COUNTING FINITE INDEX SUBGROUPS

ALEXANDER LUBOTZKY

Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel

For Karl Gruenberg on his 65th birthday.

Introduction

Let Γ be a finitely generated group. Denote by $a_n(\Gamma)$ (resp.$\sigma_n(\Gamma)$) the number of subgroups of Γ of index n (resp. of index at most n). This paper deals with the connection between the algebraic structure of the group Γ and the arithmetic properties of the sequence $a_n(\Gamma)$, $n = 1, 2, 3, \ldots$, e.g., the growth of the sequence $a_n(\Gamma)$ ("the subgroup growth") or the properties of the function $\zeta_\Gamma(s) = \sum_{n=1}^{\infty} a_n(\Gamma) n^{-s}$ which encodes the sequence $a_n(\Gamma)$.

These studies have two sources of inspiration. The first is the notion of word growth of groups; namely, denote by $b_n^\Sigma(\Gamma)$ the number of elements of Γ whose length is n with respect to a fixed finite set Σ of generators of Γ. Much work has been done on $b_n^\Sigma(\Gamma)$ and its connection with Γ– see [Ba], [Mi], [Wol], [Gro], [Gri] and the references therein. To some extent $b_n^\Sigma(\Gamma)$ measure the growth of Γ from below, while $a_n(\Gamma)$ express its growth from the top. The two types of growth have some vague connection (cf. [LM3]), but the word growth is used here only as a model for the kind of problems we want to face: groups of (subgroup) polynomial growth, intermediate growth etc. It should be noticed however that while the numbers $b_n^\Sigma(\Gamma)$ (but not their growth) depend on a choice of generators, $a_n(\Gamma)$ depend only on Γ. Thus the numbers $a_n(\Gamma)$ are of inherent interest and not merely their growth. This brings us to the second source of inspiration: the theory of rings of algebraic integers and their zeta functions. Here if O is the ring of algebraic integers in a number field k, one writes $\zeta_k(s) = \Sigma r_n n^{-s}$ where r_n is the number of ideals of O of index n. The function $\zeta_k(s)$ is called the Dedekind ζ-function of k and expresses much of the arithmetic of k. Similarly, we will study $\zeta_\Gamma(s) = \Sigma a_n(\Gamma) n^{-s}$ and describe the first steps of an analogous theory for non-commutative groups.

The reader might wonder whether $a_n(\Gamma)$ is the right analogue to r_n. One might suggest other possibilities, for example looking at the number of normal subgroups of index n. At this point it is unclear which definition would lead to a richer theory. We, however, have limited ourselves in this survey to the counting of all finite index subgroups.

Denote by $R(\Gamma)$ the intersection of all finite index subgroups of Γ. Obviously, $a_n(\Gamma/R(\Gamma)) = a_n(\Gamma)$. So, there is no harm in assuming $R(\Gamma) = \{1\}$, i.e., Γ is a residually finite group. In this respect, the subgroup growth is

more restricted than the word growth. Anyway, the class of residually finite groups is rich enough, containing, for example, all the finitely generated linear groups. Closely connected with a residually finite group Γ are its pro-finite completion $\hat{\Gamma}$ and its pro-p completion $\Gamma_{\hat{p}}$, p a prime. So our study will lead to the territory of pro-finite groups.

The earliest paper in the mathematical literature which considered systematically counting finite index subgroups is, as far as we can tell, the paper of Marshal Hall [Ha1] in 1949. (So, subgroup growth is an older subject than word growth! In fact, Hurwitz in 1902 had already studied a question which is essentially counting finite index subgroups of surface groups– see [Me4] and the references therein.) In that paper, Hall gave a recursive formula for the number of subgroups of index n in the free group on r generators. Hall's method is based on associating with every subgroup H the permutational representation of Γ on the coset space Γ/H. His method was considerably simplified by various authors who also extended it to other groups which are somehow close to free groups. Most significantly is the work of T. Müller who developed an elaborate theory for the subgroup growth of virtually free groups. This direction is described in Section 1.

A completely new direction was started approximately ten years ago by D. Segal, G. Smith and F. Grunewald ([Sm1], [Se] and [GSS]). They looked at $a_n(\Gamma)$ for a nilpotent group Γ and in particular defined the zeta function $\zeta_\Gamma(s) = \Sigma a_n(\Gamma)n^{-s}$. It is particularly natural to do so for nilpotent groups since:

(a) for such groups $a_n(\Gamma)$ grows polynomially, thus $\zeta_\Gamma(s)$ has a non-empty domain of congruence.

(b) $\zeta_\Gamma(s)$ has an "Euler factorizaton" $\zeta_\Gamma(s) = \prod_p \zeta_{\Gamma,p}(s)$.

By applying the work of Denef [De1] on the rationality of some p-adic integrals they showed that the local factors $\zeta_{\Gamma,p}(s)$ are rational. Just as important, they computed many examples suggesting some very attractive conjectures. These important developments are described in Section 2. This work accentuated the importance of pro-p groups to the topic of counting subgroups and led M. du Sautoy [dS3] to prove that the zeta function of a compact p-adic analytic group is rational. His work in turn opens up the question of explicitly calculating these functions for semi-simple groups. Very little is known in this direction (with the exception of some examples computed by Ilani [Il3]). Simultaneously, it became evident that the subgroup growth is a very useful invariant for pro-p groups: A. Lubotzky and A. Mann proved that a pro-p group G is p-adic analytic if and only if $a_n(G)$ grows polynomially. A. Shalev [Sh1] showed that for non p-adic analytic groups the growth is at least $n^{C \log n}$. Section 3 describes the current situation in this sub-area.

Section 4 considers the question: For which groups Γ, $a_n(\Gamma)$ grows poly-

nomially? A complete answer was given by A. Lubotzky, A. Mann and D. Segal ([LMS], [MS], [LM3], [Se]): This happens if and only if Γ is virtually solvable of finite rank. The proof of this theorem required an ensemble of tools such as the classification of finite simple groups, number theory and the theories of p-adic Lie groups, algebraic groups and arithmetic groups. In particular, it was shown that the growth of congruence subgroups of arithmetic groups (with non-solvable zariski closures) is not polynomially bounded. A more detailed study was done by A. Lubotzky [Lu4] where it is shown that for arithmetic groups in characteristic zero (e.g., $\Gamma = SL_r(\mathbb{Z})$) the growth of the congruence subgroups is $n^{C \log n / \log \log n}$.

Moreover, this type of growth characterizes the congruence subgroup property (CSP). Namely, if Γ fails to have CSP then the growth of $\sigma_n(\Gamma)$ is strictly larger– which means that Γ has "many more" non-congruence subgroups than congruence ones. On the other hand if Γ has the congruence subgroup property (e.g. $\Gamma = SL_r(\mathbb{Z})$, $r \geq 3$), $\sigma_n(\Gamma)$ grows as $n^{C \log n / \log \log n}$ so it has "intermediate subgroup growth" between polynomial and exponential. It should, however, be mentioned that free groups have super-exponential subgroup growth ($\sim e^{Cn \log n}$) and it is not difficult to give examples of solvable groups of exponential subgroup growth. Recently D. Segal and A. Shalev [SS] gave examples of solvable groups with fractionally exponential subgroup growth– thus adding a completely new source of groups of intermediate subgroup growth. The results on congruence subgroups are described in Section 5. They also highlight the connection between counting finite index subgroups and various counting problems in finite groups. The last mentioned area has been developed dramatically in recent years– e.g., the work of Pyber [Py1]– and it gives fruits to our topic as well.

As the reader may have sensed already from this introduction– the topic of "Subgroup Growth" is still in its infancy level. Extensive progress has been made in recent years and more development is anticipated. This makes it a wonderful topic for a series of talks in a conference– but it is an almost impossible task to accomplish a complete survey. This survey should be considered as a temporary report of the state of the art– calling attention to this beautiful chapter of asymptotic group theory. This paper is a short version of notes [Lu6] titled "Subgroup Growth" distributed at the Galway/St Andrews conference on group theory 1993. It was however updated to cover some work which was done in the last months of 1993.

This paper was written while the author was visiting the University of Chicago whose warm hospitality and support are gratefully acknowledged. We are also grateful to A. Mann for some helpful remarks.

1. Counting subgroups and permutational representations

The first paper in the literature in which the question of counting subgroups of a given index was considered is the 1949 paper of Marshal Hall [Ha1] in which a recursive formula was given for the number of subgroup of index n in the free group on r generators. Hall's method was extended and simplified by Dey [De2] and Wolfhart [Wo] to get the following form: Let Γ be a finitely generated group and H a subgroup of index n. There is an action of Γ on the set Γ/H of left cosets of H, which defines a permutational representation of Γ on a set of n elements. Identify Γ/H with the set $\{1,2,\ldots,n\}$ such that H is corresponding to 1. There are $(n-1)!$ ways to make this identification. Thus H defines $(n-1)!$ homomorphisms from Γ to S_n. Every such homomorphism $\varphi : \Gamma \to S_n$ satisfies (i) $\varphi(\Gamma)$ is transitive on $\{1,2,\ldots,n\}$ and (ii) $\operatorname{Stab}_{\Gamma,\varphi}(1) = \{\gamma \in \Gamma | \varphi(\gamma)(1) = 1\} = H$. Conversely, every transitive permutational representation of degree n (i.e. $\varphi : \Gamma \to S_n$ satisfying (i)) defines an index n subgroup $H = \operatorname{Stab}_{\Gamma,\varphi}(1)$. Hence:

Proposition 1.1. *Let $t_n(\Gamma)$ be the number of transitive permutational representations of Γ on the set $\{1,2,\ldots,n\}$. Then $a_n(\Gamma) = t_n(\Gamma)/(n-1)!$ where $a_n(\Gamma)$ is the number of subgroups of Γ of index n.*

Example 1.2. $\Gamma = \mathbb{Z}$, $a_n(\Gamma) = 1$ for every n, while $t_n(\Gamma)$ is equal to the number of n-cycles in S_n which is $(n-1)!$.

It remains to count the number of transitive actions. Let the number of all homomorphisms from Γ to S_n be $h_n(\Gamma) = |\operatorname{Hom}(\Gamma, S_n)|$. We have:

Lemma 1.3. *Let Γ be a group. Then:*

$$h_n(\Gamma) = \sum_{k=1}^{n} \binom{n-1}{k-1} t_k(\Gamma)\, h_{n-k}(\Gamma)$$

PROOF. Indeed, for every $1 \le k \le n$ there are $\binom{n-1}{k-1}$ ways to choose the orbit of 1, $t_k(\Gamma)$ ways to act on this orbit and $h_{n-k}(\Gamma)$ ways to act on its complement in $\{1,2,\ldots,n\}$. □

(1.1) and (1.3) imply:

Corollary 1.4. *Let Γ be any group. Then:*

$$a_n(\Gamma) = \frac{1}{(n-1)!} h_n(\Gamma) - \sum_{k=1}^{n-1} \frac{1}{(n-k)!} h_{n-k}(\Gamma)\, a_k(\Gamma).$$

For some groups, $h_n(\Gamma)$ are easy to compute, e.g., for the free group on r generators $h_n(F_r) = (n!)^r$. Hence:

Corollary 1.5. (M. Hall [Ha1]) *Let F_r be the free group on r generators. Then:*

$$a_n(F_r) = n(n!)^{r-1} - \sum_{k=1}^{n-1} (n-k)!^{r-1} a_k(F_r).$$

To estimate the growth of $a_n(\Gamma)$ for $\Gamma = F_r (r \geq 2)$ we notice that "most" r-tuples of permutations in S_n acts transitively on $\{1, 2, \ldots, n\}$, i.e., $\frac{t_n(F_r)}{h_n(F_r)} \to 1$ as $n \to \infty$. Indeed $h_n(F_r) = (n!)^r$ while the number of r-tuple which are *not* transitive is bounded by $P = \sum_{k=1}^{n-1} \binom{n-1}{k-1} h_k(F_r) h_{n-k}(F_r) = \sum_{k=1}^{n-1} \binom{n-1}{k-1} (k!)^r ((n-k)!)^r$ as the proof of Lemma 1.3 shows. Now, it is easy to see that $\lim_{n\to\infty} \frac{P}{(n!)^r} = 0$.

We mention in passing the result of Dixon [Di] that most r-tuples ($r \geq 2$) of permutations of S_n not merely act transitively but actually generate either S_n or A_n. But the transitivity suffices to deduce:

Proposition 1.6. (Newman [Ne2])

$$a_n(F_r) \sim n \cdot (n!)^{r-1}.$$

PROOF. By (1.1), $a_n(F_r) = t_n(F_r)/(n-1)! \sim \frac{h_n(F_r)}{(n-1)!} = n(n!)^{r-1}$. □

The next case which was considered in the literature is the case of a free product $\Gamma = *_{i=1}^r A_i$. Clearly $h_n(\Gamma) = \Pi_{i=1}^r h_n(A_i)$ and hence (1.4) implies:

Corollary 1.7. (Dey [De2]) *Let $\Gamma = *_{i=1}^r A_i$ and let $h_n^i = h_n(A_i) = |\, Hom(A_i, S_n)|$. Then*

$$a_n(\Gamma) = \frac{1}{(n-1)!} (\Pi_{i=1}^r h_n^i) - \sum_{k=1}^{n-1} \frac{1}{(n-k)!} a_k(\Gamma)(\Pi_{i=1}^r h_{n-k}^i).$$

Of course (1.5) is a special case of (1.7) when $A_i \simeq \mathbb{Z}$ and $h_n^i = n!$ for every i and n. However, in general it is not an easy task to compute $h_n(A)$ even if A is a finite group. If $A = \mathbb{Z}/d\mathbb{Z}$ then $h_n(\mathbb{Z}/d\mathbb{Z})$ is the number of degree n permutations of order dividing d. This function has received a considerable amount of attention (see [MW], [Wi], and the references therein).

For example Moser and Wyman [MW] proved:

Proposition 1.8. *Let p be a prime. Then*

$$h_n(\mathbb{Z}/p\mathbb{Z}) \sim K_p \; exp\left(\frac{p-1}{p} n \log n - \frac{p-1}{p} n + n^{1/P}\right)$$

where $K_p = p^{-1/2}$ for $p > 2$ and $K_2 = 2^{-1/2} e^{-1/4}$.

Newman [Ne2] showed that also for a free product of finite cyclic groups "most" permutational actions are transitive (provided this is not the infinite dihederal group) and hence $t_n \sim h_n$. A case of particular interest is $\mathrm{PSL}_2(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$. Hence

$$a_n(\mathrm{PSL}_2(\mathbb{Z})) \sim h_n(\mathbb{Z}/2\mathbb{Z})\, h_n(\mathbb{Z}/3\mathbb{Z})/(n-1)!$$

and therefore one can deduce from (1.8) that:

Proposition 1.9. (Newman [Ne2])

$$a_n(PSL_2(\mathbb{Z})) \sim (12\pi e^{1/2})^{-1/2}\ exp\left(\frac{n\log n}{6} - \frac{n}{6} + n^{1/2} + n^{1/3} + \frac{\log n}{2}\right)$$

He also computed $a_n(\mathrm{PSL}_2(\mathbb{Z}))$ for many $n - s$. For example:

$$a_{100}(\mathrm{PSL}_2(\mathbb{Z})) = 159299552010504751878902805384624$$

We will come back to this in Section 5 when we will show that $\mathrm{PSL}_2(\mathbb{Z})$ has far fewer congruence subgroups. Thus the congruence subgroup property fails in a very strong sense.

A different approach to computing $a_n(\mathrm{PSL}_2(\mathbb{Z}))$ is given by Stothers [St]. A recursive formula for this sequence was given by Godsil, Imrich, and Razen in [GIR]. In a series of papers Gardy and Newman ([GN1], [GN2], [GN3]) established some linear recurrences when $a_n(\Gamma)$ are considered modulo a fixed integer m when Γ is either a free group or a free product of cyclic groups.

Let us now look again at (1.4) for a general group Γ. With the notation introduced there, write $A(X) = A_\Gamma(X) = \sum_{n=1}^{\infty} a_n(\Gamma)X^n$ and $B(X) = B_\Gamma(X) = \sum_{n=0}^{\infty} b_n(\Gamma)X^n$ where $b_0(\Gamma) = 1$ and $b_n(\Gamma) = h_n(\Gamma)/n!$. Now, (1.4) means

$$n\, b_n(\Gamma) = \sum_{k=1}^{n} a_k(\Gamma) b_{n-k}(\Gamma)$$

which formally means

$$X\, B'(X) = A(X)\, B(X)$$

i.e.,

$$\frac{A(X)}{X} = \frac{B'(X)}{B(X)} = \log(B(X))'$$

and hence:

Proposition 1.10. $B(X) = exp\left(\int \frac{A(X)}{X}\, dX\right)$.

Note that $\int \frac{A(X)}{X}\,dX = \sum_{n=1}^{\infty} a_n(X)\frac{X^n}{n}$.

The last proposition has some non-trivial applications which are outside the main theme of this paper– but just to mention in brief: For a prime p let $\overline{\tau}_p(n) = \frac{\tau_p(n)}{n!}$ where $\tau_p(n)$ is the number of elements of order dividing p in S_n. Then:

$$1 + \sum_{n=1}^{\infty} \overline{\tau}_p(n) X^n = \exp\left(X + \frac{X^p}{p}\right)$$

This is deduced from (1.10) by considering the finite (!) group $\Gamma = \mathbb{Z}/p\mathbb{Z}$. So in some cases (1.10) can be useful to get information on $\mathrm{Hom}(\Gamma, S_n)$ from $a_n(\Gamma)$, rather than the opposite direction which will be our more common use of (1.10). More general results of this kind can be deduced very quickly from (1.10) using various finite groups. Special cases of it were studied over forty years ago (by more direct methods– see [MW] and [Wi] for history and references).

Far reaching generalizations of most of the above mentioned results were obtained recently by T. Müller [Mu5]. According to (1.10), $\Sigma\, b_n(X)\, X^n = \exp\left(\int \frac{A(X)}{X} dX\right)$, hence if G is a finite group of order m,

$$\sum \frac{|\mathrm{Hom}(G, S_n)|}{n!} X^n = \exp\left(\sum_{d|m} \frac{a_d(G)}{d} X^d\right)$$

Denote $P(X) = P_G(X) = \sum_{d|m} \frac{a_d(G)}{d} X^d = \sum_{i=1}^{m} C_i X^i$, then $P(X)$ is a real polynomial with non-negative coefficients, $C_1 \neq 0$, and $C_i = 0$ for $\frac{m}{2} < i < m$. Müller developed a machinery which gives a detailed asymptotic expansion for the coefficients of $\exp(P(X))$ for such $P(X)$. This way he obtained asymptotic expansion of $\mathrm{Hom}(G, S_n)$ for every finite group G. The precise result is too long to be mentioned here, but here is a corollary.

Theorem 1.11. (T. Müller [Mu5]) *Let G be a finite group of order m. Then*

$$|\,Hom(G, S_n)| \sim K_G\, n^{(1-1/m)n}\ exp\left(-(1-1/m)n + \sum_{\substack{d|m \\ d<m}} \frac{a_d(G)}{d}\, n^{d/m}\right)$$

where

$$K_G = \begin{cases} m^{-1/2} & \text{if } 2 \nmid m \\ m^{-1/2}\ exp\left(-\frac{(a_{m/2}(G))^2}{2m}\right) & \text{if } 2|m \end{cases}$$

Theorem 1.11 is an impressive generalization of Proposition 1.8 and [Wi], which proved a similar result for cyclic groups (but Müller's result is stronger even in the cyclic case as he gives the full expansion). More important for

our context is that the Theorem can be used to handle $a_n(\Gamma)$ for Γ which is a free product of finite groups in a way generalizing the deduction of (1.9) from (1.8). Here also Müller was able to give a detailed asymptotic expansion, but we bring only the asymptotic values:

Theorem 1.12. ([Mu5]) *Let $\Gamma = *_{i=1}^{s} G_i$ be a free product of $2 \leq s < \infty$ non-trivial finite groups of orders $m_1, \ldots, m_s$ respectively. If $s = 2$ assume not both G_1 and G_2 are cyclic of order 2. Then*

$$a_n(\Gamma) \sim L_\Gamma \cdot \Phi_\Gamma(n) \text{ as } n \to \infty$$

where

$$L_\Gamma = (2\pi m_1 \cdot \ldots \cdot m_s)^{-1/2} \exp\left(-\sum_{\{i \mid 2 \mid m_i\}} \frac{(a_{m_i,k}(G_i))^2}{2m_i}\right)$$

$$\Phi_\Gamma(n) = n^{-h(\Gamma)n} \exp\left(h(\Gamma)n + \sum_{i=1}^{s} \sum_{\substack{d_i < m_i \\ d_i \mid m_i}} \frac{a_{d_i}(G_i)}{d_i} n^{d_i/m_i} + \tfrac{1}{2}\log n\right)$$

and

$$h(\Gamma) = \text{ Euler characteristic of } \Gamma = \frac{1 - (m_1 - 1) \cdot \ldots \cdot (m_s - 1)}{m_1 \cdot \ldots \cdot m_s}$$

Note that Proposition 1.9 is a very special case of 1.12. As mentioned, the results of Müller are even stronger for the previously known special cases. For example for $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ he shows:

$$\begin{aligned} a_n(\Gamma) &= (12\pi e^{1/2})^{-1/2} n^{n/6} \exp\left(-\frac{n}{6} + n^{1/2} + n^{1/3} + \frac{1}{2}\log n\right) \\ &\quad \cdot \left\{1 - n^{-1/6} - \frac{1}{6} n^{-1/3} - \frac{13}{24} n^{-1/2} - \frac{7}{36} n^{-2/3} \right. \\ &\quad \left. + \frac{253}{240} n^{-5/6} - \frac{67963}{51840} n^{-1} - \frac{2449841}{362880} n^{-7/6} + 0\left(n^{-4/3}\right)\right\} \end{aligned}$$

We mention that along the way Müller shows that if Γ is as in Theorem 1.12, then as for the free group, $t_n(\Gamma) \sim h_n(\Gamma)$, i.e., "with probability one" the actions of Γ on $\{1, \ldots, n\}$ are transitive. The following generalization of Dixon's theorem mentioned above was conjectured in [Lu6] and was proved by Pyber [Py2].

Theorem 1.13. *Let G_1 and G_2 be two fixed non-trivial finite groups, not both of order 2. Then with probability 1 as n going to infinity, the images of G_1 and G_2 generate either A_n or S_n when we run over all possible homomorphisms from G_1 and G_2 (i.e., from $G_1 * G_2$) into S_n.*

Remark 1.14. We restrict ourselves to the problem of counting *all* subgroups. Much work has been done on counting free subgroups of virtually free groups. This is sometimes an easier problem as free subgroups correspond to some kind of fixed point free actions which are somewhat easier to be counted. The reader is referred to [Mu1], [Mu2], [Mu3], [St2] and the references therein.

2. Nilpotent groups and zeta functions

As mentioned in the first section, the subject of counting finite index subgroups started with the paper of M. Hall [Ha1] in 1949 which dealt with free groups. Over the next thirty-five years all papers on the topic elaborated on this and studied mainly groups which are virtually free. Approximately ten years ago, Dan Segal, Geff Smith and Fritz Grunewald ([Sm], [Se] and [GSS]- the last one appeared only in 1988 but was circulated around a few years earlier) initiated the study of the subject in "small" groups; solvable and especially nilpotent. If Γ is a finitely generated nilpotent group then it is particularly convenient to encode $a_n(\Gamma)$ (= the number of subgroups of index n in Γ) via a Dirichlet series $\zeta_\Gamma(s) = \Sigma a_n(\Gamma)n^{-s} = \Sigma[\Gamma : H]^{-s}$ where H runs over all finite index subgroups of Γ. The function $\zeta_\Gamma(s)$ is called the *Zeta function of* Γ. It has two pleasant properties:

(a) If Γ is nilpotent then $a_n(\Gamma)$ grows polynomially with n and $\zeta_\Gamma(s)$ is therefore not merely a formal series but actually converges for $Re(s) > \alpha$ where $\alpha = \alpha(\Gamma)$ is some real number.

(b) For a nilpotent Γ every subgroup H of index $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ is an intersection in a unique way of subgroups H_i $(1 \leq i \leq r)$ of index $p_i^{\alpha_i}$. Thus $a_n(\Gamma) = \Pi_{i=1}^r a_{p_i^{\alpha_i}}(\Gamma)$ and hence $\zeta_\Gamma(s)$ has Euler product decomposition $\zeta_\Gamma(s) = \prod_p \zeta_{\Gamma,p}(s)$ where the product runs over all primes and $\zeta_{\Gamma,p}(s) = \sum_{i=0}^\infty a_{p^i}(\Gamma)p^{-is}$.

So the zeta function $\zeta_\Gamma(s)$ of a nilpotent group share some of the features of Dedekind zeta function of a number field K, $\zeta_K(s) = \sum_M [O : M]^{-s}$ where O is the ring of integers of K and M runs over all finite index ideals of O. Many of the zeta functions $\zeta_\Gamma(s)$ which were computed in [Sm] and [GSS] are expressed via such $\zeta_K(s)$ and especially via $\zeta(s) = \zeta_{\mathbb{Q}}(s) = \Sigma n^{-s} = \prod_p (1 - p^{-s})^{-1}$.

It is very tempting to believe that the other properties of the classical zeta functions are also shared by $\zeta_\Gamma(s)$, e.g., the existence of a functional equation. But as of now very little is known. The reader might also suggest that the appropriate analoge of Dedekind zeta function for groups should be $\zeta_\Gamma^{\triangle}(s) = \sum_N [\Gamma : N]^{-s}$ where N runs only over the *normal* subgroups of finite index. Indeed, in [Sm] and [GSS], $\zeta_\Gamma^{\triangle}(s)$ was also studied beside $\zeta_\Gamma(s)$, as well

as two other related functions. Only the future will tell which one is more suitable for group theoretic use.

We start with the free abelian groups:

Theorem 2.1. *Let $\Gamma = \mathbb{Z}^r$ be the free abelian group of rank r. Then*

$$\zeta_{\mathbb{Z}^r}(s) = \zeta(s) \cdot \zeta(s-1) \cdot \ldots \cdot \zeta(s-r+1)$$

where ζ is the classical Riemann ζ-function.

There are five (!) different proofs in the literature for this not too difficult, yet not completely trivial, result. (See [BR2], [Sm], [Il1], [GSS], and [Man3]. In [Lu6], the first four are described in detail.) We sketch here the proof from [GSS], which while applied to a general nilpotent group gives the important Theorem 2.13 below.

We start with a simple Lemma:

Lemma 2.2. *Let Γ be a group and $\hat{\Gamma}$ its pro-finite completion. Then*

(a) For every n, $a_n(\Gamma) = a_n(\hat{\Gamma})$ where for a pro-finite group G, by $a_n(G)$ we mean the number of closed *subgroups of index n.*

(b) If $\hat{\Gamma}$ is pro-nilpotent (i.e., if every finite quotient of Γ is nilpotent or equivalently $\hat{\Gamma} = \prod_p \Gamma_{\hat{p}}$ where p runs over all primes and $\Gamma_{\hat{p}}$ denotes the pro-p completion of Γ) then:

(i) $\zeta_{\Gamma,p}(s) = \zeta_{\Gamma_{\hat{p}}}(s)$

ii) $\zeta_\Gamma(s) = \prod_p \zeta_{\Gamma,p}(s)$

This lemma is very simple and we omit the proof. But one warning should be made: $\zeta_{\Gamma,p}(s)$ is defined as $\sum_{i=0}^{\infty} a_{p^i}(\Gamma) p^{-is}$, i.e., encoding all subgroups of p- power index. For general groups Γ this is *not* the same as $\zeta_{\Gamma_{\hat{p}}}(s)$ which captures only the *sub-normal* subgroups of Γ of p-power index.

Anyway for $\Gamma = \mathbb{Z}^r$ or more generally for Γ nilpotent, we can compute $\zeta_\Gamma(s)$ via $\zeta_{\Gamma_{\hat{p}}}(s)$. Theorem 2.1 is therefore equivalent to the assertion:

$$\zeta_{\mathbb{Z}_p^r}(s) = \prod_{i=0}^{r-1} (1 - p^i p^{-s})^{-1}$$

Let $G = \mathbb{Z}_p^r$ with the standard basis $\{e_1, e_2, \ldots, e_r\}$. A finite index subgroup H of G has a basis of the following form:

$$h_1 = (\lambda_{11}, \ldots, \lambda_{1n})$$
$$h_2 = (0, \lambda_{22}, \ldots, \lambda_{2n})$$

$$h_i = (0, \dots 0, \lambda_{ii}, \dots, \lambda_{in})$$
$$\vdots$$
$$h_n = (0, \dots, 0, \lambda_{rr})$$

obtained in the following way: $H \cap \mathbb{Z}_p e_r = \lambda_{rr} e_r$, and

$$(H \cap \ \mathrm{Span}_{\mathbb{Z}_p}\{e_i, e_{i+1}, \dots, e_r\}) \equiv \lambda_{ii}\, e_i (\text{modulo } \mathrm{Span}_{\mathbb{Z}_p}\{e_{i+1}, \dots, e_r\}).$$

A basis of H of this form will be called a good basis. It is easy to see that $[G : H] = |\lambda_{11}|^{-1} \cdot \dots \cdot |\lambda_{nn}|^{-1} = p^{\alpha_1} \cdot \dots \cdot p^{\alpha_r}$ (where $\lambda_{ii} = p^{\alpha_i} u_i$ and u_i is a unit of $\mathbb{Z}_p$). Let $M(H)$ denote the subset of the upper triangular matrices M obtained by taking bases for H of the above form. Let μ be the normalized Haar measure of the additive group of the upper triangular matrices over $\mathbb{Z}_p$.

Lemma 2.3. $\mu(M(H)) = (1-p^{-1})^r p^{-\alpha_1} p^{-2\alpha_2} \cdot \dots \cdot p^{-r\alpha_r} = (1-p^{-1})^r \prod_{i=1}^r |\lambda_{ii}|^i$.

PROOF. Note first that $M(H)$ is an open set. If $\{h_1, \dots, h_r\}$ is a good basis as above, then any other good basis $\{h'_1, \dots, h'_r\}$ can be written as $h'_i = \lambda_{ii} u_i + \nu_{i+1}$ where ν_{i+1} is in the $\mathbb{Z}_p$-span of $\{h_{i+1}, \dots, h_r\}$ and $u_i \in \mathbb{Z}_p^*$- the group of units of $\mathbb{Z}_p$. Thus h_r can be "moved" in a subset of $\mathbb{Z}_p$ of measure $(1-p^{-1})|\lambda_{rr}| = (1-p^{-1})p^{-\alpha_r}$, h_{r-1} can be moved by multiplication of $\lambda_{r-1,r-1}$ by a unit and by adding $p^{\alpha_r}\mathbb{Z}_p e_r$, so as an element of $\mathbb{Z}_p \times \mathbb{Z}_p$, h_{r-1} can vary along a subset of measure $(1-p^{-1})p^{-\alpha_{r-1}} \cdot p^{-\alpha_r}$. Similarly h_{r-2} can be multiplied by $\mathbb{Z}_p^*$, i.e., $\lambda_{r-2,r-2}$ can be changed within a subset of $\mathbb{Z}_p$ of measure $(1-p^{-1})p^{-\alpha_{r-2}}$ and the pair $(\lambda_{r-2,r-1}, \lambda_{r-2,r})$ can be changed by addition of elements from the set $\mathbb{Z}_p \lambda_{r-1,r-1} e_{r-1} + \mathbb{Z}_p \lambda_{r,r} e_r$. This shows that h_{r-2} can be "moved" within a subset of $\mathbb{Z}_p^3$ of measure $(1-p^{-1})p^{-\alpha_{r-2}} \cdot p^{-\alpha_{r-1}} \cdot p^{-\alpha_r}$. In a similar way h_i can be a vector from a subset of $\mathbb{Z}_p^{r-i+1}$ of measure $(1-p^{-1})p^{-\alpha_{i+1}} \cdot \dots \cdot p^{-\alpha_r}$. Now, μ is the product measure of all these. Hence:

$$\mu(M(H)) = (1-p^{-1})^r p^{-r\alpha_r}\, p^{-(r-1)\alpha_{r-1}} \cdot \dots \cdot p^{2\alpha_2} \cdot p^{-\alpha_1}$$

as claimed. □

As said before $[G : H] = |\lambda_{11}|^{-1} \cdot \dots \cdot |\lambda_{rr}|^{-1}$. Thus:

Corollary 2.4. $[G : H]^{-s} = \frac{1}{(1-p^{-1})^r} \int_{M(H)} |\lambda_{11}|^s \cdot \dots |\lambda_{rr}|^s \cdot |\lambda_{11}|^{-1} |\lambda_{22}|^{-2} \cdot \dots \cdot |\lambda_{rr}|^{-r} d\mu$.

So we can replace the sum $\zeta_{\mathbb{Z}_p^r}(s) = \sum_{H \le_f G} [G : H]^{-s}$ by an integral

$$\zeta_{\mathbb{Z}_p^r}(s) = \frac{1}{(1-p^{-1})^r} \int_{\bigcup_H M(H)} |\lambda_{11}|^{s-1} \cdot \dots \cdot |\lambda_{rr}|^{s-r}\, d\mu.$$

To evaluate this integral note that $\cup_H M(H)$ is equal to the set all upper triangular matrices over $\mathbb{Z}_p$ with non-zero entries along the diagonal. Those with determinant zero form a set of measure zero and therefore can be ignored. Thus:

$$\begin{aligned}\zeta_{\mathbb{Z}_p^r}(s) &= \frac{1}{(1-p^{-1})^r}\int_T |\lambda_{11}|^{s-1}\cdot\ldots\cdot|\lambda_{rr}|^{s-r} \\ &= \frac{1}{(1-p^{-1})^r}\Pi_{i=1}^r\int_{\mathbb{Z}_p}|\lambda_{ii}|^{s-i}d\nu\end{aligned}$$

where $d\nu$ is the normalized Haar measure of $\mathbb{Z}_p$. A simple computation (which will be used often) shows:

Lemma 2.5. $\int_{\mathbb{Z}_p}|\lambda|^s d\nu = \sum_{i=0}^{\infty}(1-p^{-1})p^{-i}p^{-is} = \frac{1-p^{-1}}{1-p^{-s-1}}$

Thus $\zeta_{\mathbb{Z}_p^r} = (1-p^{-s})^{-1}(1-p^{-(s-1)})^{-1}\cdot\ldots\cdot(1-p^{-(s-(r-1))})^{-1}$ which proves (2.1). □

This proof can be carried a long way for an arbitrary finitely generated, torsion free, nilpotent group Γ. For such Γ there is a series of normal subgroups $\Gamma = \Gamma_1 \geq \Gamma_2 \geq \ldots \geq \Gamma_r \geq \Gamma_{r+1} = \{1\}$ such that $\Gamma_i/\Gamma_{i+1} \simeq \mathbb{Z}$ for $i = 1,\ldots,r$, where r is the Hirsch length of Γ. For $i = 1,\ldots,r$ choose $x_i \in \Gamma_i$ such that $x_i\Gamma_{i+1}$ generate Γ_i/Γ_{i+1}. Every element x of Γ can be represented *uniquely* as $x = x_1^{a_1}\cdot\ldots\cdot x_r^{a_r}$ with $a_i \in \mathbb{Z}$ and $\{x_1,\ldots,x_r\}$ is called a Malćev basis for Γ. P. Hall showed that by considering $(a_1,\ldots,a_r)$ as the cordinates of x, the group operation in Γ are given by polynomial functions whose coefficients are in $\mathbb{Q}$ (See [*Ha*]).

We can define now $G = \Gamma^{\mathbb{Z}_p}$ to be the space $\mathbb{Z}_p^r$ where the group operation are given by the same polynomials expressing the group operations of Γ. It is easy to see that $\Gamma^{\mathbb{Z}_p}$ is a pro-p group and in fact isomorphic to the pro-p completion of Γ. Thus $\zeta_{\Gamma,p} = \zeta_G$. The groups $G_i = \Gamma_i^{\mathbb{Z}_p}$ define a filtration $G = G_1 \geq G_2 \geq \ldots \geq G_r \geq G_{r+1} = \{1\}$ of G.

Definition 2.6. Let H be a finite index subgroup of G. A subset $\{h_1,\ldots,h_r\} \leq H$ is called a *good basis* for H if for every $i = 1,\ldots,r$, h_iG_{i+1} generate $(H\cap G_i)G_{i+1}/G_{i+1}$. This is indeed a basis for H and every element x of H can be represented uniquely as $x = h_1^{\lambda_1}\cdot\ldots\cdot h_r^{\lambda_r}$ with $\lambda_i \in \mathbb{Z}_p$. ($h^\lambda$ for $h \in H$ and $\lambda \in \mathbb{Z}_p$ is well defined– see [DDMS, Chapter 1]). We consider $(\lambda_1,\ldots,\lambda_2)$ as the coordinates of x in $\mathbb{Z}_p^r$.

The coordinates of a good basis of H have the form:

$$h_i = (0,\ldots,0,\lambda_{ii},\ldots,\lambda_{ir}),\quad i = 1,\ldots,r$$

(By an abuse of the language we will identify an element and its vector of coordinates.) So as before we can associate with a good basis an upper

triangular matrix. Again, $[G : H] = \Pi_{i=1}^{r} |\lambda_{ii}|^{-1}$. Let $M(H)$ be the set of all upper triangular $r \times r$ matrices over $\mathbb{Z}_p$ obtained from good bases of H.

Lemma 2.7. *$M(H)$ is open and $\mu(M(H)) = (1 - p^{-1})^r \Pi_{i=1}^{r} |\lambda_{ii}|^i$.*

(Note the $|\lambda_{ii}|$ are determined by H and not by the given basis as $|\lambda_{ii}|^{-1} = |(H \cap G_i)G_{i+1}/G_{i+1}|$).

The proof of (2.7) is identical to that of (2.3). The commutativity of $\mathbb{Z}_p^r$ did not play any role there. Just as for $\mathbb{Z}_p^r$ we can deduce:

Proposition 2.8. *$\zeta_{\Gamma,p}(s) = \zeta_G(s) = (1 - p^{-1})^{-r} \int_M \Pi_{i=1}^{r} |\lambda_{ii}|^{s-i} d\mu$ where M is the union of all $M(H)$ where H runs over all finite index subgroups of G.*

Unlike the case $G = \mathbb{Z}_p^r$ it is not so easy to describe M for general groups. Still when this can be done (2.8) can give a complete answer. We illustrate this by:

Theorem 2.9. *Let Γ be the discrete Heizenberg group, i.e.*

$$\Gamma = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$$

Then:

$$\zeta_\Gamma(s) = \frac{\zeta(s)\,\zeta(s-1)\,\zeta(2s-2)\,\zeta(2s-3)}{\zeta(3s-3)}$$

PROOF. The Heizenberg group is $P = \langle x, y, z \mid (x, y) = z,\ (x, z) = (y, z) = 1 \rangle$ and its pro-p completion $G = \Gamma_{\hat{p}}$ has, of course, the same presentation, just being considered as a presentation within the category of pro-p groups. Let G_3(resp : G_2) be the closed subgroup generated by z(resp : z and y) and $G_1 = G$. Proposition 2.8 gives a formula for $\zeta_{\Gamma,p}(s) = \zeta_G(s)$, but we have to recognize M– the set of upper triangular matrices which represent good bases of finite index subgroups of G. If $A = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ 0 & \lambda_{22} & \lambda_{23} \\ 0 & 0 & \lambda_{33} \end{pmatrix}$ is such a matrix then by Definition 2.6 it represents a good basis for an open subgroup H if and only if the following three conditions are satisfied:

(i) H is generated (as a closed subgroup) by $x^{\lambda_{11}} y^{\lambda_{12}} z^{\lambda_{13}}$, $y^{\lambda_{22}} z^{\lambda_{23}}$ and $z^{\lambda_{33}}$

(ii) $H \cap G_2$ is generated by $y^{\lambda_{22}} z^{\lambda_{23}}$ and $z^{\lambda_{33}}$ and

(iii) $H \cap G_3$ is generated by $z^{\lambda_{33}}$

So if we take H to be the subgroup generated by the three elements in (i), then it is open if and only if $\lambda_{11} \cdot \lambda_{22} \cdot \lambda_{33} \neq 0$. Assume this, then (iii) is satisfied if and only if the commutator $(x^{\lambda_{11}} y^{\lambda_{12}} z^{\lambda_{13}}, y^{\lambda_{12}} z^{\lambda_{23}})(= (x^{\lambda_{11}}, y^{\lambda_{22}}) = z^{\lambda_{11}\lambda_{22}})$ is in the subgroup generated by $z^{\lambda_{33}}$. This happens if and only if λ_{33} divides $\lambda_{11} \cdot \lambda_{22}$ in $\mathbb{Z}_p$ i.e., $v(\lambda_{33}) \leq v(\lambda_{11}) + v(\lambda_{22})$, where v is the p-adic valuation. If condition (iii) is satisfied then one easily checks that (ii) also follows. We conclude that M is the set of all upper triangular matrices of type A above for which all $\lambda_{ii} (i = 1, 2, 3)$ are non-zero and $v(\lambda_{33}) \leq v(\lambda_{11}) + v(\lambda_{22})$. Thus, by (2.8),

$$\begin{aligned} \zeta_\Gamma^p(s) &= \zeta_G(s) = (1-p^{-1})^{-3} \int_M |\lambda_{11}|^{s-1} |\lambda_{22}|^{s-2} |\lambda_{33}|^{s-3} \, d\mu \\ &= (1-p^{-1})^{-3}(1-p^{-1})^3 \sum_{e_1=0}^{\infty} \sum_{e_2=0}^{\infty} \sum_{e_3=0}^{e_1+e_2} p^{-e_1 s} p^{e_2(s-1)} p^{e_3(s-2)}. \end{aligned}$$

In the last equality we are using Lemma 2.5. A simple computation now finishes the proof of 2.9. □

Let's now look again in the general case of torsion free nilpotent groups: Proposition 2.8 gives a quite explicit integral which expresses $\zeta_{\Gamma,p}(s)$. The only difficulty is the range of integration M. This is the set of all upper triangular matrices with row-columns $h_i = (0, \ldots, 0, \lambda_{ii}, \ldots, \lambda_{ir}), i = 1, \ldots, r$, which represent good bases for open subgroups of $G = \Gamma_{\hat{p}}$.

Lemma 2.10 *An ordered set of rows $\{h_1, \ldots, h_r\}$ represents a good basis of* some *finite index subgroup H of G if and only if*

(i) $\Pi \lambda_{ii} \neq 0$ *and*

(ii) If $i \geq j$ then the commutator (h_i, h_j) is in the subgroup generated by $h_{j+1}, \ldots, h_r$, i.e., there exist $\beta_{j+1}, \ldots, \beta_r$ in $\mathbb{Z}_p$ such that $(h_i, h_j) = h_{j+1}^{\beta_{j+1}} \cdot \ldots \cdot h_r^{\beta_r}$.

PROOF. Clearly a good basis, i.e., a basis $\{h_1, \ldots, h_r\}$ of H for which $H \cap G_i = \langle h_i, h_{i+1}, \ldots, h_r \rangle$ should satisfy the conditions. Conversely, assume (i) and (ii) are satisfied and let H be the subgroup generated by $\{h_1, \ldots, h_r\}$. Condition (i) implies that H is of finite index. Denote $H_i = \langle h_i, \ldots, h_r \rangle$ and assume by induction that $H_j = H \cap G_j$ for $j < i$ and let's prove it for $j = i$: Condition (ii) implies that H_i is normal in H. As $H_{i-1} = H \cap G_{i-1}$ is generated by $h_{i-1}, h_i, \ldots, h_r$ and H_i is normal in H_{i-1} we get: $H_{i-1} = H_i \cdot \langle \overline{h_{i-1}} \rangle$. So: $H \cap G_i = H_{i-1} \cap G_i = H_i \cdot \langle \overline{h_{i-1}} \rangle \cap G_i = H_i \cap G_i = H_i$ and the lemma is proven. □

Now comes a crucial observation: Conditions (i) and (ii) of Lemma 2.10 show that M is a *definable* subset of the upper triangular matrices over $\mathbb{Z}_p$. This means that M can be described by first order statements. This is clear for condition (i). But some explanation is needed regarding condition (ii):

We mentioned earlier that P. Hall showed that by choosing a Malćev basis for Γ (and thus identifying Γ with $\mathbb{Z}^r$ as a set) the group operation of Γ are given by rational polynomials. In fact more is true: The k-power operation in Γ is polynomial in Γ *and* k, i.e., the map $\psi : \Gamma \times \mathbb{Z} = \mathbb{Z}^r \times \mathbb{Z} \to \Gamma = \mathbb{Z}^r$ given by $\psi(\gamma, k) = \gamma^k$ for $\gamma \in \Gamma$ and $k \in \mathbb{Z}$ is a polynomial map from $\mathbb{Z}^{r+1}$ to $\mathbb{Z}^r$ with rational coefficients. Therefore this map can also be extended to $\Gamma_{\hat{p}} \times \mathbb{Z}_p \to \Gamma_{\hat{p}}$.

Thus if we look at condition (ii) it says that for the commutator of h_i and h_j there exist $\beta_{j+1}, \ldots, \beta_n$ such that $\psi(h_{j+1}, \beta_{j+1}) \cdot \ldots \cdot \psi(h_r, \beta_r) = (h_i, h_j)$. As the commutator and the product are polynomials this is a statement in the first order language. We have:

Proposition 2.11. *The domain of integration M in Proposition 2.8 is a definable set.*

Everything is now ready to apply the following theorem:

Theorem 2.12. (Denef [De1]) *Let M be a definable subset of $\mathbb{Z}_p^m$ and $h : \mathbb{Z}_p^m \to \mathbb{Z}_p$ be a definable function. Then $Z_M(s) = \int_M |h(x)|^s d\mu$, where $d\mu$ is the Haar measure of $\mathbb{Z}_p^m$, is a rational function of p^{-s}.*

A definable function $h : \mathbb{Z}_p^m \to \mathbb{Z}_p$ is a function whose graph $\{(y, h(y)) \in \mathbb{Z}_p^{m+1} | y \in \mathbb{Z}_p^m\}$ is a definable subset.

While we will not go here into the proof of this Theorem, it is worth mentioning that it relies on work of Macintyre [Ma1] in logic. Macintyre studied the first order theory of the p-adic numbers: He looked at the language of valued fields (i.e., the language of fields plus one unary predicate saying whether an element of the field is in the valued ring or not). Then added to this language a sequence of unary predicate symbols $P_1, P_2, P_3, \ldots$ whose interpretation is $x \in P_n$ if X is an n power in the field. Macintyre proved that the theory of p-adic numbers admits an elimination of quantifiers in the extended language. Now, each formula $\varphi(X_1, X_2, \ldots, X_m)$ of the language defines a set $A = \{(\underline{a}) \in \mathbb{Q}_p^m | \mathbb{Q}_p \models \varphi(\underline{a})\}$ (these are the "definable sets"). The resutl of Macintyre means that every definable set has a simpler form: It is a Boolean combination of sets of the forms $\{x \in \mathbb{Q}_p^m | \exists y \in \mathbb{Q}_p \text{ s.t.} f(x) = y^n\}$ with $f \in \mathbb{Z}_p[x_1, \ldots, x_m]$ and $n \in \mathbb{N}$. Thus to prove Denef's Theorem one can assume that the domain of integration has such a form. This was the starting point of the beautiful work of Denef who used it to prove some conjectures of Serre and Igusa on the rationality of the generating function of the number of solutions mod p^n of some diophantine equations.

Theorem 2.12, Proposition 2.11 and Proposition 2.8 give us now the main theorem of this chapter:

Theorem 2.13. (Grunewald-Segal-Smith [GSS]) *The p-th Euler factor of the zeta function of a finitely generated torsion free nilpotent group is a rational function of p^{-s}*

Rationality means in particular that the coefficients $a_{p^n}(\Gamma)$ satisfie a linear recurrence relation. So:

Corollary 2.14. *There exist positive integers l and k such that the sequence $(a_{p^i}(\Gamma))_{i>l}$ satisfies a linear recurrence relation over $\mathbb{Z}$ of length at most k.*

Remark 2.15 (Uniformity in p) The set M of Propositions 2.8 and 2.11 was actually definable in a way which is independent of the prime p. The results of Denef [De2] and Macintyre [Ma2] show that in such a case the rational functions of (2.12) and (2.13) may be taken to have numerators and denominators of bounded degrees– independent of p. This also implies that l and k in (2.14) can be chosen to work for all primes p. Grunewald, Segal and Smith [GSS] suggest even a stronger possibility: Given Γ, a torsion free finitely generated nilpotent group, then there exist finitely many rational functions $W_1(X,Y),\ldots,W_n(X,Y)$ of two variables over $\mathbb{Q}$ such that for each prime p there is an i for which $\zeta_{\Gamma,p}(s) = W_i(p,p^{-s})$. The many computations and results in [GSS] give quite strong support to conjecture that this is indeed the case.

Remark 2.16. (Uniformity for groups of the same Hirsch length)) Recently M. du Sautoy proved: For a given r, there exists a polynomial $f(Y,X)$ in $\mathbb{Q}[Y,X]$ such that if G is a finitely generated torsion free nilpotent group Γ of Hirsch length r and p a prime, then there exists a polynomial $Q(X) \in \mathbb{Q}[X]$, depending on Γ and p, such $\zeta_{\Gamma,p}(s) = \frac{Q(p^{-s})}{f(p,p^{-s})}$.

We end this section mentioning some results about a different zeta function associated with a finitely generated group. Namely, let $\hat{a_n}(\Gamma)$ be the number of subgroups of Γ of index n whose profinite completion is isomorphic to $\hat{\Gamma}$. In [GSS], is was shown that $\hat{\xi_\Gamma}(s) = \sum \hat{a_n}(\Gamma)n^{-s}$ has Euler product decomposition $\hat{\xi_\Gamma}(s) = \prod_p \hat{\xi}_{\Gamma,p}(s)$ and Theorem 2.13 is also valid for it. Moreover, there exists a $\mathbb{Z}$-Lie ring L, with $\hat{\xi}_{\Gamma,p}(s) = \hat{\xi}_{L,p}(s)$ for almost every prime, where $\hat{\xi}_{L,p}(s)$ is defined in the clear analogous way. It is also shown there that for almost all primes p,

$$\hat{\xi}_{\Gamma,p}(s) = \int_{G_p^+} |\det g|_p^s d\mu_p, \qquad (*)$$

where $G \leq \mathrm{GL}(L)$ is the algebraic group of automorphisms of L, $G_p^+ = G(\mathbb{Q}_p) \cap \mathrm{End}(L \otimes \mathbb{Z}_p)$ and μ_p is the Haar integral of $G(\mathbb{Q}_p)$ normalized so that $\mu(G(\mathbb{Z}_p)) = 1$. The integral in $(*)$ was computed by Igusa [Ig] for a reductive group G (under some assumptions on the representation of G). Igusa's work

generalized earlier results of Satake and MacDonald for some classical groups. In our context, G is typically not reductive. In [dSL], duSautoy and Lubotzky show how to reduce the computation of (*), under some assumptions, to the reductive case. This way they can use Igusa's work to get: (a) explicit computation of $\hat{\xi}_{\Gamma,p}(s)$ for some interesting examples, (b) uniformity results of the type conjectured in [GSS]– see Remark 2.15 above– and (c) a functional equation for $\hat{\xi}_{\Gamma,p}$ (but not for $\hat{\xi}_{\Gamma}$).

Incidentally, the functional equation expresses the symmetry in a root system of a reductive group G between the positive and negative roots– see [Ig] and [dSL].

While the method applies only to $\hat{\xi}_{\Gamma,p}$ and not to $\xi_{\Gamma,p}$, it supports similar conjectures for $\xi_{\Gamma,p}$.

For a comprehensive survey of various zeta functions associated with groups, the reader is referred to [dS6].

3. Pro-p groups

The subject of counting finite index subgroups is intimately connected with pro-finite groups. This is of no surprise and we have already made use of it. This section will be devoted to counting questions for the pro-finite groups themselves. Beside the intrinsic interest, some of the results on pro-finite groups are useful for applications to discrete groups. In the context of pro-finite groups G, $a_n(G)$ denotes of course the number of open subgroups of index n.

For the free pro-finite group $\hat{F}_2$, there is nothing new to say: $a_n(\hat{F}_r) = a_n(F_r)$ and $a_n(F_r)$ was discussed in length in Section 1. More interesting is the case of a free pro-p group on r generators denoted $F_{r,\hat{p}}$.

For such a free pro-p group $F = F_{r,\hat{p}}$, $a_n(F) = 0$ unless $n = p^k$ and $a_{p^k}(F)$ is equal to the number of subnormal subgroups of index p^k in F_r.

The number $a_{p^k}(F_{r,\hat{p}})$ can be calculated recursively using P. Hall's enumeration principle.

Proposition 3.1. (Ilani [Il1]) *For $k \geq 1$,*

$$a_{p^k}(F_{r,\hat{p}}) = \sum_{t=1}^{r}(-1)^{t+1} \begin{bmatrix} r \\ t \end{bmatrix} p^{t(t-1)/2}\, a_{p^{k-t}}(F_{p^t(r-1),\hat{p}})$$

where $\begin{bmatrix} r \\ t \end{bmatrix}$ *is the number of subspaces of codimension t in the r-dimensional vector space $\mathbb{F}_p^r$.*

The above proposition gives a legitimate recursive formula, but it uses $a_{p^l}(F_{s,\hat{p}})$ to express $a_{p^k}(F_{r,\hat{p}})$ with $s \neq r$ ($s > r$ but $l < k$). Ilani (loc. cit.)

was able to deduce from (3.1) a recursion relation which expresses $a_{p^k}(F_{r,\hat{p}})$ using only $a_{p^t}(F_{r,\hat{p}})$ for $t < k$.

Proposition 3.2. *For $k \geq 1$,*

$$a_{p^k}(F_{r,\hat{p}}) = \sum_{l=1}^{k} (-1)^{t+1} p^{t(t-1)/2} \begin{bmatrix} p^{k-t}(r-1)+1 \\ t \end{bmatrix} a_{p^{k-t}}(F_{r,\hat{p}}).$$

Proposition 3.3. *Let $G = F_{r,\hat{p}}$ be the free pro-p group on $r \geq 2$ generators. Then:*

$$p^{\frac{r-1}{p-1}(p^n-1)-\frac{n(n-1)}{2}} \leq a_{p^n}(G) \leq p^{\frac{r-1}{p-1}(p^n-1)}$$

and hence:

$$\lim(a_{p^n}(G))^{p^{-n}} = p^{(r-1)/(p-1)}.$$

In particular $a_{p^n}(G)$ grows exponentially as a function of p^n.

This last result was extended significantly by Mann [Man3] and Pyber-Shalev [PS1]:

Theorem 3.4. *Let G be a finitely generated pro-finite group. Then*

(a) (Mann) *If G is pro-solvable then $a_n(G)$ grows at most exponentially.*

(b) (Pyber-Shalev) *If $a_n(G)$ grows super exponentially (i.e., $\frac{\log a_n(G)}{n}$ is unbounded), then every finite groups is a quotient of some finite index subgroup of G.*

Theorem 3.4(a) implies in particular that for a finitely generated solvable group Γ, $a_n(\Gamma)$ grows at most exponentially (since $a_n(\Gamma) = a_n(\hat{\Gamma})$). There are finitely generated (pro-p and discrete) solvable groups of exponential growth, e.g., $\Gamma = C_p \wr \mathbb{Z}$. It is however interesting to observe that finitely *presented* groups behave differently.

Proposition 3.5. *Let G be a finitely presented solvable pro-p group. Then $a_n(G) \leq C^{\sqrt{n}}$ for some constant C.*

PROOF. Wilson [Wn1] showed that G satisfies the Golod-Shafarevitz inequality. Namely, for arbitrary finite presentation $\langle X; R\rangle$ of G, one has

$$|R| - (|X| - d(G)) \geq \frac{d(G)^2}{4}, \qquad (*)$$

where $d(G)$ denotes the minimal number of generators of G. Moreover, Wilson deduced that this implies that there exists a constant c such that $d(H) \leq c[G : H]^{1/2}$ for every open subgroup H of G. Indeed, if G has a presentation with d generators and r relations and $[G : H] = h$, then H has a presentation

with at most hd generators and hr relations. Hence, by $(*)$ applied to H, $d(H)^2 \leq c[G:H]$.

Now, a subgroup H of index $n = p^l$ in a pro-p group is contained in a subgroup K of index p^{l-1} and given K there are at most $\frac{p^{d(K)}-1}{p-1}$ possibilities for H. From this one can easily deduce the proposition. □

Segal and Shalev [SS] constructed for every $d \geq 2$, finitely presented (pro-p and discrete) metabelian groups G with $a_n(G)$ growth like $C^{n^{1/d}}$.

Let's pass now to groups of "slow growth". The next theorem characterizes pro-p groups of polynomial subgroup growth (PSG) as the p-adic analytic pro-p groups. It plays an important role in the characterization of discrete groups of polynomial subgroup growth– to be described in the next chapter.

The equivalence of (a) and (b) is due to Lubotzky and Mann ([LM2], cf. [DDMS]) while the equivalence of (a) and (c) was shown by Shalev [Sh1]:

Theorem 3.6. *Let G be a pro-p group. The following three conditions are equivalent:*

(a) G is a p-adic analytic group.

(b) G has polynomial subgroup growth (PSG), i.e., $a_n(G) \leq n^c$ for some constant c and every n.

(c) $a_n(G) \leq C\, n^{(\frac{1}{8}-\epsilon)\log n}$ for some $C, \epsilon > 0$ and every n.

The theorem shows that there is a gap in the possible growths: if a pro-p group has growth $O(n^{(\frac{1}{8}-\epsilon)\log n})$ for some $\epsilon > 0$, then it actually has polynomial growth. The following result of Shalev [Sh1] (see also [LS]) shows that this is essentially best possible:

Theorem 3.7. *Let $G = Ker(SL_2(\mathbb{F}_p[t]) \to SL_2(\mathbb{F}_p))$. Then $a_n(G) = O(n^{(2+\epsilon)\log n})$ for every $\epsilon > 0$.*

On the other hand, Shalev [Sh2] showed that in the category of pro-finite groups there is no gap between polynomial and non-polynomial subgroup growth. Namely:

Theorem 3.8. *For every function $f: \mathbb{N} \longrightarrow \mathbb{N}$ such that $f(1) \geq 1$ and $\frac{\log f(n)}{\log n} \to \infty$, there is a finitely generated non-PSG pro-finite group G satisfying $a_n(G) \leq f(n)$ for every n.*

Lubotzky [Lu4] showed that among the finitely generated linear groups there is a gap between polynomial and non-polynomial groups.

Theorem 3.9. *Let Γ be a finitely generated non-PSG linear group (over some field F). Then there exists a constant C such that $a_n(\Gamma) \geq n^{c\log n/\log\log n}$ for infinitely many n.*

As we will see in Section 5, this result is the best possible. The answer to the following interesting problem however is not known.

Problem 3.10. Is there a gap between PSG and non-PSG in the category of all finitely generated groups? If so, what is the minimum?

We believe that groups with growth $n^{c\log n/(\log\log n)^2}$ exist, and maybe this is the minimal possible non-PSG for general finitely generated groups.

Let's go back to pro-p groups.

The next theorem deals with the regularity behavior of the number of finite index subgroups in a compact p-adic analytic groups rather than the growth. It is a far reaching extension of Theorem 2.13.

Theorem 3.11. (du Sautoy [dS3]) *Let G be a compact p-adic analytic group. Then $\zeta_{G,p}(s) = \sum_{n=1}^{\infty} a_{p^n} p^{-ns}$ is a rational function in p^{-s} with rational coefficients.*

The theorem does not assume that G is pro-p (though it has a pro-p subgroup of finite index).

The proof of 3.11 borrows its main strategy from the proof of (2.13), i.e., to express the zeta function as a p-adic integral over a set representing good bases for finite index subgroups. But (3.11) is not merely much more difficult than (2.13); it is also impractical. The parametrization given for (2.13), enables (at least in principle, and as illustrated in the proof of (2.1) and in the proof of (2.9), also in practice) to calculate the ζ-function explicitly. This however seems impossible by the proof of (3.11). As of now the only non-nilpotent pro-p groups for which the ζ-function was computed explicitly are congruence subgroups of $SL_2(\mathbb{Z}_p)$, $p \geq 3$.

Theorem 3.12. (Ilani [Il3]) *Let p be a prime greater than two and $G = Ker(SL_2(\mathbb{Z}_p) \to SL_2(\mathbb{F}_p))$. Then G is a uniform pro-p group and*

$$a_{p^n}(G) = \begin{cases} \frac{p+1}{2(p-1)}(n-1)p^{n+1} + \frac{p^3-2p-2}{(p-1)^2(p+1)}\,p^{n+1} + \frac{p^{(n+3)/2}}{(p-1)^2} + \frac{1}{(p-1)^2(p+1)} & n \text{ odd} \\ \frac{p+1}{2(p-1)}n\,p^{n+1} - \frac{2p+1}{(p-1)^2(p+1)}\,p^{n+1} + \frac{p^{(n+4)/2}}{(p-1)^2} + \frac{1}{(p-1)^2(p+1)} & n \text{ even.} \end{cases}$$

Hence

$$\zeta_G(s) = \zeta_{G,p}(s) = \Sigma a_{p^n}(G)P^{-n}$$
$$= \frac{1}{(1-p^{-s})(1-p^{1-s})(1-p^{2-s})} - \frac{p^7\,p^{-2s}}{(p-1)(p^2-1)(1-p^{2-s})} +$$
$$\frac{p^2\,p^{-2s}}{p-1}\left(\frac{p+1}{(1-p^{1-s})^2(1+p^{1-s})} + \frac{p^{1-s}(p^2-p-1)-1}{(p^2-1)(1-p^{2-2s})} + \frac{p^{-s}+1}{(p-1)(1-p^{1-2s})}\right).$$

The proof of (3.12) is based on another result of Ilani [Il2] who studied the connection between subgroups of G and sub-Lie-algebras of G - when G is a uniform pro-p group. Recall (cf. [DDMS, Chapter 4]) that on such a G, a $\mathbb{Z}_p$-Lie algebra structure is defined.

Theorem 3.13. (Ilani [Il2]) *If G is a uniform pro-p group of dimension d and $p \geq d$, then every (closed) subgroup of G is a $\mathbb{Z}_p$-sub-Lie algebra and every $\mathbb{Z}_p$-sub-Lie algebra is a (closed) subgroup.*

So, by (3.13), the problem of calculating $a_{p^n}(G)$ is equivalent to calculating the number of subalgebras of a $\mathbb{Z}_p$-Lie algebra. The latter is a much easier task as was shown in [GSS]. In fact the method of "good bases" as presented in Section 2, for abelian and nilpotent groups can be adapted for Lie algebras. This can give a much easier proof for du Sautoy's Theorem (3.11), but only when $p \geq \dim(G)$. Anyway, (3.13) is useful for proving (3.12). The $\mathbb{Z}_p$-Lie algebra corresponding to $G = \mathrm{Ker}(SL_2(\mathbb{Z}_p) \to SL_2(\mathbb{F}_p))$ is $sl_2(\mathbb{Z}_p)$. The calculation, however, needed for $sl_2(\mathbb{Z}_p)$ is not that easy and Ilani used a computer to work it out. He also gave a computer-free proof of (3.12) by explicitly analyzing the subalgebras of $sl_2(\mathbb{Z}_p/p^r\mathbb{Z}_p)$, making an essential use of the fact that $sl_2(\mathbb{Z}_p)$ is of a very small dimension, i.e., three. Neither of his methods seems to suggest how to tackle the following interesting problem:

Problem 3.14. Let $G = \mathrm{Ker}(SL_n(\mathbb{Z}_p) \to SL_n(\mathbb{F}_p))$. Calculate $\zeta_G(s)$. More generally, if $\underline{G}$ is a Chevalley group scheme and $G = \mathrm{Ker}(\underline{G}(\mathbb{Z}_p) \to \underline{G}(\mathbb{F}_p))$, calculate $\zeta_G(s)$. It is natural to expect that $\zeta_G(s)$ can be expressed using invariants derived from the root system of $\underline{G}$.

Theorem (3.13) enables one to translate the problem into a problem on the Lie algebra $sl_n(\mathbb{Z}_p)$– at least if p is large enough.

4. Groups of polynomial subgroup growth

A group Γ is said to have *polynomial subgroup growth* (a PSG-group) if there exists c such that $a_n(\Gamma) \leq n^c$ for every $n \in \mathbb{N}$, or equivalently $\sigma_n(\Gamma) \leq n^{c+1}$ where $\sigma_n(\Gamma) = \sum_{i=1}^{n} a_n(\Gamma)$. Denote $\alpha(\Gamma) = \limsup_{n\to\infty} \frac{\log \sigma_n(G)}{\log n}$.

Theorem 4.1. (Lubotzky-Mann-Segal [LMS], [MS], [LM3], [Se]) *Let Γ be a finitely generated residually finite group. Then Γ has polynomial subgroup growth if and only if Γ is virtually solvable of finite rank.*

Recall that a group is virtually solvable if it contains a solvable subgroup of finite index. It is of finite rank if every finitely generated subgroup is generated by a bounded number of generators.

Theorem 4.1 joins a number of theorems which have been proven in recent years showing that some finiteness properties of infinite residually finite groups implies finiteness or virtual solvability. It deserves a notice that various old conjectures which turned out to be false for general groups are true for residually finite groups. The most famous example is the Burnside problem: A finitely generated group of finite exponent can be infinite as was shown by Adian and Novikov, but the recent solution of the restricted Burnside problem by Zel'manov says that a residually finite finitely generated group of finite exponent is finite.

Similarly, the examples of simple infinite groups whose proper subgroup are all cyclic, constructed by Ol'sanski and Rips show that finitely generated groups of finite rank need not be solvable. The story with residually finite groups is however different. Before stating the theorem, let us recall that a group Γ is said to have upper rank $\leq r$ if the rank of every finite quotient of it is at most r or equivalently the rank of $\hat{\Gamma}$ as a pro-finite group is at most r.

Theorem 4.2. *Let Γ be a finitely generated residually finite group. Then the following three conditions are equivalent:*

(1) Γ is of finite rank.

(2) Γ is of finite upper rank.

(3) Γ is virtually solvable of finite rank.

The equivalence of (1) and (3) is due to Lubotzky and Mann [LM2] and the equivalence of (1) and (3) was proved by Mann and Segal [MS] and independently by Wilson.

The proof of Theorem 4.1 is quite involved and uses diverse methods. As it has already received various expositions in the literature (cf. [Man1], [DDMS], and [LMS]), we will be very brief here:

The easier direction is the one saying that solvable groups of finite rank are PSG (see [Se] and [Lu6]). For the other direction: assume first that Γ is a subgroup of $\mathrm{GL}_d(\mathbb{Q})$ for some d. It is therefore, as Γ is finitely generated, a subgroup of $\Delta = G(\mathbb{Z}[\frac{1}{p_1}, \ldots, \frac{1}{p_l}])$ where G is some $\mathbb{Q}$-subgroup of GL_d and $S = \{p_1, \ldots, p_l\}$ is a finite set of primes and Γ is Zariski closed in G. As our goal is to prove that Γ is virtually solvable, one can even reduce to the case where G is connected, semi-simple, and simply connected (see [LM3]). Now, the strong approximation theorem for linear groups ([No], [MVW], or [We]) can be applied to conclude that the closure of Γ in the congruence topology of Δ is a finite index subgroup Δ_0 of Δ. It implies that for every n, $\sigma_n(\Gamma) \geq \gamma_n(\Gamma)$, where $\sigma_n(\Gamma) = \sum_{i=1}^{n} a_n(\Gamma)$ and $\gamma_n(\Delta_0)$ is the number of *congruence* subgroups of index at most n in Δ_0. Using the Prime Number Theorem, one can estimate $\gamma_n(\Delta)$ to show that it does not grow polynomially and hence Γ is virtually solvable.

The case of a general linear group over $\mathbb{C}$ is carried out by showing (using results of Jordan, Wehrfritz, and Platonov) that a non-virtually-solvable finitely generated linear group over $\mathbb{C}$ has a representation over $\mathbb{Q}$ whose image is not virtually solvable.

The case of residually-p groups is handled as follows: The pro-p completion $\Gamma_{\hat{p}}$ of Γ is also PSG and hence by Theorem 3.6 above, it is p-adic analytic hence linear over $\mathbb{Q}_l$ and so Γ is linear over $\mathbb{Q}_p$ and over $\mathbb{C}$ as well. Note that by handling the residually-p case we also cover linear groups in positive characteristic. In fact with slightly more care about the counting of congruence subgroups (see Section 5) we have also just proven Theorem 3.9 (which is actually valid for all residually-p groups).

To finish the proof of Theorem 4.1 for general Γ, one analyzes, using the classification of finite simple groups, the possible composition factors of finite quotients of Γ. This (with the aid of the linear case) reduces the proof to the case where every finite quotient of Γ is solvable, i.e., $\hat{\Gamma}$ is pro-solvable PSG group. Such a group is shown to have finite rank, which means that Γ has finite upper rank. We can now apply Theorem 4.2 (whose proof is described in detail in [DDMS]) to finish the proof of 4.1.

It should be emphasized that Theorem 4.1 is valid only for finitely generated groups. There are PSG-countable groups (even linear!) which are not virtually solvable. For example, let $\Gamma = SL_n(D)$, where $D = \mathbb{Q} \cap \hat{\mathbb{Z}}_p$. From the congruence subgroup property, one deduces that $\hat{\Gamma} = SL_n(\hat{\mathbb{Z}}_p)$ which is a p-adic analytic group. Thus, $\hat{\Gamma}$ and Γ are PSG-groups. No characterization of non-finitely generated PSG-groups is known. It is also not known exactly when a general pro-finite group is PSG. Here are the two main results in this direction:

Theorem 4.3. (Mann-Segal [MS], [Man2]) *A pro-solvable group G is PSG if and only if it is of finite rank.*

Theorem 4.4. *Let G be a pro-finite group of polynomial subgroup growth. Then: G has normal subgroups $K \leq H \leq G$ such that*

(i) $(G : H) < \infty$.

(ii) *H/K is a (finite or an infinite) product of finite simple groups $\prod_{i \in I} F_i$ such that each F_i is a simple group of Lie type of the form $L_{n_i}(p_i^{r_i})$ where n_i (= the Lie-rank of F_i) and r_i are bounded.*

(iii) *K is a pro-solvable group.*

Theorem 4.4 is based on [MS] and an argument of Shalev. We finally mention another result of Mann on PSG-pro-finite groups:

Proposition 4.5. *A PSG-pro-finite group G is finitely generated (as a pro-finite group).*

PROOF. Assume $a_n(G) = O(n^r)$ and let k be a positive integer. $G^k = G\times\cdots\times G$ is endowed with a Haar measure μ. A k-tuple $\alpha = (a_1, \ldots, a_k) \in G^k$ does not generate G if and only if it is in some proper open subgroup. This shows that

$$\mu(\{\alpha \in G^k | a_1, \ldots, a_k \text{ do not generate } G\}) \leq \sum_{1<[G:H]<\infty} \frac{1}{|H|^k} = \sum_{n=2}^{\infty} \frac{a_n(G)}{n^k}.$$

Now, since G is PSG, for some k, the left hand sum is strictly less than 1 and so with a positive probability, k elements generate G, and in particular, G is finitely generated. □

Moreover, in [KL] it was shown that for $G = \hat{\mathbb{Z}}^r$ (but in fact the argument is valid for every PSG-group) we have:

(*) *There exists an integer k such that with probability 1, some k-tuple of elements of G generate an open subgroup of G.*

In particular, this applies for p-adic analytic pro-p groups. This made Mann and Lubotzky ask:

Problem 4.6. Assume G is a pro-p group satisfying (*). Is G p-adic analytic?

A positive answer will give a nice probabilistic characterization of analytic pro-p groups.

Mann ([Man3]) called a pro-finite group G for which there exists k with $\mu(\{\alpha \in G^k | \alpha \text{ generates } G\}) > 0$, *positively finitely generated* (PFG for short). So PSG is PFG. He also observes that in the proof of 4.5, it suffices to know that $m_n(G)$ grows polynomially, where $m_n(G)$ is the number of maximal subgroups of index n. He went ahead to show that for every pro-solvable group, $m_n(G)$ grows polynomially, and hence,

Theorem 4.7. ([Man3]) *A finitely generated pro-solvable group is positively finitely generated.*

Mann and Shalev [MaSh] showed an equivalence:

Theorem 4.8. *A finitely generated pro-finite group G is positively finitely generated if and only if $m_n(G)$ grows polynomially.*

We will close this section with a few more results and questions about the precise rate of growth of $a_n(G)$ for a PSG group.

It is actually more convenient to talk about $\sigma_n(G) = \sum_{i=1}^{n} a_i(G)$. Let $\alpha(G) = \limsup \frac{\log \sigma_n(G)}{\log n}$. Clearly $\alpha(G) < \infty$ if and only if $a_n(G)$ and $\sigma_n(G)$

grows (at most) polynomially– in which case we say G has polynomial subgroup growth and $\alpha(G)$ is the smallest real number α such that $\sigma_n(G) = 0(n^{\alpha+\epsilon})$ for every $\epsilon > 0$.

If $\zeta_G(s) = \Sigma a_n(G)n^{-s}$ then $\alpha(G)$ can be read of $\zeta_G(s)$; by the Tauberian theorem, $\zeta_G(s)$ may be extended analytically to the half space $Re(s) \geq \alpha(G)$ except for a pole at $s = \alpha(G)$. (If this is a simple pole then in fact $\sigma_n(G) = O(n^\alpha)$, but if it is, say, a double pole then we can only deduce $\sigma_n(G) = O(n^\alpha \log n)$). Anyway, when $\zeta_G(s)$ is explicitly known or in those cases in which it was proved to be rational we can derive some conclusions on $\alpha(G)$ and hence on the rate of growth of $\sigma_n(G)$.

For example, let G be a p-adic analytic pro-p group. By du Sautoy's theorem $\zeta_G(s)$ is a rational function of p^{-s} with rational coefficients. Actually, his result is more precise: it also says that the denominator of $\zeta_G(s)$ is of the form $\Pi_{i=1}^{l}(1 - p^{-a_i s - b_i})$ for some $l \in \mathbb{N} \cup \{0\}$, and $a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{Z}$. This shows that for real s the denominator is zero only for $s = -b_i/a_i$, $i = 1, \ldots, l$. In particular we deduce:

Proposition 4.9. (du Sautoy [dS3]) *Let G be a p-adic analytic pro-p group. Then $\alpha(G) = \limsup \frac{\log \sigma_n(G)}{\log n}$ is rational.*

The analogous result for nilpotent groups is not known, but it is quite likely to hold:

Conjecture 4.10. Let Γ be a nilpotent group then $\alpha(\Gamma)$ is rational.

It is not difficult to find examples which show that $\alpha(G)$ can be rational and not necessarily integer. For example, Theorem 2.9 shows that if $G = \Gamma_{\hat{p}}$ is the pro-p completion of the Heizenberg group then $\zeta_G(s) = \frac{\zeta_p(s)\zeta_p(s-1)\zeta_p(2s-2)\zeta_p(2s-3)}{\zeta_p(3s-3)}$, i.e., $\zeta_G(s)$ has poles for $s = 0, 1$ and $\frac{3}{2}$ (with a double pole for $s = 1$). Anyway $\alpha(G) = \frac{3}{2}$. The same remark applies for $\alpha(\Gamma)$ when Γ is the discrete Heizenberg group. In this sense subgroup growth is different from the classical word growth $b_n(\Gamma)$. Recall that $b_n(\Gamma)$ is defined as the number of elements of Γ of length at most n with respect to a fixed finite set of generators Σ. Denote $\beta(\Gamma) = \limsup \frac{\log b_n(\Gamma)}{\log n}$. It is easy to see that $\beta(\Gamma)$ depends only on Γ and not on Σ, and that if Γ is nilpotent then $\beta(\Gamma) < \infty$. In [Ba], Bass gave a formula for $\beta(\Gamma)$, from which one sees that $\beta(\Gamma)$ is always an integer. Moreover there are two constant $0 \leq C_1, C_2 \in \mathbb{R}$ such that for every n, $C_1 n^{\beta(\Gamma)} \leq b_n(\Gamma) \leq C_2 n^{\beta(\Gamma)}$. It is not known if an analogue of this later result holds for $\sigma_n(\Gamma)$, when Γ is a nilpotent group and $\beta(\Gamma)$ is replaced by $\alpha(\Gamma)$. This is not the case for uniform pro-p groups: The computation of Ilani (3.12), shows that for $G = \mathrm{Ker}(SL_2(\mathbb{Z}_p) \to SL_2(\mathbb{F}_p))$, $a_n(G)$ grows like $n \log n$ and so $\sigma_n(\Gamma)$ grows as $n^2 \log n$, so $\sigma_n(G) = O(n^{2+e})$ for every $e > 0$ but not $O(n^2)$.

Anyway, it will be very interesting to answer the following:

Problem 4.11. For a finitely generated nilpotent group and for a uniform pro-p group G, give a formula for $\alpha(G)$.

Another remark is in order here: When Γ is a finitely generated torsion free nilpotent group and H is a finite index subgroup of Γ. Then it is shown in [GSS], that $\alpha(G) = \alpha(H)$. This is not always the case for groups of polynomial subgroup growth. It was observed in [LM3] that if Γ is the infinite dihedral group then $\alpha(\Gamma) = 2$ while for the infinite cyclic group H, which is an index two subgroup in Γ, $\alpha(H) = 1$. This is again inconsistent with word growth: there $\beta(\Gamma) = \beta(H)$ whenever H is a finite index subgroup of Γ. The study of $\alpha(H)$ when H varies over finite index subgroups of a PSG group deserves some more attention.

5. Counting congruence subgroups

This section is devoted to the growth of the number of congruence subgroups in an arithmetic group. Beside its intrinsic interest as a "non-commutative analytic number theory", these examples have produced the first examples of groups of intermediate subgroup growth– i.e., growth which is greater than polynomial and smaller than exponential. (More examples at the higher end of the intermediate growth range were given recently by Dan Segal and Aner Shalev [SS].)

We shall also relate the subgroup growth of arithmetic groups with the congruence subgroup property, showing that the latter can be characterized by means of subgroup growth. This enables one to formulate a "congruence subgroup problem" for groups which do not have an arithmetic structure. In particular, it suggests the study of the subgroup growth of fundamental groups of hyperbolic manifolds. We will present some (very) partial results in this direction.

Let us start with counting the congruence subgroups: It turns out that there is a fundamental difference between arithmetic groups over global fields in characteristic zero and those of positive characteristic. They are different in the results as well as in the methods of proof. We will therefore handle them separately. The notations however will be presented simultaneously.

Let K be either $\mathbb{Q}$– the field of rational numbers or $\mathbb{F}_p(x)$– the field of rational functions over the finite field of order p. Let O be the ring of integers of K, i.e., $O = \mathbb{Z}$ or $\mathbb{F}_p[x]$. Let G be a simple, simply connected, connected algebraic group defined over K. For the simplicity of the exposition we will also assume that G splits over K. (The interested reader is referred to [Lu4] for the general case including S-arithmetic groups etc. Most readers will find it useful to assume $G = SL_r$. All essential ideas appear already in this case.) So G can be thought of as a Chevalley group (defined over $\mathbb{Z}$) and we fix an embedding of G into GL_r. Let $\Gamma = G(O)$ (e.g., $\Gamma = SL_r(\mathbb{Z})$ or $\Gamma = SL_r(\mathbb{F}_p[t])$).

For an ideal $I \neq \{0\}$ of O we denote $\Gamma(I) = \mathrm{Ker}(G(O) \to G(O/I))$. As O/I is finite, $\Gamma(I)$ is always a finite index normal subgroup– called a principal congruence subgroup. A subgroup Δ of Γ is called a congruence subgroup if it contains $\Gamma(I)$ for some $I \neq \{0\}$.

Let $\gamma_n(\Gamma)$ denote the number of congruence subgroups of Γ of index *at most* n.

Theorem 5.1. (Lubotzky [Lu4]) *Assume* $char(K) = 0$. *Then there exist positive constants* C_1 *and* C_2 *such that*

$$n^{C_1 \log n/\log\log n} \leq \gamma_n(\Gamma) \leq n^{C_2 \log n/\log\log n}.$$

Theorem 5.2. (Lubotzky [Lu4]) *Assume* $char(K) = p > 0$. *Then there exists positive constants* C_3 *and* C_4 *such that*

$$n^{C_3 \log n} \leq \gamma_n(\Gamma) \leq n^{C_4(\log n)^2}$$

The theorems show that in case all finite index subgroups of Γ are congruence subgroups, Γ has intermediate subgroup growth. This is known to be the case for $\Gamma = SL_r(O)$ when $r \geq 3$ (cf. [Rp], [Ra] and the references therein). Hence:

Corollary 5.3.

(a) If $\Gamma = SL_r(\mathbb{Z})$, $r \geq 3$, *then* $n^{C_1 \log n/\log\log n} \leq \sigma_n(\Gamma) \leq n^{C_2 \log n/\log\log n}$.

(b) If $\Gamma = SL_r(\mathbb{F}_p[t])$, $r \geq 3$, *then* $n^{C_3 \log n} \leq \sigma_n(\Gamma) \leq n^{C_4(\log n)^2}$.

Here C_1, C_2, C_3 *and* C_4 *are some positive constants, and* $\sigma_n(\Gamma)$ *is the number of subgroups of* Γ *of index at most* n.

In fact the proof can be used to get some explicit estimate on these constants. For example for $\Gamma = SL_2(\mathbb{Z})$ we can take in Theorem 5.1, $C_1 = \frac{1}{144}$ and $C_2 = 18$.

We now sketch the proofs of Theorem 5.1 and 5.2. In order to visualize better the difference between the zero and positive characteristic we will give first the proofs for the lower bounds:

Proof of lower bound of (5.1)

By the strong approximation theorem (see [Pr]– but think on SL_r), $\Gamma = G(\mathbb{Z})$ is mapped onto $G(\mathbb{Z}/M\mathbb{Z})$ for every $M \in \mathbb{Z}$. If $M = p_1^{\alpha_1} \cdot \ldots \cdot p_l^{\alpha_s}$ where p_i, $i = 1, \ldots, t$, are different primes, then by the Chinese Remainder Theorem $G(\mathbb{Z}/M\mathbb{Z}) = \Pi_{i=1}^{t} G(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$. For every prime p, $G(\mathbb{F}_p)$ has a cyclic subgroup of order $p-1$ (coming from the torus isomorphic to $(\mathbb{F}_p^*)^{\mathrm{rank}(G)}$ since G splits; but also in general a theorem of Lang ensures that over a finite field,

there is at least a one dimensional torus). Thus if $M = p_1 \cdot \ldots \cdot p_t$ a product of different primes chosen so that for $i = 1, \ldots, t$, $p_i \equiv 1 (\bmod m)$ for some number m, then $G(\mathbb{Z}/M\mathbb{Z})$ contains a subgroup isomorphic to $(\mathbb{Z}/m\mathbb{Z})^t$. Now if m itself is a product of distinct primes, say, $m = q_1 \cdot \ldots \cdot q_s$ then $(\mathbb{Z}/m\mathbb{Z})^t \simeq \Pi_{i=1}^s (\mathbb{Z}/q_i\mathbb{Z})^t$ contains at least $\Pi_{i=1}^s q_i^{t^2/4} = m^{t^2/4}$ subgroups. As the order of $G(\mathbb{Z}/M\mathbb{Z})$ is at most M^d with $d = \dim G$, we get $m^{t^2/4}$ subgroups of Γ of index $\leq M^{\dim G}$. We show now how the primes p_i and q_j can be chosen to ensure that $\gamma_n \geq n^{C \log n / \log \log n}$ for some constant C:

Denote $\gamma =$ Euler constant $= 0.57721\ldots$ and $\gamma' = e^{-\gamma}$. Let $N = n^{\gamma'/d}$ where $d = \dim(G)$, $\tau = \log(N)$ and $\beta = \log(\tau) = \log\log(N)$. Let $q_1, \ldots, q_s$ be the list of primes smaller than β and $m = \Pi_{j=1}^s q_j$. By the prime number theorem $m \approx e^\beta = \tau$ and by [El, Ex. 1.20, p. 31], $\frac{m}{\varphi(m)} \approx \frac{\log\beta}{\gamma'} = \frac{\log\log\tau}{\gamma'}$. Let $\Pi = \Pi(m\tau/\log\log\tau; m, 1)$ be the set of the t primes less than $m\tau/\log\log\tau$ and congruent to 1 mod m. From the prime number theorem along arithmetic progressions (cf. [El, Theorem 8.8, p. 277]) it follows that

$$t = \frac{m\tau}{\varphi(m)(\log\log\tau)\log(m\tau/\log\log\tau)} \approx \frac{1}{2\gamma'} \cdot \frac{\tau}{\log\tau}$$

(where here and always $f \approx g$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$). The same theorem says also that the product M of these t primes satisfies:

$$\log M \approx m/\varphi(m) \cdot \frac{\tau}{\log\log\tau} \approx \frac{\log N}{\gamma'}.$$

The discussion above shows that between Γ and $\Gamma(M)$ there are at least $m^{t^2/4}$ subgroups whose index is at most M^d which is approximately $N^{d/\gamma'} = n$. Thus $\gamma_n \geq m^{t^2/4}$, so $\log\gamma_n \underset{\approx}{>} \frac{t^2}{4}\log m \approx \frac{1}{16\gamma'^2}\frac{\tau^2}{\log\tau}$. As $\tau = \frac{\gamma'}{d}\log n$ we deduce that $\log\gamma_n \underset{\approx}{>} \frac{1}{16d^2}\frac{(\log n)^2}{\log\log n}$. This proves the lower bound with $C_1 = \frac{1}{16d^2}$. □

Proof of lower bound of (5.2)

The group $\Gamma = G(\mathbb{F}_p[t])$ is dense in the pro-finite group $H = G(\mathbb{F}_p[[t]])$, where $\mathbb{F}_p[[t]]$ denotes the ring of formal power series over $\mathbb{F}_p$. The group H is virtually pro-p. In fact, it is not difficult to see (cf. [LS]) that $H(1) = \mathrm{Ker}(G(\mathbb{F}_p[[t]] \to G(\mathbb{F}_p))$ is a pro-p group. $H(1)$ has analytic structure over $\mathbb{F}_p[[t]]$, but it is not p-adic analytic group. For example, it has an infinite torsion subgroup while p-adic analytic pro-p group cannot have such a subgroup (cf. [DDMS]. See also [LS] for a more general statement). Thus by Shalev's theorem (3.6), $\sigma_n(H(1))$ and so also $\sigma_n(H)$ grows at least as $n^{C\log n}$ for a suitable constant C. The same applies also for Γ, which proves our claim. □

Proof of the upper bound of (5.1)

A crucial ingredient in the proof of the upper bound is the following:

Proposition 5.4. ("level ≤ index") *Let $\Gamma = G(\mathbb{Z})$ be as in 5.1 and H a congruence subgroup of Γ. Then $H \supseteq \Gamma(m)$ for some $m \leq [\Gamma : H]$.*

Corollary 5.5. *Let $\Gamma = G(\mathbb{Z})$ be as in (5.1). Then*

$$\gamma_n(\Gamma) \leq \sum_{m=1}^{n} \|G(\mathbb{Z}/m\mathbb{Z})\|,$$

where for a finite group F we denote by $\|F\|$ the total number of its subgroups.

The problem is therefore transformed now to a problem on finite groups. In the following proposition we collect some useful easy results:

Proposition 5.6. *Let F be a finite group. Then:*

(i) $rank(F) \leq \log_2 |F|$.

(ii) $\|F\| \leq |F|^{rank(F)}$.

Proposition 5.7. *There exists a constant $C = C(G)$ such that $rank(G(\mathbb{F}_p))$ is bounded by C.*

PROOF. By a result of Aschbacher and Guralnick ([AG]) every finite group is generated by a solvable subgroup plus one element. It suffices therefore to bound the number of generators of solvable subgroups of $G(\mathbb{F}_p)$. Let M be a solvable subgroup of $G(\mathbb{F}_p)$. So $M = PQ$ where P is a p-sylow subgroup of M and Q is of order prime to p. As $G \hookrightarrow GL_r$, the order of P is bounded by p^{r^2} and so $d(P) \leq r^2$. Now Q, being of order prime to p, can be lifted to $GL_r(\mathbb{C})$. (This is a classical result. Here is a less classical proof: $Q \leq GL_r(\mathbb{F}_p)$. Look at the preimage R of Q in $GL_r(\mathbb{Z}_p)$. It has a normal pro-p subgroup $N = \mathrm{Ker}(GL_r(\mathbb{Z}_p) \to GL_r(\mathbb{F}_p))$ and $R/N = Q$ is of order prime to p. So by the Schur-Zassenhaus theorem, R is a semi-direct product of N and Q' where Q' is a subgroup of R isomorphic to Q. Thus Q is isomorphic to a subgroup of $GL_r(\mathbb{Z}_p)$ and of $GL_r(\mathbb{C})$). By a classical theorem of Jordan, Q has an abelian subgroup A of bounded index. A is diagonalizable and so $d(A) \leq r$. Altogether $d(Q)$ is bounded as a function of r and so is $d(M)$ and $\mathrm{rank}(G(\mathbb{F}_p))$. □

Corollary 5.8. $\mathrm{rank}(G(\mathbb{Z}/p^\alpha\mathbb{Z}))$ *is bounded independent of p and α.*

PROOF. As all $G(\mathbb{Z}/p^\alpha\mathbb{Z})$ are images of $G(\mathbb{Z}_p)$, it suffices to prove that $G(\mathbb{Z}_p)$ or $GL_r(\mathbb{Z}_p)$ is of bounded rank (depending on r but not on p). Now, by [DDMS, Chapter 5], $N = \mathrm{Ker}(GL_r(\mathbb{Z}_p) \to GL_r(\mathbb{F}_p))$ is a uniform pro-p group of rank r^2. This with (5.7) proves (5.8). □

Now we can complete the proof of the upper bound of (5.1): For $m \in \mathbb{Z}$, write $m = p_1^{\alpha_1} \cdot \ldots \cdot p_l^{\alpha_l}$ where p_i, $i = 1 \ldots, l$ are the distinct prime divisors of m. By the prime number theorem $l \leq \frac{\log m}{\log \log m}$ and so by (5.8):

$$\begin{aligned} \mathrm{rank}\,(G(\mathbb{Z}/m\mathbb{Z})) &= \mathrm{rank}\left(\prod_{i=1}^{l} G(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})\right) \\ &\leq \sum_{i=1}^{l} \mathrm{rank}\,(G(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})) = O\left(\frac{\log m}{\log \log m}\right). \end{aligned}$$

(5.6 ii) now implies that $\|G(\mathbb{Z}/m\mathbb{Z})\| \leq m^{C\frac{\log m}{\log \log m}}$. This finishes the proof in light of (5.5). □

Remark 5.9. We used along the way the result of Ashbacher and Guralnick ([AG]) which requires the classification of finite simple groups. But, as was noticed by L. Pyber, this can be avoided (see [Lu4]).

Proof of upper bound of (5.2)

Proposition 5.10. *Let $\Gamma = G(\mathbb{F}_p[t])$ be as in (5.2). Then there exists a constant C such that any congruence subgroup of Γ of index n contains a* subnormal *congruence subgroup of index at most n^C.*

The proof is based on Babai-Cameron-Palfy theorem [BCP].

Proposition 5.11. *Every subnormal congruence subgroup of $\Gamma = G(\mathbb{F}_p[t])$ of index n contains a principal congruence subgroup of index at most $n^{C' \log n}$ for some constant C'.*

Proposition 5.12. (L. Pyber [Py2]) *If F is a finite group, then $a_n(F) \leq |F|^{2\log n}$.*

The last three propositions imply the upper bound of (5.2). □

We turn now back to assume $\mathrm{char}(K) = 0$ so $\Gamma = G(\mathbb{Z})$. The congruence subgroups of Γ form a basis of neighborhoods of the identity of Γ and thus define a topology on Γ– called the congruence topology. The completion of Γ wth respect to this topology is $G(\hat{\mathbb{Z}})$, by the strong approximation theorem. In general the congruence topology is weaker than the pro-finite topology and so

the homomorphism $\pi : \hat{\Gamma} = \widehat{G(\mathbb{Z})} \to G(\hat{\mathbb{Z}})$ induced by the indentity map from Γ to Γ is an epimorphism but not a monomorphism. It is a monomorphism if and only if every finite index subgroup of Γ is a congruence subgroup. The original congruence subgroup problem asks whether this is the case, but it turns out that all the important applications of it need only that $\mathrm{Ker}(\pi)$ is finite. So following the ususal tradition we say that Γ has the *congruence subgroup property* (CSP for short) if $\mathrm{Ker}(\pi)$ is finite. It is not difficult to see that in this case $\sigma_n(\Gamma)$ has the same type of growth as $\gamma_n(\Gamma)$. The next result, from Lubotzky [Lu4], actually shows that CSP can be characterized by the property that $\sigma_n(\Gamma)$ has the same type of growth as $\gamma_n(\Gamma)$. The result is even stronger:

Theorem 5.13. *Let $\Gamma = G(\mathbb{Z})$ as in (5.1). Then Γ has the congruence subgroup property if and only if for every $\varepsilon > 0$ there exists a constant C_ε such that $\sigma_n(\Gamma) \leq C_\varepsilon n^{\varepsilon \log n}$ for every n.*

Theorem 5.13 is maybe even more interesting when expressed in the negative form: If Γ does not have CSP then for some $\varepsilon > 0$, $\sigma_n(\Gamma) \geq n^{\varepsilon \log n}$ for infinitely many n's, i.e., the subgroup rate of growth of Γ is strictly bigger than the rate of growth of the congruence subgroups.

Another interesting aspect of Theorem 5.13 is that it gives a purely group theoretical characterization to CSP, which is an arithmetic property. In particular, we can now formulate a congruence subgroup problem for groups without an arithmetic structure. This is especially interesting for non-arithmetic lattices in the simple Lie groups of rank one $SO(n,1)$ and $SU(n,1)$ in which non-arithmetic lattices are known to exist (for every n in the first family and for $n = 2$ and 3 in the second). It is very natural to conjecture (and it is compatible with Serre's conjecture on CSP– see [Sr]) that all lattices in $SO(n,1)$ and $SO(U,1)$ have subgroup growth at least $n^{C \log n}$. We actually believe that they even have exponential or super-exponential subgroup growth. At this point, however, only a very partial result is known:

Proposition 5.14.

(i) Let $H = SO(2,1) \approx PSL_2(\mathbb{R})$ and Γ a lattice (= a discrete subgroup of finite covolume) in H. Then Γ has a super-exponential growth.

(ii) Let $H = SO(3,1) \approx PSL_2(\mathbb{C})$ and Γ a lattice in H. Then $\sigma_n(\Gamma) \geq n^{C \log n}$ for some constant C.

PROOF. (i) The structure of lattices in $PSL_2(\mathbb{R})$ is well known: Γ either has a free non-abelian subgroup of finite index or it contains a finite index surface group of genus $g \geq 2$. Such a surface group is mapped epimorphically onto a free group on g generators. Thus in either case the subgroup growth of Γ is like that of a free group, i.e., super-exponential by (1.6).

(ii) Γ being a lattice in $SO(3,1)$ has a torsion free subgroup Δ which is a fundamental group of a 3-manifold. A 3-manifold group always has a presentation with no more relations than generators (see [Lu1] for details). By choosing Δ in a suitable way we can arrange that for $p = 2$ the pro-p complion $\Delta_{\hat{p}}$ of Δ, satisfies $d(\Delta_{\hat{p}}) = d \geq 5$ and it has a presentation (as a pro-p group) with r relation where $r \leq d$. Thus $r < \frac{d^2}{4}$, i.e., $\Delta_{\hat{p}}$ does not satisfy the Golod-Shafarevitz inequality. This implies ([Lu1, Theorem 1], [DDMS]) that $\Delta_{\hat{p}}$ is not p-adic analytic. Thus by (3.6), $\sigma_n(\Delta_{\hat{p}})$ grows at least at $n^{C \log n}$ and by (2.2) the same applies for Δ and hence for Γ. □

Experience with lattices in semi-simple groups show that discrete groups with Kazdhan property (T) tend to have the CSP. We end this chapter with a conjecture:

Conjecture 5.15. Let Γ be a discrete group with Kazdhan property (T). Then $\sigma_n(\Gamma)$ grows at most exponentially (one can even aspire to more ambitious bounds).

Recall that Γ has property (T) if the trivial representation of Γ is an isolated point in the dual space of the irreducible unitary representations of Γ. Though not apparent from the definition, one can show that property (T) puts severe restrictions on the finite quotients of Γ (cf. [Lu5]) so it is not unrealistic to expect some control on the subgroup growth.

A discrete group is called amenable if $L^\infty(\Gamma)$ carries an invariant mean. Amenable groups are very different from groups with property (T). Still we wonder whether for a finitely generated amenable group Γ, $\sigma_n(\Gamma)$ grows at most exponentially. Solvable groups are amenable and for solvable groups, Mann [Man3] indeed showed that their subgroup growth is at most exponential. (Note however that for some solvable groups it is exponential.)

References

[AG] M. Aschbacher, R. Guralnik, Solvable generation of groups and Sylow subgroups of the lower central series, *J. Algebra* **77**(1982), 189–201.

[BCP] L. Babai, P.J. Cameron and P.P. Palfy , On the orders of primitive groups with restricted non-abelian composition factors , *J. Algebra* **79**(1982), 161–168.

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

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

[BR1] C.J. Bushnell and I. Reiner, Solomon's conjectures and the local functional equation for zeta functions of orders, *Bull. Amer. Math. Soc.* **2**(1980), 306–310.

[BR2] C.J. Bushnell and I. Reiner, Zeta function of arithmetic orders and Solomon's conjecture, *Math. Z.* **173**(1980), 135–161.

[De1] J. Denef, The rationality of the Poincaré series associated to the p-adic points on a variety, *Invent. Math.* **77**(1984), 1–22.

[De2] J. Denef, On the degree of Igusa's local zeta function, *Amer. J. Math.* **109**(1987), 991–1008.

[DvdD] J. Denef, L. van den Dries, p-adic and real subanalytic sets, *Ann. Math.* **128**(1988), 79–138.

[De1] I.M.S. Dey, *Schreier systems in free products*, Ph.D. Thesis, Manchester, 1963.

[De2] I.M.S. Dey, Schreier systems is free products, *Proc. Glasgow Math. Soc.* **7**(1965), 61–79.

[Di] J.D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110**(1969), 199–205.

[DDMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic Pro-p Groups* (LMS Lecture Notes Series **157**, Cambridge Univ. Press, 1991).

[DM] A. Dress and Th. Müller, Logarithm of generating functions and combinatorial decomposition of functions, Universitüt Bielefeld, preprint.

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

[dS2] M.P.F. du Sautoy, Applications of p-adic methods to group theory, in *p-adic Methods and their Applications* (A. Baker and R. Plymen (eds.), Oxford Univ., to appear).

[dS3] M.P.F. du Sautoy, Finitely generated groups, p-adic analytic groups and Poincaré series, *Ann. Math.* **137**(1993), 639–670.

[dS4] M.P.F. du Sautoy, Zeta functions of groups and rings: uniformity, *Israel J. Math.* **86**(1994), 1–23.

[dS5] M.P.F. du Sautoy, Counting congruence subgroups in arithmetic subgroups, preprint.

[dS6] M.P.F. du Sautoy, Zeta functions on groups, preprint.

[dSL] M.P.F. du Sautoy and A. Lubotzky, Functional equations and uniformity for local zeta functions of nilpotent groups, in preparation.

[El] W. and F. Ellison, *Prime Numbers* (A. Wiley & Sons, 1985).

[FS] B. Fine and D. Spellman, Counting subgroups in the Hecke groups, *Internat. J. Algebra Comput.* **3**(1993), 43–49.

[GIR] C. Godsil, W. Imrich and R. Razen, On the number of subgroups of given index in the modular group, *Mh. Math.* **87**(1979), 273–280.

[GN1] M. Grady, M. Newman, Some divisibility properties of the subgroup counting function for free products, *Math. Comp.* **58**(1992), 347–353.

[GN2] M. Grady and M. Newman, Counting subgroups of given index in Hecke

groups, *Contemp. Math., Amer. Math. Soc.*, to appear.

[GN3] M. Grady and M. Newman, Residue periodicity in subgroup counting functions, preprint.

[Gri] R.I. Grigorchuck, On growth in group theory, in *Proc. of Inter. Congress of Math.* (Kyoto, Japan, 1990), 325–338.

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

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

[Ha1] M. Hall, Subgroups of finite index in free groups, *Canad. J. Math.* **1**(1949), 187–190.

[Ha2] M. Hall, *The Theory of Groups* (Macmillan, New York, 1959).

[Ha] P. Hall, *Nilpotent Groups* (Queen Mary College Math. Notes, 1969).

[Ig] J.I. Igusa, Universal p-adic zeta functions and their functional equations, *Amer. J. Math.* **111**(1989), 671–716.

[Il1] I. Ilani, Counting finite index subgroups and the P. Hall enumeration principle, *Israel J. Math.* **68**(1989), 18–26.

[Il2] I. Ilani Analytic pro-p groups and their Lie algebras, preprint.

[Il3] I. Ilani, Counting finite index subgroups in $SL_2(\mathbb{Z}_p)$, in preparation.

[Im] W. Imrich, On the number of subgroups of given index in $SL_2(\mathbb{Z})$, *Arch. Math.* **31**(1978), 224–231.

[Jo] G.A. Jones, Congruence and non-congruence subgroups of the modular group: a survey, (in *Proc. of Groups-St. Andrews 1985*, E.F. Robertson and C.M. Campbell (eds.), LMS Lecture Notes Series **121**, Cambridge Univ. Press, 1986), 223–234.

[KL] W.A. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36**(1990), 67–87.

[Lu1] A. Lubotzky, Group presentation, p-adic analytic groups and lattices in $SL_2(\mathbb{C})$, *Ann. Math.* **118**(1983), 115–130.

[Lu2] A. Lubotzky, Dimension functions for discrete groups, in *Proc. of Groups - St. Andrews 1985* (E.F. Robertson and C.M. Campbell (eds.), London Math. Soc. Lecture Notes **121**, Cambridge University Press 1986), 254–262.

[Lu3] A. Lubotzky, A group theoretic characterization of linear groups, *J. Algebra* **113**(1988), 207–214.

[Lu4] A. Lubotzky, Subgroup growth and congruence subgroups, preprint.

[Lu5] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures* (Progress in Math., Birkhauser Verlag), to appear.

[Lu6] A. Lubotzky, Subgroup Growth, Lecture notes for a series of talks in the Conference on Group Theory, Groups Galway/St Andrews 1993, August 1993.

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

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

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

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

[LS] A. Lubotzky and A. Shalev, On some Λ-analytic pro-p groups, *Israel J. Math.* **85**(1994), 307–337.

[M] I.G. Macdonald, *Symmetric Functions and Hall Polynomial* (Oxford Univ. Press, 1979).

[Ma1] A.J. Macintyre, On definable subsets of p-adic fields, *J. Symbolic Logic* **41**(1976), 605–610.

[Ma2] A.J. Macintyre, Rationality of p-adic Poincaré series: uniformity in p, *Ann. Pure. Appl. Logic* **49**(1990), 31–74.

[Man1] A. Mann, Some applications of powerful p-groups, in *Proc. of Groups - St. Andrews 1989* (C.M. Campbell and E.F. Robertson (eds.), LMS Lecture Notes Series **160**, Cambridge Univ. Press, 1991), 370–385.

[Man2] A. Mann, Some properties of polynomial subgroup growth groups, *Israel J. Math.* **82**(1993), 373–380.

[Man3] A. Mann, Positively finitely generated groups, preprint.

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

[MaSh] A. Mann and A. Shalev, Maximal subgroups of finite simple groups and positively finitely generated groups, preprint.

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

[Me1] A.D. Mednyh, Determination of the number of nonequivalent coverings over a compact Riemann surface, *Soviet Math. Dokl.* **19**(1978), 318–320.

[Me2] A.D. Mednyh, On unramified coverings of compact Riemann surfaces, *Soviet Math. Dokl.* **20**(1979), 85–88.

[Me3] A.D. Mednyh, On the solution of the Hurwitz problem on the number of nonequivalent coverings over a compact Riemann surface, *Soviet Math. Dokl.* **24** (1981), 541–545.

[Me4] A.D. Mednyh, Hurwitz problem on the number of nonequivalent coverings of a compact Riemann surface, *Sib. Math. J.* **23**(1982), 415–420.

[MP] A.D. Mednyh and G.G. Pozdnyakova, Number of nonequivalent coverings over a nonorientable compact surface, *Sib. J. Math.* **27**(1986), 99–106.

[Mi] J. Milnor, Growth of finitely generated solvable groups, *J. Diff. Geom.*

2(1968), 443–449.

[MW] L. Moser and M. Wyman, On solution of $X^d = 1$ in symmetric groups, *Canad. J. Math.* **7**(1955), 159–168.

[Mu1] T. Müller, *Kombinatorische Aspekte endlich erzeungter virtuell freier Gruppen*, Ph.D. Thesis, Universität Frankfurt am Main, 1989.

[Mu2] T. Müller, Combinatorial aspects of finitely generated virtually free groups (extended abstract), in *Proc. of Groups-St. Andrews 1989, vol. 2* (C.M. Campbell and E.F. Robertson (eds.), London Math. Soc. Lecture Notes **160**, Cambridge Univ. Press, 1990), 386–395.

[Mu3] T. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* **44**(1991), 75–94.

[Mu4] T. Müller, A group-theoretical generalization of Pascal's triangle, *European J. Combin.* **12**(1991), 43–49.

[Mu5] T. Müller, Finite group actions, subgroups of finite index in free products and asymptotic expansion of $e^{p(z)}$, preprint .

[Ne1] M. Newman, The number of subgroups of the classical modular group of index N (tables) (National Bureau of Standards, Washington D.C., 1976).

[Ne2] M. Newman, Asymptotic formulas related to free products of cyclic groups, *Math. Comp.* **30**(1976), 838–846.

[No] M. Nori, On subgroups of $GL_n(F_p)$, *Invent. Math.* **88**(1987), 257–275.

[Pr] G. Prasad, Strong approximation for semi-simple groups over function fields, *Ann. Math.* **105**(1977), 553–572.

[Py1] L. Pyber, Enumerating finite groups of given order, *Ann. Math.* **137** (1993), 203–220.

[Py2] L. Pyber, Dixon-like theorems, in preparation.

[PS1] L. Pyber and A. Shalev, Groups with super exponential subgroup growth, preprint.

[PS2] L. Pyber and A. Shalev, Subgroup growth and finite permutation groups, preprint.

[Ra] M.S. Raghunathan, On the congruence subgroup problem, *Publ. Math. IHES* **46**(1976), 107–161.

[Rp] A.S. Rapinchuk, Congruence Subgroup Problem for algebraic groups: old and new, *Astérisque* **209**(1992), 73–84.

[Se] D. Segal, Subgroups of finite index in solvable groups I, in *Proc. Groups-St. Andrews 1985* (Campbell and Robertson (eds.), Cambridge Univ. Press, 1986), 307–314.

[SS] D. Segal and A. Shalev, Groups with fractionally exponential subgroup growth, *J. Pure Appl. Alg.* **88**(1993), 205–223.

[Sh1] A. Shalev, Growth functions, p-adic analytic groups and groups of finite co-class, *J. London Math. Soc.*, to appear.

[Sh2] A. Shalev, Subgroup growth and sieve methods, preprint.

[Sm1] G.C. Smith, *Zeta functions of torsion free finitely generated nilpotent groups*, Ph.D. Thesis, University of Manchester, 1983.

[Sm2] G.C. Smith, Compressibility in nilpotent groups, *Bull. London Math. Soc.* **17**(1985), 453–457.

[Sr] J.P. Serre, Le problème des groupes de congruences pour SL_2, *Ann. Math.* **92** (1970), 489–527.

[St1] W.W. Stothers, The number of subgroups of given index in the modular groups, *Proc. Roy. Soc. Edinburgh* **78**(1977), 105–112.

[St2] W.W. Stothers, Free subgroups of the free product of cyclic groups, *Math. Comp.* **32**(1978), 1274–1280.

[St3] W.W. Stothers, On a result of Peterson concerning the modular group, *Proc. Roy. Soc. Edinburgh* **87**(1981), 263–270.

[St4] W.W. Stothers, Subgroups of finite index in free product with amalgamated subgroup, *Math. Comp.* **36**(1981), 653–662.

[St5] W.W. Stothers, Level and index in the modular group, *Proc. Royal Soc. Edinburgh* **99**(1984), 115–126.

[We] T.S. Weigel, On the profinite completion of arithmetic groups of split type, preprint.

[We] B. Weisfeiler, Strong approximation for Zariski dense subgroups of semi-simple algebraic grups, *Ann. Math.* **120**(1984), 271–315.

[Wi] H.S. Wilf, The asymptotics of $e^{p(z)}$ and the number of elements of each order in S_n, *Bull. Amer. Math. Soc.* **15**(1986), 228–232.

[Wn1] J.S. Wilson, Finite presentations of pro-p groups and discrete groups, *Invent. Math.* **105**(1991), 177–183.

[Wo] K. Wohlfahrt, Uber einen Satz von Dey und die Modulgruppe, *Arch. Math.* **29**(1977), 455–457.

[Wol] J.A. Wolf, Growth of finitely generated solvable groups and curvature of Riemannian manifolds, *J. Diff. Geom.* **2**(1968), 421–446.