TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 351, Number 9, Pages 3793–3822
S 0002-9947(99)02220-5
Article electronically published on April 20, 1999

ON THE DEGREE OF GROUPS OF POLYNOMIAL SUBGROUP GROWTH

ANER SHALEV

ABSTRACT. Let G be a finitely generated residually finite group and let $a_n(G)$ denote the number of index n subgroups of G. If $a_n(G) \leq n^\alpha$ for some α and for all n, then G is said to have polynomial subgroup growth (PSG, for short). The degree of G is then defined by $\deg(G) = \limsup \frac{\log a_n(G)}{\log n}$.

Very little seems to be known about the relation between $\deg(G)$ and the algebraic structure of G. We derive a formula for computing the degree of certain metabelian groups, which serves as a main tool in this paper. Addressing a problem posed by Lubotzky, we also show that if $H \leq G$ is a finite index subgroup, then $\deg(G) \leq \deg(H) + 1$.

A large part of the paper is devoted to the structure of groups of small degree. We show that $a_n(G)$ is bounded above by a linear function of n if and only if G is virtually cyclic. We then determine all groups of degree less than $3/2$, and reveal some connections with plane crystallographic groups. It follows from our results that the degree of a finitely generated group cannot lie in the open interval $(1, 3/2)$.

Our methods are largely number-theoretic, and density theorems à la Chebotarev play essential role in the proofs. Most of the results also rely implicitly on the Classification of Finite Simple Groups.

1. INTRODUCTION

Let G be a finitely generated residually finite group, and let $a_n(G)$ be the number of subgroups H of index n in G. We say that G has *polynomial subgroup growth* (*PSG* for short) if there is a real number $\alpha \geq 0$ such that $a_n(G) \leq n^\alpha$ for all n. The area of subgroup growth and of PSG groups in particular has been investigated quite thoroughly in the past decade; see for instance [GSS], [LM], [MS1], [LMS], [dS], [SSh1], [L1] and the recent survey papers [L2], [L3], [MS2]. In [LMS] finitely generated PSG groups are characterized as virtually soluble groups of finite rank. Non-finitely generated PSG groups have just been characterized in [SSh2] in terms of their profinite completion.

In spite of considerable progress in the understanding of PSG groups in general, very little is known about specific types of polynomial growth, and their relation to the structure of the underlying groups. Recall that the *degree* of a PSG group G is defined by

$$\deg(G) = \limsup_{n\to\infty} \frac{\log a_n(G)}{\log n}.$$

Received by the editors July 10, 1996 and, in revised form, March 8, 1997.
1991 *Mathematics Subject Classification.* Primary 20E07, 20E34.
This work was supported in part by a grant from the Israel Science Foundation.

©1999 American Mathematical Society

Thus $\alpha \geq \deg(G)$ if and only if $a_n(G) = O(n^{\alpha+\varepsilon})$ for every $\varepsilon > 0$.

While the degree of the Milnor-Wolf growth function of a finitely generated group is always an integer, which can be computed effectively using [Ba] and [Gr], the degree of a PSG group need not be an integer, and no formula is known for its computation. Furthermore, experience shows that determining $\deg(G)$ may be quite tricky, even for well-understood groups G (the most striking example is that of torsion-free nilpotent groups, where $\deg(G)$ is still unknown in general). It therefore seems unlikely that a general formula for calculating $\deg(G)$ will ever be found, and so attention focuses naturally on some nice classes of groups. Theorem 1.6 below provides a formula for computing the degree of a large class of metabelian groups.

It is shown in [Sh3] that there are no groups of degree strictly between 0 and 1. However, if $\alpha \geq 1$ is a real number, then, by [Sh2, Theorem 1.3], there exists a (topologically 2-generated) *profinite* group G whose degree is precisely α (the proof of this result relies heavily on sieve methods from analytic number theory).

In this paper we focus on finitely generated *abstract* groups of degree ≥ 1, and show that (in contrast with the profinite case), not all real numbers exceeding 1 can be obtained as degrees of such groups (see Theorem 1.5 below). We also characterize groups of given small degree, and classify the precise growth types of such groups.

It should be emphasized that (unlike the proofs in [Sh2], [Sh3]) the proofs of our results here apply the characterization of PSG groups obtained in [LMS], and therefore depend implicitly on the Classification of Finite Simple Groups (CFSG).

Note that, if $H \leq G$ is a finite index subgroup, then $\deg(G) \geq \deg(H)$; one of the subtleties in the study of the degree of PSG groups stems from the fact that $\deg(G)$ can well exceed $\deg(H)$ in this case (the simplest example which was already noted by G.C. Smith [S] is $G = D_\infty$, the infinite dihedral group which has degree 1, and $H = \mathbb{Z}$, the infinite cyclic group which has degree 0). Therefore classifying groups of given degree up to finite extensions does not make sense, and the degree preserving finite extensions of each relevant group must be carefully analyzed.

In fact, the problem of studying the relation between the subgroup growth of G and that of its finite index subgroups was suggested by Lubotzky in [L2, p. 393]. Our contribution is as follows.

Theorem 1.1. *Let G be a finitely generated group and let $H \leq G$ be a finite index subgroup. Then*

$$\deg(G) \leq \deg(H) + 1.$$

This upper bound is of course best possible. In some cases (for instance, when H is abelian) it is possible to say more on the relation between $\deg(G)$ and $\deg(H)$ (see Theorem 1.7 below).

While the process of passing from a group to a finite index subgroup is not degree preserving, there is a simple process which always preserves the degree, namely, factoring out a finite normal subgroup (see Lemma 2.3 below). So let us say that groups G_1 and G_2 are *equivalent* if there exist finite normal subgroups $N_i \lhd G_i$ $(i = 1, 2)$ such that $G_1/N_1 \cong G_2/N_2$. It is easy to see that this is indeed an equivalence relation. Since this relation respects the degrees it suffices to classify groups of given degree up to equivalence. We also say that G is *reduced* if it has no non-trivial finite normal subgroups (in particular, torsion-free groups are reduced). It can be shown that any finitely generated residually finite PSG group has a unique maximal finite normal subgroup (see Lemma 2.4 below). This enables us to assume, in studying $\deg(G)$, that G is reduced.

Let us now examine groups of small degree. We start with the characterization of groups of linear subgroup growth, which is particularly simple.

Theorem 1.2. *Let G be a finitely generated residually finite group. Then $a_n(G) = O(n)$ if and only if G is virtually cyclic.*

It is shown in [Sh3] that finitely generated residually finite groups of sublinear subgroup growth have a cyclic *central* subgroup of finite index, and that the series $\{a_n(G)\}$ is bounded for such groups. Now, if G is virtually cyclic, let $A \lhd G$ be a cyclic normal subgroup of finite index, and let $H = C_G(A)$. Then G/H has order at most 2 and H has a finite index cyclic central subgroup. It follows that, if $a_n(G) \leq cn$ for all n (where c is some constant), then there is a subgroup $H \lhd G$ of index at most 2 and a constant b such that $a_n(H) \leq b$ for all n.

Using Theorem 1.2 it is also easy to see that G has linear – but not sublinear – subgroup growth if and only if G is equivalent to D_∞.

It should be emphasized that the subgroup growth of groups of degree 1 can be super-linear; for example, $a_n(\mathbb{Z} \times \mathbb{Z}) = \sigma(n)$, the sum of divisors of n (see [Me, Theorem 1] or Lemma 2.2 below), which can go up to $cn \log\log n$. Our next result determines all groups of degree 1. We shall first introduce some notation which will be used throughout the paper. For a subring R of a number field K and a unit $u \in R$, let $R \rtimes \langle x_u \rangle$ denote the split extension of the additive group of R by the cyclic group $\langle x_u \rangle$, where the order of x_u equals the (multiplicative) order of u, and x_u acts on R as multiplication by u. By abuse of notation we shall sometimes write $R \rtimes \langle u \rangle$ instead of $R \rtimes \langle x_u \rangle$. More generally, if U is a subgroup of the group of units of R, we denote by $R \rtimes U$ (or $R \rtimes \langle x_u : u \in U \rangle$) the split extension of R by U with a similar action.

Theorem 1.3. *Let G be a finitely generated residually finite group. Then G has degree 1 if and only if G is equivalent to one of the following groups:*

1. *The dihedral group D_∞.*
2. *A plane crystallographic group which does not contain a 180° rotation.*
3. *$\mathbb{Z}[h, 1/h] \rtimes \langle h \rangle$, where $h \in \mathbb{Q} \setminus \{0, 1, -1\}$.*
4. *$\mathbb{Z}[h, 1/h] \rtimes \langle h, -1 \rangle$, where h is as above.*

The groups above are reduced, and so $\deg(G) = 1$ if and only if G has a finite normal subgroup N such that G/N is as in parts 1 – 4 above.

The crystallographic groups in part 2 are known, and split into 7 isomorphism classes, traditionally denoted by p1, pg, pm, cm, p3, p3m1, and p31m. For the precise definition and structure of these groups, see Coxeter and Moser [CM, pp. 40-52, 136-137]. They are all extensions of $\mathbb{Z} \times \mathbb{Z}$ by subgroups of the symmetric group S_3; for instance, p1 $\cong \mathbb{Z} \times \mathbb{Z}$, pm $\cong D_\infty \times \mathbb{Z}$, p3 $\cong \mathbb{Z}[\omega] \rtimes \langle \omega \rangle$ where ω is a cube root of unity, etc. In contrast, the groups in parts 3 and 4 constitute two infinite families of groups. It is a curious fact that the groups D_∞ and $D_\infty \times \mathbb{Z}$ have the same degree. We note that the zeta functions $\sum_{n \geq 1} a_n(G) n^{-s}$ associated with the 17 plane groups have just been determined by John McDermott.

The degree of G is a relatively crude invariant in the understanding of the asymptotic behaviour of $\{a_n(G)\}$. In some situations more refined information can be obtained. It turns out that there is a rather surprising trichotomy governing the subgroup growth of groups of degree 1.

For functions $f, g : \mathbb{N} \to \mathbb{R}$ we write $f \leq g$ if $f(n) \leq g(n)$ for all n, and $f \leq' g$ if $f(n) \leq g(n)$ for infinitely many n.

Theorem 1.4. *Let G be a finitely generated group of degree 1. Then there are positive constants b, c such that one of the following holds:*
(i) $bn \leq a_n(G) \leq cn$.
(ii) $bn \log\log n \leq' a_n(G) \leq cn \log\log n$.
(iii) $n^{1+b/\log\log n} \leq' a_n(G) \leq n^{1+c/\log\log n}$.

More specifically, condition (i) is satisfied when G is equivalent to the group of type 1 in 1.3, condition (ii) is satisfied if G is equivalent to a group of type 3 or 4, or to one of the groups p1, pg, pm , cm (of type 2), while condition (iii) is satisfied if G is equivalent to p3, p3m1, or p31m (of type 2).

Recall that, by [Sh3], the degree of a PSG group cannot lie in the open interval $(0, 1)$. The next result provides another restriction on $\deg(G)$, which is only valid for finitely generated groups.

Theorem 1.5. *The degree of a finitely generated group cannot lie strictly between 1 and 3/2.*

Thus Theorems 1.2 and 1.3 (combined with [Sh3]) actually determine all finitely generated groups of degree less than 3/2.

Finitely generated groups of degree 3/2 do exist, as shown by the example of the Heisenberg group

$$H = \langle x, y, z : [x, y] = z, [x, z] = [y, z] = 1\rangle;$$

see Smith [S], where the zeta functions of H and its subgroups are analyzed (see also Lubotzky [L2, p. 392] and Lemma 6.1 below).

Our results on groups of small degree depend heavily on a formula for computing the degree of certain metabelian groups. In order to state this formula, which seems to be of independent interest, we need some notation.

For an abelian group A we let $r_0(A) = \dim_{\mathbb{Q}}(A \otimes \mathbb{Q})$ be the torsion-free rank of A (namely the maximal rank of a torsion-free subgroup of A). Let us say that a finitely generated metabelian group G is of *semisimple type* if its Fitting subgroup $A = F(G)$ is abelian of finite rank, and $A \otimes \mathbb{Q}$ is a semisimple $\mathbb{Q}[G/A]$-module with no trivial irreducible components.

Theorem 1.6. *Let G be a metabelian group of semisimple type and let $A = F(G)$. Suppose G/A is infinite. Then*

$$\deg(G) = r_0(A) + r_0(G/A) - 1.$$

For examples where $F(G)$ and $G/F(G)$ are both infinite abelian and the conclusion of 1.6 is violated, see Lemma 6.1 below.

Theorem 1.6 does not cover groups which are virtually abelian. The degree of such groups can be computed as follows.

Theorem 1.7. *Let G be a finitely generated group with an abelian normal subgroup A of finite index. Then $\deg(G) = r_0(A) - 1$, unless there is an element $g \in G$ acting on $A \otimes \mathbb{Q}$ as multiplication by -1, in which case $\deg(G) = r_0(A)$.*

This theorem can be used to compute the degree of crystallographic groups.

Theorems 1.6 and 1.7 give rise to the following.

Corollary 1.8. *The degree of a metabelian group of semisimple type is always an integer.*

We close the introduction with a remark on groups which are not finitely generated (as abstract groups). It turns out that even our most basic result, namely Theorem 1.2, is not valid in this context; for example, if $G = \mathbb{Z}_p \times \mathbb{Z}_p$, then $a_n(G) = (pn-1)/(p-1)$ for all $n = p^k$ (and 0 otherwise); thus G has linear subgroup growth, although it is not virtually cyclic. The problem of characterizing non-finitely generated groups of linear subgroup growth will be discussed elsewhere.

Some words on the structure of this paper. In Section 2 we prove some preliminary results on subgroup growth (and derivations) which are used freely throughout this paper. This section concludes with the proof of Theorem 1.1, which applies [LMS] (hence CFSG) and some elementary cohomology. Section 3 is essentially number-theoretic; it focuses on growth of ideals in subrings R of number fields, and on related topics. We obtain there an important special case of Theorem 1.6, where (with previous notation) $G = R \rtimes U$ ($U \leq U(R)$). Our formula for the degree of such groups (and for the degree of metabelian groups of semisimple type in general) depends on density theorems from Number Theory. Section 4 contains the proof of Theorem 1.2, which is relatively easy modulo previous results. Section 5 is devoted to metabelian groups, and this is where Theorem 1.6 is established. In Section 6 we start the proof of Theorems 1.3–1.5, by showing that a finitely generated group of degree $< 3/2$ is either virtually abelian, or virtually (locally cyclic)-by-cyclic. In Section 7 we discuss (locally cyclic)-by-cyclic groups, their finite extensions, and the growth behaviour of these extensions. In Section 8 we analyze the growth behaviour of finite extensions of $\mathbb{Z} \times \mathbb{Z}$, thereby completing the proof of Theorems 1.3–1.5. More generally, we discuss there finite extensions of $\mathbb{Z}^d$ and prove Theorem 1.7. Some results on growth of submodules are proved along the way. Finally, in Section 9 we consider a nilpotent group of class 3 and Hirsch rank 4 and show that its degree is 5/3.

In spite of its length, this paper is just a first step towards a more general understanding of the growth behaviour of finitely generated groups. While Number Theory plays a central role here, it is still unclear whether it will also be essential in the next stages of this investigation. The results of this paper seem to open up several natural questions. For example, except for the intervals $(0,1)$, $(1,3/2)$, are there other intervals in which the degree of a finitely generated group cannot lie? Is the set of degrees of finitely generated groups discrete? Is it countable? Does it contain irrational numbers? There is also some interest in studying the related invariant $\alpha(G) = \limsup \log s_n(G)/\log n$, where $s_n(G)$ denotes the number of subgroups of index at most n in G. It can be shown that $\alpha(G)$ cannot lie in the interval $(1,2)$, and it is likely that there are additional restrictions. I hope to address some of these questions elsewhere.

Our notation is quite standard. The rank $\mathrm{rk}(G)$ of an abstract group G is the minimal r such that all finitely generated subgroups of G are r-generated. The lower central series of a group G is denoted by $\gamma_i(G)$, and $\mathrm{dl}(G)$ stands for the derived length of a soluble group G. The Fitting subgroup of a group G is denoted by $F(G)$. The soluble radical of a finite group G is denoted by $S(G)$.

For an abelian group A we denote by $\mathrm{Tor}(A)$ the subgroup of elements of finite order in A. For $n \in \mathbb{N}$, $\sigma(n)$ denotes the sum of divisors of n, and $d(n)$ is the number of divisors of n. We shall set $a_n(G) = \sigma(n) = 0$ if $n \notin \mathbb{N}$. Finally, we define

$$a'_n(G) = \max\{a_m(G) : m|n\}.$$

It is a pleasure to thank Dan Segal for useful discussions and for his very helpful criticism of an earlier version of this paper, Brian Birch and Udi de Shalit for some

number-theoretic advice, Geoff Smith and John McDermott for communicating to me some of their yet unpublished results on zeta functions of groups, and All Souls College, Oxford, for its warm hospitality while part of this work was carried out.

2. Preliminaries

For groups G, H let

$$\mathrm{der}(G,H) = \sup |\mathrm{Der}(G,H)|,$$

where the supremum is taken over all possible actions of G on H.

The following elementary result is essentially known.

Lemma 2.1. *Let G be a group and let $H \lhd G$.*

(i)

$$a_n(G) \leq \sum_{G_0,H_0} \mathrm{der}(N_{G_0}(H_0)/N_H(H_0), N_H(H_0)/H_0),$$

where the sum is taken over all subgroups $H_0 \leq H \leq G_0 \leq G$ such that

$$|G:G_0||H:H_0| = n \quad \textit{and} \quad N_G(H_0)H \geq G_0.$$

In particular,

$$a_n(G) \leq \sum_{m|n} a_{n/m}(G/H)a_m(H)D_{n,m},$$

where $D_{n,m} = \max \mathrm{der}(N_{G_0}(H_0)/N_H(H_0), N_H(H_0)/H_0)$ over subgroups H_0, G_0 as above with $|H:H_0| = m$, $|G:G_0| = n/m$.

(ii) Suppose $H = A$ is abelian. Then

$$a_n(G) \leq \sum_{G_0,A_0} |\mathrm{Der}(G_0/A, A/A_0)|,$$

where the sum is taken over all subgroups $A_0 \leq A \leq G_0 \leq G$ such that

$$|G:G_0||A:A_0| = n \quad \textit{and} \quad A_0 \lhd G_0.$$

In particular,

$$a_n(G) \leq \sum_{m|n} a_{n/m}(G/A)a_m(A)D_{n,m},$$

where $D_{n,m} = \max |\mathrm{Der}(G_0/A, A/A_0)|$ over the subgroups $A_0 \leq A \leq G_0$ with $|A:A_0| = m$, $|G:G_0| = n/m$ and $A_0 \lhd G_0$.

(iii) Suppose A is abelian and G splits over A, and let B be a complement to A in G (so that $G = A \rtimes B$). Then

$$a_n(G) = \sum_{A_0,B_0} |\mathrm{Der}(B_0, A/A_0)|,$$

where the sum is taken over all subgroups $A_0 \leq A$, $B_0 \leq B$ such that A_0 is B_0-invariant, and $|A:A_0||B:B_0| = n$.

Proof. This follows from the proof of [MS1, 3.1]. □

We now draw easy conclusions regarding the degree of PSG groups.

Lemma 2.2. *(i)* $\deg(H \times \mathbb{Z}) \leq \deg(H) + 1$, *with equality if H is abelian.*

(ii) Let A be a finitely generated abelian group of torsion-free rank $d \geq 1$. Then $\deg(A) = d - 1$, *and $a_n(A) \geq n^{d-1}$ for all n.*

(iii) $a_n(\mathbb{Z} \times \mathbb{Z}) = \sigma(n)$, the sum of divisors of n.

Proof. Apply part (i) of the preceding lemma. Since G/H is cyclic it has exactly one subgroup G_0/H of each given index, and we have

$$\mathrm{der}(N_{G_0}(H_0)/N_H(H_0), N_H(H_0)/H_0) \leq |H : H_0|.$$

This yields

$$a_n(H \times \mathbb{Z}) \leq \sum_{m|n} a_m(H)m.$$

Furthermore, by part (iii) of 2.1, equality holds if H is abelian. Part (i) of 2.2 now follows easily.

It follows immediately from (i) by induction on d that $\deg(\mathbb{Z}^d) = d - 1$. In general we have $G = \mathbb{Z}^d \times F$ where F is finite and it is easy to see that the degree is not changed (see for instance 2.3 below). The second assertion in (ii) follows by induction on d, using the inequality

$$a_n(\mathbb{Z}^d) = \sum_{m|n} a_m(\mathbb{Z}^{d-1})m \geq a_n(\mathbb{Z}^{d-1})n.$$

Applying the equality above for $d = 2$ we obtain part (iii). □

Note that 2.2(iii) was proved earlier in [Me].

Lemma 2.3. *Let G be a finitely generated PSG group, and let $F \lhd G$ be a finite normal subgroup. Then there is a constant c such that*

$$a'_n(G) \leq c \cdot a'_n(G/F) \quad \textit{for all } n.$$

In particular, $\deg(G) = \deg(G/F)$.

Proof. We have

$$a_n(G) \leq \sum_{m|n} a_{n/m}(G/F)a_m(F)D_{n,m},$$

where

$$D_{n,m} = \max_{G_0,F_0}\{\mathrm{der}(N_{G_0}(F_0)/N_F(F_0), N_F(F_0)/F_0)\},$$

where $G \geq G_0 \geq F \geq F_0$, $N_G(F_0)F \geq G_0$, $|F : F_0| = m$, $|G : G_0| = n/m$.

Let $r = \mathrm{rk}(G)$. Then $r < \infty$ by [LMS]. Since the groups $N_{G_0}(F_0)$ have finite index in G, they can be generated by at most r elements. This yields

$$D_{n,m} \leq m^r \leq |F|^r.$$

We can restrict the sum bounding $a_n(G)$ to $m \leq |F|$, and we have $\sum_{m\leq|F|} a_m(F) \leq |F|^r$ (since every subgroup of F is r-generated). We see that

$$a_n(G) \leq |F|^{2r} \cdot \max_{m|n, m\leq|F|} a_{n/m}(G/F).$$

The result follows. □

Lemma 2.4. *Let G be a finitely generated residually finite PSG group. Then G has a unique maximal finite normal subgroup F. Consequently, G has a reduced quotient $\overline{G}$ such that* $\deg(G) = \deg(\overline{G})$.

Proof. It is clear that the product of two finite normal subgroups of G is again a finite normal subgroup. Therefore it suffices to show that there is no infinite ascending chain of finite normal subgroups of G. By [LMS], G has a normal subgroup G_0 of finite index which is soluble minimax. So it suffices to show that G_0 does not contain such a chain. It is known that a soluble minimax group G_0 has a unique

maximal normal periodic subgroup, say H, which is a Chernikov group. In our case G_0 is residually finite, and so is H. However, a residually finite Chernikov group is clearly finite. Since any finite normal subgroup of G_0 is contained in H, the result follows. □

Clearly, Lemmas 2.3 and 2.4 reduce the study of the growth behaviour (in particular, the degree) of finitely generated PSG groups to the case of reduced groups.

We need a few lemmas on derivations. In applying Lemma 2.1 the following easy observation is often useful.

Lemma 2.5. *Let F be a finite group acted on by a cyclic group $\langle x\rangle$. Suppose either x has infinite order, or x has order $k<\infty$ and $a^{x^{k-1}}a^{x^{k-2}}\cdots a^x a=1$ for all $a\in F$. Then $|\mathrm{Der}(\langle x\rangle,F)|=|F|$.*

Proof. Set $C=\langle x\rangle$. Then each derivation $\delta\in\mathrm{Der}(C,F)$ is determined by $\delta(x)\in F$. Therefore $|\mathrm{Der}(C,F)|\le|F|$. To prove equality we have to show that for each $a\in F$ there is $\delta\in\mathrm{Der}(C,F)$ such that $\delta(x)=a$. Indeed, given a, we define $\delta: C\to F$ by $\delta(1)=1$,

$$\delta(x^i)=a^{x^{i-1}}a^{x^{i-2}}\cdots a^x a,$$

and

$$\delta(x^{-i})=(\delta(x^i)^{x^{-i}})^{-1},$$

where $i>0$. It is easy to see that, under our assumptions, δ is a well-defined derivation satisfying $\delta(x)=a$. The result follows. □

Remark. If A is an abelian group (not necessarily finite) and x acts on A as in 2.5, then the proof shows that $\mathrm{Der}(\langle x\rangle,A)\cong A$.

Lemma 2.6. *Let F be a finite group and let M be a finite $\mathbb{Z}F$-module. Then*

$$|\mathrm{Der}(F,M)|\le c\cdot|M/M^F|,$$

where c depends on $|F|$ and on the number of generators $d(M)$ of M (as an abelian group), and $M^F=C_M(F)$.

Proof. The subgroup of inner derivations from F to M has order $|M/M^F|$, so $|\mathrm{Der}(F,M)|=|H^1(F,M)||M/M^F|$. It therefore suffices to show that the order of $H^1(F,M)$ is bounded above in terms of $|F|$ and $d(M)$. It is well known that the abelian group $H^1(F,M)$ has exponent dividing $|F|$ (see for instance [B, 15.5]). We also have $d(H^1(F,M))\le d(F)d(M)$ (in fact the same holds for $d(\mathrm{Der}(F,M))$). It follows that

$$|H^1(F,M)|\le|F|^{d(F)d(M)}.$$

The lemma is proved. □

Proposition 2.7. *Let F,R be finite groups. Set $f=|F|$, $r=\mathrm{rk}(R)$, $S=S(R)$, the soluble radical of R, $i=|R:S|$ and $l=\mathrm{dl}(S)$. Then*

$$\mathrm{der}(F,R)\le c|R|,$$

where c depends on f,r,i,l.

Proof. We rely on the inequality

$$\mathrm{der}(F,R)\le\mathrm{der}(F,R_0)\mathrm{der}(F,R/R_0),$$

which holds for every characteristic subgroup R_0 of R. Let $S^{(j)}$ $(0 \leq j \leq l)$ be the derived series of S. Then

$$\mathrm{der}(F,R) \leq \mathrm{der}(F,R/S)\prod_{j=0}^{l-1}\mathrm{der}(F,R^{(j)}/R^{(j+1)}).$$

Now, $\mathrm{der}(F,R/S) \leq i^f$, and $\mathrm{der}(F,R^{(j)}/R^{(j+1)}) \leq C|R^{(j)}/R^{(j+1)}|$ by the preceding lemma, where C is a constant depending on f and r. It follows that

$$\mathrm{der}(F,R) \leq i^f C^l |S| \leq c|R|,$$

where $c = i^f C^l$. The result follows. □

We can now deduce the main result of this section, which implies Theorem 1.1.

Theorem 2.8. *Let G be a finitely generated PSG group, and let $H \leq G$ be a finite index subgroup. Then there is a constant c such that $a'_n(G) \leq cn \cdot a'_n(H)$ for all n. Consequently,* $\deg(G) \leq \deg(H) + 1$.

Proof. Replacing H with its core H_G if needed, we may assume that $H \lhd G$. By [LMS], G has a finite index soluble normal subgroup, say S. Set $i = |G : S|$, $l = \mathrm{dl}(S)$. We also have $r = \mathrm{rk}(G) < \infty$. Set also $f = |G : H|$. Write

$$a_n(G) \leq \sum_{m|n} a_{n/m}(G/H)a_m(H)D_{n,m},$$

where $D_{n,m}$ is as in 2.1(i). Clearly, we may restrict this sum to $m = n/k$, where k divides n and f (so $k \leq f$). Fix n and m. Then there is a finite group F of order at most f and a finite group R with $|R| \leq m$, $\mathrm{rk}(R) \leq r$, $|R : S(R)| \leq i$, $\mathrm{dl}(S(R)) \leq l$, such that $D_{n,m} = \mathrm{der}(F,R)$. It follows from Proposition 2.7 that

$$D_{n,m} \leq cm,$$

where c depends on f, i, r, l. Hence

$$a_n(G) \leq c \sum_{k|n, k\leq f} a_k(G/H)a_{n/k}(H)n/k \leq cf^{\log f} n a'_n(H).$$

The result follows. □

3. Number-theoretic preparations

In this section we record the number-theoretic results which will be applied throughout this paper.

Given a Dedekind ring R and an ideal $I \lhd R$, we let $N(I)$ denote the norm of I (which coincides with $|R/I|$). Put

$$i_n(R) = |\{I \subset R : I \text{ is an ideal of norm } n\}|.$$

Note that, by the unique factorization of ideals in number fields we have $i_{mn}(R) = i_m(R)i_n(R)$ provided m, n are coprime.

Lemma 3.1. *Let K be a number field, and let $R \subset K$ be a finitely generated subring. Then one of the following holds.*

(i) $R \subset \mathbb{Q}$, in which case $i_n(R) \leq 1$ for all n.

(ii) The series $\{i_n(R)\}$ is unbounded.

Proof. If $R \subset \mathbb{Q}$ then R is locally cyclic and we obviously have $i_n(R) \leq 1$ for all n. So suppose R is not contained in $\mathbb{Q}$.

Claim. There is a rational prime p and two distinct prime ideals $P, Q \lhd R$ such that $P \cap \mathbb{Z} = Q \cap \mathbb{Z} = p\mathbb{Z}$.

Indeed, it is easy to see that, for infinitely many rational primes p, the ideal pR is not prime (this follows, e.g., from the elementary fact that any non-linear polynomial $f(x) \in \mathbb{Q}[x]$ is reducible modulo infinitely many primes p). Let S denote this set of primes. Then for $p \in S$ we have $pR = \prod_{i=1}^{k} P_i$ where $k \geq 2$ and P_i are primes of R (not necessarily distinct). Now, only finitely many primes of R (i.e. those dividing the discriminant $\Delta(R)$) have ramification index ≥ 1. This implies that for almost all primes $p \in S$, pR is divisible by at least two distinct primes of R.

Now let P, Q be as in the claim. Then $N(P) = p^\alpha$ and $N(Q) = p^\beta$ for some positive integers α, β. Therefore

$$N(P^{\beta i} Q^{\alpha j}) = p^{\alpha\beta(i+j)}.$$

Given $k \geq 0$ there are $k+1$ pairs (i, j) with $i, j \geq 0$ and $i + j = k$. Since the corresponding ideals $P^{\beta i} Q^{\alpha j}$ are all distinct, it follows that

$$a_{p^{\alpha\beta k}}(R) \geq k + 1.$$

As k is arbitrary, the result follows. □

The proof above shows that, if R is as in part (ii), then $i_n(R) \geq c \log n$ for a fixed $c > 0$ and for infinitely many n. In fact, invoking deeper results from number theory, sharper bounds on $i_n(R)$ can be derived. We say that a subring R of a number field K is *full* if its field of fractions $\mathrm{Frac}(R)$ coincides with K.

Lemma 3.2. *Let $K \neq \mathbb{Q}$ be a number field, and let $R \subset K$ be a finitely generated full subring. Then there exist constants $b, c > 0$ such that*

(i) $i_n(R) \leq n^{c/\log\log n}$ for all n.

(ii) $i_n(R) \geq n^{b/\log\log n}$ for infinitely many n.

Proof. Let $d = [K : \mathbb{Q}]$. We claim that

$$i_n(R) \leq d(n)^d \quad \text{for all } n,$$

where $d(n)$ is the number of divisors of n. Since the functions i_n and $d(n)$ are both multiplicative (w.r.t. coprime arguments), it suffices to consider the case where n is a prime power, say $n = p^k$. Let $P_1, \ldots, P_l$ be the prime ideals above p, and let $N(P_i) = p^{d_i}$ $(i = 1, \ldots, l)$. Note that $1 \leq l \leq d$. If I is an ideal of norm n, then $I = P_1^{m_1} \cdots P_l^{m_l}$ for some $m_i \geq 0$ satisfying

$$\sum_{i=1}^{l} m_i d_i = k.$$

Since $m_i \leq k$ for all i, the number of solutions of the above equation is trivially bounded above by $(k+1)^l$. This yields

$$i_n(R) \leq (k+1)^l = d(n)^l \leq d(n)^d,$$

proving the claim.

Now, it is known that $d(n) \leq n^{(\log 2 + o(1))/\log\log n}$ [HW, Theorem 317]. Hence part (i) follows.

The proof of part (ii) is somewhat less elementary, and involves density theorems. Let S be the set of rational primes p such that pR splits as a product of d distinct

primes of R, say $P_1, \dots, P_d$ (each having degree 1). It follows from density theorems à la Chebotarev (see for instance [N, pp. 340-344] and in particular Theorem 7.10*) that S has positive density. For $x > 0$, let $S_x = \{p \in S : p \leq x\}$. Then there is a constant $\delta > 0$ such that, if x is sufficiently large, then

$$|S_x| \geq \delta \frac{x}{\log x}.$$

Let x be a sufficiently large number, and let $n = \prod_{p \in S_x} p$. Then $n \leq e^{(1+o(1))x}$ (since the product of all primes up to x is of that order). Therefore $x \geq (1 - o(1)) \log n$.

Now, to count ideals of norm n in R, note that $i_p(R) = d$ for all $p \in S$, so

$$i_n(R) = \prod_{p|n} i_p(R) = d^{|S_x|} \geq d^{\delta x / \log x}.$$

This yields

$$i_n(R) \geq d^{(\delta - o(1))(\log n / \log\log n)} = n^{(b+o(1))/\log\log n},$$

where $b = \delta \log d$. This proves part (ii). □

Corollary 3.3. *Let K be a number field, and let $R \subset K$ be finitely generated full subring. Define*

$$b_n = \sum_{m|n} i_m(R) m.$$

(i) The series $\{b_n\}$ grows super-linearly with n.

(ii) If $K = \mathbb{Q}$, then $b_n \geq (e^{-\gamma} - o(1)) n \log\log n$ for infinitely many n, where γ is the Euler constant.

(iii) If $K \neq \mathbb{Q}$, then $b_n \geq n^{1+c/\log\log n}$ for infinitely many n, where c is some positive constant.

Proof. It suffices to prove parts (ii) and (iii). Clearly $b_n \geq i_n(R) n$. Therefore part (iii) follows from 3.2. So suppose $R \subset \mathbb{Q}$. Then there exists an integer D such that

$$b_n \geq \sum_{m|n, \gcd(m,D)=1} m.$$

In particular, if n is prime to D, then $b_n = \sigma(n)$, the sum of all divisors of n. It is known that

$$\limsup \frac{\sigma(n)}{n \log\log n} = e^{-\gamma},$$

(see [HW, Theorem 323]), and it is easy to verify that the same holds if the limit is taken only over integers n which are prime to D. Part (ii) follows. □

Lemma 3.4. *Let K be a number field and let $R \subset K$ be a finitely generated full subring. Let u be a unit in R. Consider the split extension G of the additive group of R by a cyclic group $\langle y_u \rangle$ of infinite order, where y_u acts on R as multiplication by u. Then*

$$a_n(G) \geq \sum_{m|n} i_m(R) m.$$

Consequently, the subgroup growth of G is super-linear. Moreover,

(i) If $K = \mathbb{Q}$, then $a_n(G) \geq (e^{-\gamma} - o(1)) n \log\log n$ for infinitely many n.

(ii) If $K \neq \mathbb{Q}$, then $a_n(G) \geq n^{1+c/\log\log n}$ for infinitely many n.

Proof. Apply the last part of Lemma 2.1 with $A = R, B = \langle y \rangle$ where $y = y_u$. This yields

$$a_n(G) \geq \sum_{m|n,I} |\mathrm{Der}(\langle y^{n/m} \rangle, R/I)|$$

where I ranges over all norm m ideals of R. By Lemma 2.5 we have $|\mathrm{Der}(\langle x^{n/m} \rangle, R/I)| = |R/I| = m$ for these ideals I. Therefore

$$a_n(G) \geq \sum_{m|n} i_m(R)m,$$

proving the first assertion. The other assertions of the lemma follow from Corollary 3.3. □

Remark. Let G be as in case (i) above. Let π be the (finite) set of primes p satisfying $pR = R$. Given $n \in \mathbb{N}$, let $n_{\pi'}$ denote the π'-part of n (namely the maximal divisor of n which is prime to all primes in π). Then it is straightforward to verify that

$$a_n(G) = \sigma(n_{\pi'}).$$

We do not have a satisfactory formula for computing $a_n(G)$ in case (ii).

Lemma 3.5. *Let $\{p_i\}$ be an increasing sequence of primes of positive density. Then there exists a series $\{\varepsilon_k\}$ which tends to 0 with k, such that*

$$\mathrm{lcm}(p_1 - 1, p_2 - 1, \ldots, p_k - 1) \leq (p_1 p_2 \cdots p_k)^{\varepsilon_k}.$$

Proof. Fix a large number $x > 0$. Let $f(x)$ denote the least common multiple of the numbers $p-1$, where $p \leq x$ is a prime, and let $g(x)$ be the product of all primes $p \leq x$. We claim that $\log f(x)/\log g(x) \to 0$ as $x \to \infty$. It is well known that $\log g(x) = (1 + o(1))x$, and so it suffices to show that

$$\log f(x) = o(x).$$

It is clear that $\log f(x) = \sum_q \log q$, where q ranges over all prime powers with the property that, for some positive integer i, $qi + 1$ is a prime $\leq x$. Let S denote the set consisting of these prime powers.

Fix large constants $y < z < x$ such that $z < x/y$. Let $S_{x/y} = \{q \in S : q > x/y\}$. Then

$$\log f(x) \leq \sum_{q \in S, q \leq x/y} \log q + \sum_{q \in S_{x/y}} \log q \leq (1 + o(1))\frac{x}{y} + \sum_{q \in S_{x/y}} \log q. \tag{1}$$

For an integer $1 \leq i \leq y$ put

$$S_{x/y,i} = \{q \in S_{x/y} : qi + 1 \leq x \text{ is prime}\}.$$

Then $S_{x/y} = \bigcup_{1 \leq i \leq y} S_{x/y,i}$. Let $q \in S_{x/y,i}$. Then $qi + 1 > x/y > z$ is prime, hence $qi + 1 \not\equiv 0 \bmod p$ for all primes p in the interval $(y, z]$. Note that $i \not\equiv 0 \bmod p$ for these primes p (as $i \leq y < p$). We conclude that the prime powers $q \in S_{x/y,i}$ satisfy $q \not\equiv -1/i \bmod p$, where p ranges over the primes in the interval $(y, z]$.

The prime number theorem in arithmetic progressions (see for instance [E, Theorem 8.8, p. 277] for a strong version which includes an error term) shows that, if y, z are fixed and x is sufficiently large, then

$$\sum_{q \in S_{x/y,i}} \log q \leq (1 + o(1)) \prod_{y \leq p \leq z} (1 - \frac{1}{p}) \cdot x \leq (1 + o(1))\frac{\log y}{\log z} \cdot x.$$

Letting i vary we deduce that

$$\sum_{q \in S_{x/y}} \log q \leq (1+o(1)) \frac{y \log y}{\log z} \cdot x.$$

Combining this with (1) we obtain

$$\log f(x) \leq (1+o(1)) \{ \frac{1}{y} + \frac{y \log y}{\log z} \} \cdot x.$$

Choosing y large and z much larger we obtain the claim (for instance, let $z = y^{y^2}$; then $\log f(x) \leq (1+o(1)) \frac{2}{y} x$).

Now, if $\{p_i\}$ has positive density, then $\sum_{p_i \leq x} \log p_i \geq \delta x$ for all large x and some fixed $\delta \geq 0$. Therefore, if $x = p_k$, then $\mathrm{lcm}(p_1 - 1, \dots, p_k - 1) \leq \mathrm{lcm} f(x) = (e^x)^{o(1)} = (e^{\delta x})^{o(1)} \leq (p_1 \cdots p_k)^{o(1)}$. The result follows. □

The next result applies density theorems again.

Proposition 3.6. *Let K be a number field and let $R \subset K$ be a finitely generated full subring. Then there exist infinite increasing series $\{l_k\}, \{m_k\}$ of positive integers with the following properties:*

(i) $|R/m_k R| = m_k^d$ for all k, where $d = [K : \mathbb{Q}]$.

(ii) $\frac{\log l_k}{\log m_k} \to 0$ as $k \to \infty$.

(iii) $u^{l_k} \in 1 + m_k R$ for all $u \in U(R)$.

Proof. As in the proof of 3.2 we consider the set S of rational primes p with the property that $pR = P_1 \cdots P_d$ for distinct primes $P_1, \dots, P_d$ of R. Note that each P_i has dimension 1 and so $R/pR \cong (\mathbb{F}_p)^d$ for $p \in S$. As before, S has positive density. Let $\{p_i\}$ be the primes in S in increasing order, and for $k \geq 1$ set

$$m_k = p_1 p_2 \cdots p_k,$$

and

$$l_k = \mathrm{lcm}(p_1 - 1, p_2 - 1, \dots, p_k - 1).$$

Then $R/m_k R \cong \prod_{i=1}^k (\mathbb{F}_{p_i})^d$, which is of order m_k^d. Applying the previous lemma we obtain $l_k \leq (m_k)^{\varepsilon_k}$ where $\varepsilon_k \to 0$, and so part (ii) also holds. Let $u \in U(R)$. Since $p_i - 1 | l_k$ for all $i \leq k$, we see that $u^{l_k} \equiv 1 \bmod m_k R$. The result is proved. □

Corollary 3.7. *Given integers $h_1, \dots, h_s > 1$ and a constant $c > 0$, there exists an integer $l > 1$ such that*

$$\gcd(h_1^l - 1, \dots, h_s^l - 1) \geq l^c.$$

Proof. This follows from the above result taking $K = \mathbb{Q}$ and $R = \mathbb{Z}[h_1^{-1}, \dots, h_s^{-1}]$. □

We can now prove a special (yet typical) case of Theorem 1.6.

Proposition 3.8. *Let K be a number field and let $R \subset K$ be a finitely generated full subring. Let $U \leq U(R)$ be a torsion-free subgroup of the group of units of R, and let $G = R \rtimes U$. Set $d = [K : \mathbb{Q}]$ and $r = d(U)$. Then*

$$\deg(G) = d + r - 1.$$

Proof. Let l_k, m_k be as in 3.6 and set $l = l_k$, $m = m_k$ for some fixed k. Let $U_0 = \langle u^l : u \in U \rangle$, the subgroup generated by all lth powers in U. Then $|U : U_0| = l^r$ and U_0 acts trivially on $R/mR \cong (C_m)^d$. Therefore every additive subgroup R_0 of R containing mR is U_0-invariant, and U_0 acts trivially on R/R_0. In particular this holds for subgroups R_0 of index m in R. It follows that

$$a_{l^r m}(G) \geq \sum_{R_0 \leq R, |R:R_0|=m} |\mathrm{Der}(U_0, R/R_0)| = \sum_{R_0 \leq R, |R:R_0|=m} |\mathrm{Hom}(U_0, R/R_0)|.$$

Now, by 2.2, R has at least m^{d-1} subgroups R_0 of index m. Since U_0 is a free abelian group of rank r we have $|\mathrm{Hom}(U_0, R/R_0)| = |R/R_0|^r = m^r$ for all R_0 as above. This yields

$$a_{l^r m}(G) \geq m^{d-1} m^r = m^{d+r-1}.$$

By 3.6(ii), for every $\varepsilon \geq 0$ there exists k such that $l_k \leq m_k^{\varepsilon}$. Thus, if k is large, then for some $n \leq m^{1+r\varepsilon}$ we have $a_n \geq m^{d+r-1}$. It follows that

$$\limsup \frac{\log a_n(G)}{\log n} \geq \frac{d+r-1}{1+r\varepsilon}$$

for all $\varepsilon > 0$, so $\deg(G) \geq d + r - 1$.

To prove the reverse inequality, write

$$a_n(G) \leq \sum_{m|n} a_{n/m}(U) a_m(R) D_{n,m},$$

as in Lemma 2.1. Then

$$D_{n,m} = \max_{U_0, R_0} |\mathrm{Der}(U_0, R/R_0)| \leq |R/R_0|^r = m^r.$$

Since $\deg(\mathbb{Z}^k) = k - 1$ we have $a_{n/m}(U) \leq (n/m)^{r-1+o(1)}$ and $a_m(R) \leq m^{d-1+o(1)}$. Therefore

$$a_n(G) \leq (n/m)^{r-1+o(1)} m^{d-1+o(1)} m^r = n^{r-1+o(1)} m^{d+o(1)} \leq n^{d+r-1+o(1)}.$$

The result follows. □

4. Linear growth

In this section we prove Theorem 1.2. Let G be a finitely generated residually finite group of linear subgroup growth. We have to show that G is virtually cyclic. To show this we may replace G with any of its finite index subgroups. Now, by the main result of [LMS], G has a soluble finite index subgroup H of finite rank. Without loss of generality we may assume that G is soluble of finite rank. Suppose, by contradiction, that G is not virtually cyclic. Then G has a minimal non-virtually cyclic quotient (this follows from the fact that virtually cyclic groups are finitely presented). Replacing G with such a quotient, we may therefore assume that every proper quotient of G is virtually cyclic, namely, that G is just not virtually cyclic.

Since G is soluble, it has a non-trivial abelian normal subgroup $A \lhd G$. Then G/A is virtually cyclic, and so we may assume that G/A is cyclic. In particular, G is metabelian. Note that, by replacing G with a suitable quotient if necessary, we can still assume that G is just not virtually cyclic.

We claim that G is not virtually nilpotent. Suppose otherwise and replace G with a nilpotent subgroup of finite index. Since G is nilpotent and not virtually cyclic, it follows that G maps onto $\mathbb{Z} \times \mathbb{Z}$. In view of 2.2(iii), we conclude that the subgroup growth of G is super-linear, a contradiction.

Having proved that G is not virtually nilpotent, it follows that G is just non-virtually nilpotent. We also know that G is metabelian. The structure of finitely generated metabelian groups which are just non-virtually nilpotent is known; see, e.g., [HKLSh, Lemma 2.1]. It follows from that result and the fact that G has finite rank that A is torsion-free, $A \otimes_{\mathbb{Z}} \mathbb{Q}$ is a finite field extension of $\mathbb{Q}$, which we denote by K, and that G is embedded in the split extension $K \rtimes K^*$ of the additive group of K by the multiplicative group K^*. Thus, if $G = \langle A, x\rangle$, then A can be identified with an additive subgroup of K and x acts on A as multiplication by u, where $u \in K^*$ is not a root of unity. Let $R = \mathbb{Z}[u, u^{-1}]$. Then R is a finitely generated subring of K which is easily seen to be full. Since A is $\langle x\rangle$-invariant we have $AR = A$. This implies that A is a fractional ideal of K. It follows that there is a fractional ideal $A_0 \leq A$ such that A_0 is principal and $|A : A_0| \leq \infty$. Let $G_0 = \langle A_0, x\rangle$. Then G_0 is a finite index subgroup of G, and so we may replace G by G_0 and assume A is principal. It follows that $A \cong R$, and so we may identify A with R.

Lemma 3.4 now shows that $a_n(G)$ grow super-linearly with n, a contradiction. Therefore G is virtually cyclic, as required. This proves the main implication in Theorem 1.2.

The other implication follows from Theorem 2.8. Indeed, if $H \leq G$ is a finite index cyclic subgroup of G, then we have $a_n(G) \leq a'_n(G) \leq ca'_n(H)n = cn$ for some constant c (of course, a direct elementary argument can also be provided).

Theorem 1.2 is proved. □

Note that our proof applied only the first assertion in Lemma 3.4. By applying the other parts we obtain the following.

Theorem 4.1. *Let G be a finitely generated residually finite group satisfying $a_n(G) = o(n \log\log n)$. Then G is virtually cyclic, and its subgroup growth is at most linear. Thus there is a gap from subgroup growth cn to subgroup growth $cn \log\log n$ in finitely generated groups.*

5. Metabelian groups of semisimple type

We start with some well known properties of finitely generated metabelian groups. Let G be a finitely generated group, and let $A \lhd G$ be an abelian subgroup such that G/A is also abelian. Then A is finitely generated as a G/A-module, and this implies that A has no subgroups of type C_{p^∞} (though it may have sections of this type). Assuming G has finite rank, it follows that the torsion part $\mathrm{Tor}(A)$ of A is finite, and that $A/\mathrm{Tor}(A) \leq \mathbb{Q}^r$ where $r = r_0(A)$.

We say that G *almost splits* over a normal subgroup $A \lhd G$ if there is a subgroup $B \leq G$ such that $A \cap B = 1$ and $|G : AB| < \infty$. In this case we say the B is an almost complement to A in G. The following result is due to Robinson (see [R2, p. 445] and [R3, 15.2.4]).

Lemma 5.1. *Let G be a metabelian group of semisimple type. Then G almost splits over $F(G)$.*

Proof. Let $A = F(G)$. If G/A acts irreducibly on $A \otimes \mathbb{Q}$ then the result follows from Robinson [R3, 15.2.4]. Otherwise A has an infinite G/A-invariant subgroup A_0 of infinite index. Considering G/A_0 and arguing by induction on $r_0(A)$, we may assume that there is a subgroup $B_0 \geq A_0$ such that $A \cap B_0 = A_0$ and $|G : AB_0| < \infty$. Furthermore, applying the induction hypothesis for B_0 (whose Fitting subgroup

is A_0) we obtain a subgroup $B \leq B_0$ with $A_0 \cap B = 1$ and $|B_0 : A_0B| < \infty$. It now easily follows that B is an almost complement to A in G. □

In order to prove Theorem 1.6, we also need the following.

Proposition 5.2. *Let B be an infinite finitely generated abelian group acting faithfully on an abelian group A of finite rank. Then there is a constant c such that*

$$|\mathrm{Der}(B, A/A_0)| \leq c|A/A_0|^{r_0(B)},$$

for all B-invariant finite index subgroups $A_0 \leq A$. Moreover, c depends only on $\mathrm{rk}(A)$ *and* $|\mathrm{Tor}(B)|$.

Proof. Set $T = \mathrm{Tor}(B)$ and let $d = r_0(B) = d(B/T)$. It suffices to show that for any finite abelian group M acted on by B we have $|\mathrm{Der}(B, M)| \leq c|M|^d$, where c depends on $|T|, d(M)$. Note that

$$|\mathrm{Der}(B, M)| \leq |\mathrm{Der}(T, M)||\mathrm{Der}(B/T, M^T)|.$$

By Lemma 2.6 we have $|\mathrm{Der}(T, M)| \leq c|M/M^T|$ where c depends on $|T|, d(M)$. We also have $|\mathrm{Der}(B/T, M^T)| \leq |M^T|^{d(B/T)} = |M^T|^d$. Altogether we see that

$$|\mathrm{Der}(B, M)| \leq c|M/M^T||M^T|^d \leq c|M|^d.$$

(Recall that $d \geq 1$). □

Proof of Theorem 1.6. Let G, A be as in the theorem, and set $r = r_0(A)$, $d = r_0(G/A)$. We have to show that $\deg(G) = d + r - 1$. We start with the more elementary inequality $\deg(G) \leq d + r - 1$. Write

$$a_n(G) \leq \sum_{m|n} a_{n/m}(G/A)a_m(A)D_{n,m}$$

as in Lemma 2.1 (so $D_{n,m} = \max|\mathrm{Der}(G_0/A, A/A_0)|$, the maximum being taken over all subgroups $G_0 \geq A \geq A_0$ with $|G : G_0| = n/m$, $|A : A_0| = m$ and $A_0 \lhd G_0$). By the preceding result we have

$$D_{n,m} \leq c \cdot m^d,$$

where c is some fixed constant. Note that, in the special case $d = r = 1$ we obtain

$$a_n(G) \leq c \cdot \sigma(n), \tag{2}$$

an inequality which will be useful later on.

By Lemma 2.2 we have $a_{n/m}(G/A) \leq (n/m)^{d-1+o(1)}$ and $a_m(A) \leq m^{r-1+o(1)}$. Therefore

$$a_n(G) \leq c\sum_{m|n}(n/m)^{d-1+o(1)}m^{r-1+o(1)}m^d = \sum_{m|n} n^{d-1+o(1)}m^{r+o(1)} \leq n^{d+r-1+o(1)}.$$

(We have used the fact that $d(n) = n^{o(1)}$.) The upper bound on $\deg(G)$ follows.

To establish the lower bound, we may replace G by any quotient or finite index subgroup of G. Let us first reduce to the case where A is torsion-free. If A is not torsion-free, let T be the torsion subgroup of A. Then $T \lhd G$ is finite and $r_0(A) = r_0(A/T)$. Restricting to the finite index subgroup $C_G(T)$ of G we may assume that $T \leq Z(G)$. This implies that $F(G/T) = A/T$ is torsion-free, and so we may assume $T = 1$.

Now, assuming A is torsion-free of rank r, we obtain $A \leq \mathbb{Q}^r$. Since G/A acts faithfully on A, we may write $G/A \leq \mathrm{Aut}A \leq \mathrm{GL}_r(\mathbb{Q})$. Moreover, in this embedding G/A corresponds to a semisimple subgroup of $\mathrm{GL}_r(\mathbb{Q})$.

By Lemma 5.1 there is a subgroup $B \leq G$ such that $A \cap B = 1$, and $|G : AB| \leq \infty$. Clearly B is a finitely generated abelian group. Replacing B by a torsion-free finite index subgroup, we may assume that B is free abelian of rank d. Replacing G by AB we see that it suffices to prove the lower bound on $\deg(G)$ under the assumption that $G = AB = A \rtimes B$, where B can be identified with a semisimple subgroup of $\mathrm{GL}_r(\mathbb{Q})$ acting on A.

Claim. For almost all primes p, A/pA is a semisimple $\mathbb{F}_pB$-module.

Since B is abelian and finitely generated, it suffices to prove that for each element $b \in B$ there exists a number c depending on b such that, for all primes $p \geq c$, b acts on A/pA in a semisimple manner.

So fix an element $b \in B$ and consider the matrix $M \in GL_r(\mathbb{Q})$ representing its action on $A \otimes \mathbb{Q}$. We can assume that M is written in a rational canonical form. Choose a constant c_1 such that for all primes $p \geq c_1$ the reduction M_p of M mod p is well defined. Let $f_1, \dots, f_k \in \mathbb{Q}[x]$ denote the characteristic polynomials of the blocks of M. Then for $p \geq c_1$ the reductions $(f_i)_p$ of f_i mod p $(i = 1, \dots, k)$ are well defined. Since M is semisimple, the polynomials $f_1, \dots, f_k$ are irreducible over $\mathbb{Q}$. Thus $\gcd(f_i, f_i') = 1$, so we have $h_i f_i + g_i f_i' = 1$ for some polynomials $h_i, g_i \in \mathbb{Q}[x]$. Choose $c \geq c_1$ such that, for all primes $p \geq c$, the reductions of $h_1, \dots, h_k, g_1, \dots, g_k$ mod p are all well defined. It follows that for $p \geq c$, $\gcd((f_i)_p, (f_i)_p') = 1$ in $\mathbb{F}_p[x]$ for $i = 1, \dots k$, which means that $(f_1)_p, \dots, (f_k)_p$ are separable. It follows that, for $p \geq c$, the rational canonical form of $M_p \in GL_r(\mathbb{F}_p)$ consists of blocks with separable characteristic polynomials. This implies that M_p is semisimple for all primes $p \geq c$. The claim follows.

Let $b_1, \dots, b_d$ be generators for B, and let $f(x) \in \mathbb{Q}[x]$ be the product of their characteristic polynomials (as matrices in $\mathrm{GL}_r(\mathbb{Q})$). Let c be as in the claim above and let S be the set of rational primes $p \geq c$ such that the reduction of $f(x)$ mod p is well defined and splits (in $\mathbb{F}_p[x]$) into a product of linear factors. By the Chebotarev density theorem, the set S has positive density. By taking out finitely many primes of S if necessary we can also assume that $A/pA \cong C_p^r$ for all $p \in S$. Since for $p \in S$ the module A/pA is semisimple, we see that the action of B on A/pA can be represented by a diagonal subgroup of $\mathrm{GL}_r(\mathbb{F}_p)$. It follows that, for $p \in S$, if $p - 1 | l$, then b^l acts trivially on A/pA for all $b \in B$.

We now enumerate the primes in S and construct series $\{l_k\}$, $\{m_k\}$ exactly as in Proposition 3.6. Then $l_k \leq m_k^{o(1)}$ and the elements b^{l_k} $(b \in B)$ act trivially on A/m_kA. Fix a large integer $k > 0$ and let $l = l_k$, $m = m_k$. Let $B_0 = \langle b^l : b \in B \rangle$. Then $|B : B_0| = l^d$ and B_0 acts trivially on A/mA. Since G splits over A we have (by 2.1)

$$a_{l^d m}(G) \geq \sum_{A_0 \leq A, |A:A_0| = m} |\mathrm{Hom}(B_0, A/A_0)|.$$

Recall that A has at least m^{r-1} subgroups A_0 of index m. Since B_0 is a free abelian group of rank d we have $|\mathrm{Hom}(B_0, A/A_0)| = |A/A_0|^d = m^d$ for all A_0 as above. This yields

$$a_{l^d m}(G) \geq m^{r-1} m^d = m^{d+r-1}.$$

Since $l = m^{o(1)}$, it now follows (as in the proof of 3.8) that $\deg(G) \geq d + r - 1$.

The theorem is proved. □

Remarks. 1. The first part of the proof shows that, if $A \lhd G$ and $A, G/A$ are infinite abelian, then $\deg(G) \leq r_0(A) + r_0(G/A) - 1$. The assumption that $A = F(G)$ and that G is of semisimple type is only used in proving the lower bound on $\deg(G)$.

2. Our proof shows that the conclusion of 1.6 also holds if the semisimple module $A \otimes \mathbb{Q}$ has trivial components, provided G almost splits over A. For example, this is the case if G/A is infinite cyclic.

We close this section with a lower bound on $\deg(G)$ which is valid for a wider class of all metabelian groups.

Theorem 5.3. *Let G be a finitely generated metabelian group, and let $A \lhd G$ be a normal subgroup such that A and G/A are infinite abelian groups. Suppose G almost splits over A. Let $d = r_0(G/A)$, $r = r_0(A)$. Then*

$$\deg(G) \geq \max\{\frac{s(r-s+d)}{s+d} : 0 < s < r\}.$$

Proof. We may assume that $G = A \rtimes B$ where A, B are abelian. As in the proof of 1.6 we can choose a set S of primes which has positive density, such that for each $p \in S$ and $b \in B$, the eigenvalues of b acting of A/pA all lie in $\mathbb{F}_p$. However, the action of b on A/pA need not be semisimple. We can also assume that $A/pA \cong C_p^r$ for all $p \in S$. Let x be a large number, and set $m = \prod_{p \in S, p \leq x} p$, $l = \mathrm{lcm}\{p-1 : p \in S, p \leq x\}$. Fix $b \in B$. Then b^l acts unipotently on A/pA for each $p \in S, p \leq x$. Without loss of generality we can assume that $p \geq r$ for all $p \in S$. Then for $p \in S$ the Sylow p-subgroup of $\mathrm{GL}_r(\mathbb{F}_p)$ has exponent p. It follows that b^{lm} acts trivially on A/pA for all $p \in S, p \leq x$. Let $0 < s < r$. Then $A/pA \cong C_p^r$ has $\geq p^{s(r-s)}$ subgroups of index p^s, and so A/mA has $\geq m^{s(r-s)}$ subgroups A_0/mA of index m^s. Setting $n = (lm)^d m^s$ and summing over the subgroups A_0 we obtain

$$a_n(G) \geq \sum_{A_0} |\mathrm{Hom}(B^{lm}, A/A_0)| \geq m^{s(r-s)}(m^s)^d = m^{s(r-s+d)}.$$

The result follows using the inequality $l \leq m^{o(1)}$. □

Corollary 5.4. *Let G be a finitely generated metabelian group, and let $A \lhd G$ be a normal subgroup such that A and G/A are infinite abelian groups. Suppose G/A is cyclic. Then*

$$\deg(G) \geq r_0(A)/2.$$

Proof. Since G/A is infinite cyclic, G splits over A. The result now follows from Theorem 5.3 on taking $s = 1$. □

6. Groups of degree $< 3/2$ up to finite extensions

We start by computing the degree of certain metabelian groups which are not of semisimple type.

Lemma 6.1. *Let G be a finitely generated group and suppose $G = \langle A, x \rangle$ where A is an abelian group satisfying $r_0(A) = 2$, and x is an element whose action on $A \otimes \mathbb{Q}$ is given by the matrix $\begin{pmatrix} t & 1 \\ 0 & t \end{pmatrix}$, where $t \in \mathbb{Q}$. Then $\deg(G) = 3/2$.*

Proof. Let T be the torsion subgroup of A. Then $T \lhd G$ is finite and so $\deg(G) = \deg(G/T)$. We can therefore factor our T and assume that A is torsion-free. Therefore $A \leq \mathbb{Q} \oplus \mathbb{Q}$.

For natural numbers m, k, let $a_{m,x^k}(A)$ denote the number of $\langle x^k \rangle$-invariant subgroups A_0 of A of index m. Then, by 2.1(iii) and 2.5 we have

$$a_n(G) = \sum_{mk=n} m a_{m,x^k}(A).$$

Write $t = r/s$ where $r, s \in \mathbb{Z}$ are coprime and $s > 0$. Note that the subring $\mathbb{Z}[t]$ of $\mathbb{Q}$ coincides with the subring $\mathbb{Z}[s^{-1}]$. Define a subring R of $\mathbb{Q}$ by

$$R = \mathbb{Z}[t, 1/t] = \mathbb{Z}[s^{-1}, r^{-1}].$$

We claim $A \leq \mathbb{Q} \oplus \mathbb{Q}$ is an R-module. Indeed, identifying x with its image in $End(A)$, we have $(x-t)^2 = 0$ so that $s^2x^2 - 2rsx + r^2 = 0$. This shows that $r^2 A \leq sA$, and since r, s are coprime it follows that $sA = A$. Therefore A is closed under multiplication by s^{-1}. In a similar manner (considering x^{-1} instead of x) we see that A is closed under multiplication by r^{-1}, and so A is an R-module. It is also easy to see that A is a finitely generated R-module, so $A \cong R \oplus R$.

The same argument shows that, if A_0 is a finite index subgroup of A which is $\langle x^k \rangle$-invariant for some $k > 0$, then A_0 is a (finitely generated) R-module. Note that R is a PID, and so we can use freely basic facts on finitely generated modules over a PID. We can write $A_0 = R(d_1, b) \oplus R(0, d_2)$ where d_1, d_2 are positive integers which are prime to rs. Such a subgroup A_0 will be denoted by $A(d_1, d_2, b)$ and will be represented (as in [GSS]) by a matrix of the form

$$B = \begin{pmatrix} d_1 & b \\ 0 & d_2 \end{pmatrix}.$$

Note that $|A : A(d_1, d_2, b)| = d_1 d_2$, and that $A(d_1, d_2, b) = A(d_1', d_2', b')$ if and only if $d_1 = d_1', d_2 = d_2'$ and $b \equiv b' \bmod d_2$. It follows that the number of distinct subgroups $A(d_1, d_2, b)$ where d_1, d_2 are fixed and b varies is precisely d_2.

Now, the subgroup $A(d_1, d_2, b)$ is $\langle x^k \rangle$-invariant if and only if it is invariant under multiplication by $\begin{pmatrix} 0 & k \\ 0 & 0 \end{pmatrix}$ (which corresponds to the element $t^{1-k}x^k - t$). This in turn is equivalent to the divisibility condition $d_2 | k d_1$. We see that, for m prime to rs we have

$$a_{m,x^k}(A) = \sum_{d_1 d_2 = m, d_2 | k d_1} d_2,$$

while $a_{m,x^k}(A) = 0$ if m is not prime to rs. It now follows at once that $\deg(G) \geq 3/2$. Indeed, let n be a perfect square which is prime to rs. Then, choosing $d_1 = d_2 = n^{1/2}$ in the formula above we obtain $a_{n,x}(A) \geq n^{1/2}$, and so

$$a_n(G) \geq n a_{n,x} \geq n^{3/2}.$$

To bound $\deg(G)$ from above, note that if $m = d_1 d_2$ and d_2 divides $k d_1$, then $d_1 \geq d_2/k$ and so $m \geq d_2^2/k$. This yields $d_2 \leq (km)^{1/2}$, so

$$a_{m,x^k}(A) \leq \sum_{d_1 d_2 = m} (km)^{1/2} = d(m)(km)^{1/2} \leq (km)^{1/2 + o(1)}.$$

It follows that

$$a_n(G) = \sum_{km=n} m a_{m,x^k}(A) \leq n \sum_{km=n} n^{1/2+o(1)} = n^{3/2+o(1)}.$$

The result follows. □

Note that the case $t = 1$ of the lemma shows that the Heisenberg group has degree $3/2$.

Lemma 6.2. *Let G be a finitely generated group, $A \lhd G$ an abelian normal subgroup, and suppose G/A is infinite cyclic. Suppose* $\deg(G) < 3/2$. *Then $r_0(A) \leq 1$. Consequently, either G is virtually abelian (of rank at most 2), or G is virtually (locally cyclic)-by-cyclic.*

Proof. Let $r = r_0(A)$. Applying Corollary 5.4 we obtain $3/2 > \deg(G) \geq r/2$, so $r \leq 2$. Suppose, by contradiction, that $r = 2$, and write $G = A \rtimes \langle x \rangle$. If the action of x on $A \otimes \mathbb{Q}$ is semisimple, then Theorem 1.6 and the second remark preceding Theorem 5.3 show that $\deg(G) = r_0(A) + r_0(G/A) - 1 = 2$, a contradiction. Therefore the action of x is not semisimple, in particular $A \otimes \mathbb{Q}$ is reducible as an $\langle x \rangle$-module. Let $B \in GL_2(\mathbb{Q})$ be a matrix corresponding to the action of x on $A \otimes \mathbb{Q}$. Then it follows that B has a rational eigenvalue, say t, which occurs with multiplicity 2. Without loss of generality we may assume that B is written in a Jordan form. Thus $B = \begin{pmatrix} t & 1 \\ 0 & t \end{pmatrix}$. It follows from the previous lemma that $\deg(G) = 3/2$, a contradiction. This completes the proof. □

Next, we need the following result of Mal′cev (see [R1, Theorem 3.25]).

Lemma 6.3. *Let G be a soluble minimax group, and let $N = F(G)$. Then G/N is virtually abelian.*

We can now obtain the main result of this section.

Proposition 6.4. *Let G be a finitely generated residually finite group satisfying* $\deg(G) < 3/2$. *Then one of the following holds:*

(i) G has a finite index free abelian subgroup on $d \leq 2$ generators.

(ii) G has a finite index subgroup which is (locally cyclic)-by-cyclic.

Proof. In proving the result we may replace G with any finite index subgroup of G (which is also of degree less than $3/2$). By [LMS], G has a finite index subgroup G_0 which is soluble minimax. Therefore it suffices to prove that finitely generated soluble minimax groups of degree $< 3/2$ satisfy the conclusion of the proposition. We shall prove this without assuming that our given group is residually finite (a property which, unlike the property of being soluble minimax, is not inherited by quotients).

So let G be a finitely generated soluble minimax group of degree $< 3/2$. Define the length $l(G)$ of G to be the minimal length of a series $1 = G_n \lhd G_{n-1} \lhd \ldots \lhd G_0$ such that $|G : G_0| < \infty$ and each factor G_i/G_{i+1} is isomorphic to $\mathbb{Z}$ or to C_{p^∞} for some prime p. Arguing by induction on $l(G)$, we can assume that any proper quotient of G by an infinite normal subgroup satisfies the conclusion of the proposition, while G itself does not satisfy the conclusion. Let $N = F(G)$ be the Fitting subgroup of G.

Case 1. $|G : N| < \infty$.

Then we may replace G by N and assume G is nilpotent. By restricting to a suitable finite index subgroup we may assume further that G and G/G' are torsion-free. We claim that $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z} \times \mathbb{Z}$. Suppose otherwise and let $d = d(G) \geq 2$. Then $G/G' \cong \mathbb{Z}^d$ and since $\deg(\mathbb{Z}^d) = d - 1$ (by 2.2) we have $d = 2$. However, $G' \neq 1$, and it follows that $G'/\gamma_3(G)$ is infinite cyclic. Therefore

$G/\gamma_3(G)$ is isomorphic to the Heisenberg group. It follows that $\deg(G) \geq 3/2$, a contradiction.

In all the remaining cases, G/N is infinite. By Lemma 6.3, G/N is virtually abelian. Without loss of generality we can assume that G/N is abelian.

Case 2. N' is infinite.

Then G/N' is as in (i) or (ii) above. This implies $r_0(N/N') = 1$ and since N is nilpotent it follows that N is virtually locally cyclic. It now easily follows that G itself satisfies conditions (i) or (ii) above, a contradiction.

Case 3. N' is finite.

It is easy to see, using Hall's theorem that finitely generated metabelian groups are residually finite (see for instance [R1, Chapter 9]), that if G/F is as in (i) or (ii), where F is a finite normal subgroup of G, then G is of the same type. We can therefore factor out N' and assume that N is abelian.

If $N \otimes \mathbb{Q}$ is an irreducible G/N-module, then G is a metabelian group of semisimple type. Therefore by 1.6

$$\deg(G) = r_0(N) + r_0(G/N) - 1.$$

We conclude that $r_0(N) = r_0(G/N) = 1$. Therefore G/N is virtually cyclic, and N is virtually locally cyclic. It follows that G has a finite index subgroup which is (locally cyclic)-by-cyclic. Thus condition (ii) holds.

Now suppose $N \otimes \mathbb{Q}$ is reducible. Then there is an infinite G-invariant subgroup $N_0 < N$ such that $|N : N_0| = \infty$. Since G/N_0 is as in (i) or (ii), it follows that G/N is virtually cyclic. Without loss of generality we can assume that G/N is cyclic. Applying Lemma 6.2 it follows that $r_0(N) \leq 1$ and G is as in (i) or (ii). This contradiction completes the proof. □

7. (Locally cyclic)-by-cyclic groups

When we say that a group G is (locally cyclic)-by-cyclic, we mean that G has an *infinite* normal subgroup A which is locally cyclic, such that G/A is *infinite* cyclic. We shall also assume that G is not virtually abelian (thus avoiding finite extensions of $\mathbb{Z} \times \mathbb{Z}$, which are treated in the next section).

Recall that a group A is locally cyclic if and only if A is isomorphic to a subgroup of $\mathbb{Q}$ or to a subgroup of $\mathbb{Q}/\mathbb{Z}$. The latter is impossible if A is a subgroup of a finitely generated metabelian group. It is also well known that, if $A \leq \mathbb{Q}$, then $\mathrm{Aut}A \leq \mathbb{Q}^*$; more specifically,

$$\mathrm{Aut}A \cong \{h \in \mathbb{Q}^* : Ah = A\},$$

where elements of the right hand side act by multiplication.

Lemma 7.1. *Let G be a finitely generated (locally cyclic)-by-cyclic group. Then $G \cong \mathbb{Z}[h, 1/h] \rtimes \langle x_h \rangle$ for some $h \in \mathbb{Q} \setminus \{0, 1, -1\}$.*

Proof. Let $A \lhd G$ be a locally cyclic subgroup such that G/A is cyclic. Then $A \leq \mathbb{Q}$, G/A is infinite cyclic, and A is finitely generated as a G/A-module. Write $G = \langle A, x \rangle$ where $x \in G$. By previous remarks there exists $h \in \mathbb{Q}^*$ such that x acts on A as multiplication by h. If $|h| = 1$ then G is virtually abelian. Hence $h \neq 1, -1$.

Let $R = \mathbb{Z}[h, 1/h]$ and consider A as an R-module. Since G is finitely generated, A is finitely generated as an R-module. Since R is a Principal Ideal Domain, A splits into a direct sum of cyclic modules. But A has rank 1, and so A must be cyclic as an R-module. As A is infinite, we conclude that $A \cong R$.

It remains to show that $A \cap \langle x \rangle = 1$. This follows from that fact that the centralizer $C_A(x)$ is trivial. $\square$

Lemma 7.2. *Let $R \subset \mathbb{Q}$ be a subring, and let $h \in U(R)$ be a unit of infinite order. Set $H = R \rtimes \langle x_h \rangle$. Then*

$$\mathrm{Aut}H = R \rtimes U(R),$$

where a pair (a, u) ($a \in R, u \in U(R)$) acts on H by sending $(0, x_h)$ to (a, x_h) and $(b, 1)$ to $(ub, 1)$.

Proof. Let $G = \mathrm{Aut}H$. Then there is a natural homomorphism $\phi : G \to \mathrm{Aut}R$ (where R is considered as an additive group). It follows from a previous remark that $\mathrm{Aut}R \cong U(R)$ (where $u \in U(R)$ acts as multiplication by u). Since there is an automorphism g_u of H sending x_h to x_h and $a \in R$ to $u \cdot a$, it follows that ϕ is surjective.

Let $N = C_G(R)$. Then $G/N \cong \mathrm{Aut}R \cong U(R)$.

Claim. G acts trivially on H/R.

Suppose otherwise. Then some $g \in G$ induces on H/R the inverting automorphism $y \to y^{-1}$. Choose $u \in U(R)$ such that g induces on R multiplication by u. Using additive notation in R we see that, for $a \in R$,

$$g(a^{x_h}) = g(h \cdot a) = u \cdot (h \cdot a) = (uh) \cdot a.$$

On the other hand we have

$$g(a^{x_h}) = g(a)^{g(x_h)} = (u \cdot a)^{{x_h}^{-1}} = h^{-1} \cdot (u \cdot a) = (h^{-1}u) \cdot a.$$

This yields $h^2 = 1$, a contradiction.

Having proved the claim, it follows that N centralizes both R and H/R, and this implies that $N \cong \mathrm{Der}(H/R, R) \cong R$ (more explicitly, each $a \in R$ gives rise to an automorphism $h \mapsto ha$ which acts trivially on R, and N consists of precisely these automorphisms). Since G splits over N (indeed, the set $\{g_u : u \in U(R)\}$ is a complement to N) the result follows. $\square$

Lemma 7.3. *Let G be a finite extension of $H = \mathbb{Z}[h, 1/h] \rtimes \langle x_h \rangle$. Then $C_G(H) \lhd G$ is finite, and $G/C_G(H) \cong \mathbb{Z}[h, 1/h] \rtimes U$, where $U \leq U(R)$ is a finite extension of $\langle h \rangle$. Therefore, either $G/C_G(H)$ is also (locally cyclic)-by-cyclic, or $G/C_G(H) \cong \mathbb{Z}[h, 1/h] \rtimes \langle h, -1 \rangle$.*

Proof. Let $H = \mathbb{Z}[h, 1/h] \rtimes \langle h \rangle \lhd G$ and let $C = C_G(H)$. Clearly $C \lhd G$ and $H \cap C = Z(H) = 1$. Therefore C (being embedded in G/H) is finite (in fact have $HC = H \times C$). Now, G/C can be identified with a subgroup of $\mathrm{Aut}H$, so by the previous lemma $H = R \rtimes \langle h \rangle \leq G/C \leq R \rtimes U$ where $R = \mathbb{Z}[h, 1/h]$ and $U \leq U(R)$. Since G is a finite extension of H it is clear that we may take it that U is a finite extension of $\langle h \rangle$.

If U is cyclic, then G/C is (locally cyclic)-by-cyclic. Otherwise we must have $U = \langle h \rangle \times \langle -1 \rangle$, since -1 is the only non-trivial element of finite order in $\mathbb{Q}^*$. $\square$

Results 7.1 and 7.3 give rise to the following:

Corollary 7.4. *Let G be a finitely generated virtually (locally cyclic)-by-cyclic group, and suppose G is reduced. Then either $G = \mathbb{Z}[h, 1/h] \rtimes \langle h \rangle$ for some $h \in \mathbb{Q} \setminus \{0, 1, -1\}$, or $G = \mathbb{Z}[h, 1/h] \rtimes \langle h, -1 \rangle$ for h as above.*

We can now prove the main result of this section.

Proposition 7.5. *Let G be a finitely generated virtually (locally cyclic)-by-cyclic group. Then* $\deg(G) = 1$. *Furthermore, there are constants $b, c > 0$ such that*

$$bn \log\log n \leq' a_n(G) \leq cn \log\log n \text{ for all } n.$$

Proof. We may assume that G is reduced. By 7.4, G is metabelian of semisimple type, and so it follows using the formula provided in Theorem 1.6 that $\deg(G) = 1$. As for the second assertion, the upper bound on $a_n(G)$ follows from (2) (in the proof of 1.6), while the lower bound follows from 3.4(i). □

8. Crystallographic groups

In this section we prove Theorems 1.3-1.5, as well as Theorem 1.7. Let G be a group of degree $< 3/2$. We can assume that the subgroup growth of G is superlinear, otherwise its structure is determined in Theorem 1.2. If G is virtually (locally cyclic)-by-cyclic, then its structure and growth behaviour are determined in Section 7. In the remaining case, Proposition 6.4 shows that G has a finite index normal subgroup which is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. Hence, to complete the proof of 1.3-1.5, we need to study the finite extensions of $\mathbb{Z} \times \mathbb{Z}$ and analyze their growth behaviour. This will be done using the theory of plane crystallographic groups.

As usual, we may restrict our attention to reduced groups.

Lemma 8.1. *Let G be a finitely generated virtually abelian group, and suppose G is reduced. Then G has a self-centralizing torsion-free abelian normal subgroup A of finite index.*

Proof. Let $A \lhd G$ be a maximal abelian normal subgroup of finite index, and let $C = C_G(A) \lhd G$. Then $A \leq Z(C)$ and so $|C : Z(C)| < \infty$. Therefore $|C'| < \infty$ by a theorem of Schur. Since $C' \lhd G$ and G is reduced it follows that $C' = 1$, so C is abelian. Since $C \geq A$ we have $C = A$ by the maximality of A. If T is the torsion part of A, then $T \lhd G$ is finite, hence trivial. The result follows. □

It now follows that G has the structure of a 2-dimensional crystallographic group, namely, of a plane group. These groups are well known and split into 17 isomorphism classes; see [CM, pp. 40-52]. As the following result shows, not all of these 17 groups have degree 1. Recall that the group p2 is isomorphic to $\mathbb{Z}^2 \rtimes \langle -1 \rangle$ (a split extension of $\mathbb{Z} \times \mathbb{Z}$ by an involution acting as multiplication by -1).

Lemma 8.2. *Let $G = \mathbb{Z}^d \rtimes \langle -1 \rangle$. Then* $\deg(G) = d$. *In particular, the group p2 has degree* 2.

Proof. Let $A = \mathbb{Z}^d$ and let $x \in G$ be the inverting involution. Then any subgroup $A_0 \leq A$ is x-invariant, and Lemma 2.1 shows that

$$a_n(G) = a_{n/2}(A) + \sum_{A_0 \leq A, |A:A_0| = n} |\mathrm{Der}(\langle x \rangle, A/A_0)|.$$

It is clear from the action of x on A that $|\mathrm{Der}(\langle x \rangle, A/A_0)| = n$ for all such subgroups A_0 (see 2.5). It follows that

$$a_n(G) = a_{n/2}(A) + a_n(A) \cdot n.$$

Since $\deg(A) = d - 1$, this implies $\deg(G) = d$. □

Similarly, if the plane group G contains a (necessarily finite index) subgroup of type p2, then $\deg(G) = 2$. The plane groups containing p2 are precisely those containing a 180° rotation, and table 4 on p. 137 of [CM] provides a list of them. By listing the remaining groups we obtain the following.

Corollary 8.3. *Let G be a finite extension of $\mathbb{Z} \times \mathbb{Z}$, and suppose G is reduced and $\deg(G) < 2$. Then G is a plane group which does not contain a 180° rotation. Consequently, G, is isomorphic to p1, pg, pm, cm, p3, p3m1, or p31m.*

Our next goal is to show that the groups listed in 8.3 all have degree 1. We need some information on their structure. Let $i, j, k \in \mathrm{GL}_2(\mathbb{Z})$ denote the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$

respectively. Then $i^2 = j^2 = k^3 = 1$, and the group $\langle j, k\rangle$ is isomorphic to the symmetric group S_3. The groups in 8.3 can now be described as follows: p1 $\cong \mathbb{Z}^2$, pg and pm have the form $\mathbb{Z}^2.\langle i\rangle$, cm $\cong \mathbb{Z}^2 \rtimes \langle j\rangle$, p3 $\cong \mathbb{Z}^2 \rtimes \langle k\rangle \cong \mathbb{Z}[\omega] \rtimes \langle \omega\rangle$ ($\omega = e^{2\pi i/3}$), and p3m1, p31m have the form $\mathbb{Z}^2.S_3$ (and they both contain $\mathbb{Z}^2 \rtimes \langle k\rangle$).

We can now prove

Proposition 8.4. *The groups listed in 8.3 all have degree 1. More specifically, there exist positive constants b, c such that*

(i) $bn \log\log n \leq' a_n(G) \leq cn \log\log n$ if G is p1, pg, pm or cm.

(ii) $n^{1+b/\log\log n} \leq' a_n(G) \leq n^{1+c/\log\log n}$ if G is p3, p3m1 or p31m.

Proof. The lower bound in (i) follows from the obvious inequality

$$a_n(G) \geq a_{n/2}(\mathbb{Z} \times \mathbb{Z}) = \sigma(n/2).$$

To establish the upper bound it suffices to show that $a_n(G) \leq c\sigma(n)$ for some constant c.

The case of p1 is clear, so suppose first that G is an extension of $A = \mathbb{Z} \times \mathbb{Z}$ by the matrix i. By 2.1 we have

$$a_n(G) \leq a_{n/2}(A) + \sum_{A_0} |\mathrm{Der}(\langle i\rangle, A/A_0)|,$$

where A_0 ranges over the i-invariant subgroups of index n in A. If A_0 is such a subgroup, and $(k, l) \in A_0$, then we have $(k, -l) \in A_0$, so $(2k, 0), (0, 2l) \in A_0$. This shows that $2A_0 = k\mathbb{Z} \times l\mathbb{Z}$ for some positive integers k, l. Therefore A/A_0 is isomorphic to a quotient of $C_k \times C_l$ by a subgroup of order dividing 4. An easy computation shows that, in these circumstances we have $|\mathrm{Der}(\langle i\rangle, A/A_0)| \leq 2l$. It follows that

$$a_n(G) \leq \sigma(n/2) + \sum_{A_0} 2l,$$

where now A_0 ranges over all index n subgroups of A such that, for some k, l, $2A_0 \leq k\mathbb{Z} \times l\mathbb{Z} \leq A_0$. Since $kl \in \{n, 2n, 4n\}$, and given k, l there are boundedly many choices for A_0, it easily follows that $a_n(G) \leq c\sigma(n)$, as required. This settles the case of pg and pm. The argument for the group cm (in which case i is replaced by j) is similar and is left to the reader. Part (i) is proved.

Next, let $G =$ p3. Then $G \cong R \rtimes \langle x\rangle$, where $R = \mathbb{Z}[\omega]$ and $x = x_\omega$. Note that, if I is a norm n ideal of R, then $|\mathrm{Der}(\langle x\rangle, R/I) = |R/I| = n$ by 2.5. Lemma 2.1 now shows that

$$a_n(G) = a_{n/3}(\mathbb{Z} \times \mathbb{Z}) + i_n(R)n = \sigma(n/3) + i_n(R)n.$$

The required conclusion now follows from Lemma 3.2.

Finally, suppose G is p3m1 or p31m. Then G contains an index 2 subgroup of type p3, so the lower bound on $a_n(G)$ follows. To prove the upper bound write $G \cong A.S_3$ where $A = \mathbb{Z}^2$, and note that it suffices to count index n subgroups $H \leq G$ satisfying $AH = G$ (otherwise the bound follows from the previous cases). The number of such subgroups H is at most

$$b_n = \sum_{A_0} |\mathrm{Der}(S_3, A/A_0)|,$$

where A_0 ranges over the S_3-invariant subgroups of index n in A. Clearly, if we identify A with the ring $R = \mathbb{Z}[\omega]$, then every such subgroup A_0 is an ideal in R, and so A_0 can be chosen in at most $n^{c/\log\log n}$ ways (by 3.2).

Given A_0, consider A/A_0 as an S_3-module. By 2.6 there is an absolute constant c such that $|\mathrm{Der}(S_3, A/A_0)| \leq c|A/A_0| = cn$ for all A_0. Altogether it follows that

$$a_n(G) = O(n^{1+c/\log\log n}).$$

The result follows. □

The proof of Theorems 1.3-1.5 is now complete.

We now analyze the growth behaviour of virtually abelian groups in general, and prove Theorem 1.7. We need some preparations. Let M be a module over some given ring R. Denote by $a_n(M)$ the number of submodules of index n in M. As in the case of groups, we define the degree of the module M by

$$\deg(M) = \limsup \frac{\log a_n(M)}{\log n}.$$

If $\deg(M)$ is finite we say that M has *polynomial submodule growth*. It is clear that, if F is a finite group, and M is a finitely generated $\mathbb{Z}F$-module, then $\deg(M) < \infty$ (since M is finitely generated as an abelian group).

The following is an easy analogue of 2.1.

Lemma 8.5. *Let $N \leq M$ be R-modules. Then*

$$a_n(M) \leq \sum_{m|n} a_{n/m}(M/N) a_m(N) D_{n,m},$$

where $D_{n,m} = \max|\mathrm{Hom}(M_0/N, N/N_0)|$, the maximum being taken over all submodules M_0, N_0 satisfying $N_0 \leq N \leq M_0 \leq M, |M : M_0| = n/m, |N : N_0| = m$.

The next result shows that the degree of a module often coincides with the degree of its finite index submodules. As in the group case, we set $a'_n(M) = \max\{a_m(M) : m|n\}$.

Corollary 8.6. *Let M, N be modules such that $N \leq M$ and $|M : N| < \infty$. Suppose M has finite rank (as an abelian group). Then there is a constant c such that $a'_n(M) \leq c \cdot a'_n(N)$ for all n. In particular* $\deg(M) = \deg(N)$.

Proof. Set $i = |M : N|$ and $r = \mathrm{rk}(M)$. Then, in the notation of 8.5 we have $D_{n,m} \leq i^{r^2}$ for all n, m. The result follows. □

Similarly, if $\mathrm{rk}(M) < \infty$, and $N \leq M$ is finite, then $\deg(M) = \deg(M/N)$.

Proposition 8.7. *Let F be a finite group, and let M be a finitely generated $\mathbb{Z}F$-module. Set $d = \dim_{\mathbb{Q}}(M \otimes \mathbb{Q})$. Suppose the image of F in $\mathrm{GL}_d(\mathbb{Q}) = End(M \otimes \mathbb{Q})$ is not contained in the subgroup $\langle \pm 1 \rangle$ of scalar matrices. Then*

$$\deg(M) \leq d - 2.$$

Proof. Using 8.6 we can reduce to the case where M is torsion-free as an abelian group, so $M \cong \mathbb{Z}^d$. Let F_0 be a minimal subgroup of F whose image in $\mathrm{GL}_d(\mathbb{Z})$ is non-scalar. Then F_0 is cyclic and $a_n(M)$ is bounded above by the number of index n submodules of M as a $\mathbb{Z}F_0$-module. We can therefore replace F by F_0 and assume F is cyclic, say $F = \langle x \rangle$.

Suppose first that $M \otimes \mathbb{Q}$ is an irreducible $\mathbb{Q}F$-module. In this case $K = M \otimes \mathbb{Q}$ is a field extension of $\mathbb{Q}$ (of degree d), and x acts on K as multiplication by some root of unity $u \in K^*$. Furthermore, we have $K = \mathbb{Q}(u)$ and M can be identified with a fractional ideal of K, with respect to the full subring $R = \mathbb{Z}[u, u^{-1}]$. Thus M is 2-generated as a $\mathbb{Z}F$-module (since fractional ideals are 2-generated), and M has a finite index cyclic submodule M_0 (corresponding to a principal fractional ideal). Now, the submodule M_0 can be identified with R, and its submodules correspond to ideals of R. It follows from 3.2 that $a_n(M_0) \leq n^{o(1)}$. Applying the remark above we conclude that $a_n(M) \leq n^{o(1)}$. Thus $\deg(M) = 0$ if $M \otimes \mathbb{Q}$ is irreducible.

Now, consider the case where $M \otimes \mathbb{Q}$ is reducible. Choose a submodule $N < M$ such that M/N is torsion-free and $(M/N) \otimes \mathbb{Q}$ is a non-trivial irreducible module (this is possible by Maschke's Theorem). In order to apply Lemma 8.5 we need to estimate $D_{n,m}$. By the above discussion, M/N and its submodules are 2-generated (as $\mathbb{Z}F$-modules), and this yields

$$D_{n,m} \leq m^2.$$

Let $s = \dim((M/N) \otimes \mathbb{Q})$ and $t = d - s = \dim(N \otimes \mathbb{Q})$. Then we have by 8.5

$$a_n(M) \leq \sum_{m|n} (n/m)^{o(1)} m^{t-1} m^2 \leq n^{t+1+o(1)}.$$

The required conclusion follows, provided $s \geq 3$.

Suppose $s = 2$. Then x must acts on M/N as multiplication by a root of unity u of order 3 or 6. Since the class number of $\mathbb{Q}(u)$ is 1, it follows that M/N is a cyclic module in this case, and so $D_{n,m} \leq m$. Using this inequality the required conclusion follows.

We are left with the case $s = 1$. Moreover, we can also assume that every irreducible component of $M \otimes \mathbb{Q}$ is 1-dimensional, otherwise we can re-choose N so that $s \geq 2$, and apply the previous cases. This implies (by abuse of notation) that there exists a submodule N of M such that x acts trivially on $N \otimes \mathbb{Q}$ and acts on $(M/N) \otimes \mathbb{Q}$ as multiplication by -1. Then x acts trivially on N (since N is torsion-free) and it is easy to reduce to the case where x acts on M/N as multiplication by -1. Let $s = \dim((M/N) \otimes \mathbb{Q})$ and $t = \dim(N \otimes \mathbb{Q})$. Then $s, t > 0$ since the action of x is non-scalar. Now, a homomorphism ϕ from a submodule of M/N to a quotient of N satisfies $\phi(-a) = \phi(xa) = x\phi(a) = \phi(a)$, and so it follows that the image of ϕ consists of elements b with $2b = 0$. This shows that $D_{n,m} \leq c$ for some constant c not depending on n, m. Using this it now follow from the previous lemma that $a_n(M) \leq n^{d-2+o(1)}$.

The proposition is proved. $\square$

Proof of Theorem 1.7. Set $d = r_0(A)$. It is clear that $\deg(G) \geq \deg(A) = d - 1$. If G contains an inverting involution, then G contains $A \rtimes \langle -1 \rangle$ as a finite index subgroup, so $\deg(G) = d$ by 8.2. So suppose G does not contain such an involution. Let $F = G/A$. Then the image of F in $\mathrm{GL}_d(\mathbb{Z})$ does not contain the scalar matrix -1.

Now, the finite index subgroups H of G split into finitely many classes according to their image $F_0 = HA/A$ in F. So it suffices to show that each class contributes at most $n^{d-1+o(1)}$ to $a_n(G)$. This is clear if F_0 is trivial, and if $F_0 \neq 1$ then it is not contained in $\langle \pm 1 \rangle$. It suffices to deal with the case $F = F_0 \neq 1$. Let $a_{n,F}$ denote the number of index n subgroups H of G satisfying $HA = G$. Consider A as a $\mathbb{Z}F$-module. Then we have

$$a_{n,F}(G) \leq \sum_{A_0} |\mathrm{Der}(F, A/A_0)|,$$

where A_0 ranges over the index n submodules of A. By the preceding result there are at most $n^{d-2+o(1)}$ such submodules, and by 2.6 we have $|\mathrm{Der}(F, A/A_0)| \leq cn$ for all of them.

The result follows. □

9. An example

As noted in the introduction, there is no formula for computing the degree of finitely generated nilpotent groups. In fact, it seems that the explicit computations of zeta functions and degrees of nilpotent groups focused on groups of class two. In this section we compute the degree of a nilpotent group of class three. As a by-product we show that there exists a finitely generated group of degree 5/3.

Theorem 9.1. *Let G be a 2-generated nilpotent group of class 3 and Hirsch rank 4. Then* $\deg(G) = 5/3$.

Proof. We may assume that G is torsion-free. Then $G/G' \cong G' \cong \mathbb{Z}^2$ and G acts unipotently on G'. Let A denote the kernel of this action. Since the group of unipotent upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z})$ is isomorphic to $\mathbb{Z}$, we have $G/A \cong \mathbb{Z}$. Obviously $A \supseteq G'$ and $A/G' \cong \mathbb{Z}$. It follows that A, being cyclic modulo its center, is abelian. Now choose generators x, y for G such that x generates G modulo A and $y \in A$. Let $z = [x, y]$, $w = [x, z]$. Then $A = \langle y, z, w \rangle \cong \mathbb{Z}^3$, and we have $G = A \rtimes \langle x \rangle$ where the action of x on A is represented by the unipotent matrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

As usual we have

$$a_n(G) = \sum_{A_0, k} |\mathrm{Der}(\langle x^k \rangle, A/A_0)| = \sum_{A_0, k} |A : A_0|,$$

where $k|n$ and A_0 ranges over the $\langle x^k \rangle$-invariant subgroups of index n/k in A.

We now record some known and useful facts on finite index subgroups of abelian and nilpotent groups (see [GSS]).

Every finite index subgroup $A_0 \leq A$ has a triangular basis represented (with respect to the basis y, z, w of A) by the integer matrix

$$M = \begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix}$$

where $d_1, d_2, d_3 > 0$. We then have $|A : A_0| = d_1 d_2 d_3$. The integers d_1, d_2, d_3 are invariants of the subgroup A_0, but the integers a, b, c are not uniquely determined by A_0. However, the values of b, c modulo d_3 and the value of a modulo d_2 are invariants of A_0. Therefore, if we require $0 \leq a < d_2$, and $0 \leq b, c < d_3$, then different values of a, b, c will determine different subgroups A_0, and all subgroups with invariants d_1, d_2, d_3 will be obtained in this manner. In particular this shows that there are $d_2 d_3^2$ subgroups A_0 with invariants d_1, d_2, d_3.

What are the conditions on the matrix M which amount to requiring A_0 to be $\langle x^k \rangle$-invariant?

Claim 1. Let $A_0 \leq A$ be a finite index subgroup corresponding to a matrix M as above. Then A_0 is $\langle x^k \rangle$-invariant if and only if the following conditions hold:

1. $d_2 | k d_1$,
2. $d_3 | k d_2$,
3. $d_3 | \binom{k}{2} d_1 + ka - k d_1 d_2^{-1} c$.

The proof of this claim is based on the fact that x^k is represented by the matrix

$$\begin{pmatrix} 1 & k & \binom{k}{2} \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix}.$$

The details are left to the reader.

As in the proof of Lemma 6.1, we let $a_{m,x^k}(A)$ denote the number of index m $\langle x^k \rangle$-invariant subgroups of A.

Claim 2. $a_{n,x}(A) \geq n^{2/3}$ for infinitely many n.

Indeed, fix $m > 0$ and for each $0 \leq a, b < m$ consider subgroup $A(a, b)$ of A corresponding to the matrix

$$M(a, b) = \begin{pmatrix} m & a & b \\ 0 & m & a \\ 0 & 0 & m \end{pmatrix}.$$

It is clear from Claim 1 that the subgroups $A(a, b)$ are $\langle x \rangle$-invariant. By previous remarks we have $|A : A(a, b)| = m^3$ and $A(a, b) \neq A(a', b')$ if $(a, b) \neq (a', b')$. We thus obtain m^2 distinct $\langle x \rangle$-invariant subgroups of index m^3 in A. This proves the claim.

Claim 3. $a_{m,x^k}(A) \leq m^{2/3+o(1)} k^{3/2}$.

By Claim 1, the number of $\langle x^k \rangle$-invariant subgroups of index m in A_0 equals the number of integral solutions to the following system of congruences and inequalities in the 6 variables d_1, d_2, d_3, a, b, c:

$$d_1 d_2 d_3 = m,\ d_2 | k d_1,\ d_3 | k d_2,$$

and

$$0 \leq a < d_2,\ 0 \leq b, c < d_3,\ d_3 | \binom{k}{2} d_1 + ka - k d_1 d_2^{-1} c.$$

Trivially, there are at most $d(m)^3 = m^{o(1)}$ choices for d_1, d_2, d_3, so we may assume that these parameters are fixed. Now, a and b can be chosen in at most $d_2 d_3$ ways. So suppose that they are given, and note that c can then be chosen in at most $kd_1 d_2^{-1}$ ways, so that the last congruence is satisfied. Therefore, given d_1, d_2, d_3, there are at most $kd_1 d_3$ choices for a, b, c. On the other hand, if we first choose b and c (d_3^2 possibilities) then a can be chosen in at most $kd_2 d_3^{-1}$ ways. This shows that $kd_2 d_3$ also bounds the number of choices for a, b, c given d_1, d_2, d_3.

It therefore suffices to show that, for some $i \in \{1, 2\}$ we have $kd_i d_3 \leq m^{2/3} k^{3/2}$. Suppose otherwise. Then we have

$$d_i d_3 > m^{2/3} k^{1/2} \quad \text{for } i = 1, 2.$$

Recall that $m = d_1 d_2 d_3$. We therefore obtain $(d_i d_3)^3 > (d_1 d_2 d_3)^2 k^{3/2}$, namely, $d_i d_3 > d_j^2 k^{3/2}$ where $j = 3 - i$. Multiplying the last inequalities (for $i = 1, 2$) we obtain $d_1 d_2 d_3^2 > (d_1 d_2)^2 k^3$, namely, $d_3^2 > d_1 d_2 k^3$. However, it is clear from the above congruences that $d_3 \leq d_2 k \leq d_1 k^2$, so $d_3^2 \leq d_1 d_2 k^3$. This contradiction completes the proof of Claim 3.

We can now complete the proof of Theorem 9.1.

First note that, by 2.1 and 2.5, we have $a_n(G) \geq n \cdot a_{n,x}(A)$. So using Claim 2 we see that the inequality $a_n(G) \geq n^{5/3}$ holds for infinitely many n. On the other hand, using Claim 3 we obtain

$$\begin{aligned} a_n(G) &= \sum_{km=n} a_{m,x^k}(A) m \leq \sum_{km=n} m^{2/3+o(1)} k^{3/2} m \\ &\leq \sum_{km=n} (km)^{5/3+o(1)} = d(n) n^{5/3+o(1)} = n^{5/3+o(1)}. \end{aligned}$$

This concludes the proof. □

References

[B] A. Babakhanian, *Cohomological Methods in Group Theory*, Dekker, New York, 1972. MR **41:**6977

[Ba] H. Bass, The degree of polynomial growth of finitely generated nilpotent groups, *Proc. London Math. Soc.* **25** (1972), 603–614. MR **52:**577

[CM] H.S.M. Coxeter and W.O.J. Moser, *Generators and Relators for Discrete Groups*, Springer, Berlin, 1957. MR **19:**527d

[dS] M.P.F. du Sautoy, Finitely generated groups, p-adic analytic groups and Poincaré series, *Ann. of Math.* **137** (1993), 639–670. MR **94j:**20029

[E] W. Ellison and F. Ellison, *Prime Numbers*, Wiley, New York, 1985. MR **87a:**11082

[Gr] M. Gromov, Groups of polynomial growth and expanding maps, *Publ. Math. I.H.E.S.* **53** (1981), 53–78. MR **83b:**53041

[GSS] F.J. Grunewald, D. Segal and G.C. Smith, Subgroups of finite index in nilpotent groups, *Invent. Math.* **93** (1988), 185–223. MR **89m:**11084

[HKLSh] E. Hrushovski, P.H. Kropholler, A. Lubotzky and A. Shalev, Powers in finitely generated groups, *Trans. Amer. Math. Soc.* **348** (1996), 291–304. MR **96f:**20061

[HW] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers* (3rd edition), Clarendon, Oxford, 1954. MR **16:**673c

[L1] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995), 267–295. MR **95m:**20054

[L2] A. Lubotzky, Counting finite index subgroups, *Groups '93 – Galway / St Andrews*, London Math. Soc. Lecture Note Series **212**, Cambridge University Press, Cambridge, 1995, pp. 368–404. MR **96h:**20080

[L3] A. Lubotzky, Subgroup growth, *Proc. ICM Zürich '94,* vol. 1, Birkhäuser, Basel, 1995, 309–317. MR **97k:**20048

[LM] A. Lubotzky and A. Mann, On groups of polynomial subgroup growth, *Invent. Math.* **104** (1991), 521–533. MR **92a:**20038

[LMS] A. Lubotzky, A. Mann and D. Segal, Finitely generated groups of polynomial subgroup growth, *Israel. J. Math.* **82** (1993), 363–371. MR **95b:**20051

[M] A. Mann, Some properties of polynomial subgroup growth groups, *Israel J. Math.* **82** (1993), 373–380. MR **94m:**20088

[MS1] A. Mann and D. Segal, Uniform finiteness conditions in residually finite groups, *Proc. London Math. Soc.* (3) **61** (1990), 529–545. MR **91j:**20093

[MS2] A. Mann and D. Segal, Subgroup growth: survey of current results, *Infinite Groups 94*, ed. de Giovanni and Newell, Walter de Gruyter, Berlin-New York, 1995, pp. 179–197. CMP 98:03

[Me] A.D. Mednykh, On the number of subgroups in the fundamental group of a closed surface, *Comm. Alg.* **16**(10) (1988), 2137–2148. MR **90a:**20076

[N] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN, Warsaw, 1974. MR **50:**268

[R1] D.J.S. Robinson, *Finiteness Conditions and Generalized Soluble Groups, I-II*, Springer, New York, 1972. MR **48:**11314; MR **48:**11315

[R2] D.J.S. Robinson, Splitting theorems for infinite groups, *Symp. Math.* XVII (1976), 441–470. MR **53:**10936

[R3] D.J.S. Robinson, *A Course in the Theory of Groups*, Springer, New York, 1982. MR **84k:**20001

[SSh1] D. Segal and A. Shalev, Groups of fractionally exponential subgroup growth, *J. Pure and Appl. Alg.* **88** (1993), 205–223. MR **94e:**20047

[SSh2] D. Segal and A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math. Soc.* **55** (1997), 320-334 (Hartley memorial issue). MR **98c:**20053

[Sh1] A. Shalev, Growth functions, p-adic analytic groups, and groups of finite coclass, *J. London Math. Soc.* (2) **46** (1992), 111–122. MR **94a:**20047

[Sh2] A. Shalev, Subgroup growth and sieve methods, *Proc. London Math. Soc.* **74** (1997), 335–359. MR **98c:**20054

[Sh3] A. Shalev, Groups whose subgroup growth is less than linear, *Int. J. Alg. and Comp.* **7** (1997), 77–91. MR **98g:**20046

[S] G.C. Smith, *Zeta-Functions of Torsion-Free Finitely Generated Nilpotent Groups*, Ph.D. Thesis, UMIST, Manchester, 1983.

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