G is semi-simple, connected and simply connected. Then the closure of Γ is open in $G(\hat{R})$.*

Proof. See Nori [N, Theor. 5.4] or Matthews–Vaserstein–Weisfeiler [MVW, Theor. 8.1], see also Weisfeiler [W]. □

Corollary 2.7 *In the notations and assumptions above, the closure of Γ in $\Delta = G(R)$ is a subgroup Γ_0 of finite index in Δ.*

Proof. Clearly, the closure Γ_0 of Γ in $G(R)$ is $G(R) \cap \bar{\Gamma}$ where $\bar{\Gamma}$ is the closure of Γ in $G(\hat{R})$. Since $\bar{\Gamma}$ is open in $G(\hat{R})$ by (2.6) and $G(\hat{R})$ is compact, $\bar{\Gamma}$ is of finite index in $G(\hat{R})$ and so Γ_0 is of finite index in $G(R)$.

We can start now the proof of Theor. 2.4: Assume to the contrary that there is a non-virtually-solvable *PSG*-group Γ in $\mathrm{GL}_n(\mathbf{Q})$. By replacing Γ, if needed, by

a finite index subgroup, we can assume (keeping (0.1) in mind) that G — the Zariski closure of Γ — is connected. Moreover, it is not a solvable group, hence G modulo its solvable radical is a non-trivial semi-simple $\mathbf{Q}$-group. So we may further assume that $\Gamma \subsetneq G(\mathbf{Q})$ and G is semi-simple and connected. The projection of Γ to at least one of the $\mathbf{Q}$-simple factor of G is infinite and not virtually solvable. We can therefore further assume that G is simple. Let $\pi\colon \tilde{G} \to G$ be the simply connected covering of G. By Lemma 2.5,

$$\frac{G(\mathbf{Q})}{\pi(\tilde{G}(\mathbf{Q}))}$$

is abelian and torsion. The image there of the finitely generated group Γ is, therefore, finite. Hence a finite index subgroup of Γ is contained in $\pi(\tilde{G}(\mathbf{Q}))$. Since $\pi^{-1}(\Gamma)/Z \simeq \Gamma$ and $Z = \mathrm{Ker}(\pi)$ is finite, $\pi^{-1}(\Gamma)$ is also *PSG*-group by Lemma 0.2 and non-virtually solvable. We can therefore assume, by replacing Γ by $\pi^{-1}(\Gamma)$, that G, the Zariski closure of Γ, is (almost) simple, connected and simply connected. Moreover Γ is in $\Delta = G(R)$ where R is the ring of S-integers for some finite set S of primes. As Γ is infinite, so is $G(R)$ which is a discrete subgroup of $G(\mathbb{R}) \times \prod_{p \in S} G(Q_p)$. In particular, the latter one is not compact.

We are now in a position to apply Theor. 2.6 (or Coroll. 2.7). So, Γ_0, the closure of Γ in the congruence topology of $G(R)$ is of finite index in $G(R)$.

For a group L we recall that $S_n(L)$ denotes the number of subgroups of L of index at most n. Of course, L is a *PSG*-group if and only if the sequence $S_n(L)$ has polynomial growth.

For an S-arithmetic group (such as $\Delta = G(R)$ or any finite index subgroup of it, say Δ') let $C_n(\Delta')$ be the number of *congruence* subgroups of index at most n. (A congruence subgroup of Δ' is one which is open in the induced congruence topology of Δ'.)

Back to our circumstances: Γ is congruence dense in Γ_0 which is an S-arithmetic group, i.e., a finite index subgroup of $\Delta = G(R)$.

Lemma 2.8 $S_n(\Gamma) \geqq C_n(\Gamma_0)$.

Proof. For every congruence subgroup H of Γ_0, we associate the subgroup $\varphi(H) = \Gamma \cap H$ of Γ. Then $[\Gamma : \varphi(H)] \leqq [\Gamma_0 : H]$. The lemma will follow once we prove that φ is a one to one map. Indeed, let H_1 and H_2 be congruence subgroups of Γ_0 and let N be a normal congruence subgroup of Γ_0 contained in $H_1 \cap H_2$. As Γ is dense in Γ_0, the projection π of Γ to the finite "continuous" quotient Γ_0/N is surjective. In particular, for $i = 1, 2$, $\pi(\Gamma \cap H_i) = H_i/N$. This proves that $H_i = N \cdot (\Gamma \cap H_i)$. Hence, $\varphi(H_1) = \varphi(H_2)$ implies $H_1 = H_2$ and the lemma is proven.

To conclude the proof of Theor. 2.4, it suffices now to prove that $C_n(\Gamma_0)$ *does not* grow polynomially. Just as in (0.1), it suffices to prove it for $G(R)$. The next theorem which is of independent interest will conclude the proof Theor. 2.4.

Theorem 2.9 *Let G be a non-trivial (almost)-simple, connected, simply connected $\mathbf{Q}$-algebraic group. Assume S is a finite set of primes for which $G(\mathbb{R}) \times \prod_{p \in S} G(\mathbf{Q}_p)$ is not compact. Let R be the ring of S-integers, $\Delta = G(R)$ and $C_n(\Delta)$ is the number of congruence subgroups of Δ of index at most n. Then $C_n(\Delta)$ does not grow polynomially.*

We still need another lemma:

Lemma 2.10 *For almost every prime p, the finite group $\Delta/\Delta(p) = G(R/pR)$ is a group of even order.*

We will give two proofs. But first notice that indeed $\Delta/\Delta(p) \simeq G(R/pR)$, i.e., $G(R) \to G(R/pR)$ is onto. This follows from the classical strong approximation theorem for arithmetic groups (cf. [Kn, Pl, Pr]).

First Proof. For p not in S, $R/pR = \mathbf{F}_p$ and $G(\mathbf{F}_p)$ is an algebraic group which is quasi-split by a Theorem of Lang and contains therefore an $\mathbf{F}_p$-split non-trivial torus (cf. [Bo1, 16.6]), whose order is $p-1$. Hence $p-1 \,|\, |G(\mathbf{F}_p)|$ and so for $p \neq 2$, $|G(\mathbf{F}_p)|$ is even. (See also [Lu2, Lemma 2].)

Second Proof. If $\Delta/\Delta(p)$ is of odd order, then by the Feit–Thompson Theorem it is solvable. Moreover, it is solvable of bounded derived length (cf. [Di, §6]). Since $\bigcap_{p\in\mathscr{P}} \Delta(p) = \{e\}$ for every infinite set of primes $\mathscr{P}$, Δ is also solvable, which contradicts the fact that Δ is a Zariski dense subgroup of G (by Borel's density theorem, and its extensions, cf. [Bo2], [Wa] and [Bo3]).

Back to the proof of Theor. 2.9: Let S be the original S plus those primes for which 2 does not divide $|\Delta/\Delta(p)|$. By (2.10), S is still finite. Let N be a large positive integer. The number of primes p (not from S) which are less than N is approximately $l = N/\log N$, by the Prime Number Theorem. Moreover, $\sum_{S\neq p\leqq N} \log p \sim N$, by the same theorem (cf. [HW, §2.2]) and hence $M = \prod_{S\neq p\leqq N} p \sim e^N$. Let $\Delta(M)$ be the congruence subgroup mod$M$ of Δ. Then $[\Delta:\Delta(M)] \leqq M^d$ where $d = \dim G$ = the dimension of G as an algebraic group (or where $d = r^2$ and $G \subsetneq \mathrm{GL}_r$).

By the Chinese Remainder Theorem, $\Delta/\Delta(M) = \prod_{S\neq p\leqq N} \Delta/\Delta(p)$. By (2.10), $\Delta/\Delta(p)$ contains an element of order 2, and $\Delta/\Delta(M)$ contains, therefore, an elementary abelian 2-group L of rank l. Think of L as an $\mathbf{F}_2$-vector space of dimension l. It is not difficult to check that the number of subspaces of L of dimension $\left[\frac{l}{2}\right]$ is at least $2^{l^2/4}$. So, Δ has at least $2^{l^2/4}$ congruence subgroups of index at most M^d. Substituting $l \sim \dfrac{N}{\log N}$, $M \sim e^N$ we see that:

$$\frac{\log C_{M^d}(\Delta)}{\log(M^d)} \geqq \frac{l^2 \log 2}{4dN} \sim \text{constant} \cdot \frac{N}{\log^2 N}.$$

As $\lim_{N\to\infty} \left(\dfrac{N}{\log^2 N}\right) = \infty$, the sequence $C_n(\Delta)$ does not have polynomial growth. This proves Theor. 2.9. Theorem 2.4 is, therefore, now also proven. □

To summarize we actually have proved Theorem A. Indeed if Γ is as in Theorem A, then by (1.5) it is linear over $\mathbf{C}$. If Γ is not virtually solvable then by (2.1) it has a non-virtually solvable quotient in $\mathrm{GL}_m(Q)$ for some m. Such a quotient is also *PSG* in contradiction to (2.4). Hence Γ is virtually solvable. By (0.4) it is solvable and by (0.3) it is also of finite rank. This proves Theorem A. The general case of Theorem C now also follows since every finitely generated linear group (in any characteristic) is virtually residually nilpotent.

3 Some concluding remarks

I. There are infinitely generated residually finite groups Γ for which $a_n(\Gamma) < \infty$ for every n. Such groups, even if they are of polynomial subgroup growth, are not necessarily virtually solvable. Examples include all analytic pro-p groups. (Recall that for such a group G, every finite index subgroup is open [Lz, Ha], so they are *PSG*-groups in any sense of the notion.) To see a countable example: Let π be the set of all primes except for one prime p, and let $\mathbf{Z}_\pi$ be the ring of π-integers. Then it follows from the affirmative solution of the congruence subgroup problem for $SL_n(n \geqq 3)$ (cf. [BMS]), (or even SL_2- with S-integers, when $|S| \geqq 2$, see [Se2]) that $SL_n(\mathbf{Z}_\pi)$ is a *PSG*-group. Indeed, its pro-finite completion is $SL_n(\mathbf{Z}_p)$ which is p-adic analytic and so by (0.1) and (1.1) is a *PSG*-group. (We are using here the trivial fact that a group Γ is *PSG*-group iff $\hat{\Gamma}$, its pro-finite completion, is a *PSG*-group in the topological sense.)

II. As can be seen from our proof the question of polynomial growth is closely related to the "rank" of Γ. For more results in this direction see [LM2] and [MS].

III. The new characterization of analytic *pro-p* groups given in Theor. 1.1 gives a new characterization of finitely generated linear groups:

Let Γ be a group. *A pro-finite topology* on Γ is a topology for which some family of normal finite index subgroups serves as a fundamental system of neighborhoods of the identity. (*The pro*-finite topology is the one which we take *all* the normal finite index subgroups.) The topology is a *pro-p topology* if every open subgroup is of p-power index. The topology $\mathscr{F}$ is *polynomial* if $a_n(\Gamma, \mathscr{F})$ grow polynomially when $a_n(\Gamma, \mathscr{F})$ = number of open subgroups of index n.

Theorem 3.1 *Let Γ be a finitely generated group. Then the following conditions are equivalent:*

(i) Γ can be embedded in $\mathrm{GL}_n(F)$ for some field F of characteristic 0.

(ii) Γ has a finite index subgroup Δ which has a Hausdorff, polynomial pro-p topology for some prime p.

The proof is very similar to [Lu1] and will therefore be omitted.

References

[BMS] Bass, H., Milnor, J., Serre, J.P.: Solution of the congruence subgroup problem for $SL(n)$, $(n \geqq 3)$ and $Sp(2n)$, $(n \geqq 2)$. Publ. Math. IHES **33**, 59–137 (1967)

[Bo1] Borel, A.: Linear algebraic groups. New York: W.A. Benjamin Inc. 1969.

[Bo2] Borel, A.: Density and maximality of arithmetic subgroups. J. Reine Angew. Math. **224**, 78–89 (1966)

[Bo3] Borel, A.: On the set of discrete subgroups of bounded covolume in a semisimple group. Proc. Indian. Acad. Sci. (Math. Sci.) **97**, 45–52 (1987)

[BT1] Borel, A., Tits, J.: Complements á l'article, "Groupes réductifs". Publ. Math. I.H.E.S. **41**, 253–256 (1972)

[BT2] Borel A., Tits, J.: Homomorphismes "abstraits" de groupes algébriques simples. Ann. Math. **97**, 499–571 (1973)

[Di] Dixon, J.: The structure of linear groups. London: Van Nostrand Reinhold Co., 1971,

[Gr] Grigorchuk, R.I.: On the Hilbert-Poincaré series of graded algebras associated with groups. Math. USSR Sbornik **66**, 211–229 (1990)

[G] Gromov, M.: Groups of polynomial growth and expanding maps. Publ. Math. IHES **53**, 53–78 (1981)

[GSS] Grunewald, F.J., Segal, D., Smith, G.C.: Subgroups of finite index in nilpotent groups. Invent. Math. **93**, 185–223 (1988)
[H] Hall, M.: Theory of groups. New York: MacMillan Co. 1959
[HW] Hardy, G.H., Wright, E.M.: An introduction to the theory of numbers. 4th ed. Oxford: Clarendon Press 1965
[Ha] Hartley, B.: Subgroups of finite index in profinite groups. Math. Z. **168**, 71–76 (1979)
[Hu] Huppert: Endliche Gruppen I. Berlin, Heidelberg New York: Springer 1967
[Kn] Kneser, M.: Strong approximation. In: Algebraic groups and discontinuous subgroups. Proc. Symp. Pure Math., vol. IX, 187–196 (1966)
[Lz] Lazard, M.: Groupes analytiques p-adiques. Publ. Math. IHES **26**, 389–603 (1965)
[Lu1] Lubotzky, A.: A group theoretic characterization of linear groups. J. Alg. **113**, 207–214 (1988)
[Lu2] Lubotzky, A.: On finite index subgroups of linear groups. Bull. Lond. Math. Soc. **19**, 325–328 (1987)
[LM1] Lubotzky, A., Mann, A.: Powerful p-groups II, p-adic analytic groups. J. Alg. **105**, 506–515 (1987)
[LM2] Lubotzky, A., Mann, A.: Residually finite groups of finite rank. Math. Proc. Camb. Phil. Soc. **106**, 385–388 (1989)
[LMS] Lubotzky, A., Mann, A., Segal, D.: Finitely generated groups of polynomial subgroup growth. Israel J. Math., (to appear)
[MS] Mann, A., Segal, D.: Uniform finiteness conditions in residually finite groups. Proc. Lond. Math. Soc. **61**, 529–545 (1990)
[MVW] Matthews, C.R., Vaserstein, L.N., Weisfeiler, B.: Congruence properties of Zariski-dense subgroups I. Proc. Lond. Math. Soc. **48**, 514–532 (1984)
[N] Nori, M.: On subgroups of $GL_n(\mathbb{F}_p)$. Invent. Math. **88**, 257–275 (1987)
[Pl] Platonov, V.P.: The problem of strong approximation and the Kneser–Tits conjecture. Math. USSR Izv. **3**, 1139–1147 (1969); Addendum, ibid **4**, 784–786 (1970)
[Pr] Prasad, G.: Strong approximation for semi-simple groups over function fields. Ann. Math. **105**, 553–572 (1977)
[Ro1] Robinson, D.J.S.: Finiteness conditions and generalized soluble groups. 2 vols. Berlin Heidelberg New York: Springer 1972
[Ro2] Robinson, D.J.S.: A course in the theory of groups. Berlin Heidelberg New York: Springer 1980
[Sg] Segal, D.: Subgroups of finite index in soluble groups I. In: Robertson, E.F., Campbell C.M. (eds) Proc. of Groups, St. Andrews 1985, pp. 307–314
[Se1] Serre, J.P.: Lie algebras and Lie groups. New York: Benjamin 1965
[Se2] Serre, J.P.: Le problème des groupes de congruence pour SL_2. Ann. Math. **92**, 489–527 (1970)
[Ti] Tits, J.: Free subgroups in linear groups. J. Alg. **20**, 250–270 (1972)
[Wa] Wang, S.P.: On density properties of S-subgroups of locally compact groups. Ann. Math. **94**, 325–329 (1971)
[We] Wehrfritz, B.A.F.: Infinite linear groups. Berlin Heidelberg New York: Springer 1973
[W] Weisfeiler, B.: Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups. Ann. Math. **120**, 271–315 (1984)