ISRAEL JOURNAL OF MATHEMATICS 82 (1993), 363-371

FINITELY GENERATED GROUPS OF POLYNOMIAL SUBGROUP GROWTH

BY

ALEXANDER LUBOTZKY* AND AVINOAM MANN**

Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel

AND

DAN SEGAL

All Souls College, University of Oxford, Oxford OX1 4AL, England

To John Thompson, an inspiration to group theory, on his being awarded the Wolf Prize

ABSTRACT

We determine the structure of finitely generated residually finite groups in which the number of subgroups of each finite index n is bounded by a fixed power of n.

Introduction

Let G be a finitely generated group. The number $a_n(G)$ of subgroups of G of index n is a non-negative integer, and a natural problem, first suggested in [S1], is to investigate this number theoretical function. If F is the finite residual of G, namely the intersection of all subgroups of G of finite index, then $a_n(G) = a_n(G/F)$, so there is no real loss in assuming that $F = 1$, i.e. that G is a residually finite group. In this note we consider the simplest growth condition of $a_n(G)$, proving,

* Partially supported by BSF and GIF grants.

** Partially supported by a BSF grant.

Received April 1, 1991 and in revised form April 2, 1992

THEOREM: *A finitely generated residually finite group G satisfies $a_n(G) \leq n^s$, for some s, if and only if G is virtually soluble of finite rank.*

Groups satisfying the growth assumption of the Theorem will be referred to as **polynomial subgroup growth groups** (PSG groups for short). We recall that G is **virtually** X, for some class X of groups, if G contains an X-subgroup of finite index, and that G has **finite rank** r, if each finitely generated subgroup of G can be generated by r elements. Finitely generated soluble groups of finite rank form a well-understood class of groups, coinciding with the finitely generated soluble minimax groups, i.e. those having a normal series with factors satisfying either chain condition [R].

That soluble groups of finite rank, even if not finitely generated, are PSG, was already noted in [S1]. The converse was established in [LM3] and [MS], provided certain other assumptions are satisfied. It turned out that only a little further argument is needed to prove the Theorem in full, and this is done here. The complete proof employs diverse tools, such as the theory of algebraic and arithmetic groups and of linear groups in general, the theory of p-adic analytic groups and of infinite soluble groups, the classification of the finite simple groups, and the Prime Number Theorem. Therefore, rather than being satisfied with giving only the few arguments that have to be proved in full in this paper, we have taken the opportunity to describe the overall structure of the proof in some detail, referring to the earlier papers for complete proofs. This was considered advisable also because the earlier papers contain, on the one hand, some special cases of the Theorem that are now superfluous, even as intermediate stages in the proof, and, on the other hand, some other results. Thus the present paper serves also as an introduction to [LM3] and [MS]. While we have to mention that a similar description can be found in [DDMS], we note that the two descriptions are complementary, rather than repetitive.

Before proceeding with our description, let us mention a few problems whose investigation seems indicated now. First, a further investigation of $a_n(G)$. It was suggested in [GSS] to encode this function in a Dirichlet series $\zeta_G(s) = \sum a_n(G)n^{-s}$. This series converges (somewhere) exactly when G is a PSG group. In the simplest case, namely an infinite cyclic group, we obtain the classical Riemann zeta function, and in some other cases $\zeta_G(s)$ can be expressed in terms of this function [GSS, I]. Rationality results for the "local factors" of $\zeta_G(s)$ are proved in [GSS] and [dS1] for certain classes of groups, including the class of all

virtually soluble groups of finite rank. Very little is known about the abscissa of convergence of $\zeta_G(s)$, i.e. the exact exponent of polynomial growth of $a_n(G)$.

Next, there is the question of the other possible growths of $a_n(G)$. The proof below works also for growth somewhat bigger than polynomial. For pro-p groups $n^{\log n}$ is the minimal non-polynomial growth, according to [Sh], while the maximal growth, i.e. the subgroup growth of free pro-p groups, is exponential [I]. The maximal growth for discrete groups is even bigger [Ne]. The first author has recently shown that among arithmetic groups of characteristic 0, the ones with the congruence subgroup property are characterized by their subgroup growth, which is about $n^{(\log n)/(\log\log n)}$.

Finally, we can consider non-finitely-generated PSG groups. Some of the results of [MS] quoted below hold also in this case, but the Theorem does not, and examples given in that paper (see also [S1]) suggest that such groups are unlikely to have a simple characterization. Some further results for this case are derived in [M2].

This paper is one of several recent ones in which Lazard's theory of p-adic analytic groups ([La]; see also [LM1] and [DDMS]) serves as a link, enabling us to use recent advances in finite group theory to reduce problems about residually finite groups to one about linear groups. This rests on the linearity theorem of [Lu], which in turn applies [LM1], relying ultimately on some results about finite p-groups. We mention also the papers [LM2] and [Wi], and the survey papers [M1], [S2], and [dS2].

1. Linear Groups

The assumption of polynomial subgroup growth is always applied in the following way. We find in G subgroups of finite index H and K, with $K \lhd H$ and H/K an elementary abelian p-group (for some prime p) of rank r, say. We then know exactly how many subgroups of each index occur between H and K. The construction should be such that we have a reasonable upper bound on $|G : H|$. Then the PSG assumption provides a bound on r, and this either yields a contradiction or carries us further in the argument.

The main contribution of [LM3] is the proof of the Theorem for linear groups, with most of the work expended in the characteristic 0 case.

Let, then, G be a finitely generated subgroup of $\mathrm{GL}(n, F)$, for some n, and some field F of characteristic 0. The Hilbert Nullstellensatz shows that G is

residually linear of degree n over the field K of algebraic numbers. The PSG condition is transferred from G to its quotient groups in $\mathrm{GL}(n, K)$, and it suffices to know that these quotient groups are soluble by finite, because then they are soluble of bounded length by finite of bounded order (see e.g. [We], Corollary 10.11; this is a combination of a theorem of Zassenhaus on soluble linear groups of Jordan's theorem on finite linear groups).

We thus assume that G is a subgroup of $\mathrm{GL}(n, K)$. Since G is finitely generated, it is contained in a group $\mathrm{GL}(n, L)$, where L is a finitely generated subfield of K, and thus $|L : \mathbf{Q}| < \infty$. Changing n, we may assume that $G \leq \mathrm{GL}(n, \mathbf{Q})$. Finally, again because G is finitely generated, we may assume that $G \leq \mathrm{GL}(n, R)$, where $R = \mathbf{Z}[1/p_1, \ldots, 1/p_k]$ is a finitely generated ring over $\mathbf{Z}$.

At this stage we can produce some subgroups of finite index. Indeed, if m is a natural number not divisible by any of the primes $p_1, \ldots, p_k$, then the principal congruence subgroup (mod m), i.e. the kernel of the homomorphism $G \to \mathrm{GL}(n, R/mR)$, has finite index. However, we still do not have enough control on these images to estimate their number. The situation becomes better on passing from G to its Zariski closure $\bar{G}$ (in $\mathrm{GL}(n, R)$). If $\bar{G}$ is not soluble by finite, we can replace it by an image of the form $\mathbf{A}(R)$, where $\mathbf{A}$ is a semi-simple algebraic group defined over $\mathbf{Q}$, and a little further argument allows us to assume that $\mathbf{A}$ is also connected and simply connected (the reader can think about $\mathbf{A} = SL(n, -)$ as a typical example). The factor group of this group over its principal congruence subgroup is now the full group $\mathbf{A}(R/mR)$. Decomposing this group as a direct product of groups $\mathbf{A}(R/qR)$, with q being a prime power, and using the fact that this latter group is (almost always) of even order, we can produce, using the Prime Number Theorem (a weak version suffices), enough such finite images, estimate their orders and number, and construct big enough elementary abelian 2-groups in them, to show that $\bar{G}$ is not a PSG group.

The snag in this procedure is that $\bar{G}$ and G do not necessarily share the same finite quotients. Therefore we introduce also $\hat{G}$, the congruence closure of G, i.e. the closure under the topology of $\mathrm{GL}(n, R)$ induced from the topology of R with ideals mR as a basis of neighborhoods of 0. Then G and $\hat{G}$ do have the same image in $\mathrm{GL}(n, R/mR)$, indeed $\hat{G}$ can be defined as the largest subgroup of $\mathrm{GL}(n, R)$ having these images. Finally, the crucial observation is that the Strong Approximation Theorem of [MVW] and [No] shows that $\hat{G}$ has finite index in $\bar{G}$, and therefore the counting procedure employed above for $\bar{G}$ applies also to

$\hat{G}$ and G, and, unless all three of these groups are soluble by finite, produces a contradiction. Once we know that our group is virtually soluble, the fact that it has finite rank follows from [S1], or by an argument of the type described in Section 2 below.

2. Residually Soluble Groups

The next stage is the case of a residually-p group G, and this is where the theory of p-adic analytic groups comes in. We form the pro-p completion G_p of G, which is a PSG pro-p group. In such a group we consider all sections of the type H/K mentioned above. It follows that the ranks of these sections are bounded, and hence pro-p PSG groups are p-adic analytic groups, by [LM1]. This implies that G_p is linear over the p-adic field $\mathbf{Q}_p$, and the previous case applies.

Though it is not needed for the continuation of the proof, we remark that at this stage we also have the proof for the case of linear groups of characteristic p, because they are virtually residually-p. This forms an interesting instance of non-standard lifting from a finite characteristic to characteristic 0.

In [MS] this is extended to residually (finite soluble) groups. A more elaborate counting argument shows that if G is a PSG group, there exists a number r such that the ranks of all finite soluble images of G are bounded by r. If we assume that all finite images of G are soluble (an assumption that will be justified later), we see that G is what we call of **finite upper rank**, i.e. the ranks of all of its finite images are bounded (equivalently, the profinite completion of G is of finite rank). It is shown in Theorem A of [MS] that finitely generated groups of finite upper rank are virtually soluble of finite rank. It is at this stage that the theory of infinite soluble groups is needed (this proof is described in detail in section 6.2 of [DDMS]).

3. Chief Factors

Given the list of finite simple groups, it is not difficult to show that they all contain relatively big elementary abelian subgroups. Now let H/K be a finite chief factor of a group G. Suppose that H/K is not abelian, and consider the factor group G/C, where $C = C_G(H/K)$. This is the group of automorphisms that G induces on H/K, and since H/K is not abelian, this group of automorphisms includes the inner automorphisms, a subgroup isomorphic to H/K. Replacing H/K by this group of inner automorphisms, we not only can assume that $|G : H|$

is finite, we also get a reasonable bound on this index, and this enables us to play our usual game and establish the following result (Theorem 4.1 of [MS]).

PROPOSITION CF: *Let G be a PSG group. Then there exists a number n such that, if H/K is a non-abelian finite chief factor of G, then H/K is a direct product of at most n isomorphic finite simple groups, these simple groups being either sporadic, alternating of degree at most n, or of Lie type of (Lie) rank at most n, over a finite field of dimension at most n over its prime subfield.*

Unfortunately, this still leaves us with possibly infinitely many such chief factors, as we do not say anything about the characteristic of the groups of Lie type, and if G is not finitely generated, there are examples involving infinitely many non-isomorphic chief factors. We do get the following (see the proof of Theorem D of [MS]).

COROLLARY: *For a PSG group G, there exists a number m, such that for any finite chief factor H/K of G, the automorphism group of H/K has a faithful representation of degree at most m over some finite field.*

This is used in [MS] to prove a special case of the Theorem. The new ingredient that enables us to prove the full result is the following simple, but crucial, lemma, which is a variant of an argument that appears in [Wi].*

LEMMA: *Let G be a finitely generated group, n a positive integer, and Ω a family of fields. If G can be embedded in the Cartesian product $\prod GL(n,F)(F \in \Omega)$, then G is a subdirect product of finitely many linear groups of degree n. If moreover Ω contains only finitely many fields of each positive characteristic, and these are finite, then G is isomorphic to a linear group over some field of characteristic 0.*

Proof: Let S be the ring $\prod F(F \in \Omega)$. Then $G \leq \mathrm{GL}(n,S)$. Since G is finitely generated, it follows that $G \leq \mathrm{GL}(n,R)$, for some finitely generated subring R of S. Now R is a commutative Noetherian ring without nilpotent elements, hence it contains only finitely many minimal prime ideals, say $P_1,\ldots,P_t$, and these intersect in 0. Thus $\mathrm{GL}(n,R)$ can be embedded in $\prod \mathrm{GL}(n,K_i)$, where K_i is the field of fractions of the domain R/P_i. The first claim of the lemma is proved.

* See Lemma 4.2 there. The authors are grateful to the author of [Wi] for permission to quote that paper prior to publication. As mentioned, [Wi] is generally relevant to our line of ideas, containing substantial improvements of some of the results in [LM2] and [MS].

For the second claim, assume that Ω has the stated property. Suppose that $P_1, \ldots, P_s$ are those P_i for which R/P_i has finite characteristic. Let L be their intersection, and let M be the intersection of $P_{s+1}, \ldots, P_t$. Let q be the product of the characteristics of the domains $R/P_1, \ldots, R/P_s$. Then $qR \leq L$, so $qM \leq L \cap M = 0$. The hypotheses on Ω imply that S, and hence R, contains only finitely many elements of additive order q. Hence M is finite, and so is the kernel K of the projection $\mathrm{GL}(n, R) \to \prod \mathrm{GL}(n, R/P_i)$ $(i = s+1, \ldots, t)$. Thus $H = G/G \cap K$ is a product of finitely many linear groups in characteristic 0, and hence H is linear in characteristic 0. Now $G \cap K$ is finite and G is residually finite, hence G has a subgroup of finite index which is linear in characteristic 0, and then G itself is linear in characteristic 0.

We have arrived at the end of the road. ∎

Proof of the Theorem: Let G be a finitely generated PSG group. Let N be the intersection of the centralizers of all the non-abelian finite chief factors of G. Proposition CF and its Corollary show that G/N is residually linear of degree m over a set of fields as in the Lemma, so this Lemma shows that G/N is a linear group of characteristic 0. By the first stage of the proof, G/N is soluble by finite. Let M/N be a soluble normal subgroup of finite index in G/N. If H/K is a finite non-abelian chief factor of G, it is a chief factor of G/C, where $C = C_G(H/K)$, and hence also of G/N, and therefore of G/M. If M has any non-abelian finite chief factor, such a factor can be embedded in a finite chief factor of G, but such factors are centralized by M, a contradiction. This implies that all finite factor groups of M are soluble. But M itself is a finitely generated PSG group, so the result mentioned in section 3 shows that it is soluble by finite (therefore actually soluble) and so is G.

References

[DDMS] J.D. Dixon, M.P.F. duSautoy, A. Mann and D. Segal, *Analytic pro-p Groups*, London Math. Soc. LNS 157, Cambridge University Press, 1991.

[dS1] M.P.F. duSautoy, *Finitely generated groups, p-adic analytic groups and Poincaré series*, Bull. Am. Math. Soc. **23**(1990), 121–126 (also Appendix C of [DDMS]).

[dS2] M.P.F. duSautoy, *Applications of p-adic methods to group theory*, in *p-Adic Methods and Their Application* (A. Baker and R. Plyman, eds.), Oxford University Press, 1992.

[GSS] F.J. Grunewald, D. Segal and G.C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185–223.

[I] I. Ilani, *Counting finite index subgroups and the P. Hall enumeration principle*, Isr. J. Math. **68** (1989), 18–26.

[La] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. IHES **26** (1965), 389–603.

[LM1] A. Lubotzky and A. Mann, *Powerful p-group , I & II*, J. Algebra **105** (1987), 484–515.

[LM2] A. Lubotzky and A. Mann, *Residually finite groups of finite rank*, Math. Proc. Camb. Phil. Soc. **106** (1989), 385–388.

[LM3] A. Lubotzky and A. Mann, *On groups of polynomial subgroup growth*, Invent. Math. **104** (1991), 521–533.

[Lu] A. Lubotzky, *A group-theoretic characterization in linear groups*, J. Algebra **113** (1988), 207–214.

[M1] A. Mann, *Some applications of powerful p-groups*, in *Groups—St. Andrews 1989*, Vol. 2, London Math. Soc. LNS 160, Cambridge University Press, 1991, pp. 370–385.

[M2] A. Mann, *Some properties of polynomial subgroup growth groups*, Israel J. Math. **82** (1993), 373–380.

[MS] A. Mann and D. Segal, *Uniform finiteness conditions in residually finite groups*, Proc. London Math. Soc. (3) **61** (1990), 529–545.

[MVW] C.R. Matthews, L.N. Vaserstein and B. Weisfeller, *Congruence properties of Zariski-dense subgroups I*, Proc. London Math. Soc. **48** (1984), 514–532.

[Ne] M. Newman, *Asymptotic formulas related to free products of cyclic groups*, Math. Comp. **30** (1976), 838–846.

[No] M. Nori, *On subgroups of $GL_n(\mathbf{F}_p)$*, Invent. Math. **88** (1987), 257–275.

[R] D.J.S. Robinson, *Finiteness Conditions and Generalized Soluble Groups II*, Springer-Verlag, Berlin, 1972.

[S1] D. Segal, *Subgroups of finite index in soluble groups I*, in *Groups—St. Andrews 1985*, London Math. Soc. LNS 121, Cambridge University Press, 1986, pp. 307–314.

[S2] D. Segal, *Residually finite groups*, in *Groups—Canberra 1989*, Lecture Notes in Math. **1456**, Springer-Verlag, Berlin, 1990, pp. 85–95.

[Sh] A. Shalev, *Growth functions, p-adic analytic groups, and groups of finite coclass*, J. London Math. Soc., to appear.

[We] B.A.F. Wehrfritz, *Infinite Linear Groups*, Springer-Verlag, Berlin, 1973.

[Wi] J.S. Wilson, *Two-generator conditions for residually finite groups*, Bull. London Math. Soc. **104** (1991), 239–248.