SUBGROUP GROWTH

Alex Lubotzky & Dan Segal

(Corrected Draft: August 2002)

[dedication]

Preface

Let G be a finitely generated group, and for $n \in \mathbb{N}$ let $a_n(G)$ denote the number of subgroups of index n in G. By the 'subgroup growth' of G one means the asymptotic behaviour of the sequence $(a_n(G))$. The first main theme of this book is the relationship between the subgroup growth of a group and its algebraic structure.

This may be viewed as a new chapter in the theory of finiteness conditions in infinite groups, originated early in the last century by the Russian school of O. J. Schmidt and largely associated with the names of Kurosh and P. Hall. This studied questions of the following sort: let $\mathcal{P}$ be a property that is common to all finite groups F, for example 'there exist m and n such that F is generated by m elements and every element x of F satisfies $x^n = 1$'. Now let G be an arbitrary group having property $\mathcal{P}$; does it follow that G is finite? In the case of the above example this is the Burnside problem. In other cases one would only expect to deduce that G is virtually soluble, perhaps, e.g. when $\mathcal{P}$ is the property of having *finite rank*: there exists m such that every (finitely generated) subgroup can be generated by m elements. Numerous positive results were obtained in the middle of the century, pertaining to special classes of groups such as linear groups. However, many of the natural conjectures resisted all attempts at a general proof. The reason for this became clear in the 1970s, when Olshanskii and Rips constructed the so-called 'Tarski monsters': these are infinite groups G such that every proper subgroup of G is cyclic of (a fixed) prime order. Such a group G satisfies any reasonable finiteness condition and is a counter-example to any reasonable conjecture, such as the Burnside problem. On the other hand, in the '80s and '90s it gradually appeared that if one takes the old conjectures and adds the hypothesis that G is *residually finite*, then the conjectures indeed become theorems. The most famous example is the positive solution of the *restricted* Burnside problem, which may be interpreted as saying that every finitely generated residually finite group of finite exponent is finite – this earned Zelmanov a Fields medal. Other examples, closer to the spirit of this book, are the proof by Lubotzky and Mann that every finitely generated residually finite group of finite rank is virtually soluble, and results of Wilson and Zelmanov about residually finite Engel groups. These may all be seen as wide generalisations of the earlier results about finitely generated linear groups, since all such groups are indeed residually finite.

For a group to be residually finite means that it has many subgroups of finite index: enough so that their intersection is trivial. It is entirely natural, then, to ask the question "*how many* subgroups of each finite index?" From the most naive point of view, the study of subgroup growth may be seen as the project of arranging residually finite groups in a spectrum, from the 'very residually finite' – with fast subgroup growth – at one end to the 'only just residually finite' – having very slow subgroup growth – at the other.

The new developments mentioned above rest on three main planks: (i) the classification of the finite simple groups, (ii) Lie algebra methods applied to finite p-groups, and (iii) 'linearisation techniques' via p-adic analytic groups. We shall

see how (i) and (iii) are applied throughout this book, to derive information about the algebraic structure of a group, now assumed to be residually finite, when its subgroup growth is restricted: by specifying the type of subgroup growth we obtain a whole spectrum of refined finiteness conditions.

Thus subgroup growth puts a new slant on a long tradition in infinite group theory. However, it can also be seen in a quite different light. As well as the asymptotic behaviour, the arithmetic of the sequence $a_n(G)$ may be of interest; this is conveniently encoded in the Dirichlet series $\zeta_G(s) = \sum a_n(G)n^{-s}$, known as the 'zeta function of the group G' (the definition parallels that of the Dedekind zeta function of a number field, which encodes in the same way the number of ideals of each index in a ring of algebraic integers). One can now begin to develop a branch of 'non-commutative analytic number theory' that relates the analytic properties of the function $\zeta_G(s)$ to the structure of the group G. This is the second main theme of the book.

Let us mention some highlights, beginning with growth. A well established theory of 'growth of groups' relates to the 'word growth', that is the nature of the sequence $\left(b_n^S(G)\right)$ where $b_n^S(G)$ denotes the number of elements of G that can be expressed as words of length at most n in some (fixed) finite generating set S. While the precise values of the $b_n^S(G)$ depend on the choice of generating set S, their growth (i.e. asymptotic behaviour) does not. For example, free groups have exponential growth, while abelian, and more generally nilpotent, groups have polynomial growth. In fact a celebrated theorem of Gromov characterises the groups of polynomial growth precisely as those which are virtually nilpotent.

The situation with subgroup growth is similar in broad outline, but differs in interesting ways. Again, the fastest growth occurs for free groups, but now it is of type $n!$, which is like $e^{n \log n}$, that is, slightly *faster* than exponential. At the other end of the spectrum, the *PSG Theorem* (Theorem 5.1 in the book) characterises the (finitely generated) groups with polynomial subgroup growth: these are precisely the groups G such that $G/R(G)$ is virtually soluble of finite rank – here $R(G)$ denotes the intersection of all subgroups of finite index in G. (Of course the numbers $a_n(G)$ can only contain information about the quotient $G/R(G)$, so when studying subgroup growth it is natural to assume throughout that $R(G) = 1$, that is, G is *residually finite*.).

While the PSG theorem and Gromov's theorem are logically quite independent, they share a number of features. To begin with, both classify the groups of polynomial growth as (finite extensions of) groups in a well-understood subclass of the soluble groups. Moreover, both are proved following a similar pattern, centred on a reduction via topological groups to the special case of linear groups.

Gromov developed new methods in geometric group theory in order to embed his group in a topological group, at which point he was in a position to apply the solution to Hilbert's 5th problem (the characterisation of topological groups having the structure of a real Lie group). In the case of polynomial subgroup growth, the classification of the finite simple groups is invoked along the way to embedding the group in a pro-p group, at which point one is in a position to appeal to Lazard's solution of the p-adic version of Hilbert's 5th problem (the

proof that we give in Chapter 5 actually avoids p-adic Lie groups but is based on the same ideas).

The characterisation of *linear* groups with polynomial word growth depends on the 'Tits alternative': *a finitely generated linear group either is virtually soluble or else contains a non-abelian free subgroup.* The presence of a free subgroup in G implies that G has exponential word growth, but tells us nothing about the subgroup growth. To deal with linear groups of polynomial subgroup growth, a different dichotomy had to be established: now sometimes known as the 'Lubotzky alternative', this asserts that *a finitely generated linear group either is virtually soluble or else has a subgroup of finite index whose profinite completion maps onto the congruence completion of some semisimple arithmetic group.* This reduces the problem to the question of counting *congruence subgroups* in arithmetic groups.

The counting of congruence subgroups may be seen as a form of 'non-commutative number theory'. The proof of the PSG theorem is completed by an application of the Prime Number Theorem; but the precise estimation of 'congruence subgroup growth' in arithmetic groups is of interest in itself, and this involves both some serious group theory and deep number theory, such as the Bombieri-Vinogradov theorem on the 'Riemann hypothesis in the average'.

Another highlight in the story of word growth was the construction by Grigorchuk of groups of intermediate growth, strictly between polynomial and exponential. While (continuously) many such growth types have been realised, they all lie between $e^{\sqrt{n}}$ and e^n, and the nature of the 'spectrum' of possible growth types is still very much a mystery. In contrast, the spectrum of subgroup growth types is known to be essentially complete: explicit constructions that demonstrate this are given in Chapter 13. On the other hand, as is the case for word growth, there are definite 'gaps' in the subgroup growth spectrum when one restricts to special classes of groups such as linear groups.

The class of finitely generated nilpotent groups plays a special role both in word growth and subgroup growth. As mentioned above, these are (virtually) just the groups of polynomial word growth, and an exact formula for the minimal degree of a bounding polynomial was given by Bass; it takes integral values and depends on simple structural invariants of the group. Finitely generated nilpotent groups also have polynomial subgroup growth; but there is no known way to determine the degree of polynomial subgroup growth in terms of the structure of the group, and it is not always an integer. It is known, however, that this degree is a rational number.

This brings us to our second theme, the 'arithmetic of subgroup growth'. If G is a finitely generated nilpotent group, its degree in the above sense is denoted $\alpha(G)$, and is equal to the abscissa of convergence of the zeta function $\zeta_G(s)$. Such zeta functions share some of the properties of the more traditional zeta functions of number theory: for example they enjoy an Euler product decomposition, and for each prime p the local factor at p, denoted $\zeta_{G,p}(s)$, is a rational function of p^{-s}. The proof applies a beautiful rationality theorem for p-adic integrals due to Denef, based on considerations in p-adic model theory.

However, in contrast to classical zeta functions, the global behaviour of $\zeta_G(s)$

is erratic; for example, $\zeta_G(s)$ does not (usually) have analytic continuation to $\mathbb{C}$. This is related to the fact that the rational function expressing the local factor $\zeta_{G,p}(s)$ depends on the number of $\mathbb{F}_p$-rational points of a certain variety defined over $\mathbb{Z}$, and so varies wildly with the prime p. The construction of this variety is a procedure in algebraic geometry involving resolution of singularities, that leads to an explicit determination of the local factors. This is precise enough to yield the conclusion that the global abscissa $\alpha(G)$ is a rational number (using the Lang-Weil estimates for rational points on varieties over finite fields). It is also used to show that the global function $\zeta_G(s)$ is approximated in a neighbourhood of $\alpha(G)$ by an Artin L-function, and hence has a meromorphic continuation to this neighbourhood. This opens the way to methods of analytic number theory, which then yield an asymptotic formula $cn^{\alpha(G)}(\log n)^{\beta}$ for the number of subgroups of index at most n in G (here c is a constant and β is a non-negative integer) – a statement whose simplicity belies its depth.

The 'local zeta function' $\zeta_{G,p}(s)$ is also defined for a p-adic analytic pro-p group G, and again is a rational function. This depends on deep work of Denef and van den Dries in 'p-adic analytic model theory', and has remarkable and unexpected consequences for the theory of *finite* p-groups, including the proof of a delicate conjecture of Newman and O'Brien (explained in Chapter 16).

Attempts to answer the simple question: 'how many subgroups of index n does a group possess?' have thus encompassed a surprisingly broad sweep of mathematics. The full range will become apparent on looking through this book; it includes methods and results from the theories of finite simple groups, permutation groups, linear groups, algebraic and arithmetic groups, p-adic Lie groups, analytic and algebraic number theory, algebraic geometry, probability and logic. In many cases it has not been sufficient to quote results "off the peg", and new results have been obtained that have nothing to do with subgroup growth as such. Among these are criteria for an infinite group to be linear, the 'Lubotzky alternative' mentioned above, and new theorems about finite permutation groups. There have also been applications outside subgroup growth: a group-theoretic characterisation of arithmetic groups with the congruence subgroup property, estimates for the number of hyperbolic manifolds with given volume, and the results mentioned above on the enumeration and classification of finite p-groups.

Our aim in this book is not to present a completed theory: the subject is still very young. Indeed, while some of the core results (such as the PSG theorem) have been around for a few years, many were discovered even as we wrote, and are still unpublished (around 44% of those labeled 'Theorem' in the main body of the book had not been published by the end of the 20th century). This book is an attempt to present the state of the art as we reach what is perhaps the end of the 'foundational stage'. The broad outlines of a rich theory have begun to emerge; it is ripe for deeper investigation and new discoveries, and we hope that this book will encourage more mathematicians to explore an intriguing new field.

The present healthy state of the subject is largely due to the efforts and insight of a small number of colleagues (and friends): Avinoam Mann, Aner Shalev, Laci Pyber, Fritz Grunewald, Marcus du Sautoy, Thomas Müller. They have all materially contributed to the book by giving us access to their latest unpublished work, as have Andrei Jaikin-Zapirain, Benjamin Klopsch, Attila Maróti and Nikolay Nikolov. We thank them all most heartily. We are also most indebted to Efi Gelman, Dorian Goldfeld, Michael Larsen, Richard Lyons, Avinoam Mann and Laci Pyber for kindly reading various parts of the text and suggesting numerous corrections and improvements.

Some of the material is based on the first author's lectures at Groups St. Andrews/Galway, 1993, and at Yale, Columbia, Rice and the Hebrew Universities in the intervening years; he is grateful for much helpful feedback from the audiences on these occasions, and to the BSF, NSF and ISF for several research grants over the years.

[blank page]

Contents

Preface
Notation

0. Introduction and overview 1

0.1 Preliminary comments and definitions
0.2 Overview of the chapters
0.3 On CFSG
0.4 The 'windows'
0.5 The 'notes'

1. Basic methods of subgroup counting 11

1.1 Permutation representations
1.2 Quotients and subgroups
1.3 Group extensions
1.4 Nilpotent and soluble groups
1.5 Abelian groups I
1.6 Finite p-groups
1.7 Sylow's theorem
1.8 Restricting to soluble subgroups
1.9 Applications of the 'minimal index'
1.10 Abelian groups II
1.11 Growth types
Notes

2. Free groups 37

2.1 The subgroup growth of free groups
2.2 Subnormal subgroups
2.3 Counting d-generator finite groups
Notes

3. Groups with exponential subgroup growth 53

3.1 Upper bounds
3.2 Lower bounds
3.3 Free pro-p groups
3.4 Normal subgroups in free pro-p groups
3.5 Relations in p-groups and Lie algebras
Notes

4. Pro-p groups 77

4.1 Pro-p groups with polynomial subgroup growth
4.2 Pro-p groups with slow subgroup growth
4.3 The groups $\mathrm{SL}_r^1(\mathbb{F}_p[[t]])$
4.4 Λ-perfect groups

4.5 The Nottingham group
4.6 Finitely presented pro-p groups
Notes

5. Finitely generated groups with polynomial subgroup growth 97

5.1 Preliminary observations
5.2 Linear groups with PSG
5.3 Upper chief factors
5.4 Groups of prosoluble type
5.5 Groups of finite upper rank
5.6 The degree of polynomial subgroup growth
Notes

6. Congruence subgroups 117

6.1 The characteristic 0 case
6.2 The positive characteristic case
6.3 Perfect Lie algebras
6.4 Normal congruence subgroups
Notes

7. The generalised congruence subgroup problem 141

7.1 The congruence subgroup problem
7.2 Subgroup growth of lattices
7.3 Counting hyperbolic manifolds
Notes

8. Linear groups 161

8.1 Subgroup growth, characteristic 0
8.2 Residually nilpotent groups
8.3 Subgroup growth, characteristic p
8.4 Normal subgroup growth
Notes

9. Soluble groups 171

9.1 Metabelian groups
9.2 Residually nilpotent groups
9.3 Some finitely presented metabelian groups
9.4 Normal subgroup growth in metabelian groups
Notes

10. Profinite groups with polynomial subgroup growth 187

10.1 Upper rank
10.2 Profinite groups with wPSG: structure
10.3 Quasi-semisimple groups
10.4 Profinite groups with wPSG: characterisation
10.5 Weak PSG = PSG

Notes

11. Probabilistic methods 213

11.1 The probability measure
11.2 Generation probabilities
11.3 Maximal subgroups
11.4 Further applications
11.5 Pro-p groups
Notes

12. Other growth conditions 231

12.1 Rank and bounded generation
12.2 Adelic groups
12.3 The structure of finite linear groups
12.4 Composition factors
12.5 BG, PIG and subgroup growth
12.6 Residually nilpotent groups
12.7 Arithmetic groups and the CSP
12.8 Examples
Notes

13. The growth spectrum 257

13.1 Products of alternating groups
13.2 Some finitely generated permutation groups
13.3 Some profinite groups with restricted composition factors
13.4 Automorphisms of rooted trees
Notes

14. Explicit formulas and asymptotics 283

14.1 Free groups and the modular group
14.2 Free products of finite groups
14.3 Modular subgroup arithmetic
14.4 Surface groups
Notes

15. Zeta functions I: nilpotent groups 299

15.1 Local zeta functions as p-adic integrals
15.2 Alternative methods
15.3 The zeta function of a nilpotent group
Notes

16. Zeta functions II: p-adic analytic groups 323

16.1 Integration on pro-p groups
16.2 Counting subgroups in a p-adic analytic group
16.3 Counting orbits
16.4 Counting p-groups
Notes

Windows

Finite group theory 333
Finite simple groups 335
Permutation groups 353
profinite groups 363
Pro-p groups 371
Soluble groups 381
Linear groups 389
Linearity conditions for infinite groups 393
Strong approximation for linear groups 403
Primes 423
Probability 429
p-adic integrals and logic 433

Appendix: Open problems 439

Bibliography 447

Notation

Number theory

$f \sim g$ if $f(n)/g(n) \to 1$ as $n \to \infty$
$f = O(g)$ if there exists $a > 0$ such that $f(n)/g(n) \leq a$ for all large n
$f = o(g)$ if $f(n)/g(n) \to 0$ as $n \to \infty$
$f \asymp g$ if $f = O(g)$ and $g = O(f)$.

$\log x = \log_2 x$
$\ln x = \log_e x$
$[x]$: greatest integer $\leq x$
$\lceil x \rceil$: least integer $\geq x$

Group theory

$H \leq G$, $H \lhd G$, $H \lhd\lhd G$: H is a subgroup, normal subgroup, subnormal subgroup of G
$H \leq_o G$ etc.: H is an *open* subgroup of G (a profinite group)
$|G : H|$: the index of H in G
$g^x = x^{-1}gx$
$[g, x] = g^{-1}g^x$
$\langle X \rangle$: subgroup generated by a set X
$[H, K] = \langle \{[h, k] \mid h \in H, k \in K\} \rangle$
$G' = [G, G]$ derived group of G
$\gamma_n(G)$: nth term of lower central series of G ($\gamma_1(G) = G$, $\gamma_n(G) = [\gamma_{n-1}(G), G]$)
$\mathrm{C}_G(X)$, $\mathrm{N}_G(X)$: centraliser, normaliser of X in G
$\mathrm{Z}(G)$: centre of G
$\Phi(G)$: Frattini subgroup of G
$G^n = \langle \{g^n \mid g \in G\} \rangle$
$G^{(n)}$: direct product of n copies of G (also sometimes denoted G^n when G is abelian)
$G \wr S$: the permutational wreath product of G with (the finite permutation group) S
$\mathrm{d}(G)$: size of a minimal generating set for G

$$\mathrm{rk}(G) = \sup \begin{cases} d(H) : H \leq G \text{ and } d(H) < \infty & (G \text{ an abstract group}) \\ d(H) : H \leq_o G & (G \text{ a profinite group}) \end{cases}$$

$\mathrm{ur}(G) = \sup \{\mathrm{rk}(Q) : Q \text{ a finite quotient of } G\}$
$\mathrm{r}_p(G) = \mathrm{rk}(P)$ where P is a Sylow p-subgroup of G (G a finite group)
$\mathrm{ur}_p(G) = \sup \{\mathrm{r}_p(Q) : Q \text{ a finite quotient of } G\}$

$o(x)$: the order of the element x in a given group

The *Fitting length* (or height) of a soluble group G is the minimal length of a chain $1 = N_0 < N_1 < \ldots < N_k = G$ of normal subgroups such that N_i/N_{i-1} is nilpotent for each i

C_n : cyclic group of order n
Sym(n), Alt(n) : symmetric, alternating group of degree n

$a_n(G)$: the number of subgroups (or open subgroups) of index n in G
$s_n(G)$: the number of subgroups (or open subgroups) of index *at most* n in G
$s(G)$:the number of subgroups in the finite group G
$m_n(G)$, $a_n^{\triangleleft}(G)$, $a_n^{\triangleleft\triangleleft}(G)$: the number of *maximal*, resp. *normal*, resp. *subnormal* subgroups (or open subgroups) of index n in G (similarly for $s_n^{\triangleleft}(G)$, $s_n^{\triangleleft\triangleleft}(G)$)
$c_n(\Gamma)$, $c_n^{\triangleleft}(G)$: the number of *congruence subgroups* (resp. *normal congruence subgroups*) of index at most n in the arithmetic group Γ

A group G is said to be *virtually* $\mathcal{X}$, where $\mathcal{X}$ is some class of groups, if G has a normal subgroup N of finite index such that $N \in \mathcal{X}$ (when G is profinite N must be open).
A group G is *residually* $\mathcal{X}$ if

$$\bigcap_{G/N \in \mathcal{X}} N = 1;$$

equivalently, if for each element $x \neq 1$ of G there is an epimorphism $\theta : G \to H$ where $H \in \mathcal{X}$ and $\theta(x) \neq 1$.

Chapter 0

Introduction and overview

Suppose we want to bring some order into the universe of infinite groups. This is too huge and too diverse for anything like a classification up to isomorphism to be feasible; instead, we look for simple invariants, and try to see how groups are divided up according to the nature of their invariants.

The invariant we are going to study is the *subgroup growth function*. To each group G we associate the numerical function

$$n \mapsto a_n(G)$$

where $a_n(G)$ denotes the *number of subgroups of index n in G*. (We only consider groups for which these numbers are *finite*: this restriction is discussed below.)

From the group-theoretic point of view, the natural questions are

(1) what are the general features of subgroup growth functions, for groups in general?

(2) which algebraic features of a group are reflected in properties of its subgroup growth function?

If we are number theorists rather than group theorists, we may view the subject from a different angle. If G is a 'natural' sort of group, one would like to know

(3) what are the arithmetical properties of the numerical sequence $(a_n(G))$?

From this point of view, the investigation of subgroup growth functions should be seen as a branch of 'non-commutative arithmetic': it is in direct analogy to the study of the Dedekind zeta function of a number field, which encodes the arithmetical sequence $(a_n(\mathfrak{o}))$, where $a_n(\mathfrak{o})$ denotes the number of *ideals* of index n in the ring of algebraic integers $\mathfrak{o}$.

0.1 Preliminary comments and definitions

(i) First of all, we need to know that $a_n(G)$ is *finite* for each n. This forces us to restrict attention to groups G for which this is the case; every *finitely generated* group G has this property, and more generally so does every group whose *profinite completion* is finitely generated (see below). (It is shown in [Wilson 1970] that every group satisfying the *maximal condition for normal subgroups* has only finitely many subgroups of each finite index; the subgroup growth of such groups has not as yet been investigated.)

(ii) Let $R(G)$ be the intersection of all finite-index subgroups of G. Then $a_n(G) = a_n(G/R(G))$. So we may as well restrict attention from the beginning to groups G such that $R(G) = 1$. Such groups are said to be *residually finite*.

Many of the groups that arise naturally in mathematics are both finitely generated and residually finite, so these restrictions leave us with plenty of material to work on.

(iii) Every group G has a *profinite completion* $\widehat{G}$. This is the inverse limit of the system of all finite quotient groups of G; it is a compact Hausdorff topological group whose open normal subgroups form a base for the neighbourhoods of the identity, in other words a *profinite group*. If G is residually finite we may consider G as a dense subgroup of $\widehat{G}$. In that case, the mapping $H \mapsto \overline{H}$ (the closure of H in $\widehat{G}$) is an index-preserving bijection from the set of all finite-index subgroups in G to the set of all open subgroups in $\widehat{G}$. It follows that $a_n(G) = a_n(\widehat{G})$ for every n, where by $a_n(\widehat{G})$ we denote the number of *open* subgroups of index n in $\widehat{G}$. (When referring to subgroups of finite index in a profinite group, we shall *always* mean open subgroups. Whether a finitely generated profinite group can have finite-index subgroups that are not open is an interesting open problem, but not one that need concern us here.) These matters are explained in more detail in the **Profinite groups** window.

The moral is that subgroup growth is 'really' a feature of *profinite* groups. It is logical to divide our study into two stages: *one*: examine the subgroup growth of profinite groups; *two*: investigate the (abstract) groups that have a particular profinite group as their profinite completion. In practice we don't always follow this path, but it is illuminating to bear in mind these two distinct aspects of the subject (analogous to arithmetic in the p-adic numbers vs. arithmetic of the rationals). In the rest of the book we move freely between 'abstract' groups and profinite groups, according to what seems more appropriate in the context.

(iv) **'Growth types'** When studying subgroup growth in the asymptotic sense, it is natural to consider the growth rate of the 'summatory' function

$$n \mapsto s_n(G) = \sum_{j=1}^{n} a_j(G),$$

that is, the number of subgroups of index *at most* n in a group G. A rough classification of groups by subgroup growth is provided by the *growth type*: a

group G has *(subgroup) growth type at most* f, for some function f, if there exists a positive constant a such that

$$s_n(G) \leq f(n)^a \quad \text{for all large } n; \tag{1}$$

G has *growth type* f if this holds and there exists another positive constant b such that

$$s_n(G) \geq f(n)^b \quad \text{for infinitely many } n. \tag{2}$$

In other words, the growth type is f if and only if

$$\log(s_n(G)) = O(\log f(n))$$
$$\log(s_n(G)) \neq o(\log f(n)).$$

A moment's consideration shows that 'having the same growth type' is not actually an equivalence relation; however, it is a convenient way to summarize the information that we have about many groups. In some cases we can do better, namely when we have a *lower bound* as well as an upper bound for $s_n(G)$ that is valid for all large n. Thus we say that G has *strict growth type* f if (2) as well as (1) holds for all large n, in other words if

$$\log(s_n(G)) \asymp \log f(n).$$

'Having the same strict growth type' is of course an equivalence relation.

G is said to have *polynomial subgroup growth* if the growth type is at most n, i.e. if $s_n(G) \leq n^c$ for all n, where c is some constant.

We shall also be considering some other subgroup-counting functions:

$a_n^{\triangleleft}(G)$, $s_n^{\triangleleft}(G)$: the number of *normal* subgroups of index n (resp. index at most n) in G

$a_n^{\triangleleft\triangleleft}(G)$, $s_n^{\triangleleft\triangleleft}(G)$: the number of *subnormal* subgroups of index n (resp. index at most n) in G

$m_n(G)$: the number of *maximal* subgroups of index n in G,

and the language of 'growth types' is extended to these in the natural way. The results on these growth functions are less systematic and complete than in the case of subgroup growth, and this is one area where much remains to be discovered.

0.2 Overview of the chapters

Each of the chapters after the first deals with a particular aspect of subgroup growth (or a related topic). Several basic and elementary arguments appear repeatedly in different contexts, and we have collected these together in Chapter 1. The reader should not be put off by the somewhat bitty nature of this

chapter, but rather skim through it on first reading and refer back to it whenever necessary.

The next four chapters deal with groups of successively slower growth types. **Chapter 2** considers **free groups**. These exhibit the fastest possible growth: they have subgroup growth of strict type n^n. The proof is a (relatively simple) application of finite permutation group theory, of a kind that will appear (in more sophisticated forms) in several other places. The *normal*, *subnormal* and *maximal* subgroup growth types of free groups are also determined; the first of these depends on the following result of independent interest: *the number of isomorphism types of finite d-generator goups of order n is bounded above by $n^{2d \log n}$*.

An 'upper composition factor' of a group G means a composition factor of a finite quotient of G. One of the recurring themes throughout the book is the close link between subgroup growth of a group and the structure of its upper composition factors. This is first examined in detail in **Chapter 3.** The first main result there shows that a finitely generated group G has at most *exponential* subgroup growth type (and at most *polynomial maximal subgroup growth*) if G does not involve *every finite group* as an upper section (this is equivalent to a restriction on the upper composition factors). A precise relationship is then established between the actual rate of subgroup growth and the nature of the excluded finite groups.

If every upper composition factor of G is cyclic of order p, for a fixed prime p, then $\widehat{G}$ is a pro-p group; the last part of Chapter 3 determines the strict growth type of free pro-p groups, which is again exponential. The *normal subgroup growth* type of these groups is also determined; again, this is done by estimating *the number of isomorphism types of finite d-generator goups of order p^n*, which is about p^{cn^2} where c depends on d.

Chapter 4 continues the study of pro-p groups, those that are in some sense smaller than the free ones. In analogy with a result stated above, it is shown that a finitely presented pro-p group has growth type at most $2^{\sqrt{n}}$ if it does not involve every finite p-group as an upper section. Several examples of pro-p groups are examined, all of which have growth type $n^{\log n}$.

The most important result of this chapter is the following dichotomy satisfied by every finitely generated pro-p group G : let $c < 1/(8 \log p)$. Then *either* $s_n(G) > n^{c \log n}$ for infinitely many n *or* G has polynomial subgroup growth; and the latter holds if and only if G has *finite rank* (this is equivalent to G having the structure of a *p-adic analytic group*). This theorem is a forerunner of the 'PSG Theorem', which characterizes groups of polynomial subgroup growth; and it is the first case of a 'gap theorem', saying that (within a particular class of groups) the growth type cannot lie in a certain range – in this case, strictly between type n and type $n^{\log n}$.

Chapter 5 is devoted to one of the main results of the book, the aforementioned **PSG Theorem**: *a finitely generated residually finite group has polynomial subgroup growth if and only if it is virtually soluble of finite rank.* The 'if' direction is easy and already appears in Chapter 1. The proof in the other direction involves several different techniques:

- Finite group theory, including the classification of finite simple groups, to obtain restrictions on the upper composition factors.
- 'Linearisation', that is, finding sufficient conditions for an infinite group to be isomorphic (or almost so) to a linear group over a field.
- 'Strong approximation' results for linear groups, reducing questions about these to the case of arithmetic subgroups in semisimple algebraic groups.
- The Prime Number Theorem.

Much of the necessary material, which is of independent interest, is dealt with separately in 'windows' (explained below).

We jump ahead to **Chapter 10**, which treats the 'Profinite PSG Theorem', namely the characterisation of *profinite* groups with polynomial subgroup growth. Such a group need not be soluble: modulo a prosoluble normal subgroup of finite rank the group is (virtually) a product of finite simple groups of Lie type, satisfying certain precise arithmetical conditions. The proof develops further the finite group theory of Chapter 5 (but is independent of the other parts of that chapter).

Chapters 8 and **9** discuss stronger versions of the PSG Theorem that apply to linear groups, and more generally to residually nilpotent groups. In each case there is a 'gap theorem': *if the subgroup growth is of type strictly less than* $n^{\log n/\log\log n}$ *then it is polynomial.* This depends in part on results of Chapter 6, decribed below, as does the following striking theorem on **normal subgroup growth**: *if a finitely generated linear group G has polynomial normal subgroup growth, then the simple components of the Zariski closure of G (a linear algebraic group) are of types G_2, F_4 or E_8.* Here we see a remarkably subtle structural property of a group reflected in its subgroup growth; the result is 'genuine' in that the groups $G_2(\mathbb{Z})$, $F_4(\mathbb{Z})$ and $E_8(\mathbb{Z})$ really do have polynomial normal subgroup growth.

The heart of proof of the PSG Theorem is an estimation of the **congruence subgroup growth** in arithmetic groups. A fairly easy lower estimate sufficed for that proof. **Chapter 6** is devoted to the precise determination of this growth type: it is $n^{\log n/\log\log n}$ in characteristic zero and $n^{\log n}$ in positive characteristic. The methods in the two cases are quite different, depending in the first case on Bombieri's deep results on the Riemann hypothesis 'on average', in the second case on the combinatorial study of finite Lie algebras. The growth type of **normal congruence subgroups** is also determined: this depends delicately on the *type* (i.e. the Dynkin diagram) of the underlying simple algebraic group.

These results are used in **Chapter 7** to establish a group-theoretic characterisation of arithmetic groups (in characteristic zero) with the **congruence subgroup property** (CSP): *an arithmetic group has CSP if and only if it has subgroup growth of type strictly less than* $n^{\log n}$. Arithmetic groups are a particular case of **lattices in Lie groups**. Using the above criterion as a *definition* of the 'generalized CSP', the rest of Chapter 7 examines the subgroup growth of such lattices, and establishes in many cases a generalized version of

Serre's congruence subgroup conjecture, namely that a lattice in a simple Lie group L has the (generalized) CSP if and only if L has real rank greater than 1. The methods here are largely topological and geometric. As an application, it is shown that *the number of hyperbolic manifolds of a given dimension and volume at most r grows like r^{cr}, where c is a constant.*

The emphasis so far has been on determining the subgroup growth of various groups, using a more-or-less direct approach. A new angle appears in **Chapter 11**. Here we consider a profinite group G as a **probability space**, using its natural Haar measure as a compact topological group. The simple observation that the probability for random a k-tuple in G to belong to a given open subgroup H is $|G:H|^{-k}$ has far-reaching consequences. Applying this when H is a maximal subgroup, for example, we see that the probability $P(G,k)$ that G can be generated by k elements is at least $1-\sum m_n(G)n^{-k}$; this implies that if G has polynomial maximal subgroup growth then for sufficiently large k one has $P(G,k)>0$ – in this case G is said to be *positively finitely generated* or PFG (as a special case we may infer that every profinite group with PSG is finitely generated! – a non-probabilistic result proved by simple probabilistic means). In fact, *a profinite group is PFG if and only it has polynomial maximal subgroup growth*; the "only if" is a much deeper result that depends on the classification of finite simple groups. A variety of other applications of the probabilistic method are also given, including an elegant determination of the zeta function of $\mathbb{Z}^d$ (see below).

The property of having polynomial (or otherwise restricted) subgroup growth may be viewed as a finiteness condition on a group; it is an 'upper finiteness condition' in the sense that it is defined as a limitation on the finite quotients. In **Chapter 12** we consider some other upper finiteness conditions, in particular one called **polynomial index growth** (PIG): a group G has PIG if $|G^*:G^{*n}|\leq n^c$ for all n and every finite quotient G^* of G, where c is a constant. Another closely related condition is 'bounded generation': a profinite group is said to be *boundedly generated* (BG) if it is equal to the product of finitely many procyclic subgroups. The main result shows that both conditions are closely related to subgroup growth: for profinite groups, PSG $\Longrightarrow$ BG $\Longrightarrow$ PIG, while PIG *implies that the subgroup growth is of type at most* $n^{(\log n)^2}$. Both PIG and BG (for the profinite completion) can be used to characterize arithmetic groups with the *congruence subgroup property*, in analogy to the first main result of Chapter 7.

The theory of groups with upper finiteness conditions such as these is less developed than the theory of subgroup growth, and one purpose of Chapter 12 is to draw attention to the many unanswered questions in this area.

Chapter 13 concludes our study of growth types by establishing that the **subgroup growth spectrum** is essentially *complete*. That is, for any 'reasonably nice' non-decreasing unbounded function $f:\mathbb{N}\to(0,\infty)$ such that $f(n)=o(n)$ there exists a finitely generated residually finite group having subgroup growth of type $n^{f(n)}$. This means that there are no 'gaps' in the spectrum of possible growth types, between the slowest type n^1 and the fastest type n^n. (Actually the given constructions leave the possibility of a 'small gap' between types $n^{\log\log n}$ and $n^{\log n}$, but there seems little doubt that this can be filled.)

It follows in particular that there are *continuously many* distinct growth types for finitely generated groups.

The examples in this chapter are constructed in two stages: first a profinite group G is tailored to have the required growth type, and then – the more challenging part – a finitely generated dense subgroup Γ of G is found such that the natural epimorphism $\widehat{\Gamma} \to G$ is actually an isomorphism, or at least has relatively small kernel. This procedure illustrates the philosophy outlined above in Section 0.1 (iii). It is applied to two different kinds of profinite group: (a) a product of finite alternating groups, using finite permutation group theory, and (b) a 'branch group' in the sense of Grigorchuk, using the theory of groups acting on rooted trees.

The last three chapters are devoted to the **'arithmetic of subgroup growth'.** A full treatment would require a whole second book; here we provide no more than an introduction to this area, where indeed many of the most challenging open problems are to be found.

In **Chapter 14** we report first on the case where G is a *free product of finite or cyclic groups*. In this case, the sequence $a_n(G)$ can be studied by combinatorial methods, generalising the approach originally applied to free groups in Chapter 2. These lead both to remarkably precise asymptotic formulas and to some intriguing results on divisibility properties. For the proofs, which involve real analysis and combinatorics, we refer the reader to the original literature. The final section of Chapter 14 determines the subgroup growth of *surface groups*; the method is character-theoretic, and potentially opens the way to a similar study of other classes of one-relator groups.

The next two chapters introduce the (subgroup growth) *zeta function*. If G is any group with polynomial subgroup growth, the Dirichlet series

$$\zeta_G(s) = \sum_{n=1}^{\infty} \frac{a_n(G)}{n^s}$$

represents a complex analytic function, the *zeta function* of G, regular on the half-plane $\mathrm{Re}(s) > \alpha(G)$, where $\alpha(G) = \inf\{c \mid s_n(G) \leq n^c \text{ for all large } n\}$ is the 'degree of polynomial subgroup growth'.

Chapter 15 studies the case where G is a *finitely generated nilpotent group*. In this case, the zeta function has excellent properties, including (a) an *Euler product* expansion, (b) for each prime p the 'local factor'

$$\zeta_{G,p}(s) = \sum_{n=0}^{\infty} a_{p^n}(G) p^{-ns} \tag{3}$$

ia a *rational function* of p^{-s}; (c) *analytic continuation*. These are applied in the proof of the following theorem: (d) *if G is a finitely generated nilpotent group then*

$$s_n(G) \sim c n^{\alpha} (\log n)^{\beta}$$

for some $c > 0, 0 < \alpha = \alpha(G) \in \mathbb{Q}$ and $0 \leq \beta \in \mathbb{Z}$.

Claim (a) is elementary. The rationality theorem (b) is discussed in detail, and related to properties of *integrals on p-adic manifolds*. The chapter also presents *five* different proofs of the nice formula

$$\zeta_{\mathbb{Z}^d}(s) = \zeta(s)\zeta(s-1)\dots\zeta(s-d+1)$$

(here $\zeta(s)$ denotes the Riemann zeta function), each illustrating a different approach to the topic. On the other hand, (c) and (d) are very deep, and we only outline briefly the main ideas of the proofs.

Finally, **Chapter 16** considers the zeta function of a **compact p-adic analytic group.** For such a group G (which is a finite extension of a pro-p group of finite rank), the 'local zeta function' (3) is again a rational function of p^{-s} (generalising the nilpotent case). This applies for example to groups such as $\mathrm{SL}_d(\mathbb{Z}_p)$, raising the interesting challenge of actually determining the rational functions in such cases. It also has several remarkable applications to the enumeration and classification of *finite p-groups*; the simplest of these to state is the following, where

$$f(n,p,c,d)$$

denotes the number of isomorphism types of d-generator groups of order p^n and nilpotency class at most c: *for fixed p, c and d the function $n \mapsto f(n,p,c,d)$ satisfies a linear recurrence relation with integer coefficients*; while the most remarkable is the proof of a subtle conjecture of Newman and O'Brien on the classification of *p-groups of fixed coclass*. Again, the chapter gives only an outline of the main ideas of the proofs.

0.3 On CFSG

The *classification of the finite simple groups* (CFSG) is a wonderful 'black box' that enables the solution of many otherwise intractable problems in group theory. A few of the major theorems in the book rely on this black box for their proof, notably the 'PSG Theorems' of Chapters 5 and 10. This does mean that, at present, the complete proof of such theorems is about 15,000 pages long! We do not know if independent proofs will ever be found; this would certainly be desirable for aesthetic and mathematical reasons We have tried on the whole to resist the temptation to 'shorten' arguments by appealing indiscriminately to CFSG, though we occasionally mention points at which such an appeal would simplify a proof.

On the positive side, the book shows how CFSG has made possible substantial advances in infinite group theory, in a perhaps unexpected way; thus as well as being the end of one story it is the beginning of a new one.

0.4 The windows

On the whole, the individual chapters after the first are independent of one another, and can be read in any order (except that Chapters 7 and 8 rely on

Chapter 6, Chapter 10 on parts of Chapter 5, and Chapter 16 on parts of Chapter 15).

A wide range of mathematical disciplines has to be invoked in the course of our work. Each will be familiar to some readers and not to others. In an attempt to keep clear the main structure of the development within each chapter, we have separated off the discussion of various topics into twelve **windows**. Although physically they appear together at the end of the book, the reader is expected to treat them rather as 'hypertext links', and be prepared to flick to a window for illumination whenever necessary. We apologise for the (hopefully minor) inconvenience, and hope that this is compensated by the attendant streamlining of the main text.

The windows vary in style: some are little more than lists of results, with references, collected together for convenience; others discuss some topic in greater or lesser depth, and present either new material or material that is not otherwise easily available in the required form. We occasionally allow ourselves to digress, where we feel there is something interesting to be said. The windows on **Linearity conditions** and **Strong approximation** in particular are quite substantial and are really chapters in their own right; their present form is supposed to emphasize that they are of more general interest, quite apart from their applications in this book. It is our hope that these, and some of the other windows, will be a useful source for people working in related areas beyond the narrow topic of subgroup growth.

For cross-references to the windows we use boldface type and the special symbol $\looparrowright$, so for example "($\looparrowright$ **Pro-p groups**)" means "see the Window on pro-p groups".

0.5 The 'notes'

Results are usually given in the main text without attribution; needless to say this is *not* meant to imply any claim of originality. Instead, bibliographic references are collected in the 'notes' section at the end of each chapter. We have tried to give due credit to the authors of all the main results; doubtless some oversights will have occurred, and we beg the forgiveness of our respected colleagues in such cases.

Occasionally, the 'notes' also contain references to additional material not covered in the main text, and/or historical remarks.

Chapter 1

Basic techniques of subgroup counting

The purpose of this preliminary chapter is to introduce a variety of simple arguments that will serve as basic tools throughout the book. Taken *en masse* these may seem rather dry and uninspiring – the reader may prefer to skim through them fairly briskly, returning later when necessary to study particular points in more detail (the simpler results will often be used in later chapters without special mention).

There are three basic methods for obtaining *upper* bounds on the number of subgroups of finite index in a group: (i) counting homomorphisms into finite groups, (ii) counting generating sets and (iii) counting complements in extensions. We shall see how each of these methods is used, sometimes in combination. Slightly more sophisticated methods will also appear, which involve restricting to Sylow subgroups or to soluble subgroups.

We give a fairly thorough account of subgroup-counting in abelian groups; this is essential because the most usual way to obtain *lower* bounds for $s_n(G)$ in a general group G is to locate an elementary abelian section A 'near the top' of G and then relate $s_n(G)$ to $s_{n/m}(A)$, where m is the index of A in G.

We recall some notation:

$d(G)$: the minimal cardinality of a generating set for G (topological generating set if G is profinite);

$\mathrm{rk}(G) = \sup\{d(H) \mid H \text{ a finitely generated subgroup of } G\}$;

$\mathrm{r}_p(G) = \sup\{d(H) \mid H \text{ a } p\text{-subgroup of } G\}$ (when G is finite);

$a_n(G)$: the number of subgroups of index n in G (open subgroups if G is profinite);

$$s_n(G) = \sum_{j=1}^{n} a_j(G), \quad s(G) = \sum_{j=1}^{\infty} a_j(G)$$

$\widehat{G}$ denotes the profinite completion of a group G;

$\log x$ denotes the logarithm to base 2 of x.

1.1 Permutation representations

Let G be a group and H a subgroup of index n in G. Then G permutes the right cosets of H by right multiplication. If we label H with 1 and the remaining $n-1$ cosets with $2, , \ldots, n$ in any order we obtain a homomorphism

$$\varphi : G \to \mathrm{Sym}(n);$$

it is clear that (i) $\varphi(G)$ is transitive and (ii) $H = \mathrm{Stab}_{G,\varphi}(1) = \varphi^{-1}\mathrm{Sym}(\{2, \ldots, n\})$. Since there are $(n-1)!$ distinct such labellings, we see that H gives rise to $(n-1)!$ homomorphisms $\varphi : G \to \mathrm{Sym}(n)$ satisfying (i) and (ii). Conversely, to each $\varphi : G \to \mathrm{Sym}(n)$ such that $\varphi(G)$ is transitive we may associate the subgroup $\mathrm{Stab}_{G,\varphi}(1)$ which has index n in G.

Under this correspondence between subgroups and permutation representations, moreover, the *maximal* subgroups of G correspond to *primitive* representations (for the stabilizer of a block containing the point 1 is a subgroup of G containing the stabiliser of 1). Thus, writing

$$t_n(G) = |\{\varphi : G \to \mathrm{Sym}(n) : \varphi(G) \text{ is transitive}\}|$$

and

$$p_n(G) = |\{\varphi : G \to \mathrm{Sym}(n) : \varphi(G) \text{ is primitive}\}|,$$

we have

Proposition 1.1.1

$$a_n(G) = t_n(G)/(n-1)!$$
$$m_n(G) = p_n(G)/(n-1)!$$

For example, if G is infinite cyclic we have $a_n(G) = 1$ for every n, while $t_n(G)$ is equal to the number of n-cycles in $\mathrm{Sym}(n)$ which is $(n-1)!$.

Corollary 1.1.2 *If G is a finitely generated group, or a finitely generated profinite group, then*

$$a_n(G) \leq n!^{d(G)}/(n-1)! = n \cdot n!^{d(G)-1}.$$

(For the profinite case, note that the homomorphisms φ are continuous.) Asymptotically, this is the best possible upper bound, as we shall see in Chapter 2.

To go further we need to count the number of transitive permutation representations. Write $h_0 = 1$ and for $n \geq 1$ let

$$h_n(G) = |\operatorname{Hom}(G, \mathrm{Sym}(n))|.$$

Lemma 1.1.3 *Let G be any group. Then*

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

Proof. For each k, let $h_{n,k}(G)$ denote the number of representations of G in in $\mathrm{Sym}(n)$ for which the orbit of 1 has length exactly k. Now given k, there are $\binom{n-1}{k-1}$ ways to choose the orbit of 1, $t_k(G)$ ways for G to act on this orbit, and $h_{n-k}(G)$ ways for G to act on its complement in $\{1, 2, \ldots, n\}$. Therefore

$$h_{n,k}(G) = \binom{n-1}{k-1} t_k(G)\, h_{n-k}(G), \tag{1.1}$$

and the result follows. ■

Combining this with Proposition 1.1.1 we get

Corollary 1.1.4 *Let G be any group. Then*

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

This recursive formula is useful only when we have some independent information about the permutation representations of G; it will be applied to free groups (Chapter 2), to groups having restricted composition factors (Chapter 3), and to certain groups given by a finite presentation (Chapter 14).

1.2 Quotients and subgroups

The following is evident, and will be used frequently without special mention:

Lemma 1.2.1 (i) *If $N \lhd G$ then $a_n(G/N) \le a_n(G)$ and $s_n(G/N) \le s_n(G)$.*

(ii) *If $H \le G$ with $|G : H| = m$ then $a_n(H) \le a_{mn}(G)$ and $s_n(H) \le s_{mn}(G)$.*

(iii) *Provided $a_n(G)$ is finite, $a_n(G) = a_n(\overline{G})$ for some finite quotient $\overline{G}$ of G. Consequently $a_n(G) = a_n(\widehat{G})$.*

Lemma 1.2.2 *If G is finite then*

$$s_n(G) \le s(G) \le |G|^{\mathrm{rk}(G)}, \tag{1.2}$$

$$\mathrm{rk}(G) \le \log |G|. \tag{1.3}$$

Proof. (1.2) is clear since each subgroup of G can be generated by $\mathrm{rk}(G)$ elements. At least one subgroup H really needs $\mathrm{rk}(G) = r$ generators; say $H = \langle x_1, \ldots, x_r \rangle$. Put $H_i = \langle x_1, \ldots, x_i \rangle$. Then

$$|G| \ge |H| = |H : H_{r-1}| \cdot \ldots \cdot |H_2 : H_1| \cdot |H_1| \ge 2^r,$$

whence (1.3). ■

Lemma 1.2.3 *Let U be a subgroup of finite index g in G. Then for each k the number of subgroups H of G with $H \geq U$ and $|H : U| \leq k$ is at most*

$$g^{[\log k]}.$$

Proof. The maximal length of a chain of subgroups between U and H is at most $[\log k] = s$, say; so H can be generated by U and at most s further elements. Moreover,

$$\langle U, x_1, \ldots, x_s \rangle = \langle U, a_1 x_1, \ldots, a_r x_s \rangle$$

whenever $a_1, \ldots, a_s \in U$, so the number of distinct subgroups of this form is at most $|G : U|^s = g^s$. ■

Corollary 1.2.4 *Suppose that L is a subgroup of finite index m in G. Then for each n we have*

$$s_n(G) \leq (mn)^{[\log m]} s_n(L).$$

Proof. To each $H \leq G$ we associate the subgroup $H \cap L$ of L. If $|G : H| \leq n$ then $|H : H \cap L| \leq n$. Given a subgroup U of index at most n in L, if $H \leq G$ satisfies $H \cap L = U$ then $|H : U| \leq m$, so the number of such subgroups H is at most

$$|G : U|^{[\log m]} \leq (mn)^{[\log m]}.$$

The corollary follows. ■

1.3 Group extensions

In this section, we fix a normal subgroup N of G and write $Q = G/N$. We denote by

$$\mathrm{Der}(G, H)$$

the set of **derivations** (crossed homomorphisms, 1-cocycles) from G into a G-group H; that is, maps $\delta : G \to H$ such that $\delta(xy) = \delta(x)^y \cdot \delta(y)$. If H is abelian (i.e. a G-module) this set is an abelian group, with pointwise operations. When the G-action on H is trivial, $\mathrm{Der}(G, H) = \mathrm{Hom}(G, H)$. The supremum of $|\mathrm{Der}(G, H)|$ for all actions of G on the group H is denoted

$$\mathrm{der}(G, H).$$

Lemma 1.3.1 *(i) The number of complements to N in G is either zero or else equal to $|\mathrm{Der}(Q, N)|$ (for a certain action of Q on N);*
(ii)

$$\mathrm{der}(Q, N) \leq |N|^{\mathrm{d}(Q)}. \tag{1.4}$$

(iii) If N is abelian then $\mathrm{Der}(Q, N)$ is isomorphic to a subgroup of $N^{(\mathrm{d}(Q))}$ and

$$|\mathrm{Der}(Q, N)| = |N/\mathrm{C}_N(Q)| \cdot \left|H^1(Q, N)\right|. \tag{1.5}$$

(iv) If N is abelian and Q is finite then $|Q| \cdot H^1(Q, N) = 0$.
(v) If N is abelian, H is a subgroup of finite index m in Q and N has exponent coprime to m then $\left|H^1(Q, N)\right| \leq \left|H^1(H, N)\right|$.

Proof. (i) if G is a non-split extension of N by Q then there are no complements. Otherwise, G is a semi-direct product $G = N \rtimes H$, and we may identify Q with H, which acts on N by conjugation. For $\delta \in \mathrm{Der}(H, N)$ define

$$H_\delta = \{h \cdot \delta(h) \mid h \in H\}.$$

It is routine to verify that each H_δ is a complement to N in G and that $\delta \mapsto H_\delta$ is a bijection between $\mathrm{Der}(H, N)$ and the set of all complements to N.

(ii) A derivation is determined by its effect on the elements of a generating set.

(iii) Say $Q = \langle x_1, \ldots, x_d \rangle$. Then

$$\delta \mapsto (\delta(x_1), \ldots, \delta(x_d))$$

embeds $\mathrm{Der}(Q, N)$ into $N^{(\mathrm{d}(Q))}$. The first cohomology group $H^1(Q, N)$ is $\mathrm{Der}(Q, N)/\mathrm{IDer}(Q, N)$ where $\mathrm{IDer}(Q, N)$ denotes the set of inner derivations $\delta_a : x \mapsto [a, x]$ ($x \in Q$, a a fixed element of N). Now (1.5) holds because the map $a \mapsto \delta_a$ induces an isomorphism $N/\mathrm{C}_N(Q) \to \mathrm{IDer}(Q, N)$.

(iv) and (v) (Well known cohomological facts) Write N additively, and let $H \leq Q$ be as in (v). The restriction map $\mathrm{Der}(Q, N) \to \mathrm{Der}(H, N)$ induces a homomorphism $\mathrm{res} : H^1(Q, N) \to H^1(H, N)$. Put $K = \ker(\mathrm{res})$. We show that $mK = 0$. This gives (iv) if we take $H = 1$; while if $tN = 0$ then clearly $tK = 0$, so if $\gcd(t, m) = 1$ then $K = 0$, giving (v).

Now an element of K is represented by some $\delta \in \mathrm{Der}(Q, N)$ such that $\delta(H) = 0$. Let T be a transversal to the right cosets of H in Q and put

$$a = -\sum_{x \in T} \delta(x).$$

Let $y \in Q$. Then for $x \in T$ we have $xy = h_x x'$ where $h_x \in H$ and $x \mapsto x'$ is a permutation of T, so

$$\delta(xy) = \delta(h_x)^y + \delta(x') = \delta(x').$$

It follows that

$$\begin{aligned} \delta_a(y) &= \sum (\delta(x) - \delta(x)^y) = \sum \delta(x) - \sum \delta(xy) + \sum \delta(y) \\ &= \sum \delta(x) - \sum \delta(x') + m\delta(y) \\ &= m\delta(y). \end{aligned}$$

Thus $m \cdot \delta$ is the inner derivation δ_a and represents 0 in $H^1(Q, N)$. ∎

Proposition 1.3.2 *The following hold:*

(i)

$$a_n(G) \leq \sum_{t|n} a_{n/t}(Q) a_t(N) t^{\mathrm{rk}(Q)} \tag{1.6}$$

$$s_n(G) \leq s_n(Q) s_n(N) n^{\mathrm{rk}(Q)} \tag{1.7}$$

$$s_n(G) \leq s_n(Q) s_n(N) c^n \quad \textit{where} \quad c = 3^{d(Q)/3}. \tag{1.8}$$

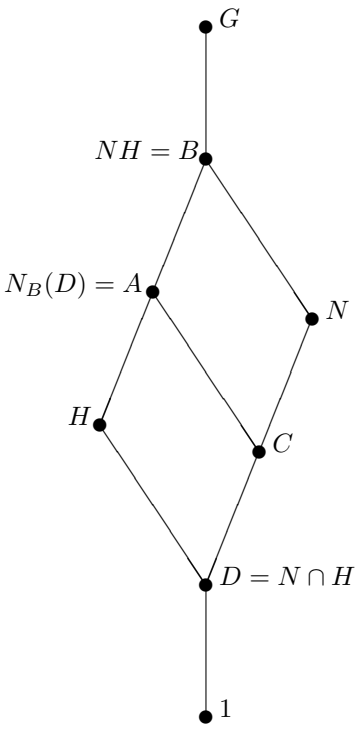
(ii) *If Q is finite then*

$$s_n(G) \le s_n(N) n^{|Q|}. \tag{1.9}$$

(iii) *If G is finite then*

$$s(G) \le s(Q) s(N) \, |N|^{\mathrm{rk}(Q)} \tag{1.10}$$

$$s(G) \le s(N) \, |G|^{\mathrm{rk}(Q)} \, . \tag{1.11}$$



Proof. Let H be a subgroup of index n in G, put $D = H \cap N$ and $B = NH$, and let $t = |N : D|$. Put $A = \mathrm{N}_B(D)$ and $C = A \cap N$. Then H/D is a complement to C/D in A/D. So for a given pair D, B the number of possibilities for H is at most

$$\mathrm{der}(A/C, C/D) \le t^{\mathrm{rk}(Q)},$$

since $|C/D| \le t$ and $A/C \cong B/N \le Q$. Given t, the number of possibilities for D is at most $a_t(N)$ and the number of possibilities for B is at most $a_{n/t}(Q)$; this gives (1.6), and (1.7) is an immediate consequence. When G is finite, this also gives (16.4.8) since $t \le |N|$, and (1.11) follows on applying (1.2) to Q (a more direct argument for (1.11) is given below).

Now put $d = d(Q)$. Keeping the above notation, note that by **Schreier's formula** ([R], **6.1.1**) we have

$$d(A/C) = d(B/N) \leq 1 + |G : B|\,(d-1) = 1 + \frac{n}{t}(d-1) \leq nd/t.$$

Hence

$$\mathrm{der}(A/C, C/D) \leq t^{nd/t} \leq 3^{nd/3},$$

since $t^{1/t} \leq 3^{1/3}$ for every $t \in \mathbb{N}$. The estimate (1.8) now follows as before.

Suppose now that $|Q| = q$ is finite. Fix n and let $D \leq N$ with $|N : D| = t \leq n$. Then fix transversals $\{x_1, \ldots, x_q\}$ to G/N and $\{y_1, \ldots, y_t\}$ to the right cosets of D in N. If H is a subgroup of G with $H \cap N = D$ then

$$H = \bigcup_{i \in S(H)} D y_{f(i)} x_i$$

for some subset $S(H)$ of $\{1, \ldots, q\}$ and some function $f : S(H) \to \{1, \ldots, t\}$. Now $|G : H| = tq/\,|S(H)|$, so if $|G : H| \leq n$ then either $t < n$ or $t = n$ and $S(H) = \{1, \ldots, q\}$. Suppose that $t < n$. Then putting $f(i) = \infty$ for each $i \notin S(H)$, we see that H is determined by a function from $\{1, \ldots, q\}$ to $\{1, \ldots, t, \infty\}$; so the number of such subgroups H is at most $(t+1)^q \leq n^q$. On the other hand, if $t = n$ then H is determined by a function from $\{1, \ldots, q\}$ to $\{1, \ldots, t\}$, so there are again at most n^q possibilities for H. Since there are $s_n(N)$ possibilities for D this gives (1.9).

Suppose finally that G is finite. If $H \leq G$ and $H \cap N = D$ then $H/D \cong HN/N \leq Q$ so H is generated by D together with at most $\mathrm{rk}(Q)$ further elements. Each of these can be chosen in at most $|G|$ ways, and (1.11) follows. ■

In part (iii) of the last proposition we bounded $s(G)$ in terms of $s(N)$ and $\mathrm{rk}(Q)$. In some circumstances it is also possible, though harder, to give a bound in terms of $s(Q)$ and $\mathrm{rk}(N)$:

Proposition 1.3.3 *Suppose that G is finite and that N is soluble, of derived length l and rank r. Then*

$$s(G) \leq s(Q)\,|N|^{3r^2+lr}\,|Q|^{lr} \leq s(Q)\,|G|^{3r^2+lr}.$$

This depends on

Lemma 1.3.4 *If Q is finite and A is a finite Q-module of (additive) rank r then*

$$\left|H^1(Q, A)\right| < |A|^{3r^2-1}\,|Q|^r.$$

Proof. Put $G = A \rtimes Q$. For each prime p let Q_p be a Sylow p-subgroup of Q and let A_p denote the p-component of A. Then

$$H^1(Q, A) \cong \bigoplus H^1(Q, A_p)$$

and Lemma 1.3.1(v) shows that $\left|H^1(Q, A_p)\right| \leq \left|H^1(Q_p, A_p)\right|$ for each p; so our claim will follow if it holds with A, Q replaced by A_p, Q_p. Thus we may assume that both A and Q are p-groups.

Put $C = \mathrm{C}_G(A)$. To each complement H to A in G associate the subgroup $D_H = H \cap C$. Each such D_H is a complement to A in C, so the number of possibilities for D_H is at most

$$\begin{aligned} |\mathrm{Der}(C/A, A)| &= |\mathrm{Hom}(C/A, A)| = \left|\mathrm{Hom}(\overline{C}, A)\right| \\ &= \left|\mathrm{Hom}(A, \overline{C})\right| \\ &\leq \left|\overline{C}\right|^r \leq |Q|^r , \end{aligned}$$

where $\overline{C} = C/AC'$. Having fixed $D_H = D$, put $R = \mathrm{N}_G(D)$ and $S = R \cap C = \mathrm{N}_C(D)$. Now $R/S \cong G/C$ acts faithfully by conjugation on A; it follows that

$$\mathrm{rk}(R/S) \leq 5(r^2 - r)/2 < 3r^2 - 1$$

($\hookrightarrow$ **Pro-p groups**, Proposition 13). Hence

$$|\mathrm{Der}(R/S, S/D)| \leq |S/D|^{3r^2-1} \leq |A|^{3r^2-1} .$$

But H/D is a complement to S/D in R/D, so this bounds the number of possibilities for H with $D_H = D$. The result follows since $\left|H^1(Q, A)\right| \leq |\mathrm{Der}(Q, A)|$ which is exactly the number of such complements H. ∎

We now complete the

Proof of Proposition 1.3.3. Suppose first that N is abelian. To each subgroup H of G associate the pair of groups $D_H = H \cap N$, $G_H = NH$. The number of possibilities for G_H is $s(G/N) = s(Q)$, and the number of possibilities for D_H is $s(N) \leq |N|^r$. Now H/D_H is a complement to N/D_H in G_H/D_H, so given $G_H = R$ and $D_H = D$, the number of possibilities for H is

$$\begin{aligned} |\mathrm{Der}(R/N, N/D)| &\leq |N/D| \cdot \left|H^1(R/N, N/D)\right| \\ &\leq |N/D| \cdot |N/D|^{3r^2-1} |R/N|^r \\ &\leq |N|^{3r^2} |Q|^r , \end{aligned}$$

by Lemma 1.3.4. Thus

$$s(G) \leq s(Q) |N|^{3r^2+r} |Q|^r$$

when N is abelian.

Now suppose that N has derived length $l > 1$, and let A be the $(l-1)$th term of the derived series of N. Inductively we may suppose that

$$s(G/A) \leq s(Q) |N/A|^{3r^2+(l-1)r} |Q|^{(l-1)r} .$$

Applying the first case with A, G/A in place of N, Q we now obtain

$$\begin{aligned} s(G) &\le s(G/A)\,|A|^{3r^2+r}\,|G/A|^r \\ &\le s(Q)\cdot|N/A|^{3r^2+(l-1)r}\cdot|A|^{3r^2+r}\cdot|G/A|^r\cdot|Q|^{(l-1)r} \\ &= s(Q)\cdot|N/A|^{3r^2+lr}\cdot|A|^{3r^2+r}\cdot|Q|^{lr} \\ &\le s(Q)\,|N|^{3r^2+lr}\,|Q|^{lr} \end{aligned}$$

as required.

An analogous result, using the Fitting length instead of the derived length of N, is established in §10.4; however in that case the proof depends on CFSG.

It is sometimes useful to have a bound for the number of *supplements* to N in G, that is, subgroups H such that $NH = G$. If in the above proof we count only subgroups H for which $G_H = G$, the factor $s(Q)$ gets replaced by 1, and essentially the same argument gives

Corollary 1.3.5 *Suppose that G is finite and that N is soluble, of derived length l and rank r. Then the number of supplements to N in G is at most $|G|^{3r^2+lr}$.*

When counting normal subgroups the following variations on (1.7) can be useful:

Proposition 1.3.6 *Put*

$$\begin{aligned} \mathcal{Z}_n(N) &= \{\mathrm{Z}(N/D) \mid D \le N,\, D \lhd G,\, |N:D| \le n\}, \\ z_n(N) &= \sup\{|Z| \mid Z \in \mathcal{Z}_n(N)\}, \\ \delta_n(N) &= \sup\{\mathrm{rk}(Z) \mid Z \in \mathcal{Z}_n(N)\}. \end{aligned}$$

Then

$$s_n^{\lhd}(G) \le s_n^{\lhd}(Q)s_n^{\lhd}(N)z_n(N)^{\mathrm{rk}(Q)} \le s_n^{\lhd}(Q)s_n^{\lhd}(N)n^{\mathrm{rk}(Q)}$$

and

$$s_n^{\lhd}(G) \le s_n^{\lhd}(Q)^2 s_n^{\lhd}(N)z_n(N)^{\delta_n(N)}.$$

Proof. To each $H \lhd G$ with $|G:H| \le n$ we associate the pair

$$X = NH,\ D = N \cap H. \tag{1.12}$$

The number of possibilities for such a pair is at most $s_n^{\lhd}(Q)s_n^{\lhd}(N)$. Having fixed the pair (X, D), let $\mathcal{H}$ denote the set of $H \lhd G$ such that (1.12) holds, and put $Z/D = \mathrm{Z}(N/D)$. It will suffice now to show that $|\mathcal{H}|$ is bounded above by both

$$|Z|^{\mathrm{rk}(Q)} \quad \text{and} \quad s_n^{\lhd}(Q)\,|Z|^{\mathrm{rk}(Z)}.$$

To do so we may factor out D and so assume that $D = 1$. Then $X = N \times H$ for each $H \in \mathcal{H}$. Now fix one $B \in \mathcal{H}$. Then any $H \in \mathcal{H}$ takes the form

$$H = \{b \cdot f(b) \mid b \in B\}$$

where $f : B \to N$ is a homomorphism with $f(B) \leq Z$. Since $d(B) = d(X/N) \leq \mathrm{rk}(Q)$ the number of such homomorphisms is at most $|Z|^{\mathrm{rk}(Q)}$, giving the first bound. For the second, note that the kernel of f is just $B \cap H$ which is normal in G, and as

$$X/(N \cdot \ker f) \cong B/\ker f \cong f(B)$$

it follows that $K = N \cdot \ker f$ is a normal subgroup of index at most n in G. There are at most $s_n^{\triangleleft}(Q)$ possibilities for such a K. Having fixed K, we have $\ker f = B \cap K$, and the number of possibilities for f is at most the number of monomorphisms from $B/(B \cap K)$ into Z. If there is at least one then $d(B/(B \cap K)) \leq \mathrm{rk}(Z)$, so in any case their number is at most $|Z|^{\mathrm{rk}(Z)}$, whence the second bound. ■

1.4 Nilpotent and soluble groups

For nilpotent groups a sharper version of Lemma 1.2.2 holds:

Lemma 1.4.1 *If G is nilpotent then for each $n > 1$*

$$a_n(G) < n^{\mathrm{rk}(G)}, \tag{1.13}$$

$$s_n(G) < n^{1+\mathrm{rk}(G)}. \tag{1.14}$$

Proof. If G has infinite rank there is nothing to prove. Otherwise, we may assume that G is finite. Let p be a prime. Then every subgroup of index p in G is normal, so is the kernel of some epimorphism $G \to C_p$. Since $d(G) \leq \mathrm{rk}(G) = r$ there are at most $p^r - 1$ such epimorphisms, and so $a_p(G) < p^r$. Now let $n > 1$. Then $n = pm$ for some prime p, and every subgroup of index n in G is contained in some subgroup M of index p in G. Arguing by induction on n we may suppose that $a_m(M) \leq m^r$. It follows that

$$\begin{aligned} a_n(G) &\leq a_p(G) \cdot \max_{|G:M|=p} a_m(M) \\ &< p^r m^r = n^r. \end{aligned}$$

This proves (1.13), and (1.14) follows. ■

Combining this with Proposition 16.4.8 we obtain a large family of groups with polynomial subgroup growth:

Proposition 1.4.2 *Suppose that the group G has a chain of subgroups*

$$1 = G_k \lhd G_{k-1} \lhd \cdots \lhd G_0 \lhd G$$

where G_{i-1}/G_i is nilpotent of rank r_i for $i = 1, \ldots, k$ and $|G/G_0| = m$ is finite. Then

$$s_n(G) \leq n^{m+k+\sum r_i}.$$

Proof. Put $s_i = r_{i+1} + \cdots + r_k$ for $0 \leq i < k$. From (1.13) we have $a_n(G_{k-1}) \leq n^{r_k} = n^{s_{k-1}}$. Let $i < k$ and suppose inductively that $a_n(G_i) \leq n^{s_i+k-i-1}$ for each n. Then (1.6) and (1.13) give

$$\begin{aligned} a_n(G_{i-1}) &\leq \sum_{t|n} a_{n/t}(G_{i-1}/G_i)a_t(G_i)t^{r_i} \\ &\leq \sum_{t|n} (n/t)^{r_i} \cdot t^{s_i+k-i-1} \cdot t^{r_i} \\ &= n^{r_i} \sum_{t|n} t^{s_i+k-i-1} \leq n^{s_{i-1}+k-i}. \end{aligned}$$

It follows by induction that $a_n(G_0) \leq n^{s_0+k-1}$ for each n, and hence that $s_n(G_0) \leq n^{s_0+k}$. An application of (1.9) now concludes the proof. ■

Corollary 1.4.3 *If G is a virtually soluble group of finite rank then there exists a constant α such that $s_n(G) \leq n^\alpha$ for all n.*

The *converse* of this result will be the main result of Chapter 5.

From the arithmetical point of view, the key fact about nilpotent groups is

Proposition 1.4.4 *Let G be a nilpotent group. If $n = \prod p^{e(p)}$ (with distinct primes p) and $a_n(G)$ is finite then*

$$a_n(G) = \prod a_{p^{e(p)}}(G).$$

Proof. Replacing G by a suitable finite quotient, we may assume that G is finite. Then $G = P_1 \times \cdots \times P_k$ where $P_1, \ldots, P_k$ are the distinct Sylow subgroups of G. The result now follows because each subgroup H of G is of the form $(H \cap P_1) \times \cdots \times (H \cap P_k)$. ■

1.5 Abelian groups I

For certain abelian groups it is possible to estimate the subgroup growth with some precision.

Proposition 1.5.1 *If p is a prime then*

$$\left(1 - \frac{1}{p^d}\right) p^{k(d-1)} \leq a_{p^k}(\mathbb{Z}^{(d)}) \leq \left(1 + \frac{1}{p-1}\right)^d p^{k(d-1)}$$

for all $k \geq 0$.

Proof. Suppose

$$a_{p^k}(\mathbb{Z}^{(d)}) = f(d,k)p^{k(d-1)}$$

for all d and k. Then $f(1,k) = 1$ for all k. Now let $d > 1$. Taking $N = \mathbb{Z}$ and $Q = \mathbb{Z}^{(d-1)}$ in (1.6) gives

$$\begin{aligned} p^{k(d-1)} f(d,k) = a_{p^k}(\mathbb{Z}^{(d)}) &\le \sum_{i=0}^{k} a_{p^i}(\mathbb{Z}^{(d-1)}) \cdot 1 \cdot p^{(k-i)(d-1)} \\ &= \sum_{i=0}^{k} f(d-1,i) p^{i(d-2)} \cdot p^{(k-i)(d-1)} \\ &= p^{k(d-1)} \sum_{i=0}^{k} f(d-1,i) \cdot p^{-i}. \end{aligned} \tag{1.15}$$

Supposing inductively that $f(d-1,i) \le (p/(p-1))^{d-1}$ for all i we deduce that

$$f(d,k) < \left(\frac{p}{p-1}\right)^{d-1} \sum_{i=0}^{\infty} p^{-i} = \left(\frac{p}{p-1}\right)^{d}.$$

This establishes the second inequality.

On the other hand, $\mathbb{Z}^{(d)}$ has p^{kd} homomorphisms into the cyclic group C_{p^k}, and hence $p^{kd} - p^{(k-1)d}$ epimorphisms onto C_{p^k}. The number of epimorphisms with a given kernel is $\left|\mathrm{Aut}(C_{p^k})\right| < p^k$; it follows that the number of distinct such kernels is at least $(p^{kd} - p^{(k-1)d})p^{-k}$. This implies the first inequality. ∎

It is worth mentioning that the above calculation gives an exact recursive formula for $f(d,k)$, because in the present case the inequality in (1.15) is actually an equality, as is clear from the proof of (1.6). This formula is elegantly summed up in the generating function identity

$$\sum_{n=0}^{\infty} a_{p^n}(\mathbb{Z}^{(d)}) X^n = \prod_{j=0}^{d-1} \frac{1}{1 - p^j X};$$

see Chapter 15.

The analogous estimate for elementary abelian groups, stated next, is the single most frequently used result in our subject. To state it, for each prime p we define the constant $\kappa(p)$ by

$$\kappa(p) = \prod_{i=1}^{\infty} (1 - p^{-i})^{-1}.$$

We also put

$$\begin{bmatrix} d \\ r \end{bmatrix}_p = \frac{(p^d - 1)(p^d - p) \dots (p^d - p^{r-1})}{(p^r - 1)(p^r - p) \dots (p^r - p^{r-1})}.$$

Note that $1 < \kappa(p) < 4$ for every p, and that $\kappa(p) \to 1$ as $p \to \infty$. Note also that

$$\begin{bmatrix} d \\ r \end{bmatrix}_p = \begin{bmatrix} d \\ d-r \end{bmatrix}_p.$$

Proposition 1.5.2 *Let $A = C_p^{(d)}$. Then for $1 \leq r < d$,*

$$\kappa(p)p^{r(d-r)} > a_{p^r}(A) = \begin{bmatrix} d \\ r \end{bmatrix}_p > p^{r(d-r)}.$$

$$(d+1)\kappa(p)p^{d^2/4} > s(A) > p^{[d^2/4]}. \tag{1.16}$$

Proof. Think of A as a d-dimensional vector space over $\mathbb{F}_p$. Now $\begin{bmatrix} d \\ r \end{bmatrix}_p$ is the number of linearly independent r-tuples in A divided by the number of distinct bases in any r-dimensional subspace, so $\begin{bmatrix} d \\ r \end{bmatrix}_p$ is equal to the number of r-dimensional subspaces in $\mathbb{F}_p^{(d)}$. By duality, this is the same as the number of subspaces of codimension r, which is $a_{p^r}(A)$. The two inequalities in the first line then follow from the fact that

$$\frac{p^{d-r}}{1-p^{-(r-i)}} > \frac{p^d - p^i}{p^r - p^i} > p^{d-r}$$

for $0 \leq i < r < d$. For the final inequality, note that $s(A) > a_{p^{d/2}}(A)$ when d is even, $s(A) > a_{p^{(d+1)/2}}(A)$ when d is odd. ■

The proof of the lower bound carries over without difficulty to homocyclic groups of prime-power exponent:

Proposition 1.5.3 *Let $A = C_{p^n}^{(d)}$ where $n \geq 1$. Then for $1 \leq r < d$ we have*

$$a_{p^{nr}}(A) > p^{nr(d-r)}.$$

Proof. Let us call a k-tuple of elements of A *independent* if it generates a subgroup isomorphic to $C_{p^n}^{(k)}$. A simple counting arument shows that the number of independent k-tuples in $A = C_{p^n}^{(d)}$ is

$$q(d,k) = \prod_{i=0}^{k-1} \left(p^{nd} - p^{(n-1)d+i} \right).$$

It follows that the number of subgroups isomorphic to $C_{p^n}^{(k)}$ is given by

$$\frac{q(d,k)}{q(k,k)} > p^{n(d-k)k}$$

if $1 \leq k < d$. The result follows on taking $k = d - r$. ■

1.6 Finite p-groups

Proposition 1.5.2 can be used to deduce an upper bound valid in every finite p-group:

Proposition 1.6.1 *Let G be a group of order p^d. Then for $1 \leq r \leq d$,*

$$a_{p^r}(G) < \kappa(p)p^{r(d-r)}.$$

Note that this is sharper than Lemma 1.4.1 only when $r > d - \mathrm{rk}(G)$.

Proof. We prove this in two ways, illustrating different techniques.

(1) By the preceding result, it suffices to show that G has at most as many subgroups of index p^r as does the elementary abelian group A of the same order, and we prove this by induction on d. Let Z be a central subgroup of order p in G. Then

$$\begin{aligned} a_{p^r}(G) &= a_{p^r}(G/Z) + \sum_K \varepsilon(K)\,|\mathrm{Hom}(K/Z, Z)| \\ &= a_{p^r}(G/Z) + \sum_K \varepsilon(K) p^{\mathrm{d}(K/Z)} \\ &\le a_{p^r}(G/Z) + a_{p^{r-1}}(G/Z) p^{d-r} \end{aligned}$$

where K runs over all subgroups of G containing Z with $|G:K| = p^{r-1}$, and $\varepsilon(K) = 1$ if Z has a complement in K, $\varepsilon(K) = 0$ otherwise. Similarly, taking Y to be a subgroup of order p in A we have

$$\begin{aligned} a_{p^r}(A) &= a_{p^r}(A/Y) + \sum_K \varepsilon(K) p^{\mathrm{d}(K/Y)} \\ &= a_{p^r}(A/Y) + a_{p^{r-1}}(A/Y) p^{d-r}, \end{aligned}$$

where K runs over all subgroups of A containing Y with $|G:K| = p^{r-1}$, and $\varepsilon(K)$ is defined analogously, so $\varepsilon(K) = 1$ for every K in this case. The result now follows by the inductive hypothesis.

(2) We adapt the argument of the elementary abelian case. Let $n \le d$ and let H be a group of order p^n with $\mathrm{d}(H) = m$. The number of n-tuples of elements that generate $H/\Phi(H)$ is at least

$$(p^m - 1)(p^m - p)\dots(p^m - p^{m-1})p^{m(n-m)} > \kappa(p)^{-1} p^{nm}.$$

Each of these corresponds to $|\Phi(H)|^n = p^{n(n-m)}$ generating n-tuples for H, so H has more than $\kappa(p)^{-1}p^{n^2}$ ordered generating sets of size n. Now the number of n-tuples of elements in G is p^{dn}; consequently the number of subgroups of order p^n in G is less than

$$\frac{p^{dn}}{\kappa(p)^{-1}p^{n^2}} = \kappa(p) p^{(d-n)n}.$$

This gives the result on putting $n = d - r$. ∎

If G is a p-group with $d(G) = d < \infty$ then $G/\Phi(G)$ is isomorphic to $\mathbb{F}_p^{(d)}$, and so for $1 \le r \le d$ we have

$$a_{p^r}(G) \ge a_{p^r}(\mathbb{F}_p^{(d)}) = \begin{bmatrix} d \\ r \end{bmatrix}_p \ge p^{r(d-r)}, \tag{1.17}$$

in particular

$$a_p(G) \ge p^{d-1}. \tag{1.18}$$

Since every subgroup of index p in G contains $\Phi(G)$, we also have

$$a_p(G) = \frac{p^d - 1}{p - 1} < \frac{p}{p-1} \cdot p^{d-1} = p^{d-\mu(p)} \tag{1.19}$$

where

$$\mu(p) = \frac{\log(p-1)}{\log p};$$

note that $0 < \mu(p) < 1$ and that $\mu(p) \to 1$ as $p \to \infty$.

Now let

- $d_n(G) = \max\{d(H) \mid H \text{ a subgroup of } G \text{ of index } p^n\}$
- $d_n^*(G) = \sum_{i=0}^{n} d_i(G)$
- $\delta_n(G) = \min\{d(H) \mid H \text{ a subgroup of } G \text{ of index } p^n\}$

Proposition 1.6.2 *Let G be a finite p group. Then for each $n \geq 1$ we have*

$$p^{d_{n-1}(G)-1} \leq a_{p^n}(G) \leq p^{d^*_{n-1}(G)-n\mu(p)}, \tag{1.20}$$

$$a_{p^n}(G) \geq \prod_{i=1}^{n} \frac{p^{\delta_{i-1}(G)} - 1}{p^i - 1}. \tag{1.21}$$

Proof. (1.20): Let H be a subgroup of index p^{n-1} with $d(H) = d_{n-1}(G)$. Applying (1.18) to H gives the first inequality in (1.20). For the second, note that every subgroup H of G of index p^n is part of a chain

$$H = H_n < H_{n-1} < H_{n-2} < \cdots < H_1 < H_0 = G \tag{1.22}$$

with $|G : H_i| = p^i$ for each i. By (1.19), H_i has at most $p^{d_i(G)-\mu(p)}$ subgroups of index p, so given H_i this is an upper bound for the number of possibilities for H_{i+1}. It follows that the number of possibilities for $H = H_n$ is at most

$$\prod_{i=0}^{n-1} p^{d_i(G)-\mu(p)} = p^{d^*_{n-1}(G)-n\mu(p)}.$$

(1.21): Write $k_n = a_{p^n}(G)$. Now let $n \geq 1$. Each subgroup of index p^{n-1} in G has at least $(p^{\delta_{n-1}(G)} - 1)/(p-1)$ subgroups of index p. On the other hand, if H is a subgroup of index p^n in G then the number of subgroups of index p^{n-1} that contain H is at most $(p^n - 1)/(p - 1)$: for each of them corresponds to a subgroup of order p in the group $\mathrm{N}_G(H)/H$, which has order at most p^n. It follows that

$$k_n \geq \frac{(p^{\delta_{n-1}(G)} - 1)/(p-1)}{(p^n - 1)/(p-1)} \cdot k_{n-1},$$

and as $k_0 = 1$ this gives (1.21). ■

Remark Proposition 1.6.2 applies without change to every *finitely generated pro-p group*, since all of the invariants $a_{p^n}(G)$, $d_n(G)$, $d_n^*(G)$ and $\delta_n(G)$ can be detected in a suitable finite quotient of a pro-p group G.

1.7 Sylow's theorem

Another method for counting subgroups in finite groups uses Sylow subgroups, to reduce to the p-group situation.

Lemma 1.7.1 *Let G be a finite soluble group. If $n = p_1^{e_1} \dots p_k^{e_k}$ where $p_1, \dots, p_k$ are distinct primes, then*

$$a_n(G) \leq n \cdot \prod_{i=1}^{k} a_{p_i^{e_i}}(P_i)$$

where for each i, P_i is a Sylow p_i-subgroup of G.

Proof. We may assume that n divides $|G|$, since otherwise $a_n(G) = 0$. According to Hall's theory of Sylow systems (↬ **Finite group theory**, §1), G has a family of Sylow p_i-subgroups P_i, one for each of the primes $p_1, \dots, p_m$ dividing $|G|$, with the following property: for every subgroup H of G there exists $x \in G$ such that

$$H^x = (H^x \cap P_1) \dots (H^x \cap P_m).$$

Now suppose that $|G : H| = n$. Then $|H^x \cap P_i|$ is the p_i-part of $|H^x| = |H| = g/n$, and so $|P_i : H^x \cap P_i| = p_i^{e_i}$ (where $e_i = 0$ if $i > k$). The number of possibilities for $H^x \cap P_i$ is therefore at most $a_{p_i^{e_i}}(P_i)$, and so the number of possibilities for H^x is at most $\prod_{i=1}^{m} a_{p_i^{e_i}}(P_i)$. The result follows since H is one of the $|G : \mathrm{N}_G(H^x)| \leq |G : H| = n$ conjugates of H^x, and $a_{p_i^{e_i}}(P_i) = 1$ for each $i > k$. ■

Corollary 1.7.2 *Let G be a finite soluble group and put $r = \max\{\mathrm{r}_p(G) \mid p \text{ prime}\}$. Then*

$$a_n(G) \leq n^{1+r},$$
$$s_n(G) \leq n^{2+r}$$

for every n.

Proof. Keep the above notation. Lemma 1.4.1 shows that

$$a_{p_i^{e_i}}(P_i) \leq p_i^{re_i}$$

for each i. The first claim now follows from the preceding lemma, and the second is an immediate consequence. ■

This provides an alternative approach to Corollary 1.4.3; it has the advantage of being truly 'local', depending only on the finite quotients of the group and not on its global structure:

Corollary 1.7.3 *Let G be a group such that every finite quotient of G is soluble of rank at most r. Then*

$$s_n(G) \leq n^{2+r}$$

for all n.

A similar argument yields a slightly weaker estimate for an arbitrary finite group:

Proposition 1.7.4 *Let G be a finite group. If $n = p_1^{e_1} \dots p_k^{e_k}$ where $p_1, \dots, p_k$ are distinct primes, then*

$$a_n(G) \leq n^k \cdot \prod_{i=1}^{k} a_{p_i^{e_i}}(P_i)$$

where for each i, P_i is a Sylow p_i-subgroup of G.

Proof. Let H be a subgroup of index n in G. For each i, H has a Sylow p_i-subgroup of the form $H \cap P_i^{x_i}$ with $x_i \in G$. Given x_i, the number of possibilities for $H \cap P_i^{x_i}$ is at most $a_{p_i^{e_i}}(P_i^{x_i})$; so the number of k-tuples of the form

$$(H \cap P_1^{x_1}, \dots, H \cap P_k^{x_k})$$

for a given k-tuple $\mathbf{x} = (x_1, \dots, x_k)$ is at most

$$\prod_{i=1}^{k} a_{p_i^{e_i}}(P_i).$$

The number of such k-tuples $\mathbf{x}$ is at most $|G|^k$; but if $\mathbf{x}$ corresponds to H as as above then so does the k-tuple $(x_1 h_1, \dots, x_k h_k)$ for any $h_1, \dots, h_k \in H$, so the number of k-tuples corresponding to distinct subgroups of index n in G is at most $|G|^k / |H|^k = n^k$. The result follows since H is generated by its Sylow subgroups $H \cap P_i^{x_i}$ $(i = 1, \dots, k)$. ■

Corollary 1.7.5 *Let $|G| = p_1^{b_1} \dots p_t^{b_t}$ where $p_1, \dots, p_t$ are distinct primes, and put $b = \max\{b_i \mid 1 \leq i \leq t\}$, $r = \max\{\mathrm{r}_{p_i}(G) \mid 1 \leq i \leq t\}$. Then*

$$a_n(G) \leq n^{\nu(n)+r} \leq n^{t+r} \leq n^{t+b} \leq n^{2\log|G|}$$

for each n, where $\nu(n)$ denotes the number of distinct prime divisors of n.

The first inequality follows on applying Lemma 1.4.1 to each P_i, and the remaining inequalities are clear (we may assume that $n \mid |G|$ since $a_n(G) = 0$ otherwise).

As an exercise, the reader can generalise this argument to show that G has at most $n^{2\log g} = g^{2\log n}$ subgroups of index n containing a given subgroup U of index g in G (the proposition above being the case $U = 1$). This is sharper than Lemma 1.2.3 when $n < g^{1/3}$.

1.8 Restricting to soluble subgroups

Write

$$\mathrm{sol}(G),\ \mathrm{nil}(G)$$

for the number of *soluble subgroups*, respectively *nilpotent subgroups* of G. The following is useful for estimating the total number of subgroups in a finite group.

Proposition 1.8.1 *Let G be a finite group.*

(i) $s(G) \leq |G| \cdot \mathrm{sol}(G)$.

(ii) *Let l be the maximal Fitting height of any soluble subgroup of G. Then*

$$s(G) \leq \mathrm{nil}(G)^{l+1}.$$

Proof. It is proved in [Aschbacher & Guralnick 1982] that every finite group can be generated by a soluble subgroup together with one further element. This immediately implies (i) (though easy to use, this hardly counts as an elementary result, since the theorem of Aschbacher and Guralnick is an application of CFSG).

Now let H be a finite soluble group of Fitting height l. We claim that H is equal to a product of l nilpotent subgroups. If $l = 1$ then H is nilpotent and the claim is trivial. Suppose that $l > 1$. Then H has a normal subgroup K of Fitting height $l - 1$ such that H/K is nilpotent, and then $H = KC$ where C is any Carter subgroup of H ($\leadsto$ **Finite group theory**). The claim now follows by induction.

In the situation of (ii), it now follows (with the theorem quoted above) that every subgroup of G is generated by at most l nilpotent subgroups together with one cyclic subgroup, so we have (ii). ■

A similar argument combined with Corollary 1.7.2 gives

Proposition 1.8.2 *Let G be a finite group and put $r = \max\{\mathrm{r}_p(G) \mid p \text{ prime}\}$. Then*

$$s_n(G) \leq |G|^b \, n^{2+r}$$

for every n, where b is an absolute constant.

Proof. This depends on the following theorem of [Borovik, Pyber & Shalev 1996]: *the number of maximal soluble subgroups of G is at most $|G|^c$*, where c is an absolute constant. If H is a subgroup of index at most n in G then $H = \langle S, x\rangle$ for some soluble subgroup S and some $x \in G$, by the theorem of Aschbacher and Guralnick; without loss of generality $S = H \cap T$ where T is a maximal soluble subgroup of G, and then $|T : S| \leq n$. There are at most $|G|^c$ choices for T, and given T there are at most n^{2+r} possibilitites for S, by Corollary 1.7.2. The result follows, with $b = c + 1$. (Borovik, Pyber and Shalev conjecture that $c = 1$ will do; if this is correct, we can take $b = 2$ in the proposition.) ■

1.9 Applications of the 'minimal index'

We have applied Proposition 16.4.8 to soluble groups in several of the above results. It is also useful for dealing with groups having non-abelian composition factors. Denote by

$$\mu(G)$$

the *minimal index of a proper subgroup of* G; of course $\mu(G) = |G|$ if G is cyclic of prime order, but there are also good lower bounds for $\mu(G)$ when G is a non-abelian simple group.

Proposition 1.9.1 *Suppose that* $1 = G_k \lhd G_{k-1} \lhd \ldots \lhd G_0 = G$. *Put* $Q_i = G_{i-1}/G_i$ *and suppose that*

$$\mu(Q_i)^c \geq |Q_i|$$
$$\mathrm{rk}(Q_i) \leq r$$

for each i, *where* $(c-1)r \geq 2$. *Then for every* n,

$$s_n(G) \leq n^{kcr}.$$

Proof. Put $Q = Q_1$. If $s_t(Q) > 1$ then $t \geq \mu(Q) \geq |Q|^{1/c}$, so for every $t \geq 1$ we have

$$s_t(Q) \leq |Q|^r \leq t^{cr}.$$

This gives the result if $k = 1$. Now suppose $k > 1$ and argue by induction. Then (1.6) gives

$$\begin{aligned}
a_n(G) &\leq \sum_{t|n} a_{n/t}(Q) a_t(G_1) t^{\mathrm{rk}(Q)} \\
&\leq a_n(G_1) n^r + \sum_{t \leq n/2} a_{n/t}(Q) a_t(G_1) t^r \\
&\leq n^{(k-1)cr+r} + \sum_{t \leq n/2} (n/t)^{cr} t^{(k-1)cr} t^r \\
&= n^{(k-1)cr+r} + n^{cr} \sum_{t \leq n/2} t^{(k-2)cr+r} \\
&\leq n^{(k-1)cr+r} + n^{cr} \cdot \frac{n}{2} \cdot n^{(k-2)cr+r} \\
&\leq n^{kcr-1}
\end{aligned}$$

for each $n \geq 2$, since $1 + n/2 \leq n$ and $(k-1)cr + r + 1 \leq kcr - 1$. The result follows. ■

Corollary 1.9.2 *Let* G *be a direct product of non-abelian simple groups. Then*

$$s_n(G) \leq n^\alpha$$

for all n, *where* α *depends only on* $\mathrm{rk}(G)$.

Proof. This depends on the classification of finite simple groups, which implies that for any simple group Q of rank at most r we have $\mu(Q)^c \geq |Q|$, where c depends only on r ($\leadsto$ **Simple groups**). If G is a product of k simple groups then G contains an elementary abelian 2-subgroup of rank k (since every non-abelian simple group has even order), so $k \leq \mathrm{rk}(G)$. The above proposition now gives the result, with $\alpha = c \cdot \mathrm{rk}(G)^2$. ■

1.10 Abelian groups II

The material of this section will only be needed in Chapter 10.

A convenient estimate for the number of subgroups in a general finite abelian group A is provided by the size of the endomorphism ring $\mathrm{End}(A)$, as shown in the next proposition. We shall frequently use the fact that

$$\mathrm{Hom}(\bigoplus A_i, \bigoplus B_j) \cong \bigoplus_{i,j} \mathrm{Hom}(A_i, B_j). \tag{1.23}$$

In particular, this implies that if $A \cong \bigoplus C_{m_i}$ and $B \cong \bigoplus C_{n_j}$ then

$$\begin{aligned} |\mathrm{Hom}(A,B)| &= \prod_{i,j} \gcd(m_i, n_j) \\ &= |\mathrm{Hom}(B,A)|\,. \end{aligned} \tag{1.24}$$

We also need

Lemma 1.10.1 *If $n \mid |A| = a$ then $a_n(A) = a_{a/n}(A)$.*

This follows from the duality between A and $A^* = \mathrm{Hom}(A, \mathbb{C}^*)$.

Now we can establish

Proposition 1.10.2 *Let A be any finite abelian group. Then*

$$s(A) \le |\mathrm{End}(A)|\,. \tag{1.25}$$

$$s(A)^4 \ge |A|^{-1} |\mathrm{End}(A)| \tag{1.26}$$

Remark. Using a more delicate argument involving Hall polynomials, [Goldfeld, Lubotzky & Pyber] establish the sharper bounds

$$|A|^{-1} |\mathrm{End}(A)|^{\frac{1}{4}} \le s(A) \le |A|^2 |\mathrm{End}(A)|^{\frac{1}{4}}\,.$$

Proof of Proposition 1.10.2. The first claim (1.25) holds because every subgroup of A is the kernel of at least one endomorphism of A.

To prove (1.26), write $A = B \oplus C$ where $C \cong C_m$ and m is the exponent of A, and suppose inductively that (1.26) holds with B in place of A. Then (1.23) gives

$$\begin{aligned} |\mathrm{End}(A)| &= |\mathrm{End}(B)| \cdot |B|^2 \cdot |C| \\ &\le s(B)^4 |B|^3 |C| \\ &= (|B|\, s(B)^2)^2 \cdot |A|\,. \end{aligned}$$

So it will suffice to establish that

$$|B|\, s(B)^2 \le s(A)^2. \tag{1.27}$$

Now for each subgroup L of index n in B there exist $|\mathrm{Hom}(C, B/L)| = n$ subgroups H of A such that $H \cap B = L$ and $H + B = A$, so we have

$$a_n(A) \geq n a_n(B).$$

Put $b = |B|$. With Lemma 1.10.1 this gives

$$\begin{aligned} 2s(A) &\geq 2\sum_{n|b} a_n(A) \\ &\geq \sum_{n|b} n a_n(B) + \sum_{n|b} n a_{b/n}(B) \\ &= \sum_{n|b} a_n(B)(n + b/n) \geq 2\sqrt{b}s(B) \end{aligned}$$

since $n + b/n - 2\sqrt{b} = (\sqrt{n} + \sqrt{b/n})^2 \geq 0$. This implies (1.27), and so completes the proof of (1.26).

We shall use this result in conjunction with the following estimates for the number of endomorphisms.

Lemma 1.10.3 *Let A and B be finite abelian groups. Then*

$$|\mathrm{Hom}(A, B)|^2 \ \textit{divides}\ |\mathrm{End}(A)| \cdot |\mathrm{End}(B)|\,.$$

Proof. Assume first that A and B are p-groups, of types $(e_1, \ldots, e_r)$ and $(f_1, \ldots, f_s)$ respectively. Using (1.24) we see that the statement is equivalent to

$$2\sum \min(e_i, f_j) \leq \sum \min(e_i, e_m) + \sum \min(f_j, f_n). \tag{1.28}$$

Suppose without loss of generality that $e_1 \leq e_2 \leq \ldots \leq e_r$ and that $f_1 \leq f_2 \leq \ldots \leq f_s$, and argue by induction on $r + s$. Now the right-hand side of (1.28) is equal to

$$\begin{aligned} &\sum_{i,m<r} \min(e_i, e_m) + \sum_{j,n<s} \min(f_j, f_n) + e_r + f_s + 2\sum_{i<r} e_i + 2\sum_{j<s} f_j \\ &\qquad \geq 2\sum_{i<r, j<s} \min(e_i, f_j) + e_r + f_s + 2\sum_{i<r} e_i + 2\sum_{j<s} f_j \end{aligned} \tag{1.29}$$

by inductive hypothesis. The left-hand side of (1.28) is equal to

$$2\sum_{i<r, j<s} \min(e_i, f_j) + 2\min(e_r, f_s) + 2\sum_{i<r} \min(e_i, f_s) + 2\sum_{j<s} \min(e_r, f_j).$$

Term by term this is is less than or equal to to (1.29); so (1.28) is true, and the lemma holds for p-groups.

The general case follows on applying (1.23) to the primary components of A and B. (For a different, algebraic, proof see [Segal & Shalev 1997], Lemma 4.1.) ■

Corollary 1.10.4

$$\left|\mathrm{End}(\bigoplus_{i=1}^{k} A_i)\right| \mid \prod_{i=1}^{k} |\mathrm{End}(A_i)|^k .$$

Proof. From (1.23), we see that the left-hand side is equal to

$$\prod |\mathrm{Hom}(A_i, A_j)| = \prod_{i=1}^{k} |\mathrm{End}(A_i)| \cdot \prod_{i<j} |\mathrm{Hom}(A_i, A_j)|^2 .$$

By the Lemma this number divides

$$\prod_{i=1}^{k} |\mathrm{End}(A_i)| \cdot \prod_{i<j} |\mathrm{End}(A_i)|\,|\mathrm{End}(A_j)| = \prod_{i=1}^{k} |\mathrm{End}(A_i)|^k .$$

■

The case $k = 2$ can be interpreted as

Corollary 1.10.5 *Let $\mathcal{M}$ and $\mathcal{N}$ be two finite families of positive integers and $\mathcal{H}$ their disjoint union. Then*

$$\prod_{a,b\in\mathcal{H}} \gcd(a,b) \mid \left(\prod_{a,b\in\mathcal{M}} \gcd(a,b) \prod_{a,b\in\mathcal{N}} \gcd(a,b) \right)^2 .$$

Lemma 1.10.6 *Suppose that*

$$0 = A_0 \leq A_1 \leq \ldots \leq A_k = A.$$

Put $Q_i = A_i/A_{i-1}$ for each i. Then

$$|\mathrm{End}(A)| \ \textit{divides}\ |\mathrm{End}(Q_1 \oplus \cdots \oplus Q_k)| .$$

Proof. Let C be any abelian group. The exact sequence

$$0 \to A_{k-1} \to A \to Q_k \to 0$$

gives rise to an exact sequence

$$0 \to \mathrm{Hom}(C, A_{k-1}) \to \mathrm{Hom}(C, A) \to \mathrm{Hom}(C, Q_k).$$

This implies that $|\mathrm{Hom}(C, A)|$ divides $|\mathrm{Hom}(C, A_{k-1})| \cdot |\mathrm{Hom}(C, Q_k)|$, and it follows by an obvious inductive argument that

$$|\mathrm{Hom}(C, A)| \mid \prod_{i=1}^{k} |\mathrm{Hom}(C, Q_i)| = |\mathrm{Hom}(C, Q_1 \oplus \cdots \oplus Q_k)| .$$

In particular we have

$$\begin{aligned} |\mathrm{Hom}(A,A)| \mid & |\mathrm{Hom}(A, Q_1 \oplus \cdots \oplus Q_k)| \\ & = |\mathrm{Hom}(Q_1 \oplus \cdots \oplus Q_k, A)| \\ & \mid |\mathrm{Hom}(Q_1 \oplus \cdots \oplus Q_k, Q_1 \oplus \cdots \oplus Q_k)| \,. \end{aligned}$$

■

Corollary 1.10.7 *In the situation of Lemma 1.10.6,*

$$|\mathrm{End}(A)| \mid \prod_{i=1}^{k} |\mathrm{End}(Q_i)|^k \,.$$

1.11 Growth types

To conclude the chapter, we interpret some of the results in terms of growth type. Recall that a group G is said to have subgroup growth of *type* f if there exist positive constants a and b such that

$$\begin{aligned} s_n(G) &\leq f(n)^a \quad \text{for all } n \\ s_n(G) &\geq f(n)^b \quad \text{for infinitely many } n; \end{aligned}$$

and that G has growth of *strict type* f if the second inequality holds for *all* large n. In particular, *polynomial subgroup growth* means growth of type at most n.

Let H be a subgroup of finite index m in a group G. Corollary 1.2.4 and Lemma 1.2.1 show that for every n,

$$\begin{aligned} s_n(G) &\leq a \cdot n^b \cdot s_n(H), \\ s_n(H) &\leq s_{mn}(G) \end{aligned}$$

where $a = m^{[\log m]}$ and $b = [\log m]$. This means that 'on the whole', G and H have the same growth type. For example, *G has polynomial subgroup growth if and only if H does.* The same holds for faster growth types, as long as we restrict to 'reasonable' functions. Let us say that a function f satisfies $(*)$ (for a given $m \in \mathbb{N}$) if

$$\begin{gathered} \log n = o(\log f(n)) \qquad ((*)) \\ \text{and} \\ \log f(mn) = O(\log f(n)). \end{gathered}$$

This holds for all 'nice' functions such as

$$\begin{aligned} f(n) &= n^{(\log\log\ldots\log n)^\beta}, \quad \text{or} \\ f(n) &= 2^{n^\gamma}, \quad \text{or} \\ f(n) &= n^{n^\gamma}. \end{aligned}$$

Now we can state

Proposition 1.11.1 *Let H be a subgroup of finite index m in a group G.*

(i) If H has growth type (or strict growth type) f_1 where f_1 satisfies $(*)$, then so does G;

(ii) if G has growth type (or strict growth type) f_2 where f_2 satisfies $(*)$, then so does H.

Proof. We have

$$\log s_n(H) \leq \log s_{mn}(G) = O\left(\log f_2(mn)\right) = O\left(\log f_2(n)\right)$$

and

$$\log s_n(G) \leq \log a + b \log n + \log s_n(H) = O\left(\log f_1(n)\right),$$

so H has growth type at most f_2 and G has growth type at most f_1. The same argument (using o in place of O) shows that the growth type of G is not strictly less than f_1 and that of H is not strictly less than f_2, so G and H do have growth types f_1 and f_2 respectively.

The proof for *strict* growth types is similar and is left to the reader (note that if n is large enough, there exists $t \in \mathbb{N}$ such that $m^2 t \geq n \geq mt$, and then

$$s_n(G) \geq s_{mt}(G) \geq s_t(H),$$

while

$$\log f_1(t) \geq \varepsilon \log f_1(m^2 t) \geq \varepsilon \log f_1(n)$$

for some fixed $\varepsilon > 0$, provided we assume that f_1 is a non-decreasing function; this assumption is justified when f_1 is the strict growth type of a group H). ■

The dual situation is similar:

Proposition 1.11.2 *Let M be a finite normal subgroup of a group G. Then*

(i) G has polynomial subgroup growth if and only if G/M does;

(ii) suppose that G/M has strict growth type f where f satisfies $(*)$ for every $m \in \mathbb{N}$; then G and G/M have the same strict growth type.

Proof. Certainly $s_n(G) \geq s_n(G/M)$ for all n. For the other direction, we may assume that G is residually finite, in which case G has a normal subgroup N of finite index such that $M \cap N = 1$. Write $Q = G/N$. By (1.9) in Lemma 16.4.8 we have

$$\begin{aligned} s_n(G) &\leq n^{|Q|} s_n(N) \\ &\leq n^{|Q|} s_{mn}(G/M) \end{aligned}$$

where $m = |G : MN|$. This clearly implies (i). For (ii) we note that

$$\log s_{mn}(G/M) = O(\log f(mn)) = O(\log f(n))$$

and deduce that

$$\log s_n(G) = O(\log f(n)) = O(\log s_n(G/M)).$$

The result follows. ■

Similar results hold for *normal subgroup growth*. Indeed, it is an easy consequence of Proposition 1.3.6 that *if $M \lhd G$ is finite then G and G/M have the same (strict) type of normal subgroup growth*, and that *if N is a normal subgroup of finite index in G then the normal subgroup growth type of G is at most that of N*. However, it is *not known* whether the normal subgroup growth type N is necessarily bounded above by that of G; even the following problem is open:

Problem Suppose that G is a group with polynomial normal subgroup growth. Does every normal subgroup of finite index in G have polynomial normal subgroup growth?

Notes

Much of this material is "folklore" (inasmuch as a subject barely 20 years old can be said to have it). Some specific references are as follows.

§1.1: [**Dey 1965**], [**Wohlfahrt 1977**]

A version of Corollary 1.3.5 appeared in an early draft of [**Goldfeld, Lubotzky & Pyber**]

Corollary 1.4.3: [**Segal 1986**$_a$]

Proposition 1.6.2: [**Ilani 1989**]

Lemma 1.7.1 and Corollary 1.7.2: [**Mann & Segal 1990**]

Proposition 1.7.4 and Corollary 1.7.5: [**Pyber 1997**]

Proposition 1.8.1 and §1.10: [**Segal & Shalev 1997**]

Proposition 1.9.2: [**Segal 2001**].

Some interesting results on groups whose subgroup growth is 'multiplicative' (as it is for nilpotent groups) are given in [**Puchta 2001**].

Further results on counting subgroups in finite abelian groups (as in §1.10) are established in [**Goldfeld, Lubotzky & Pyber**]. See also [**Butler 1994**].

Chapter 2

Free groups

The study of subgroup growth in finitely generated groups begins with the observation that there are only finitely many subgroups of each finite index. By considering homomorphisms of a d-generator group G into $\mathrm{Sym}(n)$, we showed in §1.1 that $a_n(G) \leq n \cdot (n!)^{d-1}$ for each n. It is not much harder to see that asymptotically this bound is achieved. Rather surprisingly, the same applies also to the number $m_n(G)$ of maximal subgroups of index n. The precise result is

Theorem 2.1 *Let F be a free group on $d \geq 2$ generators. Then*

$$a_n(F) \sim m_n(F) \sim n \cdot (n!)^{d-1}.$$

This is proved in Section 1, along with an exact recursive formula for the numbers $a_n(F)$. Since $n^{n/2} \leq n! \leq n^n$ for all n, it implies

Corollary 2.2 *Every finitely generated non-abelian free group has subgroup growth of strict type n^n and maximal subgroup growth of strict type n^n.*

Since $n^n = 2^{n \log n}$, this upper bound for the growth type of finitely generated groups is a little faster than exponential. Many groups, however, have at most exponential subgroup growth: in the next chapter we shall see that any group with super-exponential growth must be rather similar to a free group, in the sense that it involves *every finite group* as an upper section. The same holds, surprisingly, for groups whose *maximal* subgroups grow faster than *polynomially*.

Sections 2 and 3 deal with, respectively, subnormal subgroups and normal subgroups. While exact formulas are too much to expect, we obtain reasonably sharp upper bounds. As might be expected, there are somewhat fewer subnormal subgroups than subgroups, and many fewer normal subgroups.

Theorem 2.3 *Let F be a d-generator group. Then for all n,*

$$a_n^{\lhd\lhd}(F) \leq \frac{n^2}{2^{d-1}} 2^{(d-1)n}.$$

This upper bound is exponential. On the other hand, we shall prove in the next chapter that every non-abelian *free pro-p group* has exponential subgroup growth. Now if F is a non-abelian free group then the pro-p completion $\widehat{F}_p$ of F is a non-abelian free pro-p group, and

$$a_n(\widehat{F}_p) = a_n^{\triangleleft\triangleleft}(F)$$

whenever n is a power of the prime p ($\leadsto$ **Profinite groups**). Theorem 3.6 with $p = 2$ gives

$$a_{2^k}(\widehat{F}_2) \geq 2^{(d-1)(2^k-1)-k(k-1)/2};$$

this shows that the upper bound in Theorem 2.3 is pretty well sharp when n is a power of 2. In general, choosing k so that $2^k \leq n < 2^{k+1}$ we may deduce that $s_n^{\triangleleft\triangleleft}(F) \geq 2^{\frac{d-1}{2}n-o(n)}$. It follows that the subnormal subgroup growth of F is of *at least* exponential type, so we have

Corollary 2.4 *Every finitely generated non-abelian free group has subnormal subgroup growth of strict type* $2^n = n^{n/\log n}$.

While the proof of Theorem 2.3 as stated uses the Classification of finite simple groups, we shall give an alternative elementary proof that the growth is at most exponential; thus Corollary 2.4, like Theorem 2.1, is independent of the classification.

The number of *normal* subgroup of index n in F is closely related to the number $f(n, d)$ of *isomorphism types of d-generator groups of order n*:

Lemma 2.5 *Let F be a free group on d generators. Then for each n,*

$$f(n, d) \leq a_n^{\triangleleft}(F) \leq n^d f(n, d).$$

Indeed, if G is a d-generator group of order n then there is an epimorphism from F onto G whose kernel is a normal subgroup of index n. Clearly, non-isomorphic groups give rise to distinct kernels, so $f(n, d) \leq a_n^{\triangleleft}(F)$. On the other hand, to each normal subgroup N of index n in F we may associate the natural epimorphism $\varphi : F \to F/N$, with $N = \ker \varphi$. Given a group G of order n, the number of epimorphisms $F \to G$ is at most n^d; so the number of N for which $F/N \cong G$ is at most n^d, and the second inequality follows.

Thus the normal subgroup growth type of F is determined by the function $f(n, d)$. In Section 3 we establish

Theorem 2.6 *For every n and d we have*

$$f(n, d) \leq n^{2(d+1)\lambda(n)}.$$

Here, $\lambda(n) = \sum l_i$ when $n = \prod p_i^{l_i}$ with distinct primes $p_1, p_2, \ldots$, so $\lambda(n) \leq \log n$ for all n. With the preceding lemma this gives at once

Theorem 2.7 *Let F be a free group on d generators. Then for each n,*

$$a_n^{\triangleleft}(F) < n^{(2d+2)(1+\lambda(n))}.$$

These results seem to depend crucially on CFSG. (The best upper bound for $f(n,d)$ that can be established by elementary means seems to be an exponential one, using the bound for $a_n^{\triangleleft\triangleleft}(F)$ discussed above.)

Corresponding lower bounds are again obtained by considering normal subgroups in a free pro-p group, or equivalently the number of d-generator finite p-groups. In the following chapter we show that for each prime p and each $d \geq 2$,

$$f(p^k, d) \geq p^{ck^2}$$

for all large k, if $c < (d-1)^2/4d$. With Theorem 2.7 and Lemma 2.5 this now gives

Corollary 2.8 *Every finitely generated non-abelian free group has normal subgroup growth of strict type $n^{\log n}$.*

2.1 The subgroup growth of free groups

According to Corollary 1.1.4, the following holds for any group F and each $n \geq 1$:

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

where $h_n(F)$ denotes the number of homomorphisms $F \to \mathrm{Sym}(n)$. If F is the free group on $d \geq 2$ generators then clearly

$$h_n(F) = (n!)^d,$$

and plugging this in now yields the recursive formula

Proposition 2.1.1 *Let F be the free group on $d \geq 2$ generators. Then*

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

To better estimate the growth of $a_n(F)$, we note that, provided $d \geq 2$, "most" d-tuples of permutations in $\mathrm{Sym}(n)$ generate transitive subgroups: that is,

$$t_n(F)/h_n(F) \to 1 \text{ as } n \to \infty, \tag{2.1}$$

where $t_n(F)$ denotes the number of homomorphisms $F \to \mathrm{Sym}(n)$ with transitive image.

Indeed, by Lemma 1.1.3 the number of *intransitive* actions of F on the set $\{1, \ldots, n\}$ is just

$$\begin{aligned}\sum_{k=1}^{n-1} h_{n,k}(F) &= \sum_{k=1}^{n-1} \binom{n-1}{k-1} t_k(F) h_{n-k}(F) \\ &\leq \sum_{k=1}^{n-1} \binom{n-1}{k-1} (k!)^d ((n-k)!)^d \\ &= (n!)^d \sum_{k=1}^{n-1} \binom{n}{k}^{-(d-1)} \frac{k}{n} \\ &\leq (n!)^d \sum_{k=1}^{[n/2]} \binom{n}{k}^{-(d-1)}\end{aligned}$$

since $\binom{n}{k} = \binom{n}{n-k}$. (Here, $h_{n,k}(F)$ denotes the number of representations of F in $\mathrm{Sym}(n)$ in which the orbit of 1 has length exactly k.) Now for $1 \leq k \leq n/2$ we have

$$\binom{n}{k} \geq \left(\frac{n}{k}\right)^{k-1} (n-k+1) \geq 2^{k-1} \cdot n/2.$$

Noting that $d - 1 \geq 1$, we deduce that

$$\begin{aligned}h_n(F) - t_n(F) &= \sum_{k=1}^{n-1} h_{n,k}(F) \\ &\leq (n!)^d \sum_{k=1}^{[n/2]} \frac{2}{2^{k-1} n} \\ &< \frac{4}{n} (n!)^d = \frac{4}{n} h_n(F),\end{aligned}$$

and (2.1) follows. (We mention in passing the theorem of [Dixon 1969] that for $d \geq 2$ most d-tuples in $\mathrm{Sym}(n)$ not merely act transitively but actually generate either $\mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$.)

Now Proposition 1.1.1 gives

$$\begin{aligned}a_n(F) &= \frac{t_n(F)}{(n-1)!} \\ &\sim \frac{h_n(F)}{(n-1)!} = n \cdot (n!)^{d-1}\end{aligned} \tag{2.2}$$

by (2.1). This establishes half of Theorem 2.1.

The following easier estimate is sometimes useful: since $\mathrm{Sym}(n)$ contains $(n-1)!$ distinct n-cycles, the number of d-tuples that generate a transitive subgroup of $\mathrm{Sym}(n)$ is at least $(n-1)! \cdot (n!)^{d-1}$, so (2.2) immediately gives

Corollary 2.1.2 *Let F be the free group on $d \geq 2$ generators. Then*

$$a_n(F) \geq n!^{d-1}$$

for every n.

What about the *maximal* subgroups? Proposition 1.1.1 also shows that

$$m_n(F) = p_n(F)/(n-1)!$$

where $p_n(F)$ denotes the number of primitive actions of G on $\{1, \ldots, n\}$. Thus to show that

$$m_n(F) \sim n \cdot (n!)^{d-1} \tag{2.3}$$

it suffices to establish that

$$p_n(F)/h_n(F) \to 1 \quad \text{as} \quad n \to \infty.$$

Of course, this follows from the theorem of Dixon mentioned above, but it is easy to prove directly. Indeed, each transitive but *imprimitive* action of F on $\{1, \ldots, n\}$ preserves some non-trivial partition of this set into equal parts, of size $r = n/s$, say, and corresponds to a homomorphism from F into the wreath product

$$\mathrm{Sym}(r) \wr \mathrm{Sym}(s).$$

The number of such partitions is

$$\frac{1}{s!}\binom{sr}{r}\binom{(s-1)r}{r}\cdots\binom{2r}{r}\binom{r}{r} = \frac{n!}{(r!)^s s!},$$

and the number of homomorphisms from F into $\mathrm{Sym}(r) \wr \mathrm{Sym}(s)$ is

$$|\mathrm{Sym}(r) \wr \mathrm{Sym}(s)|^d = \left((r!)^s s!\right)^d.$$

It follows that

$$\begin{aligned} t_n(F) - p_n(F) &\leq \sum \frac{n!}{(r!)^s s!} \cdot \left((r!)^s s!\right)^d \\ &< d(n) \cdot n! \cdot \left((r!)^s s!\right)^{d-1} \\ &< d(n) n^{-(d-1)} (n!)^d, \end{aligned}$$

since it is easy to see that $(r!)^s s! < (n-1)!$ when $n = rs$ with $r > 1$ and $s > 1$ (here $d(n)$ denotes the number of divisors of n). Thus

$$\begin{aligned} \frac{t_n(F) - p_n(F)}{h_n(F)} &= (n!)^{-d}(t_n(F) - p_n(F)) \\ &< d(n) \cdot n^{-(d-1)} \end{aligned}$$

which tends to 0 as $n \to \infty$, since $d \geq 2$ and $d(n) = o(n)$ (see [HW], §18.1). Together with (2.1) this establishes (2.3), and completes the proof of Theorem 2.1.

2.2 Subnormal subgroups

The proof of Theorem 2.3 is a simple application of two facts. The first is Schreier's formula: if H is a subgroup of finite index n in a finitely generated group G, then

$$\mathrm{d}(H) - 1 \leq n(\mathrm{d}(G) - 1) \tag{2.4}$$

(see [R], Theorem 6.1.1). The second lies much deeper, and depends on CFSG:

Lemma 2.2.1 *A d-generator group has at most $2n^{d-1}$ maximal normal subgroups of index n.*

Proof. It follows from the classification (↬ **Finite simple groups**) that there are at most 2 simple groups of a given order n. So if G is a d-generator group, the number of epimorphisms from G onto simple groups of order n is at most $2n^d$. However, if n is not prime then each such simple group S has at least n automorphisms; it follows that for each epimorphism from G to S, there exist at least $n-1$ further epimorphisms with the same kernel. Thus if n is not prime, then G has at most $2n^{d-1}$ maximal normal subgroups of index n. If n is prime, there is only one group of order n, and it has $n-1$ automorphisms; in this case G has at most $n^d/(n-1) \leq 2n^{d-1}$ maximal normal subgroups of index n. ■

To prove the theorem we have to show that if G is a d-generator group then, for each n, the number of subnormal subgroups of index n in G is at most

$$\frac{n^2}{2^{d-1}} 2^{(d-1)n} = n^2 2^{(d-1)(n-1)}.$$

Arguing by induction on n, we may assume that $n > 1$ and that the corresponding result holds for all indices less than n (and all finitely generated groups). We may also assume that $d \geq 2$, as the result holds trivially if G is cyclic. Now if H is subnormal of index n in G, then there is a maximal normal subgroup N of G such that

$$H \lhd\lhd N \lhd G.$$

Let $r = |G : N|$. Then (2.4) shows that $\mathrm{d}(N) - 1 \leq r(d-1)$, and $|N : H| = n/r$. So if N is given, the number of possibilities for H is at most

$$(n/r)^2 2^{r(d-1)(n/r-1)} = \frac{n^2}{r^2 2^{r(d-1)}} 2^{(d-1)n} \tag{2.5}$$

(here we are using the inductive hypothesis). If r is given, the number of possibilities for N, according to Lemma 2.2.1, is at most $2r^{d-1}$. Consequently,

$$a_n^{\lhd\lhd}(G) \leq \sum_{1<r|n} \left(2r^{d-1} \cdot \frac{n^2}{r^2 2^{r(d-1)}} 2^{(d-1)n} \right). \tag{2.6}$$

So to complete the proof it will suffice to show that

$$\sum_{1<r} \frac{2 \cdot (2r)^{d-1}}{r^2 2^{r(d-1)}} \leq 1.$$

Now since $d \geq 2$ and $2r/2^r \leq 1/2$ for $r \geq 4$, the sum in question is bounded above by

$$\frac{2}{2^2} + \frac{2}{3^2} \cdot \frac{6}{8} + \sum_{r=4}^{\infty} r^{-2} = \frac{2}{3} + (\pi^2/6 - 1 - \frac{1}{4} - \frac{1}{9}) = 0.95\ldots < 1.$$

This completes the proof of Theorem 2.3.

We promised an alternative proof that $a_n^{\lhd\lhd}(G)$ is exponentially bounded. This is based on the following elementary result established in the **Finite simple groups** window: there is an absolute constant c such the number of simple groups of order n is bounded above by c^n. Using this in the proof of Lemma 2.2.1 we deduce that *a d-generator group has at most $c^n n^{d-1}$ maximal normal subgroups of index n.*

Now we are ready to prove by induction on n that for $d \geq 2$, *a d-generator group has at most*

$$n^2 c^n 2^{(d-1)(n-1)}$$

subnormal subgroups of index n. The argument goes as above, replacing (2.5) by

$$(n/r)^2 c^{n/r} 2^{r(d-1)(n/r-1)} = (n/r)^2 c^{n/r} 2^{(n-r)(d-1)}$$

and (2.6) by

$$\begin{aligned} a_n^{\lhd\lhd}(G) &\leq \sum_{1<r|n} \left(c^r r^{d-1} \cdot (n/r)^2 c^{n/r} 2^{(n-r)(d-1)} \right) \\ &\leq n^2 c^n 2^{(d-1)(n-1)} \cdot \sum_{1<r|n} \frac{(2r)^{d-1}}{r^2 2^{r(d-1)}}. \end{aligned}$$

The result follows since we have shown above that the final sum is at most $1/2$.

2.3 Counting d-generator finite groups

Recall that $f(n,d)$ denotes the number of isomorphism types of d-generator groups of order n. This section is devoted to the proof of Theorem 2.6, which we restate as

Theorem 2.3.1 *For every n and d we have*

$$f(n,d) \leq n^{2(d+1)\lambda(n)}.$$

We begin by stating two conjectures.

Conjecture A *Every group of order n with a given set of d generators can be defined by these generators and at most $2(d+1)\lambda(n)$ relations.*

Conjecture B *Every finite simple group G can be defined by two generators and at most $2\lambda(|G|)$ relations.*

Recall that $\lambda(n)$ denotes the total number of factors in the prime factorisation of n.

At the time of writing, Conjecture B is known for most types of finite simple group, the only unknown cases being certain Ree groups (see the *notes* below).

We will now show that Conjecture B implies Conjecture A and then we will show that Conjecture A implies Theorem 2.3.1. Subsequently, we shall introduce profinite presentations and show that *in the profinite interpretation, Conjecture B is true*, while the above mentioned implications remain valid. Thus Theorem 2.3.1 will be eventually proved unconditionally.

Conjecture B implies Conjecture A

Let G be a group of order n generated by $x_1, \ldots, x_d$. Suppose first that G is simple. By hypothesis, G has a presentation

$$\langle y,\, z\ ;\ w_1(y,z), \ldots, w_r(y,z)\rangle$$

where $r \leq 2\lambda(n)$. Say $x_i = \xi_i(y,z)$ and $y = \eta(\mathbf{x})$, $z = \zeta(\mathbf{x})$ where η, ζ and the ξ_i are words. Then it is easy to see that the $d + r \leq d + 2\lambda(n) < 2(d+1)\lambda(n)$ relations

$$\begin{aligned} x_i &= \xi_i(\eta(\mathbf{x}), \zeta(\mathbf{x})) \qquad (i = 1, \ldots, d) \\ w_j(\eta(\mathbf{x}), \zeta(\mathbf{x})) &= 1 \qquad\qquad\quad (j = 1, \ldots, r) \end{aligned}$$

define G on the given generators $x_1, \ldots, x_d$.

Suppose now that G is not simple, and let N be a minimal normal subgroup of G, of order m. By induction G/N can be defined by $r \leq 2(d+1)\lambda(n/m)$ relations in the generators $x_1N, \ldots, x_dN$. Let these relations be $u_1(\mathbf{x}N) = 1, \ldots, u_r(\mathbf{x}N) = 1$. (Here and below $\mathbf{x}N$ stands for the d-tuple $(x_1N, \ldots, x_dN)$, similarly for $\mathbf{x}$ etc.). Now, N is a product $N = S_1 \times \cdots \times S_k$ of conjugate simple groups. Put $s = |S_1|$ and let

$$S_1 = \langle y,\, z\ ;\ R\rangle$$

be a presentation of S_1, where R is a set of words on y, z with $|R| \leq 2\lambda(s)$. Now since G/N is finite, there exist *negative words* (i.e. involving no positive powers of the generators)

$$v_1 = 1,\, v_2(\mathbf{x}), \ldots, v_k(\mathbf{x})$$

such that, in G,

$$S_1^{v_i(\mathbf{x})} = S_i$$

for each i. Then $S_i = \langle y_i,\, z_i\rangle$ where $y_i = y^{v_i(\mathbf{x})}$, $z_i = z^{v_i(\mathbf{x})}$. Say $y = w(\mathbf{x})$ and $z = w'(\mathbf{x})$, and put

$$\begin{aligned} w_i(\mathbf{x}) &= w(\mathbf{x})^{v_i(\mathbf{x})} \\ w_i'(\mathbf{x}) &= w'(\mathbf{x})^{v_i(\mathbf{x})}. \end{aligned} \tag{2.7}$$

Next, find words t_i such that $u_i(\mathbf{x}) = t_i(\mathbf{y}, \mathbf{z})$ (this is possible since $u_i(\mathbf{x}) \in N$) and words s_{ij} and s'_{ij} such that

$$y_i^{x_j} = s_{ij}(\mathbf{y}, \mathbf{z}) \quad z_i^{x_j} = s'_{ij}(\mathbf{y}, \mathbf{z}).$$

We claim that G can be defined by the following relations in the generators $x_1, \ldots, x_d$, where t_i, s_{ij}, s'_{ij} will be used to denote the words in $\mathbf{x}$ obtained by substituting the word $w_l(\mathbf{x})$ for y_l and $w'_l(\mathbf{x})$ for z_l in the words t_i, s_{ij} and s'_{ij}:

$$\begin{aligned} u_i &= t_i(\mathbf{y}, \mathbf{z}) \qquad (i = 1, \ldots, r) \\ R(w_1,\, w_1') &= \{1\}, \\ [w_1, w_i] = [w_1, w_i'] &= [w_1', w_i] = [w_1', w_i'] = 1 \qquad (i = 2, \ldots, k) \\ w_i^{x_j} &= s_{ij},\ w_i'^{x_j} = s'_{ij} \qquad (i = 1, \ldots, k,\ j = 1, \ldots, d). \end{aligned} \tag{2.8}$$

Indeed, let X be the group defined by this presentation. Since the relations hold in G, there is a homomorphism ϕ from X onto G (mapping the generators x_i of X to the generators with the same name of G). Let Y be the subgroup of X generated by the $2k$ elements w_i, w_i'. The subgroup Y_1 generated by w_1 and w_1' is an image of the simple group S_1, and hence is isomorphic to S_1 since ϕ maps it onto S_1 in G; and the identities (2.7) show that $Y = \langle Y_1^{v_1}, \ldots, Y_1^{v_k}\rangle$. Note also that for every x_i the relations imply that $Y^{x_i} \le Y$; hence $Y^\pi \le Y$ whenever π is a positive word in the x_i, and since the words v_i are negative we have $Y \le Y^{v_i}$ for each i. Now the third line of (2.8) ensures that

$$Y = \langle Y_1, \mathrm{C}_Y(Y_1)\rangle\,,$$

so $Y_1 \lhd Y$. It follows that for each i, $Y_1^{v_i} \lhd Y^{v_i}$, and hence by the preceding remark $Y_1^{v_i} \lhd Y$. Therefore $Y = Y_1^{v_1} \cdot \ldots \cdot Y_1^{v_k}$ has order at most s^k, so it has exactly this order and $\phi_{|Y} : Y \to N$ is an isomorphism. Also, as Y is finite the relations $Y^{x_i} \le Y$ ensure that Y is normal in X.

Putting every w_i and w_i' equal to 1 in the above presentation we obtain a presentation of X/Y, which is just the given presentation $\langle \mathbf{x}\,;\, u_1, \ldots, u_r\rangle$ for G/N. Hence ϕ also induces an isomorphism from X/Y onto G/N. Thus ϕ is injective and $X \cong G$ as claimed.

To estimate the number of relations we separate two cases.

Case 1: where S is non-abelian. Then $\lambda(s) \geq 2$, and the number of relations is

$$\begin{aligned} r + |R| + 4(k-1) + 2kd &\leq 2(d+1)\lambda(n/m) + 2\lambda(s) + 4(k-1) + 2kd \\ &= 2(d+1)\lambda(n) - 2(d+1)\lambda(m) + 2\lambda(s) + 4(k-1) + 2kd \\ &\leq 2(d+1)\lambda(n) - 2kd \end{aligned}$$

since $\lambda(m) = k\lambda(s) \geq 2k$.

Case 2: where S_1 is cyclic of prime order. In this case, we may take $w' = 1$, $|R| = 1$, and omit the redundant relations in rows three and four of (2.8) involving the w_i'. The number remaining is then

$$\begin{aligned} r + 1 + (k-1) + kd &\leq 2(d+1)\lambda(n/m) + (d+1)k \\ &= 2(d+1)\lambda(n) - (d+1)k \end{aligned}$$

since now $\lambda(m) = k$.

In each case we have fewer than $2(d+1)\lambda(n)$ relations, and the proof is complete.

Conjecture A implies Theorem 2.3.1

Let $G = \langle x_1, \ldots, x_d \rangle$ be a group of order n. Then G has a minimal normal subgroup $N = S_1 \times \cdots \times S_k$ as above, where $S_1, \ldots, S_k$ are isomorphic simple groups, of order s, say. Once N and G/N are given, G is determined up to isomorphism by the following data: the d automorphisms

$$a \mapsto a^{x_i}$$

of N, and the r elements

$$t_i = u_i(\mathbf{x})$$

of N where $\langle x_1 N, \ldots, x_d N\,;\, u_i(\mathbf{x}N) = 1\ (i = 1, \ldots, r) \rangle$ is a presentation for G/N.

Now if S and T are simple groups and $|S|^k = |T|^{k'}$ for some k, $k' \geq 1$ then $k = k'$ and $|S| = |T|$; and given $|S|$ there are at most two possibilities for the isomorphism type of S (for both claims, ↬ **Finite simple groups**). So having fixed $|N| = m$ we have at most two possibilities for the isomorphism type of N. Since N can be generated by $2k$ elements it has at most $m^{2k} \leq m^{2\lambda(m)}$ automorphisms. By definition, there are $f(n/m, d)$ possibilities for the isomorphism type of G/N, and according to Conjecture A, the group G/N is defined by $r \leq 2(d+1)\lambda(n/m)$ relations among the generators $x_i N$. Putting these together, we see that the number of possibilities for G is

$$\begin{aligned} f(n,d) &\leq \sum_{1<m|n} 2 \cdot f(n/m, d) \cdot m^{2d\lambda(m)} \cdot m^{2(d+1)\lambda(n/m)} \\ &= \sum_{1<m|n} 2 \cdot f(n/m, d) \cdot m^{2(d+1)\lambda(n)} \cdot m^{-2\lambda(m)}. \end{aligned}$$

Assume inductively that $f(h,d) \leq h^{2(d+1)\lambda(h)}$ whenever $h < n$. Then for $n = hm$ we have

$$f(h,d)m^{2(d+1)\lambda(n)} \leq \left(h^{\lambda(h)}m^{\lambda(n)}\right)^{2(d+1)} = n^{2(d+1)\lambda(n)} \cdot h^{-2(d+1)\lambda(m)}.$$

Putting this into the above we get

$$\begin{aligned} f(n,d) &\leq n^{2(d+1)\lambda(n)} \sum_{1<m|n} 2m^{-2\lambda(m)}(n/m)^{-2(d+1)\lambda(m)} \\ &< n^{2(d+1)\lambda(n)} \end{aligned}$$

since each term inside the sum is at most $2/n^2$. This concludes the proof of Theorem 2.3.1, modulo Conjecture A.

Profinite presentations

The reader has certainly noticed that the proof shows that Conjecture A and Theorem 2.3.1 are valid if we consider groups whose composition factors satisfy Conjecture B, e.g., all soluble groups, or even all finite groups whose composition factors are not of type $U(3,q)$ or ${}^2G_2(q)$. Unfortunately, the last two families of finite simple groups are not known to have short presentations. This obstacle can be overcome by using "profinite presentations" instead.

Let $\widehat{F}_d$ be the free profinite group on d generators, i.e., $\widehat{F}_d$ is the profinite completion of the discrete free group F_d on the generators $x_1, \ldots, x_d$. $\widehat{F}_d$ has the universal property: if $\varphi : \{x_1, \ldots, x_d\} \to G$ is a map from the set $\{x_1, \ldots, x_d\}$ to a profinite group, it has a unique extension to a continuous homomorphism $\tilde{\varphi} : \widehat{F}_d \to G$. Note that for every element ("word") w in $\widehat{F}_d$, every profinite (in particular, finite) group G and every $g_1, \ldots, g_d \in G$ we can evaluate w on $g_1, \ldots, g_d$, i.e., $w(g_1, \ldots, g_d)$ is defined as $\tilde{\varphi}(w)$ when $\tilde{\varphi}$ is the unique homomorphism $\tilde{\varphi} : \widehat{F}_d \to G$ extending the map $\varphi(x_i) = g_i, i = 1, \ldots, d$. Thus we can consider the elements w of $\widehat{F}_d$ as "words", though they are not words in $x_1, \ldots, x_d$ in the usual sense. Moreover, we can speak of presentations of profinite groups by generators and relations: if $G = \widehat{F}_d/N$ and Y is a subset of N such that N is the minimal closed normal subgroup of $\widehat{F}_d$ containing Y then we say that $\langle x_1, \ldots x_d; Y\rangle$ is a profinite presentation of G.

Theorem 2.3.2 *Every finite simple group G has a profinite presentation with two generators and $2\lambda(|G|)$ relations.*

We postpone the proof of this theorem, but note first that it implies

Theorem 2.3.3 *Every group of order n generated by d elements has a profinite presentation with these generators and at most $2(d+1)\lambda(|G|)$ relations.*

Indeed the proof that Conjecture B implies Conjecture A works word for word, just replacing the set R, which was a set of ordinary relators, by a set of profinite

words. Similarly, the deduction of Theorem 2.3.1 from Conjecture A serves just as well if we replace Conjecture A by Theorem 2.3.3.

We are thus left with the need to prove Theorem 2.3.2. Once this is done, the proof of Theorem 2.3.1 will be complete.

To prove Theorem 2.3.2 we start with a proposition of some independent interest. But first we need a definition. Let G be a finite group with presentation $G = F_d/N$, where F_d is the free group on d generators. Write $N' = [N, N]$ for the commutator subgroup of N, and for a prime p put $N(p) = N' \cdot N^p$. By the Nielsen-Schreier Theorem N is a free group on $r = 1 + d(n-1)$ generators where $n = |G|$. Hence $N/N' \cong \mathbb{Z}^r$ and $N/N(p) \cong \mathbb{F}_p^r$. The free group F_d acts on N/N' and $N/N(p)$ by conjugation and in both cases the action factors through G. The G-module N/N' (resp., $N/N(p)$) is called the *relation module* (resp. mod p *relation module*) of G with respect to the presentation $G = F_d/N$.

Now, if $G = F_d/N$ is a presentation of G then G is also isomorphic to $\widehat{F}_d/\overline{N}$ where $\overline{N}$ is the closure of N in $\widehat{F}_d$. Thus $\widehat{F}_d/\overline{N}$ is a profinite presentation of G.

Proposition 2.3.4 *The number of relations needed for the profinite presentation $G = \widehat{F}_d/N$ is equal to $\max_p \mathrm{d}_G(N/N(p))$, i.e. the maximum over all primes p of the number of generators of $N/N(p)$ as a G-module.*

Remark. A deep result of R. Swan asserts that $\mathrm{d}_G(N/[N,N]) = \max_p \mathrm{d}_G(N/N(p))$, so the proposition can be reformulated as saying that *the number of profinite relations needed for G is equal to the number of generators of the relation module* (see [Gruenberg 1976]). But we will not need Swan's result for our application. It is worthwhile to mention, though, that a longstanding open problem is whether N can be generated as a normal subgroup by $\mathrm{d}_G(N/[N,N])$ elements. In view of the above Proposition, this is equivalent to asking whether the number of ordinary relations needed to define G is equal to the number of profinite relations needed for the same purpose. This is the difference between Theorem 2.3.3 and Conjecture A.

Proof of Proposition 2.3.4**.** $\overline{N}$ is a normal subgroup of $\widehat{F}_d$. Let M be the intersection of all the maximal open normal subgroups of $\overline{N}$. It is easy to see that (i) M is normal in $\widehat{F}_d$ and (ii) for a subset Y of N, Y generates N normally if and only if it does so modulo M. Moreover, we can describe quite precisely the structure of $\overline{N}/M$. In fact, $\overline{N}/M \cong \prod_S S^{m_r(S)}$ where the product runs over all the finite simple groups S and each one occurs with multiplicity $m_r(S)$, when $S^{m_r(S)}$ is the largest direct product of copies of S which is still generated by r elements. So, for example, if S is abelian, i.e. $S = C_p$ for some $p, m_r(S) = r$, but for non-abelian groups it is much larger than r (see [Kantor & Lubotzky 1990]).

Separate the product into two parts $\overline{N}/M \cong A \times B$ when $A = \prod_p C_p^r$ and $B = \prod_S S^{m_r(S)}$ where this time S runs only over the non-abelian finite simple

groups. Note that the action of $\widehat{F}_d$ on A factors through G, making A into a G-module.

Claim: The number of generators of $\overline{N}/M$ as a normal subgroup of $\widehat{F}_d/M$ is equal to $\mathrm{d}_G(A)$.

Indeed assume $\{y_1, \ldots, y_\ell\}$ is a subset of A generating A as G-module. Let z_1 be an element of B, each of whose components, in each single S, is non-trivial. As B is a product of finite simple groups, the normal closure of z_1 in B (and hence in $\widehat{F}_d/M$) is B. Since A and B have no common composition factors, it follows that $(y_1, z_1), (y_2, 1), \ldots, (y_\ell, 1)$ generate $A \times B$ as a normal subgroup of $\widehat{F}_d/M$.

Now, as the different primes are also "independent" one deduces that

$$\begin{aligned}\mathrm{d}_G(A) &= \max_p \mathrm{d}_G(\overline{N}/[\overline{N}, \overline{N}]\overline{N}^p) \\ &= \max_p \mathrm{d}_G(N/N(p))\end{aligned}$$

and Proposition 2.3.4 is proved.

This reduces the proof of Theorem 2.3.2 to the problem of evaluating the numbers $\mathrm{d}_G(N/N(p))$. The first step is to reformulate the problem, using a general formula due to [Gruenberg 1976]. Let $\mathcal{S}$ denote the set of all simple $\mathbb{F}_p[G]$-modules, and for $M \in \mathcal{S}$ put

$$\begin{aligned}\xi_M &= 0 \quad \text{if} \quad M \cong \mathbb{F}_p \\ \xi_M &= 1 \quad \text{if} \quad M \ncong \mathbb{F}_p.\end{aligned}$$

Gruenberg's formula is as follows; for the proof see the **Profinite groups** window**:**

Proposition 2.3.5

$$\mathrm{d}_G(N/N(p)) = \max_{M \in \mathcal{S}} \left\{ \left\lceil \frac{\dim H^2(G, M) - \dim H^1(G, M)}{\dim M} \right\rceil - \xi_M \right\} + d.$$

(If $p \nmid |G|$, this formula reduces to $\mathrm{d}_G(N/N(p)) = d$, a result obtained earlier by Gaschütz.)

Thus it remains to estimate the dimensions of certain cohomology groups, for a finite simple group G. The next two results, which depend on CFSG, give us what we need. For each prime p, the invariant $\ell_p(G)$ is defined by

$$\begin{aligned}p^{\ell_p(G)} &\mid |G| \\ p^{\ell_p(G)+1} &\nmid |G|.\end{aligned}$$

Proposition 2.3.6 *(↬ **Finite simple groups**) Let G be a finite non-abelian simple group. Then for every prime p,*

$$\dim H^2(G, \mathbb{F}_p) \leq 2.$$

Proposition 2.3.7 [Holt, 1987] *Let G be a finite group and M a faithful simple $\mathbb{F}_p[G]$-module. Then*

$$\dim H^2(G, M) \leq 2\ell_p(G) \dim M.$$

We can now complete the proof of Theorem 2.3.2. Let G be a finite non-abelian simple group. Then G can be generated by 2 elements (↬ **Finite simple groups**), so we have a profinite presentation $G = \widehat{F}_2/\overline{N}$; in view of Proposition 2.3.4, it will suffice to prove that

$$\mathrm{d}_G(N/N(p)) \leq 2\lambda(|G|)$$

for every prime p. According to Proposition 16.4.7 with $d = 2$, this holds provided every simple $\mathbb{F}_p[G]$-module M satisfies

$$\dim H^2(G, M) - \dim H^1(G, M) \leq \begin{cases} (2\lambda(|G|) - 1) \dim M & \text{if } M \ncong \mathbb{F}_p \\ 2(\lambda(|G|) - 1) \dim M & \text{if } M \cong \mathbb{F}_p \end{cases}. \tag{2.9}$$

Now of course $|G|$ is not a prime-power, since G is non-abelian and simple, so $\lambda(|G|) \geq 2$ and $\lambda(|G|) \geq 1 + \ell_p(G)$ for every prime p. Applying the last two propositions we see that in each case, the right hand side of (2.9) is at least $\dim H^2(G, M)$.

Thus Theorem 2.3.2 is established, and Theorem 2.3.1 follows.

Notes

The recursive formula Proposition 2.1.1 is due to [**Hall 1949**], the first modern paper to deal with subgroup-counting. The asymptotic formula for $a_n(F)$ in Theorem 2.1 is due to [**Newman 1976**], who also considers other groups, as reported in Chapter 14. The observation that Dixon's theorem implies $m_n(F) \sim a_n(F)$ was made by L. Pyber.

Theorem 2.3, including the elementary proof of the exponential upper bound for $a_n^{\lhd\lhd}(F)$, is due to **L. Pyber** and **A. Shalev** (unpublished).

The results on normal subgroup growth and the function $f(n, d)$ were established for soluble groups, and conjectured in general, by [**Mann 1998**], following a slightly weaker conjecture of [**Pyber 1996**]; [**Lubotzky 2001**] proved Theorems 2.6 and 2.7 by adapting Mann's methodology and introducing profinite presentations. The sequel [**Mann (a)**] discusses further interesting variations on this theme. It is interesting to note that while $f(n, d)$ (for a fixed d) grows like $n^{\log n}$, the number of isomorphism types of *all* groups of order n grows

like $n^{(\log n)^2}$ (see [**Pyber 1996**]), while the number of those *without abelian composition factors* grows very much more slowly, like $n^{\log \log n}$ [**Klopsch (c)**].

For a discussion of Conjecture B, including its proof in most cases, see [**Kantor 1992**]. Almost all the remaining cases are dealt with in [**Babai, Goodman & Kantor 1997**] and [**Hulpke & Seress 2001**] (these papers consider 'short presentations' rather than the 'small presentations' required for Conjecture B, but the relevant results may be deduced from them).

Chapter 3

Groups with exponential subgroup growth

We saw in the last chapter that finitely generated free groups have super-exponential subgroup growth; so for a group to have subgroup growth of merely exponential type is certainly some kind of restriction. Can it be characterised algebraically? This question seems difficult to answer, because the groups with exponential subgroup growth encompass a huge variety of examples. This is not really surprising, because a very mild algebraic condition is in fact sufficient to ensure that the growth is at most exponential:

Theorem 3.1 *Let Γ be a finitely generated group. Suppose that there exists a finite group which is not isomorphic to any upper section of Γ. Then Γ has at most* exponential *subgroup growth type.*

(An *upper section* of Γ means a quotient A/B where $B \lhd A \leq \Gamma$ and B has finite index in Γ). However, among the finitely generated groups with exponential (and even slower) subgroup growth there also exist some which do involve every finite group as an upper section: examples are given in Section 2 of Chapter 13. Thus it seems unlikely that the groups with 'superfast' – strictly above exponential – growth can be described in a uniform way, analogous to the characterizations of 'slow' – polynomial – subgroup growth to be given in Chapters 5 and 10.

Once we know that a group has exponential growth type, we can ask for a finer measure of the subgroup growth. Let us define an invariant

$$\sigma(G) = \limsup \frac{\log s_n(G)}{n}.$$

Then $\sigma(G)$ is finite precisely when G has at most exponential growth type, and $\sigma(G) > 0$ when the growth type is exponential. Thus Theorem 3.1 may be interpreted as saying that if the upper sections of Γ 'avoid' some finite group H

then $\sigma(\Gamma)$ is finite. Remarkably, the nature of the 'avoided' groups is reflected quite precisely by the actual value of σ.

This relationship is best articulated in terms of suitable relatively-free profinite groups. To set the scene, let us begin by reformulating Theorem 3.1 in this language. Let $\mathcal{C}$ be a class of finite groups closed under taking subgroups, quotients and extensions, and containing at least one non-trivial group; we call such a class 'good'. We shall denote the free pro-$\mathcal{C}$ group on d generators by $\widehat{F}_d(\mathcal{C})$. Now if Γ is a d-generator group and Γ does not involve a certain finite group H as an upper section, then the profinite completion $\widehat{\Gamma}$ is an image of $\widehat{F}_d(\mathcal{C})$ where $\mathcal{C}$ is some good class not containing H (for example, one of the classes $\mathcal{C}_k$ defined just below); so Theorem 3.1 follows from the more precise

Theorem 3.2 *Let $\mathcal{C}$ be a good class of finite groups that does not contain all finite groups. Let $d \geq 2$. Then the free pro-$\mathcal{C}$ group $\widehat{F}_d(\mathcal{C})$ has subgroup growth of strict type 2^n.*

Now for $k \geq 4$ let

$$\mathcal{C}_k$$

denote the class of all finite groups that do not involve $\mathrm{Alt}(k+1)$ as a section. Thus we have a stratification of the class of all finite groups:

$$\mathcal{S} \subset \mathcal{C}_4 \subset \mathcal{C}_5 \subset \ldots \subset \mathcal{C}_k \subset \mathcal{C}_{k+1} \subset \ldots$$

where $\mathcal{S}$ denotes the class of all finite soluble groups. Note that a d-generator group Γ does not involve $\mathrm{Alt}(k+1)$ as an upper section if and only if $\widehat{\Gamma}$ is an image of $\widehat{F}_d(\mathcal{C}_k)$. Now we can state

Theorem 3.3 *Let $d \geq 2$ and $k \geq 4$. Then*

$$\sigma(\widehat{F}_d(\mathcal{C}_k)) = \sigma^-(\widehat{F}_d(\mathcal{C}_k)) = (d-1)\frac{\log k!}{k-1}, \tag{3.1}$$

$$\sigma(\widehat{F}_d(\mathcal{S})) = \sigma^-(\widehat{F}_d(\mathcal{S})) = (d-1)\frac{\log 24}{3}. \tag{3.2}$$

Here, we have included the invariant

$$\sigma^-(G) = \liminf \frac{\log s_n(G)}{n}.$$

The theorem shows that our invariant σ is fine enough to distinguish alternating sections in free pro-$\mathcal{C}$ groups; however it cannot distinguish between prosoluble groups and groups having some other types of simple non-abelian sections, since $24^{1/3} = 4!^{1/(4-1)}$. Thus the alternating groups seem to play a special role when it comes to subgroup growth, a phenomenon we shall see again in Chapter 13.

In the cases where $\sigma(F) = \sigma^-(F) = \sigma$, say, the function $\log s_n(F)$ is asymptotic to σn; thus for any $\varepsilon > 0$ we have

$$2^{(\sigma-\varepsilon)n} < s_n(F) < 2^{(\sigma+\varepsilon)n}$$

for all large n. The theorem therefore implies (and refines) the upper bound for subgroup growth in Theorem 3.2, since any class $\mathcal{C}$ satisfying the given conditions clearly also satisfies $\mathcal{C} \subseteq \mathcal{C}_k$ for some $k \geq 4$. Applying the theorem to the profinite completion of a finitely generated group we obtain the following refinement of Theorem 3.1:

Corollary 3.4 *Let Γ be a d-generator group that does not involve $\mathrm{Alt}(k+1)$ as an upper section, where $d \geq 2$ and $k \geq 4$. Let $\varepsilon > 0$. Then*

$$s_n(\Gamma) < 2^{(\sigma+\varepsilon)n}$$

for all large n, where $\sigma = (d-1)(\log k!)/(k-1)$.

It is not known if this result is best possible: certainly Theorem 3.3 shows that it cannot be sharpened by "profinite" considerations alone, but the construction of a d-generator group Γ as in the corollary such that $\widehat{\Gamma}$ is sufficiently similar to $\widehat{F}_d(\mathcal{C}_k)$ is another problem.

Restricting the upper sections of a group also has dramatic consequences for the *maximal subgroup growth*, and again the alternating groups seem to wield particular influence.

Theorem 3.5 *Let G be a finitely generated profinite or abstract group.*

(i) *If G does not involve every finite group as an upper section then G has polynomial maximal subgroup growth.*

(ii) *If G has only finitely many distinct alternating groups as upper composition factors then G has maximal subgroup growth of type at most $n^{\log n}$.*

(iii) *If G has only finitely many distinct alternating and symmetric groups among its finite quotients then G has maximal subgroup growth of type at most $n^{\sqrt{n}}$.*

These results are established in Sections 1 and 2. The rest of the chapter concerns **pro-p groups**. In Section 3 we establish

Theorem 3.6 *Let F be the free pro-p group on $d \geq 2$ generators. Then for all $k \geq 1$ we have*

$$p^{\frac{d-1}{p-1}(p^k-1)-\frac{k(k-1)}{2}} \leq a_{p^k}(F) \leq p^{\frac{d-1}{p-1}(p^k-1)+k}.$$

It follows that $\log s_{p^k}(F) \sim p^k \cdot (d-1)\log p/(p-1)$ and hence that

$$\sigma(F) = (d-1)\log p/(p-1).$$

On the other hand, $\sigma^-(F) = \sigma(F)/p$; for the function $\log s_n(F)$ fluctuates between $n \cdot (d-1)\frac{\log p}{p-1} + o(1)$ and $\frac{n}{p} \cdot (d-1)\frac{\log p}{p-1} + o(1)$, since it is constant for n between p^k and $p^{k+1}-1$. In any case, it follows that *every non-abelian free pro-p group has strict growth type 2^n*. This implies the lower bound for

subgroup growth in Theorem 3.2, since if $\mathcal{C}$ is a good class of groups then $\mathcal{C}$ contains all finite p-groups for at least one prime p.

It is interesting to compare this result with Theorem 3.3. Thinking of F as a quotient of the free d-generator prosoluble group $\widehat{F}_d(\mathcal{S})$, we see that among all open subgroups of $\widehat{F}_d(\mathcal{S})$, the subnormal ones of p-power index have positive density, measured in a suitable logarithmic sense, and that this density is roughly proportional to $\frac{\log p}{p}$.

In Section 3 we also show how "Hall's enumeration principle" may be used to give a recursive formula for the numbers $a_{p^k}(F)$.

The last two sections deal with *normal subgroup growth*. The following result is established, as a counterpart to Theorem 2.7:

Theorem 3.7 *Let F be the free pro-p group on $d \geq 2$ generators. Then*

$$p^{k^2((d-1)^2/4d+o(1))} \leq a_{p^k}^{\lhd}(F) \leq p^{k^2(d-1)/2-k(d-3)/2-1}$$

where $o(1)$ is a term that tends to 0 as $k \to \infty$.

As before, this may be interpreted in terms of the number $f(p^k, d)$ of isomorphism types of d-generator groups of order p^k. Using Lemma 2.5 we have

Corollary 3.8 *Let $d \geq 2$. Then*

$$p^{k^2(d-1)^2/4d+o(k^2)} \leq f(p^k, d) \leq p^{k^2(d-1)/2+O(k)}.$$

(A slightly sharper upper bound will be given in §3.4 below.) As in the preceding chapter, these results are closely related to the number of (pro-p) relations required to define a d-generator finite p group. Writing

$$g(p^k, d)$$

for the smallest integer g such that every d-generator group of order p^k has a pro-p presentation on d generators with g relations, we shall prove

Theorem 3.9 *Let $d \geq 2$. Then*

$$g(p^k, d) \leq (d-1)k + 1 \quad \textit{for all } k \geq 1,$$
$$g(p^k, d) \sim (d-1)k \quad \textit{as } k \to \infty.$$

Theorem 3.7 shows that

$$\frac{(d-1)^2}{4d} \leq \liminf \frac{\log a_{p^n}^{\lhd}(F)}{n \log p^n} \leq \limsup \frac{\log a_{p^n}^{\lhd}(F)}{n \log p^n} \leq \frac{d-1}{2}.$$

This suggests the

Problem Does $\log a^{\lhd}_{p^n}(F)/n \log p^n$ tend to a limit as $n \to \infty$, and if so what is it?

It is worth remarking that all the results on 'relatively free' profinite groups may be interpreted as results about (absolutely) free abstract groups; for example, writing $\widehat{F}_d(p)$ for the d-generator free pro-p group, we have the 'dictionary'

$$\begin{aligned} a_n(\widehat{F}_d(\mathcal{S})) &= |\{H \leq F_d \mid |F_d : H| = n,\ F_d/\mathrm{core}_{F_d}(H) \text{ is soluble}\}| \\ a_{p^k}(\widehat{F}_d(p)) &= a^{\lhd\lhd}_{p^k}(F_d) \\ a^{\lhd}_{p^k}(\widehat{F}_d(p)) &= a^{\lhd}_{p^k}(F_d) \end{aligned}$$

where F_d is the free group on d generators and $\mathrm{core}_{F_d}(H)$ denotes the biggest normal subgroup of F_d contained in H.

Throughout this chapter, we shall use the convention that in the context of profinite groups, 'subgroup' means 'closed subgroup' and all homomorphisms are supposed continuous.

3.1 Upper bounds

In order to calculate the subgroup growth of a free group, we had to enumerate the transitive d-generator subgroups of $\mathrm{Sym}(n)$. Using the same approach, we can estimate the subgroup growth of a free pro-$\mathcal{C}$ group by enumerating the transitive d-generator $\mathcal{C}$-subgroups of $\mathrm{Sym}(n)$.

We begin with some generalities. Let $\mathcal{C}$ be a quotient-closed class of finite groups, and for $n \in \mathbb{N}$ let

$$\mathfrak{M}^t_{\mathcal{C}}(n)$$

denote the set of maximal transitive $\mathcal{C}$-subgroups of $\mathrm{Sym}(n)$ (i.e. maximal members of the set of subgroups that are both transitive and belong to $\mathcal{C}$). Clearly $\mathfrak{M}^t_{\mathcal{C}}(n)$ is a union of a certain number

$$\mathrm{Conj}^t_{\mathcal{C}}(n)$$

of conjugacy classes of subgroups in $\mathrm{Sym}(n)$. We write

$$\mathrm{Ord}^t_{\mathcal{C}}(n) = \max\{|H| : H \in \mathfrak{M}^t_{\mathcal{C}}(n)\}.$$

Proposition 3.1.1 *Let G be a pro-$\mathcal{C}$ group generated by d elements. Then for each n,*

$$a_n(G) \leq n \cdot \mathrm{Conj}^t_{\mathcal{C}}(n) \cdot \mathrm{Ord}^t_{\mathcal{C}}(n)^{d-1}.$$

Proof. According to Proposition 1.1.1, $a_n(G) = t_n(G)/(n-1)!$ where $t_n(G)$ is the number of transitive representations of G in $\mathrm{Sym}(n)$. Now if $\varphi : G \to$

$\mathrm{Sym}(n)$ is such a representation then $\varphi(G)$ is a transitive $\mathcal{C}$-subgroup of $\mathrm{Sym}(n)$; so for each such φ there exists $H \in \mathfrak{M}^t_{\mathcal{C}}(n)$ with $H \geq \varphi(G)$. It follows that

$$\begin{aligned} t_n(G) &\leq \sum_{H \in \mathfrak{M}^t_{\mathcal{C}}(n)} |\mathrm{Hom}(G,H)| \\ &\leq \sum_{H \in \mathfrak{M}^t_{\mathcal{C}}(n)} |H|^d . \end{aligned}$$

Now the conjugacy class of a subgroup H in $\mathrm{Sym}(n)$ has cardinality $|\mathrm{Sym}(n) : \mathrm{N}_G(H)| \leq n! \, |H|^{-1}$, so partitioning $\mathfrak{M}^t_{\mathcal{C}}(n)$ into conjugacy classes we get

$$\begin{aligned} \sum_{H \in \mathfrak{M}^t_{\mathcal{C}}(n)} |H|^d &\leq \mathrm{Conj}^t_{\mathcal{C}}(n) \cdot \max_{H \in \mathfrak{M}^t_{\mathcal{C}}(n)} \left(n! \, |H|^{-1} \, |H|^d \right) \\ &= n! \cdot \mathrm{Conj}^t_{\mathcal{C}}(n) \mathrm{Ord}^t_{\mathcal{C}}(n)^{d-1}. \end{aligned}$$

The proposition follows. ■

This simple proposition is very important: it shows that many subgroup growth questions are in essence questions about *finite permutation groups*. In this book we cannot go deeply into permutation group theory, and will have to be content with quoting a number of results. We should emphasise that these results about pemutation groups lie much deeper than the simple reduction arguments we are using here; for a proper understanding of the subgroup growth theorems of this section, the reader should really study the original literature referred to in the **Permutation groups window** (some of which was motivated by these subgroup growth questions).

Theorem 15 of the **Permutation groups** window may be stated as

Proposition 3.1.2 *Let $\mathcal{C}$ be a good class such that $\mathcal{S} \subseteq \mathcal{C} \subseteq \mathcal{C}_k$ for some k. Then there exists c depending only on $\mathcal{C}$ such that*

$$\mathrm{Conj}^t_{\mathcal{C}}(n) \leq n^c$$

for all n.

On the other hand, Theorem 8 of the **Permutation groups** window gives

Proposition 3.1.3 *Let $\mathcal{C} \subseteq \mathcal{C}_k^{\triangleleft}$ where $k \geq 4$. Then $\mathrm{Ord}^t_{\mathcal{C}}(n) \leq \mu^{n-1}$ where*

$$\mu = (k!)^{1/(k-1)}.$$

(Here $\mathcal{C}_k^{\triangleleft}$ denotes the class of all finite groups that do not have $\mathrm{Alt}(n)$ as a *composition factor* for any $n > k$; of course this class properly contains $\mathcal{C}_k$.)

Now let G be a d-generator pro-$\mathcal{C}$ group, where $\mathcal{S} \subseteq \mathcal{C} \subseteq \mathcal{C}_k$ and $k \geq 4$. Combining the last three propositions we get

$$a_n(G) \leq n \cdot n^c \cdot \mu^{(n-1)(d-1)};$$

it follows that

$$\begin{aligned}\log s_n(G) &\leq (c+1)\log n + (n-1)(d-1)\log\mu \\ &= n\cdot((d-1)\log\mu + o(1))\,.\end{aligned}$$

Thus

$$\sigma(G) \leq (d-1)\log\mu.$$

Taking $\mathcal{C} = \mathcal{C}_k$ gives the upper bound in (3.1) (which implies the upper bound for subgroup growth in Theorems 3.2 and 3.1). Taking $\mathcal{C}$ to be the class of soluble groups and $k = 4$ we get the upper bound in (3.2).

Suppose finally that $\mathcal{C}$ is the class of finite p-groups, for some prime p. Since the largest power of p dividing $n!$ is at most $(n-1)/(p-1)$, the analogue of Proposition 3.1.3 in this case has $\mu = p^{1/(p-1)}$, and we deduce in the same way that every d-generator pro-p group G satisfies

$$\sigma(G) \leq (d-1)\frac{\log p}{p-1}.$$

An alternative approach to pro-p groups, giving more precise results, is described in Section 3.

It remains to establish the upper bounds on *maximal* subgroup growth. We saw in §1.1 that $m_n(G) = p_n(G)/(n-1)!$ where $p_n(G)$ is the number of *primitive* permutation representations of G of degree n. It follows as before that if G is a d-generator pro-$\mathcal{C}$ group then

$$m_n(G) \leq n\cdot \mathrm{Conj}^p_{\mathcal{C}}(n)\cdot \mathrm{Ord}^p_{\mathcal{C}}(n)^{d-1},$$

where $\mathrm{Conj}^p_{\mathcal{C}}(n)$ denotes the number of conjugacy classes of maximal primitive $\mathcal{C}$-subgroups in $\mathrm{Sym}(n)$ and $\mathrm{Ord}^p_{\mathcal{C}}(n)$ the maximal order of a primitive $\mathcal{C}$-subgroup of $\mathrm{Sym}(n)$. It is easy to see that $\mathrm{Ord}^p_{\mathcal{C}}(n) \leq \mathrm{Ord}^t_{\mathcal{C}}(n)$ and $\mathrm{Conj}^p_{\mathcal{C}}(n) \leq \mathrm{Conj}^t_{\mathcal{C}}(n)$; part (i) of Theorem 3.5 is therefore a consequence of Proposition 3.1.2 together with

Proposition 3.1.4 *Let $\mathcal{C}$ be a good class of finite groups that does not contain all finite groups. Then there exists a constant c, depending on $\mathcal{C}$, such that*

$$\mathrm{Ord}^p_{\mathcal{C}}(n) \leq n^c$$

for every n.

(↬ **Permutation groups**, Theorem 4; note that $\mathcal{C} \subseteq \mathcal{B}_k$ for some k in the notation of the window.)

Similarly, Theorem 3.5(ii) follows from Theorems 13 and 16 of the Permutation groups window, which we restate as

Proposition 3.1.5 (i) *If $\mathcal{C} \subseteq \mathcal{C}_k^{\triangleleft}$ then*

$$\mathrm{Ord}_{\mathcal{C}}^{p}(n) \leq n^{c \log n}$$

where c depends only on k.

(ii) *If $\mathcal{C}$ is the class of all finite groups then*

$$\mathrm{Conj}_{\mathcal{C}}^{p}(n) \leq n^{c \log n} \tag{3.3}$$

where c is an absolute constant.

To prove part (iii) of Theorem 3.5, let Γ be a d-generator group and suppose that G does not have $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$ as a quotient when $n > n_0$. If $n > n_0$ and H is a primitive image of G in $\mathrm{Sym}(n)$ then H is a proper primitive group, hence satisfies $|H| \leq n^{c_0\sqrt{n}}$ where c_0 is an absolute constant ($\looparrowright$ **Permutation groups**, Theorem 1). Arguing as in the proof of Proposition 3.1.1 and using (3.3) we deduce that

$$p_n(\Gamma) \leq n^{c \log n} \cdot n! \cdot n^{(d-1)c_0\sqrt{n}}$$

for all $n > n_0$. Hence

$$m_n(\Gamma) = \frac{p_n(\Gamma)}{(n-1)!} \leq n^{1+c \log n+(d-1)c_0\sqrt{n}} \leq n^{a\sqrt{n}}$$

for sufficiently large n, if a is any constant larger than $(d-1)c_0$, and Theorem 3.5(iii) follows.

Theorem 3.5(i) shows that there is a huge jump – super-exponential to polynomial – between the maximal subgroup growth type of free groups on the one hand, and that of groups with restricted upper sections on the other. This 'jump' is not a 'gap', however: in Chapter 13 we construct finitely generated groups having a range of maximal subgroup growth types between n^n and $n^{\log n}$. These examples are all subcartesian products of finite alternating groups. Whether or not there is a gap in the possible types of maximal subgroup growth between $n^{\log n}$ and polynomial type is not at present clear.

3.2 Lower bounds

Let us begin with an easy example: it is not logically necessary for Theorem 3.3, but is instructive and has other applications. Fix a prime p, and for a positive integer t consider the group

$$\begin{aligned} G_t &= C_p \wr C_{p^t} \\ &= A \rtimes \langle x \rangle , \end{aligned}$$

where $\langle x \rangle$ is cyclic of order p^t and A is the group algebra $\mathbb{F}_p[\langle x \rangle]$, considered as an $\langle x \rangle$-module. Now A is an $\mathbb{F}_p$-vector space of dimension p^t, hence contains

$(p^{p^t}-1)/(p-1) > p^{p^t-1}$ subspaces of codimension 1. Thus G_t contains more than p^{p^t-1} subgroups of index p^{t+1}.

Now let

$$\begin{aligned}\Gamma &= C_p \wr C_\infty \\ &= \left\langle a, x;\, a^p = 1,\, [a^{x^i}, a^{x^j}] = 1 \text{ for all } i, j \right\rangle.\end{aligned}$$

Adding the relation $x^{p^t} = 1$ turns this group into G_t, so Γ maps onto each G_t. In a similar way we see that G_{t+1} maps onto G_t for each t, so we may form the inverse limit

$$G = \varprojlim G_t,$$

a two-generator metabelian pro-p group usually denoted $C_p \wr \mathbb{Z}_p$; in fact $G = \widehat{\Gamma}_p$.

Fix c with $1 < c < p^{1/p^2}$. Suppose now that $p^{t+1} \le n < p^{t+2}$. Then $s_n(\Gamma)$ and $s_n(G)$ are both at least equal to $a_{p^{t+1}}(G_t)$, which exceeds

$$p^{p^t-1} > p^{n/p^2-1} > c^n$$

for all sufficiently large values of n; thus we have established

Proposition 3.2.1 *Let p be a prime and let $1 < c < p^{1/p^2}$. Then*

$$\begin{aligned}s_n(C_p \wr C_\infty) &> c^n \\ s_n(C_p \wr \mathbb{Z}_p) &> c^n\end{aligned}$$

for all large n.

This shows that there exist 2-generator metabelian groups and 2-generator metabelian pro-p groups whose subgroup growth is *at least* exponential (indeed, the proof shows that this holds even for the growth of 2-step subnormal subgroups). This is therefore a *lower bound* for the strict growth type of any non-abelian free metabelian group, any non-abelian free metabelian pro-p group, and any non-abelian free prosoluble group.

If $\mathcal{C}$ is any good class of finite groups then $\mathcal{C}$ contains C_p for some prime p; provided $d \ge 2$ the free pro-$\mathcal{C}$ group $\widehat{F}_d(\mathcal{C})$ then maps onto $C_p \wr \mathbb{Z}_p$, hence has strict growth type which is at least exponential. This completes the proof of Theorem 3.2.

We now establish the lower bounds in Theorem 3.3. Slightly more generally, fix $k \ge 4$ and let $\mathcal{C}$ be any good class of finite groups that contains $\mathrm{Sym}(k)$ and all finite soluble groups. Let $\Phi_d = \widehat{F}_d(\mathcal{C})$ denote the free pro-$\mathcal{C}$ group on $d \ge 2$ generators, and write

$$\kappa = \frac{\log k!}{k-1}.$$

Step 1. For each $t \geq 0$,

$$\log a_{k^t}(\Phi_d) \geq \kappa(d-1)(k^t-1) - ct^2$$

where $c = (\log k)^2$.

This is trivial if $t = 0$. The general case is proved by induction on t, starting at $t = 1$. To start the induction, let F_d denote the (abstract, absolutely) free group on d generators, and let X be the intersection of the kernels of all homomorphisms from F_d into $\mathrm{Sym}(k)$. Then every subgroup of index k in F_d contains X. As $F_d/X \in \mathcal{C}$ it is an image of Φ_d, so we have

$$a_k(\Phi_d) \geq a_k(F_d) \geq k!^{d-1} \tag{3.4}$$

by Corollary 2.1.2. This gives the claim for $t = 1$ since $\kappa(k-1) = \log k!$.

Now suppose that $t > 1$, and put $m = k^{t-1}(d-1)+1$. By Schreier's formula for pro-$\mathcal{C}$ groups (↬ **Profinite groups**), each open subgroup H of index k^{t-1} in Φ_d is isomorphic to Φ_m, hence, by (3.4), contains at least $k!^{m-1}$ open subgroups of index k. By inductive hypothesis there are at least 2^n such subgroups H where

$$n = \kappa(d-1)(k^{t-1}-1) - c(t-1)^2.$$

On the other hand, given a subgroup L of index k^t in Φ_d, the number of distinct subgroups H of index k^{t-1} in Φ_d that contain L is at most

$$k^{t \log k}$$

(Lemma 1.2.3). Putting these estimates together we deduce that

$$\begin{aligned}
\log a_{k^t}(\Phi_d) &\geq n - t(\log k)^2 + (m-1)\log k! \\
&\geq \kappa(d-1)(k^{t-1}-1) - c(t-1)^2 - ct + \kappa(k-1)k^{t-1}(d-1) \\
&\geq \kappa(d-1)(k^t-1) - ct^2
\end{aligned}$$

as claimed.

Step 2. Now let $n > 1$ be arbitrary, and choose t and r so that

$$\begin{aligned}
k^{2t} &\leq n < k^{2(t+1)} \\
rk^t &\leq n < (r+1)k^t.
\end{aligned}$$

Fix an open subgroup H of index r in Φ_d; such subgroups exist, because Φ_d maps onto every finite cyclic group. As above, we see that $H \cong \Phi_{r(d-1)+1}$, so by Step 1 we have

$$\begin{aligned}
\log a_{k^t}(H) &\geq \kappa r(d-1)(k^t-1) - ct^2 \\
&\geq \kappa(d-1)n - \kappa(d-1)(r+k^t) - ct^2.
\end{aligned}$$

Since $r \leq k^{t+2} \leq k^2\sqrt{n}$ and $ct^2 \leq c(\log n/2\log k)^2 = (\log n)^2/4$, while $s_n(\Phi_d) \geq a_{k^t}(H)$, we infer that

$$\begin{aligned}\log s_n(\Phi_d) &\geq \log a_{k^t}(H)\\ &\geq \kappa(d-1)n - \kappa(d-1)(k^2+1)\sqrt{n} - (\log n)^2/4\\ &= \kappa(d-1)n - O(\sqrt{n}).\end{aligned}$$

It follows that $\sigma^-(\Phi_d) \geq \kappa(d-1)$. This completes the proof of Theorem 3.3 (for (3.2), take $k = 4$ and $\mathcal{C}$ to be the class of all finite soluble groups).

To conclude this section, let us show if $\mathcal{C}$ is a good class that includes C_p and C_q for distinct primes p and q then the free group $\widehat{F}_d(\mathcal{C})$ for $d \geq 2$ has *maximal* subgroup growth of *strict* type n. Say q is odd, and let s be the order of p modulo q. Then the order of p modulo q^{m+1} is $q^m s$ for each $m \geq 0$. Given $n \geq s$, let m be such that

$$q^m s \leq n < q^{m+1}s,$$

and put $t = q^m s$. The field $\mathbb{F}_{p^t}$ then contains a primitive element x of order q^{m+1}, and we form the group $H = \mathbb{F}_{p^t} \rtimes \langle x\rangle$ (where x acts by multiplication on the additive group of the field). It is easy to see that $\langle x\rangle$ is a self-normalising maximal subgroup of H, and that H is a 2-generator group in $\mathcal{C}$. Thus H, and therefore also $\widehat{F}_d(\mathcal{C})$, has at least $p^t \geq n^{1/q}$ maximal subgroups of index $p^t \leq n$.

3.3 Free pro-p groups

From now on we concentrate on pro-p groups. Throughout the rest of the chapter, the prime p is kept fixed, and we put

$$\mu = \frac{\log(p-1)}{\log p}.$$

Note that $0 \leq \mu < 1$ and that $\mu \to 1$ as $p \to \infty$. According to Proposition 1.6.2 and the remark following it, if G is a finitely generated pro-p group then

$$\begin{aligned}p^{d_{n-1}(G)-1} \leq a_{p^n}(G) &\leq p^{d^*_{n-1}(G)-n\mu},\\ a_{p^n}(G) &\geq \prod_{i=1}^{n} \frac{p^{\delta_{i-1}(G)}-1}{p^i-1}.\end{aligned} \tag{3.5}$$

Here

- $d_n(G) = \max\{d(H) \mid H \text{ a subgroup of } G \text{ of index } p^n\}$,
- $d^*_n(G) = \sum_{i=0}^{n} d_i(G)$,
- $\delta_n(G) = \min\{d(H) \mid H \text{ a subgroup of } G \text{ of index } p^n\}$.

Now let F be the free pro-p group on $d \geq 2$ generators. Schreier's index formula (↬ **Profinite groups**) shows that

$$\delta_k(F) = d_k(F) = p^k(d-1) + 1$$

for each $k \geq 1$. It follows that

$$d^*_{k-1}(F) - k\mu = \sum_{i=0}^{k-1} \left(p^i(d-1) + 1 - \mu\right) \leq \frac{d-1}{p-1}(p^k - 1) + k,$$

and hence that

$$a_{p^k}(F) \leq p^{\frac{d-1}{p-1}(p^k-1)+k}.$$

This gives the upper bound in Theorem 3.6.

For the lower bound, note that

$$\frac{p^{\delta_{i-1}(F)} - 1}{p^i - 1} > p^{\delta_{i-1}(F)-i}$$

for each $i \geq 1$, and

$$\sum_{i=1}^{k} (\delta_{i-1}(F) - i) = \frac{d-1}{p-1}(p^k - 1) - k(k-1)/2.$$

Combining these with (3.5) we deduce that

$$a_{p^k}(F) \geq p^{\frac{d-1}{p-1}(p^k-1)-\frac{k(k-1)}{2}}.$$

This completes the proof of Theorem 3.6.

To conclude this section, let us derive a recursive formula for $a_{p^k}(F)$. For brevity we write $\Psi_m = \widehat{F}_m(p)$ for each m, so $F = \Psi_d$. Also

$$\begin{bmatrix} d \\ t \end{bmatrix} = \frac{(p^d - 1)(p^d - p)\dots(p^d - p^{t-1})}{(p^t - 1)(p^t - p)\dots(p^t - p^{t-1})}.$$

Lemma 3.3.1 *For $k \geq 1$,*

$$a_{p^k}(\Psi_d) = \sum_{t=1}^{d} (-1)^{t+1} \begin{bmatrix} d \\ t \end{bmatrix} p^{t(t-1)/2} a_{p^{k-t}}(\Psi_{1+p^t(d-1)}). \tag{3.6}$$

Proof. Let $\Phi = \Phi(\Psi_d)$ denote the Frattini subgroup of Ψ_d. Let $\left\{K_{t,i}/\Phi \mid i = 1, \dots, \begin{bmatrix} d \\ t \end{bmatrix}\right\}$ be the list of subgroups of index exactly p^t in Ψ_d/Φ. By Schreier's theorem for pro-p groups (↬ **Pro-p groups**), each $K_{t,i}$ is a free pro-p group on $1 + p^t(d-1)$ generators. The result now follows immediately from Hall's enumeration principle (↬ **Pro-p groups**) applied to the collection of index p^k subgroups of Ψ_d. ■

This is a legitimate recursive formula, but it uses $a_{p^l}(\Psi_s)$ to express $a_{p^k}(\Psi_d)$ with $s \neq d$ ($s > d$ but $l < k$). It is not hard to deduce from this a relation which expresses $a_{p^k}(\Psi_d)$ using only $a_{p^t}(\Psi_d)$ for $t < k$:

Proposition 3.3.2 *For $k \geq 1$,*

$$a_{p^k}(\Psi_d) = \sum_{t=1}^{k} (-1)^{t+1}\, p^{t(t-1)/2} \begin{bmatrix} p^{k-t}(d-1)+1 \\ t \end{bmatrix} a_{p^{k-t}}(\Psi_d). \tag{3.7}$$

Proof. For brevity, let us write

$$a_{n,t} = a_{p^n}(\Psi_{1+p^t(d-1)}).$$

Certainly (3.7) is correct when $k = 1$. Let $n > 1$ and suppose inductively that (3.7) is valid whenever $k < n$. Putting $k = n$ in the right-hand side of (3.6) and applying the inductive hypothesis we obtain

$$\sum_{t=1}^{d} (-1)^{t+1} \begin{bmatrix} d \\ t \end{bmatrix} p^{t(t-1)/2} \cdot \sum_{s=1}^{n-t} (-1)^{s+1}\, p^{s(s-1)/2} \begin{bmatrix} p^{n-t-s}(p^t(d-1))+1 \\ s \end{bmatrix} a_{n-t-s,t}. \tag{3.8}$$

Putting $k = n$ in the right-hand side of (3.7) and applying (3.6) we obtain

$$\sum_{t=1}^{k} (-1)^{t+1}\, p^{t(t-1)/2} \begin{bmatrix} p^{n-t}(d-1)+1 \\ t \end{bmatrix} \cdot \sum_{s=1}^{d} (-1)^{s+1} \begin{bmatrix} d \\ s \end{bmatrix} p^{s(s-1)/2} a_{n-t-s,s}. \tag{3.9}$$

Observe now that (3.9) and (3.8) are equal (interchange the indices s and t). It follows that (3.7) is valid for $k = n$, and the proof is complete. ■

3.4 Normal subgroups in free pro-p groups

In the preceding chapter, we were able to estimate the number of d-generator groups of order n by obtaining an upper bound for the number of (profinite) relations needed to define such a group. The same approach is effective when dealing with finite p-groups. In fact the proof given in §2.3 applies directly to groups of p-power order; however, as the finite simple p-groups are much easier to understand than finite simple groups in general, the argument is very much simpler in this case, so let us give it here.

Proposition 3.4.1 *Let G be a group of order $p^k > 1$ with a generating set X of size d. Then G has a presentation $\langle X; R\rangle$ where $|R| \leq dk$.*

Proof. Suppose first that $k = 1$. If $G = \langle x_1, \ldots, x_d\rangle$ has order p then x_i alone generates G for some i and then G has a presentation of the form

$$G = \left\langle x_1, \ldots, x_d;\ x_i^p = 1,\ x_j = x_i^{e(j)}\ (j \neq i) \right\rangle.$$

Now let $k > 1$ and suppose that $G = \langle x_1, \ldots, x_d\rangle$ has order p^k. Then G has a central subgroup N of order p. Inductively, we may suppose that G/N has a presentation

$$G/N = \langle x_1N, \ldots, x_dN;\ u_i(\mathbf{x}N) = 1\ (1 \leq i \leq r)\rangle \tag{3.10}$$

where $r = d(k-1)$. Since $|G| > |G/N|$ and $x_1, \ldots, x_d$ generate G, the relations $u_i(\mathbf{x}) = 1$ cannot all hold in G, so there exists t such that the element $u_t(\mathbf{x}) = z$ actually generates N. Then $u_i(\mathbf{x}) = z^{e(i)}$ where $0 \leq e(i) \leq p-1$ for $i = 1, \ldots, r$. It is easy to see that the following is then a presentation for G :

$$G = \left\langle \begin{array}{c} x_1, \ldots, x_d; \\ u_t(\mathbf{x})^p = 1,\ [x_j, u_t(\mathbf{x})] = 1\ (1 \leq j \leq d), \\ u_i(\mathbf{x}) = u_t(\mathbf{x})^{e(i)}\ (1 \leq i \leq r,\ i \neq t) \end{array} \right\rangle.$$

Thus G is defined by $1 + d + d(k-1) - 1 = dk$ relations on the given generators. ■

Note that we obtain here a presentation in the category of groups. For purposes of enumeration, it is enough to consider *pro-p presentations* (just as profinite presentations sufficed in Chapter 2), and for these we have a slightly better result:

Theorem 3.4.2 *Let G be a group of order $p^k > 1$ with a generating set X of size d. Then G has a pro-p presentation $\langle X; R \rangle$ where $|R| \leq (d-1)k + 1$.*

We postpone the proof, which is couched in the language of graded Lie algebras, to the next section, and proceed now to deduce the upper bounds stated in Theorem 3.7 and Corollary 3.8.

Let F be the free pro-p group on $d \geq 2$ generators. Suppose that $N \lhd_o F$ and $|F : N| = p^n > 1$. Write

$$\Phi_F(N) = N^p[N, F],\ d_F(N) = \dim_{\mathbb{F}_p}(N/\Phi_F(N)).$$

Thus $d_F(N)$ is the number of generators required by N as a closed normal subgroup of F. According to Theorem 3.4.2, $d_F(N) \leq (d-1)n+1$, so $N/\Phi_F(N)$ is an elementary abelian p-group of rank at most $(d-1)n+1$. Such a group has fewer than $p^{(d-1)n+1}$ subgroups of index p, and this is then an upper bound for the number of open normal subgroups of F that are contained in N and have index p^{n+1}. Since every open normal subgroup of index p^{n+1} is contained in at least one of index p^n this shows that for $n \geq 1$,

$$a^{\lhd}_{p^{n+1}}(F) < a^{\lhd}_{p^n}(F) \cdot p^{(d-1)n+1}.$$

Since $a^{\lhd}_p(F) < p^d$ it follows inductively that

$$a^{\lhd}_{p^n}(F) < p^{n^2(d-1)/2 - n(d-3)/2 + d - 1}.$$

The number of isomorphism types of d-generator groups of order p^n is denoted $f(p^n, d)$. Since $f(p^1, d) = 1$, a similar argument yields

$$f(p^n, d) \leq p^{n^2(d-1)/2 - n(d-3)/2 - 1}.$$

Using Proposition 3.4.1, proved above, instead of Theorem 3.4.2, the same kind of argument yields slightly weaker upper bounds, of order $p^{n^2 d/2}$.

We turn now to the lower bounds. These will follow from a corresponding lower bound for the number of pro-p defining relations. Indeed, we shall show that Theorem 3.4.2 is very sharp in the sense that for every k, there exists a d-generator group of order p^k that needs 'about' $(d-1)k$ pro-p relations. Let

$$g(p^k, d) = \max\left\{d_F(N) \mid N \lhd_o F, |F:N| = p^k\right\}$$

where as above F is the free pro-p group on d generators; thus $g(p^k, d)$ is the least integer r such that every d-generator group of order p^k has a d-generator pro-p presentation with r relations.

Theorem 3.4.3 *Let $d \geq 2$. Then*

$$g(p^k, d) \sim (d-1)k$$

as $k \to \infty$.

This will be proved below. Now given k, we can find $N \lhd_o F$ with $|F:N| = p^k$ and $d_F(N) = g(p^k, d) = g$, say. For each n with $k < n < k+g$ we then have

$$a_{p^n}^{\lhd}(F) \geq a_{p^{n-k}}(N/\Phi_F(N)) > p^{(n-k)(g-n+k)}.$$

We would like to maximize this lower bound by choosing k optimally with respect to n. Putting $k = xn$ and supposing temporarily that $g = (d-1)k$, we find that $(n-k)(g-n+k) = n^2((d+1)x - dx^2 - 1)$ has its maximum at $x = (d+1)/2d$. This suggests that we choose $k = [(d+1)n/2d]$, which yields

$$(n-k)(g-n+k) \geq \frac{(d-1)n}{2d} \cdot \frac{(d-1+\varepsilon(k))n}{2} = \frac{(d-1)^2 n^2}{4d} + o(n^2)$$

(here $\varepsilon(k) \to 0$ as $k \to \infty$). Thus $a_{p^n}^{\lhd}(F) \geq p^{n^2(d-1)^2/4d + o(n^2)}$; with the upper bound given above this establishes

Theorem 3.7 *Let F be the free pro-p group on $d \geq 2$ generators. Then as $n \to \infty$,*

$$p^{n^2(d-1)^2/4d + o(n^2)} \leq a_{p^n}^{\lhd}(F) \leq p^{n^2(d-1)/2 + n/2};$$

if $d \geq 3$ the $n/2$ term on the right may be omitted.

The rest of this section is devoted to the proof of Theorem 3.4.3. As above, F denotes the free pro-p group on $d \geq 2$ generators (it may equally well be the abstract free group on d generators, if the reader prefers). We write

$$\Gamma_n = \gamma_n(F), \;\; P_n = P_n(F)$$

for the terms of the lower central series and of the lower central p-series of F. These are related in the following way: for each $k \geq 1$ there is a bijective mapping

$$\theta_k : \prod_{i=1}^{k} \Gamma_i/\Phi_F(\Gamma_i) \to P_k/P_{k+1}, \tag{3.11}$$

$$(\overline{x_1}, \ldots, \overline{x_k}) \mapsto x_1^{p^{k-1}} x_2^{p^{k-2}} \ldots x_k P_{k+1} \tag{3.12}$$

where $\overline{x_i} = x_i\Phi_F(\Gamma_i)$; moreover θ_k is a group isomorphism unless $p = 2$, in which case the restriction of θ_k to $\prod_{i=2}^{k}\Gamma_i/\Phi_F(\Gamma_i)$ is a homomorphism; for the proof see e.g. [HB] Chapter VIII, Theorem 1.9(b). For $k \geq 2$ and $i = 2, \ldots, k$ let

$$P_k(i)/P_{k+1} = \theta_k\left(\prod_{j=1}^{i}\Gamma_j/\Phi_F(\Gamma_j)\right),$$

so $P_k = P_k(k) > P_k(k-1) > \ldots > P_k(2) > P_{k+1}$. If p is odd these are evidently subgroups of P_k; this remains true if $p = 2$ – it suffices to check that for x, $y \in F$,

$$x^{2^k}y^{2^k} \equiv (xy)^{2^k} \mod P_k(2),$$

and this follows from the fact that

$$x^{2^k}y^{2^k}(xy)^{-2^k} \in \Gamma_2^{2^k}\prod_{l=1}^{k}\Gamma_{2^l}^{2^{k-l}},$$

an application of the 'Hall-Petrescu identity'; see e.g. [DDMS], Lemma 11.9(i). Another application of the same identity gives

Lemma 3.4.4

$$P_k(i)^p = P_{k+1}(i) \qquad \textit{if } \ 2 \leq i \leq k$$
$$P_k(i)^p \leq [P_k(i-1), F]P_{k+1}(i-1) \qquad \textit{if } \ 3 \leq i \leq k.$$

Proof. The mapping $x \mapsto x^p$ induces a homomorphism $\pi : P_k/P_{k+1} \to P_{k+1}/P_{k+2}$ such that $\theta_{k+1} = \pi \circ \theta_k$; this implies the first claim. Now let $i \geq 3$ and suppose that $x \in \Gamma_{i-1}$, $y \in F$. According to [DDMS], Lemma 11.9(ii) we have

$$[x,y]^{p^{k+1}}[x^{p^{k+1}},y]^{-1} \in \Gamma_2^{p^{k+1}}\prod_{l=1}^{k+1}\Gamma_{p^l}^{p^{k+1-l}}$$
$$\leq P_{k+2}.$$

The second claim of the lemma now follows since $P_k(i)$ is generated by $P_k(i-1)$ together with elements of the form $[x,y]^{p^k}$ with $x \in \Gamma_{i-1}$, for which $x^{p^{k+1}} \in P_k(i-1)$. ■

Corollary 3.4.5 *(i) Let $P_{k+1} \leq M \leq N \leq P_k$, where $k \geq 2$, and put $|N : M| = p^m$. Then*

$$d_F(N) \geq d_F(M) - dm.$$

(ii) Let $P_{k+1} \leq N \leq P_k$ and put $|N : P_{k+1}| = p^m$. If (a) $P_k(i-1) \leq N \leq P_k(i)$ where $i \geq 3$ or (b) $N \leq P_k(2)$ then

$$d_F(N) \geq d_F(P_{k+1}) - (d-1)m - d(d+1)/2.$$

Proof. Say $F = \langle g_1, \dots, g_d \rangle$ and $N = \langle u_1, \dots, u_m \rangle M$. Then $\Phi_F(N)$ is generated modulo $\Phi_F(M)$ by $\{u_1^p, \dots, u_m^p\} \cup \{[u_j, g_l] \mid j \leq m,\, l \leq d\}$, so

$$\dim_{\mathbb{F}_p} (\Phi_F(N)/\Phi_F(M)) \leq (d+1)m.$$

It follows that

$$\begin{aligned} m + d_F(M) = \log_p |N : \Phi_F(M)| &= d_F(N) + \log_p |\Phi_F(N) : \Phi_F(M)| \\ &\leq d_F(N) + (d+1)m. \end{aligned}$$

This gives (i).

Now let N be as in (ii)(a) and put $M = P_k(i-1)$. Then Lemma 3.4.4 gives

$$\begin{aligned} N^p \leq P_k(i)^p &\leq [P_k(i-1), F] P_{k+1}(i-1) \\ &= [M, F] M^p = \Phi_F(M); \end{aligned}$$

so $\Phi_F(N) = [N, F]\Phi_F(M)$ and the argument used above shows that now $d_F(N) \geq d_F(M) - (d-1)m_0$ where $p^{m_0} = |N : M|$. Putting $|P_k(j) : P_k(j-1)| = p^{m_j}$, we see similarly that

$$d_F(P_k(j)) \geq d_F(P_k(j-1)) - (d-1)m_j$$

for $i - 1 \geq j \geq 3$. On the other hand, part (i) applied to the pair $N = P_k(2) > M = P_{k+1}$ gives

$$d_F(P_k(2)) \geq d_F(P_{k+1}) - d(m_2 + m_1),$$

and putting these together gives

$$\begin{aligned} d_F(N) &\geq d_F(P_{k+1}) - (d-1)(m_0 + m_{i-1} + \cdots + m_3) - d(m_2 + m_1) \\ &= d_F(P_{k+1}) - (d-1)m - (m_2 + m_1). \end{aligned}$$

If $N \leq P_k(2)$ then $m \leq m_2 + m_1$, and (i) with $M = P_{k+1}$ gives

$$d_F(N) \geq d_F(P_{k+1}) - (d-1)m - m \geq d_F(P_{k+1}) - (d-1)m - (m_2 + m_1).$$

Part (ii) follows in either case since

$$m_2 + m_1 = \dim_{\mathbb{F}_p}(\Gamma_2/\Phi_F(\Gamma_2)) + \dim_{\mathbb{F}_p}(\Gamma_1/\Phi_F(\Gamma_1)) = \frac{d(d-1)}{2} + d = \frac{d(d+1)}{2}.$$

■

We can now complete the

Proof of Theorem 3.4.3 It follows from Theorem 3.4.2 (to be proved in the next section) that $g(p^n, d) \leq 1 + (d-1)n \sim (d-1)n$. Now let $n \geq d(d+1)/2$. Then for a suitable value of $k \geq 3$ we can find an open normal subgroup N of F with $|F : N| = p^n$ such that *either*

$$P_k(i-1) \leq N \leq P_k(i)$$

for some $i \geq 3$, *or*

$$P_{k+1} \leq N \leq P_k(2).$$

Write

$$p^{s(k)} = |F : P_{k+1}|\,,\ p^{r(k)} = |P_{k+1} : P_{k+2}|\,.$$

Then $|N : P_{k+1}| = p^{s(k)-n}$ and $d_F(P_{k+1}) = r(k)$, so from the Corollary we have

$$\begin{aligned} d_F(N) &\geq r(k) - (d-1)(s(k)-n) - d(d+1)/2 \\ &= (d-1)n + r(k) - (d-1)s(k) - d(d+1)/2. \end{aligned}$$

Since $g(p^n, d) \geq d_F(N)$ and $n \geq s(k-1)$, it will therefore suffice to prove that

$$\frac{(d-1)s(k) - r(k)}{s(k-1)} \to 0 \tag{3.13}$$

as $k \to \infty$.

Let $M(i) = \dim_{\mathbb{F}_p}(\Gamma_i/\Phi_F(\Gamma_i))$. Then $M(i)$ is equal to the rank of the free abelian group Γ_i/Γ_{i+1}, and this is given recursively by a famous formula due to Witt:

$$d^n = \sum_{j|n} jM(j);$$

see for example [HB] Chapter VIII, Theorem 11.15. It is easy to see that

$$M(n) \sim d^n/n;$$

indeed, if $n \geq 8$ and $C = C_n \geq 2$ is a constant such that $jM(j) \leq Cd^j$ for all $j < n$ then

$$\frac{nM(n)}{d^n} - 1 = \sum_{j|n, j<n} \frac{jM(j)}{d^n} \leq Cnd^{-n/2} \leq C/2 \leq C - 1$$

so $nM(n) \leq Cd^n$. By induction this holds for all n with $C = C_8$, and the claim follows since $Cnd^{-n/2} \to 0$ as $n \to \infty$.

The bijection θ_k shows that $r(k) = \sum_{i=1}^{k+1} M(i)$, and $s(k) = \sum_{i=0}^{k-1} r(i)$. From elementary analysis we deduce that

$$\begin{aligned} r(k) &\sim \frac{d^{k+2}}{(d-1)k}, \\ s(k) &\sim \frac{d^{k+2}}{(d-1)^2 k} \sim \frac{r(k)}{d-1}. \end{aligned}$$

Thus

$$(d-1)s(k) - r(k) = o(r(k)) = o(s(k-1))$$

and (3.13) follows.

3.5 Relations in p-groups and Lie algebras

Theorem 3.4.2, stated above, is equivalent to

Theorem 3.5.1 *Let F be the free pro-p group on $d \geq 2$ generators and N an open normal subgroup of index $p^m > 1$ in F. Then*

$$\dim_{\mathbb{F}_p}(N/[N,F]N^p) \leq (d-1)m + 1.$$

The result, and the proof, are the same if F is taken instead to denote the abstract free group. We shall deduce it from an analogous result about Lie algebras. To effect the translation, we first associate a graded Lie algebra to F, in the following way. Write Γ_i for the ith term of the lower central series of F, put $L_i = \Gamma_i/\Gamma_{i+1}$, and define a bracket operation $L_i \times L_j \to L_{i+j}$ by setting

$$[x\Gamma_{i+1}, y\Gamma_{j+1}] = [x,y]\Gamma_{i+j+1} \qquad (x \in \Gamma_i,\ y \in \Gamma_j).$$

It is easy to see that this is a well-defined bilinear mapping (writing the group operation in each L_i additively), and it extends to a binary operation on the direct sum

$$L = \bigoplus_{i=1}^{\infty} L_i.$$

This makes L into a Lie ring (the Jacobi identity follows from the group-theoretic Hall-Witt identity; see e.g. [HB] Chapter VIII, § 9). Since F is a free pro-p group, each of the factors $\Gamma_i/\Gamma_{i+1} = L_i$ is actually a free $\mathbb{Z}_p$-module of rank $M(i)$, defined in the preceding section; all we need here, however, is that L is *additively torsion-free:* indeed, each L_i is torsion-free because the lower central factors of a free group are free abelian ([HB] Chapter VIII, Theorem 11.15). Since $[L,L] = \bigoplus_{i>1} L_i$ we have

$$\dim_{\mathbb{F}_p}(L/([L,L] + pL)) = \dim_{\mathbb{F}_p}(F/(\Gamma_2 F^p)) = d.$$

Now let N be as in the theorem, put

$$N_i = \frac{(N\Gamma_{i+1}) \cap \Gamma_i}{\Gamma_{i+1}} \leq L_i$$

and let

$$L(N) = \bigoplus_{i=1}^{\infty} N_i.$$

It is easy to see that then $L(N)$ is an ideal in the Lie algebra L and that $|L : L(N)| = |F : N|$. Since $[(N\Gamma_i) \cap \Gamma_{i-1}, F] \leq [N,F]\Gamma_{i+1} \cap \Gamma_i$ for each $i > 1$, we have

$$[L(N), L] + pL(N) \subseteq L(N^*)$$

where $N^* = [N,F]N^p$. Thus $\dim_{\mathbb{F}_p}(N/N^*) \leq \dim_{\mathbb{F}_p}(L/\Phi_L(L(N)))$, where for an ideal H of L we write

$$\Phi_L(H) = [H,L] + pH.$$

Theorem 3.5.1 therefore follows from the second claim in the next result:

Theorem 3.5.2 *Let L be a Lie ring and H an ideal of L such that L/H is nilpotent. Suppose that*

$$\dim_{\mathbb{F}_p}(L/\Phi_L(L)) = d \geq 2,\ |L:H| = p^m > 1.$$

Then

$$\dim_{\mathbb{F}_p}(H/\Phi_L(H)) \leq \begin{cases} (d-1)m & \text{if } pL = 0 \\ (d-1)m+1 & \text{if } L \text{ has no additive } p\text{-torsion} \end{cases}.$$

Proof. *Case 1:* where $pL = 0$. Consider L as an $\mathbb{F}_p$-algebra. We may suppose that $\Phi_L(H) = 0$ and have to bound $\dim(H)$. Since L/H is nilpotent, there exists $x \in L \setminus H$ with $[x, L] \subseteq H$. If $m = 1$ then $L = H + x\mathbb{F}_p$ so $\Phi_L(L) = [L, H] + [x, x]\mathbb{F}_p = 0$ and $\dim L = d$, giving the result in this case. If $m > 1$, put $M = H + x\mathbb{F}_p$. Arguing by induction we may suppose that $\dim(M/\Phi_L(M)) \leq (d-1)(m-1)$. Since $[[M, L], L] \subseteq [H, L] = 0$ we have $[M, \Phi_L(L)] = 0$; since $\Phi_L(M) = [H, L] + [x, L]$ it follows that $\dim(\Phi_L(M)) \leq d$. Thus

$$\dim(H) = \dim(M) - 1 \leq (d-1)(m-1) + d - 1 = (d-1)m.$$

Case 2: where L has no p-torsion (this hypothesis is not needed until subcase 2.3, in fact).

Subcase 2.1: Where $H \supseteq \Phi_L(L)$. Then $m \leq d$ and $L = H + x_1\mathbb{Z} + \cdots + x_m\mathbb{Z}$, say. We have

$$\Phi_L(L) = \Phi_L(H) + \sum_{i=1}^{m} px_i\mathbb{Z} + \sum_{1 \leq i < j \leq m} [x_i, x_j]\mathbb{Z} \subseteq H,$$

whence

$$\begin{aligned} \dim(H/\Phi_L(H)) &= \dim(L/\Phi_L(L)) + \dim(\Phi_L(L)/\Phi_L(H)) - m \\ &\leq d + \left(m + \frac{1}{2}m(m-1)\right) - m \\ &\leq (d-1)m + 1 \end{aligned}$$

since $m \leq d$ and $d \geq 2$.

Subcase 2.2: Where $H \not\supseteq [L, L]$ but $H \supseteq pL$. Since L/H is nilpotent we can find an element $x \in [L, L] \setminus H$ such that $[x, L] \subseteq H$ and $px \in H$. Now put $M = H + x\mathbb{Z}$. Then

$$px \in p[L, L] = [pL, L] \subseteq [H, L]$$

so we have

$$\Phi_L(M) = \Phi_L(H) + [x, L].$$

The result now follows inductively in a similar way to Case 1 above.

Subcase 2.3: Suppose finally that $pL \not\subseteq H$. Again we argue by induction on m. Put $H_1 = H \cap pL$ and $H_2 = H + pL$. Applying Case 1 to the Lie algebra L/pL we have

$$\dim(H_2/(\Phi_L(H_2) + pL)) \leq (d-1)a$$

where $|L : H_2| = p^a$. Now put

$$M = p^{-1}H_1.$$

Then M properly contains H and $M \neq L$; inductively we may assume that

$$\dim(M/\Phi_L(M)) \leq (d-1)b + 1$$

where $|L : M| = p^b$. Now multiplication by p induces an (additive) isomorphism $M/\Phi_L(M) \to H_1/\Phi_L(H_1)$, so

$$\dim(H_1/\Phi_L(H_1)) \leq (d-1)b + 1.$$

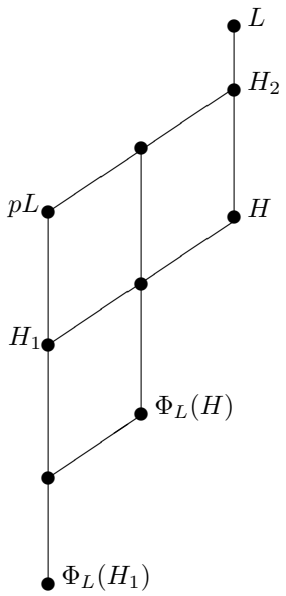
But

$$\begin{aligned} p^b = |L : M| &= |pL : pM| \\ &= |pL : H_1| = |H_2 : H| = p^{m-a}. \end{aligned}$$

The result follows, since it is easy to see from the picture that

$$\dim(H/\Phi_L(H)) \leq \dim(H_1/\Phi_L(H_1)) + \dim(H_2/(\Phi_L(H_2) + pL)).$$

■



Notes

Theorem 3.1 (as well as the upper bound in Theorem 3.2) is due to [**Pyber & Shalev 1996**]. (They state a stronger form of Theorem 3.1, concerning groups with restricted upper composition factors; however, there is a gap in the proof of Corollary 2.2(ii) of that paper, and the result in the stronger form remains in doubt; we are grateful to these authors for pointing this out.) The fundamental result Proposition 3.1.1 is also from [**Pyber & Shalev 1996**].

Theorem 3.3 was proved for $k \geq 9$ (and conjectured in general) by **A. Mann** (unpublished). The bounds for primitive permutation groups required to complete the missing cases $4 \leq k \leq 8$ were established by **Atila Maróti** ($\leadsto$ **Permutation groups**, §1).

Theorem 3.5(i) is due to [**Borovik, Pyber & Shalev 1996**]. Parts (ii) and (iii) of Theorem 3.5 are due to [**Pyber & Shalev 1997**].

Theorem 3.6 and the material of §3.3 are from [**Ilani 1989**].

Earlier versions of Theorem 3.7 and Corollary 3.8 are due to [**Neumann 1969**], who obtained slightly weaker upper bounds (of order $p^{kd^2/2}$), and [**Mann 1998**], who obtained significantly weaker lower bounds (p^{ck^2} for some small $c > 0$). The sharper results given here are due to **Andrei Jaikin-Zapirain**

(unpblished), who is responsible for Theorem 3.9 and the material of §3.5. (In a slightly longer argument he also obtains the better lower bound $p^{k^2((d-1)/4+o(1))}$ in Theorem 3.7, still some way short of the corresponding upper bound.)

Chapter 4

Pro-p groups

In this chapter we consider the subgroup growth of pro-p groups that are in some sense smaller than the free ones. We begin in Section 1 with one of the fundamental results on subgroup growth,

Theorem 4.1 *The finitely generated pro-p groups with polynomial subgroup growth are precisely the pro-p groups of finite rank.*

The pro-p groups of finite rank are just the *p-adic analytic* pro-p groups, a well-known and much studied class of groups (↬ **Pro-p groups**). Each such pro-p group has a well defined *dimension*, and we show that the 'degree' of polynomial subgroup growth is bounded above and below by constant mutliples of the dimension.

Theorem 4.1 is strengthened in Section 2, where we establish

Theorem 4.2 *Let G be a pro-p group. If*

$$s_n(G) \leq n^{c \log_p n}$$

for all sufficiently large n, where $c < 1/8$ is a constant, then G has finite rank.

A noteworthy feature of this result is that it demonstrates a *gap* in the "growth spectrum" of pro-p groups: it shows that any finitely generated pro-p group *either* has growth type $\leq n$ *or* has growth type at least $n^{\log n}$. Actually the known growth types achieved by finitely generated pro-p groups are rather sparse, but whether further gaps really exist is at present a complete mystery.

However, it is known that the gap $(n, n^{\log n})$ is not any wider. In Sections 3, 4 and 5 we determine the subgroup growth of some specific pro-p groups: the Nottingham group, the groups $\mathrm{SL}_d^1(\mathbb{F}_p[[t]])$, and more generally the so-called 'Λ-perfect' analytic groups over pro-p rings. All these groups have infinite rank and growth type $n^{\log n}$, showing that Theorem 4.2 is best possible as regards growth type; the more delicate problem of finding the best bound for c is still open: this bound lies somewhere between 1/8 and 1/2.

The final section is devoted to **finitely presented pro-p groups**. The main result here is

Theorem 4.3 *Let G be a finitely presented pro-p group. Then* either *G has subgroup growth of type at most $2^{\sqrt{n}}$* or *G contains a non-abelian free pro-p subgroup.*

It follows that if G does not involve every finite p-group as an upper section, then the subgroup growth of G is significantly less than that of a free pro-p group (which is exponential): so the theorem is a pro-p analogue to Theorem 3.1. This striking result depends on a deep theorem of Zelmanov about pro-p groups satisfying the Golod-Shafarevich condition.

We continue to use the convention that in the context of profinite groups, 'subgroup' means 'closed subgroup'.

4.1 Pro-p groups with polynomial subgroup growth

The most thoroughly studied class of pro-p groups is the pro-p groups of *finite rank.* We recall that the *rank* of a profinite group G is defined by

$$\begin{aligned}\mathrm{rk}(G) &= \sup\{d(H) \mid H \text{ a closed subgroup of } G\}\\ &= \sup\{d(H) \mid H \text{ an open subgroup of } G\}.\end{aligned}$$

Several alternative characterisations are known for the class of pro-p groups of finite rank, some of which are listed in the **Pro-p groups** window**.** The most spectacular one is that a *pro-p group has finite rank if and only if it has the structure of a p-adic analytic group*; for present purposes, some more algebraic criteria are relevant, and we shall state them below. The purpose of this section is establish Theorem 4.1 which characterises this class in terms of subgroup growth.

Suppose to begin with that G is a pro-p group of finite rank r. Each finite quotient Γ of G is a p-group of rank at most r, hence satisfies

$$s_n(\Gamma) \leq n^{1+r}$$

for each n, by Lemma 1.4.1. Since $s_n(G)$ is the supremum of $s_n(\Gamma)$ over all such Γ it follows that $s_n(G) \leq n^{1+r}$. Thus G has polynomial subgroup growth.

A sharper bound can be deduced from Proposition 1.6.2, which shows that

$$a_{p^k}(G) \leq p^{d^*_{k-1}(G)-k\mu}$$

where $\mu = \log(p-1)/\log p$ and

$$d^*_{k-1}(G) = \sum_{i=0}^{k-1} d_i(G) \leq kr;$$

recall that $d_i(G) = \max\{d(H) \mid |G : H| = p^i\}$. It follows that $a_{p^k}(G) \leq p^{(r-\mu)k}$ and hence that

$$s_n(G) \leq \sum_{p^k \leq n} p^{(r-\mu)k} < c \cdot n^{r-\mu},$$

where $c = p^{r-\mu}/(p^{r-\mu} - 1)$. Hence

$$\alpha(G) := \limsup \frac{\log s_n(G)}{\log n} \leq r - \mu.$$

It remains to show that polynomial subgroup growth implies finite rank. This depends on the following fact (↬ **Pro-p groups**):

Proposition 4.1.1 *Let G be a pro-p group. Then G has finite rank if and only if there exists $k < \infty$ such that $d(N) \leq k$ for every open* normal *subgroup N of G.*

This will be applied in conjunction with

Lemma 4.1.2 *Let G be a finitely generated pro-p group and k a positive integer. Let N be an open normal subgroup of G maximal with the property that $d(N) \geq k$. Then*

$$|G : N| \leq p^{(k-1)\lambda}$$

where $\lambda = \lceil \log d(N) \rceil$.

Proof. Put $C = \mathrm{C}_G(N/\Phi(N))$; then $N \leq C \lhd G$. Suppose that $C > N$. Then $(C/N) \cap \mathrm{Z}(G/N)$ contains a subgroup $M/N = \langle N, x \rangle / N$ of order p. Now

$$[M, M] \leq [N, N] \cdot [N, x] \leq \Phi(N)$$

so $M/\Phi(N)$ is abelian; therefore

$$d(M) \geq d(M/\Phi(N)) \geq d(N/\Phi(N)) = d(N) \geq r.$$

This contradicts the choice of N as $M > N$. It follows that $N = \mathrm{C}_G(N/\Phi(N))$.

The p-group G/N therefore acts faithfully on the $\mathbb{F}_p$-vector space $N/\Phi(N)$, hence may be embedded in the group $U_d(\mathbb{F}_p)$ of $d \times d$ upper uni-triangular matrices over $\mathbb{F}_p$, where $d = d(N)$ is the dimension of this vector space. Now it is easy to see that $U_d(\mathbb{F}_p)$ has a filtration $(U(i))_{i=0}^{\lambda}$ of normal subgroups such that each factor $U(i-1)/U(i)$ is elementary abelian. Intersecting this with G/N gives a chain $G = N_0 > N_1 > \ldots > N_t = N$, where $t \leq \lambda$ and each N_{i-1}/N_i is elementary abelian. From the choice of N we have $d(N_{i-1}/N_i) \leq d(N_{i-1}) \leq k - 1$ for each i, so $|N_{i-1} : N_i| \leq p^{k-1}$ for each i. Hence $|G : N| \leq p^{(k-1)t} \leq p^{(k-1)\lambda}$. ■

Now let G be a pro-p group and suppose that $s_n(G) \leq n^\alpha$ for all n. We have to show that G has finite rank. We note to begin with that G is finitely

generated: otherwise $G/\Phi(G)$ would have infinitely many subgroups of index p. Now let k be such that $d(N) \geq k$ for some open normal subgroup N of G. Our aim is to prove that *k is bounded above in terms of α*. Once established, this will imply that there is a fixed upper bound for $d(N)$ as N ranges over all the open normal subgroups of G, and the result will follow in view of Proposition 4.1.1.

Since the set of open normal subgroups N of G satisfying $d(N) \geq k$ is non-empty, we may choose a maximal member, that we call N. Put $d(N) = d$, so $d \geq k$. The preceding lemma tells us that

$$|G : N| \leq p^{(k-1)\lambda} \leq p^{(d-1)\lambda}$$

where $\lambda = \lceil \log d \rceil$. On the other hand, $N/\Phi(N) \cong \mathbb{F}_p^d$ has at least $p^{[d^2/4]}$ subgroups of index $p^{[d/2]}$. Thus for $n = p^{[d/2]+(d-1)\lambda}$, G has at least $p^{[d^2/4]}$ subgroups of index at most n, and so

$$\begin{aligned}[d^2/4] \leq \log_p s_n(G) &\leq \alpha \log_p n \\ &= \alpha[d/2] + \alpha(d-1)\lambda \leq \alpha d/2 + \alpha(d-1)(1 + \log d).\end{aligned}$$

Since $(\log d)/d$ tends to 0 as $d \to \infty$ it follows that d is bounded above by a number depending only on α. As $k \leq d$ we have achieved our aim, and the proof is complete.

(Essentially the same argument would work under the weaker hypothesis $s_n(G) \leq n^{\alpha(\log n)^{1-\varepsilon}}$ where $\varepsilon > 0$ is a constant; in the next section we shall do much better than this.)

We have seen above that if G has rank r then the 'degree of polynomial growth' $\alpha(G)$ is at most $r - \mu$, where $\mu = \log(p-1)/\log p$. It is not clear if this bound is best possible. When p is large, it is close to the correct bound for the free abelian pro-p group $G = \mathbb{Z}_p^r$, which has $\alpha(G) = r - 1$: this follows from Proposition 1.5.1, which implies that

$$s_{p^k}(\mathbb{Z}_p^r) = s_{p^k}(\mathbb{Z}^r) = \sum_{i \leq k} a_{p^i}(\mathbb{Z}^r)$$

is bounded above and below by constant multiples of $p^{k(r-1)}$. It is also known that $\alpha(G)$ is always a rational number: this follows from the theory of 'local zeta functions', discussed in Chapter 16.

The *dimension* $\dim(G)$ is defined to be the rank of any uniform open subgroup of G ($\looparrowright$ **Pro-p groups**). In general we have

Theorem 4.1.3 *Let G be a pro-p group of finite rank. Then provided $\dim(G) > 1$ we have*

$$\alpha(G) \geq \dim(G)/6.$$

Proof. The group G has an open normal subgroup H which is a uniform pro-p group, and $\alpha(G) \geq \alpha(H)$ (see §1.11), so replacing G by H we may as well

assume that G is uniform, of dimension d say. Let $G_i = P_i(G)$ denote the ith term of the lower central p-series of G. Then for $i > 1$,

$$|G : G_i| = p^{d(i-1)}, \qquad |G_i : G_{2i}| = p^{di},$$

and G_i/G_{2i} is an abelian group of exponent p^i and rank d ($\looparrowright$ **Pro-p groups**). Thus G_i/G_{2i} is homocyclic, and Proposition 1.5.3 shows that

$$a_{p^{ri}}(G_i/G_{2i}) > p^{ir(d-r)}$$

for $1 \leq r < d$. Hence

$$n = p^{i(d+r)} \Longrightarrow s_n(G) > p^{ir(d-r)} = n^{c(d,r)}$$

where $c(d,r) = r(d-r)/(d+r)$. As i can be arbitrarily large we see that

$$\alpha(G) \geq \max_{1 \leq r < d} c(d,r).$$

The result follows since

$$c(d, \frac{d}{2}) = \frac{d}{6} \ (d \text{ even}),$$
$$c(d, \frac{d-1}{2}) = \frac{(d-1)(d+1)}{2(3d-1)} \geq \frac{d}{6} \ (d \geq 3 \text{ odd}).$$

■

Choosing r more carefully one obtains the estimate

$$\alpha(G) \geq (3 - 2\sqrt{2}) \cdot \dim(G) - (\sqrt{2} - 1),$$

which is sharper when $\dim(G)$ is large; but we do not know if the lower bound given here is best possible. Indeed, the precise determination of $\alpha(G)$ for pro-p groups of finite rank in general seems to be a difficult problem. An example of a pro-p group of finite rank is the 'first principal congruence subgroup' $G_m = \ker(\mathrm{SL}_m(\mathbb{Z}_p \to \mathrm{SL}_m(\mathbb{F}_p))$, which has rank $m^2 - 1$ (if p is odd) and therefore satisfies $\alpha(G_m) \leq m^2 - 1 - \mu$. This is very likely not the best bound. The best bound is not known except for the case $m = 2$, where [Ilani 1999] showed that $a_{p^k}(G_2)$ grows like kp^k; it follows that $\alpha(G_2) = 1 = \mathrm{rk}(G_2) - 2$.

4.2 Pro-p groups with slow subgroup growth

To show that a pro-p group of infinite rank has faster than polynomial subgroup growth, we counted subgroups in a suitably large elementary abelian section. Doing this more carefully leads to more explicit lower bounds for the subgroup growth; the main step is

Lemma 4.2.1 *Let G be a pro-p group. Suppose that G has an open subgroup X with*

$$|G : X| = p^k, \ d(X) = d \geq \lambda k$$

where $\lambda > 0$. Put

$$\gamma = \frac{\lambda^2}{4(\lambda+1)}.$$

Then there exists $e < d$ such that for $t = k + e$ we have

$$a_{p^t}(G) > p^{\gamma(1-\varepsilon)t^2}$$

where $\varepsilon = (2+\lambda)/k\lambda$.

When applying this, we think of λ as fixed while k is very large, so that ε is very small.

Proof. The idea is to choose e so as to maximize $e(d-e)/(k+e)^2$; this will give the best value for γ. As the given expression for $\gamma(1-\varepsilon)$ is an increasing function of λ, we may as well assume that $\lambda = d/k$. Then elementary calculus shows that e should be close to τd where $\tau = 1/(\lambda+2)$. Taking

$$e = [\tau d]$$

we find that

$$\frac{e(d-e)}{(k+e)^2} > \frac{\lambda^2}{4(\lambda+1)}(1 - \frac{1}{\tau d}) = \gamma(1-\varepsilon).$$

Thus for $t = k + e$ we have

$$\begin{aligned} p^{\gamma(1-\varepsilon)t^2} < p^{e(d-e)} &\leq \begin{bmatrix} d \\ e \end{bmatrix} \\ &= a_{p^e}(X/\Phi(X)) \leq a_{p^t}(G). \end{aligned}$$

■

Taking advantage of a more subtle characterisation of the pro-p groups of finite rank, we can now weaken the hypothesis of (the harder implication in) Theorem 4.1 and prove Theorem 4.2. This says that if G is a pro-p group of infinite rank and $0 < c < 1/8$ then

$$s_n(G) > n^{c \log_p n} \tag{4.1}$$

for infinitely many values of n.

To this end, it will suffice to find a chain $G = X_0 > X_1 > \cdots > X_m > \cdots$ of open normal subgroups of G such that if $|G : X_m| = p^{k(m)}$ and $d(X_m) = d(m)$ then

$$d(m) \geq \lambda k(m) \tag{4.2}$$

for infinitely many values of m, where $\lambda > 2c(1 + \sqrt{1 + c^{-1}})$. Indeed, if this holds then the preceding lemma shows that there exist arbitrarily large values $n = p^t$ such that

$$s_n(G) > a_{p^t}(G) > p^{\gamma(1-\varepsilon_n)t^2} = n^{\gamma(1-\varepsilon_n)\log_p n},$$

where

$$\gamma = \frac{\lambda^2}{4(\lambda+1)} > c$$

and $\varepsilon_n \to 0$ as $n \to \infty$. It follows that if n is big enough then $\gamma(1-\varepsilon_n) > c$, and (4.1) follows.

A suitable chain (G_i) is provided by the 'Jennings-Zassenhaus' series of G, defined recursively as follows:

Definition $D_1(G) = G$; for $i > 1$, $D_i(G) = D_i$ where

$$D_i = (D_{\lceil i/p \rceil})^p \cdot \prod_{j+k=i} [D_j, D_k].$$

When G is a finitely generated pro-p group, the chain (D_i) is the fastest descending chain of open subgroups of G, starting with G, such that $[D_j, D_k] \leq D_{j+k}$ and $D_j^p \leq D_{pj}$ for all j and k. For properties of this series, see [DDMS], Chapter 11. Jennings proved that $D_i(G)$ is equal to the ith *modular dimension subgroup* of G; however, the important fact for us is the following theorem of Lazard and Lubotzky & Mann ([DDMS], Theorem 11.4):

Proposition 4.2.2 *Let G be a finitely generated pro-p group. Then G has finite rank if and only if $D_i = D_{i+1}$ for some i.*

To return to the proof of Theorem 4.2, suppose G is a pro-p group of infinite rank and $0 < c < 1/8$. If G is not finitely generated then $s_n(G)$ is infinite for all $n \geq p$, so we may as well assume that G is finitely generated. Then $D_i > D_{i+1}$ for every i. Now put

$$X_m = D_{2^m}$$

and define $d(m)$, $k(m)$ as above. Since $c < 1/8$, we have $2c(1+\sqrt{1+c^{-1}}) < 1$, and we may choose λ with $1 > \lambda > 2c(1+\sqrt{1+c^{-1}})$. To complete the proof, it now suffices to show that (4.2) holds for infinitely many values of m.

Note that for each m we have

$$\Phi(X_m) = [X_m, X_m] X_m^p \leq D_{2 \cdot 2^m} D_{p \cdot 2^m} = D_{2^{m+1}} = X_{m+1}.$$

This implies that

$$p^{d(m)} = |X_m : \Phi(X_m)| \geq |X_m : X_{m+1}| = p^{k(m+1)-k(m)},$$

so

$$k(m+1) - k(m) \leq d(m).$$

Suppose now that $d(m) < \lambda k(m)$ for all $m \geq m_0$. Then $k(m+1) < (1+\lambda)k(m)$ for all $m \geq m_0$, and so

$$k(m_0+n) < (1+\lambda)^n k(m_0)$$

for all $n > 0$. But $k(m_0 + n) \geq 2^n$ since $D_i > D_{i+1}$ for $2^{m_0} \leq i < 2^{m_0+n}$; consequently

$$2^n < k(m_0)(1+\lambda)^n$$

for all n. This is impossible since $k(m_0)$ is finite while $2^n/(1+\lambda)^n \to \infty$ because $\lambda < 1$. It follows that $d(m) \geq \lambda k(m)$ for infinitely many values of m, which is what we had to prove.

4.3 The groups $\mathrm{SL}_r^1(\mathbb{F}_p[[t]])$

We have seen that a little knowledge of the dimension subgroup series (D_i) in a pro-p group G may enable us to deduce a lower bound for $s_n(G)$, at least for infinitely many values of n. If we know more about the series (D_i), we can do better: in the rest of this chapter we obtain both upper bounds, and lower bounds valid for *all* large n, for some groups whose dimension subgroups are explicitly known.

We begin in this section with certain special linear groups.

Fix an integer $r \geq 2$ (or $r \geq 3$ if $p = 2$). For $n \geq 1$ let G_n denote the nth principal congruence subgroup in $G_0 = \mathrm{SL}_r(\mathbb{F}_p[[t]])$:

$$G_n = \ker\left(\mathrm{SL}_r(\mathbb{F}_p[[t]]) \to \mathrm{SL}_r(\mathbb{F}_p[[t]]/(t^n))\right),$$

that is the group of matrices congruent to the identity modulo $t^n\mathbb{F}_p[[t]]$. The group G_0 inherits a topology from the (t)-adic topology on the matrix ring, in which the subgroups G_n form a base for the neighbourhoods of 1. Since the residue-class mappings above are all surjective (because $\mathbb{F}_p[[t]]$ is a principal ideal ring), we have

$$|G_0 : G_n| = |\mathrm{SL}_r(\mathbb{F}_p[[t]]/(t^n))| = |\mathrm{SL}_r(\mathbb{F}_p)| \cdot p^{(r^2-1)(n-1)}$$

for each $n \geq 1$. It follows that

$$|G_1 : G_n| = p^{(r^2-1)(n-1)}$$

so the group $G = G_1$ is a pro-p group. It can be verified that $G_n = D_n(G) = P_n(G)$ for each n; hence in particular

$$d(G) = \log_p |G : G_2| = r^2 - 1.$$

Proposition 4.3.1 "Level vs. index " *Let H be an open subgroup of index p^k in G. Then $H \geq G_{k+1}$.*

The proof of this key result involves the associated *graded Lie algebra* of G. Now $[G_i, G_j] \leq G_{i+j}$ and $G_i^p \leq G_{pi}$ for all $i,\ j \geq 1$. This means that $L_n := G_n/G_{n+1} \cong \mathbb{F}_p^{r^2-1}$ and that there is a well-defined operation

$$(\ ,\ ) : L_i \times L_j \to L_{i+j}$$

given by $(xG_{i+1}, yG_{j+1}) = [x,y]G_{i+j+1}$; thus we obtain a graded Lie algebra over $\mathbb{F}_p$,

$$L = \bigoplus_{n=1}^{\infty} L_n.$$

In fact $L \cong L_0 \otimes t\mathbb{F}_p[t]$ where $L_0 = \mathfrak{sl}_r(\mathbb{F}_p)$, with L_n corresponding to $L_0 \otimes t^n$; for details, see [DDMS], §13.4.

Note that the Lie algebra L_0 is *perfect*, that is, $(L_0, L_0) = L_0$. It follows that if V is a subspace of codimension 1 in L_0, so $L_0 = V + a\mathbb{F}_p$ for some element a, then

$$L_0 = (V + a\mathbb{F}_p, V + a\mathbb{F}_p) = (V, L_0). \tag{4.3}$$

Lemma 4.3.2 *For each $n \geq 1$ let V_n be a subspace of L_0 and assume that $(V_i, V_j) \subseteq V_{i+j}$ for all i, j. Put $k_n = \dim L_0 - \dim V_n$ for each n and suppose that $k = \sum_{n=1}^{\infty} k_n$ is finite. Then $k_n = 0$ for all $n > k$.*

Proof. Suppose n is such that $k_n \neq 0$. Then $V_n < L_0$. If $i + j = n$ then $(V_i, V_j) \subseteq V_n < L_0$, so (4.3) implies that $k_i + k_j \geq 2$. Thus if $n = 2m$ then $k_m \geq 1$, $k_n \geq 1$, and

$$n - 2 = 2(m-1) \leq \sum_{i=1}^{m-1} (k_i + k_{n-i}) \leq k - k_m - k_n \leq k - 2;$$

while if $n = 2m + 1$ then

$$n - 1 = 2m \leq \sum_{i=1}^{m} (k_i + k_{n-i}) \leq k - k_n \leq k - 1.$$

In either case it follows that $n \leq k$. ■

We can now complete the

Proof of Proposition 4.3.1 The open subgroup H has index p^k in G. For each n put

$$H_n = (H \cap G_n)G_{n+1}/G_{n+1} \leq L_n.$$

Then $(H_i, H_j) \subseteq H_{i+j}$ and $k = \sum_{n=1}^{\infty} k_n$ where $k_n = \dim L_n - \dim H_n$. Identifying L_n with $L_0 \otimes t^n$ as above, we can write $H_n = V_n \otimes t^n$ where V_n is a subspace of L_0, and the hypotheses of Lemma 4.3.2 are satisfied. It follows that $k_n = 0$ for all $n > k$, which means that $H \geq G_{k+1}$. □

It follows from Proposition 4.3.1 that $a_{p^k}(G) = a_{p^k}(G/G_{k+1})$. Now Proposition 1.6.1 shows that if H is a group of order p^d then

$$a_{p^r}(H) < \kappa \cdot p^{r(d-r)}$$

for $1 \leq r \leq d$, where κ is a constant lying between 1 and 4. Applying this to the group G/G_{k+1}, which has order $p^{(r^2-1)k}$, we deduce

Theorem 4.3.3 *Let $G = \mathrm{SL}_r^1(\mathbb{F}_p[[t]])$, where $r \geq 2$ ($r \geq 3$ if $p = 2$). Then*

$$a_{p^k}(G) \leq \kappa \cdot p^{(r^2-2)k^2}.$$

Taking $r = 2$ (and $p \geq 3$) we find that $s_n(G) \leq n^{(2+\varepsilon)\log_p n}$ for all large n, if $\varepsilon > 0$. Since G has infinite rank (as it contains an additive copy of $\mathbb{F}_p[[t]]$), this shows that the bound $c < 1/8$ in Theorem 4.2 cannot be weakened to $c < 2 + \varepsilon$ for any $\varepsilon > 0$. A slightly different approach, that we shall indicate in the following section, allowed [Barnea & Guralnick 2002] to establish

Proposition 4.3.4 *Let $G = \mathrm{SL}_2^1(\mathbb{F}_p[[t]])$, where $p \geq 3$. Then*

$$a_{p^k}(G) \leq p^{(k^2+5k)/2}.$$

So in fact

$$s_n(G) \leq n^{(1/2+\varepsilon)\log_p n}$$

for all large n, and the best possible bound for c therefore lies between $1/8$ and $1/2$.

Now let us determine a lower bound for the subgroup growth. As in the preceding section we put

$$X_m = G_{2^m},$$

and see that

$$\begin{aligned} d(X_m) &\geq \log_p |G_{2^m} : G_{2^{m+1}}| \\ &= (r^2-1)2^m > \log_p |G : X_m|. \end{aligned}$$

Thus we may apply Lemma 4.2.1 with $\lambda = 1$. For $k = \log_p |G : X_m| = (r^2 - 1)(2^m - 1)$ and $t = t(m) = k + e$ where $e = [k/3]$ this gives

$$a_{p^t}(G) > p^{(1/8)(1-3/k)t^2}.$$

Let $\varepsilon > 0$ and let n be a large positive integer. Then there exists m such that $p^{t(m)} \leq n < p^{t(m+1)}$, giving

$$s_n(G) > p^{(1/8)(1-3/k)t(m)^2} > n^{(1/32-\varepsilon)\log_p n},$$

since $t(m+1)$ is approximately $2t(m)$. Thus for the groups $\mathrm{SL}_r^1(\mathbb{F}_p[[t]])$ the lower bound $s_n(G) > n^{c\log_p n}$ holds for *all* large n, if c is any constant with $c < 1/32$.

It follows that $\mathrm{SL}_r^1(\mathbb{F}_p[[t]])$ has strict growth type $n^{\log n}$. This means that for $G = \mathrm{SL}_r^1(\mathbb{F}_p[[t]])$ the quantity

$$\frac{\log s_n(G)}{(\log n)^2}$$

is bounded above and below by positive constants. The following is an interesting problem:

- Does $\log s_n(G)/(\log n)^2$ tend to a limit as $n \to \infty$? If so, determine this limit as a function of r.

4.4 Λ-perfect groups

The results of the preceding section can be generalised in the following way. A *pro-p domain* is a complete local integral domain (commutative, Noetherian with identity) Λ whose residue class field F is finite and has characteristic p. We denote the maximal ideal of Λ by $\mathfrak{m}$, so $F = \Lambda/\mathfrak{m}$, and assume for technical reasons that the associated graded ring

$$\mathrm{gr}\Lambda = \bigoplus_{n=0}^{\infty} \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

has no zero divisors. Familiar examples of such rings are the power series rings $\mathbb{F}_q[[t_1, \ldots, t_s]]$, where q is a power of p, and $\mathfrak{o}[[t_1, \ldots, t_{s-1}]]$ where $\mathfrak{o}$ is a finite extension of $\mathbb{Z}_p$. Each of these rings has Krull dimension s, and in general we let s denote the Krull dimension of Λ. In this section we consider only the *equicharacteristic case*, where $p\Lambda = 0$.

A Λ-*standard group of dimension* d is a pro-p group G which carries a coordinate system with values in $\mathfrak{m}^{(d)}$, such that the group operations are given by power series with coefficients in Λ. We shall not go into the details here, and refer the reader to Chapter 13 of [DDMS] for a full discussion, where it shown that $\mathrm{SL}_r^1(\Lambda)$ is Λ-standard group of dimension r^2-1, the coordinates of a matrix M being $m_{ij} - \delta_{ij}$ for $(i,j) \neq (r,r)$. More generally, if $\mathcal{G}$ is any simple Chevalley group scheme (other than A_1 if $p = 2$) then the first congruence subgroup

$$\mathcal{G}^1(\Lambda) = \ker\left(\mathcal{G}(\Lambda) \to \mathcal{G}(\Lambda/\mathfrak{m})\right)$$

is a Λ-standard group (see [DDMS], Exercise 13.11). These examples will be important in Chapter 6, when we consider arithmetic groups over global fields of characteristic p.

Using the coordinates, it is usual to identify G with the set $\mathfrak{m}^{(d)}$. Having done this, we write G_n for the subset $(\mathfrak{m}^n)^{(d)}$. Then each G_n is a normal subgroup of $G = G_1$, and the family (G_n) is a base for the neighbourhoods of 1 in G. We say that G is Λ-*perfect* if $G_2 = [G, G]$. In this case,

$$\begin{aligned} [G_m, G_n] &= G_{m+n} \\ G_m^p &\leq G_{pn} \end{aligned} \tag{4.4}$$

for all m and n (the second line depends on our standing assumption that $p\Lambda = 0$). This holds, for example, for the groups $\mathcal{G}^1(\Lambda)$ except when $p = 2$ and $\mathcal{G}$ is of type A_1 or C_n. One may define a graded Lie algebra

$$L = \bigoplus_{n=1}^{\infty} G_n/G_{n+1}$$

as in the preceding section, and there exists a d-dimensional Lie algebra L_0 over F such that

$$L \cong L_0 \underset{F}{\otimes} \mathrm{gr}\mathfrak{m} = \bigoplus_{n=1}^{\infty} \left(L_0 \underset{F}{\otimes} \mathfrak{m}^n/\mathfrak{m}^{n+1} \right), \tag{4.5}$$

with $G_n/G_{n+1} \cong L_0 \otimes \mathfrak{m}^n/\mathfrak{m}^{n+1}$. This construction works for any Λ-standard group G; and G is Λ-perfect precisely when L_0 is a perfect Lie algebra (this is expressed in (4.4)).

Now $|G_n : G_{n+1}| = \left|\mathfrak{m}^n/\mathfrak{m}^{n+1}\right|^d$, and

$$\dim_F(\mathfrak{m}^n/\mathfrak{m}^{n+1}) \sim cn^{(s-1)}$$

for some positive constant c, by the Hilbert-Samuel theorem ([AM], Theorem 11.14). It follows that

$$|G : G_{2^m}| \leq (1 + o(1))\,|G_{2^m} : G_{2^{m+1}}|\,,$$

and the argument at the end of the preceding section now gives

Theorem 4.4.1 *Let G be a Λ-perfect pro-p group. Then there exists $c > 0$ such that*

$$s_n(G) > n^{c \log_p n}$$

for all large n.

We can also repeat the proof of Theorem 4.3.3 in the present more general setting, at least when $F = \mathbb{F}_p$. However, if $s > 1$ this approach only yields an upper bound of the form

$$s_n(G) \leq n^{c(\log_p n)^s}.$$

The correct generalisation of Theorem 4.3.3 depends on a deeper analysis of the graded Lie algebra. The key result is

Proposition 4.4.2 ([Lubotzky & Shalev 1994], Proposition 4.2) *Let L be the Lie algebra (4.5). There exists a constant c, depending only on Λ and d, such that*

$$\dim_{\mathbb{F}_p}(K/(K,K)) \leq c \cdot \dim_{\mathbb{F}_p}(L/K)$$

for every graded $\mathbb{F}_p$-Lie subalgebra K of finite codimension in L.

(A more precise result in the case where Λ has Krull dimension 1 is proved in Chapter 6, §6.3).

Now suppose that H is an open subgroup of index p^k in G. To H we associate the graded Lie subalgebra K (over $\mathbb{F}_p$) of L with nth homogeneous component

$$H_n = (H \cap G_n)G_{n+1}/G_{n+1} \leq L_n.$$

Then $\dim_{\mathbb{F}_p}(L/K) = k$. It follows by the proposition that $\dim_{\mathbb{F}_p}(K/(K,K)) \leq ck$. Since

$$(H_i, H_j) = [H \cap G_i, H \cap G_j]G_{i+j+1}/G_{i+j+1} \leq ([H,H] \cap G_{i+j})G_{i+j+1}/G_{i+j+1},$$

we see that $(K,K) \subseteq \bigoplus([H,H] \cap G_n)G_{n+1}/G_{n+1}$ and hence that

$$|H : [H,H]| \leq p^{ck}.$$

This implies that $d(H) \leq ck$.

We have shown that $d_k(G) \leq ck$ for each k, and applying Proposition 1.6.2 we deduce

Theorem 4.4.3 *Let G be a Λ-perfect group. Then there exists c such that*

$$a_{p^k}(G) \leq p^{ck^2}$$

for all n.

Thus $s_n(G) \leq n^{c' \log_p n}$ for some constant c', and we have shown that *every Λ-perfect group has strict growth type $n^{\log n}$.*

We remark that Proposition 4.3.4, in the preceding section, was deduced in a similar way by [Barnea and Guralnick 2002] from a variant of Proposition 4.4.2: they prove that

$$d(K) \leq \dim_{\mathbb{F}_p}(L/K) + 3$$

for every graded Lie subalgebra K of L, in the case $G = \mathrm{SL}_2^1(\mathbb{F}_p[[t]])$.

4.5 The Nottingham group

This interesting pro-p group is the group of normalised automorphisms of the power series ring $\mathbb{F}_p[[t]]$. For each $n \geq 1$, let $\mathcal{N}_n$ denote the group of (continuous) automorphisms of the $\mathbb{F}_p$-algebra $\mathbb{F}_p[[t]]$ that induce the identity on $\mathbb{F}_p[[t]]/t^{n+1}\mathbb{F}_p[[t]]$, and write $\mathcal{N} = \mathcal{N}_1$. This is the *Nottingham group*, and it is a pro-p group having the chain

$$\mathcal{N} = \mathcal{N}_1 > \mathcal{N}_2 > \cdots > \mathcal{N}_n > \cdots$$

as a base for the neighbourhoods of 1. For details, we refer to [NH], Chapter 6 and Chapter 10, where it is shown that $\mathcal{N}$ is (topologically) generated by 2 elements and that it contains a copy of every countably based (in particular, every finitely generated) pro-p group. The second fact implies that $\mathcal{N}$ does not have finite rank, so it is not p-adic analytic. More generally, it is shown in [NH], Chapter 1, Section 5.1 that $\mathcal{N}$ is not analytic over any pro-p ring; so it is distinct form the Λ-perfect groups considered above. The following was proved by Leedham-Green and Shalev; see [NH] Chapter 6, Theorem 8:

Proposition 4.5.1 *Suppose that $p \neq 2$. Let H be an open subgroup of index p^k in $\mathcal{N}$. Then $H \geq \mathcal{N}_n$ where $n = \lceil 2kp/(p-1) \rceil$.*

It follows that

$$a_{p^k}(\mathcal{N}) = a_{p^k}(\mathcal{N}/\mathcal{N}_n)$$

where $n = \lceil 2kp/(p-1) \rceil$. Now it is easy to see that $|\mathcal{N}/\mathcal{N}_n| = p^{n-1}$, so applying Proposition 1.6.1, as in Section 3 above, we deduce

Theorem 4.5.2 *Suppose that $p \neq 2$. Then*

$$a_{p^k}(\mathcal{N}) \leq \kappa \cdot p^{k^2(p+1)/(p-1)}$$

for all $k \geq 0$.

Thus for large n we have $s_n(\mathcal{N}) \leq n^{c \log_p n}$ where c is any constant exceeding $(p+1)/(p-1)$. Since $\mathcal{N}$ has infinite rank it follows from Theorem 4.2 that the growth type of $\mathcal{N}$ is $n^{\log n}$.

The same holds more generally for the Nottingham group over $\mathbb{F}_q$ where q is any power of p; see [NH], Chapter 6.

4.6 Finitely presented pro-p groups

Let G be a finitely presented pro-p group. A *minimal presentation* for G is a pro-p presentation

$$G = \langle X; R \rangle$$

by generators and relations such that $|X| = d(G)$. If *every* minimal presentation of G satisfies the condition

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

the group G is said to satisfy the *Golod-Shafarevich inequality*. The celebrated theorem of Golod and Shafarevich states that this holds for every finite p-group G; a far-reaching generalisation of this fact has been proved by Zelmanov:

Theorem 4.6.1 [Zelmanov 2000] *Let $G \ncong \mathbb{Z}_p$ be a finitely presented pro-p group. If G does not satisfy the Golod-Shafarevich inequality then G contains a non-abelian free pro-p group as a closed subgroup.*

An elementary lemma (↬ **Pro-p groups**) shows that to every finite presentation $\langle Y; S \rangle$ of G there corresponds a minimal presentation $\langle X; R \rangle$ with

$$|R| = |S| - (|Y| - |X|).$$

It follows that if G satisfies the Golod-Shafarevich inequality then

$$|S| - (|Y| - d(G)) \geq \frac{d(G)^2}{4}. \tag{4.6}$$

Lemma 4.6.2 *Let G be a finitely presented pro-p group. Then there exists $c > 0$ with the following property: if H is an open subgroup of G and H satisfies the Golod-Shafarevich inequality then*

$$d(H) \leq c\sqrt{|G : H|}.$$

Proof. We may suppose that $G = F/K$ where F is a finitely generated free pro-p group and $K = \overline{\langle R^F \rangle}$ is the closed normal subgroup of F generated by the finite set R. Let H be an open subgroup of index h in G. Then $H = E/K$ where E is open and of index h in F. Now E is a finitely generated free pro-p group, and it is clear that K is generated as a closed normal subgroup of E by

the union of h conjugates of R. Thus H has a finite presentation $\langle Y; S\rangle$ with $|S| \leq h\,|R|$. Applying (4.6) to H we deduce that

$$h\,|R| \geq h\,|R| - (|Y| - d(H)) \geq d(H)^2/4.$$

Thus $d(H) \leq 2\sqrt{|R|} \cdot \sqrt{h}$. ■

If G is such that *every* open subgroup of G satisfies the Golod-Shafarevich inequality, the lemma shows that $d_n(G) \leq cp^{n/2}$ for each n, and hence that

$$d_n^*(G) \leq c\frac{p^{(n+1)/2} - 1}{p^{1/2} - 1}$$

(Proposition 1.6.2). With Proposition 3.3.1 this gives

$$a_{p^n}(G) \leq p^{d^*_{n-1}(G) - n\mu} < p^{c' p^{n/2}}$$

for a suitable constant c' (recall that $\mu = \log(p-1)/\log p$). Thus we have established

Proposition 4.6.3 *Let G be a finitely presented pro-p group such that every open subgroup of G satisfies the Golod-Shafarevich inequality. Then there is a constant a such that*

$$a_n(G) \leq a^{\sqrt{n}}$$

for all n.

Thus a pro-p group satisfying the hypothesis of Proposition 4.6.3 has growth type $\leq 2^{\sqrt{n}}$.

The condition that every open subgroup satisfies the Golod-Shafarevich inequality would seem to be rather a strong one. In fact, however, it is fulfilled by a large class of finitely presented pro-p groups: indeed, Zelmanov's theorem implies that if G is a finitely presented pro-p group that is not virtually procyclic, then *either* G satisfies the hypothesis of Proposition 4.6.3 *or* G contains a non-abelian free pro-p group. Since a virtually procyclic group has polynomial subgroup growth (e.g. by Corollary 1.2.4) this now implies Theorem 4.3:

A finitely presented pro-p group that contains no non-abelian free pro-p subgroup has subgroup growth type at most $2^{\sqrt{n}}$.

This applies, for example, to all finitely presented soluble pro-p groups. It also applies to every finitely presented pro-p group that is linear over a local field, since [Barnea and Larsen 1999] have shown that such a linear pro-p group cannot contain a non-abelian free pro-p subgroup.

It is interesting to observe that this result is best possible from two points of view. Firstly, Theorem 4.3 does not hold for finitely generated pro-p groups in general: indeed we saw in Chapter 3 that the soluble pro-p group $C_p \wr \mathbb{Z}_p$

has exponential growth type. This difference between finitely presented and infinitely presented soluble groups deserves further exploration. Secondly, the exponent $\sqrt{n}$ is best possible: in Section 9.3 we construct a finitely presented metabelian pro-p group having strict growth type $2^{\sqrt{n}}$.

Proposition 4.6.3 also has a sort of converse:

Theorem 4.6.4 *Let G be a finitely presented pro-p group. If there exists $\varepsilon > 0$ such that*

$$a_n(G) \leq n^{(\log n)^{2-\varepsilon}} \tag{4.7}$$

for all large n then G, and every open subgroup of G, satisfies the Golod-Shafarevich inequality.

This may be viewed as another generalisation of the Golod-Shafarevich theorem, different in spirit from Zelmanov's theorem since it refers to the finite quotients rather than the subgroup structure of G. The proof is along similar lines to that of Theorem 4.2; the key step is the following result, proved as Theorem D1 in [DDMS], Interlude D:

Proposition 4.6.5 *Let G be a finitely presented pro-p group with Jennings-Zassenhaus series (D_i), and suppose that*

$$|G : D_i| = p^{s_i}.$$

If

$$\limsup s_i^{1/i} \leq 1$$

then G satisfies the Golod-Shafarevich inequality.

Keeping the notation of this proposition, we also have

Lemma 4.6.6 *Suppose that $\limsup s_i^{1/i} > 1$. Then for each $\delta > 0$ there exist infinitely many values of i such that*

$$s_{2i} > s_i^{2-\delta}.$$

We prove this below, and first complete the proof of Theorem 4.6.4. If G satifies the subgroup growth condition (4.7), then so does every open subgroup of G (with possibly a different ε), so it will suffice to show that G itself satisfies the G-S inequality. Let us suppose that it doesn't, and aim for a contradiction. Assume without loss of generality that $\varepsilon < 1$ and put $\delta = \varepsilon/2$. The two preceding results together imply that $s_{2i} > s_i^{2-\delta}$ for infinitely many values of i. In particular, $s_i \to \infty$ with i. Now D_i/D_{2i} is an elementary abelian p-group of rank $s_{2i} - s_i$, hence contains at least $p^{s_i(s_{2i}-s_i)}$ subgroups of index p^{s_i}. So for $n = p^{2s_i}$ we have

$$a_n(G) \geq p^{s_i(s_{2i}-s_i)}.$$

But if i is large then $a_n(G) \leq n^{(\log n)^{2-\varepsilon}}$ by hypothesis, whence

$$\begin{aligned} s_i(s_{2i} - s_i)\log p &\leq (\log n)^{3-\varepsilon} \\ &= (2\log p)^{3-\varepsilon} s_i^{3-2\delta}. \end{aligned}$$

On the other hand, for infinitely many values of i we have

$$s_i(s_{2i} - s_i) > s_i(s_i^{2-\delta} - s_i) \geq \frac{1}{2} s_i^{3-\delta},$$

say, giving

$$s_i^{\delta} \leq 2^4 (\log p)^2.$$

This contradicts $s_i \to \infty$, and the result follows.

Proof of Lemma 4.6.6. We may assume that $\delta < 1$. Put $t_i = s_i^{1/i}$. Then for $i < j \leq 2i$

$$t_j = s_j^{1/j} \leq s_{2i}^{1/j} = t_{2i}^{2i/j} \leq t_{2i}^2. \tag{4.8}$$

Suppose there exists k such that $s_{2i} \leq s_i^{2-\delta}$ for every $i \geq k$. Then

$$t_{2i} = (s_{2i})^{1/2i} \leq (s_i^{2-\delta})^{1/2i} = t_i^{1-\delta/2}$$

for each $i \geq k$, and by induction we get

$$t_{2^j k} \leq t_k^{(1-\frac{\delta}{2})^j}$$

for all $j \geq 1$. Since $0 < 1 - \frac{\delta}{2} < 1$ it follows that

$$t_{2^j k} \to 1$$

as $j \to \infty$.

Now, for a general large ℓ, pick j with $2^{j-1}k < \ell \leq 2^j k$. Then (4.8) shows that

$$t_\ell \leq t_{2^j k}^2 \to 1$$

and so $\limsup t_\ell \leq 1$. The lemma follows.

4.7 Notes

Theorem 4.1 is due to [**Lubotzky & Mann 1991**]. Theorem 4.1.3 was pointed out to us by **Laci Pyber**.

The theorem of [**Zelmanov 2000**] is actually stronger than we stated: Zelmanov says that a finitely generated pro-p group satisfies the *Golod-Shafarevich condition* if it has a (not necessarily finite) presentation in which the relators 'grow rapidly' in a precise sense. This holds in particular if the group is finitely presented and does *not* satisfy the Golod-Shafarevich inequality as we have stated it.

[**Wilson 1991**] discussed the Golod-Shafarevich inequality in pro-p groups and established Lemma 4.6.2.

Applications of the Jennings-Zassenhaus ('modular dimension subgroup') series to subgroup growth were pioneered by A. Shalev. He proved Theorem 4.2 in [**Shalev 1992**], and Theorem 4.6.4 in recent unpublished work. These methods are discussed in detail in [**DDMS**], Chapter 11.

The methods and results of §4.3 are based on [**Shalev 1992**], Section 4. The sharper result for $\mathrm{SL}_2(\mathbb{F}_p[[t]])$ is due to [**Barnea & Guralnick 2002**]. The material of §4.3 is from [**Lubotzky & Shalev 1994**].

Recently, [**Abért, Nikolov & Szegedy**] have proved the following: let $\mathfrak{G}$ be a simple Chevalley group scheme of dimension m and $G = \mathfrak{G}^1(\mathbb{F}_p[[t]])$ (excluding $p = 2$ if $\mathfrak{G}$ is A_1 or C_l); then

$$s_{p^k}(G) \leq p^{7k(k-1)/2+mk}.$$

Thus $s_n(G) \leq n^{(\frac{7}{2}+o(1))\log n}$ for every $\mathbb{F}_p[[t]]$-perfect group G of this kind, the constant $7/2$ being *independent of the group*.

Theorem 4.5.2 on the Nottingham group is due to **Leedham-Green** and **Shalev**; see [**NH**], Chapter 6.

[**Klopsch (a)**] examines pro-p groups with slow subgroup growth. This paper gives a number of results about the degree; the main result is a complete classification of pro-p groups with *linear* subgroup growth; apart from easy soluble cases the main examples are of the form $\mathrm{SL}_1(\Delta_p)$ where Δ_p is a maximal order in a central $\mathbb{Q}_p$-division algebra of index 2.

Chapter 5

Finitely generated groups with polynomial subgroup growth

A group G has *polynomial subgroup growth,* or *PSG*, if there exists $c > 0$ such that

$$s_n(G) \leq n^c$$

for all n. The most familiar infinite group with this property is of course $\mathbb{Z}$; in fact, since the property depends only on the finite images of the group, it is clear that, more generally, every additive subgroup of $\mathbb{Q}$ has PSG. Elementary considerations then show that any group that is obtained from the identity by finitely many iterated extensions by such subgroups of $\mathbb{Q}$ or by finite groups will still have PSG; we proved this in Chapter 1. The class of groups so obtained is the class of *residually finite virtually soluble groups of finite rank*. General properties of these relatively straightforward groups are discussed in the **Soluble groups** window; in particular, a finitely generated residually finite group is virtually soluble of finite rank if and only if it is virtually soluble and linear over $\mathbb{Q}$.

Thus we have a good supply of easy examples of PSG groups. Are there any others? To approach this question one should examine groups that are very unlike soluble groups of finite rank. Now these groups are 'tall and thin' – think of $\mathbb{Z}$ on top of $\mathbb{Z}$ – and 'close to abelian'; at the opposite extreme one might consider groups that 'low and wide' and 'very non-abelian': infinite direct products of finite non-abelian simple groups. Among these, it turns out, we also find some infinite groups with PSG (as we shall see in Chapter 10). However, such groups can never be finitely generated. Familiar examples of finitely generated groups that are far from soluble are the *semisimple arithmetic groups*, that is, arithmetic subgroups of semisimple algebraic groups. While some of these, such as $\mathrm{SL}_2(\mathbb{Z})$, are close to free groups and therefore clearly

don't have PSG, it is more usual for arithmetic groups to satisfy the so-called *congruence subgroup property*; such groups have relatively few subgroups of finite index, and so provide a possible source of non-soluble PSG groups.

As a subgroup of $\mathrm{GL}_d(\mathbb{Z})$, an arithmetic group Γ maps naturally into $\mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z})$ for each m; the kernels of these mappings are the *principal congruence subgroups* of Γ, and any subgroup of Γ that contains such a principal congruence subgroup is called a *congruence subgroup*. We can estimate the number of congruence subgroups in Γ by examining the images of Γ in the finite matrix groups $\mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z})$; when we do this, we find that in fact the growth of congruence subgroups (let alone *all* finite-index subgroups) is strictly *faster* than polynomial. The reason for this is number-theoretic: as we shall see, there are many congruence subgroups because there are many primes below any given bound (the Prime Number Theorem).

At this point, one begins to suspect that maybe there really are no further kinds of PSG groups; and indeed this is true:

Theorem 5.1 (The PSG Theorem) *Let G be a finitely generated residually finite group. Then G has* PSG *if and only if G is virtually soluble of finite rank.*

This result is sharp, in the following sense: given any increasing function f such that $f(n) \neq O(n^c)$ for every c, there exist finitely generated, residually finite groups that have subgroup growth of type at most f, but are neither virtually soluble nor of finite rank. The construction of such groups is given in Chapter 13.

Polynomial subgroup growth is essentially a restriction on the finite quotients of a group: it says that they have relatively few subgroups of each given index. A possible reason for having few subgroups is that every subgroup has a small generating set. The *upper rank* of a group G is

$$\mathrm{ur}(G) = \sup\left\{\mathrm{rk}(\overline{G}) : \overline{G} \text{ a finite quotient of } G\right\}$$

(this is the same as the rank of the profinite completion of G). An analogue to the PSG Theorem, and an intermediate step in its proof, is

Theorem 5.2 *Let G be a finitely generated residually finite group. Then G has finite upper rank if and only if G is virtually soluble of finite rank.*

It is often easier to estimate the number $s(G)$ of all subgroups in a finite group G than to determine the numbers $s_n(G)$. We therefore tend to work with the following concept. A group G has *weak PSG* (wPSG) if there exists $c > 0$ such that

$$s(\overline{G}) \leq \left|\overline{G}\right|^c$$

for every finite quotient $\overline{G}$ of G; it is obvious that PSG implies wPSG, and we show in Chapter 10 that wPSG is actually *equivalent* to PSG. This is quite a deep result, being a major step in the proof of the 'Profinite PSG Theorem'; however it is not needed when dealing with finitely generated (abstract)

groups: we actually prove the 'only if' direction of the PSG Theorem using the weaker condition, from which it will follow that the weaker condition implies the stronger one in the finitely generated case.

The proof of the PSG Theorem required the development of some new techniques in infinite group theory. Some of them have wider application, and we have separated off the discussion of these in the **Linearity conditions** and the **Strong approximation** windows. There are four logically independent parts to the argument.

I. The 'linear case': this is the heart of the proof. In Section 2 we show that a semisimple arithmetic group can *never* have wPSG (unless it is finite); this is an application of the Prime Number Theorem. Then using the 'Lubotzky alternative' ($\looparrowright$ **Strong approximation**), we deduce that every finitely generated characteristic-zero linear group with wPSG is virtually soluble.

II. The 'main reduction': in Section 3 we show that every group G with wPSG has *restricted upper chief factors*, that is, there is a finite upper bound for the ranks of all non-abelian upper chief factors of G (factors A/B where B is a normal subgroup of finite index in G and A/B is a minimal normal subgroup of G/B). This depends on CFSG. Together with a result from the **Linearity conditions** window, this implies the following: if G is finitely generated and has wPSG then G has a normal subgroup D such that

(i) G/D is a linear group over a field of characteristic zero, and

(ii) the image of D in every finite quotient of G is soluble.

III. The 'prosoluble case': in Section 4 we prove that *every prosoluble group with wPSG has finite rank* (as a profinite group); this is essentially a result about finite soluble groups. It means in particular that if a group G with wPSG has all its finite quotients soluble, then G has finite upper rank.

IV. The proof of Theorem 5.2 is given in Section 5. This depends on the Feit-Thompson Odd Order Theorem and P. Hall's theory of finitely generated soluble groups, and applies another result from the **Linearity conditions** window**.**

Together these four steps complete the proof of Theorem 5.1. We have already observed that if G is virtually soluble of finite rank then G has PSG (Corollary 1.4.3). Suppose conversely that G is a finitely generated residually finite group with weak PSG, and let D be the normal subgroup provided by Step **II**. Step **I** shows that G/D has a soluble normal subgroup G_0/D of finite index; and then from property (ii) of D it follows that every finite quotient of G_0 is soluble. An elementary lemma, proved in Section 1, shows that G_0 also has wPSG, and it follows by Step **III** that G_0 has finite upper rank. Finally, Theorem 5.2 shows that G_0 is virtually soluble of finite rank, and hence so is G.

To any group G with PSG one may associate its 'minimal degree of polynomial growth', namely

$$\begin{aligned}\alpha(G) &= \inf\{c \mid s_n(G) \leq n^c \text{ for large enough } n\} \\ &= \limsup \frac{\log s_n(G)}{\log n}.\end{aligned}$$

It seems to be a difficult problem to determine $\alpha(G)$ in terms of the algebraic structure of G. In the final section we show that $\alpha(G)$ is bounded above and below by constant multiples of the Hirsch length of G.

Is it possible to characterise the PSG groups that are not necessarily finitely generated? Since subgroup growth is a property of the profinite completion of a group, this may be construed as a question about the *general profinite PSG group*. A structural description of these is given in Chapter 10, where we shall see that every profinite group with PSG is, roughly speaking, an extension of a prosoluble group of finite rank by a product of finite simple groups; from this more general point of view, it then appears that the restriction to finitely generated groups has the effect of killing off the infinite semisimple 'top layer'.

Let us conclude this introduction with a philosophical remark. It is a remarkable feature of both Theorems 5.1 and 5.2 that a hypothesis which mentions only a *finiteness condition* leads to the conclusion of *solubility*. Two facts in particular lie behind this, one 'local', one 'global'.

First of all, The Odd Order Theorem, which lies at the heart of Theorem 5.2: this infers the solubility of a *finite* group from a purely arithmetical hypothesis, and takes us to the point where we know that every finite quotient of our group is soluble. Secondly, the structure of semisimple algebraic groups. This leads to the 'global' conclusion of solubility by way of a contradiction: an algebraic group that is not virtually soluble must have a non-trivial image which is semisimple, at which point we can examine the congruence structure of a suitable arithmetic group and find that the original hypotheses (of an arithmetical nature) are violated.

5.1 Preliminary observations

For any group G we define

$$\begin{aligned}\alpha^\dagger(G) &= \inf\left\{\alpha > 0 : s(\overline{G}) \leq \left|\overline{G}\right|^\alpha \text{ for every finite quotient } \overline{G} \text{ of } G\right\}, \\ \alpha^*(G) &= \inf\{\alpha > 0 : s_n(G) \leq n^\alpha \text{ for all } n \in \mathbb{N}\},\end{aligned}$$

where conventionally $\inf \emptyset = \infty$. Thus G has weak PSG if and only if $\alpha^\dagger(G)$ is finite. It is clear that

$$\alpha^\dagger(G) \leq \alpha^*(G),$$

so wPSG is indeed a (possibly) weaker condition than PSG.

The *upper rank* of a group G is

$$\begin{aligned}\mathrm{ur}(G) &= \sup\left\{\mathrm{rk}(\overline{G}) : \overline{G} \text{ a finite quotient of } G\right\}\\ &= \mathrm{rk}(\widehat{G}).\end{aligned}$$

Since $s(G) \leq |G|^{\mathrm{rk}(G)}$ when G is finite, we see that for every group G

$$\alpha^\dagger(G) \leq \mathrm{ur}(G).$$

It is also true that $\alpha^*(G)$ is bounded above by a function of $\mathrm{ur}(G)$, but this fact lies deeper, and will be proved in Section 1 of Chapter 10.

It is *not* true that $\mathrm{ur}(G)$ is in general bounded above by a function of $\alpha^*(G)$: in Section 3 of Chapter 10 we shall see examples of groups with PSG that have infinite upper rank. That there is such a bound when one restricts to (pro)*soluble* groups is established in Section 4, below; it is the essential link between Theorem 5.1 and Theorem 5.2 in the (pro)soluble case.

It is obvious that each of the three properties PSG, wPSG and finiteness of upper rank is preserved on passing to quotients. The main point we wish to establish here is that each property is also preserved on passing to finite extensions and to subgroups of finite index. We shall use these facts freely throughout the rest of the chapter.

Proposition 5.1.1 *Suppose $H \leq G$ where $|G : H| = m \leq \infty$. Then*

$$\mathrm{ur}(H) \leq \mathrm{ur}(G) \leq \mathrm{ur}(H) + \log m; \tag{5.1}$$

$$\alpha^\dagger(G) \leq \alpha^\dagger(H) + \log m; \tag{5.2}$$

$$\alpha^\dagger(H) \leq \begin{cases} (m + \log m)\alpha^\dagger(G) & \text{if } H \lhd G \\ (m! + \log m!)\alpha^\dagger(G) + \log(m-1)! & \text{in general} \end{cases}; \tag{5.3}$$

$$\alpha^*(H) \leq (1 + \log m)\alpha^*(G); \tag{5.4}$$

$$\alpha^*(G) \leq m + \alpha^*(H) \quad \text{if } H \lhd G. \tag{5.5}$$

Proof. Since every subgroup of finite index in H contains a normal subgroup of finite index in G, it is enough to consider the case where G is a finite group.

(5.1) is clear, since if $L \leq G$ then L is generated by $L \cap H$ and at most $\log |L : L \cap H| \leq \log m$ further elements. A similar argument establishes (5.2).

For (5.3), suppose first that $H \lhd G$. If $N \lhd H$ has index $n \geq 2$ then N contains a normal subgroup N^0 of G with $\left|H : N^0\right| \leq n^m$, and then

$$\begin{aligned}s(H/N) \leq s(G/N_0) &\leq \left|G : N^0\right|^{\alpha^\dagger(G)}\\ &\leq (mn^m)^{\alpha^\dagger(G)} \leq n^{(m+\log m)\alpha^\dagger(G)}.\end{aligned}$$

The general case follows on replacing H by its normal core, and then applying (5.2).

(5.4) is clear since $s_n(H) \leq s_{mn}(G)$ for each n. Finally, (5.5) follows from Proposition 1.3.2(ii) of Chapter 1. ■

5.2 Linear groups with PSG

Let G be a finitely generated linear group over a field of characteristic zero, and suppose that G is not virtually soluble. We shall prove that G does *not* have wPSG. According to the 'Lubotzky alternative' ($\looparrowright$ **Strong approximation**), there exist a subgroup G_1 of finite index in G, a finite set of primes S, and a connected, simply connected simple algebraic group $\mathfrak{S}$ over $\mathbb{Q}$ such that every congruence quotient of $\Gamma = \mathfrak{S}(\mathbb{Z}_S)$ appears as a quotient of G_1 (and Γ is infinite). If G has wPSG then so does G_1; hence $s(\Gamma^*)$ is bounded by some fixed power of $|\Gamma^*|$ as Γ^* ranges over the congruence quotients of Γ. It will therefore suffice to show that

$$\frac{\log s(\Gamma/\Delta)}{\log |\Gamma/\Delta|}$$

is unbounded as Δ ranges over the principal congruence subgroups of Γ.

Let us suppose that $\mathfrak{S} \leq \mathrm{GL}_d$. The fact that Γ is infinite implies that the topological group

$$\mathfrak{S}(\mathbb{R}) \times \prod_{p \in S} \mathfrak{S}(\mathbb{Q}_p)$$

is non-compact, because it contains Γ as a discrete subgroup. This means that the algebraic group $\mathfrak{S}$ satisfies the hypotheses of the Strong Approximation Theorem with respect to the set $S \cup \{\infty\}$. It follows in particular that for $m = q_1 \dots q_k$ where $q_1, \dots, q_k$ are distinct primes not in S, the natural homomorphism π_m of Γ into $\mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z})$ maps Γ onto

$$\mathfrak{S}(\mathbb{Z}/m\mathbb{Z}) = \prod_{i=1}^{k} \mathfrak{S}(\mathbb{Z}/q_i\mathbb{Z}).$$

Thus writing $\Gamma(m)$ for the congruence subgroup $\ker \pi_m$, we have

$$\Gamma/\Gamma(m) \cong \prod_{i=1}^{k} \mathfrak{S}(\mathbb{F}_{q_i}).$$

(For all this, see the **Strong approximation** window.)

Next, we observe that for almost all primes p, the group $\mathfrak{S}(\mathbb{F}_p)$ has even order; this follows from Lang's theorem on finite algebraic groups ($\looparrowright$ **Linear groups**), or it can be deduced from the Odd Order Theorem, as follows: if $\mathfrak{S}(\mathbb{F}_p) \leq \mathrm{GL}_d(\mathbb{F}_p)$ has odd order, then it is soluble, of derived length bounded in terms of d (Zassenhaus's Theorem, $\looparrowright$ **Linear groups**); so if T is the set of all such primes p then $\Gamma/\bigcap_{p\in T}\Gamma(p)$ is also soluble. But if T is infinite then $\bigcap_{p\in T}\Gamma(p) = 1$, whence Γ is soluble. This is impossible because Γ is Zariski-dense in the simple algebraic group $\mathfrak{S}$ (Borel's density theorem, [PR], Theorem 4.10). The set T of exceptional primes must therefore be finite.

Write p_n to denote the nth prime (in ascending order starting from $p_1 = 2$), and let t be the biggest index for which either $p_t \in S$ or $\mathfrak{S}(\mathbb{F}_p)$ has odd order.

If

$$m = \prod_{n=t+1}^{t+k} p_n,$$

then the group $\Gamma/\Gamma(m)$ contains an elementary abelian subgroup of order 2^k, and it follows that

$$s(\Gamma/\Gamma(m)) \geq 2^{[k^2/4]},$$

(Proposition 1.5.2). On the other hand,

$$|\Gamma/\Gamma(m)| \leq |\mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z})| \leq m^{d^2};$$

so the essence of the matter is to compare m with k. This is exactly what the Prime Number Theorem does. In fact, for present purposes we only need an easier weak version of it, originally proved by Chebyshev (↬ **Primes**): there exists $A > 0$ such that

$$\log\left(\prod_{i=1}^{n} p_i\right) \leq An \log n$$

for all $n \geq 1$. Taking $n = t + k$ where $k \geq t$, say, gives $\log m < 4Ak \log k$, so we have

$$\frac{\log s(\Gamma/\Delta_m)}{\log|\Gamma/\Delta_m|} > \frac{k^2/4}{4d^2Ak\log k} = a\frac{k}{\log k}$$

where $a = (16d^2A)^{-1} > 0$.

As $k/\log k \to \infty$ with k, it follows that $\log s(\Gamma/\Delta)/\log|\Gamma/\Delta|$ is unbounded as Δ ranges over the principal congruence subgroups, as required.

Note that if n is large then there exists k such that

$$4d^2A \cdot k\log k \leq \log n < 8d^2A \cdot k\log k.$$

With m as above, the number $c_n(\Gamma)$ of congruence subgroups of index at most n in Γ is then at least $s(\Gamma/\Delta_m) \geq 2^{[k^2/4]}$; while

$$\frac{\log n}{\log\log n} \leq \frac{8d^2Ak\log k}{\log(4d^2A) + \log k + \log\log k} < 8d^2Ak.$$

Thus

$$c_n(\Gamma) \geq 2^{[k^2/4]} > 2^{b(\log n/\log\log n)^2} = n^{b\log n/(\log\log n)^2}$$

where $b = (256A^2d^4)^{-1} > 0$. Sharper bounds for the congruence subgroup growth of arithmetic groups will be obtained in Chapter 6, by applying a more delicate form of the Prime Number Theorem along arithmetic progressions.

5.3 Upper chief factors

The PSG theorem depends ultimately on two particular properties of the finite simple groups: the first is that each contains a relatively large elementary abelian subgroup, which implies that a semisimple group contains many subgroups relative to its order; the second is that a simple group has relatively few automorphisms, which is used to show that any non-abelian chief factor in a group appears in the group with relatively small index (in fact it suffices to know that a simple group S can be generated by two elements, which implies that S has at most $|S|^2$ automorphisms). In this section we spell out the details. In Chapter 10, we shall see that the 'Profinite PSG Theorem' depends on some more delicate information about the simple groups, namely that for a simple group of bounded rank, both the outer automorphism group and the Schur multiplier have bounded orders.

Definition An *upper composition (*respectively *chief) factor* of a group G is a composition factor *(*respectively *chief factor)* of some finite quotient of G.

Definition The group G has *restricted upper composition (*respectively *chief) factors* if there is a finite upper bound to the ranks of all non-abelian upper composition (respectively chief) factors of G.

The key result is

Proposition 5.3.1 *Every group with* weak PSG *has restricted upper chief factors.*

We denote by

$$\mathcal{X}(n, e)$$

the set of all simple groups of Lie type ${}^*X_n(\mathbb{F}_{p^e})$, that is, groups of Lie rank n over finite fields having degree e over a prime field. It follows from CFSG (↬ **Finite simple groups**) that a family of non-abelian finite simple groups has bounded rank if and only if there exists a positive integer β such that the family is contained in the union of the following three families of groups:

$\mathcal{S}_0$**:** *the sporadic finite simple groups*

$\mathcal{A}(\beta)$**:** *alternating groups of degree at least 5 and at most* β

$\mathcal{X}(\beta) = \bigcup\{\mathcal{X}(n, e) \mid n \leq \beta \text{ and } e \leq \beta\}$

(here 'rank' is meant in the group-theoretic sense, i.e. Prüfer rank, *not* Lie rank).

Lemma 5.3.2 *Let* $S = \mathrm{Alt}(n)$ *where* $n \geq 5$*. Then* S *contains an elementary abelian* 2*-subgroup* E *with* $2 \mid \mathrm{rk}(E) > n/4$.

Proof. Say $n = 4k + r$ $(0 \leq r < 4)$. Then S contains the direct product of k copies of Alt(4), and for E we take the corresponding product of k Klein 4-groups. Thus E has rank $2k > n/4$. ■

Lemma 5.3.3 *Let $S = {}^*X_n(\mathbb{F}_{p^e})$ be simple of Lie type. Then S contains an elementary abelian p-subgroup E with* $\mathrm{rk}(E) > ne/8$ *and* $|E|^{248} \geq |S|$.

Proof. Note that

$$|S| \leq p^{248e} \text{ if } n \leq 8$$
$$|S| \leq p^{n(2n+1)e} \text{ if } n > 8$$

(↬ **Finite simple groups).**

Suppose first that $n \leq 8$. We take E to be an additive one-parameter subgroup (a root subgroup or a suitable subgroup of a root subgroup). Then E is elementary abelian of rank $e \geq \frac{1}{8}ne$, and $|E| = p^e \geq |S|^{1/248}$.

Now suppose that $n = 4k + r > 8$ $(0 \leq r < 4)$. Then S is a classical group, hence contains a copy of $(\mathrm{P})\mathrm{SL}_{[n/2]}(\mathbb{F}_{p^e})$ (↬ **Finite simple groups**). The upper unitriangular matrices in this group having non-zero off-diagonal entries only in the top $k \times k$ right corner form an elementary abelian p-subgroup E of rank $k^2e \geq \frac{1}{4}ne$, and

$$|E| = p^{k^2e} \geq |S|^{1/64}.$$

■

Definition For a group G,

$$\beta(G)$$

denotes the least natural number β such that every non-abelian upper composition factor of G lies in $\mathcal{S}_0 \cup \mathcal{A}(\beta) \cup \mathcal{X}(\beta)$ (if there is no such number then $\beta(G) = \infty$).

$$w(G)$$

denotes the supremum of the natural numbers m such that some finite quotient of G has a normal subgroup isomorphic to $S^{(m)}$ for some non-abelian finite simple group S.

Now Proposition 5.3.1 will follow from the slightly stronger

Proposition 5.3.4 *There is a function $f : \mathbb{N} \to \mathbb{N}$ such that for any group G with* weak PSG *we have*

$$w(G) \leq f(\alpha^\dagger(G)),$$
$$\beta(G) \leq f(\alpha^\dagger(G)).$$

Proof. As we are concerned only with the finite quotients of G, we may suppose that G is in fact finite. Put $\alpha = \alpha^\dagger(G)$. It will suffice to show the following: if $M \cong S^{(m)}$ is a non-abelian normal subgroup of G and S is simple then $m \leq f(\alpha)$ and $S \in \mathcal{S}_0 \cup \mathcal{A}(\beta) \cup \mathcal{X}(\beta)$ where $\beta \leq f(\alpha)$.

Replacing G by a suitable quotient we may assume in addition that $\mathrm{C}_G(M) = 1$. Then G acts faithfully by conjugation on M, and permutes the m simple factors of M among themselves. The kernel G_0 of this permutation action has index at most $m!$ in G; on the other hand, since S can be generated by 2 elements ($\twoheadrightarrow$ **Finite simple groups**), $|\mathrm{Aut}(S)| \leq |S|^2$, and it follows that $|G_0| \leq |S|^{2m}$. Thus $|G| \leq m!\,|S|^{2m}$, which implies that

$$s(G) \leq (m!\,|S|^{2m})^\alpha < m^{m\alpha}\,|S|^{2m\alpha}.$$

Now we separate three cases.

Case 1: $S \in \mathcal{S}_0$. Let C be the maximal order of a sporadic simple group (so C is the order of the Monster simple group in fact). The group S contains an involution, so M has an elementary abelian 2-subgroup of rank m, hence contains at least $2^{[m^2/4]}$ subgroups. Hence

$$2^{[m^2/4]} \leq s(G) \leq m^{m\alpha} C^{2m\alpha}.$$

Case 2: $S = \mathrm{Alt}(n)$ where $n \geq 5$. Using Lemma 5.3.2 we see similarly that M contains at least $2^{m^2n^2/8}$ subgroups. As $|S| = n!/2 < n^n$ we infer that

$$2^{m^2n^2/8} \leq s(G) < m^{m\alpha} n^{2mn\alpha}.$$

Case 3: $S = {}^*X_n(\mathbb{F}_{p^e})$. By Lemma 5.3.3, S contains an elementary abelian p-subgroup E of rank r, say, where $r > ne/8$ and $|S| \leq p^{248r}$. As above, this implies that

$$p^{[m^2r^2/4]} \leq m^{m\alpha} p^{496mr\alpha}.$$

In each case, taking the logarithm of each side of the given inequality, and noting that $\log x/x \to 0$ as $x \to \infty$, we may deduce

in *Case 1* that m is bounded by a function of α ;

in *Case 2* that m and n are bounded by functions of α ;

in *Case 3* that m and r are bounded by functions of α , which implies that n and e are also so bounded since $ne < 8r$.

This completes the proof. ■

Now the following is proved as Corollary 3 in the **Linearity conditions** window:

Proposition 5.3.5 *Let G be a finitely generated group with restricted upper chief factors. Then there is an exact sequence*

$$1 \to D \to G \to \mathrm{GL}_n(F)$$

where F is a field of characteristic zero and the closure of D in $\widehat{G}$ is prosoluble.

With Proposition 5.3.1 this now gives the main result of this section,

Proposition 5.3.6 *Let G be a finitely generated group with* wPSG. *Then G has a normal subgroup D such that (i) G/D is linear over a field of characteristic zero and (ii) $D/(N \cap D)$ is soluble for every normal subgroup N of finite index in G.*

This conclusion applies only to finitely generated groups. Propositions 5.3.1 and 5.3.4, on the other hand, are quite general, and will be used in Chapter 10 where we characterise the profinite groups with wPSG.

Similar restrictions on the upper composition factors of a group G can be inferred, using the same kind of argument, if G has subgroup growth slightly faster than PSG: if we assume merely that G has subgroup growth of type strictly less than $n^{\log n/(\log\log n)^2}$, then there exist β_0 and for each prime p some finite β_p such that every non-abelian upper composition factor S of G belongs to

$$\mathcal{S}_0 \cup \mathcal{A}(\beta_0) \cup \bigcup_p \{{}^*X_n(\mathbb{F}_{p^e}) \mid n \leq \beta_p,\ e \leq \beta_p\}\,.$$

If $M \cong S^{(m)}$ is a normal subgroup of some finite quotient of G, then m is bounded for $S \in \mathcal{S}_0 \cup \mathcal{A}(\beta_0)$ and m is bounded by some number depending on p if $S = {}^*X_n(\mathbb{F}_{p^e})$ (see [Segal (a)]). However, the dependence on p is unavoidable in this case, as shown by the examples constructed in Chapter 13.

5.4 Groups of prosoluble type

Let us say that a group G is of *prosoluble type* if G is residually finite and every finite quotient of G is soluble; in other words, G embeds naturally in its profinite completion $\widehat{G}$, and $\widehat{G}$ is a prosoluble group. The aim of this section is to establish

Theorem 5.4.1 *Every group of prosoluble type with* weak PSG *has finite upper rank.*

This follows from the quantitative version:

Proposition 5.4.2 *There is a function $f : \mathbb{N} \to \mathbb{N}$ such that*

$$\mathrm{rk}(G) \leq f(\alpha^\dagger(G))$$

for every finite soluble group G.

Proof. Kovacs's Theorem (↬ **Finite groups)** says that

$$\mathrm{rk}(G) \leq 1 + \max_p \mathrm{r}_p(G),$$

so let us fix a prime p and show that $\mathrm{r}_p(G)$ is bounded above by some function of $\alpha^\dagger(G) = \alpha$. Since $\mathrm{r}_p(G) = \mathrm{r}_p(G/O_{p'}(G))$, we may now factor out $O_{p'}(G)$ and assume further that $O_{p'}(G) = 1$.

Put $F = O_p(G)$. Then $F = \mathrm{Fit}(G)$ and so $\mathrm{C}_G(F) = \mathrm{Z}(F)$ ($\leadsto$ **Finite group theory**). Now considering $F/F'F^p$ as an $\mathbb{F}_pG$-module, let V denote the direct sum of its $\mathbb{F}_pG$-composition factors and C the kernel of the action of G on V. Then $C/\mathrm{Z}(F)$ acts faithfully and nilpotently on the p-group F, and it follows that C is a p-group; hence $C = F$ and so G/F acts faithfully on the completely reducible $\mathbb{F}_pG$-module V. It follows by the theorem of Pálfy and Wolf ($\leadsto$ **Permutation groups**) that $|G : F| \leq p^{3d}$ where $d = \dim_{\mathbb{F}_p}(V) = \dim_{\mathbb{F}_p}(F/F'F^p)$. Since $F/F'F^p$ contains at least $p^{[d/2]^2}$ subspaces, we have

$$p^{[d/2]^2} \leq s(G/F'F^p) \leq |G/F'F^p|^\alpha \leq p^{4d\alpha},$$

giving $d \leq 16\alpha + 2$. Hence $|G : F| \leq p^m$ where $m = 48\alpha + 6$.

Now put $F_0 = F$ and for $i \geq 0$ let $F_{i+1} = F_i'F_i^p$. Let $s = \max_i \dim_{\mathbb{F}_p}(F_{i-1}/F_i)$, $q = 2 + [\log s]$. Then F_q is a powerful p-group, $|F : F_q| \leq p^{sq}$ and $\mathrm{rk}(F) \leq s(q+1)$. Since F_q is powerful, we have $\dim_{\mathbb{F}_p}(F_{i-1}/F_i) \leq \dim_{\mathbb{F}_p}(F_q/F_{q+1})$ for all $i > q$; hence $\dim_{\mathbb{F}_p}(F_{i-1}/F_i) = s$ for some $i \leq q+1$. (For properties of powerful p-groups, $\leadsto$ **Pro-p groups**.) Then $|G : F_i| \leq p^{(q+1)s+m}$, and as above we infer that $[s/2]^2 \leq ((q+1)s + m)\alpha$. Since $q \leq 2 + \log s$ this implies that s is bounded by some function of m and α. As

$$\mathrm{r}_p(G) \leq \mathrm{r}_p(G/F) + \mathrm{rk}(F) \leq m + (q+1)s,$$

the result follows. ■

As we shall see repeatedly, a key step in the investigation of PSG groups is to establish upper bounds for the index of elementary abelian sections in a group: this connects the subgroup growth of the elementary abelian section to that of the group, and can then be used to estimate the rank of the section. In the preceding proof, the required upper bound was provided by the Pálfy-Wolf theorem which bounds the order of a completely reducible soluble linear group over $\mathbb{F}_p$; the generalisation of this result to linear groups with restricted composition factors will play the analogous role in Section 2 of Chapter 10.

5.5 Groups of finite upper rank

Here we prove Theorem 5.2. As with the PSG Theorem, the proof has a 'local' part and a 'global' part.

The 'local' part concerns the finite images of a group, and does not depend on finite generation. For a finite group G with Sylow p-subgroup $S_p(G)$, let

$$\begin{aligned} \mathrm{ds}_p(G) &= d(S_p(G)), \\ \mathrm{r}_p(G) &= \mathrm{rk}(S_p(G)); \end{aligned}$$

for any group G, write

$$\begin{aligned} \mathrm{uds}_p(G) &= \sup\left\{\mathrm{ds}_p(\overline{G}) \mid \overline{G} \text{ a finite quotient of } G\right\}, \\ \mathrm{ur}_p(G) &= \sup\left\{\mathrm{r}_p(\overline{G}) \mid \overline{G} \text{ a finite quotient of } G\right\}; \end{aligned}$$

equivalently, $\mathrm{uds}_p(G) = d(S_p(\widehat{G}))$ and $\mathrm{ur}_p(G) = \mathrm{rk}(S_p(\widehat{G}))$ where $S_p(\widehat{G})$ is a Sylow pro-p subgroup of the profinite completion $\widehat{G}$. It is clear that

$$\mathrm{uds}_p(G) \leq \mathrm{ur}_p(G) \leq \mathrm{ur}(G)$$

for each prime p and every group G.

Recall that a group G is *of prosoluble type* if G is residually finite and $\widehat{G}$ is prosoluble, which amounts to saying that every finite quotient of G is soluble.

Theorem 5.5.1 *Let G be a residually finite group. If $\mathrm{uds}_2(G)$ is finite then G is virtually of prosoluble type.*

Proof. Let K be a normal subgroup of finite index in G such that $\mathrm{ds}_2(G/K) = \mathrm{uds}_2(G)$. We claim that every finite quotient of K is soluble. To establish this, let K/N_1 be a finite quotient of K. Then N_1 contains a finite-index normal subgroup N of G, and it will suffice to show that K/N is soluble.

Now Tate's theorem (↬ **Finite groups**) shows that the group K/N has a normal 2-complement, Q/N say. Then Q/N is soluble by the Odd order theorem, and K/Q is soluble because it is a 2-group. The claim follows. ■

Remark The first part of this argument is equally valid for odd primes p; it shows that if $\mathrm{uds}_p(G)$ is finite then G has a normal subgroup G_0 of finite index such that every finite quotient of G_0 has a normal p-complement. In this case, *every subgroup of p-power index in G_0 is subnormal.*

We now proceed to the 'global' part of the argument. Let G be a finitely generated residually finite group of finite upper rank. By Theorem 5.5.1, G has a normal subgroup G_0 of finite index that is of prosoluble type. Replacing G by G_0, we may as well assume that G is of prosoluble type. Then G satisfies the hypotheses of Corollary 5 in the **Linearity conditions** window: this asserts that *a finitely generated group of prosoluble type and finite upper rank is virtually nilpotent-by-abelian.* Again replacing G by a finite-index subgroup, we may therefore suppose that G is nilpotent-by-abelian; and Theorem 5.2 will follow once we have established

Proposition 5.5.2 *Let G be a finitely generated nilpotent-by-abelian group. If $\mathrm{ur}_p(G)$ is finite for every prime p then G has finite rank.*

Proof. Let A be the derived group of G, and A' the derived group of A. Thus A is nilpotent; if A/A' has finite rank then A has finite rank (↬ **Soluble groups**), so we may replace G by G/A' and assume that A is abelian. Then A may be considered as a module for the group ring $\mathbb{Z}[G/A] = S$, with the elements

of G/A acting via inner automorphisms of G (we shall write the group operation in A as addition). According to P. Hall's theory (↬ **Soluble groups**), we have the following:

(i) every quotient of G is residually finite;

(ii) A is a Noetherian S-module;

(iii) A contains a free abelian subgroup F such that A/F is a π-torsion group for some finite set π of primes.

Let T be the torsion subgroup of A. Since G is residually finite, each finite subgroup of T maps injectively into some finite quotient of G, which implies that for each prime p, the p-rank of T is at most $\mathrm{ur}_p(G)$. On the other hand, it follows from (ii) that T has finite exponent, q say. We conclude that T is finite, of order at most q^r where $r = \max\{\mathrm{ur}_p(G) \mid p \mid q\}$.

Replacing G by G/T, we may therefore suppose that A is torsion-free. Let p be any prime not in π. Then

$$pA \cap F = pF,\ pA + F = A$$

and so $F/pF \cong A/pA$. Since G/pA is residually finite we see that $\mathrm{rk}(A/pA) \leq \mathrm{ur}_p(G)$. It follows that $\mathrm{rk}(F) = \mathrm{rk}(F/pF) \leq \mathrm{ur}_p(G)$ is finite. Since the rank of A is equal to $\mathrm{rk}(F)$ and G/A is a finitely generated abelian group, G has finite rank as claimed. ■

This concludes the proof of Theorem 5.2, and with it of the PSG Theorem.

5.6 The degree of polynomial subgroup growth

Recall that

$$\alpha(G) = \limsup \frac{\log s_n(G)}{\log n},$$

which is finite if and only if G has polynomial subgroup growth. We call this the *degree* of G. (The reader is warned, however, that this differs from the usage of [Shalev 1999]: see the *Notes* below.) How does this invariant relate to the structure of G?

It is not hard to see that

$$\alpha(\mathbb{Z}^{(d)}) = d,$$

either directly by applying the lemma below, or by identifying $\alpha(G)$ as the abscissa of convergence of the associated zeta function (see Chapter 15). In general, a finitely generated residually finite PSG group is virtually soluble of finite rank; for such a group G, the invariant corresponding to the dimension of $\mathbb{Z}^{(d)}$ is the *Hirsch length* $h(G)$, defined as follows. Let T be the maximal periodic normal subgroup of G. According to the structure theory (↬ **Soluble groups**), there is a chain of subgroups

$$T = G_0 \lhd G_1 \lhd \ldots \lhd G_h \lhd G \tag{5.6}$$

such that each factor G_i/G_{i-1} is torsion-free abelian of rank 1, and G/G_h is finite. Also T is finite if G is residually finite. We set $h(G) = h$ (an invariant of G by the Jordan-Hölder theorem).

Lemma 5.6.1 *Let G be a group and N a normal subgroup such that G/N has rank 1. Then for each $n \geq 1$,*

$$s_n(G) \leq n \cdot s_n(N).$$

Proof. Write $Q = G/N$. From Proposition 1.3.2(i) we have

$$a_m(G) \leq \sum_{t|m} a_{m/t}(Q) a_t(N) t^{\mathrm{rk}(Q)} \leq \sum_{t|m} 1 \cdot a_t(N) \cdot t.$$

Therefore

$$s_n(G) \leq \sum_{t \leq n} \left[\frac{n}{t}\right] t a_t(N) \leq n \sum_{t \leq n} a_t(N) = n s_n(N).$$

■

Applying this to (5.6) we deduce that $s_n(G_h/G_0) \leq n^h$ for each n, so $\alpha(G_h/G_0) \leq h$. The next two propositions will enable us to deal with the 'missing' factors G_0 and G/G_h.

Proposition 5.6.2 *Let G be a group of finite rank and T a finite normal subgroup of G. Then $\alpha(G/T) = \alpha(G)$.*

Proof. Write $Q = G/T$. Clearly $\alpha(Q) \leq \alpha(G)$, and we may assume that $\alpha(Q)$ is finite. Put $r = \mathrm{rk}(Q)$. As above, we have

$$\begin{aligned} s_n(G) &\leq \sum_{j \leq n} \sum_{t|j} a_{j/t}(Q) a_t(T) t^r \\ &\leq s(T) \, |T|^r \sum_{t||T|} \sum_{j \leq n} a_{j/t}(Q) \\ &\leq s(T) \, |T|^{r+1} \, s_n(Q), \end{aligned}$$

since $a_t(T) = 0$ when $t \nmid |T|$. It follows that $\alpha(G) \leq \alpha(Q)$. ■

Lemma 5.6.3 *Let Q be a finite group and S a finite soluble group of derived length l. Then*

$$\mathrm{der}(Q, S) \leq q^{rsl} \, |S|$$

where $s = \mathrm{rk}(S)$, $r = \mathrm{rk}(Q)$ and q is the exponent of Q.

Proof. Suppose to begin with that S is abelian. From §1.3 we have

$$\begin{aligned} \mathrm{der}(Q, S) &\leq |S| \cdot \left|H^1(Q, S)\right|, \\ q \cdot H^1(Q, S) &= 0, \\ \mathrm{rk}(H^1(Q, S)) &\leq rs, \end{aligned}$$

the last because $\mathrm{Der}(Q,S)$ is isomorphic to a subgroup of $S^{(d(Q))}$. It follows that

$$\left|H^1(Q,S)\right| \leq q^{rs}$$

and hence that $\mathrm{der}(Q,S) \leq q^{rs}\left|S\right|$.

For the general case, let $A_1,\ldots,A_l$ be the successive factors in the derived series of S. It is an elementary fact that then

$$\mathrm{der}(Q,S) \leq \prod_{i=1}^{l} \mathrm{der}(Q,A_i).$$

Applying the first part to each A_i we obtain

$$\mathrm{der}(Q,S) \leq q^{rsl}\prod_{i=1}^{l}\left|A_i\right| = q^{rsl}\left|S\right|.$$

■

Proposition 5.6.4 *Let H be a subgroup of finite index in a virtually soluble group G. Then*

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

Proof. Since $s_n(H) \leq s_{mn}(G)$ for all n, where $m = \left|G:H\right|$, it is easy to see that $\alpha(H) \leq \alpha(G)$. So we may assume that $\alpha(H)$ is finite and have to prove the second inequality. Let $N \leq H$ be a soluble normal subgroup of finite index in G, and put $Q = G/N$.

Now the first part of the proof of Proposition 1.3.2 shows that

$$a_n(G) \leq \sum_{t|n} a_{n/t}(Q)a_t(N)\psi(t)$$

where $\psi(t)$ denotes the maximum value taken by

$$\mathrm{der}(Q_1,S)$$

as Q_1 ranges over subgroups of Q and S ranges over sections C/D of N such that $D \lhd N$ and $\left|N/D\right| = t$. Writing q, r for the exponent and rank of Q and l, s for the derived length and rank of N, respectively, we may deduce from the preceding lemma that

$$\psi(t) \leq q^{rsl}t.$$

Thus taking $c = q^{rsl}s(Q)$ we get

$$a_n(G) \leq c\cdot\sum_{t|n} ta_t(N)$$

whence

$$\begin{aligned} s_n(G) &\leq c \sum_{j \leq n} \sum_{t|j} t a_t(N) \\ &= c \sum_{t \leq n} \left[\frac{n}{t} \right] t a_t(N) \leq cn \sum_{t \leq n} a_t(N) \\ &= cn s_n(N). \end{aligned}$$

It follows that $\alpha(G) \leq 1 + \alpha(N)$, and this gives the result since $\alpha(N) \leq \alpha(H)$. ■

Putting these together gives

Proposition 5.6.5 *Let G be a virtually soluble group of finite rank. Then*

$$\alpha(G) \leq h(G) + 1.$$

This estimate is best possible, as shown for example by the infinite dihedral group D which has $\alpha(D) = 2$. The same example shows also that Proposition 5.6.4 is best possible.

In the other direction we have

Theorem 5.6.6 *Let G be an infinite virtually soluble minimax group. Then*

$$\alpha(G) \geq \frac{1}{6} h(G).$$

Proof. Replacing G by G_0/T where T is periodic and $|G : G_0|$ is finite, we may suppose that G is soluble and residually finite.

Suppose first that $h(G) > 1$. Let p be any prime not in $\mathrm{spec}(G)$. According to Proposition 11 in the **Soluble groups** window, G then has a normal subgroup H of finite index whose pro-p completion $\widehat{H}_p$ is a pro-p group of finite rank and of dimension equal to $h(G)$. Now

$$\alpha(\widehat{H}_p) \geq \frac{1}{6} \dim \widehat{H}_p$$

by Theorem 4.1.3, and the result follows since

$$\alpha(G) \geq \alpha(H) \geq \alpha(\widehat{H}_p).$$

If $h(G) = 1$ then G has a normal subgroup H of finite index such that $\widehat{H} \cong \widehat{\mathbb{Q}_\pi}$ where $\mathbb{Q}_\pi = \mathbb{Z}[\frac{1}{p} \mid p \in \pi]$ and $\pi = \mathrm{spec}(G)$ is a finite set of primes. Since $s_n(\mathbb{Q}_\pi) \geq n - (\log n)^{|\pi|}$ for each n, we have

$$\alpha(G) \geq \alpha(H) \geq 1$$

in this case. ■

We do not know if this lower bound (or the slightly sharper one mentioned in §4.1) is best possible, or even close. It is interesting to note that the proof actually gives a lower bound for the growth of *subnormal* subgroups; it seems likely that in general $\alpha^{\triangleleft\triangleleft}(G)$ will be strictly less than $\alpha(G)$, but this is not at present clear (most of the examples for which $\alpha(G)$ is known explicitly are nilpotent groups, where of course all subgroups are subnormal).

5.7 Notes

The question of which finitely generated groups have PSG was first raised in [**Segal 1986a**], and answered there for the special case of residually nilpotent, soluble groups. New methods were introduced in [**Lubotzky & Mann 1991**], which proved the same result without assuming solubility. Key contributions of this paper were (1) the proof that pro-p groups with PSG are p-adic analytic, which is then used to reduce to the case of linear groups; (2) the 'Lubotzky alternative', reducing the problem further to arithmetic groups; and (3) the lower estimate for congruence subgroup growth in arithmetic groups (given at the end of Section 5.2 above).

The next step was taken in [**Mann & Segal 1990**]. The three main contributions of this paper were (1) bringing finite simple groups into the picture, and thereby essentially establishing the results of Section 5.3, above. (2) The proof of Theorem 5.2, about groups of finite upper rank; this was based on the methods of [**Lubotzky & Mann 1989**], which first introduced the use of Tate's theorem to deduce solubility from finite rank. Together, (1) and (2) sufficed to establish the PSG theorem for groups that are residually finite-soluble. (3) The construction of (infinitely-generated) groups with PSG that are direct products of simple groups $\mathrm{PSL}_2(\mathbb{F}_p)$ (this was important for later developments – see Chapter 10).

The full PSG theorem was finally established in [**Lubotzky, Mann & Segal 1993**], by combining the preceding arguments with an idea from [**Wilson 1991**] ($\looparrowright$ **Linearity conditions**, Theorem 2). Further properties of PSG groups were established in [**Mann 1993**]; the ideas of this paper were also important for later developments, reported in Chapter 10, as were those of [**Segal 1996b**] which introduced the concept of 'weak PSG'.

Most of the above papers make a reduction to the case of linear groups by showing that suitable pro-p completions are p-adic analytic, and then using Ado's theorem via p-adic Lie theory (the 'Lubotzky linearity criterion'). A simple alternative approach to this step was provided by [**Segal 1996a**] ($\looparrowright$ **Linearity conditions**, Section 2). This is the approach we have followed in this chapter.

Some estimates for the **degree** of finitely generated nilpotent groups were obtained in [**Grunewald, Segal & Smith 1988**], where it is shown in particular that if G is such a group and H is a subgroup of finite index then

$\alpha(G) = \alpha(H)$. [**Klopsch 2000**] established the lower bound $\alpha(G) \geq \frac{1}{7}h(G)$ for a PSG group G; the interesting proof is different from the one given above.

[**Shalev 1999**] studies a slightly different growth invariant:

$$\deg(G) = \limsup(\log a_n(G)/\log n);$$

it is easy to see that $\deg(G) \leq \alpha(G) \leq \deg(G) + 1$, but the precise relationship between the two degrees depends very much on the group in question. He proves analogues of Propositions 5.6.2 and 5.6.4 (our proofs are based on his), and determines $\deg(G)$ precisely for certain groups. Perhaps the most remarkable result of this paper is that $\deg(G)$ never takes values in the open interval $(1, 3/2)$; the result of [**Shalev 1997**] stated below implies that $(0, 1)$ is another such interval. Whether any further gaps exist in the spectrum of $\deg(G)$ is an interesting open problem. Shalev states that the $\alpha(G)$ never lies in the interval $(1, 2)$; beyond this, equally little is known about possible gaps in the spectrum of $\alpha(G)$.

Residually finite groups with very slow subgroup growth have been characterised. [**Shalev 1999**] shows that if G is finitely generated, then $a_n(G) = O(n)$ if and only if G is virtually cyclic, while in [**Shalev 1997**] it is shown that $a_n(G) = o(n)$ if and only if G has a central subgroup of finite index whose finite quotients are all cyclic, in which case $a_n(G) = O(1)$.

Chapter 6

Congruence subgroups

Among the most interesting finitely generated groups that occur 'in nature' are the *arithmetic groups*. These come equipped with a distinguished family of finite-index subgroups, the *congruence subgroups*, and the aim of this chapter is to examine their growth rate. The results, as well as being satisfying in their own right, have implications (via strong approximation methods) for linear groups in general: a foretaste appeared in Chapter 5 and more will be seen in Chapter 8.

For background on arithmetic and S-arithmetic groups, the reader is referred to the book [PR] of Platonov and Rapinchuk. However, readers unfamiliar with algebraic groups may safely ignore the more technical details, as many of the results to be discussed in this chapter make sense, and are of interest, when applied to the 'classical' groups such as $\mathrm{SL}_d(\mathbb{Z})$ or $\mathrm{SL}_d(\mathbb{Z}[1/m])$.

Before stating the results let us fix some notation.

Let k be a global field: a finite extension field of $\mathbb{Q}$ or of $\mathbb{F}_p(x)$. We denote by $\mathcal{O}$ or $\mathcal{O}_k$ the ring of integers of k. The set of all primes (equivalence classes of valuations) of k is denoted V_k. The 'infinite primes' (non-archimedean valuations) form a subset V_∞, and the set of all 'finite primes' is denoted V_f (so V_f may be identified with the set of non-zero prime ideals of $\mathcal{O}$). We recall that V_∞ is a finite set, empty if $\mathrm{char} k \neq 0$ (See e.g. [Cassels 1986].) For each $v \in V_k$ the v-completion of k is denoted k_v.

Throughout, S will denote a finite subset of V_k containing V_∞. The ring of *S-integers* is

$$\mathcal{O}_S = \{x \in k \mid v(x) \geq 0 \text{ for all } v \notin S\}.$$

Let $\mathbf{G}$ be a connected, simply-connected, simple, algebraic group defined over k with a fixed embedding $\mathbf{G} \hookrightarrow \mathrm{GL}_r$. Our main interest in this chapter is the *S-arithmetic group*

$$\Gamma = \mathbf{G}(\mathcal{O}_S) = \mathbf{G} \cap \mathrm{GL}_r(\mathcal{O}_S).$$

We assume throughout that Γ is *infinite* (or equivalently that $\prod_{v \in S} \mathbf{G}(k_v)$ is not compact).

Typical examples of such Γ are the groups $\mathrm{SL}_r(\mathbb{Z})$ or $\mathrm{SL}_r(\mathbb{Z}[1/m])$ with $r \geq 2$, in characteristic zero, and $\mathrm{SL}_r(\mathbb{F}_q[x])$ (with $r \geq 2$) in characteristic p, where $q = p^e$.

For each non-zero ideal J of $\mathcal{O}_S$ the *principal congruence subgroup* modulo J is

$$\begin{aligned}\Gamma(J) &= \ker\left(\Gamma \to \mathrm{GL}_r(\mathcal{O}_S/J)\right) \\ &= \left\{g \in \Gamma \mid g \equiv 1_r (\mathrm{mod}\, J)\right\}.\end{aligned}$$

Any subgroup of Γ containing $\Gamma(J)$ for some ideal $J \neq 0$ is called a *congruence subgroup*.

Definition $c_n(\Gamma)$ denotes *the number of congruence subgroups of index at most n in Γ.*

The first two theorems determine the strict growth type of c_n:

Theorem 6.1 *Suppose that* $\mathrm{char}\, k = 0$. *Then there exist positive constants a and b such that*

$$n^{a \log n/\log\log n} \leq c_n(\Gamma) \leq n^{b \log n/\log\log n}$$

for all $n > 1$.

In other words, in the characteristic zero case Γ has *congruence subgroup growth of strict type* $n^{\log n/\log\log n}$. On the other hand, in positive characteristic the congruence growth type is (usually) $n^{\log n}$:

Theorem 6.2 *Suppose that* $\mathrm{char}\, k = p > 0$, *that G is k-split, and if $p = 2$ that* $\mathbf{G}$ *is not of type A_1 or C_l. Then there exist positive constants a and b such that*

$$n^{a \log n} \leq c_n(\Gamma) \leq n^{b \log n}$$

for all n.

The lower bound is valid also in the excluded cases (A_1 and C_l in characteristic 2), but for these an upper bound is not known (apart from the exponential bound provided by Theorem 3.1).

There is another way to look at these results. It follows from the Strong Approximation Theorem (↬ **Strong Approximation**) that

$$\varprojlim \Gamma/\Gamma(J) \cong \varprojlim \mathbf{G}(\mathcal{O}_S/J) = \mathbf{G}(\widehat{\mathcal{O}_S}),$$

where

$$\widehat{\mathcal{O}_S} = \prod_{v \notin S} \mathcal{O}_v$$

is the profinite completion of the ring $\mathcal{O}_S$. The profinite group $\widetilde{\Gamma} = \mathbf{G}(\widehat{\mathcal{O}_S})$ is the *congruence completion* of Γ, and its open subgroups are in 1 – 1 correspondence

with the congruence subgroups of Γ; thus $c_n(\Gamma) = s_n(\widetilde{\Gamma})$ for each n and thus the 'congruence subgroup growth' of Γ may be interpreted as the subgroup growth of the profinite ('adelic') group $\widetilde{\Gamma}$.

The congruence subgroups are the 'obvious' subgroups of finite index in an arithmetic group; there may or may not be others as well. This question, the 'congruence subgroup problem', will be addressed in depth in the following chapter. The answer, for any particular arithmetic group Γ, depends on the difference between $\widetilde{\Gamma}$ and the profinite completion $\widehat{\Gamma}$ of Γ, and we shall see that it can be detected from the subgroup growth type of Γ. As this is the same as that of $\widehat{\Gamma}$, we may interpret the congruence subgroup problem as that of comparing the subgroup growth types of two profinite groups.

Theorem 6.1 is proved in Section 1 and Theorem 6.2 in Sections 2 and 3. In the final section we consider *normal* congruence subgroups. Here a startling new phenomenon appears. Let

$$c_n^{\triangleleft}(\Gamma)$$

denote *the number of normal congruence subgroups of index at most n in Γ*.

It turns out that the growth type of $c_n^{\triangleleft}(\Gamma)$ depends crucially on the 'fundamental group' of the adjoint group associated with $\mathbf{G}$. This is the quotient group $\pi(\mathbf{G})$ of the lattice of weights of $\mathbf{G}$ modulo the sublattice generated by the roots, and is isomorphic to the centre of the group scheme associated to the simply-connected cover $\widetilde{\mathbf{G}}$ of $\mathbf{G}$; usually (that is, unless $\mathrm{char}k \mid |\pi(G)|$), $\pi(\mathbf{G})$ is isomorphic to $\mathrm{Z}(\widetilde{\mathbf{G}}(\overline{k}))$ where $\overline{k}$ denotes the separable closure of k). In any case, $\pi(\mathbf{G})$ depends only on the type (i.e. Dynkin diagram) of $\mathbf{G}$, as shown in the following table:

A_l	B_l, C_l or E_7	D_l, l even	D_l, l odd	E_6	G_2, F_4, E_8
$\mathbb{Z}/(l+1)\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	0

We can now state:

Theorem 6.3 *Let $p \geq 0$ be the characteristic of k. Then the strict growth type of $c_n^{\triangleleft}(\Gamma)$ is:*

(i) n if $\mathbf{G}$ is of type G_2, F_4 or E_8,

(ii) $n^{\log n/(\log\log n)^2}$ if $\pi(\mathbf{G}) \neq 0$ and $p \nmid |\pi(\mathbf{G})|$,

(iii) $n^{\log n}$ if $p \mid |\pi(\mathbf{G})|$.

The proof of Theorem 6.3 partially depends on studying first the normal subgroup growth of open compact subgroups in algebraic groups over local fields.

Theorem 6.4 *Let K be a non-archimedean local field of characteristic $p \geq 0$ and $\mathcal{O}_K$ its valuation ring. Let $\mathbf{G}$ be a connected, simply connected K-simple subgroup of GL_r. Let*

$$\Delta = \mathbf{G}(\mathcal{O}_K) = \mathbf{G}(K) \cap \mathrm{GL}_r(\mathcal{O}_K).$$

Then the normal subgroup growth of Δ is of strict type

(i) $n^{\log n}$ *if* $p \,\big|\, |\pi(\mathbf{G})|$

(ii) n *if* $\mathbf{G}$ *is of* Ree type*, i.e., either* $p = 2$ *and* $\mathbf{G}$ *is of type* F_4 *or* $p = 3$ *and* $\mathbf{G}$ *is of type* G_2*.*

(iii) $\log n$ *otherwise.*

The proofs of Theorems 6.3 and 6.4 are sketched in section 6.4 below. The proofs show that the groups of Ree type which play a special role in Theorem 6.4 appear for an entirely different reason than G_2, F_4, and E_8 appear in Theorem 6.3. In fact, G_2, F_4 and E_8 appear in Theorem 6.3 because their *fundamental group is trivial*, while the groups of Ree type appear in 6.4 as exceptions because their *adjoint representations are reducible*. There are other cases of reducibility, e.g. when $p = 2$ and $\mathbf{G}$ is of type A_1, but in all of them p divides $|\pi(\mathbf{G})|$ and so they are covered by case (i). In particular, this is the case for the groups of Suzuki type.

The following two tables summarize the growth types of $s_n(\Delta), s_n^{\triangleleft}(\Delta), c_n(\Gamma)$ and $c_n^{\triangleleft}(\Gamma)$; in items marked $(*)$ we assume that $\mathbf{G}$ satisfies the hypotheses of Theorem 6.2.

Table 1: Local Groups
Δ as in Theorem 6.4

$p = 0$		$p > 0$	
$s_n(\Delta)$:	n	$s_n(\Delta)$:	$n^{\log n}$ $(*)$
$s_n^{\triangleleft}(\Delta)$:	$\log n$	$s_n^{\triangleleft}(\Delta)$:	$n^{\log n}$ if $p \,\big|\, \lvert\pi(\mathbf{G})\rvert$ n if $\mathbf{G}$ is of Ree type $\log n$ otherwise

The results on $s_n(\Delta)$ follow from results of Chapter 4. When K has characteristic zero and residue characteristic q, Δ is a linear group over $\mathbb{Z}_q$ and hence virtually a pro-q group of finite rank ($\looparrowright$ **Pro-p groups**). When $\mathrm{char}\, K = p > 0$, Δ is virtually an $\mathcal{O}_K$*-perfect* pro-p group in the sense of §4.4 (see [DDMS] Exercise 13.11).

Table 2: S-Arithmetic Groups
Γ as in Theorems 6.1, 6.2, 6.3

$\mathbf{G}$	$p = 0$	$p > 0$
G_2, F_4, E_8	$c_n(\Gamma) \quad : \quad n^{\log n/\log\log n}$ $c_n^{\triangleleft}(\Gamma) \quad : \quad n$	$c_n(\Gamma) \quad : \quad n^{\log n} \ (*)$ $c_n^{\triangleleft}(\Gamma) \quad : \quad n$
$\pi(\mathbf{G}) \neq 1$, $p \nmid \lvert\pi(\mathbf{G})\rvert$	$c_n(\Gamma) \quad : \quad n^{\log n/\log\log n}$ $c_n^{\triangleleft}(\Gamma) \quad : \quad n^{\log n/(\log\log n)^2}$	$c_n(\Gamma) \quad : \quad n^{\log n} \ (*)$ $c_n^{\triangleleft}(\Gamma) \quad : \quad n^{\log n/(\log\log n)^2}$
$p \mid \lvert\pi(\mathbf{G})\rvert$	cannot occur	$c_n(\Gamma) \quad : \quad n^{\log n} \ (*)$ $c_n^{\triangleleft}(\Gamma) \quad : \quad n^{\log n}$

6.1 The characteristic 0 case

In this section we determine the strict congruence subgroup growth type of an S-arithmetic group over a number field k. In this case, $S \setminus V_\infty = S_0$ may be identified with a (finite) set of prime ideals of $\mathcal{O}$.

To simplify matters, we shall assume that $k = \mathbb{Q}$ and S_0 is a finite set of rational primes. (The general case can be reduced to this one by 'restriction of scalars'; see [PR], §2.1.2. This needs some care in case S is not the full set of primes lying over some set of rational primes.)

Thus $\Gamma = \mathbf{G}(\mathbb{Z}_S)$ where $\mathbf{G} \leq \mathrm{GL}_r$ is a connected, simply-connected, simple algebraic group defined over $\mathbb{Q}$, (so in fact $\mathbf{G} \leq \mathrm{SL}_r$). Let d denote the dimension of the algebraic group $\mathbf{G}$ (so $d \leq r^2 - 1$).

The notation $\mathbf{G}(\mathbb{Z}/m\mathbb{Z})$ means the group of $\mathbb{Z}/m\mathbb{Z}$-rational points of the algebraic group $\mathbf{G}$. For present purposes we may as well take it to mean the image of Γ in $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$, as long as m is coprime to S; this is justified by the Strong Approximation Theorem ($\looparrowright$ **Strong Approximation**) which ensures that Γ maps *onto* $\mathbf{G}(\mathbb{Z}_S/m\mathbb{Z}_S)$.

We begin by establishing the upper bound. The key to this is the following fact:

Proposition 6.1.1 ("level $\leq$ index") *Let H be a congruence subgroup of Γ. Then $H \geq \Gamma(m)$ for some $m \leq c \cdot |\Gamma : H|$, where $c > 0$ depends only on $\mathbf{G}$.*

Let us say that a subgroup H of $M = \mathbf{G}(\mathbb{Z}/m\mathbb{Z})$ is **essential** if H does not contain

$$M(r) = \ker(M \to \mathbf{G}(\mathbb{Z}/r\mathbb{Z}))$$

for any $r \mid m$ with $r < m$. The proposition is then clearly equivalent to

Proposition 6.1.2 *There exists a constant $C > 0$ such that for each $m \in \mathbb{Z}$, every essential subgroup H of $M = \mathbf{G}(\mathbb{Z}/m\mathbb{Z})$ satisfies $|M : H| \geq Cm$.*

For the proof, we need the following facts: for almost all primes p,

(i) $\mathbf{G}(\mathbb{Z}/p\mathbb{Z})$ is a perfect central extension of a product of finite simple groups of Lie type in characteristic p. It is generated by elements of order p. No non-abelian simple factor of $\mathbf{G}(\mathbb{Z}/p\mathbb{Z})$ is involved in $\mathbf{G}(\mathbb{Z}/q\mathbb{Z})$ for a prime $q \neq p$.

(ii) $K = \ker(\mathbf{G}(\mathbb{Z}_p) \to \mathbf{G}(\mathbb{Z}/p\mathbb{Z}))$ is a uniform pro-p group of dimension $\dim(\mathbf{G})$. The congruence subgroup modulo p^s is equal to $\Phi_{s-1}(K)$ where $\Phi_0(K) = K$ and $\Phi_{i+1}(K) = \Phi(\Phi_i(K))$ (the Frattini subgroup of $\Phi_i(K)$).

(iii) $\Phi(\mathbf{G}(\mathbb{Z}_p)) = K$.

(iv) For each $e \geq 1$ the group $\mathbf{G}(\mathbb{Z}/p^e\mathbb{Z}))$ is perfect.

For (i), see the **Finite simple groups** window; (ii) and (iii) are proved in the **Strong approximation** window. (iv) is a direct consequence of (i) and (iii).

We will argue as if (i) – (iv) hold for all primes, and show that $C = 1$ will do in that case. It is left for the reader to verify that one can compensate for the finitely many "bad" primes by making C smaller. Note that also for them, (ii) is 'essentially' correct: $\mathbf{G}(\mathbb{Z}_p)$ has an open uniform pro-p subgroup and the congruence sequence and the sequence $\Phi_i(K)$ are still "very close" to each other.

Note first that if p is a prime, then $\mathbf{G}(\mathbb{Z}/p\mathbb{Z})$ is generated by its Sylow p-subgroups and therefore every proper subgroup H of $\mathbf{G}(\mathbb{Z}/p\mathbb{Z})$ satisfies

$$|\mathbf{G}(\mathbb{Z}/p\mathbb{Z}) : H| \geq |P : P \cap H| \geq p$$

for some such Sylow subgroup P.

Now let $m = p_1^{e_1} \dots p_r^{e_r}$ where $p_1, \dots, p_r$ are distinct primes. Then

$$M = M_1 \times \cdots \times M_r$$

where

$$M_i = M(m/p_i^{e_i}) \cong \mathbf{G}(\mathbb{Z}/p_i^{e_i}\mathbb{Z}).$$

We claim that for each i, the projection $\pi_i(H)$ of H to $M(m/p_i)$ is a proper subgroup of $M(m/p_i)$. Indeed, suppose (w.l.o.g.) that $\pi_1(H) = M(m/p_1)$. Since $M(m/p_1)$ is the Frattini quotient of M_1 it follows that H projects onto M_1. Then H has all the non-abelian composition factors of $\mathbf{G}(\mathbb{Z}/p_1\mathbb{Z})$ as composition factors (with at least the same multiplicities), and as $H/(H \cap M_1)$ embeds into $M_2 \times \cdots \times M_r$ all these composition factors occur already inside $H \cap M_1$. But $H \cap M_1$ is a normal subgroup of M_1 (because H projects onto M_1); since M_1 is a perfect group it follows that $H \cap M_1 = M_1$. But this is impossible since H is supposed to be essential.

Therefore $|M_i : \pi_i(H)| \geq p_i$ for each i, and it follows that

$$|M : H| \geq \prod |M_i : \pi_i(H)| \geq \prod p_i.$$

If $e_i = 1$ for each i this concludes the proof.

Suppose now that $e_i > 1$ for some i, and put $m' = \prod_{i=1}^r p_i$, so that $m' < m$. Let H be an essential subgroup of $M = \mathbf{G}(\mathbb{Z}/m\mathbb{Z})$, and let H' denote the projection of H into $\mathbf{G}(\mathbb{Z}/m'\mathbb{Z}) = \prod_{i=1}^r \mathbf{G}(\mathbb{Z}/p_i\mathbb{Z})$. Then $\pi_i(H') = \pi_i(H)$ is a proper subgroup of $\mathbf{G}(\mathbb{Z}/p_i\mathbb{Z})$ for each i, so H' is an essential subgroup of $\mathbf{G}(\mathbb{Z}/m'\mathbb{Z})$. Thus the index of H' in $\mathbf{G}(\mathbb{Z}/m'\mathbb{Z})$ is at least m', and it suffices therefore to prove now that the index of $H \cap M(m')$ in $M(m')$ is at least $m/m' = \prod_{i=1}^r p_i^{e_i-1}$.

Now $M(m')$ is the direct product of the p_i-groups $L_i = \ker\left(\mathbf{G}(\mathbb{Z}/p_i^{e_i}\mathbb{Z}) \to \mathbf{G}(\mathbb{Z}/p_i\mathbb{Z})\right)$ and $H \cap M(m')$ is the product of the $H \cap L_i$. It will therefore suffice to show that $|L_i : H \cap L_i| \geq p_i^{e_i-1}$ for each i.

Fix i, put $p = p_i$, $e = e_i$, and $M = \mathbf{G}(\mathbb{Z}/p^e\mathbb{Z})$. Then $L_i = M(p)$, and $H \cap L_i = D$, say, does not contain $M(p^{e-1})$. We claim that then $DM(p^j)$ does not contain $M(p^{j-1})$ for $e > j > 1$. Indeed, since $M(p^j) = \Phi(M(p^{j-1}))$,

$$\begin{aligned} M(p^{j-1}) \leq DM(p^j) &\Longrightarrow M(p^{j-1}) = (D \cap M(p^{j-1}))\Phi(M(p^{j-1})) \\ &\Longrightarrow M(p^{j-1}) = D \cap M(p^{j-1}) \\ &\Longrightarrow D \geq M(p^{j-1}) \geq M(p^j), \end{aligned}$$

so our claim follows by reverse induction. It follows that

$$|M(p) : D| = \prod_{j=2}^{e} \left|DM(p^{j-1}) : DM(p^j)\right| \geq p^{e-1}.$$

Thus $|L_i : H \cap L_i| \geq p_i^{e_i-1}$ as required, and the proof is complete.

Corollary 6.1.3

$$c_n(\Gamma) \leq \sum_{m=1}^{cn} s_n\left(\mathbf{G}(\mathbb{Z}/m\mathbb{Z})\right).$$

Thus the problem is reduced to estimating the number of subgroups in certain finite groups. This depends on the following information:

Proposition 6.1.4 *Suppose that m is divisible by h distinct primes. Then for each prime q we have*

$$\mathrm{r}_q(\mathbf{G}(\mathbb{Z}/m\mathbb{Z})) < 3r^2h. \tag{6.1}$$

Proof. Since $\mathbf{G}$ is a subgroup of SL_r,

$$\begin{aligned} \mathrm{r}_q(\mathbf{G}(\mathbb{Z}/m\mathbb{Z})) &\leq \mathrm{r}_q(\mathrm{SL}_r(\mathbb{Z}/m\mathbb{Z})) \\ &\leq \sum_{p|m} \left(\mathrm{r}_q(\mathrm{SL}_r(\mathbb{F}_p)) + \mathrm{ur}_q(\mathrm{SL}_r^1(\mathbb{Z}_p))\right) \\ &\leq \sum_{p|m} \mathrm{r}_q(\mathrm{SL}_r(\mathbb{F}_p)) + (2r^2 - 2), \end{aligned}$$

where $\mathrm{SL}_r^1(\mathbb{Z}_p)$ is the kernel of $\mathrm{SL}_r(\mathbb{Z}_p) \to \mathrm{SL}_r(\mathbb{F}_p)$ which is a pro-p group of rank at most $2r^2-2$ (↬ **Pro-p groups**). The q-rank of $\mathrm{SL}_r(\mathbb{F}_p)$ is at most $r^2/2$ for each prime p (↬ **Finite group theory**). Thus (6.1) follows. ■

Of course, sharper bounds can be given, depending on the dimension d of $\mathbf{G}$. See the *Remark* below.

Proof of Theorem 6.1: the upper bound. Let $j \leq n$ and $m \leq n$. Suppose that $|\mathbf{G}(\mathbb{Z}/m\mathbb{Z})| = g$ is divisible by t distinct primes, and let $s = \max_p \mathrm{r}_p(\mathbf{G}(\mathbb{Z}/m\mathbb{Z}))$. Corollary 1.7.5 of Chapter 1 shows that

$$a_j(\mathbf{G}(\mathbb{Z}/m\mathbb{Z})) \leq j^{t+s}.$$

Say m is divisible by h distinct primes. Now there exists an absolute constant A such that

$$t \leq A \log g / \log\log g,$$
$$h \leq A \log m / \log\log m$$

(↬ **Prime Numbers**). From the preceding proposition we have $s < 3r^2h$, and $g \leq m^{r^2}$. It follows that $t + s \leq r^2(1+3A)\log m/\log\log m$. Thus

$$s_n(\mathbf{G}(\mathbb{Z}/m\mathbb{Z})) = \sum_{j=1}^{n} a_j\left(\mathbf{G}(\mathbb{Z}/m\mathbb{Z})\right) \leq \sum_{j=1}^{n} j^{t+s} \leq n^{B\log n/\log\log n}$$

where $B = 1 + r^2(1+3A)$.

With Corollary 6.1.3 this gives

$$c_n(\Gamma) \leq n^{b\log n/\log\log n},$$

where b depends only on B and c. This is the required upper bound.

(The argument can be simplified by quoting the fact that $\mathrm{SL}_r(\mathbb{F}_p)$ has rank at most $r^2/2+1$, together with the trivial estimate $s(G) \leq |G|^{\mathrm{rk}(G)}$; but the only known proof for this rank estimate depends on CFSG: see the **Finite simple groups** window.)

The lower bound for $c_n(\Gamma)$ given in Section 2 of Chapter 5 was of the form $n^{b\log n/(\log\log n)^2}$. We need to sharpen this to obtain a lower bound of the correct order. The group-theoretic part of the argument can remain much the same, but we must appeal now to some more powerful number theory. Let us recall the argument given in Chapter 5. Let x be a large real number, $\mathcal{P}(x)$ the set of primes p with $p \leq x$ and $m = \prod_{p\in\mathcal{P}(x)} p$. Then

$$\Gamma/\Gamma(m) \cong \mathbf{G}(\mathbb{Z}/m\mathbb{Z}) = \prod_{p\in\mathcal{P}(x)} \mathbf{G}(\mathbb{F}_p).$$

The latter is the direct product of $t = |\mathcal{P}(x)|$ finite quasi-simple groups, hence contains a subgroup isomorphic to $\mathbb{F}_2^{(t)}$. This gives at least $2^{[t^2/4]}$ congruence subgroups of index at most $|\mathbf{G}(\mathbb{Z}/m\mathbb{Z})| \sim m^d$ in Γ, and the Prime Number Theorem provides estimates for m and t which suffice to yield the stated lower bound. Now we present a slight variation on this argument. Let q be a prime of size approximately $x^{1/2}$, and put

$$\mathcal{P}(x,q) = \{p \leq x \mid p \equiv 1 \,(\mathrm{mod}\, q)\}$$

(p ranging over primes). Now take $m = \prod_{p\in\mathcal{P}(x,q)} p$. By Lang's theorem (↬ **Linear groups**), each $\mathbf{G}(\mathbb{F}_p)$ contains a cyclic subgroup of order $p-1$, and hence if $p \equiv 1 \,(\mathrm{mod}\, q)$ a cyclic subgroup of oder q. It follows that

$$\Gamma/\Gamma(m) \cong \prod_{p\in\mathcal{P}(x,q)} \mathbf{G}(\mathbb{F}_p)$$

contains a copy of $\mathbb{F}_q^{(t)}$ where $t = |\mathcal{P}(x,q)|$, and as above we infer that Γ has at least $q^{[t^2/4]}$ congruence subgroups of index at most $|\mathbf{G}(\mathbb{Z}/m\mathbb{Z})| \sim m^d$. Now Dirichlet's theorem on arithmetic progressions says that $|\mathcal{P}(x,q)|$ is approximately equal to $(q-1)^{-1} \cdot |\mathcal{P}(x)|$, and *assuming the Generalised Riemann Hypothesis* it can be shown that the resulting estimates for m and t are good enough to yield the stronger lower bound stated in Theorem 6.1.

We only have to get round the little difficulty that the number theorists have so far failed to prove the Riemann Hypothesis! Fortunately, Bombieri has proved that, in a suitable sense, the Riemann Hypothesis is 'true in the average'; that is, if one *averages* the error terms when estimating the number of primes along arithmetic progressions, then one indeed obtains the result predicted by the Riemann Hypothesis. This means that there does exist a prime q (though we may not know which one!) for which the argument given above will work.

We now proceed to spell out the proof, using some precise consequences of Bombieri's theorem that are explained in the **Primes** window. For a real number x, a *Bombieri prime* for x is a prime q such that

$$\left|\vartheta(y;q,1) - \frac{y}{\phi(q)}\right| \leq \frac{1}{\ln x} \cdot \frac{x}{\phi(q)}$$

for every $y \leq x$, where $\vartheta(y;q,1) = \sum_{p\in\mathcal{P}(y;q)} \ln p$. We fix $\rho \in (0, \frac{1}{2})$. Then for every sufficiently large x, there exists a Bombieri prime lying in the interval $(x^\rho/\ln x,\, x^\rho)$, and we make a fixed choice q_x of such a Bombieri prime. Moreover, writing

$$P_x = \prod_{p\in\mathcal{P}(x;q_x)} p,$$

we have

$$|\mathcal{P}(x;q_x)| = \frac{x}{\phi(q_x)\ln x}\,(1+o(1)) \geq \frac{x^{1-\rho}}{\ln x}\,(1+o(1)), \tag{6.2}$$

$$\ln P_x = \vartheta(x;q_x,1) = \frac{x}{\phi(q_x)}\,(1+o(1)) = x^{1-\rho}\,(1+o(1)), \tag{6.3}$$

where $o(1)$ stands for a number that tends to 0 as $x \to \infty$ (the second line follows directly from the definition of q_x).

Proof of Theorem 6.1: the lower bound. We fix $\sigma > 1$. It follows from (6.3) that for every sufficiently large integer n there exists x such that

$$(P_x)^d \le n \le (P_{\sigma x})^d,$$

and then, writing $\lambda = \log_2 \mathrm{e}$, we have

$$\frac{(\log n)^2}{\log\log n} < \frac{\lambda(\ln n)^2}{\ln\ln n} \le \frac{\lambda d^2 \sigma^{2-2\rho} x^{(2-2\rho)}}{(1-\rho)\ln x}\,(1+o(1))\,. \tag{6.4}$$

Now put $P = P_x$, $q = q_x$ and consider the congruence subgroup $\Gamma(P)$ of Γ. From the Strong Approximation Theorem for arithmetic groups (↬ **Strong Approximation**) it follows that

$$\Gamma/\Gamma(P) \cong \mathbf{G}(\mathbb{Z}/P\mathbb{Z}) \cong \prod_{p\in\mathcal{P}(x,q)} \mathbf{G}(\mathbb{F}_p).$$

We have shown above that Γ then has at least $q^{\lceil L^2/4\rceil}$ subgroups containing $\Gamma(P)$, where $L = |\mathcal{P}(x,q)|$. Each of these is a congruence subgroup of index at most

$$|\mathbf{G}(\mathbb{Z}/P\mathbb{Z})| = \prod_{p\in\mathcal{P}(x,q)} |\mathbf{G}(\mathbb{F}_p)| \le P^d$$

(↬ **Finite simple groups**).

As $P^d \le n$ it follows that $c_n(\Gamma) \ge q^{\lceil L^2/4\rceil}$, and using (6.2) and (6.4) we obtain

$$\begin{aligned}
\log c_n(\Gamma) &\ge \lambda\left\lceil L^2/4\right\rceil \ln q \\
&\ge \frac{\lambda}{4}\left(\frac{x^{1-\rho}}{\ln x}\right)^2 \cdot \rho \ln x \cdot (1+o(1)) \\
&\ge \frac{(\log n)^2}{\log\log n} \cdot \frac{\rho(1-\rho)}{\sigma^{(2-2\rho)} 4d^2} \cdot (1+o(1))\,.
\end{aligned}$$

Let a be any positive constant strictly smaller than $1/(16d^2)$. Choosing ρ very close to $\frac{1}{2}$ and σ very close to 1, we infer that

$$c_n(\Gamma) \ge 2^{a(\log n)^2/\log\log n} = n^{a\log n/\log\log n}$$

for all sufficiently large n, as claimed.

Remark. Better estimates can be obtained by arguing more carefully. The paper [Goldfeld, Lubotzky & Pyber] initiates the study of the constants appearing in the exponent. We will not describe this work in detail, but we will review it briefly.

Let $\mathbf{G}$ be a Chevalley group scheme, k a number field, $\mathcal{O}$ and S as before. Let $\Gamma = \mathbf{G}(\mathcal{O}_s)$ and

$$\alpha_+(\Gamma) = \limsup \frac{\log C_n(\Gamma)}{(\log n)^2/\log\log n}$$
$$\alpha_-(\Gamma) = \limsup \frac{\log C_n(\Gamma)}{(\log n)^2/\log\log n}.$$

[Goldfeld, Lubotzky & Pyber] conjecture that

(a) $\alpha_+(\Gamma) = \alpha_-(\Gamma)$.

(b) $\alpha_+(\Gamma)$ depends only on $\mathbf{G}$ and not on $\mathcal{O}$ (it is relatively easy to see that it does not depend on S).

(c) $\alpha_+(\Gamma) = \frac{(\sqrt{R(R+1)}-R)^2}{4R^2}$ where $R = R(\mathbf{G}) = \frac{\dim \mathbf{G} - \mathrm{rank}\mathbf{G}}{2\mathrm{rank}\mathbf{G}}$.

(Here rank$\mathbf{G}$ denotes the Lie rank of $\mathbf{G}$.) They prove all three conjectures for $\mathbf{G} = \mathrm{SL}_2$, and show that the expression given in (c) is at least a lower bound for $\alpha_-(\Gamma)$ in the general case.

The proof given above for the lower bound in Theorem 6.1 is a slight variation of that in [Goldfeld, Lubotzky & Pyber]. The more careful treatment there gives the optimal lower bound at least for SL_2. The generalization to other number fields is based on a corresponding extension of Bombieri's work. The proof of the upper bound (for SL_2) is based on a series of reductions, which shows that the dominant term of $c_n(\Gamma)$ comes from counting subgroups of $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ that lie between $B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ and $U = \begin{pmatrix} -1 & * \\ 0 & 1 \end{pmatrix}$. The problem is then reduced to one of counting subgroups in finite abelian groups.

6.2 The positive characteristic case

We turn now to the proof of Theorem 6.2. In this case when the characteristic is positive we have added two assumptions: (a) $\mathbf{G}$ is k-split and (b) If $p = 2$, $\mathbf{G}$ is not of type A_1 or C_l. While the first assumption is just a question of convenience, and it seems very likely that the theorem holds without it, the second assumption is essential for the proof. We are not sure whether the theorem holds without it: in any case, it will need a new idea. The crucial point in assumption (b) is to ensure that the associated Lie algebra is perfect. It should be stressed however that the two assumptions are only needed for the proof of the *upper bound*. The lower bound holds unconditionally.

So let's start with the lower bound whose proof is quite easy (and uses only the local completion).

Choose one valuation $\nu \notin S$. Then $\mathbf{G}(\widehat{\mathcal{O}_S})$ maps onto $K = \mathbf{G}(\mathcal{O}_\nu)$. We claim that K has subgroup growth of strict type at least $n^{\log n}$ (in fact it is

equal to $n^{\log n}$, by Theorem 4.4.3). Indeed, let $\mathfrak{m}_v$ be the maximal ideal of $\mathcal{O}_v$ and for each $i \geq 1$ put

$$K_i = \ker\left(\mathbf{G}(\mathcal{O}_v) \to \mathbf{G}(\mathcal{O}_v/\mathfrak{m}_v^i)\right).$$

For each $i \geq 1$ the quotient K_i/K_{i+1} is isomorphic to $(\mathcal{O}_v/\mathfrak{m}_v)^d$ ($\looparrowright$ **Strong approximation**, Corollary 6). One then verifies easily that

(i) $\log_p |K : K_i| \sim ci$ for some constant c,

(ii) $[K_i, K_i] \leq K_{2i}$ for each i,

(iii) $K_i^p \leq K_{pi}$ for each i.

This implies that K_i/K_{2i} is an elementary abelian p-group of rank approximately ci. Thus there are at least $p^{[c^2i^2/4]}$ subgroups between K_i and K_{2i}, all having index at most p^{2ci} in K, and the claim follows (essentially the same argument was used to obtain lower bounds in §§4.3 and 4.4).

To prove the upper bound we note first that as $\mathbf{G}$ is split and simple over k, it is absolutely simple. We write

$$M = \mathbf{G}(\widehat{\mathcal{O}_S})$$

and note that $c_n(\Gamma) = s_n(M)$.

Proposition 6.2.1 *There exists a constant c such that every open subgroup of index n in M contains a subnormal subgroup of M having index at most n^c in M.*

In other words, M satisfies the 'polynomial subnormal core condition'.

Proof. Every non-abelian upper composition factor of L is a quotient of $\mathbf{G}(\mathbb{F}_q)$ for some power q of p, hence is a simple group of Lie type and bounded Lie rank. Thus M lies in one the classes $\mathcal{B}_{c'}$ of groups satisfying the 'Babai-Cameron-Pálfy condition'. The proposition follows by Proposition 10 of the **Permutation groups** window . ■

Now given a subnormal subgroup of index at most n^c in M, the number of subgroups containing it is at most $n^{c\log(n^c)} = n^{c^2\log n}$, by Lemma 1.2.3. It will therefore suffice to show now that M has at most $n^{b\log n}$ *subnormal* subgroups of index n, for some constant b (a similar bound will then of course follow for those of index at most n).

Let us refresh our notations: Let $V = V_k \setminus S$ be the set of places of k outside S. For $v \in V$, let $\mathcal{O}_v$ be the completion of $\mathcal{O}_S$ with respect to v and let $\mathfrak{m}_v$ be the unique maximal ideal of $\mathcal{O}_v$. Thus $\mathcal{O}_v/\mathfrak{m}_v$ is a finite field of order $q^{e(v)}$, where q is the size of the maximal finite subfield of k.

Put

$$M_v = \mathbf{G}(\mathcal{O}_v)$$
$$K_v(i) = \ker\left(\mathbf{G}(\mathcal{O}_v) \to \mathbf{G}(\mathcal{O}_v/\mathfrak{m}_v^i)\right).$$

Then

$$M = \mathbf{G}(\widehat{\mathcal{O}}_S) = \prod_{v\in V} M_v.$$

Write

$$\pi_v : M \to M_v$$

for the natural projection map.

Because $\mathbf{G}$ is absolutely simple, each of the groups $M_v/K_v(1) \cong \mathbf{G}(\mathcal{O}_v/\mathfrak{m}_v)$ is a finite quasi-simple group. Let $W(M_v)$ be the 'weak-Frattini subgroup' of M_v, namely the intersection of the maximal open normal subgroups. Then $W(M_v)$ contains $K_v(1)$, and is in fact equal to the preimage Z_v in M_v of the centre $\mathrm{Z}\left(\mathbf{G}(\mathcal{O}_v/\mathfrak{m}_v)\right)$.

Now let H be a subnormal open subgroup of M. Then $H_v = H \cap M_v$ is a subnormal subgroup of M_v. As $M_v/W(M_v)$ is a simple group, it follows that *either* $H_v = M_v$ *or* $H_v \leq W(M_v)$. Thus putting

$$V_0(H) = \{v \in V \mid H \cap M_v \neq M_v\},$$

we have

$$\pi_v(H) \leq Z_v \text{ for every } v \in V_0(H).$$

This shows that H is contained in the group $\prod_{v\notin V_0(H)} M_v \times \prod_{v\in V_0(H)} Z_v$. Suppose $|M : H| = n$. Since the order of $|M_v/Z_v|$ is approximately $q^{e(v)d}$, where d is a constant (the dimension of $\mathbf{G}$), it follows that

$$n \geq \prod_{v\in V_0(H)} q^{e(v)d'} \tag{6.5}$$

(where d' is slightly less than d). Applying the characteristic-p Prime Number Theorem ($\rightsquigarrow$ **Primes**) we deduce that $V_0 = V_0(H)$ satisfies

$$|V_0| \leq \frac{A\log n}{\log\log n} \tag{6.6}$$

for some constant A.

Note next that the number of possibilities for the set $V_0(H)$ is bounded as a function of n. Indeed, if $v \in V_0(H)$, then $|\mathcal{O}_v/\mathfrak{m}_v| = q^{e(v)} \leq n^{1/d'}$, and another application of the Prime Number Theorem shows that the number of possibilities for v is $O\left(n/\log n\right)$. With the preceding result this shows that the number of possibilities for $V_0(H)$ is

$$O\left(\left(\frac{n}{\log n}\right)^{A\log n/\log\log n}\right) = o(n^{\log n}).$$

We may therefore fix a finite set V_0 of places and count subnormal subgroups H of index n in M for which $V_0(H) = V_0$. Each such H contains $\prod_{v \notin V_0} M_v$ and projects into $\prod_{v \in V_0} Z_v$, so this amounts to counting the subnormal subgroups of $\prod_{v \in V_0} Z_v$ that have index n in $\prod_{v \in V_0} M_v$.

Put

$$Y = \prod_{v \in V_0} Z_v \quad \text{and} \quad K = \prod_{v \in V_0} K_v(1).$$

Then K is a pro-p group and $Y/K \cong \prod_{v \in V_0} \mathrm{Z}\left(G(\mathcal{O}_v/\mathfrak{m}_v)\right)$ is a finite abelian p'-group, of rank at most $2\,|V_0|$ and exponent E, say, depending only on $\mathbf{G}$ (each of the direct factors is an image of the fundamental group $\pi(\mathbf{G})$ discussed in the introduction). It follows that

$$s_n(Y/K) \leq |Y/K|^{\mathrm{rk}(Y/K)} \leq E^{4|V_0|^2} = n^{o(\log n)},$$

in view of (6.6).

To each subnormal subgroup H of index $\leq n$ in Y we associate $H \cap K \leq K$ and $HK/K \leq Y/K$. Given $H \cap K = D$ and $HK = P$, let $N = \mathrm{N}_P(D)$; then $(N \cap K)/D$ is a p-group because D is open in the pro-p group K, while $N/(N \cap K)$ has order prime to p. Since H/D is a subnormal complement for $(N \cap K)/D$ in N/D it follows that $H/D = O^p(N/D)$. Thus H is uniquely determined by $H \cap K$ and HK, and so the number of possibilities for H is bounded above by

$$s_n(Y/K) \cdot s_n(K) = n^{o(\log n)} s_n(K).$$

We are thus left with the problem of bounding $s_n(K)$.

Say $V_0 = \{v_1, \ldots, v_t\}$. Write $e_j = e(v_j)$, so $\mathcal{O}_{v_j}/\mathfrak{m}_{v_j} \cong \mathbb{F}_{q^{e_j}}$, and put $K_j(i) = K_{v_j}(i)$ for $j = 1, \ldots, t$ and each $i \geq 1$. Now consider the graded $\mathbb{F}_p$-Lie algebra

$$\mathcal{L}_j = \bigoplus_{i=1}^{\infty} K_j(i)/K_j(i+1),$$

with Lie bracket induced on homogeneous elements by the group commutator in K_j. It is shown in [DDMS], Chapter 13 (we used the same construction in §4.4) that

$$\mathcal{L}_j \cong L_0 \otimes t\mathbb{F}_{q^{e_j}}[t]$$

where L_0 is the Lie algebra over $\mathbb{F}_p$ associated with $\mathbf{G}$; that is, given the (split) form of $\mathbf{G}$, its Lie algebra has the well known Chevalley basis and multiplication table with integral structure constants, and L_0 is the $\mathbb{F}_p$-Lie algebra with these structure constants reduced modulo p. It is not always the case that L_0 is a simple Lie algebra; even worse, if $p = 2$ and G is of type A_1 or C_l then L_0 is not even perfect. This is the reason we have excluded these cases (we won't need simplicity but we do require perfection).

Put $K(i) = \bigoplus_{j=1}^{t} K_j(i)$. To the group K with its filtration $(K(i))$ we associate the graded $\mathbb{F}_p$-Lie algebra

$$\begin{aligned}\mathcal{L} &= \bigoplus_{i=1}^{\infty} K(i)/K(i+1) \\ &= \bigoplus_{j=1}^{t} \mathcal{L}_j \cong \bigoplus_{j=1}^{t} L_0 \otimes t\mathbb{F}_{q^{e_j}}[t] \\ &\cong \left(\bigoplus_{j=1}^{t} L_0 \otimes \mathbb{F}_{q^{e_j}} \right) \otimes t\mathbb{F}_p[t] = L \otimes t\mathbb{F}_p[t]\end{aligned}$$

where $L = \bigoplus_{j=1}^{t} L_0 \otimes \mathbb{F}_{q^{e_j}}$.

To each closed subgroup H of K one associates the graded $\mathbb{F}_p$-Lie subalgebra

$$L(H) = \bigoplus_{i=1}^{\infty} (HK(i+1) \cap K(i))/K(i+1).$$

If $|K : H| = p^r$ then $\dim_{\mathbb{F}_p}(\mathcal{L}/L(H)) = r$. It is easy to see that the derived algebra $L(H)' = [L(H), L(H)]$ is contained in $L(H')$ where $H' = [H, H]$ is the (closed) derived group of H.

Now the heart of the proof is the following proposition, which will be proved in the next section:

Proposition 6.2.2 *Let $\mathcal{H}$ be a graded $\mathbb{F}_p$-Lie subalgebra of $\mathcal{L}$. Then*

$$\dim(\mathcal{L}/\mathcal{H}') \leq \dim L + 4 \dim L_0 \cdot \dim(\mathcal{L}/\mathcal{H})$$

(where all dimensions are over $\mathbb{F}_p$).

Using this we can now finish the proof of Theorem 6.2. Let H be an open subgroup of index p^r in K. By the above proposition and the preceding remarks we have

$$|K : H'| \leq p^{f(r)}$$

where $f(r) = \dim L + 4 \dim L_0 \cdot r$. It follows that $|H : H'| \leq p^{f(r)-r}$ and hence that

$$d(H) = \dim(H/H'H^p) \leq f(r) - r = h + (4d-1)r$$

where $h = \dim L$ and $d = \dim L_0$.

Now $d = \dim \mathbf{G}$, while

$$h = d \cdot \sum_{j=1}^{t} \log_p \left| \mathcal{O}_{v_j}/\mathfrak{m}_{v_j} \right| \leq (d/d') \log n$$

by (6.5). Thus $d(H) \leq c' \log n + cr$ where c' and c are constants.

In the notation of §1.6, we have established that $d_r(K) \leq c' \log n + cr$ for each r, and Proposition 1.6.2 now shows that for each m,

$$a_{p^m}(K) \leq p^{\sum_{r<m} d_r(K)} \leq p^{c' m \log n + O(m^2)}.$$

Since $m \leq \log n$ if $p^m \leq n$ it follows that

$$s_n(K) \leq p^{O((\log n)^2)} = n^{O(\log n)}.$$

This completes the proof, modulo Proposition 6.2.2.

6.3 Perfect Lie algebras

Let F be a field and L_0 a perfect Lie algebra of dimension d over F. Let $F_1, \ldots, F_t$ be finite field extensions of F, and put

$$L_j = L_0 \otimes F_j$$
$$L = \bigoplus_{j=1}^{t} L_j$$

(all tensor products over F). Thus L is a Lie algebra over F. For a subspace U of L, $\dim U$ denotes the F-dimension of U and $\operatorname{codim} U = \dim L - \dim U$. For subspaces U and V of L, we write

$$[U, V] = \langle [u, v] \mid u \in U,\, v \in V \rangle$$

where for any subset X, $\langle X \rangle$ denotes the F-subspace spanned by X.

Proposition 6.3.1 *Let U and V be F-subspaces of L. Then*

$$\operatorname{codim} [U, V] \leq d(\operatorname{codim} U + \operatorname{codim} V).$$

Before proving this, let us deduce Proposition 6.2.2. This concerns the graded Lie algebra

$$L \otimes t\mathbb{F}_p[t] = \mathcal{L}$$

and a graded $\mathbb{F}_p$-Lie subalgebra $\mathcal{H}$ of finite codimension in $\mathcal{L}$.

Say

$$\mathcal{H} = \bigoplus_{i=1}^{\infty} U_i \otimes t^i$$

where each U_i is a subspace of L. Then

$$[\mathcal{H}, \mathcal{H}] = \bigoplus_{i=2}^{\infty} \left(\sum_{n=1}^{i-1} [U_n, U_{i-n}] \right) \otimes t^i$$

and so

$$\begin{aligned}\dim(\mathcal{L}/[\mathcal{H},\mathcal{H}]) &= \dim L + \sum_{i=2}^{\infty} \operatorname{codim}\left(\sum_{n=1}^{i-1}[U_m,U_n]\right)\\ &\le \dim L + \sum_{n=1}^{\infty}(\operatorname{codim}[U_n,U_n] + \operatorname{codim}[U_n,U_{n+1}])\\ &\le \dim L + \sum_{n=1}^{\infty} d(3\operatorname{codim} U_n + \operatorname{codim} U_{n+1}) \qquad \text{by Proposition 6.3.1}\\ &\le \dim L + 4d\sum_{n=1}^{\infty}\operatorname{codim} U_n = \dim L + 4d\dim(\mathcal{L}/\mathcal{H}).\end{aligned}$$

This establishes Proposition 6.2.2.

Remark In fact the same result holds for an arbitrary $\mathbb{F}_p$-Lie subalgebra $\mathcal{H}$ of $\mathcal{L}$, graded or not. Taking U_n to be the subspace of *leading terms* of elements of degree n in $\mathcal{H}$, the reader can easily verify that the argument still works.

Now let us prove Proposition 6.3.1. Let K be the algebraic closure of F. Then for each j we have

$$L_j \otimes K = (L_0 \otimes F_j) \otimes K \cong L_0 \otimes (F_j \otimes K) \cong L_0 \otimes K^{(e_j)} \cong (L_0 \otimes K)^{(e_j)}$$

where $e_j = (F_j : F)$. So $L \otimes K \cong M^{(n)}$ where $M = L_0 \otimes K$ is a d-dimensional perfect Lie algebra over K, and $n = \sum e_j$. Since extending the base field preserves the dimensions of subspaces, Proposition 6.3.1 will therefore follow once we establish

Lemma 6.3.2 *Let K be an infinite field and $M_1, \dots, M_n$ perfect d-dimensional Lie algebras over K. Let U and V be subspaces of $L = M_1 \oplus \cdots \oplus M_n$. Then*

$$\operatorname{codim}[U,V] \le d(\operatorname{codim} U + \operatorname{codim} V).$$

Proof. Write $\pi_j : L \to M_j$ for the projection map and put $U_j = \pi_j(U)$. Let S_j be the set of d-tuples $\mathbf{x} \in U_j^{(d)}$ such that

$$\operatorname{codim}_{M_j}([x_1,M_j] + \cdots + [x_d,M_j]) \le d\operatorname{codim}_{M_j} U_j.$$

We claim that each S_j is non-empty. Indeed, if $U_j < M_j$ then $d\operatorname{codim}_{M_j} U_j \ge d$, while if $U_j = M_j$ then $\operatorname{codim}_{M_j}([x_1,M_j] + \ldots + [x_d,M_j]) = 0$ whenever $\{x_1,\dots,x_d\}$ is a basis for U_j.

Now S_j is a Zariski-open set in $U_j^{(d)}$ (its complement is defined by the vanishing of certain determinants whose entries are linear functions of the coordinates of $x_1,\dots,x_d$); therefore $\pi_j^{-1}(S_j)$ is a non-empty Zariski-open subset in U (writing π_j also for the projection $L^{(d)} \to M_j^{(d)}$). The intersection of finitely many

such sets is non-empty (because U is a vector space over an infinite field). Hence there exist $y_1, \dots, y_d \in U$ such that $\pi_j(y_1, \dots, y_d) \in S_j$ for every j.

Putting $\pi_j(y_i) = x_i^j$, we have

$$[y_1, L] + \cdots + [y_d, L] = \bigoplus_j \left([x_1^j, M_j] + \cdots + [x_d^j, M_j] \right);$$

the codimension of this subspace in $L = \bigoplus_j M_j$ is at most

$$d \sum_j \mathrm{codim}_{M_j} U_j \leq d\mathrm{codim} U.$$

Now let W be a complementary subspace to V in L. Then

$$\sum_{i=1}^{d} [y_i, L] = \sum_{i=1}^{d} [y_i, V] + \sum_{i=1}^{d} [y_i, W].$$

Since $\dim [y_i, W] \leq \dim W = \mathrm{codim} V$ for each i this implies that the codimension of $\sum [y_i, V]$ in $\sum [y_i, L]$ is at most $d\mathrm{codim} V$. The result follows since $\sum [y_i, V] \subseteq [U, V]$. ■

6.4 Normal congruence subgroups

We will start with sketching the proof of Theorem 6.4. We won't give a complete proof, sending the reader to [Larsen & Lubotzky] for details. Instead we describe a special case which illustrates the general method.

Let $\Delta = \mathrm{SL}_d(\mathbb{F}_p[[t]])$. For $r \in \mathbb{N}$ put

$$\Delta(r) = \ker \left(\mathrm{SL}_d(\mathbb{F}_p[[t]]) \to \mathrm{SL}_d(\mathbb{F}_p[[t]]/(t^r)) \right).$$

Then $\Delta/\Delta(1) \cong \mathrm{SL}_d(\mathbb{F}_p)$ and for every $i, j \geq 1, [\Delta(i), \Delta(j)] \subseteq \Delta(i+j)$ and $\Delta(i)^p \subseteq \Delta(pi)$. Thus for each $r \geq 1$, $\Delta(r)/\Delta(r+1)$ is an elementary abelian p-group of rank $d^2 - 1$, central in $\Delta(1)/\Delta(r+1)$. The action of $\Delta/\Delta(1)$ on $\Delta(r)/\Delta(r+1)$ is equivalent to the adjoint action of $\mathrm{SL}_d(\mathbb{F}_p)$ on its Lie algebra $\mathfrak{sl}_d(\mathbb{F}_p)$.

Now, if $p \nmid d$, then $\mathfrak{sl}_d(\mathbb{F}_p)$ is a simple $\mathrm{SL}_d(\mathbb{F}_p)$-module. Using this one can easily prove that for every proper open normal subgroup N of Δ, there exists $r \in \mathbb{N}$ such that $\Delta(r) \subseteq N \subseteq Z(r)$ where $Z(r)/\Delta(r) = \mathrm{Z}(\Delta/\Delta(r))$. So N is of index approximately $p^{(d^2-1)r}$. As $Z(r)/\Delta(r)$ has order bounded independently of r, it follows that for a given r there is only a bounded number of possibilities for such N. This implies that $s_n^{\triangleleft}(\Delta)$ is bounded above, as well as below, by constant multiples of $\log n$.

On the other hand, if $p \mid d$, then for $r \geq 1$ the group $\Delta/\Delta(pr)$ has a large centre: this consists of all the scalar matrices of the form $(1+y)I_d$ where $y \in (t^r)/(t^{pr})$. Note that $(1+y)^p = 1$ in the ring $\mathbb{F}_p[[t]]/(t^{pr})$, so $\det((1+y)I_d) = 1$. Now, $|(t^r)/(t^{pr})| = p^{(p-1)r}$ and so $\Delta/\Delta(pr)$ has a central elementary abelian

p-subgroup of rank $(p-1)r$. Hence Δ has at least $p^{[(p-1)^2r^2/4]}$ normal subgroups of index at most $|\Delta/\Delta(pr)| \sim p^{(d^2-1)pr}$. Therefore $s_n^{\triangleleft}(\Delta)$ grows at least as fast as $n^{\log n}$. As this is the fastest possible normal subgroup growth type (Corollary 2.8), it follows that the strict growth type of $s_n^{\triangleleft}(\Delta)$ is $n^{\log n}$.

Note that SL_d is of type A_{d-1} whose fundamental group is of order d, so $p \mid |\pi(\mathbf{G})|$ if and only if $p \mid d$ and we have proved Theorem 6.4 for the special case of $\Delta = \mathrm{SL}_d(\mathbb{F}_p[[t]])$. The general case is based on similar considerations but it is technically much more complicated. The groups of Ree type in particular need special consideration. Here $\Delta(r)/\Delta(r+1)$ is not a simple $\Delta/\Delta(1)$ module, which leaves room for more normal subgroups. In the positive characteristic case (in contrast to $G_2(\mathbb{Z}_3)$ and $F_4(\mathbb{Z}_2)$) there are indeed many more normal subgroups, though their number is still polynomially bounded. There are more cases for which the finite $\mathbb{F}_p$-Lie algebra is not a simple module for $\mathbf{G}(\mathbb{F}_p)$ – (see [Hogeweij 1982]), but in all of them $p \mid |\pi(\mathbf{G})|$ which already gives the maximal possible normal subgroup growth type $n^{\log n}$.

For later use we make another remark. There is another difference between the cases $p \mid d$ and $p \nmid d$. In the first case the centres of the finite quotients can be arbitrarily large, as we saw above for $\Delta = \mathrm{SL}_d(\mathbb{F}_p[[t]])$. In the second case, we have the following:

Proposition 6.4.1 *Let* $\mathbf{G}$ *be a simply connected, simple algebraic group over a local field* k *of characteristic* $p \geq 0$. *If* $p \nmid |\pi(\mathbf{G})|$ *then for every open compact subgroup* Δ_0 *of* $\mathbf{G}(k)$ *there exists a constant* $C = C(\Delta_0)$ *such that* $|\mathrm{Z}(Q)| < C$ *for every finite quotient* Q *of* Δ_0.

This is not difficult to check when $\Delta = \mathrm{SL}_d(\mathbb{F}_p[[t]])$, $p \nmid d$; for the general case see [Larsen & Lubotzky].

Before we turn to the proof of Theorem 6.3, we illustrate the main idea of the proof by treating the example

$$\Gamma = \mathrm{SL}_3(\mathbb{Z}).$$

If $p \equiv 1 \pmod 3$ then the centre of $\mathrm{SL}_3(\mathbb{F}_p)$, the group of scalar matrices, is a cyclic group of order 3. Now let x be a large real number and $p_1, \ldots, p_\ell$ the primes of size at most x with $p_i \equiv 1 \pmod 3$. By the Prime Number Theorem along arithmetic progressions (↬ **Primes**), $\ell \sim x/2\ln x$ and $\sum_{i=1}^{\ell} \ln p_i \sim x/2$. Let $m = \prod_{i=1}^{\ell} p_i$ so m is approximately $e^{x/2}$. The Strong Approximation theorem shows that $\mathrm{SL}_3(\mathbb{Z})$ maps onto $\mathrm{SL}_3(\mathbb{Z}/m\mathbb{Z}) \cong \prod_{i=1}^{\ell} \mathrm{SL}_3(\mathbb{F}_{p_i})$; this group has order at most m^9, while its centre is an elementary abelian 3-group of rank ℓ. It follows as usual that Γ has at least $3^{[\ell^2/4]}$ normal subgroups of index $\leq m^9$, and with the preceding estimates for ℓ and m this shows that the normal subgroup growth of Γ is of strict type at least $n^{\log n/(\log\log n)^2}$. It is also not difficult to prove an upper bound of the same type.

Note however that $\mathrm{SL}_3(\mathbb{Z})$ has trivial centre. Its Zariski closure $\mathrm{SL}_3(\mathbb{C})$ has a centre of order 3, but the argument would work equally well for $\mathrm{PSL}_3(\mathbb{Z})$ whose

Zariski closure $\mathrm{PSL}_3(\mathbb{C})$ has no centre. What really matters is the centre of the simply connected cover, i.e. the fundamental group of the adjoint group, which ensures that for sufficiently many primes p the centre of the mod p congruence quotient is non-trivial.

Now we sketch the proof of Theorem 6.3 in general. Recall that the congruence completion of $\Gamma = \mathbf{G}(\mathcal{O}_S)$ is

$$M = \mathbf{G}(\widehat{\mathcal{O}_S}) = \prod_{v \notin S} \mathbf{G}(\mathcal{O}_v),$$

and that $c_n^{\triangleleft}(\Gamma) = s_n^{\triangleleft}(M)$.

Let us start with part (iii). By Theorem 6.4.(i), already for one single $v \notin S$, the normal subgroup growth type of $\mathbf{G}(\mathcal{O}_v)$ is of type at least $n^{\log n}$, hence so is that of $s_n^{\triangleleft}(M)$. As this is the maximal possible, this establishes (iii).

Next, we consider the lower bounds in parts (i) and (ii).

For (i): $\mathcal{O}_S$ has at least cn ideals of index at most n, for some fixed $c > 0$ (depending on $\mathcal{O}_S$) and for all n sufficiently large. The principal congruence subgroup $\ker(\Gamma \to \mathbf{G}(\mathcal{O}_S/I))$ associated to an ideal I of index $\leq n$ is normal, and has index at most n^d for some constant d. This shows that the growth type of $c_n^{\triangleleft}(\Gamma)$ is at least n.

For (ii): Note first that we are in the case where $p \nmid |\pi(\mathbf{G})|$. Recall that $\pi(\mathbf{G})$ in this case is isomorphic to the centre of $\mathbf{G}(\overline{k})$, where $\overline{k}$ denotes the separable closure of k, as $\mathbf{G}$ is simply connected. There exists a finite Galois extension k' of k such that $\mathbf{G}(k')$ contains $\mathrm{Z}(\mathbf{G}(\overline{k}))$. Let $\mathcal{P}_1$ be the set of primes in k that split completely in k' and $\mathcal{P} = \mathcal{P}_1 \setminus S$. By the Chebotarev density theorem ($\rightsquigarrow$ **Primes**) the set $\mathcal{P}_1$ has positive density, and as S is finite so does $\mathcal{P}$. For a large real number x, let $\mathcal{P}_x$ be the set of all primes in $\mathcal{P}$ of norm at most x. By the Prime Number Theorem and the positive density of $\mathcal{P}$, each of the functions

$$\frac{\pi(x)}{x/\ln x} \quad \text{and} \quad \frac{\psi(x)}{x}$$

is bounded away from both zero and infinity, where

$$\pi(x) = |\mathcal{P}_x|, \;\; \psi(x) = \sum_{P \in \mathcal{P}_x} \ln |P|$$

and $|P|$ denotes the norm of P (i.e. the index $|\mathcal{O} : P|$).

Put $J(x) = \prod_{P \in \mathcal{P}_x} P$ and let $M(J(x))$ denote the principal congruence subgroup modulo $J(x)$. Now $|\mathcal{O}_S/J(x)| = \prod_{P \in \mathcal{P}_x} |P| = e^{\psi(x)}$. It follows that $M/M(J(x)) \cong \prod_{P \in \mathcal{P}_x} \mathbf{G}(\mathcal{O}_S/P)$ is of order approximately C_1^{dx} where C_1 is some constant and $d = \dim \mathbf{G}$. Now fix a (rational) prime q dividing $|\pi(\mathbf{G})|$. For each $P \in \mathcal{P}_x$, the group $\mathbf{G}(\mathcal{O}_S/P)$ contains a central element of order q. Thus $\prod_{P \in \mathcal{P}_x} \mathbf{G}(\mathcal{O}_S/P)$ has a central elementary abelian q-subgroup of rank $|\mathcal{P}_x|$. It

follows that $M/M(J(x))$ has at least $q^{[\pi(x)^2/4]}$ central subgroups and hence that M has at least

$$q^{[\pi(x)^2/4]} \geq q^{\frac{1}{4C^2}\cdot\frac{x^2}{(\ln x)^2}}$$

normal subgroups of index at most C_1^{dx}. This proves that the normal subgroup growth of M is of type at least $n^{\log n/(\log\log n)^2}$ as claimed.

We turn finally to the proof of the upper bounds.

Let $\mathcal{P}$ be the set of all primes of k which are not in S. Let $\mathcal{P}_1$ be the set of all primes $v \in \mathcal{P}$ such that:

(a) $\mathbf{G}(\mathbb{F}_v)$ is a quasi-simple group, where $\mathbb{F}_v = \mathcal{O}_v/m_v$ and $\mathbf{G}(\mathbb{F}_v)$ is the image of $\mathbf{G}(\mathcal{O}_v)$ in $\mathrm{GL}_r(\mathbb{F}_v)$;

(b) if $Q_v(i) = \ker(\mathbf{G}(\mathcal{O}_v) \to \mathbf{G}(\mathcal{O}_v/m_v^i))$, then

$$[Q_v(1), Q_v(i)] = Q_v(i+1)$$

for every $i \geq 1$;

(c) the elementary abelian p-group $Q_v(1)/Q_v(2)$ is a simple $\mathbf{G}(\mathbb{F}_v)$-module, and

(d) If $p = 0$, the rational prime below v does not divide $|\pi(\mathbf{G})|$.

Now, unless $\mathbf{G}$ is of Ree type (i.e., $p = 2$ and $\mathbf{G}$ of type F_4 or $p = 3$ and $\mathbf{G}$ of type G_2), the set $\mathcal{P}_1$ contains almost all primes in $\mathcal{P}$. This is well known when $\mathbf{G}$ splits, but also holds in general (the reader is referred to [Larsen & Lubotzky] for details and references).

We will leave aside the two exceptional cases when $\mathbf{G}$ is of Ree type. Consider $S_1 = S \cup \{v \mid v \notin \mathcal{P}_1\}$ and $H_1 = \mathbf{G}(\widehat{\mathcal{O}_{S_1}}) = \prod_{v\in\mathcal{P}_1} \mathbf{G}(\mathcal{O}_v)$. One proves by induction, using properties (a), (b) and (c), that for each open normal subgroup N of H_1, there exists an ideal I of $\mathcal{O}_{S_1}$ such that $Q(I) \subseteq N \subset Z(I)$ where

$$Q(I) = \ker \mathbf{G}(\widehat{\mathcal{O}_{S_1}}) \to \mathbf{G}(\widehat{\mathcal{O}_{S_1}}/\overline{I})$$

and $Z(I)$ is the preimage in H_1 of the centre of $\mathbf{G}(\widehat{\mathcal{O}_{S_1}}/\overline{I})$ (here $\overline{I}$ denotes the closure of I in $\widehat{\mathcal{O}_{S_1}}$). It now follows, by a similar computation to the one carried out above for the lower bound, that the normal subgroup growth type of H_1 is n in case (i) and $n^{\log n/(\log\log n)^2}$ in case (ii).

Now $M = H_1 \times H_2$ where $H_2 = \prod_{v\notin\mathcal{P}_1\cup S} \mathbf{G}(\mathcal{O}_v)$. The latter is a product of finitely many groups, each of them having at most polynomial normal subgroup growth . We claim:

(A) The normal subgroup growth of H_2 is at most polynomial.

(B) The normal subgroup growth of M is at most polynomial in case (i) and at most $n^{\log n/(\log\log n)^2}$ in case (ii).

Claim (B) completes the proof of Theorem 6.3, except for groups of Ree type. For these cases the proof is similar but more care is needed as the modules in condition (c) are not simple. The reader is referred to [Larsen & Lubotzky] for details.

Applying Proposition 1.3.6 of Chapter 1 to a group extension of the form $A \lhd A \times B$ we obtain

Lemma 6.4.2 *Let $H = A \times B$ be a product of two groups. Then*

$$s_n^{\lhd}(H) \leq s_n^{\lhd}(B)^2 s_n^{\lhd}(A) z_n(A)^{\delta_n(A)}$$

where

$$z_n(A) = \max\{|\mathrm{Z}(A/D)| \,\big|\, D \lhd A \text{ and } |A:D| \leq n\},$$
$$\delta_n(A) = \max\{d(\mathrm{Z}(A/D)) \big| N \lhd A \text{ and } |A:D| \leq n\}.$$

To prove Claim (A), we combine this with Theorem 6.4 and Proposition 6.4.1.

Now for Claim (B).

Case (i): the only open normal subgroups of H_1 in this case are the principal congruence subgroups, and the finite quotients have no centre. It follows therefore that

$$s_n^{\lhd}(M) = s_n^{\lhd}(H_1 \times H_2) \leq s_n^{\lhd}(H_1) s_n^{\lhd}(H_2)^2,$$

and so it is polynomially bounded.

Case (ii): We observed above that the normal subgroups of H_1 lie between $Q(I)$ and $Z(I)$ for some $I \lhd \mathcal{O}_{S_1}$. Now if I is an ideal of index n^s which is a product of m prime powers then the Prime Number Theorem implies that $m \leq c \log n / \log\log n$, where c is a constant. So the abelian group $Z(I)/Q(I)$ has order at most $z^{C \log n / \log\log n}$, where $z = |\pi(\mathbf{G})|$, and its rank is at most $C' \log n / \log\log n$. Thus in the notation of Lemma 6.4.2, $z_n(H_1) \leq z^{C \log n / \log\log n}$ and $\delta_n(H_1) \leq C' \log n / \log\log n$, while $s_n^{\lhd}(H_1) \leq z^{CC'(\log n / \log\log n)^2}$. It follows that

$$s_n^{\lhd}(H) \leq s_n^{\lhd}(H_2)^2 \cdot z^{2CC'(\log n / \log\log n)^2},$$

and the claim follows by (A) (since z is constant).

Notes

Theorem 6.1 is from [**Lubotzky 1995**$_a$], but the proof of the lower bound given there relies on a version of the Prime Number Theorem along arithmetic progressions which is known only modulo the Generalized Riemann Hypothesis. This gap was subsequently filled in [**Goldfeld, Lubotzky & Pyber**], where it is shown that by a different choices of the parameters one can appeal to a theorem of Linnik and make the proof unconditional. We have preferred, however, to use Bombieri's result (also following [**Goldfeld, Lubotzky & Pyber**]) as that

result (a) enables to present the proof in a cleaner way and (b) gives a better constant (in fact the same constant one would get using the GRH). There is, though, one disavantage to this approach: the prime chosen in the proof, though its existence is assured by Bombieri, is not explictly specified, and hence nor is the set of arithmetic subgroups presented to demonstrate the lower bound. To this extent the proof is non-constructive.

Proposition 6.1.1, comparing level and index, is due to [**Lubotzky 1995**$_a$]. It has a long history, going back to Galois for the case of $\mathrm{SL}_2(\mathbb{Z})$ and prime level; see [Jones 1986] for further references.

The lower bound in Theorem 6.2 is from [**Lubotzky 1995**$_a$], where a weaker upper bound ($n^{(\log n)^2}$) was also established. The sharp upper bound in Theorem 6.2, and the material on Lie algebras in Section 6.3, are due to **Nikolay Nikolov** (unpublished); the short proof of Lemma 6.3.2 given here was suggested by **M. Abért** and **B. Szegedy**.

[**Abért, Nikolov & Szegedy**] establish a stronger version of Proposition 6.2.2, showing that

$$\dim(\mathcal{L}/\mathcal{H}') \leq \dim L + 7\dim(\mathcal{L}/\mathcal{H}).$$

(The proof only applies to the Lie algebras arising, as above, from split simple algebraic groups.) This implies that the number of *subnormal* congruence subgroups of index at most n in Γ is bounded above by $n^{b\log n}$ where the constant b is *independent of the group* $\mathbf{G}$; whether the same can be said for the number of all congruence subgroups of index at most n is at present unclear, because the constant c in Proposition 6.2.1 does depend on the Lie rank of $\mathbf{G}$.

The results on normal subgroups are all from [**Larsen & Lubotzky**].

Chapter 7

The generalized congruence subgroup problem

We keep the notation of the preceding chapter, restricting attention now to an *algebraic number field* k, with ring of integers $\mathcal{O} = \mathcal{O}_k$. The set of all primes (equivalence classes of valuations) of k is denoted V_k, the finite subset of 'infinite primes' (non-archimedean valuations) is V_∞, and $V_k \setminus V_\infty = V_f$; so V_f may be identified with the set of non-zero prime ideals of $\mathcal{O}$. For each $v \in V_k$ the v-completion of k is denoted k_v.

Throughout, S will denote a finite subset of V_k containing V_∞. The ring of *S-integers* is

$$\mathcal{O}_S = \{x \in k \mid v(x) \geq 0 \text{ for all } v \notin S\}.$$

Let $\mathbf{G}$ be a connected, simply-connected, simple, algebraic group defined over k with a fixed embedding $\mathbf{G} \hookrightarrow \mathrm{GL}_r$. We assume throughout that

- $\mathbf{G}(k_v)$ *is non-compact for* every $v \in S \setminus V_\infty$
- $\mathbf{G}(k_v)$ *is non-compact for* at least one $v \in S$.

In the preceding chapter we determined the *congruence subgroup growth* of the S-arithmetic group

$$\Gamma = \mathbf{G}(\mathcal{O}_S);$$

it is of type $n^{\log n/\log\log n}$. What about its subgroup growth? Obviously this will be the same if every subgroup of finite index is a congruence subgroup, and it is easy to see that it will still be the same if the following slightly weaker condition holds: *the natural map*

$$\widehat{\Gamma} \to \mathbf{G}(\widehat{\mathcal{O}_S})$$

has finite kernel (it is an epimorphism, by the Strong Approximation Theorem). In this case Γ is said to have the *congruence subgroup property* (CSP). We remark that if $\mathbf{G}(k_v)$ were compact for some $v \in S \setminus V_\infty$, then the CSP would fail for

formal reasons (because in that case, $\mathbf{G}(\mathcal{O}_S)$ is commensurable with $\mathbf{G}(\mathcal{O}_{S'})$ where $S' = S \setminus \{v\}$); so our global hypothesis that $\mathbf{G}(k_v)$ be non-compact for each finite $v \in S$ is no real loss of generality. (If $\mathbf{G}(k_v)$ were compact for *every* $v \in S$ then Γ, being a discrete subgroup of $\prod_{v\in S} \mathbf{G}(k_v)$, would be a finite group.)

The first main result shows that if Γ does *not* have CSP then its subgroup growth is significantly faster. In Section 1 we prove

Theorem 7.1 *Let $\Gamma = \mathbf{G}(\mathcal{O}_S)$ be as above and assume that $\mathbf{G}(k)$ has the* 'standard description of normal subgroups'. *Then Γ has the congruence subgroup property if and only if Γ has subgroup growth of type strictly less than $n^{\log n}$; that is, if and only if*

$$s_n(\Gamma) = O(n^{\varepsilon \log n})$$

for every $\varepsilon > 0$.

The extra hypothesis imposed on $\mathbf{G}$ is explained in §7.1; it is conjectured to hold in all cases, and known to hold in almost all cases.

The theorem shows that when Γ fails to have the congruence subgroup property, *most* of its finite-index subgroups are not congruence subgroups: for infinitely many integers n, Γ has at least $n^{c_1 \log n}$ subgroups of index $\leq n$, but no more than $n^{c_2 \log n/\log\log n}$ of these are congruence subgroups (where c_1 and c_2 are positive constants). We actually believe (and many known examples support this) that when the congruence subgroup property fails the subgroup growth is in fact much faster than $n^{\log n}$ (probably super-exponential).

It follows from the theorem, but is easy to see anyway, that if Γ has the CSP then no subgroup of finite index in Γ can have a non-abelian free quotient. It is less obvious but also true that in fact no subgroup of finite index can have an infinite cyclic quotient; as Γ is finitely generated this is equivalent to saying that *if Γ has the CSP then every finite-index subgroup of Γ has finite abelianisation.* The proof of this is sketched in §7.1 below.

The interest of Theorem 7.1 is that it provides a characterisation of the *arithmetically-defined* congruence subgroup property in purely *group-theoretic* terms (for further results of this nature, see Chapter 12). An important application is that it enables one to formulate the 'congruence subgroup problem' without referring to the arithmetic structure of Γ; this is of particular interest for *lattices in semisimple Lie groups*. The classical congruence subgroup problem concerns S-arithmetic groups as above. Such an S-arithmetic group is a *lattice* (a discrete subgroup of finite covolume) in a suitable semisimple group. Here by *semisimple group* we mean a product $H = \prod_{i=1}^{r} \mathbf{G}_i(K_i)$ where each K_i is a local field and $\mathbf{G}_i$ is a simple algebraic group defined over K_i. A famous theorem of Margulis shows that in many cases, *every* lattice in H is S-arithmetic. On the other hand, when $r = 1$ and $\mathbf{G}_1$ has K_1-rank equal to 1, it is possible (sometimes) that H also has *non-arithmetic* lattices. (The *K_i-rank* of $\mathbf{G}_i$ is the

maximal dimension of a K_i-split torus in $\mathbf{G}_i$). Using Theorem 7.1 as a guide, it makes sense to formulate the

Generalized congruence subgroup problem Let Γ be a lattice in a semisimple group over local fields of characteristic 0. Is the subgroup growth type of Γ strictly less than $n^{\log n}$? In this case we say that Γ has the *generalized congruence subgroup property.*

Serre's conjecture, which is largely proved by now, asserts, loosely speaking, that an S-arithmetic lattice in a semi-simple group H has the congruence subgroup property if and only if the rank of H is at least 2 (see §7.1 for a precise formulation). In particular, the conjecture implies that the validity of the congruence subgroup property for (arithmetic) lattices Γ in H depends only on H and not on Γ. This is compatible with other known properties of lattices. Extending this philosophy to arbitrary lattices in H, it is natural to conjecture that *non-arithmetic lattices never have the generalized congruence subgroup property* (these only exist in groups of rank one, by Margulis's theorem mentioned above).

In Section 2 we summarize what is known about the subgroup growth of lattices in rank-1 groups. This is not sufficient to establish the 'generalized conjecture', but all the results support it. Taken together they amount to

Theorem 7.2 *Let $H = \mathbf{G}(K)$ where K is a local field of characteristic 0 and $\mathbf{G}$ is a simple, connected algebraic group defined over K with K-rank 1. Let Γ be a lattice in H. Then Γ does not have the generalized congruence subgroup property in each of the following cases:*

(1) *if K is non-archimedean;*

(2) *if $K = \mathbb{R}$ and one of the following holds:*

(2a) *H is locally isomorphic to $\mathrm{SO}(2,1)$ or $\mathrm{SO}(3,1)$;*

(2b) *H is locally isomorphic to $\mathrm{SO}(m,1), m \geq 4$, and either Γ is arithmetic and $m \neq 7$ or Γ is one of the (currently) known non-arithmetic lattices;*

(2c) *$H = \mathrm{SU}(m,1)$ and Γ is an arithmetic lattice of* 'simple type'*, or $H = \mathrm{SU}(2,1)$ and Γ is one of several non-arithmetic lattices constructed by Livne.*

In most cases, one actually proves that Γ *has a subgroup of finite index that has a non-abelian free quotient*; this implies (by Corollary 2.2) that Γ has subgroup growth of strict type n^n. It seems likely that this always holds for such lattices, the only doubtful cases in the above list being $\mathrm{SO}(3,1)$, some arithmetic lattices (of 'complex type') in $\mathrm{SO}(m,1)$, m odd, and the arithmetic lattices of simple type in $\mathrm{SU}(m,1)$.

When K is a local field of *positive* characteristic, *uniform* lattices in rank-one groups are virtually free, while the non-uniform ones are not even finitely generated, and have *uncountably many* subgroups of finite index.

The arguments in §7.2 are topological and geometric. The debt to geometry is repaid by the following application, discussed in the final section:

Theorem 7.3 *For $n \geq 4$ and $r > 0$ let $\rho_n(r)$ denote the number of isomorphism classes of n-dimensional hyperbolic manifolds of volume at most r. Then there exist positive constants $a = a(n)$ and $b = b(n)$ such that*

$$r^{ar} \leq \rho_n(r) \leq r^{br}$$

for all sufficiently large r.

7.1 The congruence subgroup problem

In many cases, for example if $\mathbf{G}$ splits over k, it is known that $\mathbf{G}(k) = G$ is a *projectively simple* group, i.e. $G/\mathrm{Z}(G)$ is simple. This is not the case in general. For example, let $\mathcal{H}$ be the Hamiltonian quaternion algebra and $\mathbf{G} = \mathcal{H}^1$ the group of quaternions of norm 1. It is well known that if p is an odd prime then $\mathcal{H}$ splits in $\mathbb{Q}_p$ and hence $\mathbf{G}(\mathbb{Q}_p) \cong \mathrm{SL}_2(\mathbb{Q}_p)$, but $\mathcal{H}$ does not split in $\mathbb{Q}_2$ and $\mathbf{G}(\mathbb{Q}_2)$ is a compact, indeed profinite, group. As $\mathbf{G}(\mathbb{Q}_2)$ contains $\mathbf{G}(\mathbb{Q})$ this group is also residually finite, hence has many normal subgroups of finite index.

The *Platonov-Margulis conjecture* asserts that essentially all normal subgroups of $\mathbf{G}(k)$ are obtained this way. More formally, let

$$T = \{v \in V_f \mid \mathbf{G}(k_v) \text{ is compact}\}.$$

It is known that T is a finite set, and our standing assumption is that

$$T \cap S = \emptyset.$$

Let $\delta : \mathbf{G}(k) \to \mathbf{G}_T = \prod_{v \in T} \mathbf{G}(k_v)$ be the diagonal embedding of $\mathbf{G}(k)$ into the profinite group $\mathbf{G}_T = \prod_{v \in T} \mathbf{G}(k_v)$.

Platonov-Margulis Conjecture For every non-central normal subgroup N of $G = \mathbf{G}(k)$ there exists an open normal subgroup $\widetilde{N}$ of $\mathbf{G}_T$ such that $N = \delta^{-1}(\widetilde{N})$. In this case one says that G *has the standard description of normal subgroups*.

The Platonov-Margulis conjecture has been proved in almost full generality (see [PR], Chapter 9 and [Segev 1999]). Margulis has also proved that in any case, every non-central normal subgroup of $G = \mathbf{G}(k)$ has finite index. We will **assume throughout the section** that G **has the standard description of normal subgroups**. Note that if T is empty, as is the case for example if $\mathbf{G}$ splits or even quasi-splits, this implies that G is projectively simple.

The standing assumption that $\mathbf{G}_S = \prod_{v \in S} \mathbf{G}(k_v)$ is non-compact, which is equivalent to

$$\mathrm{rank}_S \mathbf{G} = \sum_{v \in S} \mathrm{rank}_{k_v}(\mathbf{G}) \geq 1,$$

implies that the S-arithmetic group $\Gamma = \mathbf{G}(\mathcal{O}_S)$ is *infinite*; in this case Γ is a lattice (i.e. a discrete subgroup of finite covolume) in $\mathbf{G}_S$.

The *congruence subgroup problem* concerns the family of all finite-index subgroups of Γ. As every non-zero ideal of $\mathcal{O}_S$ has finite index, the principal congruence subgroups $\Gamma(J)$, and hence all congruence subgroups of Γ, have finite index. The classical congruence subgroup problem asks whether these are *all* the subgroups of finite index in Γ.

A modern reformulation is due to Serre. Consider $G = \mathbf{G}(k)$ as a topological group with two topologies. The *arithmetic topology* is defined by taking as a base of neighbourhoods of the identity the family of all finite-index subgroups of Γ. The *S-congruence topology* is defined similarly by taking just the *congruence subgroups* of Γ. Let $\widehat{G}$ (resp. $\widetilde{G}$) be the completion of G with respect to the arithmetic (resp: S-congruence) topology. Note that $\widehat{G}$ is *not* the profinite completion of G, which may have no proper subgroups of finite index; but the closure $\widehat{\Gamma}$ of Γ in $\widehat{G}$ is indeed the profinite completion of Γ. By the strong approximation theorem for $\mathbf{G}$ ($\nrightarrow$ **Strong Approximation**), $\mathbf{G}(k)$ is dense in $\mathbf{G}(\mathbb{A}_S)$, where $\mathbb{A}_S$ is the ring of S-adeles of k; then $\widetilde{G}$ is isomorphic to $\mathbf{G}(\mathbb{A}_S)$ and the closure $\widetilde{\Gamma}$ of Γ in $\widetilde{G}$ is isomorphic to $\mathbf{G}(\widehat{\mathcal{O}}_S)$; this is the *congruence completion* of Γ.

The arithmetic topology is stronger than the S-congruence topology and hence the identity map on G extends to an epimorphism $\pi : \widehat{G} \to \widetilde{G}$. We put

$$C = C(\mathbf{G}, S) = \ker \pi.$$

It follows from the definitions that $C \leq \widehat{\Gamma}$, and we have the exact sequence

$$1 \to C \to \widehat{\Gamma} \to \widetilde{\Gamma} \to 1.$$

If indeed every finite-index subgroup of Γ is a congruence subgroup, then the two topologies are the same and π is an isomorphism, so $C = 1$. Otherwise C is non-trivial. In any case, C is a profinite group.

Proposition 7.1.1 *One of the following holds:*
(a) $C(\mathbf{G}, S)$ *is finite and central, or*
(b) $C(\mathbf{G}, S)$ *is not finitely generated as a topological group.*

In view of this strong dichotomy, and since for most applications (e.g. superrigidity – see [Bass, Milnor & Serre 1967]) the finiteness of $\ker \pi$ suffices, we make the following

Definition $\Gamma = G(\mathcal{O}_S)$ is said to have the *congruence subgroup property* (CSP) if $C(\mathbf{G}, S)$ is finite (and hence central).

Warning: some authors call this the "weak congruence subgroup property", keeping "congruence subgroup property" to its original meaning, i.e. $\ker \pi = 1$.

If Γ has CSP then it has subgroup growth of strict type $n^{\log n / \log \log n}$, by Theorem 6.1 and Proposition 1.11.2. So to complete the proof of Theorem 7.1 it remains to establish

Proposition 7.1.2 *If $\Gamma = G(\mathcal{O}_S)$ does not have CSP then Γ has subgroup growth of type at least $n^{\log n}$.*

This will occupy the rest of this section. We shall assume for simplicity that in fact T is empty, so that G *is projectively simple*; for the general case see [Lubotzky 1995_a].

We begin by sketching the proof of Proposition 7.1.1. Suppose that (b) does not hold, i.e. that C is finitely generated as a profinite group. The infinite simple group $G/\mathrm{Z}(G)$ acts on C via conjugation in $\widehat{G}$, and the action cannot be faithful because the group of (continuous) automorphisms of C is residually finite (indeed a profinite group; see for example [DDMS], §5.3). Hence the action is trivial, which means that C is centralized by G, and hence central in $\widehat{G}$ as G is dense.

Before proceeding we remark that the same argument shows the following (whether or not C is finitely generated):

(♮) If M is an open subgroup of C which is invariant under conjugation by G (or equivalently normal in $\widehat{G}$) then $[C, \widehat{G}] \leq M$.

In the present case, we see that $\widehat{G}$ is a central extension of the adelic group $\widetilde{G} \cong \mathbf{G}(\mathbb{A}_S)$. This implies that C is a quotient of the 'metaplectic kernel' $M(\mathbf{G}, S)$, which is always a finite group: see [PR], §9.5, [Prasad & Raghunathan 1983]. Thus (a) holds.

The next step is the following result, which was essentially proved in [Rapinchuk 1990] and called 'Rapinchuk's Lemma' in [Lubotzky 1995_a]:

Proposition 7.1.3 *If Γ does not have the congruence subgroup property, then there exist the following: a subgroup Γ_0 of finite index in Γ, a profinite group E containing Γ_0 as a dense subgroup, and an exact sequence of profinite groups*

$$1 \to W \to E \to H \to 1, \qquad (*)$$

where
◇ *W is the Cartesian product of infinitely many copies of a fixed non-trivial finite simple group F, and*
◇ *H is an open subgroup of the congruence completion $\widetilde{\Gamma}$ of Γ.*
Furthermore, if F is abelian then
◇ *H can instead be taken to be a pro-p group of finite rank, for some prime p.*

Proof. (Sketch) Let $K = \overline{[C, G]}$ denote the closure of $[C, G]$ in $\widehat{G}$. Then $1 \to C/K \to \widehat{G}/K \to \widetilde{G} \to 1$ is a central extension of $\widetilde{G}$, since G is dense in $\widehat{G}$. It follows from the 'Metaplectic Theorem' mentioned above that C/K is finite. So K is open in C and normal in $\widehat{G}$. Let M be a maximal proper open normal subgroup of K, so $K/M = F$ is a non-trivial finite simple group. Now $N = \bigcap_{g \in G} M^g$ is a closed normal subgroup in $\widehat{G}$. If N has finite index in C, then by (♮) we have $M \geq N \geq [C, \widehat{G}] = K$, a contradiction; N therefore has infinite index in K. Moreover K/N is a subcartesian product of copies of F (a subgroup of $\prod_{g \in G} K/M^g$ which maps onto each factor). As F is a finite simple

group, it follows that K/N is isomorphic to an infinite Cartesian product of copies of F (actually the number of factors is countable because $G = \mathbf{G}(k)$ is a countable group).

We now have the exact sequence

$$1 \to C/N \to \widehat{G}/N \to \widetilde{G} \to 1,$$

and as $C \leq \widehat{\Gamma} \leq \widehat{G}$ this induces an exact sequence

$$1 \to C/N \to \widehat{\Gamma}/N \to \widetilde{\Gamma} \to 1.$$

Replacing Γ with a suitable finite index subgroup Γ_0 which satisfies $\widehat{\Gamma_0} \cap C = K$, we get

$$1 \to K/N \to \widehat{\Gamma_0}/N \to \overline{\Gamma_0} \to 1$$

where $\overline{\Gamma_0}$ is the closure of Γ_0 in $\widetilde{G} = \mathbf{G}(\widehat{\mathcal{O}}_S)$. So the main part of the proposition is proved with $E = \widehat{\Gamma_0}/N$ and $W = K/N \cong F^{\aleph_0}$.

When F is abelian, one can take H to be a suitable open subgroup of $\widetilde{\Gamma} \cap \mathbf{G}(k_v)$, for some $v \in V \setminus S$. The latter is virtually a pro-p group for the rational prime p lying under v, so its sufficiently small open subgroups are pro-p groups. For details of the proof see [Lubotzky 1995a], (5.3). ■

We can now complete the proof of Proposition 7.1.2. Suppose that Γ does not have the congruence subgroup property. We have to show that the subgroup growth type of Γ is at least $n^{\log n}$. Now let E be the profinite group given in Proposition 7.1.3. Since the profinite completion of Γ_0 maps onto E, it will suffices to prove that the subgroup growth of E is at least that fast. Given what we know about E, the argument now follows a pattern familiar from Sections 3 and 4 of Chapter 5.

Case 1. Where the finite simple group F is non-abelian. Now the upper composition factors of E are either congruence images of $\mathbf{G}(\mathcal{O}_S)$ or else isomorphic to F; consequently every finite quotient of E belongs to the class $\mathcal{B}_c$ of groups satisfying the 'Babai-Cameron-Pálfy condition', relative to some bound c (↬ **Permutation groups**). We now apply

Lemma 7.1.4 *Let Q be a finite group belonging to the class $\mathcal{B}_c$, and suppose that Q has a normal subgroup N isomorphic to $F^{(m)}$ for some non-abelian simple group F. Let $n = |Q : \mathrm{C}_Q(N)|$. Then*

$$s_n(Q) \geq n^{A \log n}$$

where $A > 0$ depends only on c and F.

This is proved below. Now let K be any open normal subgroup of E. Then $KW/K \cong F^{(m)}$ for some m, and applying the lemma to $Q = E/K$ we deduce that $s_n(E) \geq n^{A \log n}$ where $n = |E : \mathrm{C}_E(KW/K)|$. Since $F^{(m)}$ has trivial

centre, it is clear that $n \geq |KW/K| = |K : K \cap W|$; as W is infinite, n takes arbitrarily large values as K ranges over all the open normal subgroups of E, and it follows that the subgroup growth type of E is at least $n^{\log n}$.

Proof of lemma 7.1.4 Replacing Q by $Q/\mathrm{C}_Q(N)$ we may assume that Q acts faithfully by conjugation on N, and $n = |Q|$. Now Q permutes the m simple factors of N, with kernel K, say. Then K is isomorphic to a subgroup of $\mathrm{Aut}(F)^{(m)}$, so $|K| \leq |F|^{2m}$ because F can be generated by 2 elements ($\looparrowright$ **Finite simple groups**). Also Q/K is isomorphic to a subgroup of $\mathrm{Sym}(m)$, and Theorem 8 of the **Permutation groups** window implies that $|Q/K| \leq b^m$ for some b depending only on c. Thus $n \leq b^m |F|^{2m}$ and $\log n \leq mB$ where $B = b|F|^2$.

On the other hand, N contains an elementary abelian subgroup of order p^m for some prime $p \mid |F|$ (of course we can take $p = 2$, by the Odd Order theorem); hence Q has at least $p^{\lceil m^2/4 \rceil}$ subgroups. Then

$$\begin{aligned} \log s_n(Q) = \log s(Q) &\geq \lceil m^2/4 \rceil \\ &\geq A(\log n)^2 \end{aligned}$$

where $A = (8B)^{-1}$, say. The lemma follows.

Case 2. Where F is abelian. In this case W is an infinite elementary abelian q-group for some prime q, and we have the exact sequence $(*)$ in which H is now a pro-p group.

If $p = q$ then E is a pro-p group of infinite rank, hence E has subgroup growth type at least $n^{\log n}$, by Theorem 4.2.

We are left with the case where $p \neq q$. Let K be any open normal subgroup of E and put $Y = \mathrm{C}_E(KW/K)$. Then $KW/K \cong \mathbb{F}_q^m$ for some m, and E/Y is a finite p-group acting faithfully on KW/K. It follows that $|E/Y| \leq (2q)^m \leq q^{2m}$ ($\looparrowright$ **Finite group theory).** Now Y/KW is also a p-group, so Y/K is nilpotent and therefore equals $KW/K \times D/K$ for some open normal subgroup D of E. Then $Y/D \cong \mathbb{F}_q^m$ contains at least $q^{\lceil m^2/4 \rceil}$ subgroups, each of which corresponds to an open subgroup of index at most $|E : D| \leq q^{3m}$ in E. Hence for $n = q^{3m}$ we have

$$\begin{aligned} \log s_n(E) &\geq \lceil m^2/4 \rceil \log q \\ &\geq A(\log n)^2 \end{aligned}$$

where $A = (72 \log q)^{-1}$, say. As above, the fact that W is infinite implies that n takes arbitrarily large values, and again we conclude that the subgroup growth type of E is at least $n^{\log n}$. This completes the proof of Proposition 7.1.2, and with it the proof of Theorem 7.1.

Remark. A *sufficient* condition for $C(\mathbf{G}, S) = C$ to be infinite is that Γ possess an infinite virtually abelian quotient. Indeed, if this holds and C is finite then $\widetilde{\Gamma} = \widehat{\Gamma}/C$ also has such a quotient. Since $\widetilde{\Gamma} \cong \prod_{\mathfrak{p} \notin S} \mathbf{G}(\mathcal{O}_\mathfrak{p})$ it follows that $\mathbf{G}(\mathcal{O}_\mathfrak{p})$ has a non-trivial abelian qotient for infinitely many $\mathfrak{p}$; this contradicts the fact that $\mathbf{G}(\mathcal{O}_\mathfrak{p})$ is a perfect group for almost all $\mathfrak{p}$ (see §6.1).

7.2 Subgroup growth of lattices

By a *semisimple group* we mean a product $H = \prod_{i=1}^{r} \mathbf{G}_i(K_i)$ where for each i, K_i is a local field and $\mathbf{G}_i$ is a connected simple algebraic group over K_i. The *rank* of H is defined to be

$$\mathrm{rank}(H) = \sum_{i=1}^{r} \mathrm{rank}_{K_i}(\mathbf{G}_i)$$

where $\mathrm{rank}_K(\mathbf{G})$ denotes the maximal dimension of a K-split torus in $\mathbf{G}$. We assume throughout that **none of the $\mathbf{G}_i(K_i)$ is compact** (this is equivalent to $\mathrm{rank}_{K_i}(\mathbf{G}_i) \geq 1$ for each i).

A discrete subgroup Γ of a locally compact topological group H is called a *lattice* if H/Γ carries a finite H-invariant measure. Γ is *uniform* (or cocompact) if H/Γ is compact, and *non-uniform* otherwise. A lattice Γ in H is called *irreducible* if no finite index subgroup of Γ can be represented in the form of a direct product of two infinite groups.

Irreducible lattices in a semisimple group H are always finitely generated except when $r = 1$, K_1 is a local field of positive characteristic, and Γ is a *non-uniform* lattice in $H = G_1(K_1)$. For this, and other facts about lattices, see the book [M] of Margulis.

The S-arithmetic groups discussed above provide important examples of irreducible lattices. Let k be a global field, $S \supseteq V_\infty$ a finite subset of V_k, and $\mathbf{G}$ an absolutely almost simple algebraic group defined over k. Then $\Gamma = \mathbf{G}(\mathcal{O}_S)$ is an irreducible lattice of $G = \prod_{v \in S} \mathbf{G}(k_v)$, via the diagonal embedding. This is a well known result of Borel and Harish-Chandra (in the characteristic 0 case) and Behr and Harder (in the positive characteristic case).

Now let H be a semisimple group and Γ an irreducible lattice of H. Then Γ is called *arithmetic* if there exist $k, \mathbf{G}$ and S as above and a continuous epimorphism $\varphi : G = \prod_{v \in S} \mathbf{G}(k_v) \to H$, with compact kernel, such that $\varphi(\mathbf{G}(\mathcal{O}_S))$ is commensurable to Γ.

The celebrated theorem of Margulis is

Theorem 7.2.1 *If* $\mathrm{rank}(H) \geq 2$ *then every irreducible lattice in* H *is arithmetic.*

Our main focus in this section is the subgroup growth of lattices in semisimple groups. For *arithmetic* lattices there is the

Conjecture [Serre 1972] Let $\mathbf{G}$ be a simple simply connected algebraic group over a global field k, satisfying our non-compactness assumptions w.r.t. the set S. Then $\Gamma = \mathbf{G}(\mathcal{O}_S)$ has the congruence subgroup property if and only if $\mathrm{rank}_S \mathbf{G} \geq 2$.

Recall that

$$\mathrm{rank}_S \mathbf{G} = \mathrm{rank}(G) = \sum_{v \in S} \mathrm{rank}_{k_v}(\mathbf{G}(k_v)).$$

Now, the affirmative part of Serre's conjecture (i.e. that Γ has the congruence subgroup property if $\mathrm{rank}_S(\mathbf{G}) \geq 2$) has been proved in many cases (see [PR] §9.5 and [Rapinchuk 1997]). In these cases Theorems 6.1 and 6.2 give the subgroup growth of Γ. We should mention that the assumptions of simple connectedness and non-compactness of $\mathbf{G}(k_v)$ for $v \in S \setminus V_\infty$ are not really essential as regards the subgroup growth of Γ (for the first, Γ may be replaced by a suitable covering group with finite kernel, and for the second by a suitable subgroup of finite index).

For groups of S-rank 1 the situation is less clear. Note also that Margulis's Theorem allows for the existence of non-arithmetic lattices.

Before going further, let us call the attention of the reader to the fact that Serre's conjecture on the congruence subgroup problem implies in particular that the answer to this problem for an arithmetic group $\mathbf{G}(\mathcal{O}_S)$ does not depend on the arithmetic group, but rather on the ambient semisimple group in which it sits as a lattice (and actually only on its rank). We have seen in Theorem 7.1 that the congruence subgroup property is eventually a question of the subgroup growth type of the arithmetic group. Putting this together, we would expect that all lattices $\mathrm{SO}(n,1)$ and $\mathrm{SU}(n,1)$ should fail to have the generalized CSP, as we know that some of them do; as these are the simple real Lie groups that have non-arithmetic lattices, we should therefore expect that the generalized CSP fails for every non-arithmetic lattice. This would be so if the following conjecture is verified:

Conjecture Let H be a semisimple group and Γ_1, Γ_2 two irreducible lattices in H. Then the subgroup growth type of Γ_1 is the same as the subgroup growth type of Γ_2, unless one of them is not finitely generated.

(Recall that H can contain a non-finitely generated lattice only if it is a rank-1 group over a local field of positive characteristic.)

We should mention however that the conjecture is not true for more general topological groups H. For example, some arithmetic groups are also lattices in $H = \mathrm{Aut}(X_{p+1}) \times \mathrm{Aut}(X_{q+1})$, where p and q are primes and X_r denotes the r-regular tree, while [Burger & Mozes 2000] have constructed lattices in H which are simple groups and so have *no* proper subgroups of finite index.

If indeed Serre's conjecture is valid and arithmetic lattices in higher rank semisimple groups do have the congruence subgroup property, then combining this with Margulis's arithmeticity result and using Theorem 6.1, one can see that our conjecture holds at least in the case of higher-rank groups. Thus its main new content concerns rank one groups, where non-arithmetic lattices are possible. Let us see what can be said in this case.

We shall say that a group Γ is of *VF type* if Γ contains a normal subgroup Γ_0 of finite index such that Γ_0 has a non-abelian free quotient.

Case 1: Non-archimedean fields

Theorem 7.2.2 *Let K be a* non-archimedean *local field and $H = \mathbf{G}(K)$ a simple group of K-rank* 1*. Let Γ be a lattice in H.*

(i) If Γ is uniform then Γ is virtually free.

(ii) If Γ is non-uniform then Γ is not finitely generated, and there exists n such that Γ has uncountably many subgroups of index n.

Case (ii) only occurs when $\mathrm{char}(K)$ is positive (see e.g. [Tits 1979]).

Proof. (See [Sr] Chapter II, §§1.7, 2.6). To each simple K-group H is associated a *Bruhat-Tits building*: this is an aspherical building X of dimension equal to $\mathrm{rank}(H)$, on which H acts so that $H \setminus X$ is a finite complex. In our case X is a tree. If Γ is cocompact then $\Gamma \setminus X$ is a finite graph, and Γ is the fundamental group of a finite graph of finite groups. Hence it is finitely generated and virtually free.

If Γ is a non-uniform lattice, then it is a "non-uniform tree lattice" in the terminology of [Bass & Lubotzky 2001], and hence not finitely generated. Moreover from the structure theorem proved in [Lubotzky 1991] it follows that Γ has a subgroup of finite index m with an infinite elementary abelian p-quotient, where $p = \mathrm{char}(K)$. Evidently Γ then has uncountably many subgroups of index mp. ■

Case 2: $K = \mathbb{C}$

Here there is (up to local isomorphism) just one rank-one group.

Proposition 7.2.3 *Let Γ be a lattice in $\mathrm{SL}_2(\mathbb{C})$. Then Γ has subgroup growth of type at least $n^{(\log n)^{2-\varepsilon}}$ for every $\varepsilon > 0$.*

We will deduce this from Theorem 4.6.4: this says that if P is a finitely presented pro-p group having subgroup growth of type at most $n^{(\log n)^{2-\varepsilon}}$ for some $\varepsilon > 0$, then every minimal pro-p presentation of P must satisfy the *Golod-Shafarevich inequality*. Suppose we can show that Γ has a subgroup Δ of finite index such that (some minimal presentation of) $P = \widehat{\Delta}_p$ does *not* satisfy the Golod-Shafarevich inequality: that is, P has a pro-p presentation on $d(P)$ generators and r relations where $r < d(P)^2/4$. We may then conclude that the subgroup growth type of P is at least $n^{(\log n)^{2-\varepsilon}}$ for every $\varepsilon > 0$, and hence that the same holds for Δ and for Γ.

We may assume that Γ is torsion-free. Now Γ is not a virtually soluble group because it is Zariski-dense in $\mathrm{SL}_2(\mathbb{C})$ ([Ra], Cor. 5.16). It follows that Γ has infinite upper p-rank for every prime p, by Corollary 18 in the **Strong approximation** window; in fact we only need the fact that Γ has upper p-rank at least 5 for one prime p. In any case this means that some subgroup Δ of finite index in Γ satisfies

$$d(\widehat{\Delta}_p) \geq 5.$$

We now appeal to the following result due to [Epstein 1961]:

Proposition 7.2.4 *If Δ is a torsion-free lattice in $\mathrm{SL}_2(\mathbb{C})$ then Δ has a finite presentation $\langle X; R\rangle$ such that $|R| \leq |X|$.*

We sketch the proof for the case where Δ is uniform, i.e. $\Delta \setminus \mathrm{SL}_2(\mathbb{C})$ is compact. Let $\mathcal{H} = \mathrm{SL}_2(\mathbb{C})/SU(2)$ denote the 3-dimensional hyperbolic space. Then $M = \Delta \setminus \mathcal{H}$ is a 3-dimensional hyperbolic manifold, compact by our hypopthesis, and $\Delta \cong \pi_1(M)$. Take a cell decomposition for M with C_i i-cells, $i = 0, 1, 2, 3$, where $C_3 = 1$. A presentation for $\pi_1(M)$ can be obtained from this decomposition: the generators correspond to edges outside a maximal subtree and the relations are given by the 2-cells. This gives $C_1 - (C_0 - 1)$ generators and C_2 relations, so we only need to show that

$$C_1 - C_0 + 1 - C_2 \geq 0.$$

But $C_1 - C_0 + 1 - C_2$ is equal to the Euler characteristic of M, which is equal to 0 by Poincaré duality.

The proof for the non-uniform case is similar. In fact [Epstein 1961] proves more precisely that the *deficiency* of Δ, namely the maximum of $|X| - |R|$ over all finite presentations $\langle X; R\rangle$ of Δ, is equal to 0 if Δ is uniform and equal to 1 otherwise.

The same presentation $\langle X; R\rangle$ may be taken as a pro-p presentation for the pro-p completion $P = \widehat{\Delta}_p$ of Δ ($\rightsquigarrow$ **Profinite groups**). It is shown in the **Pro-p groups** window that P then has a pro-p presentation $\langle Y; S\rangle$ such that

$$\begin{aligned} |Y| &= d(P) \\ |S| &= |R| - (|X| - |Y|). \end{aligned}$$

Since $|X| \geq |R|$ and $d(P) \geq 5$ this gives

$$|S| \leq |Y| < |Y|^2/4.$$

Thus we have a minimal presentation for P that violates the Golod-Shafarevich inequality, and the proof is complete.

Proposition 7.2.3 shows that, as expected, lattices in $\mathrm{SL}_2(\mathbb{C})$ don't have the generalized CSP. However it gives only a rather weak lower bound for the subgroup growth. In many cases (probably all in fact), the growth is much faster. In particular, the following are known:

(i) *Every non-uniform lattice in $\mathrm{SL}_2(\mathbb{C})$ is of VF type* [Cooper, Long & Reed 1997], [Grunewald & Noskov].

(ii) *Let Γ be a torsion-free uniform lattice in $\mathrm{SL}_2(\mathbb{C})$ such that $\Gamma/[\Gamma, \Gamma]$ is finite. Then there exists $\alpha > 0$ such that $s_n(\Gamma) \geq 2^{n^\alpha}$ for infinitely many values of n* [Reznikov & Moree 1997].

Since $\mathrm{SL}_2(\mathbb{C})$ is locally isomorphic to $\mathrm{SO}(3,1)$, some of the examples discussed in the next subsection provide further instances of (uniform) lattices in $\mathrm{SL}_2(\mathbb{C})$ that are of VF type. It is not known however if *every* uniform lattice in $\mathrm{SL}_2(\mathbb{C})$ has this property. A well-known conjecture of Thurston asserts that every lattice in $\mathrm{SL}_2(\mathbb{C})$ has a subgroup of finite index that maps onto $\mathbb{Z}$ (or in geometric formulation: *every compact hyperbolic 3-manifold has a finite-sheeted cover with positive first Betti number*). But at present this conjecture is wide open.

Case 3: $K = \mathbb{R}$

We turn finally to the most interesting case, where H is a real rank-one group. It is known that H is locally isomorphic to one of the following: $\mathrm{SO}(m,1)$ $(m \geq 2)$, $\mathrm{SU}(m,1)$ $(m \geq 2)$, $\mathrm{Sp}(m,1)$ $(m \geq 2)$ or $F_4^{(-20)}$.

Now $\mathrm{SO}(2,1)$ is locally isomorphic to $\mathrm{SL}_2(\mathbb{R})$ and $\mathrm{SO}(3,1)$ is locally isomorphic to $\mathrm{SL}_2(\mathbb{C})$. The second case has been dealt with above, and the first is easy:

Proposition 7.2.5 *Every lattice in* $\mathrm{SL}_2(\mathbb{R})$ *is of VF type .*

Proof. Let Γ be a lattice in $\mathrm{SL}_2(\mathbb{R})$. Replacing Γ by a subgroup of finite index, we may suppose that Γ is torsion-free. Then identifying the upper half-plane $\mathcal{H}$ with $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2)$, we find that Γ is isomorphic to the fundamental group $\pi_1(M)$, where $M = \Gamma\backslash\mathcal{H}$ is a Riemann surface of genus $g \geq 2$ with r puncture points say. Now $\pi_1(M)$ has a presentation

$$\left\langle a_1, b_1, \ldots, a_g, b_g, c_1, \ldots, c_r \,;\, \prod_{i=1}^{g} [a_i, b_i] \prod_{j=1}^{r} c_j = 1 \right\rangle .$$

If M is compact, then $r = 0$ and $\pi_1(M)$ maps onto the free group on g generators: add the relations $a_i = b_i, i = 1, \ldots, g$. (Note that $g \geq 2$ because the the torus of genus 1 is not covered by $\mathcal{H}$.) If M is not compact then $r \geq 1$ and $\pi_1(M)$ is free on the $2g + r - 1$ generators $a_1, b_1, \ldots, a_g, b_g, c_1, \ldots, c_{r-1}$. ■

Next we consider the groups $\mathrm{SO}(m,1)$ where $m \geq 3$. First the *arithmetic lattices:* except when $m = 3$ or $m = 7$, these are of two kinds:

I The lattices of *simple type*: Let k be a totally real number field with ring of integers $\mathcal{O}$, and $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_r$ the $r = (k : \mathbb{Q})$ distinct embeddings of k into $\mathbb{R}$. Let f be a diagonal quadratic form in $m + 1$ variables over k, say $f = \sum_{i=1}^{m+1} a_i x_i^2$. Assume that f is of type $(m, 1)$ while f^{σ_i} is positive definite (i.e. of type $(m + 1, 0)$) for $i = 2, \ldots, r$, (where $f^{\sigma_j} = \sum_{i=1}^{m+1} \sigma_j(a_i) x_i^2$). Then $\mathrm{SO}(f, \mathcal{O})$ is a lattice in $\prod_{i=1}^{r} \mathrm{SO}(f^{\sigma_i}, \mathbb{R})$. As the last $r-1$ factors are compact (isomorphic to $\mathrm{SO}(m+1)$), the projection of $\mathrm{SO}(f, \mathcal{O})$ into the first factor $\mathrm{SO}(f, \mathbb{R}) \cong \mathrm{SO}(m, 1)$ is an arithmetic lattice there.

II The lattices of *complex type* (which exist only if m is odd). Let k be a totally real number field, D a quaternion algebra over k with the involution σ given by $\sigma(x) = tr(x) - x$ $(x \in D)$. Let $m = 2d-1, V$ a d-dimensional D-vector space and $h : V \times V \to D$ a a non-degenerate skew-Hermitian form (so that for $\lambda, \mu \in D$ and $v, w \in V$, $h(\lambda v, \mu w) = \sigma(\lambda)h(v, w)\mu$.) Let $\mathbf{G} = \mathrm{SU}(h)$ be the special unitary group of this form h. Assume that h was chosen in such a way that $\mathbf{G}(k \otimes \mathbb{R}) \cong \mathrm{SU}(m, 1) \times C$ where C is a compact group. If $\mathcal{O}$ is the ring of integers of k, then the projection Γ of $G(\mathcal{O})$ to $SU(m, 1)$ is an arithmetic lattice (see [Vinberg & Shvartsman 1993] or [Li & Millson 1993] for details).

Proposition 7.2.6 *Every arithmetic lattice of simple type in* $\mathrm{SO}(m, 1)$ $(m \geq 3)$ *is of VF type .*

Proposition 7.2.7 *If* Γ *is an arithmetic lattice of complex type in* $\mathrm{SO}(m, 1)$ $(m \geq 3)$ *then* Γ *does not have the congruence subgroup property.*

Proposition 7.2.7 is the accumulation of the work of several authors; see [Lubotzky 1996_a)] for a unified approach. As the proof does not give any new information on the subgroup growth we won't go into the details here; the main point of the proof is to show the existence of some congruence subgroup of Γ with an infinite abelianization. It is well known that this suffices to contradict the congruence subgroup property.

On the other hand we will prove Proposition 7.2.6, as the method will also be used again below. The proof depends on the following observation:

Lemma 7.2.8 *Let* Γ *be group and assume that one of the following holds:*

(i) $\Gamma = A_1 \underset{B}{*} A_2$, *a free product with amalgamation, or*

(ii) $\Gamma = A_{*B}$, *an* HNN*-extension of* A *over a subgroup* B.

Suppose that there exists an epimorphism $\pi : \Gamma \to C$ *of* Γ *onto a finite group* C *such that*

- *in case* (i) $\pi(B)$ *is a proper subgroup of both* $\pi(A_1)$ *and* $\pi(A_2)$ *and has index at least* 3 *in one of them,*
- *in case* (ii) $\pi(B)$ *is a proper subgroup of* $\pi(A)$.

Then Γ *has a subgroup of finite index that maps onto a non-abelian free group.*

This is a consequence of the universal properties of amalgamated free products and HNN extensions, and the fact that the groups $\pi(A_1) \underset{\pi(B)}{*} \pi(A_2)$ and $\pi(A)_{*\pi(B)}$ are virtually free when the constituents are finite groups and their relative indices satisfy the given inequalities (see for example [Sr] Chapter II, §2.6).

If B is closed in the profinite topology of Γ, then the epimorphisms from Γ onto finite groups separate the cosets of B, and we may infer

Corollary 7.2.9 *Let Γ be as in Lemma 7.2.8. Assume that B is closed in the profinite topology of Γ and that $(|A_1 : B| - 1)(|A_2 : B| - 1) > 1$ in case (i) or $|A : B| > 1$ in case (ii). Then Γ has a subgroup of finite index that maps onto a non-abelian free group.*

We now apply this to prove Proposition 7.2.6. We may choose an ideal J of $\mathcal{O}$ so that the congruence subgroup $\Gamma(J)$ is contained in the identity component $\mathrm{SO}_0(m,1)$ of $\mathrm{SO}(m,1)$, see [Millson 1976]. Write $\Gamma_m = \Gamma(J)$. As explained in Millson's paper, there is a reflection τ through the hyperplane $x_1 = 0$ which normalizes Γ_m. Let Γ_{m-1} be the centralizer of τ in Γ_m; then Γ_{m-1} is the principal congruence subgroup modulo J in the subgroup of $\mathrm{SO}(m-1,1)$ that preserves the restriction of f to the hyperplane $x_1 = 0$, and Γ_{m-1} is a lattice in $\mathrm{SO}_0(m-1,1)$. Moreover, $Y_{m-1} = \Gamma_{m-1} \backslash \mathrm{SO}_0(m-1,1)/\mathrm{SO}(m-1)$ is an embedded totally geodesic hypersurface of the manifold $Y_m = \Gamma_m \backslash \mathrm{SO}_0(m,1)/\mathrm{SO}(m)$. This implies that $\Gamma_m = \pi_1(Y_m)$ is equal to either $A_1 \underset{B}{*} A_2$ or A_{*B}, where $B = \Gamma_{m-1}$ and A_1 and A_2 (or A) are subgroups of Γ_m: the first case occurs if Y_{m-1} separates Y_m, the second case otherwise. In either case, $B = \Gamma_{m-1}$, being a congruence subgroup of a Zariski-closed subgroup of Γ_m, is closed in the profinite topology of Γ_m. We may therefore apply Corollary 7.2.9 and infer that Γ_m has a subgroup of finite index that maps onto a non-abelian free group. The proposition follows since Γ_m has finite index in Γ.

The lattices of simple type for $m = 3$ include the groups $\mathrm{SL}_2(\mathbb{Z}[\sqrt{-d})$ where d is a square-free positive integer, so these groups also virtually map onto free groups (a result proved by different methods in [Grunewald & Schwermer 1981]; see also [Elstrodt, Grunewald & Mennicke 1998], Chapter 7). There are further arithmetic lattices in $\mathrm{SO}(3,1)$, which are of neither simple nor complex type, coming from the units of some quaternionic algebras; Proposition 7.2.3 shows that they all have subgroup growth of type at least $n^{(\log n)^{2-\varepsilon}}$, but in general their precise growth type is not known.

For $m = 7$ there are also some additional lattices, coming from the triality phenomenon of D_4. Nothing is known about the congruence subgroup problem (or the subgroup growth) for these lattices.

There are two known methods to construct *non-arithmetic lattices* in $\mathrm{SO}(m,1)$.

I. Certain *groups generated by reflections*; these exist for small values of m ($2 \le m \le 10$); see [Vinberg & Shvartsman 1993] for history and details.

II. The so-called "*interbreeding lattices*" constructed for every m by [Gromov & Piatetskii-Shapiro 1988]; see also [Vinberg & Shvartsman 1993].

As we are going to use the interbreeding lattices in §7.3, we will sketch their construction. Let f and f' be two diagonal quadratic forms defined over the same number field k. Let f_0 and f_0' be their restrictions to the hyperplane $x_1 = 0$. We will assume that f and f' are not equivalent over k, but that f_0 and f_0' are equivalent. We now take an ideal J and $\Gamma_m, \Gamma_m', \Gamma_{m-1}, \Gamma_{m-1}', Y_m, Y_m', Y_{m-1}$

and Y'_{m-1} to be as in the above proof, where symbols with $'$ refer to f'. Our assumptions mean that Y_m and Y'_m are not isometric to each other but Y_{m-1} and Y'_{m-1} are. Assume for simplicity that Y_{m-1} (resp. Y'_{m-1}) separates Y_m (resp. Y'_m) into two disjoint pieces Z_1 and Z_2 (resp. Z'_1 and Z'_2). Now let M be the m-dimensional manifold obtained by gluing Z_1 and Z'_2 along their boundaries (which are Y_{m-1} and Y'_{m-1} respectively – these are isometric so the gluing is possible). Being hyperbolic manifolds means that the curvature at every point is -1. As curvature is a local property, M is a hyperbolic manifold whose fundamental group $\Gamma_0 = \pi_1(M)$ is a lattice in $\mathrm{SO}(m,1)$. As explained in [Gromov & Piatetskii-Shapiro 1988], Γ_0 is a non-arithmetic lattice.

In group theoretic terms Γ_0 is obtained as follows: after suitable conjugation in $\mathrm{SO}(m,1)$ we can assume that $\Gamma_{m-1} = \Gamma'_{m-1}$ and then $\Gamma_m = A_1 *_{\Gamma_{m-1}} A_2$ and $\Gamma'_m = A'_1 *_{\Gamma'_{m-1}} A'_2$ where $A_i = \pi_1(Z_i)$ and $A'_i = \pi_1(Z'_i)$ for $i = 1, 2$. Now, Γ_0 is the subgroup generated by A_1 and A'_2, and as Y_{m-1} separates M, $\Gamma_0 = A_1 *_{\Gamma_{m-1}} A'_2$. Also $\Gamma_{m-1} = \Gamma_0 \cap \mathrm{SO}(m-1,1)$ is Zariski-closed in Γ_0, hence closed in the profinite topology of Γ_0. So Corollary 7.2.9 implies that Γ_0 has a subgroup of finite index that maps onto a non-abelian free group.

A common generalization of what we have shown so far is

Theorem 7.2.10 *Let M be an oriented m-dimensional hyperbolic manifold of finite volume. Assume that M has a codimension-one totally geodesic submanifold. Then $\pi_1(M)$ is of VF type .*

The proof, which is quite similar to the special cases seen above, can be found in [Lubotzky 1996(b)]. This result includes also the case where the lattice Γ in $\mathrm{SO}(m,1)$ is inside a group generated by reflections (or just contains a reflection), since in that case the fixed-point set of the reflection is a totally geodesic submanifold of codimension one. We can therefore deduce:

Corollary 7.2.11 *Let Γ be a non-arithmetic lattice in $\mathrm{SO}(m,1)$ which is either generated by reflections or else of 'interbreeding' type. Then Γ is of VF type .*

Let us mention that this corollary covers *all the known examples* of non-arithmetic lattices in $\mathrm{SO}(m,1)$ for $m \geq 4$.

So far we have summarized what we know on the subgroup growth of lattices in $\mathrm{SO}(m,1)$. We turn now to $\mathrm{SU}(m,1)$. Here the story is much shorter as we know very little.

In $\mathrm{SU}(m,1)$ there are also arithmetic lattices similar to those of simple type in $\mathrm{SO}(m,1)$, namely the integral matrices preserving suitable Hermitian forms. For these, it was shown by Kazhdan, Shimura and Borel & Wallach that there exists a congruence subgroup with an infinite abelian quotient (see [Lubotzky 1996_a)]. Hence, again, they do not have the congruence subgroup property and so have subgroup growth type at least $n^{\log n}$. But there are more arithmetic

groups. It is interesting to mention that for some of these, every congruence subgroup has finite abelianisation (though it is not known if the same holds for all subgroups of finite index) – see [Rogawski 1990], Theorem 15.3 and [Clozel 1993]. It is therefore difficult to predict at this point whether they have the congruence subgroup property or not (of course, Serre's conjecture predicts that they do not!). Nor can we say anything about their subgroup growth (beyond the fact that it is of type at least $n^{\log n/\log\log n}$, provided by the congruence subgroups).

For $m = 2$ and 3, some *non-arithmetic lattices* in $\mathrm{SU}(m,1)$ are known (see [Deligne & Mostow 1993]. Also for them we do not know the subgroup growth, except for one of the lattices in $\mathrm{SU}(2,1)$ constructed by Livne and described in [Deligne & Mostow 1993], §16. This lattices has a non-abelian free quotient; it is the only lattice in $\mathrm{SU}(m,1)$ whose subgroup growth type is known.

We turn now to the last remaining cases $\mathrm{Sp}(m,1)$ and $F_4^{(-20)}$. Let us recall right away that by results of [Corlette 1992] and [Gromov & Schoen 1992], all lattices in $\mathrm{Sp}(m,1)$ and in $F_4^{(-20)}$ are arithmetic. According to Serre's conjecture, these arithmetic lattices are not supposed to have the congruence subgroup property. But it should be mentioned that Serre's conjecture is in doubt for these cases: since 1972 when Serre made his conjecture, it has been discovered that lattices in $\mathrm{Sp}(m,1)$ and in $F_4^{(-20)}$ behave in many ways (though not in all ways) like lattices in higher rank groups, e.g. they have Kazhdan's property (T) and super-rigidity. (Recall also that super-rigidity follows from the CSP). On the other hand, there are good reasons to believe that these lattices do *not* have the CSP: the cocompact ones are hyperbolic groups and as such have plenty of normal subgroups of infinite index, while in all cases where the CSP has been proved, it has also been proved that every non-central normal subgroup is of finite index. Anyway, the answer to the congruence subgroup problem is not known for *any single lattice* in these groups. Neither do we know the subgroup growth type.

7.3 Counting hyperbolic manifolds

The following was proved by [Wang 1972]:

Theorem 7.3.1 *For $m \geq 4$ and $0 < r \in \mathbb{R}$, there is only a finite number of m-dimensional hyperbolic manifolds of volume at most r (up to isomorphism).*

[Carlip 1997] and [Carlip 1998], motivated by questions from theoretical physics, raised the question of quantitative estimates for these finite numbers.

Isomorphism classes of m-dimensional hyperbolic manifolds of volume r are in one-to-one correspondence with conjugacy classes of torsion-free lattices of covolume r (with respect to a suitable fixed normalization of the Haar measure) in $\mathrm{SO}(m,1)$. In fact, Wang's Theorem is much more general than our statement: it applies to all lattices (not necessarily torsion free) and most semisimple Lie

groups. Writing $\rho_G(r)$ to denote the number of conjugacy classes of lattices of covolume at most r in a group G, his result is

Theorem 7.3.2 *Let G be a semisimple real Lie group without compact factor, and assume also that no factor of G is locally isomorphic to $\mathrm{PSL}_2(\mathbb{R})$ or $\mathrm{PSL}_2(\mathbb{C})$. Then $\rho_G(r)$ is finite for every positive real number r.*

Counting conjugacy classes of lattices in Lie groups can be thought of as a generalisation of counting finite index subgroups, since in a discrete group (for which the Haar measure of a finite subset is its cardinality) the finite index subgroups are exactly the subgroups of finite covolume. Moreover, it turns out that subgroup growth plays a crucial role in the proof of the lower bound of the following result, which is the response to Carlip's question:

Theorem 7.3.3 *For each $m \geq 4$, there exist positive real numbers $a = a(m)$ and $b = b(m)$ such that*

$$r^{ar} \leq \rho_m(r) \leq r^{br}$$

for all large r, where $\rho_m(r)$ is the number of (isomorphism types of) m-dimensional hyperbolic manifolds of volume at most r.

We give here only the proof of the lower bound, which is based on subgroup growth. For the proof of the upper bound see [Burger, Gelander, Lubotzky & Mozes]. The proof depends on the following theorem of Margulis:

Theorem 7.3.4 [M] *Let Γ be a finitely generated irreducible lattice in a semisimple group H without compact factors. If Γ has infinite index in its commensurator then Γ is arithmetic.*

Here, the *commensurator* of Γ is the group

$$\mathrm{comm}_H(\Gamma) = \left\{ h \in H \mid \Gamma^h \cap \Gamma \text{ has finite index in both } \Gamma \text{ and } \Gamma^h \right\}.$$

Fix $m \geq 4$ and let Γ be one of the "interbreeding lattices" in $\mathrm{SO}(m,1)$ described in the preceding section. Thus Γ is a torsion-free non-arithmetic lattice, of finite covolume v_0 say in $\mathrm{SO}(m,1)$, and by Corollary 7.2.11 there exists $c > 0$ such that

$$s_n(\Gamma) \geq n^{cn}$$

for all large n.

Let $\mathcal{H}^m = \mathrm{SO}(m,1)/\mathrm{SO}(m)$; this is the m dimensional hyperbolic space which is the universal cover of every m-dimensional hyperbolic manifold. Γ acts on $\mathcal{H}^m$, and v_0 is the volume of the hyperbolic manifold $\Gamma\backslash\mathcal{H}^m$. Each subgroup Δ of index t in Γ gives rise to an m-dimensional hyperbolic manifold $M_\Delta = \Delta\backslash\mathcal{H}^m$ which is a t-fold cover of $\Gamma\backslash\mathcal{H}^m$ and has volume tv_0. Now suppose Δ and Δ' are two such subgroups of Γ. If M_Δ and $M_{\Delta'}$ are isomorphic (=isometric) then an isomorphism $\varphi : M_\Delta \to M_{\Delta'}$ lifts to an isometry $\tilde{\varphi} : \mathcal{H}^m \to \mathcal{H}^m$. Now the group of isometries of $\mathcal{H}^m$ is $G = \mathrm{O}(m,1)$ and hence $\tilde{\varphi}$ is given by an

element g of G which conjugates $\Delta = \pi_1(M_\Delta)$ to $\Delta' = \pi_1(M_{\Delta'})$. As Δ and Δ' are of finite index in Γ, it follows that Γ^g is commensurable with Γ, that is, $g \in \mathrm{Comm}_G(\Gamma) = \Gamma_1$, say.

Now, as Γ is a non-arithmetic lattice, Margulis's Theorem 7.3.4 implies that the index $|\Gamma_1 : \Gamma| = h$, say, is finite. Then for a given Δ of index t in Γ_0, there are at most ht subgroups of Γ which are conjugate to Δ in Γ_1. In view of the preceding paragraph, this implies that the manifolds of the form M_Δ lie in at least $a_t(\Gamma)/ht$ isomorphism classes when Δ ranges over the $a_t(\Gamma)$ subgroups of index t in Γ.

It follows that for each positive integer n,

$$\rho_m(nv_0) \geq \sum_{t=1}^{n} a_t(\Gamma)/ht \geq \frac{s_n(\Gamma)}{hn} \geq \frac{n^{cn-1}}{h}.$$

Let r be a large positive number, and put $n = [r/v_0]$. Then

$$\rho_m(r) \geq \rho_m(nv_0) \geq r^{ar}$$

where a is any positive constant strictly smaller than c/v_0, provided r is large enough. This is the required lower bound.

Remark One can give explicit estimates for c and v_0 in this proof, and thereby obtain an explicit bound for $a = a(m)$.

An interesting aspect of the proof of Theorem 7.3.3 is that the rate of growth of the number of hyperbolic manifolds is governed by the subgroup growth of **one** lattice. One may wonder whether this is the case in more general circumstances. If G is a simple Lie group of rank at least 2 and Γ is a lattice in G, then by Margulis's Theorem 7.2.1, Γ is arithmetic and by Serre's conjecture (which is proved in most cases) Γ has the congruence subgroup property; hence its subgroup growth is of type $n^{\log n/\log\log n}$ by Theorem 6.1. These observations motivate the following conjecture posed in [Burger, Gelander, Lubotzky & Mozes].

Conjecture Let G be a simple Lie group of $\mathbb{R}$-rank at least 2. Let $\rho^*_G(r)$ be the number of manifolds covered by $X = G/K$ of volume at most r, where K is a maximal compact subgroup of G. (Equivalently, $\rho^*_G(r)$ is the number of conjugacy classes of torsion-free lattices of covolume at most r in G). Then the function $\rho^*_G(r)$ has strict growth type

$$r^{\log r/(\log\log r)}.$$

A similar conjecture can be stated for $\rho_G(r)$ as defined at the beginning of this section. The connection between $\rho_G(r)$ and $\rho^*_G(r)$ needs some clarification. It is quite likely that they have similar growth type. For more results on $\rho_G(r)$ see [Gelander].

Notes

Theorem 7.1 is from [**Lubotzky 1995**$_a$]. Part 1 of Theorem 7.2 follows readily from well-known results, as does the case of $\mathrm{SO}(2,1)$ in part 2(a). The case of $\mathrm{SO}(3,1) \approx \mathrm{SL}_2(\mathbb{C})$ is treated in [**Lubotzky 1995**$_a$], but the critical ingredients are from [**Lubotzky 1983**] and the unpublished result of Shalev, Theorem 4.6.4.

As mentioned in §7.2, [**Cooper, Long & Reid 1997**] and [**Grunewald & Noskov**] give sharp results for non-uniform lattices, while [**Reznikov & Moree 1997**] give a sharper result for some cocompact lattices. We mention in passing that a standard way to contradict the CSP for arithmetic groups is to provide a finite-index subgroup having infinite abelianisation. Indeed, according to a well-known conjecture of Thurston it is expected that all lattices in $\mathrm{SO}(n,1)$ have such a subgroup. This is still wide open in the case of $\mathrm{SO}(3,1)$, even for arithmetic lattices; for the case of arithmetic lattices in $\mathrm{SO}(n,1)$ with $n \neq 3,7$ see [**Lubotzky 1996**$_a$].

On the other hand, for $n \geq 4$, a strong form of Thurston's conjecture (property VF) for the *known* non-arithmetic lattices in $\mathrm{SO}(n,1)$ is established in [**Lubotzky 1996**$_b$], giving Part 2(b) of Theorem 7.2. However, Thurston's conjecture (and the subgroup growth type) is not known as yet for arbitrary non-arithmetic lattices (if any more exist!).

As for Part 2(c), the failure of the CSP for some of the arithmetic lattices in $\mathrm{SU}(n,1)$ was established by **Kazhdan**, **Shimura**, **Borel** and **Wallach**; see [**Lubotzky 1996**$_a$**)**]. The claim about Livne's non-arithmetic lattices follows directly from their construction. There are further non-arithmetic lattices, about which nothing is known.

Theorem 7.3 is established in [**Burger, Gelander, Lubotzky & Mozes**].

Chapter 8

Linear groups

Given a major result such as the PSG Theorem, it is usually worth while to try and deconstruct its proof: by following up various intermediate steps one may achieve deeper insights and, possibly, be led to new results. The material of Chapter 6 is a case in point, as are some of the methods described in the **Linearity conditions** and **Strong Approximation** windows. Here we consider the subgroup growth of finitely generated linear groups, and will see that for these, a stronger form of the PSG Theorem holds.

Theorem 8.1 *Let G be a finitely generated linear group over a field of characteristic* 0*. Then* either *G is virtually soluble of finite rank (hence has* PSG*)* or *there exists $b > 0$ such that*

$$s_n(G) \geq n^{b \log n / \log \log n}$$

for all sufficiently large n.

Thus for such groups there is a *gap* in the possible growth types: a finitely generated characteristic-0 linear group has subgroup growth of strict type at least $n^{\log n / \log \log n}$ or at most n.

In positive characteristics the gap is even wider:

Theorem 8.2 *Let G be a finitely generated linear group over a field of positive characteristic. Then* either *G is virtually abelian (hence has* PSG*)* or *there exists $b > 0$ such that*

$$s_n(G) \geq s_n^{\lhd\lhd}(G) > n^{b \log n}$$

for all sufficiently large n.

Both Theorems 8.1 and 8.2 are best possible. As shown in Chapter 6, the groups $\mathrm{SL}_3(\mathbb{Z})$ and $\mathrm{SL}_3(\mathbb{F}_p[t])$ have congruence subgroup growth of type $n^{\log n / \log \log n}$ and $n^{\log n}$ respectively; as both groups also have the congruence subgroup property, these are also the respective subgroup growth types.

Although they cannot be sharpened, these results can be generalized. Every f.g. linear group has a *residually nilpotent* normal subgroup N of finite index: that is, the lower central series $(\gamma_i(N))$ intersects in the identity. For groups in this wider class we still have a 'gap theorem':

Theorem 8.3 *Let G be a finitely generated group that is virtually residually nilpotent. If G has subgroup growth of type strictly less than $n^{\log n/\log\log n}$ then G is virtually soluble of finite rank (hence has* PSG*).*

Theorem 8.1 is proved in Section 1; more precisely, it is reduced to the special case of *metabelian groups*, which is postponed to the following chapter. Theorem 8.3 is deduced from it in Section 2. The proof of Theorem 8.2 is given in Section 3. Unlike the PSG Theorem, these results do not depend on CFSG, which was invoked only in the 'reduction to the linear case'.

In Section 4 we turn to *normal subgroup growth*. We saw in Chapter 2 that the normal subgroup growth type of a free group is $n^{\log n}$. This is just slightly faster than polynomial, so one cannot expect *polynomial normal subgroup growth* (PNSG) to imply very strong structural restrictions in the way that PSG does. Indeed, the examples produced in Chapter 13 below have normal subgroup growth that is slower than linear, and they are far from being soluble. In spite of this, we have

Theorem 8.4 *Let G be a finitely generated linear group. Let $\mathbf{G}$ be the Zariski closure of G, $\mathbf{G}^0$ its identity component and $R(\mathbf{G})$ the maximal soluble normal subgroup of $\mathbf{G}^0$. Write*

$$\mathbf{G}^0/R(\mathbf{G}) = \prod_{i=1}^{r} \mathbf{S}_i$$

where each $\mathbf{S}_i$ is a simple algebraic group. If G has normal subgroup growth of type strictly less than $n^{\log n/(\log\log n)^2}$ then one of the following holds:

(i) *$r = 0$, in which case $\mathbf{G}$ and G are virtually soluble, or*

(ii) *each $\mathbf{S}_i$ is of type G_2, F_4 or E_8.*

This theorem is quite surprising in two ways. First, it shows that unlike the situation for residually finite groups in general, even a slight limitation on normal subgroup growth (weaker than PNSG) *does* imply strong structural restrictions on a linear group. Moreover, these restrictions are of a subtle nature: they manifest themselves only in the *algebraic group* generated by the linear group; like the congruence subgroup property discussed in the last chapter, this is another case of an abstract group-theoretic property influencing how a group can sit as a group of matrices.

Secondly, one may wonder about the distinguished role played by the exceptional simple groups G_2, F_4 and E_8. What is so special about them? These are the only simple algebraic groups whose *fundamental group is trivial*: this

means that they have a trivial centre over any field. After reading Chapter 6 the reader may not find the occurrence of G_2, F_4 and E_8 all that surprising, since we have already seen there that they behave differently when we count normal *congruence* subgroups. In fact Theorem 6.3 shows that $G_2(\mathbb{Z}), F_4(\mathbb{Z})$ and $E_8(\mathbb{Z})$ each have polynomial normal congruence subgroup growth; since they are also known to have the congruence subgroup property, this is the same as saying that they have PNSG. Theorem 8.4 is thus best possible in the sense that G_2, F_4 and E_8 indeed appear as exceptions.

The result proved in Section 4 is actually even stronger, and reflects the trichotomy for normal congruence subgroup growth given in Theorem 6.3.

8.1 Subgroup growth, characteristic 0

Let G be a finitely generated linear group over a field of characteristic zero. We separate two cases.

Case 1. Where G is not virtually soluble.

Just as in §5.2, it follows by the 'Lubotzky alternative' (↬ **Strong approximation**) that there exist a subgroup G_1 of finite index in G, a finite set of primes S, and a connected, simply connected simple algebraic group $\mathfrak{S}$ over $\mathbb{Q}$ such that every congruence quotient of $\Gamma = \mathfrak{S}(\mathbb{Z}_S)$ appears as a quotient of G_1 (and Γ is infinite). Then by Theorem 6.1 we have

$$s_n(G_1) \geq c_n(\Gamma) \geq n^{a \log n / \log\log n}$$

for all n, where $a > 0$ is a constant (and $c_n(\Gamma)$ denotes the number of congruence subgroups of index at most n in Γ). Since $s_n(G) \geq s_{[n/m]}(G_1)$ where $m = |G : G_1|$ it follows in this case that

$$s_n(G) \geq n^{b \log n / \log\log n}$$

for all large n, for a suitable constant $b > 0$.

Case 2. Where G is virtually soluble, of infinite rank.

This case depends on the following result, which will be established in Section 1 of the following chapter:

Proposition 8.1.1 *Let H be a finitely generated virtually metabelian group of infinite rank. Then there exist $c > 1$ and $d \in \mathbb{N}$ such that*

$$s_n^{\lhd\lhd}(H) \geq c^{n^{1/d}}$$

for all large n.

Now according to the Lie-Kolchin-Mal'cev Theorem (↬ **Linear groups**), G has a nilpotent normal subgroup N such that G/N is virtually abelian. Since G is finitely generated, the quotient G/N has finite rank, so N must have infinite rank. As N is nilpotent, this implies that N/N' also has infinite rank

($\looparrowright$ **Soluble groups**). Hence the virtually metabelian group G/N' has infinite rank. Proposition 8.1.1 now shows that there exist $c > 1$ and $d \in \mathbb{N}$ such that

$$s_n^{\triangleleft\triangleleft}(G/N') \geq c^{n^{1/d}}$$

for all large n. Since $s_n^{\triangleleft\triangleleft}(G) \geq s_n^{\triangleleft\triangleleft}(G/N')$ and $c^{n^{1/d}} > n^{\log n/\log\log n}$ for large n, we see that

$$s_n(G) \geq s_n^{\triangleleft\triangleleft}(G) > n^{\log n/\log\log n}$$

for all large n.

This completes the proof of Theorem 8.1, modulo Proposition 8.1.1.

Remark The argument in Case 2 does not depend on the characteristic being zero; it shows that *any f.g. linear group that is virtually soluble and of infinite rank has subnormal subgroup growth of strict type at least* 2^{n^ε} *for some* $\varepsilon > 0$. This will be used in Section 8.3.

8.2 Residually nilpotent groups

Let G be a finitely generated group that is virtually residually nilpotent, and assume that G has subgroup growth of type strictly less than $n^{\log n/\log\log n}$. Let H be a residually nilpotent normal subgroup of finite index m in G, and let p be any prime. Then for all sufficiently large n we have

$$s_n(\widehat{H}_p) \leq s_n(H) \leq s_{mn}(G) < n^{(\log_p n)/16}.$$

It follows by Theorem 4.2 that for each prime p, the pro-p completion $\widehat{H}_p$ of H is a pro-p group of finite rank. Now Theorem 8 of the **Linearity conditions** window shows that H is a linear group over a field of characteristic zero. Therefore so is G.

We may therefore apply Theorem 8.1 and infer that G is virtually soluble of finite rank, thus establishing Theorem 8.3.

8.3 Subgroup growth, characteristic p

Since a finitely generated linear group in any characteristic is virtually residually nilpotent, we already know that such a group is either virtually soluble of finite rank or else has subgroup growth of type at least $n^{\log n/\log\log n}$. When the characteristic is positive, however, we can say more. Here we prove

Theorem 8.2 *Let F be a field of characteristic $p > 0$ and Γ a finitely generated subgroup of $\mathrm{GL}_m(F)$. Then one of the following holds:*

(a) *Γ is virtually abelian, hence has* PSG;

(b) *there exists a constant $c > 0$ such that $s_n(\Gamma) \geq s_n^{\triangleleft\triangleleft}(\Gamma) \geq n^{c\log n}$ for all sufficiently large n.*

This depends on the following important structure theorem for linear groups over local fields:

Theorem 8.3.1 [Pink 1998] *Let K be a local field of characteristic $p > 0$ and L a compact subgroup of $\mathrm{GL}_m(K)$. Then there exist closed normal subgroups $L_3 \leq L_2 \leq L_1$ of L such that:*

1 *L/L_1 is finite;*

2 *L_1/L_2 is abelian of finite exponent;*

3 *if L_2/L_3 is infinite, there exist a local field E of characteristic p, a connected adjoint semi-simple algebraic group $\mathbf{H}$ over E with universal covering $\varpi : \widetilde{\mathbf{H}} \to \mathbf{H}$, and an open compact subgroup $\Delta \leq \widetilde{\mathbf{H}}(E)$, such that L_2/L_3 is isomorphic as topological group to $\varpi(\Delta)$;*

4 *L_3 is a soluble group of derived length at most m.*

Now let Γ be a finitely generated subgroup of $\mathrm{GL}_m(F)$. As Γ is finitely generated it is contained in $\mathrm{GL}_m(A)$ for some finitely generated subring A of F. Now A can be embedded into the ring of integers R of some local field K of characteristic p, so we may suppose that Γ is a subgroup of $M = \mathrm{GL}_m(R)$. Also M is virtually a pro-p group, so by passing to a normal subgroup of finite index we may assume that the closure L of Γ in M is a pro-p group. In this case, L is a homomorphic image of the pro-p completion $\widehat{\Gamma}_p$ of Γ, and $s_n(L) \leq s_n^{\triangleleft\triangleleft}(\Gamma)$ for every n.

Suppose first that Γ is virtually soluble. Then Γ has a unipotent normal subgroup U such that Γ/U is virtually abelian (The Lie-Kolchin Theorem, ↬ **Linear groups**). U is a nilpotent group of exponent dividing p^m, so if Γ has *finite rank* then U is finite; as Γ is residually finite it follows that Γ is virtually abelian, and we are in Case (a) of Theorem 8.2. If Γ has *infinite rank* then the *remark* at the end of Section 8.1 shows that the subnormal subgroup growth of Γ is of strict type at least 2^{n^ε} where $\varepsilon > 0$, and we are in Case (b).

Suppose next that Γ is not virtually soluble. Then L is not virtually soluble. We apply Pink's theorem. Since L is a finitely generated pro-p group, L/L_2 is finite and therefore L_2/L_3 is infinite. Let $\mathcal{O}$ be the valuation ring of the local field E given in the theorem. Then Δ is commensurable with $\widetilde{\mathbf{H}}(\mathcal{O})$, and the argument given in §6.2 shows that $\widetilde{\mathbf{H}}(\mathcal{O})$ has subgroup growth of strict type at least $n^{\log n}$. The same therefore holds for Δ, and as $\ker \varpi$ is finite it holds for $L_2/L_3 \cong \varpi(\Delta)$, and hence for L since L/L_2 is finite. Thus there exists $c > 0$ such that $s_n^{\triangleleft\triangleleft}(\Gamma) \geq s_n(L) \geq n^{c \log n}$ for all large n, and we are in Case (b).

This completes the proof of Theorem 8.2.

Remark It is interesting to observe that the proof of Theorem 8.2 given here is very different from the proof of Theorem 8.1. In the characteristic 0 case we used "global" arithmetic groups and the strong approximation theorem for linear groups. Here we apply only "local" methods, and yet get a stronger result. On the other hand, there is some formal similarity in the structure of the proofs: Pink's theorem in the one case, and the Weisfeiler-Nori theorem in the other, being used to replace an arbitrary linear group by an 'arithmetically

defined' subgroup of some semisimple algebraic group, where the structure can be seen fairly explicitly.

8.4 Normal subgroup growth

In this section we outline the proof of the following theorem, which is a stronger form of Theorem 8.4. Let us fix some notation.

F is an algebraically closed field of characteristic $p \geq 0$, G is a finitely generated subgroup of $\mathrm{GL}_r(F)$, and $\mathbf{G}$ is the Zariski closure of G, with connected component $\mathbf{G}^0$. The maximal soluble normal subgroup of $\mathbf{G}^0$ is denoted $R(\mathbf{G})$, and we have a decomposition

$$\mathbf{G}^0/R(\mathbf{G}) = \prod_{i=1}^{r} \mathbf{S}_i$$

where each $\mathbf{S}_i$ is a simple algebraic group over F. The fundamental group of the adjoint group scheme associated to $\mathbf{S}_i$ is denoted $\pi(\mathbf{S}_i)$ – recall from Chapter 6 that $\pi(\mathbf{S}_i) = 0$ if and only if $\mathbf{S}_i$ is of type G_2, F_4 or E_8; otherwise it is a finite group of order $l+1$ if $\mathbf{S}_i$ is of type A_l, of order 2, 3 or 4 in all other cases.

Theorem 8.4.1 (i) *If $\pi(\mathbf{S}_i) \neq 0$ for at least one i then there exists $c > 0$ such that*

$$s_n^{\triangleleft}(G) \geq n^{c \log n/(\log\log n)^2}$$

for all n.

(ii) *If $p \mid |\pi(\mathbf{S}_i)|$ for at least one i then there exists $c > 0$ such that*

$$s_n^{\triangleleft}(G) \geq n^{c \log n}$$

for all n.

A serious technical difficulty in the proof comes from the fact that we do not know the answer to the following simple question:

Problem. Let G be a finitely generated group and H a normal subgroup of finite index in G. Is the normal subgroup growth type of H the same as that of G?

(It is easy to see that the normal subgroup growth type of H is *at least* that of G.)

When studying subgroup growth we often pass without loss of generality to a subgroup of finite index. The fact that we are not allowed (as of now) to do so with normal subgroup growth is a real headache.

Let us first prove the theorem *assuming that the problem has an affirmative answer*. Then we will indicate how the proof is carried out even without this assumption.

One of the advantages in assuming that the problem has an affirmative answer is that we are allowed to replace $\mathbf{G}$ by $\mathbf{G}^0$, and so assume that $\mathbf{G}$ is

connected. As we need to prove only lower bounds on the normal subgroup growth, we may also replace $\mathbf{G}$ (and hence also G) by any suitable quotient. Without loss of generality, we shall therefore assume that $\mathbf{G}$ is a connected simple algebraic group with $\pi(\mathbf{G}) \neq 0$, and in case (ii) that $p \mid |\pi(\mathbf{G})|$.

Recall now that a *specialisation* of G means a group homomorphism $\psi : G \to \mathrm{GL}_r(k)$ that is induced by some ring homomorphism from R into some field k, where R is a subring of F such that $G \leq \mathrm{GL}_r(R)$; note that if $\mathrm{char}(F) = p \neq 0$ then also $\mathrm{char}(k) = p$. We now quote the following 'specialisation theorem', which appears in the **Strong approximation** window:

Theorem 8.4.2 *Let G be a finitely generated subgroup of $\mathrm{GL}_r(F)$ whose Zariski closure $\mathbf{G}$ is a connected simple algebraic group. Then there exist a global field k and a specialisation $\psi : G \to \mathrm{GL}_r(k)$ such that the Zariski closure of $\psi(G)$ in $\mathrm{GL}_r(\overline{k})$ is isomorphic to $\mathbf{G}$.*

Applying this theorem, we may replace G by $\psi(G)$, and so reduce to the case where $G \leq \mathrm{GL}_n(k)$ where k is a global field of characteristic p. As G is finitely generated, there exists a finite set of primes S of k (containing all the archimedean ones) such that $G \leq \mathbf{G}(\mathcal{O}_S) = \mathbf{G} \cap \mathrm{GL}_r(\mathcal{O}_S)$, where $\mathcal{O}_S$ denotes the ring of S-integers of k.

According to the Strong Approximation Theorem for linear groups (↬ **Strong Approximation**), there is a finite set $S' \supseteq S$ of primes of k such that G is dense in $\mathbf{G}(\widehat{\mathcal{O}_{S'}})$. It follows that G has at least as many normal subgroups of index n as $\mathbf{G}(\mathcal{O}_{S'})$ has normal congruence subgroups of index n; according to Theorem 6.3, this is at least $n^{c \log n/(\log\log n)^2}$ for some constant $c > 0$. This establishes (i) (and also Theorem 8.4), under our simplifying assumption.

Suppose now that we are in **case (ii)**, i.e., $p \mid |\pi(\mathbf{G})|$. We again apply Pink's theorem, Theorem 8.3.1 stated in the preceding section.

Choose a prime v of k outside S and take K to be the completion k_v, with valuation ring $\mathcal{O}_\nu$. Then G is contained in $\mathbf{G}(\mathcal{O}_\nu)$, and the closure L of G in $\mathbf{G}(\mathcal{O}_\nu)$ is a compact subgroup of $\mathrm{GL}_r(K)$ (topological terms refer here to the v-topology on k_v, which makes $\mathbf{G}(\mathcal{O}_\nu)$ a profinite, indeed virtually pro-p, group). We therefore have closed normal subgroups $L_3 \leq L_2 \leq L_1$ of L such that

L/L_2 is virtually abelian of finite exponent;

if L_2/L_3 is infinite, there exist a local field E of characteristic p, a connected adjoint semi-simple algebraic group $\mathbf{H}$ over E with universal covering $\varpi : \widetilde{\mathbf{H}} \to \mathbf{H}$, and an open compact subgroup $\Delta \leq \widetilde{\mathbf{H}}(E)$, such that L_2/L_3 is isomorphic as topological group to $\varpi(\Delta)$;

L_3 is soluble.

Since G is finitely generated, L is topologically finitely generated and so L/L_2 is finite. Also L_3 is finite and L_2/L_3 is infinite, since L is Zariski dense

in the simple algebraic group $\mathbf{G}$, and L_2 is Zariski-dense in $\mathbf{G}$ because $\mathbf{G}$ is connected.

It follows (see [Pink 1998]) that the algebraic group $\widetilde{\mathbf{H}}$ is isogenous to $\mathbf{G}$ and hence that $|\pi(\widetilde{\mathbf{H}})|$ is also divisible by p. Now Theorem 6.4(i) shows that the group $\widetilde{\mathbf{H}}(\mathcal{O}_E)$ has normal subgroup growth of strict type $n^{\log n}$. Using our simplifying assumption (twice!) we may infer that the commensurable group Δ has the same strict normal subgroup growth type, and hence so does $L_2/L_3 \cong \varpi(\Delta)$, as $\ker \varpi$ is finite. Using the simplifying assumption once more we deduce that L/L_3, and hence L, has at least $n^{c \log n}$ normal subgroups of index at most n for each n, where $c > 0$ is a constant. Since L is an image of the profinite completion of G it follows that G has at least this many normal subgroups, and case (ii) is established.

Let us now indicate how one still proves Theorem 8.4.1 without knowing that the open problem has an affirmative answer in general. Whenever we pass from G to a finite index normal subgroup H, we have to make sure that at least a *good proportion* of the finite-index normal subgroups of H are still normal in G. We illustrate the basic idea by considering a special case.

Let $\mathbf{G}$ be a simple Chevalley group with $\mathbb{Z}$-structure and put $H = \mathbf{G}(\mathbb{Z})$. The outer automorphism group $\mathrm{Out}(\mathbf{G})$ is a finite group acting on H. Let $G = H \rtimes \mathrm{Out}(\mathbf{G})$. Now, if $\mathbf{G}$ is not of type G_2, F_4 or E_8 (i.e., if $\pi(\mathbf{G}) \neq 0$), we have produced many normal congruence subgroups in the following way (see the proof of Theorem 6.3, and the example preceding it, in §6.4): let $\mathcal{P}$ be a finite set of primes with $|\mathcal{P}| = \ell$ (in the example of §6.4, $\mathcal{P}$ consists of all primes $p \leq x$ with $p \equiv 1 (\mathrm{mod}\, 3)$). Put $m = \prod_{p \in \mathcal{P}} p$, so $\mathbf{G}(\mathbb{Z}/m\mathbb{Z}) = \prod_{p \in \mathcal{P}} \mathbf{G}(\mathbb{F}_p)$. Let $H(m) = \ker(H \to \mathbf{G}(\mathbb{Z}/m\mathbb{Z}))$. The group $H(m)$ is also normal in $G = H \rtimes \mathrm{Out}(\mathbf{G})$. Now $\mathrm{Z}(\mathbf{G}(\mathbb{Z}/m\mathbb{Z}))$ is not necessarily central in $G/H(m)$, and the subgroups of $\mathrm{Z}(\mathbf{G}(\mathbb{Z}/m\mathbb{Z}))$ may not all be normal in $G/H(m)$. However, if we fix a prime q such that $q \mid |\mathrm{Z}(\mathbf{G}(\mathbb{F}_p))|$ for each $p \in \mathcal{P}$, then for each such p the set V_p of elements of order dividing q in $\mathrm{Z}(\mathbf{G}(\mathbb{F}_p))$ is an elementary abelian q-group (it is usually cyclic, unless H is of type D_n, in which case $q = 2$ and $V_p \cong C_2 \times C_2$), and it is $\mathrm{Out}(\mathbf{G})$-invariant. Hence we get in $\mathbf{G}(\mathbb{Z}/m\mathbb{Z})$ a central subgroup $W = \prod_{p \in \mathcal{P}} V_p \cong V \otimes \mathbb{F}_q^\ell$ (where V is the common isomorphism type of the V_p). The action of $\mathrm{Out}(\mathbf{G})$ on W is its action on V tensored with the trivial action on $\mathbb{F}_q^\ell$. So, while not every subgroup of W is $\mathrm{Out}(\mathbf{G})$-invariant, every $\mathbb{F}_q$-subspace U of $\mathbb{F}_q^\ell$ gives rise to a subgroup $V \otimes U$ which is $\mathrm{Out}(\mathbf{G})$-invariant, and hence gives a normal subgroup of G. It is now easy to count and to show that this gives a supply of at least $q^{[\ell^2/4]}$ normal subgroups in $G = H \rtimes \mathrm{Out}(\mathbf{G})$ of index at most $m^{\dim(\mathbf{G})} \cdot |\mathrm{Out}(\mathbf{G})|$. This suffices to ensure that the normal subgroup growth of G is (at least) of the same strict type as the the normal congruence subgroup growth of H (though possibly with a smaller constant).

The proof in general involves considerable technicalities; the reader is referred to [Larsen & Lubotzky] for details.

Notes

Theorem 8.1 appeared in [**Lubotzky 1995**$_a$]. A slightly weaker form of Theorem 8.2 appears in [**Abért, Lubotzky & Pyber**]. All the material on normal subgroup growth is from [**Larsen & Lubotzky**].

Chapter 9

Soluble groups

The first version (historically) of the PSG Theorem to be proved dealt with the very special case of groups that are assumed to be both soluble and residually nilpotent; under these hypotheses, an elementary argument sufficed for the proof, involving none of the sophisticated mathematics that we have seen in Chapter 5. In section 2 of this chapter we give a slightly more sophisticated (though still elementary) proof of the following sharper result:

Theorem 9.1 *Let G be a finitely generated virtually soluble group that is virtually residually nilpotent. Then* either *G has finite rank (and hence PSG),* or *there exist $c > 1$ and $d \in \mathbb{N}$ such that*

$$s_n(G) \geq s_n^{\triangleleft\triangleleft}(G) \geq c^{n^{1/d}}$$

for all large n.

This shows that the subgroup growth gap for residually nilpotent *soluble* groups is much larger than that for residually nilpotent groups in general, which was given in Theorem 8.2. In Section 3 we show that this theorem is best possible, by constructing for every integer $d \geq 2$ a finitely presented metabelian group having subgroup growth, and subnormal subgroup growth, of strict type $2^{n^{1/d}}$.

Whether a similar (or perhaps smaller) gap occurs in the growth types of finitely generated soluble groups that are *not* virtually residually nilpotent is a major open problem, and present techniques seem to shed little light on this question; for more on this see the *notes* at the end of this chapter. It is worth remarking that *no example is known (*to us*) of a finitely generated residually finite soluble group that is not virtually residually nilpotent.* If the two conditions in fact turn out to be equivalent, then of course Theorem 9.1 will provide a positive solution to this 'soluble gap problem'.

Among finitely generated soluble groups, the *metabelian* ones are the easiest to understand; questions about these often reduce to commutative algebra. This

is illustrated by the construction given in Section 3, and also in the rest of the chapter. We begin in Section 1 by proving the special case of Theorem 9.1 where G is virtually metabelian; as well as introducing in simplified form the ideas needed for the general case, this fills the gap left in the proof of Theorem 8.1 in the preceding chapter.

In Section 4 we consider *normal subgroup growth*. While little is known about this for soluble groups in general, the metabelian case is fairly well understood. To each finitely generated metabelian group G we associate an invariant $\kappa(G)$, which is the Krull dimension of the ring

$$\mathbb{Z}[G^{\mathrm{ab}}]/\mathrm{ann}(G');$$

here G' denotes the derived group of G, considered as a module for the group ring of $G^{\mathrm{ab}} = G/G'$. When G is infinite, $\kappa(G)$ is a positive integer.

Theorem 9.2 *Let G be a finitely generated metabelian group with $\kappa(G) = k \geq 1$. Then there exist positive constants a and b such that*

$$n^{b(\log n)^{1-2/k}} \leq s_n^{\lhd}(G) \leq n^{a(\log n)^{1-1/k}}$$

for all large n.

Thus we have an infinite sequence of normal subgroup growth types, faster than polynomial and slower than those exhibited by arithmetic groups (see Chapter 6). This theorem is a litte imprecise (a statement of our ignorance, not of mathematical fact!); but for polynomial normal subgroup growth (PNSG) the result is definitive:

Theorem 9.3 *Let G be a finitely generated metabelian group. Then G has PNSG if and only if $\kappa(G) \leq 2$.*

Analogous results hold for metabelian pro-p groups. The proofs are not given in full, but we explain how these results are deduced from corresponding results in commutative ring theory.

9.1 Metabelian groups

Here we prove the special case of Theorem 9.1 dealing with *virtually metabelian* groups. This step will suffice to complete the remaining case of Theorem 8.1, concerning virtually soluble linear groups (see Chapter 8).

The essential idea of the proof has already been used in Section 2 of Chapter 3, where we considered the group $C_p \wr C_\infty$; it merely requires some technical elaboration. Let G be a finitely generated virtually metabelian group of infinite rank. Thus G has an abelian normal subgroup A and a normal subgroup G_0 of finite index, containing A, such that $G_0/A \cong \mathbb{Z}^d$ for some $d \in \mathbb{N}$. The group ring $R = \mathbb{Z}(G_0/A)$ is Noetherian, and the action of G_0/A by conjugation makes A into a finitely generated R-module (which we shall write additively). Since

G/A has finite rank, A must have infinite rank, and it follows that for at least one prime p the quotient $A/pA = \overline{A}$ has infinite rank; this follows from Hall's 'generic freeness lemma' (↬ **Soluble groups,** §3). There exist prime ideals $P_1, \ldots, P_k$ of R and a filtration $0 = M_0 < M_1 < \ldots < M_k = \overline{A}$ such that for each i the factor module M_i/M_{i-1} is a torsion-free R/P_i-module; we fix an index j such that M_j/M_{j-1} is infinite and put $M = M_j/M_{j-1}$, $P = P_j$. Let L be a maximal ideal of R containing P, and put

$$K/A = (1 + L) \cap (G_0/A).$$

Note that L has finite index in R (↬ **Soluble groups**, §3); it follows that K has finite index in G_0, so K contains a subgroup H of finite index which is normal in G, with $H \geq A$.

Since M is a torsion-free Noetherian module for R/P, Krull's Intersection Theorem ([AM], Theorem 10.17) shows that

$$\bigcap_{n=1}^{\infty} ML^n = 0.$$

As M/ML^n is finite for each n it follows that $ML^n > ML^{n+1}$ for each n, whence

$$\dim_{\mathbb{F}_p}(M/ML^n) \geq n.$$

The Artin-Rees Lemma ([AM], Chapter 10) says that for some fixed k, we have $\overline{A}L^{n+k} \cap M_j \subseteq M_j L^n$ for every n. Therefore

$$\dim_{\mathbb{F}_p}(\overline{A}/\overline{A}L^{n+k}) \geq n.$$

Now if $x \in H$ and $n \geq 1$ then $x^{p^m} - 1 \equiv (x-1)^{p^m} \pmod{p}$. Since H/A is abelian and $p\overline{A} = 0$ it follows that

$$\overline{A}(H^{p^m} - 1) \subseteq \overline{A}(H-1)^{p^m} \subseteq \overline{A}L^{p^m}$$

and hence that

$$\dim_{\mathbb{F}_p}(\overline{A}/\overline{A}(H^{p^m} - 1)) \geq p^m - k$$

whenever $p^m > k$.

Let us translate this back into group-theoretic notation. Given m as above, put $H_m = AH^{p^m}$ and $B_m = A^p[A, H_m]$. Then $B_m < A < H_m$, $H_m/A \cong \mathbb{Z}^d$ and A/B_m is an elementary abelian p-group of rank at least $p^m - k$, central in H_m/B_m. Now let $x, y \in H_m$. If $p \geq 3$ then $x^p y^p \equiv (xy)^p \pmod{B_m}$, while if $p = 2$ then $x^4 y^4 \equiv (xy)^4 \pmod{B_m}$. It follows (putting $\mathbf{p} = p$ if $p \geq 3$, $\mathbf{p} = 4$ if $p = 2$) that the subgroup $H_m^{\mathbf{p}} B_m/B_m$ consists of $\mathbf{p}$th powers in H_m/B_m and hence that

$$H_m^{\mathbf{p}} B_m \cap A = B_m.$$

Therefore $H_m^{\mathbf{p}} A/H_m^{\mathbf{p}} B_m \cong A/B_m$ is an elementary abelian p-group of rank at least $p^m - k$. Thinking of this as an $\mathbb{F}_p$-vector space we see that it contains at

least p^{p^m-k-1} subgroups of index p (and each of these is normal in H_m, which in turn is normal in G).

On the other hand,

$$\begin{aligned} |G : H_m^{\mathbf{p}}A| &= |G : H| \cdot |H : H_m| \cdot |H_m : H_m^{\mathbf{p}}A| \\ &= a \cdot p^{dm} \cdot \mathbf{p}^d \\ &\leq ap^{d(m+2)} \end{aligned}$$

where $a = |G : H|$ is a constant independent of m.

Now given a large positive integer n let m be such that

$$ap^{d(m+2)+1} \leq n < ap^{d(m+3)+1}.$$

From the above we see that G contains at least p^{p^m-k-1} (2-step subnormal) subgroups of index at most n. If n is sufficiently large this number exceeds $c^{n^{1/d}}$ where $c = p^{(2a)^{-1/d}} > 1$.

This completes the proof of Theorem 9.1 for the case where G is virtually metabelian.

The reader familiar with commutative algebra will have realised that we used less than full information about the R-module $\overline{A}$ in the above argument. Using the Hilbert-Samuel Theorem, one can show that in fact

$$\dim_{\mathbb{F}_p}(M/ML^n) \geq n^r$$

where r is the Krull dimension of the local ring $(R/P)_{L/P}$; and we could have worked with the group ring $\mathbb{F}_p(G_0/\mathrm{C}_{G_0}(M))$ instead of $\mathbb{Z}(G_0/A)$. In this way, one can show that G has at least $c^{n^{r/d'}}$ 2-step subnormal subgroups of index at most n, for all large n, where r (in general > 1) and d' (in general less than d) are appropriate invariants of G. For details, see [Segal & Shalev 1993]. We believe that in this form, the result obtained is sharp, in the sense that there exist metabelian groups G, with these invariants, for which $s_n(G)$ is also bounded *above* by $c_1^{n^{r/d'}}$ for some $c_1 > 1$; however, the only examples so far constructed have either $r = 1$ or $r = d - 1$ (for the former, see Section 3, below).

9.2 Residually nilpotent groups

Here we prove Theorem 9.1. The heart of the argument is similar to that in the metabelian case, but we shall need to go a little deeper into the structure of soluble groups of finite rank.

Let G be a finitely generated soluble group that is residually nilpotent, and suppose that G has infinite rank. We shall show that

$$s_n^{\lhd\lhd}(G) \geq c^{n^{1/d}} \tag{9.1}$$

for some $c > 1,\ d \in \mathbb{N}$ and all large n. This will imply Theorem 9.1, for if G is normal and of finite index m in a group G_1 we then have

$$s_n^{\lhd\lhd}(G_1) \geq c_1^{n^{1/d}}$$

for all large n, where $c_1 = c^{(2m)^{-1/d}} > 1$. The proof will in fact show that G has at least $c^{n^{1/d}}$ 2-step subnormal subgroups of index at most n, so we get the corresponding result for 3-step subnormal subgroups in G_1; however, a few small adjustments to the proof – left for the interested reader – will suffice to show that the subgroups to be counted can be taken 2-step subnormal in G_1.

We need an elementary lemma:

Lemma 9.2.1 *Let G be a residually nilpotent group. If A is a maximal abelian normal subgroup of G then G/A is residually nilpotent.*

Proof. Write $G_n = \gamma_n(G)$. Then

$$[G_nA, G_nA] \leq [G_n, G][A, A] = G_{n+1}$$

for each n. So if $B = \bigcap_{n=1}^{\infty}(G_nA)$ then

$$B' \leq \bigcap_{n=1}^{\infty} G_{n+1} = 1.$$

Thus B is an abelian normal subgroup of G containing A, and so $B = A$. The lemma follows since $\bigcap_{n=1}^{\infty} \gamma_n(G/A) = B/A$. ■

The proof now proceeds by induction on the derived length of the soluble group G. Let A be maximal among the abelian normal subgroups of G that contain the last non-trivial term of the derived series. The lemma ensures that then G/A is again residually nilpotent; and G/A has smaller derived length than G. So if G/A still has infinite rank, we may assume that (16.2) holds with G/A in place of G. The result now follows since $s_n^{\lhd\lhd}(G) \geq s_n^{\lhd\lhd}(G/A)$ for each n.

Henceforth, we may therefore assume that G/A *is a soluble group of finite rank*. We now separate two cases.

Case 1: Suppose that for every prime p, the pro-p completion $\widehat{G}_p$ of G has finite rank. Then Lemma 9 of the **Linearity conditions** window shows that G embeds in $\prod_{l\in\pi} \widehat{G}_l$ for some finite set π of primes. It follows that G is residually (finite nilpotent of rank $\leq r$) where $r = \max_{l\in\pi} \mathrm{rk}(\widehat{G}_l)$ is finite. Since G is also soluble, we may now deduce from Corollary 5 of the same window that G is virtually nilpotent-by-abelian. Since G has infinite rank, this implies that G has a virtually metabelian quotient of infinite rank ($\leadsto$ **Soluble groups**), and (16.2) now follows by the result of Section 9.1.

Case 2: For some prime p, the pro-p completion $\widehat{G}_p$ of G has infinite rank. Writing

$$G_n = \gamma_{n+1}(G)G^{p^n},$$

this means that $\mathrm{rk}(G/G_n)$ tends to ∞ as $n \to \infty$. Since G/A has finite rank, it follows that $\mathrm{rk}(A/(A \cap G_n))$ tends to ∞. But $A/(A \cap G_n)$ is an abelian p-group, so putting

$$A_n = [A, \underbrace{G, \ldots, G}_{n}]A^p \leq (A \cap G_n)A^p$$

we have

$$\mathrm{rk}(A/A_n) \geq \mathrm{rk}(A/(A \cap G_n)) \to \infty$$

as $n \to \infty$. Now it is clear that if $A_{n+1} = A_n$ for some n then the chain (A_i) is stationary from $i = n$ onwards; hence either A/A_n has infinite rank for some n, or else $A_{n+1} < A_n$ for all n. In either case, it follows that

$$\mathrm{rk}(A/A_n) \geq n$$

for all n.

Now fix $m \in \mathbb{N}$ for the moment and put $t = p^m$, $H = AG^{p^m}$. Since A/A_t is abelian of exponent p we see that $[A, H] \leq A_t$. It follows from the lemma to be proved below that there exists a normal subgroup S/A_t of H/A_t such that

$$S \cap A = A_t$$
$$|H : AS| \leq k$$

where $k \in \mathbb{N}$ depends only on the group G/A, not on m. Then $AS/S \cong A/A_t$ is an elementary abelian p-group of rank at least t, hence contains at least p^{t-1} subgroups of index p (each of which is normal in H, hence 2-step subnormal in G).

Let us denote by d the sum of the ranks of the (abelian) factors in the derived series of G/A. As G/H has exponent p^m we have $|G : H| \leq p^{md}$. Hence G has at least p^{t-1} 2-step subnormal subgroups of index at most $k \cdot p^{md+1}$.

Now put

$$c = p^{(kp^{d+1})^{-1/d}/2} > 1.$$

Given a large positive integer n, let $m \in \mathbb{N}$ satisfy

$$kp^{md+1} \leq n < kp^{(m+1)d+1}.$$

Then

$$\begin{aligned} n^{1/d} \log c &< (kp^{d+1})^{1/d} p^m \log c \\ &= \frac{1}{2} p^m \log p < (t-1) \log p \end{aligned}$$

where $t = p^m$. Thus G has at least $c^{n^{1/d}}$ 2-step subnormal subgroups of index at most n, and (16.2) follows.

The existence of the normal subgroup S of H is assured by the following lemma, which we apply to the group G/A_t; note that G/A is virtually torsion-free because it is finitely generated and residually nilpotent, hence residually finite (↬ **Soluble groups**).

Lemma 9.2.2 *Let G be a group and $A \leq H$ normal subgroups of G such that*
(i) G/A is soluble of finite rank and virtually torsion-free,
(ii) $A^p[A,H] = 1$, where p is a prime.
Then there exists $S \lhd H$ with $S \cap A = 1$ and $|H : AS| \leq k$, where k depends only on G/A.

Proof. The group G/A has normal subgroups $G_1/A > G_2/A$ such that G/G_1 is finite, G_1/G_2 is free abelian, and G_2/A is torsion-free nilpotent (↬ **Soluble groups**). Write $b-1$ for the nilpotency class of G_2/A, and let d be as defined above.

Since A is central in H, the group $G_2 \cap H$ is nilpotent of class at most b; this implies that every element of $S_1 := (G_2 \cap H)^{p^b}$ is the pth power of an element of $G_2 \cap H$ (a lemma of Mal'cev, see [Sg], Chapter 6 §B, Prop. 2). As G_2/A is torsion-free it follows that

$$S_1 \cap A \subseteq A^p = 1.$$

Now put

$$H_1 = \mathrm{C}_H((G_2 \cap H)/AS_1) \cap G_1.$$

Then $H_1/(G_2 \cap H_1)$ is free abelian and H_1/S_1 is nilpotent of class at most 3. It follows as above that every element of $S/S_1 := ({H_1}^{p^{3b}} S_1)/S_1$ is the p^bth power of an element of H_1/S_1, and hence that

$$S \cap (G_2 \cap H_1) \subseteq (G_2 \cap H_1)^{p^b} \subseteq S_1.$$

Therefore $S \cap A = 1$, and it remains to bound the index $|H : AS|$. We claim that $|H : AS| \leq k$ where $k = |G : G_1|\, p^{bd^2+3bd}$. Indeed, $|H : H \cap G_1| \leq |G : G_1|$. Next, the group $(H \cap G_1)/H_1$ acts faithfully on $(G_2 \cap H)/AS_1$; this has order at most p^{bd} and rank at most d, hence has at most p^{bd^2} automorphisms, which implies that $|H \cap G_1 : H_1| \leq p^{bd^2}$. Finally, H_1/AS has order at most p^{3bd}, and our claim follows. ■

9.3 Some finitely presented metabelian groups

In this section we construct, for each integer $d \geq 2$, a finitely presented metabelian group G having subgroup growth (and subnormal subgroup growth) of type $2^{n^{1/d}}$. This shows that Theorem 9.1 is best possible. Given any prime p, we can choose G so that its pro-p completion also has this growth type; thus taking $d = 2$, we obtain examples of finitely presented metabelian pro-p groups with growth type $2^{\sqrt{n}}$, which shows that Theorem 4.3 is also best possible.

Our construction is also interesting for a different reason. As we shall see in Chapter 13, the 'growth spectrum' of finitely generated groups in general essentially contains no gaps; that is, there is a continuous range of growth types between PSG (type n) and n^n; in particular, there is a continuum of distinct growth types. If we restrict attention to groups in any of the following classes, however – (a) finitely presented groups, (b) f.g. soluble groups, (c) f.g. pro-p

groups – the picture is dramatically different: only a countable family of growth types is known to occur, namely

- PSG (type n)
- finitely many 'particular' types, such as $n^{\log n}$ in pro-p groups, $n^{\log n/\log\log n}$ in arithmetic groups
- the sequence of types $2^{n^{1/d}}$ exhibited here, and the sequence $2^{n^{(d-1)/d}}$, obtained by B. Klopsch using a variation of the same construction.

One of the most challenging open problems is to discover whether there are any, or infinitely many, or uncountably many further growth types achieved by groups in classes (a), (b) and (c). (As there are only countably many isomorphism types of finitely presented groups, the third possibility is of course excluded in case (a); the same applies to the classes of finitely generated metabelian groups and finitely generated linear groups.)

The construction is as follows. We fix a prime p and an integer $d \geq 2$, and let

$$\Gamma = \langle x_1, \ldots, x_d \rangle$$

be a free abelian group of rank d. Choose distinct monic irreducible polynomials $f_i(X)$ $(i = 1, \ldots, d-1)$ of degree at least 2 over $\mathbb{F}_p$, write $R = \mathbb{F}_p\Gamma$ for the group ring and let P be the ideal of R generated by

$$\{f_i(x_d) - x_i \mid 1 \leq i \leq d-1\}.$$

Thus writing $x = x_d + P$ we have

$$R/P = \mathbb{F}_p[x][x^{-1},\, f_1(x)^{-1}, \ldots, f_{d-1}(x)^{-1}]. \tag{9.2}$$

The action of Γ by mutiplication on R makes R/P into a Γ-module M, and we now set

$$G = M \rtimes \Gamma.$$

Theorem 9.3.1 (i) *The group G is a $(d+1)$-generator finitely presented metabelian group. There exist constants b, $c > 1$ such that*
(ii)

$$b^{n^{1/d}} \leq s_n^{\lhd\lhd}(G) \leq s_n(G) \leq c^{n^{1/d}}$$

for all large n, and
(iii) *G has a normal subgroup K of finite index such that*

$$b^{n^{1/d}} \leq s_n(\widehat{K}_p) \leq c^{n^{1/d}}$$

for all large n.

Proof of the lower bounds The lower bound in (ii) is a special case of the result established in Section 1. For (iii), we choose a maximal ideal L/P of R/P and let K be the inverse image in G of

$$(1+L)\cap\Gamma.$$

Then the argument of Section 1 shows that for large values of n, K has at least $b^{n^{1/d}}$ two-step subnormal subgroups of p-power index at most n, where $b>1$ is a suitable constant. The same therefore holds for $\widehat{K}_p$.

The **proof of the upper bounds** is a little longer, and more interesting. The key step is the following lemma, where we write

$$\mu=(d!)^{1/d}\cdot\max_{1\le j<d}\deg f_j.$$

Lemma 9.3.2 *Let Δ be a subgroup of finite index in Γ and let N be an $\mathbb{F}_p\Gamma$-submodule of finite index in M. Then*

$$d_{\mathbb{F}_p\Delta}(M/N)\le\mu\,|\Gamma:\Delta|^{1/d}.$$

Here, $d_{\mathbb{F}_p\Delta}(M/N)$ denotes the number of generators required by M/N as an $\mathbb{F}_p\Delta$-module. Before proving this, let us deduce the upper bound in (ii). This will also imply the upper bound in (iii) (replacing c by a larger constant if necessary).

To each subgroup H of index n in G we associate

$$D=D(H)=H\cap M,$$
$$\Delta=\Delta(H)=(MH)\cap\Gamma.$$

Then D is an $\mathbb{F}_p\Delta$-submodule of finite index $m=p^l$, say, in M, and $|\Gamma:\Delta|=n/m$. Also H/D is a complement to M/D in $M\Delta/D$; so the number of possibilities for H, given the pair $(\Delta,\,D)$, is equal to

$$|\mathrm{Der}(\Delta,M/D)|\le m^d$$

since Δ is a d-generator group.

Note that D contains the $\mathbb{F}_p\Gamma$-submodule $M(n)=M\cap G(n)$ where $G(n)$ is the intersection of all subgroups of index n in G; as G is finitely generated, $G(n)$ has finite index in G and so $M(n)$ has finite index in M.

Now suppose Δ is given, and put $r=\left[\mu t^{1/d}\right]$ where $t=|\Gamma:\Delta|$. By the lemma, $M/M(n)$ is an r-generator $\mathbb{F}_p\Delta$-module. The number of isomorphism types of $\mathbb{F}_p\Delta$-modules of dimension l is at most

$$|\mathrm{Hom}(\Delta,\mathrm{GL}_l(\mathbb{F}_p))|<p^{dl^2},$$

hence the number of $\mathbb{F}_p\Delta$-submodules of codimension l in the free $\mathbb{F}_p\Delta$-module $(\mathbb{F}_p\Delta)^r$ is at most $p^{dl^2}\cdot p^{lr}$. It follows that the number of possibilities for D is at most

$$p^{dl^2+lr}=m^{d\log_p m+\mu t^{1/d}}.$$

The number of possibilities for Δ is $a_t(\Gamma) \leq n^d$. Putting everything together we obtain

$$\begin{aligned} a_n(G) &\leq \sum_{mt=n} m^d \cdot n^d \cdot m^{d \log_p m + \mu t^{1/d}} \\ &\leq n^{(2+\log n)d} \cdot c_1^{n^{1/d}} \end{aligned}$$

where c_1 is a suitable constant; we leave it as an exercise for the reader to verify that

$$mt = n \Longrightarrow m^{t^{1/d}} \leq \sigma^{n^{1/d}}$$

where $\sigma = \mathrm{e}^{d/\mathrm{e}}$ (e the base of the natural logarithms). It follows that $s_n(G) \leq c^{n^{1/d}}$ for all large n if c is any constant strictly larger than c_1.

Proof of Lemma 9.3.2 To begin with, identify Γ with $\mathbb{Z}^{(d)}$ using the basis $x_1, \ldots, x_d$. Then Δ is a lattice in $\mathbb{R}^{(d)}$ with determinant $|\Gamma : \Delta|$. It follows by Minkowski's theorem (see [HW], Theorem 447) that there exist integers $a_1, \ldots, a_d$ such that

$$\begin{aligned} \sum_{i=1}^{d} |a_i| &\leq (d! \, |\Gamma : \Delta|)^{1/d}, \\ 1 \neq \prod x_i^{a_i} &= y \in \Delta. \end{aligned}$$

Suppose for clarity that $a_1, \ldots, a_s$ are non-negative and $a_{s+1}, \ldots, a_d$ are negative. Write $x = f_d(x) = x_d$. Then in the ring $R = \mathbb{F}_p\Gamma$ we have

$$\prod_{i=1}^{s} f_i(x)^{a_i} \equiv y \cdot \prod_{i=s+1}^{d} f_i(x)^{|a_i|} \pmod{P}. \tag{9.3}$$

Now N is an R-submodule of finite index in $M = R/P$, so $\overline{M} = M/N$ is a finite ring image of R/P and from (9.2) we have $\overline{M} = \mathbb{F}_p[\overline{x}]$ where $\overline{x}$ denotes the image of x in $\overline{M}$. Suppose L is a maximal ideal of $\mathbb{F}_p\Delta$ such that $\overline{M}L = 0$. Then (9.3) shows that $\overline{x}$ satisfies an equation of degree at most $q = \sum_{i=1}^{d} |a_i| \deg(f_i)$ over the field $F = (\mathbb{F}_p\Delta)/L$, and hence that $\dim_F(\overline{M}) \leq q$.

In general, we may deduce that $\overline{M}/\overline{M}L$ can be generated as an $\mathbb{F}_p\Delta$-module by q elements, for every maximal ideal L of $\mathbb{F}_p\Delta$. This implies that the same holds for $\overline{M}/\overline{M}L^n$ for every n, and then by the Chinese Remainder Theorem that $d_{\mathbb{F}_p\Delta}(\overline{M}) \leq q$.

The lemma follows since

$$\begin{aligned} q = \sum_{i=1}^{d} |a_i| \deg(f_i) &\leq (d! \, |\Gamma : \Delta|)^{1/d} \cdot \max_i \deg(f_i) \\ &= \mu \, |\Gamma : \Delta|^{1/d}. \end{aligned}$$

To complete the proof of Theorem 9.3.1, it remains only to show that G has a finite presentation on $d+1$ generators. Denote by u the element of G corresponding to $1 \in R/P$, so u generates M as a Γ-module, and put $x = x_d$. Thus

$$G = \langle u, x, x_1, \ldots, x_{d-1} \rangle .$$

We claim that the following relations present G on these generators:

$$\begin{aligned} u^p &= 1 \\ [x, x_j] &= 1 \qquad (1 \le j \le d-1) \\ [x_i, x_j] &= 1 \qquad (1 \le i < j \le d-1) \\ u^{x_i} &= u^{f_i(x)} \qquad (1 \le i \le d-1) \\ [u, u^{x^n}] &= 1 \qquad (1 \le n \le \deg f_1) \end{aligned} \tag{9.4}$$

where $u^{f(x)} = \prod_{n=0}^{h} (u^{x^n})^{c_n}$ for a polynomial $f(X) = \sum_{n=0}^{h} c_n X^n$.

It is straightforward to verify that these relations together with the infinitely many additional relations

$$[u, u^{x^n}] = 1 \qquad (n > \deg f_1)$$

do give a presentation for G; it remains to show is that these additional relations are consequences of (9.4). So let us assume (9.4), and suppose inductively that $[u, u^{x^n}] = 1$ for $1 \le n \le k$ where $k \ge h = \deg f_1$. Write

$$f_1(X) = c_h X^h + c_{h-1} X^{h-1} + \cdots + c_1 X + c_0.$$

Then

$$u^{x_1} = \prod_{n=0}^{h} (u^{x^n})^{c_n}$$

commutes with

$$u^{x^{k+1-h} x_1} = \prod_{n=0}^{h} (u^{x^{n+k+1-h}})^{c_n}.$$

Since $[u^{x^i}, u^{x^j}] = 1$ whenever $|i-j| \le k$, it follows that u^{c_0} commutes with $(u^{x^{k+1}})^{c_h}$. As $c_h = 1$ and c_0 is a non-zero element of $\mathbb{F}_p$ this implies that $[u, u^{x^{k+1}}] = 1$. Our claim follows by induction, and the proof of Theorem 9.3.1 is complete.

9.4 Normal subgroup growth in metabelian groups

In this section we discuss Theorems 9.2 and 9.3. Throughout this section, G denotes *either* a finitely generated metabelian group (*case 1)*, *or* a finitely generated metabelian pro-p group (*case 2*).

Let $G^{ab} = G/G'$ be the abelianisation of G, and let

$$R = \mathbb{Z}\left[G^{ab}\right] \quad \text{in case 1}$$
$$R = \mathbb{Z}_p\left[\left[G^{ab}\right]\right] \quad \text{in case 2}$$

(in case 2, R is the 'completed group algebra' of the pro-p group G^{ab}, see [DDMS], Chapter 7). The conjugation action of G on the derived group G' (which is closed in case 2) makes G' into a Noetherian R-module that we denote by M. We now define a structural invariant of G by setting

$$\kappa(G) = \mathrm{Dim}(R/\mathrm{ann}_R(M))$$

(here Dim denotes the *Krull dimension* of a ring).

Theorem 9.3 *G has polynomial normal subgroup growth if and only if $\kappa(G) \leq 2$.*

In general, as remarked in the preceding chapter, it seems difficult to relate the normal subgroup growth of a group with that of a finite-index subgroup (in contrast to the question of subgroup growth). In the metabelian case, however, we can deduce

Corollary 9.4.1 *If H is a subgroup of finite index in G then H has polynomial normal subgroup growth if and only if G does.*

This follows from Theorem 9.3 together with the easily verified fact that $\kappa(H) = \kappa(G)$.

Theorem 9.2 *Suppose that $\kappa(G) = k \geq 1$. Then there exist positive constants a and b such that*

$$n^{b(\log n)^{1-2/k}} \leq s_n^{\triangleleft}(G) \leq n^{a(\log n)^{1-1/k}}$$

for all large n.

It must be admitted that the second theorem is not quite satisfactory: it should be possible to obtain the *same* exponent for $\log n$ on both sides of the inequality, but this is still an open problem. In any case, since it is easy to construct metabelian groups G where $\kappa(G)$ takes any positive integral value, we see that there are infinitely many distinct types of normal subgroup growth, both in f.g. metabelian groups and in f.g. metabelian pro-p groups.

Example Let p be a prime. Then the wreath products

$$G = C_p \wr \mathbb{Z}^{(k)}, \; H = \mathbb{Z} \wr \mathbb{Z}^{(k-1)}$$

are metabelian groups with $\kappa(G) = \kappa(H) = \kappa(\widehat{G}_p) = \kappa(\widehat{H}_p) = k$ (provided $k \geq 1$ for G, $k \geq 2$ for H).

Both theorems are reduced to ring theory by means of the next lemma, where $s_n(M)$ denotes the number of R-submodules of index at most n in M:

Lemma 9.4.2 *There exist positive constants h, f and g such that*

$$s_n(M) \leq s^{\lhd}_{n^h f}(G)$$
$$s^{\lhd}_n(G) \leq n^g s_n(M)$$

for all n.

Proof. The abelian group $\Gamma = G^{ab}$ contains a torsion-free subgroup Γ_0 of finite index f, say. Let r denote the rank of Γ and m the number of generators required by M as an R-module. Put $h = m + 2r + 1$.

To each submodule N of finite index in M we associate a normal subgroup N^* of G as follows. Let e be the exponent of M/N, let

$$C/G' = \mathrm{C}_{\Gamma_0}(M/N),$$

and put

$$N^* = C^{e^2} N.$$

It is then easy to verify that $N^* \cap G' = N$, so the mapping $N \mapsto N^*$ is one-to-one; and

$$\begin{aligned} |G : N^*| &= |\Gamma : \Gamma_0| \cdot |\Gamma_0 : C| \cdot \left|C : C^{e^2} G'\right| \cdot \left|C^{e^2} G' : C^{e^2} N\right| \\ &\leq f \cdot n^m \cdot e^{2r} \cdot n \\ &\leq n^h f \end{aligned}$$

since $\Gamma_0/C \leq \mathrm{Aut}_R(M/N)$ which has order at most n^m, and $e \leq n$. This implies the first claim.

For the second claim, we associate to each normal subgroup N of finite n in G the pair $(K = G'N,\ D = G' \cap N)$. Given $|G : K| = q$ and $|M : D| = s$, the number of possibilities for D is at most $s_s(M)$, and that for K is at most $a_q(G^{ab}) \leq q^r$. Moreover, N/D is a complement for M/D in K/D, so the number of possibilities for N is at most

$$|\mathrm{Hom}(K/M, M/D)| \leq s^r.$$

It follows that

$$s^{\lhd}_n(G) \leq \sum_{qs \leq n} s_s(M) \cdot q^r \cdot s^r \leq n^{r+1} s_n(M).$$

■

Theorems 9.3 and 9.2 now follow from the corresponding results in ring theory. For these, R can be either a finitely generated commutative ring or a commutative local ring with finite residue field, M is a finitely generated R-module, and $\mathrm{Dim}(M)$ denotes the Krull dimension of $R/\mathrm{ann}_R(M)$.

Theorem 9.4.3 (i) $s_n(M)$ *is bounded above by a polynomial in* n *if and only if* $\mathrm{Dim}(M) \leq 2$.

(ii) *If* $\mathrm{Dim}(M) = k \geq 1$ *then there exist positive constants* a *and* b *such that*

$$n^{b(\log n)^{1-2/k}} \leq s_n(M) \leq n^{a(\log n)^{1-1/k}}$$

for all large n.

Let us sketch the proof of the lower bound in (ii); this also implies the 'only if' direction on (i). Suppose, then , that M is a finitely generated R-module. We may assume that $\mathrm{ann}_R(M) = 0$ and that $\mathrm{Dim}(R) = k \geq 1$. If R is not already a local ring, we may localize at a maximal ideal of height k and so reduce to the case where R is local, with maximal ideal $\mathfrak{q}$; let $F = R/\mathfrak{q}$ be the (finite) residue field. According to the Hilbert-Samuel theory (see e.g. [E], §12.1 and Lemma 1.12), there exist polynomials $P(X)$, $\overline{P}(X)$ of degrees $k-1$, k respectively, and positive constants α and β, such that

$$\dim_F(M\mathfrak{q}^m/M\mathfrak{q}^{m+1}) = P(m) \geq \alpha m^{k-1}$$
$$\sum_{j=0}^{m} \dim_F(M\mathfrak{q}^j/M\mathfrak{q}^{j+1}) = \overline{P}(m+1) \leq \beta m^k$$

for all sufficiently large integers m. Hence if $|F| = q$ then for large m, $M\mathfrak{q}^m/M\mathfrak{q}^{m+1}$ contains at least $q^{[(\alpha m^{k-1})^2/4]}$ distinct F-subspaces. Each of these corresponds to an R-submodule of index at most $q^{\beta m^k}$ in M.

Now let n be a large positive integer. There exists m such that

$$\beta m^k \leq \log_q n < \beta(m+1)^k \leq 2^k \beta m^k,$$

and then

$$\begin{aligned} \log_q(s_n(M)) &\geq [(am^{k-1})^2/4] \\ &> \gamma(\log_q n)^{2-2/k} \end{aligned}$$

where $\gamma > 0$ is a suitable constant. Thus $s_n(M) \geq n^{b(\log n)^{1-2/k}}$ where $b = \gamma/\log q$.

The *upper bounds* in theorem 9.4.3 are harder to prove; in case (ii) they depend on estimates for the number of generators needed by ideals of finite index in local rings, due to [Boratynski, Eisenbud & Rees 1979]. For details see [Segal 1997].

Notes

The original PSG Theorem for residually nilpotent soluble groups appeared in [**Segal 1986**$_a$]; the sharper Theorem 9.1 was announced in [**Mann & Segal 1996**].

The results on subgroup growth of metabelian groups in Sections 1 and 3 are from [**Segal & Shalev 1993**]. **Benjamin Klopsch** (in unpublished work) has modified the construction of Section 3 to obtain metabelian groups with subgroup growth of type $2^{n^{1-1/d}}$ for every positive integer d. We conjecture that $2^{n^{\varepsilon}}$ should occur for every rational $\varepsilon \in (0,1)$, but this remains to be established.

The results on normal subgroup growth of metabelian groups are from [**Segal 1997**].

The subgroup growth of finitely generated soluble groups is discussed in [**Segal (a)**] and [**Segal 2000**$_b$]. The latter paper states the conjecture that *if a finitely generated soluble group has finite upper p-rank for every prime p, then it has finite rank*. In the former paper it is shown that if this conjecture is true, then there is a *gap* in the possible subgroup growth types of f.g. soluble groups, between PSG and type $n^{\log n}$. The bulk of the second paper is devoted to establishing the conjecture in a special case: namely for f.g. groups G that have a chain of normal subgroups $1 < A \leq K < G$ such that *A is abelian and finitely generated as a G/A-module, K/A is abelian of finite rank, and G/K is polycyclic*. It follows that there is a 'subgroup growth gap' for groups in this class (which includes in particular all soluble groups of derived length 3 with the maximal condition on normal subgroups). While this result is too special to be of great interest, the proof introduces new methods; these may lead to further progress on this problem, as well as to other applications in the theory of f.g. soluble groups.

Chapter 10

Profinite groups with polynomial subgroup growth

We showed in Chapter 5 that the finitely generated, residually finite groups with polynomial subgroup growth are just those that are virtually soluble of finite rank. The proof involved two kinds of argument: a 'local' part, analysing the finite quotients of the group, and a 'global' part which involved representing the group as a linear group. The latter depended crucially on the group being finitely generated, and the result is not true without that hypothesis. However, it makes sense to ask: can one characterize the general PSG group, including those that are not finitely generated? The answer is a qualified 'yes', in the sense that we can describe its profinite completion.

In this chapter, we determine precisely which profinite groups have PSG. To begin with, let us consider some examples. As mentioned in the introduction to Chapter 5, we already know that soluble groups of finite rank, and hence also their profinite completions, are among the PSG groups. More generally, we shall establish

Theorem 10.1 *Every profinite group of finite rank has* PSG.

In terms of abstract group theory, this says that *every group of finite upper rank has PSG.*

What about the other examples mentioned in Chapter 5, namely infinite products of finite simple groups? On studying such examples, it becomes clear that a product of finite simple groups has 'few' subgroups of finite index if there is minimal 'overlapping' between the orders of the simple factors: if many of the factors have order divisible by a prime p, for example, then their direct product will contain a large elementary abelian p-subgroup which in turn has many subgroups relative to its order; and knowing enough about the structure

of finite simple groups one can see that this is essentially the main obstacle to the group having PSG. To formalize these vague ideas, we make the following

Definition Let N be a family of natural numbers. Then N satisfies the *gcd condition* if there exists a positive number γ such that for every finite subfamily F of N,

$$\prod_{x\in F}\prod_{y\in F}\gcd(x,y)\leq\left(\prod_{x\in F}x\right)^{\gamma}.$$

Our second family of examples is provided by

Theorem 10.2 *Let (T_i) be a sequence of finite nonabelian simple groups of bounded ranks, each occurring with bounded multiplicity, and suppose that the sequence of orders $(|T_i|)$ satisfies the gcd condition. Then the profinite group*

$$\prod T_i$$

has PSG.

Some examples of this type are exhibited at the end of Section 10.3, below.

Now we can ask the question: do the two preceding theorems between them provide all possible profinite PSG groups? Liberally interpreted, the answer turns out be 'yes'. The complete characterisation of profinite groups with PSG is given in the following theorem, whose terminology is explained below:

Theorem 10.3 (The Profinite PSG Theorem) *Let G be a profinite group. Then G has* PSG *if and only if G has closed normal subgroups $S\leq G_1$ such that S is prosoluble of finite rank, G/G_1 is finite, and G_1/S is a quasi-semisimple group of bounded type such that $\mathcal{N}(G_1/S)$ satisfies the gcd condition.*

Here, a profinite group Q is said to be *quasi-semisimple of bounded type* if Q is perfect (equal to the closure of its derived group) and $Q/\mathrm{Z}(Q)\cong\prod T_i$ where (T_i) is a sequence of finite groups of bounded rank, each occurring with bounded multiplicity, and each T_i is a simple group of Lie type; and $\mathcal{N}(Q)$ denotes the numerical sequence $(|T_i|)$.

It is worth noting that the simple groups T_i have bounded ranks if and only if (1) *they are of bounded Lie rank* and (2) *the underlying fields have bounded degree over their prime fields*. This follows from the classification of finite simple groups, and it means that in principle, we can recognise 'on sight' whether a group is quasi-semisimple of bounded type. (The groups we term 'quasi-semisimple' are more usually called 'semisimple'; we use the longer term to emphasize the possible presence of a non-trivial centre, which in the present context may be of infinite rank.) Of course Theorem 10.3 includes Theorem 10.2 as a special case. That it also generalizes Theorem 10.1 is less obvious: this follows from the profinite version of Theorem 5.2, namely the fact that *every profinite group of finite rank is virtually prosoluble* (see Section 1 below).

This theorem has two remarkable consequences.

Corollary 10.4 *The class of all* PSG *groups is extension-closed.*

It is striking that (at present) no direct proof of this simple statement is known.

Corollary 10.5 *If G is a profinite group with* PSG *then every (topologically) finitely generated closed subgroup of G has* PSG.

The restriction to finitely generated subgroups in this corollary is certainly necessary, as we shall see in a moment. It is worth remarking that Corollary 10.5 is a special property of *polynomial* subgroup growth; for example, the pro-p group $C_p \wr \mathbb{Z}_p$ has exponential subgroup growth type, but embeds as a closed subgroup in $\mathrm{SL}_2(\mathbb{F}_p[[t]])$ which has the much slower growth type $n^{\log n}$ (see Chapter 4).

Another result that may be regarded as a consequence of Theorem 10.3 is the following; though in fact it has a surprisingly simple probabilistic proof, given in Chapter 11:

Theorem 10.6 *Every profinite group with* PSG *is finitely generated.*

The proof of Theorem 10.3 is long, and we shall omit some of the more technical details. For these, and the proofs of the two corollaries, the reader is referred to [Segal & Shalev 1997].

Now let us outline the broad structure of the argument. As in Chapter 5, we work mostly with the concept of *weak PSG* (wPSG); whereas before this was merely a flourish, it seems to be an essential tool for the considerations of this chapter. Recall that G has wPSG if there exists α such that

$$s(\overline{G}) \leq \left|\overline{G}\right|^{\alpha}$$

for every finite quotient $\overline{G}$ of G.

The first stage in the proof of Theorem 10.3, given in Section 10.2, is to show that every profinite group with weak PSG is virtually an extension of a prosoluble group of finite rank by a quasi-semisimple group of bounded type. Having established this, we are left with three (more or less logically independent) tasks:

- the characterisation of quasi-semisimple groups with wPSG (in Section 10.3);
- proving that every extension of a prosoluble group of finite rank by a group with wPSG has wPSG, a special case of Corollary 10.4 (in Section 10.4);
- proving that wPSG is equivalent to PSG (in Section 10.5).

Most theorems of this chapter are initially proved in the form of results about finite groups, saying that certain structural invariants of a finite group G can be effectively bounded in terms of $\alpha^\dagger(G)$, the 'exponent of weak PSG' defined in Chapter 5. This is true in particular of the invariant $\alpha^*(G)$ defined as follows (we also recall the definition of $\alpha^\dagger(G)$):

Definition

$$\alpha^*(G) = \inf\{\alpha > 0 : s_n(G) \leq n^\alpha \text{ for all } n\}$$
$$\alpha^\dagger(G) = \inf\left\{\alpha > 0 : s(\overline{G}) \leq \left|\overline{G}\right|^\alpha \text{ for every finite quotient } \overline{G} \text{ of } G\right\},$$

where conventionally $\inf \emptyset = \infty$.

Thus G has PSG if $\alpha^*(G)$ is finite, while G has weak PSG if $\alpha^\dagger(G)$ is finite.

We shall write f, f_1 etc. to denote certain functions, whose existence is supposed to be asserted when they occur in a statement (the same symbol may denote different functions in different sections).

10.1 Upper rank

Theorem 10.1 follows directly from part (ii) of

Proposition 10.1.1 *(i) If G is a prosoluble group then*

$$\alpha^*(G) \leq \mathrm{rk}(G) + 2.$$

(ii) There is a function $f : \mathbb{N} \to \mathbb{N}$ such that

$$\alpha^*(G) \leq f(\mathrm{rk}(G))$$

for all profinite groups G.

Proof. Since both sides of the stated inequalities depend only on the finite quotients of G, we may assume that G is a finite group.

(i) This is merely a slightly weaker version of Corollary 1.7.2.

(ii) Put $r = \mathrm{rk}(G)$. Suppose to begin with that G has no non-trivial soluble normal subgroup, and put

$$K = \bigcap_{M \in \mathcal{M}} M \cdot \mathrm{C}_G(M),$$

where $\mathcal{M}$ denotes the set of all minimal normal subgroups of G. Now if $M \in \mathcal{M}$ then $M \cong S^{(m)}$, where S is a finite simple group of rank at most r and $m \leq r$ because S has even order, whence $S^{(m)}$ contains an elementary abelian 2-subgroup of rank m. The outer automorphism group of M embeds in $\mathrm{Out}(S) \wr \mathrm{Sym}(m)$, and $|\mathrm{Out}(S)|$ is bounded by some function of r (↬ **Finite simple groups**); therefore $|\mathrm{Out}(M)| \leq f_1(r)$, and it follows that $|G : M\mathrm{C}_G(M)| \leq f_1(r)$. Now G is a quotient of the free group F on r generators; F has only a finite number of normal subgroups of index $f_1(r)$, and their intersection therefore has finite index, $f_2(r)$ say, in F. It follows that

$$|G : K| \leq f_2(r).$$

Now suppose that $M \in \mathcal{M}$ is contained in K. Then

$$K = K \cap M\mathrm{C}_G(M) = M \times \mathrm{C}_K(M)$$

(because $M \cap \mathrm{C}_K(M)$ is an abelian normal subgroup of G). It follows that $K = M_1 \times \cdots \times M_k$ for some $M_1, \ldots, M_k \in \mathcal{M}$, and hence that K is a direct product of non-abelian simple groups. Now we apply Corollary 1.9.2 to deduce that

$$s_n(K) \leq n^{f_3(r)}.$$

With Proposition 1.3.2(ii) this gives

$$s_n(G) \leq n^{f_3(r)+f_2(r)}$$

for all n.

Now consider the general case, and let R denote the soluble radical of G. The special case above gives $s_n(G/R) \leq n^{f_3(r)+f_2(r)}$, and from part (i) we have $s_n(R) \leq n^{2+r}$ for all n. We conclude by Proposition 1.3.2(i) that

$$s_n(G) \leq n^{f(r)}$$

for all n, where

$$f(r) = (2 + r) + (f_3(r) + f_2(r)) + r.$$

This completes the proof. ■

Part (ii) depends implicitly on CFSG. A more elementary derivation of Theorem 10.1 goes by way of Tate's theorem (↬ **Finite group theory**), which implies

Theorem 10.1.2 *Let G be a profinite group whose Sylow pro-2 subgroups are finitely generated. Then G is virtually prosoluble.*

Recall that this depends on the Odd Order Theorem but not CFSG. This reduces Theorem 10.1 to an application of part (i) of Proposition 10.1.1. It should be noted, however, that this is weaker than Proposition 10.1.1 (ii), since the proof of Theorem 5.5.1 does *not* provide an effective bound for the index of a prosoluble subgroup.

10.2 Profinite groups with wPSG: structure

In this section we elucidate the structure of the general profinite group with weak PSG. This will enable us, In Section 10.5, to show finally that weak PSG is the same as PSG. It also prepares the ground for the exact characterisation of these groups.

Throughout this section, G will denote a profinite group with wPSG, and $\alpha = \alpha^\dagger(G)$. We begin with two elementary lemmas.

Lemma 10.2.1 *Let $K \lhd_o G$ with $|G:K| = m < \infty$. Then*

$$\alpha^\dagger(G) - \log m \leq \alpha^\dagger(K) \leq (1+\log m)\alpha^\dagger(G)$$
$$\alpha^*(G) \leq \alpha^*(K) + m.$$

Proof. As usual we may assume that G is finite. Proposition 1.3.2(iii) shows that

$$s(G) \leq s(K)\,|G|^{\mathrm{rk}(G/K)}\,.$$

Since $\mathrm{rk}(G/K) \leq \log m$ this gives

$$s(G) \leq |K|^{\alpha^\dagger(K)}\,|G|^{\log m} \leq |G|^{\alpha^\dagger(K)+\log m}\,,$$

whence the first inequality. For the second inequality, note that

$$\begin{aligned} s(K) \leq s(G) &\leq |G|^{\alpha^\dagger(G)} \\ &= (m\,|K|)^{\alpha^\dagger(G)} \leq |K|^{(1+\log m)\alpha^\dagger(G)} \end{aligned}$$

provided $|K| \geq 2$. The final inequality is immediate from Proposition 1.3.2(ii). ■

Lemma 10.2.2 *Put*

$$G(n) = \bigcap \{N \lhd_o G \mid |G:N| \ \textit{divides } n\}\,.$$

Then

$$|G:G(n)| \leq f(\alpha, n).$$

Proof. If we can prove this under the assumption that $G/G(n)$ is finite, it will follow in general. So let us make this assumption; then replacing G by $G/G(n)$ we may suppose that G is finite and that $G(n) = 1$. Now choose normal subgroups $K_1, \ldots, K_t$ of index dividing n in G so that $K_1 \cap \ldots \cap K_t = 1$ and t is minimal, and put

$$L_i = \bigcap_{j \neq i} K_j.$$

Then $|L_i|$ divides $|G:K_i|$ and hence divides n.

Now suppose that n is divisible by $\mu = \mu(n)$ distinct primes. Then at least one prime, p say, must divide $|L_i|$ for at least $[t/\mu]$ distinct values of i. Since the groups L_i generate their direct product in G it follows that G contains an elementary abelian p-subgroup of rank at least $[t/\mu]$. Consequently

$$p^{\left[[t/\mu]^2/4\right]} \leq s(G) \leq |G|^\alpha \leq n^{t\alpha}.$$

This implies (crudely) that

$$t \leq 8\mu^2 \alpha \log n$$

(since $p \geq 2$). As $|G| \leq n^t$ this shows that we can take

$$f(\alpha, n) = n^{8\mu(n)^2 \alpha \log n}.$$

■

Now we recall some notation and a result from Section 5.3.

$\mathcal{S}_0$ denotes *the set of sporadic finite simple groups*

$\mathcal{A}(\beta)$ denotes *the set of alternating groups of degree at least 5 and at most* β

$\mathcal{X}(\beta)$ denotes *the set of all simple groups of Lie type* $X_n^*(\mathbb{F}_{p^e})$ *where the Lie rank* n *and the field degree* e *are at most* β.

For any group G, $\beta(G)$ denotes the least natural number β such that every non-abelian upper composition factor of G belongs to $\mathcal{S}_0 \cup \mathcal{A}(\beta) \cup \mathcal{X}(\beta)$ (or ∞ if there is no such β); and $w(G)$ denotes the supremum of all natural numbers m such that some finite quotient of G hs a normal subgroup isomorphic to $S^{(m)}$ for some non-abelian simple group S.

Proposition 5.3.4 asserts that *if* G *has wPSG, then both* $\beta(G) = \beta$ *and* $w(G) = w$ *are finite, and bounded by some function of* $\alpha^\dagger(G) = \alpha$. This fact is the key to our first major structural observation:

Proposition 10.2.3 *G has closed normal subgroups $R \leq G_0$ such that R is prosoluble, G/G_0 is finite (of order bounded by some function of α), and*

$$G_0/R \cong \prod_{T \in \mathcal{T}} T^{(m(T))},$$

where $\mathcal{T} \subseteq \mathcal{X}(\beta)$ and $m(T) \leq w$ for each $T \in \mathcal{T}$.

Proof. This is very similar to the proof of Proposition 10.1.1(ii). Let M be a non-abelian upper chief factor of G. Then $M \cong S^{(m)}$ where $m \leq w$ and $S \in \mathcal{S}_0 \cup \mathcal{A}(\beta) \cup \mathcal{X}(\beta)$. If $S \in \mathcal{S}_0 \cup \mathcal{A}(\beta)$ put $G_M = \mathrm{C}_G(M)$, while if $S \in \mathcal{X}(\beta)$ let G_M be the kernel of the natural map $G \to \mathrm{Out}(M)$. Then $|G : G_M| \leq n$ where n is bounded by some function of β and w; this is clear in the first case, and in the second case follows as in the proof of Proposition 10.1.1. So putting

$$G_0 = \bigcap G_M$$

where M ranges over all the non-abelian upper chief factors of G, we see by Lemma 10.2.2 that $|G : G_0|$ is finite and bounded by some function of α.

For each $N \lhd_o G$ with $N \leq G_0$, let R_N/N be the maximal soluble normal subgroup of G_0/N, and put

$$R = \bigcap \{R_N \mid G_0 \geq N \lhd_o G\}.$$

Then R is a closed, prosoluble normal subgroup of G contained in G_0, and

$$G_0/R \cong \varprojlim G_0/R_N.$$

The proposition will therefore follow if we can show that, for each $N \lhd_o G$ with $N \leq G_0$, the group G_0/R_N is a direct product of simple groups belonging to $\mathcal{X}(\beta)$.

So replacing G by G/R_N and changing notation, we may as well assume that G *is finite* and that G_0 *contains no non-identity soluble normal subgroup of* G. Now let K be the product of all minimal normal subgroups of G contained in G_0. Each of these minimal normal subgroups is a non-abelian upper chief factor of G, so the definition of G_0 ensures that $G_0 = K\mathrm{C}_{G_0}(K)$; and $K \cap \mathrm{C}_{G_0}(K) = 1$. As $\mathrm{C}_{G_0}(K) \lhd G$ it follows that $\mathrm{C}_{G_0}(K) = 1$ and hence that $G_0 = K$, a direct product of simple groups in $\mathcal{S}_0 \cup \mathcal{A}(\beta) \cup \mathcal{X}(\beta)$. However, any chief factor of G which is a product of groups in $\mathcal{S}_0 \cup \mathcal{A}(\beta)$ is centralized by G_0, hence cannot lie inside K; hence G_0 is a product of groups in $\mathcal{X}(\beta)$ as required. ■

Now Lemma 10.2.1 shows that G_0 has wPSG, and that $\alpha^\dagger(G_0)$ is bounded by some function of $\alpha^\dagger(G)$ and $|G : G_0|$; to simplify notation, we may as well replace G by G_0 and so assume in the following discussion that G has a closed prosoluble normal subgroup R such that G/R is a Cartesian product of simple groups in $\mathcal{X}(\beta)$. Can we now deduce that the prosoluble group R has finite rank? Unfortunately things are not quite that simple, as we shall see in Section 10.3. The correct statement is given in the following proposition.

Proposition 10.2.4 *The group* $\overline{[R,G]}$ *has finite rank, bounded by a function of* α.

Here, $\overline{[R,G]}$ denotes the closure in R of the subgroup $[R,G]$.

Proof. This is an elaboration of the proof of Proposition 5.4.2. In that proposition, the hypothesis of solubility was used essentially in bounding the order of a completely reducible linear group. Although we cannot invoke this here, we do know that G has restricted composition factors, and fortunately, thanks to the linear version of the theorem of Babai, Cameron and Pálfy, that suffices to provide a similar bound at the corresponding point in the argument.

As in Proposition 5.4.2, we may assume that G is finite and that p is a prime such that $O_{p'}(G) = 1$, and have to show that $r_p([R,G])$ is bounded in terms of α. Note that R is now the maximal soluble normal subgroup of G and that G/R is a direct product of simple groups belonging to $\mathcal{X}(\beta)$.

Let $E = E(G)$ be the subgroup generated by all the quasi-simple subnormal subgroups of G. Recall (↬ **Finite group theory**) that the *generalized Fitting subgroup*

$$F^*(G) = \mathrm{Fit}(G)E(G)$$

has the property $\mathrm{C}_G(F^*(G)) = \mathrm{Z}(F^*(G))$. We also need the fact that

$$\mathrm{C}_G(E) = \mathrm{C}_G(E/\mathrm{Z}(E)) \geq R.$$

Let us suppose to begin with that

$$E(G) = O_{p'}(G) = 1.$$

Then $O_p(G) = \mathrm{Fit}(G) = F^*(G) = F$, say. We now repeat the proof of Proposition 5.4.2, with just one change: the derivation of the inequality $|G : F| \leq p^{3d}$, where $d = \dim_{\mathbb{F}_p}(V)$ and V denotes the direct sum of the $\mathbb{F}_pG$-composition factors of $F/F'F^p$, depended on the solubility of G; instead of the Pálfy/Wolf theorem we now quote Theorem 4 of the **Permutation groups** window, which gives instead

$$|G : F| \leq p^{hd},$$

where h is a number that depends only on $\beta(G)$. The rest of the argument goes exactly as before, to show that

$$r_p(R) \leq r_p(G) \leq f(\alpha)$$

for a suitable function f.

We now return to the general case, still assuming that $O_{p'}(G) = 1$. Put $Z = \mathrm{Z}(E)$ and $C = \mathrm{C}_G(E) = \mathrm{C}_G(E/Z)$. Then $G/Z = E/Z \times C/Z$, because E/Z is a product of non-abelian chief factors of G and G induces only inner automorphisms on each such chief factor. It follows in particular that $Z \leq \mathrm{Z}(G)$.

Now write

$$\overline{} : G \to G/E$$

for the quotient mapping. We claim that $E(\overline{G}) = O_{p'}(\overline{G}) = 1$. To see this, suppose that X/E is a quasi-simple subnormal subgroup of G/E. Then $(X \cap C)/Z = Y/Z$, say, is quasi-simple and it follows easily that Y' is a quasi-simple group. But Y' is also subnormal in G, so $Y' \leq E$; this now implies that X/E is abelian, a contradiction. Thus X cannot exist, and so $E(\overline{G}) = 1$ as claimed. Next, suppose that X/E is a minimal normal p'-subgroup of G/E, and define Y as above. Since $E(\overline{G}) = 1$, the group X/E is elementary abelian; hence so is Y/Z, whence Y is nilpotent. But $Y \lhd G$ so $O_{p'}(Y) \leq O_{p'}(\overline{G}) = 1$; thus Y is a p-group, and therefore so is $X/E \cong Y/Z$, a contradiction. Thus again X cannot exist, and $O_{p'}(\overline{G}) = 1$ as claimed.

The special case done above now shows that

$$r_p(\overline{R}) \leq f(\alpha).$$

Since $R \leq C$ we have

$$R \cap E = Z \leq \mathrm{Z}(R);$$

and hence in particular that $R/Z \cong \overline{R}$. It follows from the definition of E that Z is a quotient of the Schur multiplier $M(E/Z)$. Also E/Z is a direct product of simple groups belonging to $\mathcal{X}(\beta)$, and the multiplier of each such group has order at most $16(\beta + 1)$ (↬ **Finite simple groups**); consequently Z has exponent dividing $(16(\beta + 1))!$. On the other hand, Z is a p-group since $O_{p'}(G) = 1$. If $p > 16(\beta + 1)$ it follows that $Z = 1$, in which case

$$r_p([R, G]) \leq r_p(R) = r_p(\overline{R}) \leq f(\alpha),$$

and we are done. We may therefore suppose henceforth that

$$p \leq 16(\beta + 1).$$

The Schur multiplier $M(R/Z)$ has p-rank bounded by a number depending only on $r_p(\overline{R})$ ($\leadsto$ **Finite group theory**). This implies that

$$r_p(R' \cap Z) \leq r_p(M(R/Z)) \leq f_1(\alpha)$$

for some function f_1, and hence that

$$r_p(R') \leq r_p(\overline{R'}) + r_p(R' \cap Z) \leq f(\alpha) + f_1(\alpha).$$

It remains to deal with the factor $[R, G]/R'$. Now let p^n be the p-part of the exponent of R/R', and let $m = r_p(\overline{R}/\overline{R'})$, so $m \leq f(\alpha)$. Consider the group

$$K = \mathrm{C}_G(R/R'R^pZ).$$

This is the kernel of the action of G on an $\mathbb{F}_p$-vector space of dimension m. Since $p \leq 16(\beta+1)$ it follows that $k = |G : K| \leq |\mathrm{GL}_m(\mathbb{F}_p)|$ is bounded by some $f_2(\alpha)$ depending only on α. On the other hand, $K/\mathrm{C}_K(R/R'R^p)$ is abelian (since Z is central in G), and $\mathrm{C}_K(R/R'R^p)/\mathrm{C}_K(R/R'R^{p^n})$ is a p-group; but G/R is a product of non-abelian simple groups and $R \leq \mathrm{C}_K(R/R'R^{p^n})$, so we must have $K = \mathrm{C}_K(R/R'R^{p^n}) = \mathrm{C}_G(R/R'R^{p^n})$.

Let $x_1, \ldots, x_m$ generate R modulo $R'R^{p^n}Z$ and let $\{y_1, \ldots, y_k\}$ be a transversal to the cosets of K in G. Then

$$[R, G]R^{p^n} = \langle [x_i, y_j] \mid 1 \leq i \leq m,\, 1 \leq j \leq k \rangle\, R'R^{p^n}.$$

Since the p-part of $[R, G]/R'$ is isomorphic to $[R, G]R^{p^n}/R'R^{p^n}$ it follows that

$$r_p([R, G]/R') \leq mk \leq f(\alpha)f_2(\alpha)$$

and hence that $r_p([R, G]) \leq f(\alpha)f_2(\alpha) + f(\alpha) + f_1(\alpha)$.

This completes the proof. ■

We are now ready to state the main structure theorem. A profinite group H is said to be *quasi-semisimple of bounded type* if H is *perfect* (that is, $H = \overline{H'}$) and

$$H/\mathrm{Z}(H) \cong \prod_{X \in \mathcal{X}} X^{(m(X))},$$

where for some finite β we have $\mathcal{X} \subseteq \mathcal{X}(\beta)$ and $m(X) \leq \beta$ for each X. The least such β is called the *type* of H. The fact that the Schur multiplier $M(X)$ has order at most $16(\beta + 1)$ for each such X, alluded to in the preceding proof, implies that $\mathrm{Z}(H)$ is then an abelian group of exponent dividing $(16(\beta + 1))!$.

Theorem 10.2.5 *Let G be a profinite group with* wPSG. *Then*
(i) G is finitely generated;

(ii) G has closed normal subgroups $S \leq G_1$ such that S is prosoluble of finite rank, G/G_1 is finite, and G_1/S is a quasi-semisimple group of bounded type having wPSG.
Moreover, $\mathrm{d}(G)$*, the index* $|G : G_1|$*, the rank of* S*, the type of* G_1/S *and* $\alpha^\dagger(G_1/S)$ *are all bounded by functions of* $\alpha^\dagger(G)$.

Proof. We shall say that a number is 'bounded' if it is bounded in terms of $\alpha^\dagger(G)$. Let $R \leq G_0$ be the closed normal subgroups of G provided by Proposition 10.2.3, and put $e = (16(\beta+1))!$. Now put

$$S = \overline{[R, G_0]R^e}$$
$$G_1 = \overline{G_0' R^e}.$$

Note first that $\alpha^\dagger(G_0)$ is bounded, by Lemma 10.2.1. Applying Proposition 10.2.4, with G_0 in place of G, we see that $\overline{[R, G_0]}$ has bounded rank, so factoring out this closed normal subgroup we may suppose for the rest of the proof that $[R, G_0] = 1$.

Write $D = R \cap \overline{G_0'}$. Since G_0/R is a product of non-abelian simple groups we have $G_0 = R\overline{G_0'}$. By Proposition 5.4.2 (or an elementary argument!), the abelian group $G_0/\overline{G_0'}$ has bounded rank r, say, so $R/D \cong G_0/\overline{G_0'}$ also has rank r. On the other hand, $\overline{G_0'}$ is perfect since R is central in G_0, so in fact $\overline{G_0'}$ is quasi-semisimple of bounded type (at most β) with centre D, and it follows that $D^e = 1$. As R is abelian, this now implies that $\mathrm{rk}(\overline{R^e}) \leq r$. This completes the proof that $S = \overline{[R, G_0]R^e}$ has bounded rank; and of course S is prosoluble because $S \leq R$.

Now

$$G_1/S = \overline{G_0' R^e}/\overline{R^e} \cong \overline{G_0'}/(\overline{G_0'} \cap \overline{R^e})$$

is the quotient of $\overline{G_0'}$ by a central closed subgroup; hence G_1/S is again quasi-semisimple of bounded type at most β. Finally,

$$G_0/G_1 \cong R/D\overline{R^e}$$

which has order at most e^r, and so $|G : G_1| \leq |G : G_0|e^r$ is bounded.

This completes the proof of (ii). Part (i) now follows, because

$$\begin{aligned}\mathrm{d}(G) &\leq \mathrm{d}(G/G_0) + \mathrm{d}(G_0/S) + \mathrm{d}(S)\\ &\leq \log|G : G_0| + 2\beta + \mathrm{rk}(S).\end{aligned}$$

To see that $\mathrm{d}(G_0/S) \leq 2\beta$, note first that $\mathrm{d}(G_0/S) = \mathrm{d}(G_0/Z)$ where $Z/S = \mathrm{Z}(G_0/S)$, because G_0/S is perfect. On the other hand, we can write G_0/Z as the direct product of at most β closed subgroups, each of which is a Cartesian product of pairwise non-isomorphic non-abelian simple groups; since every simple group can be generated by 2 elements the same holds for each of these cartesian products. (The fact that profinite PSG groups are finitely generated can be proved very simply by a quite different method, given in Chapter 11). ■

The significance of this theorem is that, to a large extent, it reduces the characterisation of profinite groups with wPSG to the case of *quasi-semisimple groups*, which can be described in terms of certain numerical parameters.

10.3 Quasi-semisimple groups

A quasi-semisimple group with trivial centre is a Cartesian product of finite simple groups. Such a group G is determined, up to a small amount of ambiguity, just by the *orders* of its simple factors, with their multiplicities (the ambiguity results from the occasional coincidence of the orders of non-isomorphic simple groups). Ignoring the ambiguity, it follows that (roughly) any property of G is equivalent to some arithmetical property of the corresponding family of natural numbers. Which arithmetical property expresses the condition that G have wPSG? There is no *a priori* reason to expect that this property should have a concise arithmetical definition; quite remarkably, however, it does. Moreover, it applies to all quasi-semisimple groups, even those with non-trivial centres.

Let G be a quasi-semisimple group of bounded type. Thus for some finite β we have $G/\mathrm{Z}(G) = \prod_{i\in\mathcal{I}} T_i$, where $T_i \in \mathcal{X}(\beta)$ for each i and no factor occurs more than β times. Define

$$\mathcal{N}(G) = (|T_i|)_{i\in\mathcal{I}}.$$

We say that a family N of natural numbers satisfies the *gcd condition* if there exists a positive number γ such that for every finite subfamily F of N,

$$\prod_{x\in F}\prod_{y\in F}\gcd(x,y) \le \left(\prod_{x\in F} x\right)^{\gamma}.$$

We can now state

Proposition 10.3.1 *Let G be a quasi-semisimple profinite group of bounded type. Then G has* wPSG *if and only if the family $\mathcal{N}(G)$ satisfies the gcd condition.*

The appearance of the gcd condition is explained by Proposition 1.10.2, which relates $s(A)$ for an *abelian* group $A \cong \bigoplus C_{e_i}$ to

$$|\mathrm{End}(A)| = \prod_{i,j}\gcd(e_i,e_j).$$

The idea behind the proof of Proposition 10.3.1 is that we can 'model' a finite quotient of G by a suitable abelian group.

The argument in the 'only if' direction depends on the following property of simple groups:

Lemma 10.3.2 ([Segal & Shalev 1997], Lemma 6.2). *Let $T \in \mathcal{X}(\beta)$. Then T contains elements $g_1,\dots,g_m$, where m depends only on β, such that*

$$\prod_{j=1}^{m} o(g_j) = |T|.$$

We omit the rather technical proof, but illustrate the result with an example:

Example Let $T = \mathrm{PSL}_2(\mathbb{F}_p)$ where $p \geq 5$ is a prime. Then $m = 4$ will do: let

$$g_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ g_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ g_3 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

where λ is a generator for the multiplicative group $\mathbb{F}_p^*$, and $g_4 = \sigma^{p-1}$ where σ is a Singer-cycle (acting like multiplication by a generator of $\mathbb{F}_{p^2}^*$ on $\mathbb{F}_{p^2} \cong \mathbb{F}_p \oplus \mathbb{F}_p$). The images of $g_1, \ldots, g_4$ in T have orders 2, p, $(p-1)/2$ and $(p+1)/2$ respectively, while $|T| = p(p^2-1)/2$.

Now suppose that G as above has wPSG, and let F be a finite subfamily of $\mathcal{N}(G)$. To simplify notation, we may as well assume that $F = (|T_1|, \ldots, |T_k|)$. Then $T_1 \times \cdots \times T_k = \overline{G}$ is a quotient of G. For each i, put $n_i = |T_i|$ and let $g_{i1}, \ldots, g_{im}$ be the elements of T_i provided by Lemma 10.3.2.

The idea is to 'model' $\overline{G}$ with the correponding abelian group $B = C_{n_1} \times \cdots \times C_{n_k}$. For $j = 1, \ldots, m$, let

$$A_j = \langle g_{ij} \mid i = 1, \ldots, k \rangle \leq \overline{G}.$$

Then $A_j \cong C_{e(1,j)} \times \cdots \times C_{e(k,j)}$ where $e(i,j) = o(g_{ij})$, and we may construct a filtration

$$B = B_m \geq B_{m-1} \geq \ldots \geq B_1 \geq B_0 = 1$$

so that $B_j / B_{j-1} \cong A_j$ for $j = 1, \ldots, m$.

Now on the one hand,

$$|\mathrm{End}(A_j)| \leq |A_j|\, s(A_j)^4 \leq |A_j|\, s(\overline{G})^4$$

for each j. On the other hand,

$$\prod_{i=1}^{k} \prod_{j=1}^{k} \gcd(n_i, n_j) = |\mathrm{End}(B)| \leq \prod_{j=1}^{m} |\mathrm{End}(A_j)|^m .$$

For both of these, see §1.10. Putting them together and noting that $\prod_{j=1}^{m} |A_j| = \left|\overline{G}\right|$ we obtain

$$\begin{aligned} \prod_{i=1}^{k} \prod_{j=1}^{k} \gcd(n_i, n_j) &\leq \left|\overline{G}\right|^m \cdot s(\overline{G})^{4m^2} \\ &\leq \left|\overline{G}\right|^{m+4m^2\alpha} = \left(\prod_{i=1}^{k} n_i \right)^{m+4m^2\alpha} \end{aligned}$$

where $\alpha = \alpha^\dagger(G)$.

It follows that $\mathcal{N}(G)$ satisfies the gcd condition with constant $\gamma = m + 4m^2\alpha$.

The converse will be deduced from the following general result about finite linear groups:

Proposition 10.3.3 *Let $p_1, \dots, p_k$ be primes and $m \in \mathbb{N}$. For each i let X_i be a subgroup of $\mathrm{GL}_m(\mathbb{F}_{p_i})$ of even order, and let $H = X_1 \times \cdots \times X_k$. Suppose that*

$$\prod_{i=1}^{k} \prod_{j=1}^{k} \gcd(|X_i|, |X_j|) \leq \left(\prod_{i=1}^{k} |X_i| \right)^{\nu}.$$

Then

$$s(H) \leq |H|^{f(m,\mu,\nu)}$$

where μ is the maximum multiplicity of any prime in the sequence $p_1, \dots, p_k$.

Before giving the proof, let us complete the deduction of Proposition 10.3.1. So let G be quasi-semisimple of bounded type β, and suppose that $\mathcal{N}(G)$ satisfies the gcd condition with the constant γ. We have to show that if $\overline{G}$ is any finite quotient of G then $s(\overline{G}) \leq \left|\overline{G}\right|^s$ where s is bounded in terms of β and γ.

Now $\overline{G}$ is a finite perfect group and $\overline{G}/Z(\overline{G}) = T_1 \times \cdots \times T_k$ where each $T_i \in \mathcal{X}(\beta)$. It follows that $\overline{G}$ is an epimorphic image of $\widetilde{T}_1 \times \cdots \times \widetilde{T}_k = H$, say, where $\widetilde{T}_i$ denotes the universal covering group of T_i. For each i we have $\left|\widetilde{T}_i\right| < |T_i|^2$ (the order is actually very much less: $\leadsto$ **Finite simple groups**); so $|H| < \left|\overline{G}\right|^2$, and as $s(\overline{G}) \leq s(H)$ it will therefore suffice to show that $s(H) \leq |H|^s$ where s is bounded in terms of β and γ. This we do by verifying that Proposition 10.3.3 is applicable, taking $X_i = \widetilde{T}_i$ for each i. That is, we find m, μ and ν as in the proposition and check that each is bounded in terms of β and γ.

What is m? Suppose $T_i = X^*_{n_i}(\mathbb{F}_{p_i^{e_i}})$. Then $X_i = \widetilde{T}_i$ has a faithful linear representation over $\mathbb{F}_{p_i^{e_i}}$ of degree bounded in terms of $n_i \leq \beta$. Since also $e_i \leq \beta$ for each i, there exists m, bounded in terms of β, such that $X_i \leq \mathrm{GL}_m(\mathbb{F}_{p_i})$ for each i.

What is μ? There are at most 14β possibilities for the symbol ${}^*X_{n_i}$, at most β possibilities for e_i, and each T_i occurs at most β times up to isomorphism. It follows that no prime occurs more than $14\beta^3$ times in the sequence $p_1, \dots, p_k$, and so $\mu \leq 14\beta^3$.

What is ν? The Schur multiplier $M(T_i)$ is the kernel of the covering map $\widetilde{T}_i \to T_i$. Let h be the least common multiple of the orders $|M(T_i)|$, so $|X_i|$ divides $h\,|T_i|$ for each i. Then

$$\gcd(|X_i|, |X_j|) \leq h \gcd(|T_i|, |T_j|) \leq \gcd(|T_i|, |T_j|)^{1+\log h}$$

since $\gcd(|T_i|, |T_j|) \geq 2$; thus

$$\begin{aligned} \prod_{i=1}^{k} \prod_{j=1}^{k} \gcd(|X_i|, |X_j|) &\leq \prod_{i=1}^{k} \prod_{j=1}^{k} \gcd(|T_i|, |T_j|)^{1+\log h} \\ &\leq \left(\prod_{i=1}^{k} |T_i| \right)^{\gamma(1+\log h)} \leq \left(\prod_{i=1}^{k} |X_i| \right)^{\nu}, \end{aligned}$$

where $\nu = \gamma(1 + \log h)$. Since each $T_i \in \mathcal{X}(\beta)$, we know that h is bounded in terms of β ($\leadsto$ **Finite simple groups**); hence ν is bounded in terms of β and γ.

This completes the deduction of Proposition 10.3.1, and it remains to prove Proposition 10.3.3. We shall use Proposition 1.8.1, which we restate here (recall that for a finite group G, $\mathrm{nil}(G)$ denotes the number of nilpotent subgroups of G):

Lemma 10.3.4 *Let H be a finite group, and let l be the maximum Fitting height of any soluble subgroup of H. Then*

$$\mathrm{s}(H) \leq \mathrm{nil}(H)^{l+1}.$$

Proof of Proposition 10.3.3. We shall say that a number is 'bounded' if it is bounded in terms of m, μ and ν. The soluble subgroups of H have bounded derived lengths, by Zassenhaus's Theorem ($\leadsto$ **Linear groups**), and *a fortiori* bounded Fitting heights; in view of the above Lemma, it will therefore suffice to show that $\mathrm{nil}(H) \leq |H|^s$ where s is bounded.

Write $\pi_i : H \to X_i$ for the ith projection mapping. Let Y be a nilpotent subgroup of H. Then $\pi_i(Y) = P_i(Y) \times Q_i(Y)$ where $P_i(Y)$ is a p_i-group and $Q_i(Y)$ is a p_i'-group, and we have $Y \leq P(Y) \times Q(Y)$ where

$$P(Y) = \prod P_i(Y),\ Q(Y) = \prod Q_i(Y).$$

Now for each i, the rank of $P_i(Y)$ is at most m^2 ($\leadsto$ **Finite group theory**). Since the rank of a nilpotent group is just the maximum of the ranks of its Sylow subgroups, it follows that $\mathrm{rk}(P(Y)) \leq \mu m^2$. Therefore Y is generated by $Y \cap Q(Y)$ and at most μm^2 further elements. Thus given $Y \cap Q(Y)$, the number of possibilities for Y is at most $|H|^{\mu m^2}$.

Let us call a subgroup Y of H *non-modular* if $\pi_i(Y)$ is a p_i'-group for each i, and suppose that H contains n nilpotent non-modular subgroups. The preceding discussion shows that

$$\mathrm{nil}(H) \leq |H|^{\mu m^2} n.$$

To each nilpotent p_i'-subgroup Q_i of X_i we assign one of its maximal abelian normal subgroups A_i. Then A_i is a diagonalisable group and Q_i/A_i embeds in $\mathrm{Sym}(m)$, which implies that $\mathrm{rk}(A_i) \leq m$ and $\mathrm{rk}(Q_i/A_i) \leq m$ ($\leadsto$ **Linear groups**). Hence Q_i has rank at most $2m$. It follows that the number of such subgroups Q_i of X_i is at most $|X_i|^{2m}$. To estimate n, we now associate to each nilpotent non-modular subgroup Y of H the k-tuple

$$\mathbf{Q}(Y) = (\pi_1(Y), \ldots, \pi_k(Y)).$$

The number of such k-tuples is at most $\prod |X_i|^{2m} = |H|^{2m}$, so it will suffice now to estimate the number $n(\mathbf{Q})$ of such Y for a fixed choice of $\mathbf{Q}(Y) = (Q_1, \ldots, Q_k)$.

Put $A = A_1 \times \cdots \times A_k$ and $Q = Q_1 \times \cdots \times Q_k$. Then $Y \leq Q$; we estimate separately the number of possibilities for $A \cap Y$, for AY, and then, given these two groups, for Y itself.

Since each A_i has rank at most m, the abelian group A is isomorphic to a subgroup of

$$(C_{t_1} \times \cdots \times C_{t_k})^{(m)}$$

where $t_i = |X_i|$ for each i. It follows by Proposition 1.10.2 and Corollary 1.10.7 that

$$\begin{aligned} s(A) \leq |\mathrm{End}(C_{t_1} \times \cdots \times C_{t_k})|^{m^2} &= \left(\prod_{i=1}^{k} \prod_{j=1}^{k} \gcd(t_i, t_j) \right)^{m^2} \\ &\leq \left(\prod_{i=1}^{k} t_i \right)^{\nu m^2} = |H|^{\nu m^2}. \end{aligned}$$

This gives an upper bound to the number of possibilities for $A \cap Y$.

The group $Q/A \cong Q_1/A_1 \times \cdots \times Q_k/A_k$ has rank at most km and order at most $(m!)^k$, hence contains at most $(m!)^{k^2 m}$ subgroups. However, since each t_i is even we have

$$2^{k^2} \leq \prod_{i=1}^{k} \prod_{j=1}^{k} \gcd(t_i, t_j) \leq |H|^{\nu},$$

which implies that

$$(m!)^{k^2} = 2^{k^2 \log m!} \leq |H|^{\nu \log m!}. \tag{10.1}$$

Hence the number of possibilities for the subgroup AY of Q is bounded above by $|H|^{\nu m \log m!}$.

Finally, having fixed $A \cap Y = B$ and $AY = E$, we estimate the number of possibilities for Y. Since Y/B is a complement to A/B in E/B, this number is at most

$$d = |\mathrm{Der}(E/A, A/B)|.$$

Put $B_0 = A \cap Y$ and, for $i \geq 1$, let $B_i = B_{i-1} A_i$. Put $C_i = C_E(B_i/B_{i-1})$ and write $d_i = |\mathrm{Der}(E/A, B_i/B_{i-1})|$. Then $d \leq d_1 \ldots d_k$, and for each i we have

$$d_i \leq |\mathrm{Der}(E/C_i, B_i/B_{i-1})| \cdot |\mathrm{Hom}(C_i/A), B_i/B_{i-1}|.$$

Now $C_i/A \leq Q/A$ has exponent dividing $m!$ and rank at most km, while $B_i/B_{i-1} \cong A_i/(A_i \cap B_{i-1})$ is abelian and has rank at most m; therefore

$$|\mathrm{Hom}(C_i/A), B_i/B_{i-1}| \leq (m!)^{km^2}.$$

On the other hand, since $C_i \geq \prod_{j \neq i} A_j$, the quotient E/C_i is isomorphic to a section of Q_i/A_i and so has rank at most m. Therefore

$$|\mathrm{Der}(E/C_i, B_i/B_{i-1})| \leq |B_i/B_{i-1}|^m \leq |A_i|^m.$$

Putting these together we get

$$d \leq \prod_{i=1}^{k} \left(|A_i|^m \, (m!)^{km^2} \right) \leq |H|^m \, (m!)^{k^2 m^2} \leq |H|^{m+m^2 \nu \log m!}.$$

The conclusion is that

$$n(\mathbf{Q}) \leq |H|^s$$

where

$$s = \nu m^2 + \nu m \log m! + (m + m^2 \nu \log m!).$$

The result follows.

To conclude this section, let us show how Proposition 10.3.1 may be used to construct many groups with wPSG (which is equivalent to PSG, as we show in §10.5 below). Let (p_i) be a sequence of distinct primes greater than 3 such that for each i,

$$\begin{aligned} &p_i \geq 2^i \\ &p_i \equiv \pm 3 \pmod 8 \\ &p_i \not\equiv 1 \pmod q \text{ for each prime factor } q \text{ of } \prod_{j<i} p_j(p_j^2 - 1). \end{aligned}$$

The existence of such sequences is guaranteed by Dirichlet's theorem on arithmetic progressions. Now put

$$L_i = \mathrm{PSL}_2(\mathbb{F}_{p_i}), \ \widetilde{L}_i = \mathrm{SL}_2(\mathbb{F}_{p_i}).$$

Then $|L_i| = p_i(p_i^2 - 1)/2$ for each i, so for $i > j$ we have

$$\gcd(|L_j|, |L_i|) = 12,$$

and a short calculation shows that the sequence $(|L_i|)$ satisfies the gcd condition with $\gamma = 4$. It follows that the profinite groups

$$G = \prod_{i=1}^{\infty} L_i \ \text{ and } \ \widetilde{G} = \prod_{i=1}^{\infty} \widetilde{L}_i$$

both have (w)PSG. Note that the centre of $\widetilde{G}$ is an infinite group of exponent 2; this explains the remark made in an earlier section that the prosoluble radical of a PSG group need not necessarily have finite rank.

Now let $R = \mathbb{Z}[\{p^{-1} : p \in S\}]$ where S is the complement of $\{p_i \mid i \in \mathbb{N}\}$ in the set of all primes. The group $\mathrm{SL}_2(R)$ has the congruence subgroup property (see Chapter 6), so its profinite completion is isomorphic to

$$\mathrm{SL}_2(\widehat{R}) \cong \prod_{i=1}^{\infty} \mathrm{SL}_2(\mathbb{Z}_{p_i}).$$

Let K_i be the principal congruence subgroup $\ker(\mathrm{SL}_2(\mathbb{Z}_{p_i}) \to \mathrm{SL}_2(\mathbb{F}_{p_i}))$. Then K_i is a pro-p_i group of rank 3, and so $K = \prod_{i=1}^{\infty} K_i$ is pronilpotent of rank 3 ($\rightsquigarrow$ **Pro-p groups**). The exact sequence

$$1 \to K \to \mathrm{SL}_2(\widehat{R}) \to \prod_{i=1}^{\infty} \mathrm{SL}_2(\mathbb{F}_{p_i}) = \widetilde{G} \to 1$$

now shows that $\mathrm{SL}_2(\widehat{R})$ is an extension of K by $\widetilde{G}$; Proposition 10.4.3, to be proved below, now implies that $\mathrm{SL}_2(\widehat{R})$ has (w)PSG, and hence that $\mathrm{SL}_2(R)$ also has PSG. Thus we obtain a plentiful supply of countable, non-soluble linear groups with PSG.

10.4 Profinite groups with wPSG: characterisation

We now have all the ingredients, and it remains to put them together. The main step is the following result about group extensions, similar to Proposition 1.3.3:

Proposition 10.4.1 *Let G be a finite group and S a soluble normal subgroup of rank r. Then*

$$\mathrm{s}(G) \leq \mathrm{s}(G/S)^{f_1(l)}\, |S|^{f_2(l,r)}$$

where l denotes the maximal Fitting height of all soluble subgroups of G.

This will be proved below. For the present application we also need

Lemma 10.4.2 *Let Q be a finite group and H a soluble subgroup of Q. Then*

$$l(H) \leq \min\{f_3(\mathrm{rk}(H)),\ f_4(\alpha^\dagger(Q))\}.$$

Recall that $l(H)$ denotes the Fitting height of H.

Proof. Put $r = \mathrm{rk}(H)$, and let K denote the intersection of the centralizers of all chief factors of H. Since these chief factors are elementary abelian of rank at most r, we see that H/K is a subdirect product of soluble linear groups of degree at most r. It follows by Zassenhaus's Theorem ($\rightsquigarrow$ **Linear groups**) that the derived length of H/K is bounded by a function of r. As K is nilpotent this shows that $l(H) \leq f_3(r)$.

Now applying Theorem 10.2.5 to the group Q, we find normal subgroups $S \leq R \leq Q_1$ of Q such that S is soluble, R/S is central in Q_1/S and Q_1/R is a product of simple groups in $\mathcal{X}(\beta)$, where $\mathrm{rk}(S)$, β and $|Q : Q_1|$ are all bounded in terms of $\alpha^\dagger(Q)$. In particular, Q_1/R is a product of linear groups of bounded degree, so as above it follows that $l((Q_1 \cap H)/(R \cap H))$ is bounded (where 'bounded' now means in terms of $\alpha^\dagger(Q)$). Clearly $l((Q_1 \cap H)/(S \cap H)) = l((Q_1 \cap H)/(R \cap H))$. Also $l(H/(Q_1 \cap H)) \leq \log |Q : Q_1|$, while $l(S \cap H) \leq f_3(\mathrm{rk}(S))$ by the preceding paragraph. Since the Fitting height is sub-additive on extensions we deduce that $l(H)$ is bounded in terms of $\alpha^\dagger(Q)$. ■

Corollary 10.4.3 *Let $S \lhd_c G$ where G is a profinite group, S is prosoluble of finite rank r, and $\alpha^\dagger(G/S) = \alpha$ is finite. Then*

$$\alpha^\dagger(G) \leq f(r, \alpha).$$

Proof. We may assume that G is finite, and have to bound $\mathrm{s}(G)$ in terms of $|G|$. Put $Q = G/S$. Since Fitting height is sub-additive on extensions, we see from Lemma 10.4.2 that the Fitting height of every soluble subgroup of G is bounded by $f_3(r) + f_4(\alpha) = l$, say. Then Proposition 10.4.1 gives

$$\begin{aligned}\mathrm{s}(G) &\leq \mathrm{s}(Q)^{f_1(l)}\, |S|^{f_2(l,r)} \\ &\leq |Q|^{\alpha f_1(l)}\, |S|^{f_2(l,r)} \leq |G|^{f(r,\alpha)}\end{aligned}$$

where $f(r, \alpha) = \max\{\alpha f_1(f_3(r) + f_4(r)),\ f_2(f_3(r) + f_4(r))\}$. ■

Combining this with Theorem 10.2.5, Proposition 10.3.1 and Lemma 10.2.1, we obtain the characterisation of profinite groups with wPSG:

Theorem 10.4.4 *Let G be a profinite group. Then G has* wPSG *if and only if G has closed normal subgroups $S \leq G_1$ such that S is prosoluble of finite rank, G/G_1 is finite, and G_1/S is a quasi-semisimple group of bounded type such that $\mathcal{N}(G_1/S)$ satisfies the gcd condition.*

The proof of Proposition 10.4.1 depends on a further lemma (cf. Lemma 1.3.4):

Lemma 10.4.5 *Let A and B be finite nilpotent groups, with A acting on B. Let $r = \mathrm{rk}(B)$. Then*

$$|\mathrm{Der}(A, B)| \leq s^{\lhd}(A) \cdot |B|^{1+(7r^2+r)/2}.$$

Proof. Write A_p, B_p to denote the Sylow p-subgroups of A, B respectively, and $A_{p'}$ for the (normal) p-complement of A. Then

$$|\mathrm{Der}(A, B)| = \prod_p |\mathrm{Der}(A, B_p)| = \prod_p |\mathrm{Der}(A_{p'}, B_p)|\, |\mathrm{Der}(A_p, B_p)|$$

where the product ranges over all primes p. Now every derivation $A_{p'} \to B_p$ is inner (the conjugacy part of the Schur-Zassenhaus theorem), so $|\mathrm{Der}(A_{p'}, B_p)| \leq |B_p|$.

Fix p and put $P = B_p$, $Q = A_p$. Let $\delta \in \mathrm{Der}(Q, P)$ and put $K = K_\delta = \mathrm{C}_Q(P) \cap \ker \delta$. It is easy to verify that $K \lhd Q$. Since the restriction of δ to $\mathrm{C}_Q(P)$ is a homomorphism with kernel K, we deduce that $\mathrm{C}_Q(P)/K$ is isomorphic to a subgroup of P, hence has rank at most r. On the other hand, according to Proposition 9 in the **Pro-p groups** window, every p-subgroup of $\mathrm{Aut}(P)$ has rank at most $\frac{1}{2}(7r^2 - r)$, so this is an upper bound for $\mathrm{rk}(Q/\mathrm{C}_Q(P))$. It follows that Q/K has rank at most $\frac{1}{2}(7r^2 + r)$. Now δ is determined by the

induced derivation $Q/K \to P$, so once K_δ is given there are at most $|P|^{(7r^2+r)/2}$ possibilities for δ. This shows that

$$|\mathrm{Der}(Q,P)| \le s^{\lhd}(Q) \cdot |P|^{(7r^2+r)/2}.$$

The lemma follows since $s^{\lhd}(A) = \prod_p s^{\lhd}(A_p)$ and $|B| = \prod_p |B_p|$. ■

Proof of Proposition 10.4.1. Recall that $\mathrm{s}(G) \le \mathrm{nil}(G)^{l+1}$ by Lemma 10.3.4, so it will suffice to find an upper bound for $\mathrm{nil}(G)$.

Let F be the Fitting subgroup of S and put $n_1 = \mathrm{nil}(G/F)$. To each nilpotent subgroup H of G we associate $Y_H = HF$ and $D_H = H \cap F$. Given a nilpotent subgroup Y/F of G/F and a subgroup D of F, the number of possibilities for H such that $Y_H = Y$ and $D_H = D$ is at most

$$\mathrm{der}(\mathrm{N}_Y(D)/\mathrm{N}_F(D),\, \mathrm{N}_F(D)/D),$$

because H/D is a complement to $\mathrm{N}_F(D)/D$ in $\mathrm{N}_Y(D)/D$. Since $\mathrm{N}_Y(D)/\mathrm{N}_F(D) \cong Y/F$ and $\mathrm{N}_F(D)/D$ is a section of F, Lemma 10.4.5 shows that this number is at most

$$\mathrm{s}(Y/F) \cdot |F|^{1+(7r^2+r)/2} \le n_1 \, |F|^{1+(7r^2+r)/2}.$$

The number of possible choices for Y is at most n_1, and there are at most $|F|^r$ possibiities for D. It follows that

$$\mathrm{nil}(G) \le n_1^2 \, |F|^{1+(7r^2+3r)/2}.$$

To get rid of n_1 we now repeat this argument, going up the Fitting series of S, which has length at most l; the conclusion is that

$$\mathrm{nil}(G) \le \mathrm{nil}(G/S)^{2^l} \cdot |S|^{2^{l-1}(1+(7r^2+3r)/2)}.$$

Thus

$$\mathrm{s}(G) \le \mathrm{s}(G/S)^{f_1(l)} \, |S|^{f_2(l,r)}$$

where $f_1(l) = (l+1)2^l$ and $f_2(l,r) = (l+1)2^{l-1}(1+(7r^2+3r)/2)$. This completes the proof.

For the proofs of Corollaries 10.4 and 10.5, we refer the reader to [Segal & Shalev 1997]. The first of these, which says that extensions of PSG groups again have PSG, is quite easily reduced using Corollary 10.4.3 to the case of quasi-semisimple groups; in that case, it comes down to the elementary arithmetical fact that if two sequences satisfy the gcd condition then so does their union, by Corollary 1.10.5. Corollary 10.5 depends on a slightly tricky application of Jordan's theorem (↬ **Linear groups**) .

10.5 Weak PSG = PSG

To complete the proof of the Profinite PSG Theorem it only remains to establish

Theorem 10.5.1 *Every group with* weak PSG *has* PSG. *More precisely, there exists a function f such that*

$$\alpha^\dagger(G) \leq \alpha^*(G) \leq f(\alpha^\dagger(G)) \tag{10.2}$$

for all groups G.

We have already remarked that $\alpha^\dagger(G) \leq \alpha^*(G)$ holds trivially. Now let G be a group with $\alpha = \alpha^\dagger(G)$ finite. Since $\alpha^*(G)$ depends only on the finite quotients of G, to complete the proof of (10.2) we may replace G by one of its finite quotients, and so assume henceforth that G is *finite*. As before, we shall call a number 'bounded' if it is bounded above by some function of α. According to Theorem 10.2.5, G has a normal subgroup G_1 of bounded index and a soluble normal subgroup $S \leq G_1$ of bounded rank such that G_1/S is quasi-semisimple of bounded type β,say. Now Lemma 10.2.1 shows that $\alpha^\dagger(G_1)$ is bounded, and that $\alpha^*(G)$ is bounded by a function of $\alpha^*(G_1)$. Thus it will suffice to show that $\alpha^*(G_1)$ is bounded in terms of $\alpha^\dagger(G_1)$; so we may replace G by G_1 and assume henceforth that $G = G_1$. In this case, we have

$$S \leq R \lhd G$$

where $S \lhd G$ is soluble of bounded rank r, $R/S = \mathrm{Z}(G/S)$, G/S is perfect and G/R is a product of simple groups in $\mathcal{X}(\beta)$, each occurring with multiplicity at most β.

Suppose we can show

A that G has at most $n^{f_1(\alpha)}$ *normal* subgroups of index at most n, for each n, and

B that if $H \leq G$ and $|G : H| = n$ then $|G : H_G| \leq n^{f_2(\alpha)}$, for each n,

where $H_G = \bigcap_{g \in G} H^g$. Then every subgroup of index n in G contains a normal subgroup of index at most $n^{f_2(\alpha)}$; there are at most $n^{f_2(\alpha)f_1(\alpha)}$ such normal subgroups, and each of them is contained in at most $n^{f_2(\alpha)\alpha}$ subgroups of G. Consequently

$$a_n(G) \leq n^{f_2(\alpha)f_1(\alpha)} n^{f_2(\alpha)\alpha} = n^{f_2(\alpha)(f_1(\alpha)+\alpha)}.$$

Therefore $s_n(G) \leq n^{f(\alpha)}$ where $f(\alpha) = 1 + f_2(\alpha)(f_1(\alpha) + \alpha)$, and (10.2) follows.

The proof of (A) depends on the following simple lemma.

Lemma 10.5.2 *Let H be a direct product of non-abelian simple groups, each of which appears at most β times. Then the number of normal subgroups of index at most n in H is bounded above by*

$$n^{2+2\beta}.$$

Proof. Let c_m denote the number of isomorphism types of images of H of order m, and b_m the number of normal subgroups of index m in H. Since $\mathrm{d}(H) \leq 2\beta$ there are at most $m^{2\beta}$ epimorphisms from H to a given group F of order m. However, since $\mathrm{Z}(F) = 1$, the group F has at least m automorphisms, so at least m epimorphisms from H to F share the same kernel. It follows that

$$b_m \leq m^{2\beta-1} c_m.$$

Now $H = \prod S_i^{(f_i)}$ where $S_1, S_2, \ldots$ are pairwise non-isomorphic simple groups, $f_i \leq \beta$ for each i, and, putting $s_i = |S_i|$, we may suppose that

$$60 \leq s_1 \leq s_2 \leq \ldots.$$

Since there are at most 2 non-isomorphic simple groups of each order, no integer appears more than twice in the sequence (s_i). Now c_m is just the number $N(m)$ of sequences (e_i) such that $0 \leq e_i \leq f_i$ and $\prod s_i^{e_i} = m$. We claim that $N(m) < m^2$. The lemma will follow, since we then have

$$\sum_{m=1}^{n} b_m < \sum_{m=1}^{n} m^{2\beta-1}.m^2 \leq n^{2\beta+2}.$$

The claim is proved by induction on m. If $m < 60$ then $N(m) = 0$. Suppose that $m \geq 60$. Then

$$N(m) \leq \sum_{s_i | m} N(m/s_i) \leq \sum_{s_i | m} (m/s_i)^2 \leq 2m^2 \sum_{r \geq 60} r^{-2} < m^2.$$

(The fact that there are at most 2 simple groups of each order depends on the classification; for the present application it suffices to know this for groups in $\mathcal{X}(\beta)$.) ■

Proof of (A). Let $N \lhd G$ have index $\leq n$. The preceding lemma shows that there are at most $n^{2+2\beta}$ possibilities for the subgroup RN/R in G/R. So given $K/R \lhd G/R$ with $|G : K| \leq n$, it will suffice to bound the cardinality of the set $\bigcup_{m \leq n} \mathcal{N}(m)$ where

$$\mathcal{N}(m) = \{N \lhd G \mid RN = K,\ |K : N| = m\}.$$

Fix $m \leq n$ and put $D = \bigcap \mathcal{N}(m)$. Since R is soluble, each of the quotients K/N with $N \in \mathcal{N}(m)$ is soluble, of exponent dividing m, so K/D is also soluble of exponent dividing m. As K/R is a product of non-abelian simple groups, this implies in particular that $RD = K$.

Put $T = SD$. Then G/T is perfect with centre $RD/T = K/T$, and G/K is a product of at most $\log n$ simple groups in $\mathcal{X}(\beta)$. It follows that K/T is an image of $M(G/T)$ which has order at most

$$(16(\beta+1))^{\log n} = n^{\log(16(\beta+1))}.$$

On the other hand, T/D is a soluble group of rank at most r and exponent at dividing m, hence

$$|T/D| \leq m^{r(3+\log r)}$$

(↬ **Finite group theory**, Proposition 21). Putting these together we deduce that

$$|G/D| \leq n^t$$

where $t = 1 + \log(16(\beta+1)) + r(3+\log r)$. It follows that

$$|\mathcal{N}(m)| \leq n^{t\alpha},$$

and hence that $\left|\bigcup_{m\leq n} \mathcal{N}(m)\right| \leq n^{1+t\alpha}$.

The conclusion is that G has at most $n^{(2+2\beta)+(1+t\alpha)}$ normal subgroups of index at most n; this concludes the proof of (A).

The statement (B) is another application of the Babai-Cameron-Palfy Theorem; specifically, we use Proposition 12 in the **Permutation groups window** which bounds the product of the orders of the non-abelian composition factors of a transitive permutation group with restricted composition factors.

Let $H \leq G$ with $|G:H| = n$. Replacing G by G/H_G, we may assume that in fact $H_G = 1$, and have to show that $|G| \leq n^{f_2(\alpha)}$. In this case G acts faithfully as a transitive permutation group of degree n on the right cosets of H. Now the non-abelian composition factors of G are just the simple direct factors of G/R, so each one occurs with multiplicity at most β; the result just quoted shows that

$$|G:R| \leq n^{\beta\cdot f(\beta)}$$

for a certain function f. Put $k = \beta\cdot f(\beta)$. Since R/S is a quotient of the Schur multiplier $M(G/R)$, it now follows as in the proof of (A), above, that

$$|R:S| \leq n^{k\log(16(\beta+1))}.$$

Now put $F = \mathrm{Fit}(S)$. Since F is nilpotent and $|F : H\cap F|$ divides n we have $F^n \leq H$, and as $F^n \lhd G$ it follows that $F^n = 1$. As above, this implies that $|F| \leq n^{r(3+\log r)}$, and Theorem 7 in the **Finite group theory** window now shows that

$$|S| \leq n^{4r(3+\log r)}.$$

Altogether we deduce that

$$|G| \leq n^{f_2(\alpha)}$$

where $f_2(\alpha) = k(1+\log(16(\beta+1))) + 4r(3+\log r)$.

This establishes (B), and so completes the proof of Theorem 10.5.1.

Notes

The 'Profinite PSG theorem' and its corollaries were proved in [**Segal & Shalev 1997**]. Important ingredients were obtained earlier: the equivalence of weak PSG and PSG was established in [**Segal 1996**$_b$], and the structure Theorem 10.2.5 (essentially) in [**Shalev 1997**]. (These two latter papers were being written at around the same time, and their authors realized serendipitously that a combination of their methods might point the way to the full characterisation of profinite PSG groups.)

The paper [**Shalev 1997**] also presents a delicate analysis of the subgroup growth of profinite groups of the form

$$G = \prod_i \mathrm{PSL}_2(\mathbb{F}_{p_i}).$$

Using some powerful analytic number theory, Shalev shows that the sequence (p_i) can be chosen so as to ensure that the corresponding group G can have polynomial subgroup growth of any specified degree, or that G can be made to have arbitrarily slow *non-polynomial* subgroup growth. Much easier (pronilpotent) examples of groups with slow non-polynomial subgroup growth are given in [**Mann & Segal 1995**]; yet different examples are given in Chapter 13, below.

The paper [**Segal 1996**$_b$] was inspired by the methods of [**Mann 1993**], which showed how the Babai-Cameron-Pálfy theorem and the generalized Fitting subgroup could be used to bound the ranks of abelian upper chief factors in a PSG group.

Chapter 11

Probabilistic methods

Probability has entered into group theory along several paths. One, initiated by Erdős and Turan in the 1960s, is the investigation of probabilistic properties of finite groups; a typical example of this is the classic theorem of Dixon that a random pair of elements generates the alternating group $\mathrm{Alt}(n)$ with probability that tends to 1 as $n \to \infty$, and its recent extension by Kantor, Lubotzky, Liebeck and Shalev to the definitive result: a random pair of elements generates a finite simple group with probability that tends to 1 as the group order tends to ∞. Another path is based on the fact that a profinite group G, being a compact topological group, has a finite *Haar measure* μ. Normalising this so that $\mu(G) = 1$, we may consider G as a probability space: this means that the measure of a subset X of G is construed as the probability that a random element of G lies in X. It is now natural to ask questions such as: what is the probability that a random k-tuple of elements generates G? Formally, this probability is defined as

$$P(G,k) = \mu\left\{(x_1,\ldots,x_k) \in G^{(k)} \mid \langle x_1,\ldots,x_k\rangle = G\right\}, \tag{11.1}$$

where μ denotes also the product measure on $G^{(k)}$.

When G is finite we have $\mu(X) = |X| \,/\, |G|$ for each subset X, so the concept of probability in profinite groups reduces to the usual one in finite groups. Indeed, this second path is really a special case of the first one, because (under certain reasonable conditions)

$$\mu(X) = \inf \frac{|XN/N|}{|G/N|} \tag{11.2}$$

as N ranges over the open normal subgroups of G, so the probability of an event in G is a limit of probabilities associated to some family of finite groups. However, as usual, the profinite language provides a suggestive framework for articulating questions and constructing proofs.

The connection of these ideas to subgroup growth is made by associating to each tuple of elements in the profinite group G the (closed) subgroup generated

(topologically) by that tuple. (Henceforth, when talking about profinite groups we shall understand 'subgroup' to mean 'closed subgroup' and 'generated' to mean 'topologically generated'.) The most striking applications of probabilistic methods to subgroup growth questions (though by no means the only ones) concern *maximal subgroup growth*; these are based on the following major theorem:

Theorem 11.1 *Let G be a profinite group. Then G has polynomial maximal subgroup growth if and only if $P(G,k)$ is positive for some natural number k.*

A profinite group G is said to be *positively finitely generated*, or PFG, if $P(G,k)$ is positive for some natural number k. We call G a PMSG group if G has polynomial maximal subgroup growth. Thus the theorem asserts that PFG is equivalent to PMSG. The 'only if' direction is easy, and will be proved in Section 2.

Now to say that $P(G,k)$ is positive means that the set of generating k-tuples in G has positive measure (in $G^{(k)}$), hence is certainly non-empty; so it implies in particular that G can be generated by k elements. Thus we immediately derive the following corollary (from the *easier* implication in Theorem 1!); this makes no mention of probability and may be taken as justifying the chapter heading:

Corollary 11.2 *Every profinite group with PMSG is finitely generated. In particular this holds for every profinite group with PSG.*

Applying this to the profinite completion of an abstract group gives

Corollary 11.3 *Let G be a group with polynomial maximal subgroup growth. Then there exists $k \in \mathbb{N}$ such that every finite quotient group of G can be generated by k elements.*

In fact the proof will show that if $m_n(G) \leq n^\gamma$ for all n then we can take $k = \lceil \gamma + 2 \rceil$.

Applying Theorem 11.1 in conjunction with Theorem 3.5, we see that very many groups are positively finitely generated:

Corollary 11.4 *Let G be a finitely generated profinite group. Then G is PFG unless every finite group occurs as an upper section of G.*

This applies, for example, to the congruence completion of every arithmetic group. However, it is not the whole story: it is shown in [Mann & Shalev 1997] that the Cartesian product of any collection of distinct finite nonabelian simple groups has PMSG; further examples are provided by the following theorem, proved in section 3:

Theorem 11.5 *Let G be a group (abstract or profinite) such that*

$$s_n^{\triangleleft}(G) \leq (\log n)^\gamma$$

for all n, where γ is a constant. Then

$$m_n(G) \leq cn^{5+2\gamma}$$

for all n, where c is an absolute constant.

Thus 'logarithmic' *normal* subgroup growth implies polynomial maximal subgroup growth, so every profinite group with this property is PFG, and hence in particular is finitely generated. Finitely generated abstract groups with this property that have arbitrarily large finite alternating groups as upper composition factors are described at the end of §13.4.

The harder implication in Theorem 11.1 depends on detailed information about the subgroup structure of finite simple groups, and in particular on CFSG; the proof is outlined in Section 3. It shows in fact that if $P(G,k) > 0$ then $m_n(G) = o(n^{k+6})$.

In Section 2 we establish

Proposition 11.6 *The class of profinite PFG groups is closed under extensions.*

This now gives

Corollary 11.7 *The class of PMSG groups is closed under extensions.*

Like the analogous result for polynomial subgroup growth (Corollary 10.4), this applies to *all groups*, not just profinite groups; indeed, suppose that $N \lhd G$ and both N and G/N have PMSG. Then $\widehat{G}$ is an extension of $\overline{N}$ by $\widehat{G}/\overline{N}$, where $\overline{N}$ is the closure of N in $\widehat{G}$; now $\widehat{G}/\overline{N}$ is isomorphic to $\widehat{G/N}$ and $\overline{N}$ is a homomorphic image of $\widehat{N}$, so both $\overline{N}$ and $\widehat{G}/\overline{N}$ are profinite PMSG groups, hence $\widehat{G}$ has PMSG and then so does G. We do not know a non-probabilistic proof for this corollary – a striking result, since a maximal subgroup of G does not generally intersect N in a maximal subgroup of N.

The probabilistic approach also yields other kinds of information. Write

$$a_{n,d}(G)$$

to denote the number of *d-generator* subgroups of index n in a group G. In Section 4 we establish

Theorem 11.8 *Let G be a group that does not involve $\mathrm{Alt}(m+1)$ as an upper section. Then for each $d \in \mathbb{N}$ there exist $C = C(m,d)$ and $k = k(m,d)$ such that*

$$a_{n,d}(G) \leq Cn^k$$

for all n.

The proof is given for a profinite group G. Applied to the profinite completion of an abstract group, it yields the analogous estimate for the number $\overline{a}_{n,d}$ of index-n subgroups H such that every finite quotient of H can be generated by d elements; of course, $a_{n,d} \leq \overline{a}_{n,d}$. This result is a broad generalisation of the fact, established in Chapter 10, that every group of finite upper rank has PSG – since if G has upper rank r then $a_n(G) = \overline{a}_{n,r}(G)$ for every n.

In the reverse direction, we saw in that chapter that if the PSG group G is *prosoluble* then the numbers $d(H)$ are bounded by a constant (the rank of G), but in general they need not be. The next theorem shows that their growth is in any case extremely slow (compared for example with the *linear* growth $d(H) \sim |F : H|\, d(F)$ for a free profinite group F):

Theorem 11.9 *Let G be a profinite PSG group. Then there exists a constant C such that*

$$d(H) \leq C\sqrt{\log |G : H|}$$

for every open subgroup H of G.

Like Corollary 11.2, this is derived from elementary probabilistic considerations quite independent of the difficult classification theorem of Chapter 10.

The quantity $P(G, k)$ is particularly transparent when G is a pro-p group. This is discussed in Section 5, where we give two applications. The first, analogous to Theorem 11.8, concerns the number $a^{\lhd}_{n,r}(G)$ of *normal* subgroups of index n in G that can be generated (as normal subgroup) by r elements:

Theorem 11.10 *Let G be a finitely generated pro-p group. Then for each r,*

$$a^{\lhd}_{n,r}(G) = o(n^r) \quad \text{as } n \to \infty.$$

This (perhaps rather recondite) result has the following interesting consequence:

Corollary 11.11 *Let $h(p^k, r)$ denote the number of (isomorphism types) of groups of order p^k that have a finite presentation with r relations. Then*

$$h(p^k, r) = o(p^{kr}) \quad \text{as } k \to \infty.$$

For comparison, recall that the number of *d-generator* groups of order p^k grows roughly like p^{k^2} (Chapter 3). The corollary follows on applying the theorem to the free pro-p group G on r generators: for every finite presentation of a finite group needs at least as many relations as generators**,** so the groups being counted take the form G/N where N is the normal subgroup of G generated normally by the r relators.

The final, rather surprising, application shows how probabilistic considerations can sometimes deliver exact results, not just estimates. It is a (virtually one-line) proof of the formal Dirichlet series identity

$$\sum_{n=1}^{\infty} \frac{a_n(\mathbb{Z}^d)}{n^s} = \prod_{i=0}^{d-1} \zeta(s-i) \tag{11.3}$$

where $\zeta(s)$ is the Riemann zeta function This will be proved again, in several different ways, in Chapter 15, where it is the starting point for the theory of 'subgroup-counting zeta functions'.

We begin in Section 1 by recalling some essential features of the Haar measure on profinite groups.

11.1 The probability measure

The distinguishing features of a Haar measure μ on a compact topological group are (1) finiteness and (2) translation-invariance (left or right, each of which implies the other). If the group G is profinite and we fix $\mu(G) = 1$, in which case μ is said to be *normalized*, it follows that

$$\mu(gH) = \mu(Hg) = \frac{1}{|G : H|}$$

for every coset of every open subgroup H of G. Let us call such cosets *basic open sets*. If the set

$$X = \bigcup x_{ij} H_j \cup \bigcup K_l y_{kl}$$

is the union of a finite collection of basic open sets, we can find an open normal subgroup N of G contained in $\bigcap_j H_j \cap \bigcap_l K_l$, and then X is equal to the union of finitely many, say n, cosets of N, in which case

$$\mu(X) = n\mu(N) = \frac{n}{|G : N|}.$$

If X is the union of a *countable* family of basic open sets, we can write X as an ascending union $X = \bigcup_{i=1}^{\infty} X_i$ where each X_i is a finite union as above, and obtain

$$\mu(X) = \lim_{i \to \infty} \mu(X_i).$$

In particular, if the set $\mathcal{N}$ of all open normal subgroups is *countable*, this determines the measure of every open set in G, and thus also of every closed set since

$$\mu(G \setminus X) = 1 - \mu(X).$$

In this case G is said to be *countably based*; this applies for example when G is finitely generated.

For a detailed justification of these observations, including a proper definition of the Haar measure in the general case of a non-countably-based profinite group, the reader is referred to Chapter 16 of the book [FJ] by Fried and Jarden. We shall make tacit use of several basic facts established there in the general context of measurable sets, but will usually apply them only to sets that are closed or open. These facts include the existence and uniqueness of the normalized Haar measure μ, as well as

(1) the product measure on $G^{(k)}$ is the same as the Haar measure of $G^{(k)}$ ([FJ], Prop. 16.10);

(2) if $X \subseteq Y$ are measurable sets then $\mu(X) \leq \mu(Y)$;

(3) if the measurable sets X_i are pairwise disjoint then

$$\mu(\bigcup_{i=1}^{\infty} X_i) = \sum_{i=1}^{\infty} \mu(X_i);$$

(4) if the sets X_i are measurable then

$$\mu(\bigcup_{i=1}^{\infty} X_i) \leq \sum_{i=1}^{\infty} \mu(X_i);$$

this follows from (3) and (2) on replacing X_i by $X_i \setminus (X_1 \cup \ldots \cup X_{i-1})$ for each $i > 1$;

(5) if the sets X_i are measurable then

$$\mu(\bigcup_{i=1}^{\infty} X_i) = \lim_{i \to \infty} \mu(X_i) = \sup \mu(X_i) \text{ if } X_i \subseteq X_{i+1} \text{ for all } i$$

$$\mu(\bigcap_{i=1}^{\infty} X_i) = \lim_{i \to \infty} \mu(X_i) = \inf \mu(X_i) \text{ if } X_i \supseteq X_{i+1} \text{ for all } i.$$

As an illustration, let us derive the identity (11.2) stated in the introduction, assuming that G is *countably based* and that X is a *closed* subset of G. In this case, $X = \bigcap_{i=1}^{\infty} XN_i$ where $N_1 > N_2 > \ldots$ is a descending chain in $\mathcal{N}$. From (5) we have

$$\begin{aligned} \mu(X) &= \inf_i \mu(XN_i) \\ &\geq \inf_{N \in \mathcal{N}} \mu(XN) \geq \mu(X) \end{aligned}$$

since $X \subseteq XN$ for each N; so $\mu(X) = \inf_{N \in \mathcal{N}} \mu(XN)$. Now for each $N \in \mathcal{N}$ the set XN is the union of $|XN/N|$ cosets of N, so $\mu(XN) = |XN/N| \, \mu(N) = |XN/N| \, / \, |G : N|$, and (11.2) follows.

Lemma 11.1.1 *Assume that G is countably based. Let K be a closed normal subgroup of G and $\pi : G \to G/K$ the natural epimorphism. If X is a closed subset of G then $\mu(\pi(X)) \geq \mu(X)$; if Y is a closed subset of G/K then $\mu(\pi^{-1}(Y)) = \mu(Y)$.*

Proof. Using (11.2) we reduce to the case where G is a finite group. In that case, if $X \subseteq G$ then $|\pi(X)| \leq |X| \, / \, |K|$, with equality if $X = \pi^{-1}(Y)$; both claims follow directly. ■

11.2 Generation probabilities

Throughout this section, G denotes a profinite group and μ the normalized Haar measure, on G or on some direct power $G^{(k)}$. Now fix k and write

$$X(G,k) = \left\{ \mathbf{x} \in G^{(k)} \mid \langle \underline{\mathbf{x}} \rangle = G \right\},$$

where $\underline{\mathbf{x}} = \{x_1, \ldots, x_k\}$ when $\mathbf{x} = (x_1, \ldots, x_k)$ (and $\langle \underline{\mathbf{x}} \rangle$ means the *closed* subgroup *topologically* generated by the set $\underline{\mathbf{x}}$). Since a subset T fails to generate G if and only if T is contained in some maximal open subgroup of G, it is clear that

$$G^{(k)} \setminus X(G,k) = \bigcup_{M \max G} M^{(k)}, \tag{11.4}$$

where $M \max G$ means 'M is a maximal (proper) open subgroup of G'. This is an open subset of $G^{(k)}$, so $X(G,k)$ is closed, hence measurable. We may therefore define

$$P(G,k) = \mu(X(G,k)) :$$

the *probability that a random k-tuple generates G*. Thus $0 \leq P(G,k) \leq 1$, and if $P(G,k) > 0$ then $d(G) \leq k$ (for if $d(G) > k$ then the set $X(G,k)$ is empty). Using (11.2) we can interpret $P(G,k)$ in the following way:

$$P(G,k) = \inf \{ P(G/N,k) \mid N \lhd G,\ N \ \text{ open} \}; \tag{11.5}$$

when G/N is a finite group, of course, $P(G/N,k)$ is simply the proportion of all k-tuples in G/N that generate G/N. If G is finitely generated this follows directly from (11.2), since in that case G is countably based (and X is a closed set). If G is not finitely generated then $P(G,k) = 0$, as we have just observed; on the other hand, there exist finite quotients of G that cannot be generated by k elements, since $d(G) = \sup d(G/N)$; consequently $P(G/N,k) = 0$ for some open normal subgroup N of G and the right-hand side of (11.5) is also equal to zero.

Proposition 11.2.1 *Let K be a closed normal subgroup of G and let H be an open subgroup of G. Then*

(i) $P(G/K,k) \geq P(G,k)$;

(ii) $P(G,k+l) \geq P(G/K,l)P(K,k)$;

(iii) $P(G,k+d) \geq |G:H|^{-(k+d)} P(H,k)$ *for any integer* $d \geq \log |G:H|$.

Proof. We may assume that G is finitely generated, since otherwise the right-hand side of each inequality is zero. Write $\pi_k : G^{(k)} \to (G/K)^{(k)}$ for the natural map. Then π_k maps $X(G,k)$ into $X(G/K,k)$, and applying Lemma 11.1.1 to the pair $K^{(k)} \lhd G^{(k)}$ we deduce that

$$\mu(X(G/K,k)) \geq \mu(X(G,k)),$$

which is (i).

For (iii), note that $G = \langle H, y_1, \ldots, , y_d \rangle$ for suitable elements y_i, since d is an upper bound for the length of any subgroup chain between H and G. Now put $X = X(H,k)$. Then

$$X \times Hy_1 \times \cdots \times Hy_d \subseteq X(G, k+d).$$

Now (iii) follows since $\mu(X) = P(H,k)\mu(H^{(k)}) = |G:H|^{-k} P(H,k)$ and $\mu(Hy_i) = |G:H|^{-1}$ for each i.

The proof of (ii) is more transparent when G is a finite group; the general case follows from this one on applying (11.5). Suppose that $\mathbf{x} \in X(K,k)$ and $\mathbf{y} \in \pi_l^{-1}(X(G/K,l)$; then the subgroup $\langle \underline{\mathbf{y}} \rangle$ of G covers the quotient G/K, so $|\langle \underline{\mathbf{y}} \rangle| \geq |G:K|$. If $u_1, \ldots, u_k \in \langle \underline{\mathbf{y}} \rangle$ then

$$\langle x_1 u_1, \ldots, x_k u_k, y_1, \ldots, y_l \rangle = G;$$

therefore $P(G, k+l)$ is at least equal to $|G|^{-(k+l)}$ times the number of such $k+l$-tuples. This number is at least

$$|K|^l \, |X(G/K,l)| \cdot |G:K|^k \, |X(K,k)| = |G|^{k+l} \, P(G/K,l) P(K,k).$$

■

Thus the class of profinite groups with PFG is closed under extensions. In particular it follows that a profinite group is PFG if it has an open normal PFG subgroup; intriguingly, however, the answer to the following question is unknown:

Problem *Is every open subgroup of a PFG group itself a PFG group?*

If we assume that G has only a finite number $m_n(G)$ of maximal open subgroups of index n for each n, then the set of all maximal open subgroups is countable, and we obtain the following estimate from (11.4):

$$\begin{aligned} 1 - P(G,k) &= \mu\left(\bigcup_{M \max G} M^{(k)} \right) \\ &\leq \sum_{M \max G} \mu(M^{(k)}) \\ &= \sum_{M \max G} |G:M|^{-k} = \sum_{n>1} m_n(G) n^{-k}. \end{aligned} \tag{11.6}$$

This is all that is needed to establish the easier direction of Theorem 11.1:

Proposition 11.2.2 *Let γ be a positive constant, and suppose that $m_n(G) \leq n^\gamma$ for every n. Then $P(G,k) > \frac{1}{3}$ for every integer $k \geq \gamma + 2$.*

Proof. Indeed,

$$1 - P(G,k) \leq \sum_{n>1} m_n(G) n^{-k} \leq \sum_{n=2}^{\infty} n^{\gamma - k} \leq \sum_{n=2}^{\infty} n^{-2} = \pi^2/6 - 1 < 0.65$$

so $P(G,k) > 0.35$. ■

Essentially the same argument shows that if G has PMSG then in fact $P(G,k) \to 1$ as $k \to \infty$.

11.3 Maximal subgroups

The proof of (the harder direction in) Theorem 11.1 depends on some deep finite group theory and on some further probability theory. Let us begin with the latter, which is quite elementary. The result we need is the so-called *Borel-Cantelli Lemma* (we use the notation introduced in Section 1):

Proposition 11.3.1 *Let (X_i) be a sequence of measurable subsets of G, and put*

$$X = \bigcap_{n=1}^{\infty} \left(\bigcup_{i=n}^{\infty} X_i \right).$$

(i) *If the series $\sum_{n=1}^{\infty} \mu(X_i)$ is convergent then $\mu(X) = 0$.*
(ii) *If the sets X_i are pairwise independent and the series $\sum_{n=1}^{\infty} \mu(X_i)$ is divergent then $\mu(X) = 1$.*

Note that the set X consists precisely of those elements that belong to infinitely many of the X_i. Here two sets X and Y are said to be *independent* if

$$\mu(X \cap Y) = \mu(X)\mu(Y).$$

The proof of Proposition 11.3.1 is given in the **Probability** window.

When applying part (ii) of the Borel-Cantelli Lemma, we need to recognise when certain sets are independent. The relevant case is

Lemma 11.3.2 *Let A and B be maximal open subgroups of G with distinct cores. Then for each k, the subsets $A^{(k)}$ and $B^{(k)}$ of $G^{(k)}$ are independent.*

Proof. Put $A_0 = \mathrm{core}_G A$ and $B_0 = \mathrm{core}_G B$. If $A_0 \leq B$ then $A_0 \leq B_0$, so B_0 is not contained in A_0 and hence also not contained in A. Thus we may suppose without loss of generality that A_0 is not contained in B, in which case $A_0 B = G$, and hence $AB = G$. This implies that $|G : A \cap B| = |G : A|\,|G : B|$, whence

$$\mu(A^{(k)} \cap B^{(k)}) = |G : A \cap B|^{-k} = |G : A|^{-k}\,|G : B|^{-k} = \mu(A^{(k)})\mu(B^{(k)}).$$

■

Suppose now that $P(G, k) > 0$. Then G is finitely generated, so has only a countable collection of maximal subgroups. Let us call two maximal subgroups *equivalent* if they have the same core, and in each equivalence class choose a representative having minimal index in G. Let this set of representatives be $(M_i)_{i \in \mathbb{N}}$, and let q_n denote the number of indices i such that $|G : M_i| = n$.

Now consider the series

$$\sum_{i=1}^{\infty} \mu({M_i}^{(k)}) = \sum_{i=1}^{\infty} |G : M_i|^{-k} = \sum_{n>1} q_n n^{-k}.$$

We claim that this series is convergent. Indeed, according to Borel-Cantelli (ii) and the preceding lemma, if the series diverges then the subset of $G^{(k)}$ consisting of tuples $\mathbf{x}$ that lie in only finitely many of the sets ${M_i}^{(k)}$ has measure zero. But if $\mathbf{x} \in X(G,k)$ then $\mathbf{x}$ lies in *none* of the ${M_i}^{(k)}$; thus $P(G,k) = \mu(X(G,k)) = 0$, contradicting hypothesis.

It follows that

$$q_n = o(n^k).$$

To deduce that G has PMSG, it now remains to bound $m_n(G)$ in terms of q_n. This is where finite group theory comes in.

Theorem 11.3.3 *There is an absolute constant c such that, in any group G, the number of core-free maximal subgroups of index n in G is at most cn^5 for each n.*

A subgroup M of G is *core-free* if $\mathrm{core}_G M = 1$; of course, if G has *any* such subgroup M of finite index then G is a finite group. The theorem implies that a group has at most cn^5 inequivalent faithful primitive permutation representations of degree n. For the proof, we must refer to the paper [Mann & Shalev 1997]. The result established there is slightly weaker, with the exponent 5 replaced by $d(G)$; the present version may be obtained by combining their proof with that of Lemma 2.8(a) in [Lucchini & Morini 2002] and a little extra argument. (The original, weaker, theorem suffices for the present application.)

Given Theorem 11.3.3 we can now complete the

Proof of Theorem 11.1. Suppose that the profinite group G satisfies $P(G,k) > 0$. Then $d(G) \leq k$. Let $N_i = \mathrm{core}_G M_i$. If M is a maximal subgroup of index n in G then $\mathrm{core}_G M = N_i$ for some i such that $|G : M_i| \leq n$; the number of possibilities for i is therefore at most $q_2 + \cdots + q_n$. Applying Theorem 11.3.3 to G/N_i we see that given N_i, the number of such maximal subgroups M is at most cn^5. On the other hand, we have shown above that $q_n = o(n^k)$. The number of possibilities for M is therefore

$$m_n(G) \leq cn^5(q_2 + \cdots + q_n) = o(n^{k+6}).$$

Thus G has polynomial maximal subgroup growth, and the proof is complete.

Now suppose that G is a profinite group with

$$s_n^{\lhd}(G) \leq (\log n)^\gamma$$

for all n. Since $|G : \mathrm{core}_G M| \leq n!$ when $|G : M| = n$, Theorem 11.3.3 gives

$$\begin{aligned} m_n(G) &\leq cn^5 \cdot s_{n!}^{\lhd}(G) \\ &\leq cn^5(\log n!)^\gamma \leq cn^{5+2\gamma}, \end{aligned}$$

and Theorem 11.5 follows.

Before leaving this topic, we should mention a striking application of Theorem 11.3.3, due to L. Pyber.

Theorem 11.3.4 [Pyber (a)] *There is an absolute constant c such that for every finite group G, the number of maximal subgroups of G is at most $|G|^c$.*

It is interesting to compare this with Theorem 10.5.1. We showed there that if $s(\overline{G}) \leq \left|\overline{G}\right|^c$ for every finite quotient $\overline{G}$ of a group G, then G has PSG, of degree bounded in terms of c; thus a polynomial bound for the number of *all* subgroups is a strong structural restriction on a finite group, whereas Pyber's theorem shows that a corresponding bound for *maximal* subgroups is no restriction at all: adapting the language of Chapter 10 one can say that *every* group has 'weak PMSG'. This is another aspect of the principle illustrated by Theorem 3.1, that polynomial *maximal* subgroup growth is a relatively mild condition on groups.

11.4 Further applications

As before G denotes a profinite group and μ the normalized Haar measure on G. Define

$$X'(G,k) = \left\{ \mathbf{x} \in G^{(k)} \mid \langle \underline{\mathbf{x}} \rangle \leq_o G \right\}$$

where $H \leq_o G$ means H is an *open* subgroup of G. Thus $X'(G,k)$ is the disjoint union

$$X'(G,k) = \dot{\bigcup_{H \leq_o G}} X(H,k).$$

If $X'(G,k)$ is non-empty then G has at least one k-generator open subgroup, so G is finitely generated and hence countably based, and the union on the right has countably many terms. So writing

$$Q(G,k) = \mu(X'(G,k))$$

we have

$$\begin{aligned} Q(G,k) &= \sum_{H \leq_o G} \mu(X(H,k)) \\ &= \sum_{H \leq_o G} P(H,k)\mu(H^{(k)}) = \sum_{H \leq_o G} P(H,k)\,|G:H|^{-k}\,. \end{aligned} \tag{11.7}$$

From this we may draw several conclusions.

(1)

$$\begin{aligned} &P(G,k) \leq Q(G,k), \\ &Q(G,k) > 0 \Longrightarrow P(G,k+d) > 0 \ \text{ for some } d; \end{aligned}$$

so $Q(G,k)$ is positive for some k if and only if G is PFG. The first inequality is clear, and the second follows from Proposition 11.2.1(iii), taking $d = \lceil \log |G:H| \rceil$ where H is some open subgroup of G for which $P(H,k) > 0$.

(2) Fix a real number $c \in (0,1]$ and let $\mathcal{H}(k,c)$ denote the set of all open subgroups H of G such that $P(H,k) \geq c$. Write $a_n(k,c)$ for the number of $H \in \mathcal{H}(k,c)$ such that $|G:H| = n$. Then

$$c \cdot \sum_{n=1}^{\infty} a_n(k,c) n^{-k} \leq \sum_{H \in \mathcal{H}(k,c)} P(H,k) \, |G:H|^{-k} \leq Q(G,k) \leq 1.$$

Consequently

$$a_n(k,c) \leq c^{-1} n^k$$

for each n. Thus we have the *polynomial growth* of certain families of open subgroups in G.

Suppose for example that G *does not involve* $\mathrm{Alt}(m+1)$ *as an upper section*. Then every finite quotient of G belongs to the class $\mathcal{C}_m$ of finite groups that do not involve $\mathrm{Alt}(m+1)$. Now fix a positive integer d and let F be the free pro-$\mathcal{C}_m$ group on d generators. Theorem 11.4 tells us that F is a PFG group: so for some k we have $P(F,k) > 0$. Now every d-generator open subgroup H of G is an image of F, hence satifies

$$P(H,k) \geq P(F,k)$$

by Proposition 11.2.1(i), and so lies in $\mathcal{H}(k,c)$ where $c = P(F,k)$. It follows that

$$a_{n,d}(G) \leq a_n(k,c) \leq c^{-1} n^k$$

for each n, and we have established Theorem 11.8 (with $C = c^{-1}$); note that c and k here depend only on m and d.

(3) Suppose G has the property that $P(H,k) = q_k$ is *constant* over all open subgroups H of G. Then from (11.7) we have

$$\sum_{n=1}^{\infty} a_n(G) n^{-k} = \sum_{H \leq_o G} |G:H|^{-k} = q_k^{-1} Q(G,k). \tag{11.8}$$

As we shall see in the next section, this can be used in some circumstances to determine the numbers $a_n(G)$.

For the rest of this section, we assume that the profinite group G has *polynomial subgroup growth*, so there exists $c \in \mathbb{N}$ such that

$$a_n(G) \leq n^c$$

for all n.

Lemma 11.4.1 *If* $a_n(G) = O(n^{k-1-\varepsilon})$ *where* $\varepsilon > 0$ *then* $Q(G,k) = 1$.

Proof. Let $\mathbf{x} \in G^{(k)}$. If the closed subgroup $\langle \underline{\mathbf{x}} \rangle$ is not open in G then it is contained in infinitely many open subgroups; from the Borel-Cantelli Lemma, Proposition 11.3.1(i), the probability of this event is zero if the series

$$\sum_{H \leq_o G} \mu(H^{(k)}) = \sum_{n=1}^{\infty} a_n(G) n^{-k}$$

is convergent, which indeed it is. ■

Now we give the

Proof of Theorem 11.9. Let H be an open subgroup of index $n \geq 2$ in G. We shall show that $d(H) \leq C\sqrt{\log n}$ where C depends only on c. For $k, m \in \mathbb{N}$ let

$$P(H, k, m)$$

denote the probability that a random k-tuple in H generates a subgroup of index $> m$ in H. Thus $P(H, k, m) = \mu_H(Y)$ where μ_H is the normalized Haar measure on H and

$$Y = \bigcup_{\substack{L \leq_o H \\ |H:L| > m}} L^{(k)} \subseteq H^{(k)}$$

(note that each closed subgroup of infinite index is contained in open subgroups of arbitrarily large finite index). It follows that

$$\begin{aligned} P(H, k, m) \leq \sum_{\substack{L \leq_o H \\ |H:L| > m}} |H : L|^{-k} &\leq \sum_{j > m} a_j(H) j^{-k} \\ &\leq \sum_{j > m} a_{nj}(G) j^{-k} \leq n^c \sum_{j > m} j^{c-k}. \end{aligned}$$

Now choose

$$r = \left\lceil \sqrt{c \log n} \right\rceil, \ m = \left\lceil 2^{\sqrt{c \log n}} \right\rceil, \ k = c + r + 1.$$

Then

$$\sum_{j > m} j^{c-k} \leq \sum_{j > m} j^{-(r+1)} < \int_m^{\infty} x^{-(r+1)} dx = r^{-1} m^{-r} \leq m^{-r},$$

and

$$m^r \geq 2^{r\sqrt{c \log n}} \geq 2^{c \log n} = n^c,$$

so $P(H, k, m) < n^c m^{-r} \leq 1$.

It follows that H contains at least one k-generator open subgroup L of index at most m. Then H is generated by L together with at most $\log |H : L| \leq \log m$

further elements, so

$$\begin{aligned} d(H) &\leq k + \log m \\ &\leq c + (1 + \sqrt{c \log n}) + 1 + (1 + \sqrt{c \log n}) \\ &\leq C\sqrt{\log n} \end{aligned}$$

where $C = 2\sqrt{c} + c + 3$, say. This completes the proof.

11.5 Pro-p groups

Let G be a pro-p group, with $d(G) = d$ finite. A set $\{x_1, \ldots, x_k\}$ generates G if and only its image $\{x_1\Phi(G), \ldots, x_k\Phi(G)\}$ in $G/\Phi(G)$ generates $G/\Phi(G)$; so

$$P(G, k) = P(G/\Phi(G), k)$$

by Lemma 11.1.1. Now $G/\Phi(G) \cong \mathbb{F}_p^{(d)} = V$, say. The generating k-tuples in V are represented by $d \times k$ matrices of rank d over $\mathbb{F}_p$; since row rank equals column rank, the number of such matrices is just the number of linearly independent d-tuples in $\mathbb{F}_p^{(k)}$, which is

$$(p^k - 1)(p^k - p) \ldots (p^k - p^{d-1})$$

(this is zero if $k < d$). Dividing by $\left|V^{(k)}\right| = p^{kd}$ we get

$$\begin{aligned} P(G, k) = P(V, k) &= \prod_{j=0}^{d-1} (1 - p^{j-k}) \qquad (11.9) \\ &= \Pi_p(d, k), \quad \text{say.} \end{aligned}$$

Thus *every finitely generated pro-p group is positively finitely generated*. Of course, this is a very special case of Theorem 11.1, since every maximal subgroup has index p; but here we have the added feature that if G can be generated by d elements, then d elements generate G with positive probability – this is not the case e.g. for $G = \widehat{\mathbb{Z}}$, a one-generator group for which $P(G, 1) = 0$ (as we shall see below).

Let us consider now the number $a_{n,r}^{\lhd}(G)$ of normal subgroups of index n in the pro-p group G that can be normally generated by r elements. Let

$$P^G(N, k)$$

denote the probability that a random k-tuple in the (closed) normal subgroup N of the pro-p group G generates N as a normal subgroup: that is, the measure (w.r.t. $\mu_{N^{(k)}}$) of the set

$$\left\{ \mathbf{x} \in N^{(k)} \mid \langle \underline{\mathbf{x}}^G \rangle = N \right\}.$$

Let $\mathcal{N}(k,c)$ denote the set of all open normal subgroups N of G such that $P^G(N,k) \geq c$, and write $b_n(k,c)$ for the number of $N \in \mathcal{N}(k,c)$ such that $|G:N| = n$. Just as in the preceding section we infer that

$$c \cdot \sum_{n=1}^{\infty} b_n(k,c) n^{-k} \leq \sum_{N \in \mathcal{N}(k,c)}^{\infty} P^G(N,k) \, |G:N|^{-k} \leq 1,$$

and hence that $b_n(k,c) = o(n^k)$ provided $c > 0$.

To estimate the numbers $P^G(N,k)$, note that $\langle \underline{\mathbf{x}}^G \rangle = N$ if and only if $\langle \underline{\mathbf{x}}^G \rangle \, \Phi_G(N) = N$ where $\Phi_G(N) = [N,G]N^p$, and that this holds if and only if $\langle \underline{\mathbf{x}} \rangle \, \Phi_G(N) = N$. It follows by a now familiar argument that

$$\begin{aligned} P^G(N,k) &= P(N/\Phi_G(N), k) \\ &= \Pi_p(s,k) \end{aligned}$$

where $s = d(N/\Phi_G(N))$; and reversing this argument we see that s is exactly the minimal number of generators required by N as a normal subgroup of G. If N can be normally generated by r elements then $s \leq r$ and so $P^G(N,k) = \Pi_p(s,k) \geq \Pi_p(r,k)$; thus $N \in \mathcal{N}(k,c)$ where $c = \Pi_p(r,k)$.

Taking $k = r$ we deduce that

$$a_{n,r}^{\triangleleft}(G) \leq b_n(r,c) = o(n^r)$$

where $c = \Pi_p(r,r) > 0$; and we have proved Theorem 11.10.

Next, consider the example $G = \mathbb{Z}_p^{(d)}$. In this case, every open subgroup H of G is isomorphic to G, so $P(H,k) = P(G,k) = \Pi_p(d,k)$. Also $Q(G,k) = 1$ for every $k > d+1$, by Lemma 11.4.1, so for such k the formula (11.8) reads

$$\sum_{n=1}^{\infty} a_n n^{-k} = \Pi_p(d,k)^{-1}$$

where $a_n = a_n(\mathbb{Z}_p^{(d)})$. Writing $X = p^{-k}$ and noting that $a_n = 0$ when n is not a power of p this becomes

$$\sum_{i=0}^{\infty} a_{p^i} X^i = \prod_{j=0}^{d-1} (1 - p^j X)^{-1}. \tag{11.10}$$

On the right we have a rational function of X and on the left a power series in X, which converges to the same value when $X = p^{-k}$ for any large integer k. Therefore (11.10) is an *identity*, and by multiplying out the geometric series $\sum_n (p^j X)^n$ we obtain explicit formulae for the numbers a_{p^i}.

Let us replace X by p^{-s} where s is a complex variable. Then $(1-X)^{-1} = (1-p^{-s})^{-1}$ is just the p-factor $\zeta_p(s)$ in the Euler product expansion of the Riemann zeta function $\zeta(s)$, so we can restate our conclusion as

$$\sum_{i=0}^{\infty} a_{p^i} p^{-is} = \zeta_p(s)\zeta_p(s-1)\ldots\zeta_p(s-d+1).$$

Leaving pro-p groups now, let us apply this to the group $\mathbb{Z}^{(d)}$. It is easy to see that if $n = p_1^{e_1} \dots p_r^{e_r}$ where $p_1, \dots, p_r$ are distinct primes then

$$a_n(\mathbb{Z}^{(d)}) = \prod_{j=1}^{r} a_{p_j^{e_j}}(\mathbb{Z}^{(d)}) = \prod_{j=1}^{r} a_{p_j^{e_j}}(\mathbb{Z}_{p_j}^{(d)}).$$

This now implies the following identity of formal Dirichlet series:

$$\begin{aligned}\sum_{n=1}^{\infty} a_n(\mathbb{Z}^{(d)}) n^{-s} &= \prod_p \sum_{i=0}^{\infty} a_{p^i}(\mathbb{Z}_p^{(d)}) p^{-is} \\ &= \prod_p \zeta_p(s)\zeta_p(s-1)\dots\zeta_p(s-d+1) \\ &= \zeta(s)\zeta(s-1)\dots\zeta(s-d+1).\end{aligned}$$

The first equality, a formal consequence of unique factorisation, generalizes to all nilpotent groups. It will be discussed in Chapter 15, where we exhibit several different ways of deriving this remarkable identity.

As an exercise, the reader may derive the same identity by applying the above method directly to the group $\widehat{\mathbb{Z}^{(d)}}$, rather than going via the factors $\mathbb{Z}_p^{(d)}$. The main step is to establish that

$$P(\widehat{\mathbb{Z}^{(d)}}, k) = \left(\zeta(k)\zeta(k-1)\dots\zeta(k-d+1)\right)^{-1},$$

(this includes the cases $k \leq d$, interpreting $\zeta(1)^{-1}$ as 0). Applying (11.5) reduces this to evaluating $P(A, k)$ for a finite abelian group A; then note that

$$P(A, k) = \prod_p P(A_p, k),$$

where A_p is the p-component of A, and use (11.9). This approach replaces the multiplicative property of a_n with that of $P(A, k)$, and the identity theorem for power series with the identity theorem for Dirichlet series; the essential – combinatorial – content is of course the same in both approaches.

Notes

The study of generation probabilities in the style of this chapter was initiated by [**Jarden 1975**], who introduced the use of the Borel-Cantelli lemma in such investigations and applied it to examine the probability of generating a procyclic group. See [**FJ**], §16, where Fried and Jarden also raised the question of probabilistic generation for free profinite groups. This was taken up by [**Kantor & Lubotzky 1990**], who determine several families of PFG groups, and show that non-abelian free profinite groups are not PFG.

Most results of this chapter that are not otherwise attributed are due to [**Mann 1996**]. This paper was the first to develop the topic systematically

(and introduced the term PFG). In particular, Mann proved the easier direction of Theorem 11.1 and many special cases of the harder direction, including the case of virtually prosoluble groups. The paper introduces several other ideas, including the definition of a 'probabilistic zeta function' (see §15.2 below), and raises a number of problems.

Theorem 11.1 is due to [**Mann & Shalev 1997**]. They prove that if G is a finite almost-simple group, then $m_n(G) \leq cn^{1.9}$ for every n, where c is an absolute constant; using this, they deduce that a finite d-generator group has at most $2n^d$ core-free maximal subgroups of index n, if d is sufficienetly large; as remarked above this suffices for Theorem 11.1. The stronger Theorem 11.3.3 is due to **L. Pyber** (unpublished); by a more careful argument he obtains the still sharper bound cn^2. Further applications of this result appear in [**Lubotzky (a)**], where the "expected number" of random elements required to generate a finite d-generator group is determined.

[**Bhattacharjee 1994**] proves directly that infinitely iterated wreath products of finite alternating groups are PFG; this shows that Corollary 11.4 does not have a converse.

Surveys of probabilistic methods and results in group theory, particularly finite group theory, are given in [**Kantor 1992**], [**Shalev 1998**] and [**Shalev 1999**$_b$]. Further results and problems, closer to the spirit of this chapter, are to be found in [**Mann (b)**].

Chapter 12

Other growth conditions

Subgroup growth is one way to measure the growth of finite images of a group. Of course there are other, equally natural, ways to do this. One that has received a certain amount of attention is known (not quite accurately) as 'index growth': that is, the growth of $|G : G^n|$ as a function of n. Novikov and Adian showed that this index is in general infinite, even for finitely generated groups G (the negative solution of the original Burnside problem); as we are concerned here primarily with finite quotients, we concentrate rather on

$$|\widehat{G} : \widehat{G}^n| = \sup\left\{|\widetilde{G} : \widetilde{G}^n| : \widetilde{G} \text{ a finite quotient of } G\right\},$$

(here $\widehat{G}^n$ denotes the closed subgroup generated by all nth powers in the profinite completion of G). The positive solution of the *restricted* Burnside problem by Zelmanov shows that if G is finitely generated then this number is indeed finite, for every n. However, it can grow *exceedingly* fast – a multiply-iterated exponential function of n (see [Vaughan-Lee & Zelmanov 1999], §2). Thus the following should be a strong restriction: a group G has *polynomial index growth,* or **PIG,** if there exists $\gamma > 0$ such that $|\widehat{G} : \widehat{G}^n| \leq n^\gamma$ for all n.

However, the problem of characterising finitely generated, residually finite groups with PIG seems to be harder than the corresponding question for PSG groups, and may in a real sense be intractable (see the remarks following Theorem 12.8 below). In this chapter, we discuss what is known on the topic, and take the opportunity to examine the relationships between PSG, PIG and other conditions that, in one way or another, restrict the size of the finite quotients of a group. Not unexpectedly, the PIG condition imposes weaker restrictions on a group than PSG does; remarkably, it turns out that PIG is actually a *consequence* of PSG – this is far from obvious, and comes at the end of a long chain of reasoning that relies in particular on CFSG.

A profinite group G is *boundedly generated,* or **BG**, if it is equal to the product of finitely many procyclic subgroups; this holds if and only if there exists k such that every finite quotient of G is the product of at most k cyclic subgroups (by a familiar inverse-limit argument that we recall in Section 1,

below). In that case, a finite quotient of exponent dividing n clearly has order at most n^k. Thus for profinite groups, bounded generation is a sufficient condition for PIG.

On the other hand, many interesting profinite groups turn out to be boundedly generated. Important classes of such groups are provided by the first two theorems.

Theorem 12.1 *Every profinite group of finite rank is boundedly generated.*

A profinite group G is said to be *adelic* if G is isomorphic to a closed subgroup of

$$\mathrm{SL}_m(\widehat{\mathbb{Z}}) = \prod_p \mathrm{SL}_m(\mathbb{Z}_p),$$

for some $m \geq 2$.

Theorem 12.2 *Every finitely generated adelic group is boundedly generated.*

Further examples of BG profinite groups are described in Section 12.8.

Now suppose that G is a profinite group with polynomial subgroup growth. We saw in Chapter 10 that G has closed normal subgroups $R \leq G_0$ such that G/G_0 is finite, R is prosoluble of finite rank, and G_0/R is a 'quasi-semisimple group of bounded type'. It is not hard to deduce (see Section 2 below) that G_0/R is a homomorphic image of an adelic group A. Also G, hence also G_0/R, is finitely generated (see Corollary 11.2), so G_0/R is an image of some finitely generated (closed) subgroup of A. It follows by Theorem 12.2 that G_0/R is BG, and by Theorem 12.1 that R is BG. Hence G itself is boundedly generated, and we have the second implication in

Theorem 12.3 *For a profinite group the following implications hold:*

$$\textit{finite rank} \Longrightarrow \mathrm{PSG} \Longrightarrow \mathrm{BG} \Longrightarrow \textit{f.g. and } \mathrm{PIG}. \tag{12.1}$$

Moreover, each of these implications is strict.

The easy third implication was established above, while the first was proved as Theorem 10.1.

Profinite groups with PSG but of infinite rank were exhibited at the end of §10.3. In view of Theorem 12.2, an example of a BG profinite group that does not have PSG is $\mathrm{SL}_m(\widehat{\mathbb{Z}})$ itself (for any $m \geq 2$); that this group has faster than polynomial subgroup growth follows from the proof of Theorem 6.1 (or the easier argument in §5.2), and it is finitely generated because its dense subgroup $\mathrm{SL}_m(\mathbb{Z})$ is finitely generated. The fact that the third implication in (12.1) is strict will follow from Theorem 12.8, stated below.

On the other hand, in the domain of pro-p groups all four conditions in (12.1) are equivalent (see Section 12.6 below). We shall see that some of these conditions also turn out to be equivalent within various classes of finitely generated (abstract) groups.

The circle of implications (12.1) is completed with

Theorem 12.4 *Let G be a profinite group. Then*

(i) *if G is* BG *then G has subgroup growth of type at most $n^{\log n}$, and polynomial maximal subgroup growth;*

(ii) *if G has* PIG *then G has subgroup growth of type at most $n^{(\log n)^2}$, and if G is also finitely generated then G has maximal subgroup growth of type at most $n^{\log n}$.*

It is interesting to note that the first claim in (ii) applies to profinite PIG groups that need not be finitely generated. An example in §12.8 will show that the claim about subgroup growth in (i) is best possible.

The theorem will be deduced from the next proposition, which concerns composition factors. We saw in Chapter 10 that a profinite group of finite rank has only finitely many non-abelian upper composition factors, because it is virtually prosoluble; while the upper composition factors of a PSG group have bounded ranks (Chapter 5). It turns out that the finiteness conditions BG and PIG also impose (successively weaker) restrictions on composition factors. Let us say that

- $G \in \mathcal{C}^{\triangleleft}$ if G does not have arbitrarily large alternating groups as upper composition factors, and that
- $G \in \mathcal{B}$ if among the upper composition factors of G, the alternating ones have bounded degrees and those that are classical simple groups of Lie type have bounded Lie ranks.

It is shown in the **Permutation groups window** that $G \in \mathcal{B}$ *if and only if G does not involve every finite group as an upper section.*

Proposition 12.5 *Let G be a profinite group.*

(i) *If G is* BG *then $G \in \mathcal{B}$.*

(ii) *If G has* PIG *then $G \in \mathcal{C}^{\triangleleft}$.*

This is proved in Section 12.4, along with some further related properties of BG and PIG groups. It leads to the following structure theorem (which falls short, however, of complete characterisations):

Theorem 12.6 *Let G be a finitely generated profinite* PIG *group. Then G has closed normal subgroups*

$$1 \leq R \leq N \leq G \tag{12.2}$$

such that G/N is virtually metabelian, R is prosoluble, and N/R is a Cartesian product of finite simple groups of Lie type, each occurring with bounded multiplicity.

If G is boundedly generated then the simple factors of N/R have bounded Lie ranks, and N may be taken so that G/N is virtually abelian.

In discussing profinite groups, we have limited ourselves to 'local information', that is, information that is implicit in the structure of the finite images

of a group. How much further can we go if we start from a finitely generated (abstract) group? The magic key that unlocked the PSG theorem was *linearisation*: the methods of the **Linearity Conditions** window show that a finitely generated group satisfying a sufficiently strong upper finiteness condition has a linear representation with a relatively harmless kernel (of 'prosoluble type', say). However, the condition PIG is *not* sufficiently strong; the underlying reason for this is

Proposition 12.7 *There exists a universal constant R such that*

$$|S| \leq \exp(S)^R$$

for every finite simple group S of Lie type,

where $\exp(S)$ denotes the exponent of S. Using this, it is easy to see that a Cartesian product of such simple groups whose orders grow suitably fast will be a PIG group. To find a finitely generated group whose profinite completion is such a product is not so easy, but in Section 12.8 we sketch the proof of

Theorem 12.8 *There exists a finitely generated residually finite* PIG *group Γ such that*

(i) $\widehat{\Gamma}$ *is not* BG*;*

(ii) Γ *is not linear, indeed every linear quotient of Γ is virtually cyclic.*

In fact, the proof will show that there are $2^{\aleph_0}$ non-isomorphic such groups; this is in stark contrast to the case of finitely generated residually finite PSG groups, of which there are only countably many, since by the PSG theorem they are all linear over $\mathbb{Q}$. Thus it is probably hopeless to look for a characterisation of f.g. residually finite PIG groups analogous to the PSG theorem.

It would be interesting to investigate further the class of BG (abstract) groups – an abstract group is said to be BG if it is equal to the product of finitely many cyclic subgroups. These groups include the f.g. soluble minimax groups [Kropholler 1984] and many arithmetic groups [Tavgen 1991] (see below). Are there any essentially different examples?

Problems

- Are there uncountably many residually finite boundedly generated groups?
- If G is a f.g. residually finite group, does $\widehat{G}$ BG imply that G is BG?
- Is every residually finite BG group linear?
- Is every just-infinite BG linear group isomorphic to an S-arithmetic group?
- Does every *soluble* f.g. residually finite group with PIG have finite rank?

Some properties of boundedly generated (abstract) groups are established in [Abért, Lubotzky & Pyber]; in particular, it is shown that *every BG linear group over a field of positive characteristic is virtually abelian.* We shall not go into this further, as bounded generation (for abstract groups) is not primarily a condition on the finite quotients.

As might be expected, pathologies like Theorem 12.8 cannot arise in residually nilpotent groups:

Theorem 12.9 *Let G be a finitely generated virtually residually nilpotent group with* PIG. *Then*

(i) *G is a linear group in characteristic zero;*

(ii) *if G is virtually soluble, then G has finite rank, and G is the product of finitely many cyclic subgroups.*

Thus for finitely generated virtually residually nilpotent groups that are virtually soluble, all the conditions (12.1) are equivalent. This is certainly *not* the case without assuming solubility, in view of the following theorem, which should be compared with the results of Chapter 7:

Theorem 12.10 *Let Γ be an S-arithmetic group in a simply-connected, absolutely almost simple algebraic group $\mathfrak{G}$ over a number field k. Then the following are equivalent:*

(a) Γ has the congruence subgroup property

(b) $\widehat{\Gamma}$ is BG

(c) Γ has PIG.

Of course, (b) implies (c). Assuming without loss of generality that Γ is a subgroup of $\mathrm{SL}_m(\mathbb{Z}[1/t])$ for some t, we may consider the congruence completion $\widetilde{\Gamma}$ of Γ as a closed subgroup of $\mathrm{SL}_m(\widehat{\mathbb{Z}})$, so by Theorem 12.2 it is always true that $\widetilde{\Gamma}$ is BG. If Γ also has the congruence subgroup property then $\widetilde{\Gamma}$ differs from $\widehat{\Gamma}$ by at most a finite kernel, and this is enough to establish that (a) implies (b). The proof of remaining implication is given in Section 12.7.

It is known [Tavgen 1991] that if $\mathfrak{G}$ is quasi-split and has k-rank at least 2 then Γ is itself boundedly generated; this gives an alternative, group-theoretic proof for the congruence subgroup property in this large class of arithmetic groups.

Before concluding this introduction we should mention another growth condition. The **rank function** of a profinite group G is

$$d_n(G) = \sup\{d(H) : H \leq_o G,\ |G:H| \leq n\}.$$

Thus G has finite rank if $d_n(G)$ is bounded; in general, the slow growth of $d_n(G)$ as a function of n is another upper finiteness condition of a similar type to PSG and PIG. We have seen in Chapter 1 that when G is a pro-p group, there is a tight relation between the rank function and the subgroup growth (*warning*:

the notation $d_n(G)$ was used there in a slightly different sense). In general, Theorem 11.8 showed *if the profinite group G has PSG then*

$$d_n(G) = O\left(\sqrt{\log n}\right).$$

A number of other results relating to the rank function have been obtained, but to avoid overloading this chapter we do not discuss most of them. However, let us state

Theorem 12.11 [Lubotzky 1995] *Let Γ be as in Theorem 12.10. Then Γ has the congruence subgroup property if and only if $d_n(\widehat{\Gamma}) = o(\log n)$.*

The proof is along similar lines to that of Theorem 12.10.

Little is known about the 'index growth' $|\widehat{G} : \widehat{G}^n|$ in general, beyond the case of PIG. It remains to be seen whether a theory as rich as that of subgroup growth is waiting to be developed; the same applies to the study of the 'rank function'.

Let us conclude with some speculative remarks. In chapter 5, we characterized the PSG-groups: these are the "smallest" groups from the point of view of subgroup growth. We shall see in Chapter 13 that right above PSG there is a continuous spectrum of possible growth types, so in general one cannot expect to have a "next type of growth" after PSG.

Still, a very remarkable class of groups stands out as a candidate to be the "next class", namely the *S-arithmetic groups* in higher rank semi-simple algebraic groups over algebraic number fields (see Chapters 6 and 7). Conjecturally these groups have the congruence subgroup property (this has been proved in most cases), and hence according to Theorem 6.1 have subgroup growth of type $n^{\log n/\log\log n}$. Among finitely generated linear groups this is indeed the next possible growth type above PSG (see Chapter 8).

It is now natural to wonder whether a finitely generated linear group with subgroup growth of type $n^{\log n/\log\log n}$ is necessarily of arithmetic type. This question reminds one of the Platonov conjecture: if a characteristic-zero linear group is *rigid* (i.e. has for each n only finitely many irreducible representations of degree n) then it is of arithmetic type (see [PR], [Bass & Lubotzky 2000] and references therein). This conjecture, widely believed for a number of years, was recently disproved in [Bass & Lubotzky 2000]. We therefore have to look for other characterizations of these arithmetic groups. One such is given in [Lubotzky & Venkataramana 2002], but it is not very natural or satisfactory. It may be hoped that a more natural algebraic characterization of these arithmetic groups, among the finitely generated linear groups, will be found in terms of subgroup growth or one of the other finiteness conditions discussed above, as suggested by Theorems 12.10 and 12.11 (in view of the history of Platonov's conjecture, however, one should be rather cautious about making too specific a conjecture!).

12.1 Rank and bounded generation

We begin by sketching the proof of

Theorem 12.1.1 *If G is a finite group of rank r then G is a product of $f(r)$ cyclic subgroups, where $f(r)$ depends only on r.*

The first step is the following lemma, which was essentially proved as part of Proposition 10.1.1:

Lemma 12.1.2 *If G is a finite group of rank r then G has normal subgroups $R \leq K$ such that*

$$|G/K| \leq f_1(r),$$

K/R is a direct product of at most r non-abelian simple groups, and R is soluble.

Now if R is a product of a cyclic groups and each simple factor of K/R is a product of b cyclic groups, it follows that G is a product of $a + rb + \log(f_1(r))$ cyclic groups. So it will suffice to prove the theorem in the special cases (a) where G is soluble, and (b) where G is simple.

Step 1. Where G is a p-group. Now G has a powerful normal subgroup P of index dividing $p^{r(1+\lceil \log r \rceil)}$. The group P is a product of r cyclic subgroups, and G/P is a product of at most $r(1 + \lceil \log r \rceil)$ cyclic subgroups. So G is a product of $f_2(r) = r(2 + \lceil \log r \rceil)$ cyclic subgroups. (↬ **Finite group theory**).

Step 2. Where G is nilpotent. Since the direct product of cyclic groups of coprime orders is cyclic, it follows from Step 1 that G is a product of $f_2(r)$ cyclic subgroups.

Step 3. Where G is soluble. Lemma 10.4.2 shows that the Fitting height of G is bounded by some function $f_3(r)$ of r. It follows that G is the product of $f_3(r) \cdot f_2(r)$ cyclic subgroups.

Step 4. Where G is simple (and non-cyclic). If G is sporadic or alternating then G has bounded order. Otherwise, G is of Lie type, and the Lie rank is bounded in terms of r. It follows that the Weyl group W of G has bounded order. Now G has a Bruhat decomposition

$$G = UNU$$

where U is nilpotent and N is the normalizer of a maximal torus H; here H is abelian and $N/H \cong W$. Hence N is a product of at most $r \cdot \log |W|$ cyclic groups; and by Step 2, U is the product of $f_2(r)$ cyclic subgroups. It follows that G is the product of $f_4(r)$ cyclic subgroups, where $f_4(r)$ depends only on r. (For the Weyl group and Bruhat decomposition, see [GLS] Theorem 2.3.5**.**)

This concludes the proof of Theorem 12.1.1. Theorem 12.1 is a formal consequence, in view of the following routine argument:

Lemma 12.1.3 *Let G be a profinite group. If every finite quotient of G is a product of k cyclic subgroups then G is a product of k procyclic subgroups, and conversely.*

Proof. For each open normal subgroup N of G let $\mathcal{X}(N)$ denote the set of all k-tuples

$$(x_1N, \ldots, x_kN)$$

in G/N such that $G = N\langle x_1\rangle \ldots \langle x_k\rangle$. If $M \leq N$ are open normal subgroups then the quotient mapping $G/M \to G/N$ induces a map $\pi_{M,N} : \mathcal{X}(M) \to \mathcal{X}(N)$. Thus we obtain an inverse system of finite sets $\mathcal{X}(N)$, ordered by reverse inclusion of open normal subgroups of G. If every finite quotient of G is a product of k cyclic subgroups, each of the sets $\mathcal{X}(N)$ is non-empty; it follows that the inverse limit of this system is non-empty (see for example [DDMS], Chapter 1). This means that there exists a family $(\mathfrak{x}_N)$, labeled by the open normal subgroups N of G, such that $\mathfrak{x}_N \in \mathcal{X}(N)$ for each N and $\pi_{M,N}(\mathfrak{x}_M) = \mathfrak{x}_N$ whenever $M \leq N$. Thus if $\mathfrak{x}_N = (x_{1,N}N, \ldots, x_{k,N}N)$ and $M \leq N$ then $x_{i,M}M \subseteq x_{i,N}N$ for each i. Since cosets of open subgroups are compact, it follows by the finite intersection property that for each $i = 1, \ldots, k$,

$$\bigcap_N x_{i,N}N \neq \emptyset.$$

Now choose $g_i \in \bigcap_N x_{i,N}N$ for each i, and let $\langle g_i\rangle$ denote the procyclic subgroup of G generated by g_i. Then $G = N\langle g_1\rangle \ldots \langle g_k\rangle$ for each $N \lhd_o G$, and as $\langle g_1\rangle \ldots \langle g_k\rangle$ is a closed subset of G (being a product of compact subsets) it follows that

$$\langle g_1\rangle \ldots \langle g_k\rangle = \bigcap_N N\langle g_1\rangle \ldots \langle g_k\rangle = G.$$

The converse is evident. ■

12.2 Adelic groups

The following general structure result for finite linear groups is proved in [Liebeck & Pyber 2001]; some of the key ingredients in its proof are sketched in the next section.

Proposition 12.2.1 *Let $X \leq \mathrm{GL}_m(\mathbb{F}_p)$, where p is sufficiently large compared to m. Then X has normal subgroups $X_1 \geq X_2 \geq X_3$ such that*

(a) *$|X : X_1| \leq f_1(m)$ where $f_1(m)$ depends only on m,*

(b) *X_1/X_2 is abelian,*

(c) *X_2/X_3 is a p-group,*

(d) *X_3 is equal to a product of at most $25m(m-1)/2$ subgroups of order p, and every simple quotient of X_3 is a group of Lie type in characteristic p.*

Now let $p_1, \dots, p_k$ be sufficiently large, distinct primes and for each i let X^i be a subgroup of $\mathrm{GL}_m(\mathbb{F}_{p_i})$. Suppose that G is a subdirect product in $X^1 \times \cdots \times X^k$ (a subgroup that maps onto each of the direct factors), and that G can be generated by d elements. We claim that G is the product of at most $g(d,m)$ cyclic subgroups, where $g(d,m)$ depends only on d and m (but *not* on k).

For $j = 1, 2, 3$ write X^i_j for the normal subgroup of X^i given in Proposition 12.2.1, and put

$$G_j = G \cap \left(X^1_j \times \cdots \times X^k_j\right).$$

Step 1. The free group F_d on d generators has only finitely many normal subgroups of index at most $f_1(m)$. Let K be their intersection and put $f_2(d,m) = |F_d : K|$. Fixing an epimorphism $\psi : F_d \to G$ we obtain composed epimorphisms

$$\psi_i : F_d \to G \to X^i/X^i_1.$$

Evidently $\ker \psi_i \geq K$ for each i, so $\psi(K) \leq G_1$. It follows that

$$|G : G_1| \leq f_2(d,m).$$

Step 2. The group G_1/G_2 is abelian, and can be generated by $d \cdot f_2(d,m)$ elements, by Schreier's formula.

Step 3. The group G_2/G_3 is isomorphic to a subgroup of $\prod X^i_2/X^i_3$. The order of X^i_2/X^i_3 divides that of a Sylow p-subgroup of $\mathrm{GL}_m(\mathbb{F}_{p_i})$, namely $p_i^{m(m-1)/2}$, so X^i_2/X^i_3 is a p_i-group of rank at most $m(m-1)/2$. Consequently G_2/G_3 is nilpotent of rank at most $m(m-1)/2$.

Step 4. We claim that $G_3 = X^1_3 \times \cdots \times X^k_3$. To see this, note that G/G_3 is an extension of a soluble group by a group of order at most $f_2(d,m)$; provided the prime p_i is sufficiently large this implies that G/G_3 has no section that is a simple group of Lie type in characteristic p_i, and it follows that the projection $G \to X^i$ maps G_3 onto X^i_3. This holds for each i, and so G_3 is a subdirect product in $X^1_3 \times \cdots \times X^k_3$. However, since the primes p_i are distinct and large, the groups X^i_3 have no common simple quotients, and this implies that the only subdirect product in $X^1_3 \times \cdots \times X^k_3$ is the full direct product.

Now it follows from Step 4 that G_3 is a product of at most $25m(m-1)/2$ cyclic subgroups. Steps 1 – 3 together imply that G/G_3 has rank at most $m(m-1)/2 + df_2(d,m) + \log f_2(d,m)$. With Theorem 12.1.1 these together imply that G is the product of at most $g(d,m)$ cyclic subgroups, where $g(d,m)$ depends only on d and m (it suffices to quote here the easier case of Theorem 12.1.1 concerning nilpotent groups).

To complete the proof of Theorem 12.2, let H be a closed subgroup of $\mathrm{SL}_m(\widehat{\mathbb{Z}})$ and N an open normal subgroup of H. Suppose that H/N can be generated by d elements. Since N is open it contains $H \cap \prod_{p \notin S} \mathrm{SL}_m(\mathbb{Z}_p)$ where S is some finite set of primes; so writing H_1 for the projection of H in $\prod_{p \in S} \mathrm{SL}_m(\mathbb{Z}_p)$ we

may identify H/N with a finite quotient H_1/N_1. Next, consider the natural projection

$$\pi : \prod_{p\in S} \mathrm{SL}_m(\mathbb{Z}_p) \to \prod_{p\in S} \mathrm{SL}_m(\mathbb{F}_p)$$

and let $K = H_1 \cap \ker \pi$. Now the kernel of π is $\prod_{p\in S} \mathrm{SL}^1_m(\mathbb{Z}_p)$, a pronilpotent group of rank at most m^2 ($\looparrowright$ **Pro-p groups**); by (an easy case of) Theorem 12.1.1, it follows that KN_1/N_1 is a product of at most $f(m^2)$ cyclic groups.

On the other hand, H_1/KN_1 is a d-generator image of $\pi(H_1)$, hence it is an image of some d-generator subgroup Y of $\prod_{p\in S} \mathrm{SL}_m(\mathbb{F}_p)$. Write $S = S_1 \cup S_2$ where S_1 consists of primes that are not sufficiently large, in the sense used above, and let $\varphi : Y \to \prod_{p\in S_2} \mathrm{SL}_m(\mathbb{F}_p)$ denote the projection mapping. The result established above shows that $\varphi(Y)$ is the product of at most $g(d, m)$ cyclic subgroups; while the order of $\ker \varphi$ is bounded by a function of m alone (namely the product over all 'insufficiently large' primes p of $|\mathrm{SL}_m(\mathbb{F}_p)|$).

Putting everything together we infer that H_1/N_1, and hence H/N, is equal to the product of at most $g_1(d, m)$ cyclic subgroups, where $g_1(d, m)$ depends only on d and m.

Thus if H is a d-generator group then every finite quotient of H is a product of at most $g_1(d, m)$ cyclic subgroups, and it follows by Lemma 12.1.3 that H is the product of $g_1(d, m)$ procyclic subgroups. This completes the proof of Theorem 12.2, modulo Proposition 12.2.1.

To conclude this section, we recall the following definition from Chapter 10: a profinite group Q is said to be *quasi-semisimple of bounded type* if Q is perfect and $Q/\mathrm{Z}(Q) \cong \prod T_i$ where (T_i) is a sequence of finite groups of bounded rank, each occurring with bounded multiplicity, and each T_i is a simple group of Lie type. It follows that Q is a quotient of

$$\widetilde{Q} = \prod \widetilde{T}_i$$

where $\widetilde{T}_i$ is the univeral cover of T_i. Since the groups T_i have bounded rank, each T_i is of the form ${}^*X_l(\mathbb{F}_{p^e})$ where the Lie rank l and the field degree e are bounded ($\looparrowright$ **Finite simple groups**). Thus only finitely many, say t, different Lie types ${}^*X_l$ occur. For each of these, the universal group ${}^*\widetilde{X}_l(\mathbb{F}_{p^e})$ has a faithful representation in $\mathrm{SL}_m(\mathbb{F}_{p^e})$, and we may take m to be the same for all of them. If f is a bound for the field degrees e and w is a bound for the multiplicity of each simple factor, we see that

$$\widetilde{Q} \le \prod_p \mathrm{SL}_m(\mathbb{F}_{p^f})^{(tw)} \le \prod_p \mathrm{SL}_r(\mathbb{F}_p) \tag{12.3}$$

where $r = twfm$. Let G be the inverse image of $\widetilde{Q}$ in $\prod_p \mathrm{SL}_r(\mathbb{Z}_p) = \mathrm{SL}_r(\widehat{\mathbb{Z}})$. Since $\widetilde{Q}$ is a product of subgroups in the individual factors, it is a closed subgroup of the product (12.3), so G is a closed subgroup of $\mathrm{SL}_r(\widehat{\mathbb{Z}})$. Thus we have established

Lemma 12.2.2 *Let Q be a profinite group. If Q is quasi-semisimple of bounded type then Q is a homomorphic image of an adelic group.*

With the remarks in the introduction, this completes the proof that every profinite group with PSG is boundedly generated. (As the reader will have noticed, this proof does not need to go via adelic groups: the relevant part of of the proof of Theorem 12.2 can be applied directly.)

12.3 The structure of finite linear groups

Here we state without proof some of the results established in [Liebeck & Pyber 2001], that lie behind Proposition 12.2.1.

By a delicate analysis of the Bruhat decomposition (cf. §12.1 above), Liebeck and Pyber established

Proposition 12.3.1 *Let H be a quasi-simple group of Lie type over a finite field of characterstic p, other than ${}^2F_4(2)'$. Then H is equal to the product of 25 of its Sylow p-subgroups.*

The transition to linear groups in general relies on the following theorem of [Larsen & Pink]:

Theorem 12.3.2 *Let G be a finite subgroup of $\mathrm{GL}_m(F)$, where F is a field of characteristic p. Then G has normal subgroups*

$$G_1 \geq G_2 \geq G_3$$

such that

(a) *$|G : G_1|$ is bounded by a function of m,*

(b) *G_1/G_2 is a direct product of simple groups of Lie type in characteristic p,*

(c) *G_2/G_3 is an abelian p'-group, and*

(d) *$G_3 = O_p(G)$.*

Combining these results, Liebeck and Pyber prove

Theorem 12.3.3 *Let G be a finite subgroup of $\mathrm{GL}_m(F)$, where F is a field of characteristic p and p is sufficiently large relative to m. If G is generated by elements of order p then G is equal to the product of 25 of its Sylow p-subgroups.*

Note that as long as $p > m$, every element of p-power order in $\mathrm{GL}_m(F)$ has order p, so any subgroup G of $\mathrm{GL}_m(F)$ without nontrivial p'-quotients is generated by elements of order p. Moreover, if $F = \mathbb{F}_p$ and P is a p-subgroup of G then $|P|$ divides $p^{m(m-1)/2}$, so P is a product of at most $m(m-1)/2$ cyclic subgroups (each having order p). It follows that G is the product of at most $25m(m-1)/2$ subgroups of order p. This conclusion is applied, together with

another application of the Larsen-Pink theorem, to establish Proposition 12.2.1, stated in the preceding section.

A remarkable feature of these results is that, although the simple groups of Lie type play a central role, the proofs are all independent of CFSG: this is possible thanks to the powerful theorem of Larsen and Pink, which can often be used to eliminate the need for CFSG.

12.4 Composition factors

Here we establish some consequences of BG and PIG. Let G be a profinite group, and suppose to begin with that G has PIG. Thus there exists $\gamma = \gamma(G)$ such that

$$|Q : Q^n| \leq n^\gamma$$

for every finite quotient Q of G.

Let L be a non-abelian upper composition factor of G. Then G has an upper chief factor $N \cong L^{(k)}$ for some k. Consider the finite group $Q = G/\mathrm{C}_G(N)$. Identifying N with its image in Q we have

$$1 < N \leq K \lhd Q$$

where K is the kernel of the permutation action of Q (by conjugation) on the k simple factors of N. Thus Q/K is a transitive subgroup of $\mathrm{Sym}(k)$ and $K \leq \mathrm{Aut}(L)^{(k)}$.

Suppose that $L \cong \mathrm{Alt}(m)$ for some $m \geq 7$. Then $\mathrm{Aut}(L) \cong \mathrm{Sym}(m)$. Since the exponent of $\mathrm{Sym}(n)$ is at most 3^n for each n ($\looparrowright$ **Finite group theory,** §9) it follows that the exponent of Q is at most $3^k \cdot 3^m$, and hence that

$$|Q| \leq 3^{(k+m)\gamma}.$$

On the other hand,

$$|N| = \left(\frac{m!}{2}\right)^k \geq \left(\frac{m}{2}\right)^{mk/2}.$$

Hence

$$mk(\log m - 1) \leq 2(k+m)\gamma \log 3.$$

This implies that $m < 2 \cdot 3^{3\gamma}$.

It follows that *G has no alternating upper composition factor of degree exceeding* $2 \cdot 3^{3\gamma}$, and we have proved part (ii) of Proposition 12.5.

Assume now that G is the product of m procyclic subgroups. We claim that *the upper composition factors that are simple of classical Lie type have bounded Lie ranks.* As above, let

$$L^{(k)} \cong N \leq K \lhd Q \tag{12.4}$$

where Q is a finite quotient of G, N is a minimal normal subgroup of Q and K is the kernel of $Q \to \mathrm{Sym}(k)$.

The maximal order of an element of $\mathrm{Sym}(k)$ is at most 2^k ($\looparrowright$ **Finite group theory**, §9), so if $g \in Q$ then $g^n \in K$ for some $n \leq 2^k$, and if h is an upper bound for the orders of automorphisms of L it follows that g has order at most $(2h)^k$. As Q is the product of m cyclic subgroups this implies that $|Q| \leq (2h)^{km}$.

Suppose now that $L = {}^*X_l(q)$ is a classical simple group of Lie type, with $l > 4$ say. Then $\mathrm{Out}(L)$ has exponent dividing $2e(q \pm 1)$ (where $q = p^e$) and $L \leq \mathrm{PSL}_{2l+1}(\mathbb{F}_q)$ ($\looparrowright$ **Finite simple groups**). Since elements of $\mathrm{GL}_{2l+1}(\mathbb{F}_q)$ have order at most $q^{2l+1} - 1$ ($\looparrowright$ **Finite group theory**, §9) it follows that the maximal order of any automorphism of L is at most

$$2e(q \pm 1)(q^{2l+1} - 1) < q^{3l},$$

say. On the other hand,

$$|L| \geq q^{l(l+2)}(1 - o(1)) > q^{l^2}$$

if l is large ($\looparrowright$ **Finite simple groups**). With the result of the previous paragraph this gives

$$q^{kl^2} < |L|^k \leq |Q| \leq (2q^{3l})^{km}.$$

Thus $l < 4m$.

We conclude that the Lie rank of any classical simple upper composition factor of G is at most $\max\{4m, C\}$ where C is some absolute constant. Since the alternating upper composition factors have bounded degrees, because G has PIG, it follows that G belongs to the class $\mathcal{B}$, and Proposition 12.5 is proved.

As a consequence we can derive another finiteness property of BG groups. A group G is said to satisfy the *polynomial core condition*, or **PCC**, if there exists c such that

$$|G : \mathrm{core}_G(H)| \leq |G : H|^c$$

for every (open) subgroup H of finite index in G.

Proposition 12.4.1 *Let G be a profinite group. If G has* PIG *and $G \in \mathcal{B}$ then G satisfies* PCC.

Proof. If $G \in \mathcal{B}$ then there exists k such that every finite quotient of G belongs to the class $\mathcal{B}_k$ ($\looparrowright$ **Permutation groups**) Let H be an open subgroup of index n in G and put $Q = G/\mathrm{core}_G(H)$. Then Q is a transitive permutation group of degree n, and $Q \in \mathcal{B}_k$. It is shown in the **Permutation groups** window that under these conditions, the exponent of Q is at most $n^{f_1(k)}$. If G also has PIG it follows that $|Q| \leq n^{f_1(k)\gamma}$ where $\gamma = \gamma(G)$. The proposition follows. ■

In view of Proposition 12.5, this implies that *every profinite* BG *group satisfies* PCC.

In §5.3 we defined the invariant $w(G)$ as the supremum of natural numbers k such that G has a normal upper section (normal subgroup of a finite quotient) of the form $L^{(k)}$ with L a non-abelian simple group. Proposition 5.3.4 shows that $w(G)$ is finite if G has PSG; the next result generalizes this:

Proposition 12.4.2 *Let G be a profinite group. If G has* PIG *then $w(G)$ is finite.*

Proof. Let Q be a finite quotient of G and $L^{(k)} \cong N \lhd Q$ where L is an arbitrary non-abelian simple group. In order to bound k, we may replace Q by $Q/\mathrm{C}_Q(N)$, and so assume as above that $\mathrm{C}_Q(N) = 1$. Let K be as in (12.4).

Suppose to begin with that N is a minimal normal subgroup of Q. Then Q/K is a transitive permutation group of degree k, and by Proposition 12.5(ii), proved above, Q/K has no alternating composition factors of degree exceeding δ, say, where δ depends only on G. It follows ($\leadsto$ **Permutation groups**) that the exponent of Q/K is at most $k^{c \log k}$, where c depends only on δ. Also the exponent of $\mathrm{Aut}(L)$ is bounded by $|\mathrm{Aut}(L)| \leq |L|^2$ ($\leadsto$ **Finite simple groups**). As above it follows that

$$|L|^k \leq |Q| \leq \left(|L|^2 k^{c \log k}\right)^\gamma$$

where $\gamma = \gamma(G)$. Hence

$$k - 2\gamma < (k - 2\gamma) \log |L| \leq c\gamma (\log k)^2,$$

which implies that $k \leq f(\gamma)$ where $f(\gamma)$ depends only on γ.

In the general case, we have $N = M_1 \times \cdots \times M_t$ where each M_i is a chief factor of G. Thus $M_i \cong L^{k_i}$ where $k_i \leq f(\gamma)$ for each i. Put $D_i = \mathrm{C}_Q(M_i)$ and let K_i be the kernel of the permutation action of Q on the set of simple factors of M_i. Then

$$Q/K_i \leq \mathrm{Sym}(k_i) \leq \mathrm{Sym}(f) \quad \text{where} \quad f = \max\{k_1, \ldots, k_t\} \leq f(\gamma).$$

Let e denote the exponent of $\mathrm{Aut}(L)$ and h the exponent of $\mathrm{Sym}(f)$. Then each Q/D_i has exponent dividing eh, and as $D_1 \cap \ldots \cap D_t = \mathrm{C}_Q(N) = 1$ it follows that the exponent of Q divides eh. As $e \leq |L|^2$ and $h \leq 3^{f(\gamma)}$ we deduce that

$$|L|^k \leq |Q| \leq |L|^{2\gamma}\, 3^{\gamma f \gamma)} < |L|^{\gamma(2+f(\gamma))}.$$

Thus

$$k \leq \gamma(2 + f(\gamma)),$$

and so $\gamma(2 + f(\gamma))$ is an upper bound for $w(G)$. ■

Remark. In §13.3 we exhibit profinite groups G having arbitrarily slow non-polynomial subgroup growth. Each of them has $w(G) = \infty$, so G does not have PIG. This shows that the implication "PSG $\Longrightarrow$ PIG" in Theorem 12.3 is strict. This is true even among finitely generated abstract groups, because for G as above, a finitely generated abstract group Γ such that $\widehat{\Gamma} = G$ is constructed in §13.4.

Theorem 12.6 is a formal consequence of what we have proved so far in this section, together with the classification of finite simple groups. Indeed, the following is true:

Proposition 12.4.3 *Let G be a profinite group such that $a_n(G)$ is finite for all n. Assume that $G \in \mathcal{C}^{\triangleleft}$ and that $w(G)$ is finite. Then G has closed normal subgroups*

$$R \leq N \leq H$$

such that G/H is finite, H/N is metabelian, R is prosoluble, and N/R is a Cartesian product of finite simple groups of Lie type, each occurring with bounded multiplicity.

If also $G \in \mathcal{B}$ then the simple factors of N/R have bounded Lie ranks, and H may be taken so that H/N is abelian.

We omit the proof, which is very similar to that of Proposition 10.2.3. The key extra facts required concern the structure of $\mathrm{Out}(L)$ where L is simple of Lie type: namely, $\mathrm{Out}(L)$ has a metabelian normal subgroup of index dividing 6, and if L is of bounded Lie rank then $\mathrm{Out}(L)$ has an abelian normal subgroup of bounded index (↬ **Finite simple groups**). For details, see [Balog, Pyber & Mann 2000], Theorem 2.3 and Corollary 2.4.

12.5 BG, PIG and subgroup growth

We can now deduce Theorem 12.4. The claims about *maximal subgroup growth* follow directly from Proposition 12.5, in view of Theorem 3.3 and (the proof of) Theorem 3.2 (see Chapter 3).

Proposition 12.5.1 *Let G be a profinite group satisfying* PCC. *If G either has* PIG *or else is finitely generated then there exists c such that*

$$s_n(G) \leq n^{c \log n} \quad \textit{for all } n.$$

Proof. Let H be an open subgroup of index n in G. Then H contains an open normal subgroup H_0 of G having index at most n^a in G, where a is a constant; therefore H contains G^m for some $m \leq n^a$. Now suppose that G has PIG. Then $|G/G^m| \leq m^\gamma$ where γ is a constant, and so by Corollary 1.7.5 we have

$$\begin{aligned} a_n(G/G^m) &\leq n^{2 \log |G/G^m|} \\ &\leq n^{2\gamma \log m}. \end{aligned}$$

It follows that

$$a_n(G) \leq \sum_{m \leq n^a} n^{2\gamma \log m} \leq n^{c' \log n}$$

where $c' = (2\gamma + 1)a$, giving the result with $c = c' + 1$.

If G is finitely generated then there exists b such that $s_k^{\triangleleft}(G) \leq k^{b \log k}$ for every k, by Corollary 2.8. So in this case there are at most $n^{a^2 b \log n}$ possibilities for H_0, and applying Corollary 1.7.5 in a similar way we obtain

$$a_n(G) \leq n^{a^2 b \log n} \cdot n^{2a \log n}.$$

The result follows as before with $c = 1 + 2a + a^2b$. ■

This applies in particular if G is a boundedly generated profinite group, by Propositions 12.5 and 12.4.1, and this completes the proof of Theorem 12.4(i).

Now let G be a profinite group with PIG. By Proposition 12.5, there exists k such that every finite quotient of G lies in the class $\mathcal{C}_k^{\triangleleft}$ (groups with no alternating composition factors of degree exceeding k). It is shown in the **Permutation groups** window that if $Q \in \mathcal{C}_k^{\triangleleft}$ is a transitive permutation group of degree n then the exponent of Q is at most $n^{b \log n}$, where b depends only on k. It follows as in the proof of Proposition 12.4.1 (in §12.4) that if H is an open subgroup of index n in G then H contains an open normal subgroup of index at most $n^{b\gamma \log n}$, where γ is a constant. Arguing as above we deduce that

$$s_n(G) \leq \sum_{m \leq n^{b\gamma \log n}} n^{2\gamma \log m} \leq n^{c(\log n)^2}$$

where $c = b\gamma(2\gamma + 1)$.

This completes the proof of Theorem 12.4(ii).

12.6 Residually nilpotent groups

For any group G let

$$\gamma(G) = \inf \left\{ \beta : |\widetilde{G} : \widetilde{G}^n| \leq n^\beta \text{ for every finite quotient } \widetilde{G} \text{ of } G \right\}.$$

The results of the last two sections all effectively bound various invariants of a *finite* group G in terms of $\gamma(G)$. We begin this section with another such result,

Proposition 12.6.1 *There is a function f such that*

$$\mathrm{rk}(G) \leq f(\gamma(G))$$

for every finite p-group G.

Proof. Let G be a finite p-group and put

$$k = \max\{d(K) \mid K \lhd G\}.$$

It follows from the theory of powerful p-groups that $\mathrm{rk}(G) \leq k(2 + \lceil \log k \rceil)$ (↬ **Finite group theory**, Cor. 19), so it will suffice to bound k in terms of $\gamma = \gamma(G)$.

Choose $K \lhd G$ maximal subject to $d(K) = k$. A simple argument (see the proof of Lemma 4.1.2) shows that $K = \mathrm{C}_G(K/\Phi(K))$, so G/K acts faithfully by conjugation on $K/\Phi(K) \cong \mathbb{F}_p^k$. Hence if $g \in G$ and $p^m \geq k$ then $g^{p^m} \in K$. Taking $m = \lceil \log k \rceil$ we thus have

$$G^{p^{m+1}} \leq K^p \leq \Phi(K).$$

It follows that

$$p^k = |K/\Phi(K)| \leq |G/\Phi(K)| \leq p^{(m+1)\gamma},$$

so $k \leq \gamma(\lceil \log k \rceil + 1)$, and this implies an upper bound for k depending only on γ. ■

A similar result (Proposition 5.4.2) was proved for finite *soluble* groups with a given degree of polynomial subgroup growth; however, this can *not* be carried over to the present context, as is shown by the example

$$G = \mathbb{F}_{p^d} \rtimes \mathbb{F}_{p^d}^*, \tag{12.5}$$

a finite metabelian group with $\gamma(G) \leq 2$ and arbitrarily large rank d.

Corollary 12.6.2 *A pro-p group has* PIG *if and only if it has finite rank.*

Now Theorem 8 of the **Linearity conditions** window asserts that a finitely generated residually nilpotent group Γ is linear over a field of characteristic zero if each of its pro-p completions $\widehat{\Gamma}_p$ has finite rank. In view of the last corollary, this holds if Γ has PIG. Since a subgroup of finite index in a PIG group clearly has PIG, and a finite extension of a linear group is linear, it follows that *a f.g.* PIG *group that is virtually residually nilpotent is linear in characteristic zero.*

Suppose now that G is a finitely generated soluble group, that G is virtually residually nilpotent and that G has PIG. We claim that then G *has finite rank.*

We have just shown that G is a linear group. It follows by the Lie-Kolchin-Mal'cev theorem (↬ **Linear groups**) that G is virtually nilpotent-by-abelian (alternatively, apply Corollary 5 of the **Linearity conditions** window). Replacing G by a suitable normal subgroup of finite index and factoring out the second derived group, we reduce to the case where G is a finitely generated metabelian group (↬ **Soluble groups**, Proposition 1).

Let $A = G'$ be the derived group of G. According to Hall's theory (↬ **Soluble groups**, §3), if A has infinite rank then there exists a prime p such that A/A^p has infinite rank. So replacing G by G/A^p we may assume that $A^p = 1$. The group G is still virtually residually nilpotent (*loc.cit.*), so let G_1 be a residually nilpotent normal subgroup of finite index in G, put $G_n = \gamma_n(G_1)$ for each n, and let $A_1 = A \cap G_1$. Then for each $n \geq 2$, G_1/G_n is a finitely generated nilpotent group with torsion subgroup A_1/G_n. It follows that G_1/G_n is residually a finite p-group and hence that A_1/G_n embeds into some finite p-quotient of G_1. Now Proposition 12.6.1 shows that

$$\mathrm{rk}(A_1/G_n) \leq f(\gamma)$$

where $\gamma = \gamma(G_1)$ is finite. As $\bigcap_{n=2}^{\infty} G_n = 1$ this implies that

$$|A_1| = \sup_n |A_1/G_n| \leq p^{f(\gamma)}.$$

Thus A_1 is finite, so A is finite, and G has finite rank.

Thus G is a f.g. minimax group (↬ **Soluble groups**); [Kropholler 1984] shows that such a group is equal to a product of finitely many cyclic subgroups. This completes the proof of Theorem 12.9.

12.7 Arithmetic groups and the CSP

In this section we sketch the proof that for arithmetic groups, PIG implies the congruence subgroup property; as remarked in the introduction, this will complete the proof of Theorem 12.10. The proof is similar to that of the corresponding subgroup growth result in Chapter 7, and depends likewise on 'Rapinchuk's lemma' Proposition 7.1.4. Throughout, Γ denotes an S-arithmetic group that satisfies the hypotheses of Theorem 12.10. We restate Rapinchuk's lemma:

Proposition 12.7.1 *If Γ does not have the congruence subgroup property, then there exist the following: a subgroup Γ_0 of finite index in Γ, a profinite group E containing Γ_0 as a dense subgroup, and an exact sequence of profinite groups*

$$1 \to W \to E \to H \to 1,$$

where
◇ *W is the Cartesian product of infinitely many copies of a fixed non-trivial finite simple group F, and*
◇ *H is an open subgroup of the congruence completion $\widetilde{\Gamma}$ of Γ.*
Furthermore, if F is abelian then
◇ *H can instead be taken to be a pro-q group for some prime q.*

Let us assume that Γ has PIG but not CSP. Then Γ_0 has PIG, and it follows that the profinite group E has PIG. Proposition 12.4.2 now shows that $w(E)$ is finite, so F cannot be a non-abelian simple group. Therefore W is an elementary abelian p-group of infinite rank, for some prime p. If H is a pro-p group then E is a pro-p group with PIG, which contradicts Corollary 12.6.2. We may therefore suppose that H is a pro-q group for some prime $q \neq p$.

Let Q be a finite quotient of E, and let A be the image of W in Q. We claim that the rank of A is bounded, independently of Q. Now A is a p-group and Q/A is a q-group, so $Q = A \rtimes Y$ for some subgroup Y, and $\mathrm{C}_Q(A) = A \times \mathrm{C}_Y(A)$. So factoring out the normal subgroup $\mathrm{C}_Y(A)$ we may assume that $\mathrm{C}_Q(A) = A$. Suppose now that $A \cong \mathbb{F}_p^k$, where $k \geq 2$ say. Then Q/A is a q-subgroup of $\mathrm{GL}_k(\mathbb{F}_p)$, hence has exponent dividing $p^k - 1$ (each element is semisimple and has eigenvalues in $\mathbb{F}_{p^k}$). At first glance, this looks unhelpful – compare the example (12.5); however, the fact that we are dealing with powers of a fixed prime q makes all the difference, in view of the following elementary observation:

Lemma 12.7.2 *Let $p \neq q$ be fixed primes. Then there exists a constant c (depending on p and q) such that for $k \geq 2$,*

$$p^k \equiv 1 \pmod{q^n} \Longrightarrow n \leq c \log k.$$

Accepting this for now, we see that the exponent of Q/A is at most $q^{c \log k}$. Thus Q has exponent at most $p \cdot q^{c \log k}$ and so

$$p^k = |A| \leq |Q| \leq (pq^{c \log k})^\gamma$$

where $\gamma = \gamma(E)$. This implies that k is bounded above in terms of p, q, c and γ, and our claim is established.

Since W, as a closed subgroup of E, is the inverse limit of its images such as A, it follows that W has finite rank, a contradiction. This completes the proof of Theorem 12.10.

Proof of Lemma 12.7.2. If q is odd put $v = p^{q-1}$, if $q = 2$ put $v = p^2$. Then $v = 1 + aq^s$ with $s \geq 1$ ($s \geq 2$ if $q = 2$) and $q \nmid a$. Now for each $m \geq 1$,

$$v^{q^m} \equiv 1 + aq^{s+m} \,(\mathrm{mod}\, q^{s+m+1})$$

(induction on m and the binomial theorem). It follows that if $n > s$, then the order of v modulo q^n is exactly q^{n-s}. Hence if $p^k \equiv 1 \,(\mathrm{mod}\, q^n)$ then q^{n-s} divides k and it follows that

$$n \leq s + \log_q k \leq c \log k$$

where c depends only on p and q.

12.8 Examples

The following somewhat easier variation on Theorem 12.3.3 is established in [Abért, Lubotzky & Pyber]:

Proposition 12.8.1 *Let $d \geq 2$ and let $q > 3$ be a prime power. Then $\mathrm{SL}_d(\mathbb{F}_q)$ is a product of $10d(d-1)$ cyclic subgroups of order $q - 1$.*

Now let (p_i) be a sequence of distinct primes and put $q_i = 2^{p_i}$. Then $q_i - 1$ and $q_j - 1$ are relatively prime whenever $i \neq j$, so any finite direct product of the form $\prod_i C_{q_i - 1}$ is a cyclic group. With the preceding proposition this gives

Theorem 12.8.2 *Let $d \geq 2$. Then the Cartesian product*

$$G = \prod_{i=1}^{\infty} \mathrm{PSL}_d(\mathbb{F}_{q_i})$$

is equal to the product of $10d(d-1)$ procyclic subgroups.

Thus G is a boundedly generated profinite group, rather different from the adelic groups considered earlier. It is again clear, from the results of Chapter 10, that G is not a PSG group.

Next, let us examine a metabelian example. For a field F let $A(F)$ denote the 1-dimenional affine group over F, that is the semidirect product $F_+ \rtimes F^*$.

Lemma 12.8.3 *For each finite field F with $|F| > 2$ the group $A(F)$ is equal to the product of 3 cyclic subgroups of order $|F| - 1$.*

Proof. Let λ be a generator for the cyclic group F^*. Then $\mu = \lambda - 1 \neq 0$, so each non-zero element of F is equal to $\mu\lambda^i$ for some i. Write $A(F) = V\langle x\rangle$ where V is the additive group of F and x acts like multiplication by λ, and let $e = 1_F \in V$. Then

$$\mu\lambda^i = x^{-i}(e^{-1}e^x)x^i = x^{-i}(x^{-1})^e x^{i+1}.$$

Thus $V \subseteq \langle x\rangle \cdot \langle x\rangle^e \cdot \langle x\rangle$ and so $A(F) = \langle x\rangle \cdot \langle x\rangle^e \cdot \langle x\rangle$. ∎

Taking $q_i = 2^{p_i}$ as above, we deduce the first claim in

Theorem 12.8.4 *The Cartesian product*

$$G = \prod_{i=1}^{\infty} A(\mathbb{F}_{q_i})$$

is equal to the product of 3 *procyclic subgroups. For each* $c < 1/8$ *there exist infinitely many integers* n *such that*

$$s_n(G) > n^{c\log n}.$$

This shows that Theorem 12.4 (i) is best possible. To establish the second claim, observe that if $p = p_i$ and $1 \leq r < p$ then $\mathbb{F}_{q_i}$ has at least $2^{r(p-r)}$ additive subgroups of index 2^r (Proposition 1.5.2), so for $n = 2^{p+r}$ we have

$$s_n(G) \geq s_n(A(\mathbb{F}_{q_i})) \geq 2^{r(p-r)}.$$

This exceeds $n^{c\log n}$ as long as $r(p-r)/(p+r)^2 > c$. Now taking $r = [p/3]$ one verifies that

$$\frac{r(p-r)}{(p+r)^2} = \frac{1}{8} - o(\frac{1}{p}),$$

and the claim follows.

Now we turn to index growth. Let us begin by estimating the exponent of $\mathrm{GL}_d(q)$, where $q = p^e$. It is easy to see that for each $r \leq d$ this group contains an element of order $q^r - 1$ (a 'Singer cycle', a generator for the multiplicative group $\mathbb{F}_{q^r}^*$ acting on the additive group of $\mathbb{F}_{q^r}$, considered as an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^d$). Writing

$$q^r - 1 = \prod_{m|r} \Phi_m(q),$$

where $\Phi_m(X)$ denotes the mth cycloctomic polynomial, we deduce that the exponent of $\mathrm{GL}_d(q)$ is divisible by

$$L(d,q) = \operatorname*{lcm}_{1\leq m\leq d} \Phi_m(q).$$

In fact $L(d,q)$ is exactly the p'-part of the exponent, since an element of p'-order is semisimple with eigenvalues in $\mathbb{F}_{q^r}^*$ for some $r \leq d$. Now we want to compare $L(d,q)$ with

$$P(d,q) = \prod_{1\leq m\leq d} \Phi_m(q).$$

Let $l \neq p$ be a prime, and let f be the order of q modulo l. The following fact of elementary number theory is proved in [HB], Chapter IX, Lemma 8.1:

- if $m \neq fl^i$ for any i then l does not divide $\Phi_m(q)$
- if $m = fl^i$ with $i \geq 1$ then l^2 does not divide $\Phi_m(q)$.

Hence if l^k is the exact power of l dividing $\Phi_f(q)$, then the l-part of $P(d,q)$ is $l^{k+s(l)}$ where $s(l) \leq \log_l d$. It follows that

$$P(d,q) \leq L(d,q) \prod l^{s(l)} \leq d! \cdot L(d,q) < q^{d \log d} \cdot L(d,q). \tag{12.6}$$

Next, note that

$$|\Phi_m(q)| = \prod_{\zeta} |q - \zeta| \geq (q-1)^{\phi(m)}$$

where ζ ranges over the primitive mth roots of unity and ϕ denotes the Euler function. According to [HW], Theorem 330,

$$\sum_{m=1}^{d} \phi(m) = \frac{3}{\pi^2} d^2 + O(d \log d).$$

Hence

$$P(d,q) \geq (q-1)^{ad^2 - bd \log d}$$

where $a = 3/\pi^2$ and b is a constant. With (12.6) this gives

$$\begin{aligned} L(d,q) &\geq (q-1)^{ad^2 - (b+1)d \log d} \\ &\geq q^{cd^2} \end{aligned}$$

for some absolute constant c.

If the exponent of $\mathrm{PSL}_d(\mathbb{F}_q)$ is E then the exponent of $\mathrm{GL}_d(q)$ divides $2(q-1)E$. So replacing c by a suitable smaller constant we have

Lemma 12.8.5 *Let $E(d,q)$ denote the exponent of $\mathrm{PSL}_d(\mathbb{F}_q)$. Then there exists an absolute constant $c > 0$ such that*

$$E(d,q) \geq q^{cd^2}$$

for all $d \geq 2$ and all prime-powers q.

We can now deduce

Proposition 12.7 *There exists a universal constant R such that*

$$|S| \leq \exp(S)^R$$

for every finite simple group S of Lie type.

Proof. Let $S = {}^*X_l(q)$ in the notation of the **Finite simple groups** window. Then

$$|S| = q^d(1 + o(1)) < q^{2d}$$

where d is the dimension of the associated Lie algebra.

If S is of exceptional type then $d \leq 248$. Also S contains a copy of $(\mathrm{P})\mathrm{SL}_2(\mathbb{F}_q)$, hence an element of order $q + 1$ or $(q + 1)/2$. Thus the exponent of S exceeds $q^{1/2}$, say.

If S is a classical group then $l > \sqrt{d/3}$ and S contains a copy of $(\mathrm{P})\mathrm{SL}_m(\mathbb{F}_q)$ where $m > l/2$. It follows by the preceding lemma that the exponent of S it at least $q^{cd/12}$.

The result follows, with R the maximum of 4×248 and $24/c$.

Thus, although as we have seen the PIG condition imposes various structural restrictions on the finite images of a group, it has no implications for the finite *simple* images, apart from excluding large alternating groups.

Now let (S_n) be an infinite sequence of finite simple groups of Lie type and suppose that

$$\prod_{i=1}^{n-1} |S_i| \leq |S_n|$$

for each $n > 1$. Then the profinite group

$$G = \prod_n S_n$$

has PIG. Indeed , if Q is any finite quotient of G then $Q \cong S_{n_1} \times \cdots \times S_{n_k}$ for some $n_1 < n_2 < \ldots < n_k$ and

$$|Q| = \prod_{i=1}^{k} |S_{n_i}| \leq \prod_{i=1}^{n_k-1} |S_i| \cdot |S_{n_k}| \leq |S_{n_k}|^2 \leq \exp(S_{n_k})^{2R} \leq \exp(Q)^{2R}; \quad (12.7)$$

so $\gamma(G)$ is at most $2R$. On the other hand, if the groups S_n have unbounded Lie ranks then G is not boundedly generated, according to Proposition 12.5.

It is easy to find a sequence of the required kind. For example, let q be a fixed prime-power and take

$$S_n = \mathrm{PSL}_{d(n)}(\mathbb{F}_q)$$

where $d(1) \geq 2$ (or ≥ 3 if $q = 2$) and for each $n > 1$,

$$d(n) \geq d(1) + \cdots + d(n - 1);$$

then S_n contains a copy of $S_1 \times \cdots \times S_{n-1}$. Thus for profinite groups BG *is a strictly stronger condition than* PIG.

To show that this is true also for finitely generated abstract groups, we appeal to the following construction due to [Lubotzky, Pyber & Shalev 1996]:

Proposition 12.8.6 *Let q be a fixed prime-power and $(d(n))$ an arbitrary strictly increasing sequence of integers ≥ 2. Then there exists a finitely generated residually finite group Γ such that*

$$\widehat{\Gamma} \cong \widehat{\mathbb{Z}} \times \prod_n \mathrm{PSL}_{d(n)}(\mathbb{F}_q).$$

Choosing $(d(n))$ as above, we obtain a finitely generated group Γ such that $\widehat{\Gamma}$ is not boundedly generated; and a trivial adjustment to the argument (12.7) shows that $\gamma(\Gamma) \leq 2R + 1$, so Γ has PIG. This establishes the first claim of Theorem 12.8.

Now let Δ be a quotient of Γ and suppose that Δ is a linear group. Then Δ has a residually finite-nilpotent normal subgroup Δ_0 of finite index (↬ **Linear groups**). Let $N < \Delta_0$ be a normal subgroup of finite index Δ such that Δ_0/N is nilpotent. Then Δ/N is an image of $\widehat{\Gamma}$, hence takes the form

$$\Delta/N = C \times M$$

where C is cyclic and M is a product of non-abelian simple groups. Then $M \cap (\Delta_0/N) = 1$ so Δ_0/N is cyclic. It follows that Δ_0 is residually cyclic, hence abelian; and moreover every finite quotient of Δ_0 is cyclic. As Δ_0 is also finitely generated it follows that Δ_0 is a cyclic group.

Thus every linear quotient of Γ is virtually cyclic, and this completes the proof of Theorem 12.8.

Notes

The problem of characterising (soluble) PIG groups was raised in [**Segal 1986**$_b$], where Theorem 12.9(ii) was proved. It was also shown in that paper that for a f.g. residually finite soluble group G of finite rank, the invariant defined by

$$\inf\{\gamma : |G : G^n| \leq n^\gamma \quad \text{for all } \textit{large } n\}$$

(an asymptotic version of our $\gamma(G)$) is equal to the Hirsch length of G.

Theorem 12.9(i) was proved in [**Mann & Segal 1990**], where it was also shown that groups of finite upper rank satisfy PIG.

The equivalence of finite rank, BG, PSG and PIG in pro-p groups was proved partly by [**Lazard 1965**] and partly by [**Lubotzky & Mann 1991**]; for further variations see [**DDMS**], Chapter 3.

The topic of bounded generation in arithmetic groups has received considerable attention; see [**PR**] §4.4, page 203 and references therein. The characterisation of arithmetic groups with the congruence subgroup property in terms of PIG, and hence Theorem 12.10, is due to [**Platonov & Rapinchuk 1993**] and to [**Lubotzky 1995**$_a$].

[**Pyber & Shalev 1997**] proved that a finite group of rank r is the product of $f(r)$ cyclic subgroups; this implies Theorem 12.1. [**Pyber 2000**] proved

that profinite groups with PSG are boundedly generated. His proof is based on the following theorem of [**Hrushovski & Pillay 1995**], which was proved by model-theoretic techniques:

Theorem *Let G be a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$, and G^+ the normal subgroup of G generated by the elements of order p. Then G^+ is a product of k subgroups of order p, where k depends only on n.*

The fact that BG profinite groups have subgroup growth of type at most $n^{\log n}$ is proved in the same paper of Pyber.

The proof that adelic groups are boundedly generated, and all the material of §12.3, is due to [**Liebeck & Pyber 2001**].

Theorems 12.8.2 and 12.8.4 are due to [**Abért, Lubotzky & Pyber**]. Among many other results, this paper establishes further restrictions on the structure of a boundedly generated profinite group (in the spirit of Theorem 12.6) if it is the completion of a BG abstract group, as well as results on the representation theory of BG abstract groups.

All the remaining main results on PIG groups are due to [**Balog, Mann & Pyber 2000**].

The group given in Proposition 12.8.6 was constructed in [**Lubotzky, Pyber & Shalev 1996**] to give the first example of a finitely generated group having subgroup growth type $n^{\log n}$; it was not then known that this is also the growth type for arithmetic groups in positive characteristic having CSP. The same paper gave a construction of a f.g. group with subgroup growth type $n^{\log n/(\log\log n)^2}$, the slowest non-polynomial type known at that time.

Various forms of the 'rank function' $d_n(G)$ were introduced in [**Lubotzky 1986**], where a number of conjectures are proposed.

Chapter 13

The growth spectrum

The group $\mathbb{Z}$ has subgroup growth of type n, while the free group on two generators has growth type n^n, and this is the upper limit for finitely generated groups. In earlier chapters we have seen many intermediate types of subgroup growth; we have also seen that among 'reasonable' classes of groups, such as linear groups, certain intermediate types cannot occur. If one considers arbitrary finitely generated groups, however, then essentially every type of growth between these limits is possible. The main result we establish in this chapter is

Theorem 13.1 *Let $g : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be a non-decreasing function that satisfies the condition $(*)$. Then there exists a 4-generator group having subgroup growth of type $n^{g(n)}$.*

The condition $(*)$ is as follows:

$$\begin{aligned} \text{either} \quad (*)_1 : &\qquad \log x = O(g(x)) \ \text{ and } \ g(x) = o(x) \\ \text{or} \quad (*)_2 : &\qquad g(x^{\log x}) = O(g(x)). \end{aligned}$$

Condition $(*)_1$ corresponds to subgroup growth of types ranging from $n^{\log n}$ up to (though not including) n^n. Condition $(*)_2$ allows a range of growth types down to (though not including) polynomial growth, type n. It means that g must grow rather gently, and implies in particular that

$$g(x) = O((\log\log x)^k)$$

for some $k > 0$, and so excludes examples such as $g(x) = (\log x)^\varepsilon$ with $0 < \varepsilon < 1$. However, every function of the form

$$g(x) = (\log\log \ldots \log x)^k$$

(at least two iterations of log, and any $k > 0$) does satisfy $(*)_2$. The possible small gap in the 'growth spectrum' left by the above statement is partially filled by the

Scholium *For each positive integer k there exists a 4-generator group having growth type at most $n^{(\log n)^{1/k}}$ and at least $n^{(\log n)^{1/(k+1)}}$.*

It should be said that the condition $(*)$ is merely a technical requirement of the proof, and is probably not really necessary for the theorem.

The proof of Theorem 13.1 consists of two quite different constructions. These have a common strategy, however. Let us call growth of type $n^{g(n)}$ 'fast' if $\log n = O(g(n))$, and 'slow' if $g(n) = o(\log n)$. In each case, we begin by constructing a *profinite* group G having the requisite growth type: fast in Section 1, slow in Section 3. Then in Sections 2 and 4 we exhibit a finitely generated dense subgroup Γ of G whose profinite completion $\widehat{\Gamma}$ is not too different from G: the construction of Section 4 actually gives $\widehat{\Gamma} \cong G$, while in Section 2 we obtain $\widehat{\Gamma} \cong G \times \widehat{\mathbb{Z}}$. In each case, the subgroup growth of Γ will be determined by that of G.

In the case of fast subgroup growth, the results obtained are sharper: the group Γ actually has growth of *strict* type $n^{g(n)}$ and *maximal subgroup* growth type $n^{g(n)}$, provided the function g grows fairly smoothly.

The results stated above exhibit a wide range of subgroup growth types. Within any given growth type, of course, there is room for finer classification; for example, groups of exponential growth type were further distinguished in chapter 3 by the invariant σ, and we shall see that this can take *every positive value*. Of particular interest is the class of groups with polynomial subgroup growth, where the relevant invariant is the *degree*, that is,

$$\alpha(G) = \inf \{\alpha \mid s_n(G) = O(n^\alpha)\}.$$

Some suggestive results about the 'degree spectrum' – the possible range af values taken by $\alpha(G)$ – are discussed in the *Notes* at the end of the chapter.

13.1 Products of alternating groups

Here we establish

Theorem 13.1.1 *Let J be a set of integers ≥ 5 and let $g : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be a non-decreasing function. For $j \in J$ put $f(j) = \lceil j^{g(j)} \rceil$. Then the profinite group*

$$G = G(J, f) = \prod_{j \in J} \mathrm{Alt}(j)^{(f(j))}$$

satisfies

$$m_n(G) \geq n^{g(n)} \quad \textit{for all } n \in J$$
$$m_n(G) \leq s_n(G) \leq n^{g(n)+20\log n+29} \quad \textit{for all } n.$$

Thus provided J is infinite and $\log n = O(g(n))$, both the subgroup growth and the maximal sugroup growth of G are of type $n^{g(n)}$. (**Exercise**: supposing $g(n)$ grows much faster than n, why does this not contradict the absolute upper bound n^n established in Chapter 2?) If J contains *all* large integers then G even has subgroup growth of *strict* type $n^{g(n)}$; the same holds as long as J is infinite and $\log f(j_{k+1})/\log f(j_k)$ is bounded, where j_k is the kth element of J in ascending order.

Example Let $g(j) = cj/\log j$, where c is a positive constant. Then (provided J is infinite) the group G has exponential subgroup growth, and

$$\sigma(G) = \limsup \frac{\log s_n(G)}{n} = c.$$

Thus the invariant σ takes the full spectrum of values.

The lower bound in Theorem 13.1.1 is easy to see. Indeed, since $\mathrm{Alt}(j)$ has a maximal subgroup $\mathrm{Alt}(j-1)$ of index j, it is clear that G has at least $f(j)$ maximal (open) subgroups of index j for each $j \in J$.

The rest of this section is devoted to the proof of the upper bound. This depends on the following concept:

Definition Let Ω be a finite set. A *standard subgroup* of $\mathrm{Sym}(\Omega)$ is a subgroup of the form

$$\mathrm{Alt}(\Omega_1) \times \cdots \times \mathrm{Alt}(\Omega_r)$$

where $\Omega_1, \ldots, \Omega_r$ are disjoint subsets of Ω of cardinality at least 5. We allow $r = 0$, corresponding to the identity subgroup.

Here and below, the convention is that for a subset Δ of Ω, we identify $\mathrm{Alt}(\Delta)$ with the pointwise stabilizer of $\Omega \setminus \Delta$ in $\mathrm{Alt}(\Omega)$. Now the key to understanding subgroup growth in products of alternating groups is the next theorem, whose proof is sketched in the **Permutation groups** window, §3:

Theorem 13.1.2 *Let Ω be a finite set and S a standard subgroup of* $\mathrm{Sym}(\Omega)$. *Then each subgroup H of S contains a standard subgroup H_* of* $\mathrm{Sym}(\Omega)$ *such that*

$$|S : H_*| \leq |S : H|^5.$$

To prove the upper bound in Theorem 13.1.1 we proceed in steps.

Step 1 Let Ω be a finite set and $S = \mathrm{Alt}(\Omega_1) \times \cdots \times \mathrm{Alt}(\Omega_r)$ a standard subgroup of $\mathrm{Sym}(\Omega)$. Then *the number $N_S(m)$ of core-free standard subgroups of index m in S is at most m^4.*

A subgroup H of S is *core-free* if it contains no non-identity normal subgroup of S; since the direct factors $A_i = \mathrm{Alt}(\Omega_i)$ are simple, this is equivalent to saying that $H_i = H \cap A_i < A_i$ for each i. Moreover, it is clear that H is standard if and only if $H = H_1 \times \cdots \times H_r$ and H_i is a standard subgroup of A_i for each i. So

$$N_S(m) = \sum N_{A_1}(m_1) \ldots N_{A_r}(m_r),$$

summed over all factorisations $m = m_1 \dots m_r$ with each $m_i \geq 2$.

An elementary exercise shows that the number of such factorisations of m is less than m^2. We claim that for each i,

$$N_{A_i}(m_i) \leq m_i^2. \tag{13.1}$$

Once established, this will complete the proof of Step 1, since it implies

$$N_S(m) \leq \sum m_1^2 \dots m_r^2 = \sum m^2 \leq m^2 \cdot m^2 = m^4.$$

It remains to prove (13.1). Write $n_i = |\Omega_i|$. Modulo even permutations, the number of proper partitions of Ω_i that give rise to a standard subgroup of index m_i in $\mathrm{Alt}(\Omega_i)$ is at most the number of (unordered) tuples $(b_1, \dots, b_t)$, with $t \geq 2$ and each $b_j \geq 1$, such that

$$n_i = b_1 + \dots + b_t \tag{13.2}$$

and

$$\frac{1}{2} n_i! = m_i \cdot \prod (\frac{1}{2} b_j!).$$

Using induction on k, it is a simple exercise to show that for any $k > 1$, there are no more than k (ordered) tuples $(b_1, \dots, b_t)$, with $t \geq 2$ and each $b_j \geq 1$, such that (13.2) holds and $n_i! / \prod b_j! < k$. We may infer that the number of conjugacy classes of standard subgroups of index $m_i > 1$ in $\mathrm{Alt}(\Omega_i)$ is at most m_i, and (13.1) follows since each such subgroup has at most m_i conjugates.

Step 2 With S as in Step 1, *the number of core-free subgroups of index n in S is at most $n^{25+20 \log n}$.*

According to Theorem 16.4.17, each subgroup H of index n in S contains a standard subgroup H_* having index at most n^5 in S. Of course H_* is core-free if H is, and by Step 1 the number of possibilities for such an H_* is at most $n^5 \times n^{20} = n^{25}$. On the other hand, given H_*, the number of subgroups of index n in S that contain H_* is at most $|S : H_*|^{\log(|S:H_*|/n)} \leq n^{20 \log n}$ (see Lemma 1.2.3). Putting these together gives the stated bound.

Step 3 *Conclusion.*

Let H be an open subgroup of G with $|G : H| \leq n$. Put $K = \mathrm{core}_G(H)$, the biggest normal subgroup of G contained in H. Now each open normal subgroup of G is the product of all but finitely many of the direct factors $\mathrm{Alt}(j)$ (as these are all simple groups), so

$$G/K \cong \prod_{j \in J} \mathrm{Alt}(j)^{(t_j)}$$

where $t_j \leq f(j)$ for all j and $t_j = 0$ for almost all j. On the other hand, G/K acts faithfully and transitively on the right cosets of H.

Lemma 13.1.3 *If* $\mathrm{Sym}(m)$ *contains a transitive subgroup isomorphic to* $\prod \mathrm{Alt}(j)^{(t_j)}$ *then*

$$\prod j^{t_j} \leq m.$$

Postponing the proof of this, we apply it with $m = |G : H| \leq n$ and deduce that $n \geq \prod j^{t_j} = q$, say. Now given q, the number of factorisations of this form is at most $q^2 \leq n^2$, and there are at most n possibilities for q. So the number of possibilities for the sequence $\mathbf{t} = (t_j)$ is at most n^3.

Given t_j, there are $\binom{f(j)}{t_j}$ ways to choose a normal subgroup $\mathrm{Alt}(j)^{(f(j)-t_j)}$ in $\mathrm{Alt}(j)^{(f(j))}$. Hence the number of possibilities for K, given the sequence $\mathbf{t}$, is

$$\begin{aligned}\prod \binom{f(j)}{t_j} \leq \prod f(j)^{t_j} = \prod \left\lceil j^{g(j)} \right\rceil^{t_j} &\leq \prod j^{(g(j)+1)t_j} \\ &\leq \Big(\prod j^{t_j}\Big)^{g(n)+1} = q^{g(n)+1} \leq n^{g(n)+1};\end{aligned}$$

here we may replace $g(j)$ by $g(n)$ because g is non-decreasing and $t_j = 0$ whenever $j > n$.

Altogether, the number of possibilities for K is thus at most $n^{g(n)+4}$. Given K, the number of possibilities for H is equal to the number of core-free subgroups of index at most n in the standard group G/K, which by Step 2 is at most $n \times n^{25+20\log n}$. Thus

$$s_n(G) \leq n^{g(n)+20\log n+30}.$$

This completes the proof, apart from

Proof of Lemma 13.1.3 Suppose $A_1 \times \cdots \times A_k$ is a transitive subgroup of $\mathrm{Sym}(m)$, where $A_i \cong \mathrm{Alt}(n_i)$ and

$$5 \leq n_1 \leq n_2 \leq \ldots \leq n_k.$$

We have to show that $\prod_{i=1}^{k} n_i \leq m$, and argue by induction on m. We may clearly assume that $k \geq 2$.

Case 1. Suppose that each A_i is transitive. Then both A_1 and $A_2 \times \cdots \times A_k$ are regular, so

$$\frac{1}{2}n_1! = \prod_{i=2}^{k}(\frac{1}{2}n_i!) = m,$$

which forces $k = 2$, $n_1 = n_2$ and $n_1 n_2 < m$ since $n_1 \geq 5$.

Case 2. Suppose that A_j is intransitive. Put $B = \prod_{i \neq j} A_i$ and let $U_1, \ldots, U_r$ be the orbits of A_j. Then B permutes the set $\mathcal{U} = \{U_1, \ldots, U_r\}$ transitively, with kernel K say. Now $B = K \times C$ where

$$K = \prod_{i \in X} A_i, \qquad C = \prod_{i \in Y} A_i$$

and $X \cup Y = \{1, \ldots, k\} \setminus \{j\}$. Moreover, C acts faithfully and transitively on $\mathcal{U}$ so inductively we have

$$\prod_{i \in Y} n_i \leq r.$$

On the other hand, $A_j \times K$ acts faithfully and transitively on U_1, giving

$$\prod_{i \in X \cup \{j\}} n_i \leq m/r.$$

The result follows.

13.2 Some finitely generated permutation groups

Let

$$G = G(J, f) = \prod_{j \in J} \mathrm{Alt}(j)^{(f(j))}$$

be the profinite group discussed in the preceding section. Under suitable conditions on J and f, we shall see that G contains a finitely generated dense subgroup Γ that has essentially the same subgroup growth as G.

We assume that f takes the form $f(j) = \left\lceil j^{g(j)} \right\rceil$ for some non-decreasing function $g : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ such that

$$\log x = O(g(x)) \quad \text{and} \quad g(x) = o(x). \tag{$(*)_1$}$$

Theorem 13.2.1 *Suppose that J is an infinite set of sufficiently large odd integers. Then there exists a 4-generator group Γ such that*

$$\widehat{\Gamma} \cong G(J, f) \times \widehat{\mathbb{Z}}.$$

Before embarking on the proof let us deduce

Corollary 13.2.2 *Let $g : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be a non-decreasing function that satisfies I. Then there exist a 4-generator group Γ and a constant $a > 0$ such that*

$$\begin{aligned} n^{g(n)} \leq m_n(\Gamma) \leq s_n(\Gamma) \quad & \textit{for all large odd } n \\ s_n(\Gamma) \leq n^{ag(n)} \quad & \textit{for all large } n. \end{aligned}$$

Proof. We take J to consist of all odd integers $\geq j_1$. According to Theorem 13.1.1, $G = G(J, f)$ satisfies

$$\begin{aligned} n^{g(n)} \leq m_n(G) \quad & \text{for all } n \in J \\ s_n(G) \leq n^{g(n)+20\log n+29} \quad & \text{for all } n. \end{aligned}$$

Since G is isomorphic to a quotient of $\widehat{\Gamma}$ we deduce that $s_n(\Gamma) \geq m_n(\Gamma) \geq n^{g(n)}$ for all odd $n \geq j_1$.

On the other hand, Proposition 1.3.6(i) shows that

$$\begin{aligned} s_n(\Gamma) = s_n(\widehat{\Gamma}) &= s_n(G \times \widehat{\mathbb{Z}}) \\ &= s_n(G \times \mathbb{Z}) \leq s_n(\mathbb{Z}) \cdot s_n(G) \cdot n \\ &\leq n^{g(n)+20\log n+31} \leq n^{ag(n)} \end{aligned}$$

for large values of n, where $a > 0$ depends on the constant implied in $\log x = O(g(x))$. ■

Remarks (i) Suppose that the function g is reasonably smooth in the sense that $g(n)/g(n-1)$ is bounded above for all n (this further restriction on g is a pretty mild one). Then Γ actually has subgroup growth of *strict* type $n^{g(n)}$: for when n is large and even we have $s_n(\Gamma) \geq m_{n-1}(\Gamma) \geq (n-1)^{g(n-1)} \geq n^{\varepsilon g(n)}$ where ε is some positive constant.

(ii) Take $g(n) = cn/\log n$, where $c > 0$. Then

$$g(n) + 20\log n + 31 = g(n)(1 + o(1)),$$

so the finitely generated group Γ satisfies

$$\sigma(\Gamma) = \limsup \frac{\log s_n(\Gamma)}{n} = c.$$

The rest of this section is devoted to the proof of Theorem 13.2.1. We have to set up some notation. J is an infinite set of odd integers greater than or equal to some constant $c \geq 5$, and $f : J \to \mathbb{N}$ is a function. Define $f(n) = 0$ for $n \notin J$, and let $n_1 \leq n_2 \leq \ldots$ be the non-decreasing sequence in which each integer n occurs exactly $f(n)$ times. Let

$$\begin{aligned}\Omega &= \{(i,m) \mid i \in \mathbb{N},\ 1 \leq m \leq n_i\} \\ &= \bigcup_{i=1}^{\infty} \Omega_i \subset \mathbb{N} \times \mathbb{N}\end{aligned}$$

where $\Omega_i = \{(i,m) \mid 1 \leq m \leq n_i\}$, and let G be the subgroup of $\mathrm{Sym}(\Omega)$ consisting of permutations g such that $\Omega_i g = \Omega_i$ and $g_{|\Omega_i}$ is an even permutation, for each i. Identifying Ω_i with the set $\{1, \ldots, n_i\}$ via the second component gives an isomorphism $\theta_i : \mathrm{Alt}(\Omega_i) \to \mathrm{Alt}(n_i)$, and for $g \in G$ we write

$$g_i = \psi_i(g) = \theta_i(g_{|\Omega_i}) \in \mathrm{Alt}(n_i).$$

Evidently $g \mapsto (g_i)_{i \in \mathbb{N}}$ gives an isomorphism

$$G \cong G(J,f) = \prod_{j \in J} \mathrm{Alt}(j)^{(f(j))}.$$

The *support* of g is

$$\mathrm{supp}(g) = \{\omega \in \Omega \mid \omega^g \neq \omega\}.$$

Let D denote the set of all elements of G having finite support; thus D is just the restricted direct product of the groups $\mathrm{Alt}(\Omega_i)$. It is a normal subgroup of G.

Fix a sequence (k_i) of positive integers such that $k_i + 1 \leq n_i/2$ for each i and n_i/k_i is unbounded as $i \to \infty$. Put

$$l_i = \left[\frac{n_i}{1 + k_i} \right], \tag{13.3}$$

so $k_i l_i \leq n_i - l_i$, and (l_i) is an unbounded sequence of integers ≥ 2. Now let

$$\begin{aligned} L_i &= \{i\} \times \{l_i, 2l_i, \ldots, k_i l_i\} \subseteq \Omega_i, \\ L &= \bigcup_{i=1}^{\infty} L_i \subset \Omega. \end{aligned}$$

Let Q be a subgroup of G such that

$$\begin{aligned} &\operatorname{supp}(g) \subseteq L \text{ for every } g \in Q, \\ &Q \cap D = 1, \\ &\quad \text{if } n_i = n_j \text{ and } i \neq j \text{ then } \psi_{i|Q} \neq \psi_{j|Q}. \end{aligned} \tag{13.4}$$

The existence and nature of such a subgroup is a point we shall return to later. Now define two elements μ, τ of G by setting

$$\begin{aligned} \mu_i &= (123) \quad \text{for all } i \\ \tau_i &= (123 \ldots n_i) \quad \text{for all } i, \end{aligned}$$

and let

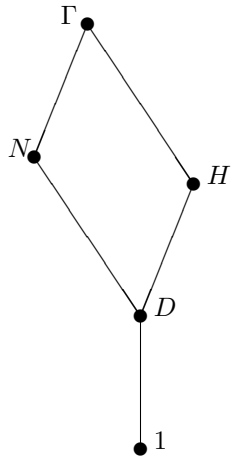
$$\begin{aligned} \Gamma &= \langle \mu, \tau, Q \rangle \leq G \\ N &= \left\langle \mu^{\Gamma} \right\rangle, \ H = D \langle \tau, Q \rangle . \end{aligned}$$

Proposition 13.2.3 *The following hold:*

$\Gamma = NH$ *and* $N \cap H = D$;

$N/D \cong \mathrm{Alt}(\mathbb{Z})$;

$H/D \cong Q \wr \mathbb{Z}$.



Corollary 13.2.4 *Let K be the kernel of the map $\iota : \widehat{\Gamma} \to G$ induced by the inclusion $\Gamma \to G$ and let $\overline{D}$ be the closure of D in $\widehat{\Gamma}$. Then*

$$\widehat{\Gamma} = \overline{D} \times K \cong G \times \widehat{Q \wr \mathbb{Z}}.$$

Proof. We may identify the profinite completion $\widehat{D}$ of D with G. The universal property of $\widehat{D}$ gives a commutative diagram

$$\begin{array}{ccccc} & & D & & \\ & \swarrow & & \searrow^{j} & \\ \widehat{D} & & \xrightarrow{\pi} & & \overline{D} \xrightarrow{\iota_{|\overline{D}}} G \end{array},$$

where j denotes the inclusion $D \to \overline{D}$. Then π is surjective and $\iota_{|\overline{D}} \circ \pi$ is the identity map $\widehat{D} \to G$, and it follows that $\iota_{|\overline{D}}$ is an isomorphism. Hence $\overline{D} \cong G$ and $\overline{D} \cap K = 1$. Since $\iota_{|\overline{D}}$ is surjective we also have $\widehat{\Gamma} = \overline{D}K$; but $\overline{D} \lhd \widehat{\Gamma}$ because $D \lhd \Gamma$, so $\widehat{\Gamma} = \overline{D} \times K$ as claimed.

Finally,

$$K \cong \widehat{\Gamma}/\overline{D} \cong \widehat{(\Gamma/D)} = \widehat{(\Gamma/N)}$$

since $N/D \cong \mathrm{Alt}(\mathbb{Z})$ is an infinite simple group, and $\Gamma/N \cong H/D \cong Q \wr \mathbb{Z}$ by the proposition. ■

Before proving Proposition 13.2.3 let us complete the

Proof of Theorem 13.2.1. Recall that $f(j) = \left\lceil j^{g(j)} \right\rceil$ where $g : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is non-decreasing and

$$\log x = O(g(x)), \quad g(x) = o(x).$$

Since the function $x \mapsto x \log x$ is strictly increasing, we may define k_i by

$$k_i \log k_i = \lceil 8g(n_i) \log n_i \rceil .$$

The conditions on g ensure that n_i/k_i is unbounded as $i \to \infty$ and that $5 \leq k_i \leq n_i/2 - 1$ for each i provided n_1 is large enough. Now we need the following observation:

Lemma 13.2.5 *Let $k \geq 5$. Then there are at least $k^{k/4}$ distinct monomorphisms from* Alt(5) *into* Alt(k).

Proof. Write $k = 5r + e$ where $0 \leq e \leq 4$. Let $A \cong \mathrm{Alt}(5)$ be the diagonal subgroup in

$$\prod_{j=0}^{r-1} \mathrm{Alt}(E_j) \leq \mathrm{Alt}(k)$$

where $E_j = \{5j + 1, 5j + 2, \ldots, 5j + 5\}$. It is easy to see that $\mathrm{C}_{\mathrm{Sym}(k)}(A) \cong \mathrm{Sym}(r) \times \mathrm{Sym}(e)$, so that by applying inner automorphisms of $\mathrm{Sym}(k)$ we obtain $k!/r!e!$ distinct monomorphisms $A \to \mathrm{Alt}(k)$. The lemma follows since

$$\frac{k!}{r!e!} \geq \frac{k!}{(r+e)!} \geq \left(\frac{k}{2}\right)^{k/2} \geq k^{k/4}.$$

■

It follows that for each i, there are at least $f(n_i)$ distinct monomorphisms from Alt(5) into Alt(k_i). Indeed,

$$\log f(n_i) \leq 2g(n_i) \log n_i \leq \frac{1}{4} k_i \log k_i = \log \left(k_i^{k_i/4} \right).$$

Given $n \in J$, let $i, i+1, \ldots, i+f(n)-1$ be all the indices t for which $n_t = n$, and let $\eta_i, \ldots, \eta_{i+f(n)-1}$ be distinct monomorphisms from Alt(5) into Alt(k_i). Let $u = (123)$ and $v = (12345) \in \mathrm{Alt}(5)$, and for $i \leq t \leq i + f(n) - 1$ define elements α_t, $\beta_t \in \mathrm{Alt}(L_t)$ by

$$\theta_t(\alpha_t) = \eta_t(u)$$
$$\theta_t(\beta_t) = \eta_t(v).$$

Now take $\alpha = (\alpha_i)$ and $\beta = (\beta_i) \in G$ and put $Q = \langle \alpha, \beta \rangle$.

Then Q satisfies the conditions (13.4), and by Corollary 13.2.4 we have $\widehat{\Gamma} = G \times \widehat{Q \wr \mathbb{Z}}$. Evidently, $u \mapsto \alpha$, $v \mapsto \beta$ gives an isomorphism $\mathrm{Alt}(5) \cong Q$, so Q is a perfect group. This implies that

$$\widehat{Q \wr \mathbb{Z}} = \widehat{\mathbb{Z}}.$$

To see this, write $Q \wr \mathbb{Z} = Q \wr \langle x \rangle$, and note that if π is any homomorphism from $Q \wr \langle x \rangle$ to a group of finite order $n > 1$, then

$$\pi(Q) = \pi([Q, Q]) = \pi([Q, Q^{x^n}]) = 1,$$

which implies that the profinite completion of $Q \wr \langle x \rangle$ is the same as that of $\langle x \rangle$.

Thus in fact $\widehat{\Gamma} \cong G \times \widehat{\mathbb{Z}}$ as claimed. This completes the proof of Theorem 13.2.1, modulo Proposition 13.2.3.

Proof of Proposition 13.2.3. Write $A_i = \mathrm{Alt}(\Omega_i) < G$, and for each subset I of $\mathbb{N}$ let

$$\pi_I : G \to A_I = \prod_{i \in I} A_i$$

denote the projection mapping (and $\pi_i = \pi_{\{i\}}$). Recall that $N = \langle \mu^\Gamma \rangle$.

Step 1. We claim that $\pi_I(N) = A_I$ for every finite set I. When $|I| = 1$ this is clear since $\pi_i(N) \geq \left\langle \mu_i^{\langle \tau_i \rangle} \right\rangle = A_i$ for each i. Now we argue by induction on $|I|$; suppose that $|I| > 1$ and that $B = \pi_I(N) < A_I$. Let $i \in I$ and put $K = I \setminus \{i\}$. Inductively we may suppose that $\pi_K(B) = A_K$. Since A_i is simple and $|B| < |A_I|$ it follows that $B \cap A_i = 1$ and that $\pi_{K|B}$ is an isomorphism $B \to A_K$. Composing its inverse with $\pi_{i|B}$ we obtain an epimorphism $A_K \to A_i$, which restricts to an isomorphism

$$\phi_{ki} : A_k \to A_i$$

for some $k \in K$. Certainly $n_k = n_i = n$, say, in this case, and we obtain a commutative diagram

$$\begin{array}{ccccc} & & N & & \\ & \swarrow^{\pi_k} & & \searrow^{\pi_i} & \\ A_k & & \xrightarrow{\phi_{ki}} & & A_i \\ \downarrow & & & & \downarrow \\ \mathrm{Alt}(n) & & \xrightarrow{\sigma} & & \mathrm{Alt}(n) \end{array},$$

the vertical maps being θ_k and θ_i and σ some automorphism of $\mathrm{Alt}(n)$. Now let $0 \leq m \leq n-3$ and observe that

$$\begin{aligned} \sigma(m+1, m+2, m+3) &= \sigma\theta_k\pi_k((\mu^{t^m})) \\ &= \theta_i\pi_i((\mu^{t^m})) = (m+1, m+2, m+3). \end{aligned}$$

It follows that σ is the identity automorphism of $\mathrm{Alt}(n)$, and hence that $\psi_k = \theta_k\pi_k$ and $\psi_i = \theta_i\pi_i$ have the same restriction to N. Now let $x \in Q$ and let $\gamma \in \mathrm{Alt}(n)$, so $\gamma = \psi_k(a) = \psi_i(a)$ for some $a \in N$. Then

$$\gamma^{\psi_k(x)} = \psi_k(a^x) = \psi_i(a^x) = \gamma^{\psi_i(x)};$$

hence $\psi_k(x) = \psi_i(x)$ since $\mathrm{Alt}(n)$ has trivial centre. This contradicts (13.4), and the claim follows.

Step 2. Next we show that $N \geq D$. It will suffice to show that $N \geq A_i$ for each i. Fix i and put

$$\gamma(i) = [\mu, \mu^{\tau^{n_i-2}}].$$

Then $\gamma(i) \in N$ and

$$\begin{aligned} \pi_j(\gamma(i)) &= 1 \quad \text{if } \ n_j > n_i \\ \pi_j(\gamma(i)) &= \sigma_j \quad \text{if } \ n_j = n_i \end{aligned}$$

where $\sigma_j = \theta_j^{-1}(1, n_i - 1, 2) \neq 1$. In particular, $\gamma(i) \in A_I$ where $I = \{j \mid n_j \leq n_i\}$. Now let $\alpha \in A_i$. Step 1 shows that there exists $x \in N$ such that $\pi_I(x) = \alpha$. Then $[\gamma(i), x] \in N$ and

$$\begin{aligned} &\pi_j([\gamma(i), x]) = 1 \quad \text{if } \ n_j > n_i \\ &\pi_j([\gamma(i), x]) = [\sigma_j, 1] = 1 \quad \text{if } \ n_j = n_i \text{ and } j \neq i \\ &\pi_i([\gamma(i), x]) = [\sigma_i, \alpha]. \end{aligned}$$

Thus $[\sigma_i, \alpha] = [\gamma(i), x] \in A_i \cap N$, and as $\sigma_i \neq 1$ it follows that $A_i \leq N$ as required.

Step 3. We claim that for each $t \neq 0$,

$$[Q, Q^{\tau^t}] \subseteq D.$$

It suffices to verify this for $t \geq 1$. Note now that $L_i \cap L_i\tau^t = \emptyset$ whenever $l_i > t$. This implies that the support of $[Q, Q^{\tau^t}]$ is contained in the finite set

$$\bigcup_{l_i \leq t} L_i,$$

and the claim follows.

Hence there is a natural epimorphism

$$\phi : \operatorname*{Dr}_{t=-\infty}^{\infty} Q^{\tau^t} \to \frac{\left\langle Q^{\langle\tau\rangle} \right\rangle D}{D}.$$

Since $\mathrm{supp}(Q^t) \cap \mathrm{supp}(Q^s)$ is finite whenever $s \neq t$, while every non-identity element of Q has infinite support, we see that $\ker \phi = 1$. Thus ϕ is an isomorphism.

It is easy to see that no positive power of τ lies in $\left\langle Q^{\langle\tau\rangle} \right\rangle D$. Thus

$$H/D = D \left\langle \tau, Q \right\rangle / D = \frac{\left\langle Q^{\langle\tau\rangle} \right\rangle D}{D} \cdot \langle\tau\rangle \cong Q \wr \mathbb{Z}.$$

Step 4. To show that $N/D \cong \mathrm{Alt}(\mathbb{Z})$, let $\mathcal{T}$ denote the set of all integer sequences $(\underline{t}) = (t_i)_{i \in \mathbb{N}}$ with

$$1 \leq t_i \leq n_i$$

for all i. Define an equivalence relation on $\mathcal{T}$ by setting

$$(\underline{t}) \sim (\underline{s}) \Longleftrightarrow t_i = s_i \text{ for sufficiently large } i.$$

We denote the equivalence class of $(\underline{t})$ by $\mathbf{t}$. The group G permutes $\mathcal{T}$ by $(\underline{t})^g = (\underline{s})$ where

$$(i, s_i) = (i, t_i)^g$$

for each i, and this action respects $\sim$. Clearly D is contained in the kernel of the induced action of G on $\mathcal{T}/\sim$. For each $n \in \mathbb{Z}$ we define the element $\mathbf{n} \in \mathcal{T}/\sim$ to be the equivalence class of a sequence $(\underline{t})$ such that for sufficiently large indices i,

$$\begin{aligned} t_i &= n_i \quad \text{if} \quad n = 0 \\ t_i &= n \quad \text{if} \quad n > 0 \\ t_i &= n_i + n \quad \text{if} \quad n < 0 \end{aligned}$$

(the value of t_i for small i is immaterial). The set $\mathbf{Z} = \{\mathbf{n} \mid n \in \mathbb{Z}\}$ is naturally bijective with $\mathbb{Z}$. Our aim is to show that the action of N on $\mathcal{T}/\sim$ preserves the subset $\mathbf{Z}$, induces on it the full alternating group $\mathrm{Alt}(\mathbf{Z})$ (consisting of all even permutations of finite support), and that the kernel of the induced action is exactly D.

Now $N = \left\langle \mu^{\langle Q,\tau\rangle} \right\rangle$. It is straightforward to verify that Q acts as the identity on $\mathbf{Z}$, that τ acts as the shift $\mathbf{n} \mapsto \mathbf{n}+\mathbf{1}$, and that μ acts as the three-cycle $(\mathbf{1}, \mathbf{2}, \mathbf{3})$. Since $\mathrm{Alt}(\mathbb{Z})$ is generated by the three-cycles $(n, n+1, n+2)$ it follows that the action of N induces $\mathrm{Alt}(\mathbf{Z})$ on $\mathbf{Z}$. That the kernel of this action is exactly D is not quite as obvious as it seems, and we leave it as an exercise for the reader: the key point is to show that if $y \in N$ then there exists b, independent of i, such that

$$\mathrm{supp}(y_i) \subseteq \{i\} \times (\{1, 2, \ldots, b\} \cup \{n_i - b, n_i - b + 1, \ldots, n_i\})$$

for all large i. It follows that if $y \notin D$ then y must move $\mathbf{n}$ for some n with $|n| \leq b$.

Step 5. It only remains to show that $N \cap H \leq D$. This follows from the preceding step: for if $h \in H = D\langle \tau, Q\rangle$ then h acts on $\mathbf{Z}$ as some power of the shift $\mathbf{n} \mapsto \mathbf{n}+\mathbf{1}$, while N acts by permutations of finite support; so if $h \in N \cap H$ then h acts as the identity on $\mathbf{Z}$ and hence belongs to D. This concludes the proof of Proposition 13.2.3.

13.3 Some profinite groups with restricted composition factors

In Section 1 we obtained groups with relatively fast subgroup growth by putting together arbitrarily large finite alternating groups. Results from several earlier chapters suggest that groups having relatively slow subgroup growth are likely

to have more restricted (upper) composition factors; here we consider some examples where these factors are of uniformly bounded rank.

Let $(T_k)_{k\geq 0}$ be a sequence of finite groups, satisfying the following conditions for all k, where $\tau_k = |T_k|$ and r and t are fixed positive constants:

$$\tau_k \geq \tau_{k-1}; \tag{i}$$
$$\mathrm{rk}(T_k) \leq r; \tag{ii}$$

T_k contains an elementary abelian subgroup A_k such that

$$\tau_k \leq |A_k|^t; \tag{iii}$$

if μ_k is the minimal index of any proper subgroup in T_k then

$$\mu_k \geq \mu_{k-1} \quad \text{and} \quad \tau_k \leq \mu_k^t. \tag{iv}$$

For example, we could have $T_k = X(\mathbb{F}_{p_k^e})$ where $X(F)$ is a simple group of fixed Lie type over the field F, (p_k) is an increasing sequence of primes and e is constant: see the **Finite simple groups** window.

Let $(l_k)_{k\geq 0}$ be a sequence of integers ≥ 2, for $k \geq 1$ put

$$m_k = \prod_{j=0}^{k-1} l_j, \tag{13.5}$$

and write

$$B_k = T_k^{(m_k)}.$$

Now let $W_1 = T_0$, and for $k > 1$ let W_k be an extension group of B_{k-1} by W_{k-1}. Thus we have an exact sequence

$$1 \to B_{k-1} \to W_k \to W_{k-1} \to 1,$$

and we may form the inverse limit

$$W = W((\underline{T}), (\underline{l})) = \varprojlim W_k.$$

This is a profinite group, whose finite quotients are just the images of the various groups W_k.

Let us estimate the subgroup growth of W, assuming for simplicity that l_0 is even.

Lemma 13.3.1 *If $n < \mu_{k+1}$ then $s_n(W) \leq n^{2trm_k}$.*

Proof. Note to begin with that

$$\sum_{j=0}^{k} m_j < 2m_k, \tag{13.6}$$

since $m_j = l_{j-1}m_{j-1} \geq 2m_{j-1}$ for each $j \geq 1$. Now if $i > k$ then $\mu_i \geq \mu_{k+1} > n$ so B_i has no proper subgroup of index n or less. It follows that every subgroup of index $\leq n$ in W_{i+1} contains B_i, and hence that

$$s_n(W_{i+1}) = s_n(W_i) = \ldots = s_n(W_{k+1}).$$

Now W_{k+1} has a subnormal series of length $\sum_{j=0}^{k} m_j < 2m_k$, whose factors T_j satisfy conditions (ii) and (iv). Applying Proposition 1.9.1 from Chapter 1 we deduce that

$$s_n(W_{k+1}) \leq n^{2trm_k}.$$

The lemma follows since $s_n(W)$ is the supremum of the $s_n(W_i)$. ■

Lemma 13.3.2 *For $n = \tau_k^{2m_k}$ we have*

$$s_n(W) \geq n^{m_k/8t}.$$

Proof. Let us write $\tau = \tau_k$ and $m = m_k$. Using (13.6) we have

$$|W_{k+1}| = \prod_{j=0}^{k} \tau_j^{m_j} \leq \tau^{\sum m_j} < \tau^{2m} = n.$$

On the other hand,

$$W_{k+1} \geq B_k \geq A_k^{(m)}.$$

If $A_k \cong C_p^e$ then $p^{et} \geq \tau$, and $A_k^{(m)}$ has at least $p^{e^2m^2/4}$ subgroups. Since $|W_{k+1}| < n$ it follows that

$$\begin{aligned} s_n(W) \geq s_n(W_{k+1}) &= s(W_{k+1}) \\ &\geq p^{e^2m^2/4} \geq \tau^{m^2/4t} = n^{m/8t}. \end{aligned}$$

■

The two lemmas show that we can control the subgroup growth of W by fine-tuning the growth of m_k as against τ_k and μ_k. Let us apply this to a specific example. Let g be an unbounded, non-decreasing positive real-valued function such that

$$g(x^{\log x}) \leq Ag(x) \tag{13.7}$$

for all large x, where A is a positive constant. Then the following holds:

Lemma 13.3.3 *There are constants $B, C > 0$ such that for each integer $m \geq C$ there exists a prime $p > m$ with*

$$g(p) \geq 2m \geq Bg(p^m). \tag{13.8}$$

This will be proved below. Now choose a sequence of primes recursively as follows. Let $p_0 \geq \max\{12, C\}$ be a prime such that $g(p_0) \geq 12$. Having chosen $p_0, \ldots, p_{k-1}$, put $l_i = 1 + p_i$ for $i < k$ and let $m = 6m_k$ where m_k is given by (13.5) above. Then take $p_k = p$ where $p > m$ is a prime satisfying (13.8). Thus

$$g(p_k) \geq 12m_k \geq Bg(p_k^{6m_k}) \tag{13.9}$$

for every $k \geq 1$. Now let

$$T_k = \mathrm{PSL}_2(\mathbb{F}_{p_k}).$$

Then T_k has rank 2, $\mu_k = 1 + p_k = l_k$, and

$$p_k^2 < \tau_k = p_k(p_k^2 - 1)/2 < |A_k|^3 < \mu_k^3,$$

where A_k is a subgroup of order p_k ($\leadsto$ **Finite simple groups**). Thus conditions (i) – (iv) are satisfied with $t = 3$ and $r = 2$. (We could use $X(\mathbb{F}_{p_k^e})$ instead of $\mathrm{PSL}_2(\mathbb{F}_{p_k})$, for any fixed Lie type X and any constant e, by suitably adjusting the parameters in the following proofs.)

Theorem 13.3.4 *If (T_k), (l_k) are as above then the profinite group $W((\underline{T}), (\underline{l}))$ has subgroup growth type $n^{g(n)}$.*

Proof. Let $n = p_k^{6m_k}$,where $k \geq 1$. Then $n > \tau_k^{2m_k} = n'$, say, so according to Lemma 13.3.2, we have

$$s_n(W) \geq n'^{m_k/24} > p_k^{m_k^2/6} = n^{m_k/36}.$$

Now (13.9) gives $m_k \geq Bg(n)/12$, so taking $c = B/(12 \times 36)$ we have

$$s_n(W) \geq n^{cg(n)}.$$

Thus the growth type of W is not less than $n^{g(n)}$.

For the upper bound, let $n > p_0$. There exists k such that $\mu_k \leq n < \mu_{k+1}$, and then Lemma 13.3.1 gives

$$s_n(W) \leq n^{12m_k}.$$

But

$$12m_k \leq g(p_k) \leq g(n)$$

by (13.9), since $p_k < \mu_k \leq n$ and g is non-decreasing. Thus $s_n(W) \leq n^{g(n)}$ for all large n. ■

The condition (13.7) on g excludes some perfectly nice functions such as $(\log n)^\varepsilon$ with $0 < \varepsilon < 1$, and it is worth mentioning two variations of the above construction, that allow for a wider range of growth types but for which we have less precise information.

Variation 1 Let g be any unbounded function. Then the sequence of primes (p_k) can be chosen so that $s_n(W) \leq n^{g(n)}$ for all large n, while W does not have polynomial subgroup growth. The proof is similar but simpler: it suffices to ensure that $p_k \geq p_{k-1}^{6m_{k-1}}$ and $g(p_k) \geq 72m_k^2$ for each $k \geq 1$.

Variation 2 Let h be a positive integer, put $g(n) = (\log n)^{1/h}$ and $g^*(n) = (\log n)^{1/(h+1)}$. Then the sequence of primes (p_k) can be chosen so that

$$s_n(W) \leq n^{g(n)} \text{ for all large } n,$$
$$s_n(W) \geq n^{cg^*(n)} \text{ for infinitely many } n,$$

where c is a positive constant. Again the proof is similar: it suffices to ensure that

$$(12m_k)^h \leq \log p_k \leq 2 \cdot (12m_k)^h$$

for each $k \geq 1$. The details are left to the reader.

Before proving Lemma 13.3.3, let us establish

Lemma 13.3.5 *If $g(x^{\log x}) = O(g(x))$ then $g(x) = O((\log\log x)^k)$ for some k.*

Proof. Suppose that $g(x^{\log x}) \leq Ag(x)$ for all $x \geq x_0$, where $x_0 \geq 4$ and $A > 1$. Put $k = \log A$, $N_0 = 1 + x_0^{\log x_0}$ and let

$$B = \sup\left\{ \frac{g(x)}{(\log\log x)^k} \mid x \in [x_0, N_0] \right\}.$$

We claim that then $g(x) \leq B(\log\log x)^k$ for all $x \geq x_0$. Indeed, suppose that this holds for all $x \in [x_0, N]$ where $N \geq N_0$. Let $y \in [N, N^{\log N}]$. Then $y = x^{\log x}$ where $x \in [x_0, N]$, and

$$\begin{aligned} g(y) = g(x^{\log x}) &\leq 2^k g(x) \\ &\leq 2^k B(\log\log x)^k = B(\log\log y)^k. \end{aligned}$$

The claim follows since $N^{\log N} > N^2$. ■

Proof of Lemma 13.3.3. Recall that g is an unbounded, non-decreasing positive real-valued function that satisfies (13.7). Let m be a large positive integer and let n be the least positive integer such that $g(n) \geq 2m$. There exists a prime p with $n \leq p < 2n$ ('Bertrand's postulate', ↬ **Prime numbers**). Then

$$g(p) \geq g(n) \geq 2m.$$

Since $g(x) = o(\log x)$ by the preceding lemma, this implies also that $p > \log p > g(p) > m$ provided m is large enough. Then

$$g(p^m) \leq g(p^{\log p}) \leq Ag(p).$$

Finally,

$$g(p) \leq g(2n) \leq Ag(n-1) < 2Am$$

provided $2n \leq (n-1)^{\log(n-1)}$, which holds if $m \geq 10$ since $2n > p > m$.

Thus provided m is large enough we obtain (13.8) with $B = A^{-1}$, and the lemma is proved.

Note that we never specified the group extensions in the construction of W from the sequence of groups (T_k); for example, W could simply be the product of all the groups $T_k^{(m_k)}$. However, such a group would not be finitely generated (as a profinite group). A more interesting example is the following: noting that each T_k has a natural doubly-transitive permutation representation of degree l_k, on the points of the projective line over $\mathbb{F}_{p_k}$ (or equivalently, on the right cosets of a maximal subgroup of index l_k), we form the groups W_k as a sequence of iterated *permutational wreath products*. That is, $W_1 = T_0$, a permutation group of degree $l_0 = m_1$; having obtained W_i for $i \leq k$ as a permutation group of degree m_i, we take

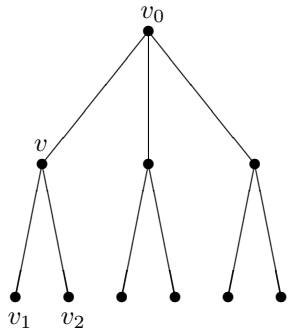
$$W_{k+1} = T_k \wr W_k$$

to be the permutational wreath product of T_k with W_k. This is the semi-direct product of $B_k = T_k^{(m_k)}$ by W_k, which acts by permuting the m_k direct factors, and W_{k+1} has a natural faithful imprimitive permutation representation of degree $l_k \cdot m_k = m_{k+1}$.

The inverse limit W of these iterated wreath products turns out to be a finitely generated profinite group; indeed, we shall see in the next section that W is the profinite completion of a finitely generated (abstract) group.

13.4 Automorphisms of rooted trees

A *rooted tree* is a tree $\mathfrak{T}$ with a distinguished vertex v_0, the root. A vertex of $\mathfrak{T}$ is said to have *level* n if n is the distance from v_0 to v, that is, the length of the unique path from v_0 to v. We consider an infinite *spherically homogeneous* rooted tree $\mathfrak{T}$, that is one where for each $n \geq 1$, all vertices of level n have the same (finite) valency $l_n + 1$. In this case we say that $\mathfrak{T}$ is of type $(l_n)_{n \geq 0}$, where l_0 is the valency of v_0. Thus if v is a vertex of level $n \geq 1$ then a unique edge e leads out of v towards v_0 (upwards, let us say), and the component of $\mathfrak{T} \setminus \{e\}$ not containing v_0 is a spherically homogeneous rooted tree of type $(l_k)_{k \geq n}$ having v as its root. This subtree is denoted $\mathfrak{T}_v$. We picture $\mathfrak{T}$ as growing downwards ('a peculiarity of the Northern hemisphere' according to M. F. Newman), and embedded in the plane; this fixes an ordering (left to right, say) on the vertices of each level.



$\mathfrak{T}[2]$

We denote by $\mathfrak{T}[n]$ the finite rooted subtree containing of all the vertices of level at most n.

Let $\Omega(n)$ denote the set of all vertices of level n; thus $\Omega(n)$ is the 'bottom layer' of $\mathfrak{T}[n]$, and each automorphism of $\mathfrak{T}[n]$ is determined by the permutation it induces on $\Omega(n)$; we use this to identify $\mathrm{Aut}(\mathfrak{T}[n])$ with a subgroup of $\mathrm{Sym}(\Omega(n))$. We may identify $\Omega(n+1)$ with the set $\{1,\dots,l_n\}\times\Omega(n)$. Having done this, we see that $\mathrm{Aut}(\mathfrak{T}[n+1])$ is precisely the permutational wreath product

$$\mathrm{Sym}(l_n)\wr\mathrm{Aut}(\mathfrak{T}[n]).$$

Starting with $\mathrm{Aut}(\mathfrak{T}[1])=\mathrm{Sym}(l_0)$ we deduce that for each $n\geq 1$,

$$\mathrm{Aut}(\mathfrak{T}[n])=\mathrm{Sym}(l_{n-1})\wr\mathrm{Sym}(l_{n-2})\wr\dots\wr\mathrm{Sym}(l_0).$$

(Another way to see this is to observe that $\mathrm{Aut}(\mathfrak{T}[n])$ consists of all permutations of $\Omega(n)$ that respect the sequence of equivalence relations

$$d(v,w)\leq 2r$$

for $r=1,\dots,n-1$, where d denotes the distance between two vertices.)

Finally, since each automorphism of $\mathfrak{T}$ is determined by a sequence of compatible automorphisms of the subtrees $\mathfrak{T}[n]$, we have

$$\mathrm{Aut}(\mathfrak{T})=\varprojlim_{n\to\infty}\mathrm{Aut}(\mathfrak{T}[n])=\varprojlim_{n\to\infty}\left(\mathrm{Sym}(l_{n-1})\wr\mathrm{Sym}(l_{n-2})\wr\dots\wr\mathrm{Sym}(l_0)\right)$$

We write $\pi_n:\mathrm{Aut}(\mathfrak{T})\to\mathrm{Aut}(\mathfrak{T}[n])\leq\mathrm{Sym}(\Omega(n))$ to denote the restriction mapping.

Suppose that for each $n\geq 0$ we have a subgroup $T_n\leq\mathrm{Sym}(l_n)$. Then

$$W_n=T_{n-1}\wr T_{n-2}\wr\dots\wr T_0\leq\mathrm{Aut}(\mathfrak{T}[n]),\tag{13.10}$$

and the profinite group

$$W=W((\underline{T}),(\underline{l}))=\varprojlim_{n\to\infty}W_n\tag{13.11}$$

is naturally embedded in $\mathrm{Aut}(\mathfrak{T})$.

For a subgroup Γ of W, let $\mathrm{st}_\Gamma(n)$ denote the pointwise stabilizer in Γ of $\Omega(n)$; this is the kernel of the restriction map $(\pi_n)_{|\Gamma}$. We say that Γ has the *congruence subgroup property* if every subgroup of finite index in Γ contains $\mathrm{st}_\Gamma(n)$ for some n, and that Γ is *dense* in W if

$$\pi_n(\Gamma) = W_n$$

for every n, that is if Γ is dense in the natural profinite topology of W. The following is now clear, since the subgroups $\mathrm{st}_\Gamma(n)$ form a base for the neighourhoods of 1 in Γ relative to the topology induced from the natural topology of W:

Lemma 13.4.1 *Let $\iota : \widehat{\Gamma} \to W$ be the map induced by the inclusion $\Gamma \to W$. Then ι is surjective if and only if Γ is dense in W, and ι is injective if and only if Γ has the congruence subgroup property.*

We need some notation for tree automorphisms.

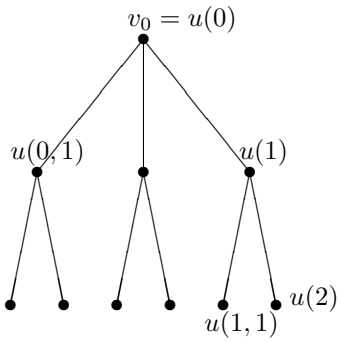
$$g = (g_1, \ldots, g_m)_n$$

indicates that $g \in \mathrm{st}_{\mathrm{Aut}(\mathfrak{T})}(n)$ and that g_i is the restriction of g to the subtree $\mathfrak{T}_{v_i}$, where v_i is the ith vertex in $\Omega(n)$ (in our chosen order, reading from left to right); here $m = |\Omega(n)|$. For any $\alpha \in \mathrm{Sym}(l_n)$ and any vertex $v \in \Omega(n)$, we write $\dot{\alpha}$ to denote the automorphism of $\mathfrak{T}_v$ that induces α on the vertices of level 1 in $\mathfrak{T}_v$ and preserves the ordering of vertices within all the subtrees $\mathfrak{T}_w$ for vertices $w \neq v$ of $\mathfrak{T}_v$; in other words, $\dot{\alpha}$ corresponds to $\alpha \in \mathrm{Sym}(l_n)$ when $\mathrm{Aut}(\mathfrak{T}_v)$ is identified with $\ldots \wr \mathrm{Sym}(l_{n+1}) \wr \mathrm{Sym}(l_n)$; we say that $\dot{\alpha}$ is *rooted at* v. For example, taking $n = 0$, we can write any automorphism g of $\mathfrak{T}$ as

$$g = (h_1, \ldots, h_{l_0})_1 \cdot \dot{\alpha}$$

where $h_i \in \mathrm{Aut}(\mathfrak{T}_{v_i})$ and $\alpha \in \mathrm{Sym}(l_0)$ is the action of g on $\Omega(1) = \{v_1, \ldots, v_{l_0}\}$.

For each $n \geq 1$, let $u(n)$ denote the rightmost vertex of level n in $\mathfrak{T}$ and $u(n, 1)$ the leftmost vertex immediately below $u(n)$ (that is, the vertex $l_{n+1} - 1$ steps to the left of the rightmost vertex in $\Omega(n + 1)$).



Now let us get down to specifics. Let $P = \langle x, y \rangle$ be a two-generator perfect group, and suppose that for each $n \geq 0$ we have an epimorphism

$$\phi_n : P \to T_n,$$

where T_n is a doubly-transitive subgroup of $\mathrm{Sym}(l_n)$. Write $\alpha_n = \phi_n(x)$ and $\beta_n = \phi_n(y)$. We now define four automorphisms of $\mathfrak{T}$.

$$\begin{aligned} \xi &= \dot{\alpha}_0 \ \text{ rooted at } v_0 \\ \eta &= \dot{\beta}_0 \ \text{ rooted at } v_0 \\ a \ &\text{ and } \ b \end{aligned}$$

where a acts on each of the disjoint subtrees $\mathfrak{T}_{u(n,1)}$ for $n \geq 0$ by $\dot{\alpha}_{n+1}$ rooted at $u(n,1)$, and b acts likewise with $\dot{\beta}_{n+1}$ in place of $\dot{\alpha}_{n+1}$.

Theorem 13.4.2 *The group $\Gamma = \langle \xi, \eta, a, b \rangle$ is a dense subgroup of W (defined by (13.11) and (13.10)) and Γ has the congruence subgroup property.*

Before proving this, let us complete the proof of Theorem 13.1. Given a function g that satisfies condition $(*)_2$, Theorem 13.3.4 asserts that we can choose a sequence of primes (p_k) so that the profinite group $W = W((\underline{T}), (\underline{l}))$ has subgroup growth type $n^{g(n)}$, where $l_k = 1 + p_k$ and $T_k = \mathrm{PSL}_2(\mathbb{F}_{p_k})$. Now $p_k \geq 5$ for each k, so T_k is a quotient of the group $P = \mathrm{SL}_2(\mathbb{Z}[\frac{1}{6}])$. Moreover, P is generated by the two matrices

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{6} \\ 0 & 1 \end{pmatrix},$$

and P is a perfect group [Bass 1964]. Also the natural action of T_k on the l_k points of the projective line over $\mathbb{F}_{p_k}$ is doubly transitive. Now Theorem 13.4.2 provides a 4-generator subgroup Γ of W, which by Lemma 16.4.1 satisfies $\widehat{\Gamma} \cong W$.

Thus $s_n(\Gamma) = s_n(W)$ for all n and Γ has growth type $n^{g(n)}$, as required. The same applies if g is a function of the type mentioned in *Variation 1* or *Variation 2* in the preceding section.

Theorem 13.4.2 depends on two key facts. One of them is a weak form of the congruence subgroup property that holds in great generality. Here, for any subgroup G of $\mathrm{Aut}(\mathfrak{T})$ we denote by $\mathrm{rst}_G(v)$ the *pointwise stabilizer* in G of $\mathfrak{T} \setminus \mathfrak{T}_v$.

Lemma 13.4.3 *Let G be a subgroup of $\mathrm{Aut}(\mathfrak{T})$ that acts transitively on each $\Omega(n)$. If N is a subgroup of finite index in G then there exists n such that $N \geq \mathrm{rst}_G(v)'$ for every vertex v of level n.*

Proof. We may assume that $N \lhd G$. Then G/N contains only a finite number, say k, of distinct subgroups. Let n be so large that $|\Omega(n)| > k$; since $|\Omega(j)| \geq 2\,|\Omega(j-1)|$ for each j we could take any $n > \log k$. Then there exist distinct vertices $u, w \in \Omega(n)$ such that $N\mathrm{rst}_G(u) = N\mathrm{rst}_G(w)$. Since $\mathrm{rst}_G(u)$ and $\mathrm{rst}_G(w)$ have disjoint supports in $\mathfrak{T}$, they commute elementwise. Consequently

$$\begin{aligned}\mathrm{rst}_G(w)' \leq [N\mathrm{rst}_G(w), N\mathrm{rst}_G(w)] &= [N\mathrm{rst}_G(u), N\mathrm{rst}_G(w)] \\ &\leq N[\mathrm{rst}_G(u), \mathrm{rst}_G(w)] = N.\end{aligned}$$

The result follows since $\mathrm{rst}_G(v)'$ is conjugate in G to $\mathrm{rst}_G(w)'$ for each $v \in \Omega(n)$, because G acts transitively on $\Omega(n)$. ■

The second key fact is a structural property of the group Γ, expressed in the next lemma. In order to state it, we need to define a series of groups as follows. Consider a vertex v of level m. The tree $\mathfrak{T}_v$ is a spherically homogeneous rooted tree of type $(l_n)_{n \geq m}$, and we now define $\Gamma(\mathfrak{T}_v) \leq \mathrm{Aut}(\mathfrak{T}_v)$ in the same way that we defined $\Gamma \leq \mathrm{Aut}(\mathfrak{T})$ but using α_{n+m} and β_{n+m} in place of α_n and β_n, for each n.

Lemma 13.4.4 *Let $n \geq 1$. Then (i)*

$$\mathrm{st}_\Gamma(n) = \prod_{v \in \Omega(n)} \mathrm{rst}_\Gamma(v),$$

and (ii) for each $v \in \Omega(n)$, the group of automorphisms of $\mathfrak{T}_v$ induced by the action of $\mathrm{rst}_\Gamma(v)$ is precisely $\Gamma(\mathfrak{T}_v)$.

Proof. Suppose we can prove this for $n = 1$. The argument can then be repeated with $\Gamma(\mathfrak{T}_v)$ in place of Γ and the result will follow for every n. So we assume that $n = 1$.

Say $\Omega(1) = \{v_1, \ldots, v_l\}$ where $l = l_0$, and denote the restriction of $\mathrm{rst}_\Gamma(v_i)$ to $\mathfrak{T}_{v_i}$ by Δ_i. Write $\Gamma(i) = \Gamma(\mathfrak{T}_{v_i})$.

Now Γ contains $\langle \xi, \eta \rangle = \dot{T}_0$ which permutes $\Omega(1)$ transitively. If $\sigma \in T_0$ sends l to i then $\dot{\sigma}$ induces an isomorphism between the trees $\mathfrak{T}_{v_l}$ and $\mathfrak{T}_{v_i}$ that

preserves the ordering of vertices, and hence sends $\Gamma(l)$ to $\Gamma(i)$ as well as sending Δ_l to Δ_i. Let us call this 'property $*$'.

By definition, $\Gamma(l)$ is generated by $\xi(1) = \dot{\alpha}_1$ and $\eta(1) = \dot{\beta}_1$, rooted at $v_l = u(1)$, together with $a(1)$ and $b(1)$, where $a(1)$ and $b(1)$ denote the restrictions of a and of b to the tree $\mathfrak{T}_{v_l}$.

Since a and b fix all vertices of level 1 , we have

$$\mathrm{rst}_\Gamma(v_l) \leq \mathrm{st}_\Gamma(1) = \langle a, b\rangle^{\dot{T}_0} (\mathrm{st}_\Gamma(1) \cap \dot{T}_0) = \langle a, b\rangle^{\dot{T}_0},$$

because $\dot{T}_0$ acts faithfully on $\Omega(1)$. Now let $\sigma \in T_0$. If σ fixes l then $a^{\dot{\sigma}}$ acts as $a(1)$ on $\mathfrak{T}_{v_l}$. If σ sends 1 to l then $a^{\dot{\sigma}}$ acts on $\mathfrak{T}_{v_l}$ as $\xi(1)$; in every other case $a^{\dot{\sigma}}$ acts as the identity on $\mathfrak{T}_{v_l}$. Similar conclusions apply to $b^{\dot{\sigma}}$, and it follows that the group of automorphisms induced on $\mathfrak{T}_{v_l}$ by $\mathrm{st}_\Gamma(1)$ is precisely $\Gamma(l)$. In view of property $*$, this implies that $\mathrm{st}_\Gamma(1)$ induces the group $\Gamma(i)$ on $\mathfrak{T}_{v_i}$ for each i, so we have

$$\mathrm{st}_\Gamma(1) \subseteq (\Gamma(1), \ldots, \Gamma(l))_1 . \tag{13.12}$$

Now let $\sigma = w(\alpha_1, \beta_1)$ and $\tau = w'(\alpha_1, \beta_1)$ be elements of T_1, where w, w' are words. Put $h = w(a, b)$ and $h' = w'(a, b)$. Then

$$h = (\dot{\sigma}, 1, \ldots, 1, *)_1, \ h' = (\dot{\tau}, 1, \ldots, 1, *)_1$$

where the ... represent identity automorphisms and the $*$s some automorphisms of $\mathfrak{T}_{v_l}$. Since T_0 is doubly transitive it contains an element ρ that fixes 1 and moves l. Then

$$h^{\dot{\rho}} = (\dot{\sigma}, 1, \ldots, *, \ldots, 1)_1$$

and then

$$[h^{\dot{\rho}}, h'] = ([\dot{\sigma}, \dot{\tau}], 1, \ldots, 1)_1,$$
$$[h^{\dot{\rho}}, h']^{\dot{\mu}} = (1, \ldots, 1, [\dot{\sigma}, \dot{\tau}])_1 = g, \ \text{say}$$

where $\mu \in T_0$ sends 1 to l. Evidently $g \in \mathrm{rst}_\Gamma(v_l)$, and this shows that $[\sigma, \tau]^{\cdot} \in \Delta_l$. As T_1 is a perfect group it follows that Δ_l contains the whole of $\dot{T}_1$, in particular both $\xi(1)$ and $\eta(1)$.

This argument also shows that Γ contains the element $(\dot{\alpha}_1, 1, \ldots, 1)_1$. Therefore

$$((\dot{\alpha}_1, 1, \ldots, 1)_1)^{-1} \cdot a = (1, \ldots, 1, a(1))_1 \in \mathrm{rst}_\Gamma(v_l)$$

and so $a(1) \in \Delta_l$. Similarly $b(1) \in \Delta_l$, and it follows that $\Delta_l \geq \Gamma(l)$. Using property $*$ we deduce that $\Delta_i \geq \Gamma(i)$ for each i. With (13.12) this gives

$$\mathrm{rst}_\Gamma(v_i) \leq \mathrm{st}_\Gamma(1) \subseteq (\Gamma(1), \ldots, \Gamma(l))_1 \subseteq (\Delta_1, \ldots, \Delta_l)_1 .$$

This implies both (i) and (ii). ■

Proof of Theorem 13.4.2 We have to show that $\Gamma \leq W$ and that $\pi_n(\Gamma) = W_n$ for each n. In fact the second claim implies the first, since W is the inverse limit of the W_n.

From the definition we see that Γ induces T_0 on $\Omega(1)$. Similarly, for a vertex v of level $n-1$, the group $\Gamma(\mathfrak{T}_v)$ induces T_{n-1} on the set of vertices of level 1 in the tree $\mathfrak{T}_v$. It follows by Lemma 13.4.4 that $\mathrm{st}_\Gamma(n)$ induces $T_{n-1} \times \cdots \times T_{n-1}$ on $\Omega(n)$, acting as the base group of W_n. Supposing inductively that $\pi_{n-1}(\Gamma) = W_{n-1}$ we may infer that

$$\pi_n(\Gamma) = T_{n-1} \wr W_{n-1} = W_n.$$

We also have to establish that Γ has congruence subgroup property. Let N be a subgroup of finite index in Γ. Since each T_j is transitive, $\pi_n(\Gamma) = W_n$ is transitive on $\Omega(n)$ for each n. We may therefore apply Lemma 13.4.3 to deduce that there exists n such that $N \geq \mathrm{rst}_\Gamma(v)'$ for every $v \in \Omega(n)$. Now we claim that each of the groups $\mathrm{rst}_\Gamma(v)$ is *perfect*; this will be proved below. Given the claim, it follows by Lemma 13.4.4(i) that

$$N \geq \prod_{v \in \Omega(n)} \mathrm{rst}_\Gamma(v) = \mathrm{st}_\Gamma(n),$$

which is what we had to prove.

It remains to show that $\mathrm{rst}_\Gamma(v)$ is perfect. Now Lemma 13.4.4(ii) shows that $\mathrm{rst}_\Gamma(v) \cong \Gamma(\mathfrak{T}_v)$. As the latter group is defined in just the same way as Γ, it will suffice to show that Γ itself is perfect. Recall that $P = \langle x, y \rangle$ is a perfect group and that $\Gamma = \langle \xi, \eta, a, b \rangle$. Here $\langle \xi, \eta \rangle = \dot{T}_0 \cong T_0 = \phi_0(P)$, while a and b act on each of the disjoint subtrees $\mathfrak{T}_{u(n,1)}$ as $\dot{\alpha}_{n+1}$ and $\dot{\beta}_{n+1}$ respectively, where $\alpha_{n+1} = \phi_{n+1}(x)$ and $\beta_{n+1} = \phi_{n+1}(y)$. It follows that any relation satisfied by x and y in P is satisfied by each of the pairs $\alpha_{n+1}, \beta_{n+1}$ and hence by a and b, so

$$x \mapsto a,\ y \mapsto b$$

defines an epimorphism from P onto $\langle a, b \rangle$. Thus Γ is generated by two images of the perfect group P and hence is perfect as claimed.

This completes the proof.

Remarks (i) Similar results may be obtained under more general hypotheses. For example, it is not necessary to asume that the permutation groups T_n are doubly transitive: it suffices to assume that each one is transitive. Using this, one can obtain a finitely generated group whose profinite completion is the iterated wreath product of any sequence of non-abelian finite simple groups. It is also not hard to show that groups like Γ are *just-infinite*, that is, every non-identity normal subgroup has finite index. For all this, see [Segal 2001] (it is assumed in that paper that the groups T_n are not only transitive but have distinct point-stabilizers: this hypothesis can be removed with a little extra argument).

(ii) In particular, the proof of Theorem 5 in [Segal 2001] shows that there is a 5-generator group Γ such that $\widehat{\Gamma} \cong W = \varprojlim W_n$ where

$$W_n = \mathrm{Alt}(n+5) \wr \ldots \wr \mathrm{Alt}(6) \wr \mathrm{Alt}(5).$$

It is easy to see that the only open normal subgroups of W are the 'level stabilizers' $\ker(W \to W_n)$, and hence that for each m,

$$s_m^{\triangleleft}(W) < \log m.$$

It follows by Theorem 11.5 that W, and hence also Γ, has *polynomial maximal subgroup growth*. Thus the sufficient condition for PMSG given in Theorem 3.5(i) is not necessary, either in profinite groups or in finitely generated abstract groups.

Notes

The construction of §§13.1 and 13.2 is due to **L. Pyber** (personal communication); it will appear in [**Pyber(b)**].

Finitely generated dense subgroups in infinite products of (pairwise non-isomorphic) alternating groups were constructed by [**Neumann 1937**], to give continuously many non-isomorphic finitely generated groups. Using a variant of Neumann's construction, [**Lubotzky, Pyber & Shalev 1996**] obtained examples of finitely generated groups with the slowest then known non-polynomial subgroup growth, of type $n^{\log n/(\log\log n)^2}$; an analogous construction using finite special linear groups instead of alternating groups provided examples with growth type $n^{\log n/\log\log n}$. In order to obtain a continuum of distinct growth types, Pyber had (a) to generalize Neumann's approach by allowing each of the alternating groups to appear several times in the product, and (b) determine the subgroup growth of what we have called 'standard subgroups' of $\mathrm{Sym}(\Omega)$; for this he had to establish an interesting new result on finite permutation groups, Theorem 13.1.2.

The construction of §§13.3 and 13.4 is from [**Segal 2001**]. Possible variations are discussed in [**Segal (a)**].

Groups generated by 'rooted' and 'directed' automorphisms of rooted trees were studied in a series of papers by R. I. Grigorchuk and others, see [**Grigorchuk 2000**]; it was the study of this article (in his role as an editor of the book [**NH**] in which it appears) that inspired the author of [**Segal 2001**]; in particular this article gives sufficient conditions for such groups to have the 'congruence subgroup property'.

The groups of Grigorchuk are mostly prosoluble. Iterated wreath products of finite simple groups were studied by [**Neumann 1986**] and [**Bhattacharjee 1994**], using permutation-group methods. The simple proof of the 'congruence subgroup property' given in §13.4 is taken from the former paper. In the latter,

Bhattacharjee showed that iterated wreath products of finite simple alternating groups are (positively) finitely generated.

The spectrum of $\alpha(G)$ – the 'degree of polynomial subgroup growth' – is discussed in [**Shalev 1999**$_a$], though he concentrates mainly on the slightly different invariant

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

Shalev proves that $\deg(G)$ never takes values in the interval $(1, 3/2)$, and states that $\alpha(G)$ never lies in the interval $(1, 2)$. It is unknown whether further 'gaps' of this kind exist.

[**du Sautoy & Grunewald 2000**] prove that $\alpha(G)$ is a rational number if G is a finitely generated nilpotent group; see Chapter 15 below.

Chapter 14

Explicit formulas and asymptotics

So far we have concentrated mainly on subgroup growth type, a rough-and-ready estimate for the rate of growth of $a_n(G)$. In the last three chapters of the book, we take a closer look at the numbers $a_n(G)$ themselves. Of course, the detailed arithmetical and asymptotic properties of this sequence will depend on the nature of the groups G under consideration, as will the methods appropriate to studying them.

In this chapter we focus on some classes of virtually free groups and on surface groups. Of course, (almost) all these groups have subgroup growth of type $n!$, but we will look at explicit formulas for the numbers $a_n(G)$, their congruence behaviour modulo primes, and asymptotic estimates.

Already, these examples lead to a rich and interesting theory. We cannot in this chapter go into this theory in depth: rather, we shall indicate some of the highlights, and say a little about the kind of methods used to prove them. The forthcoming survey article [Müller (e)] presents a comprehensive account of current knowledge on 'modular subgroup arithmetic'.

14.1 Free groups and the modular group

Let us begin by recalling the recursive formula for the number of subgroups of index n in the free group F_d on d generators:

Theorem 14.1.1

$$a_n(F_d) = n \cdot (n!)^{d-1} - \sum_{k=1}^{n-1} (n-k)!^{d-1} a_k(F_d).$$

This formula is due to Marshall Hall, whose paper [Hall 1949] can be probably considered as the birth of the subject of subgroup growth. We deduced it in

Chapter 2 from some simple combinatorial observations presented in Chapter 1, §1.1. As these will be fundamental for most of what follows we restate them here, and take the opportunity to fix some notation.

- $h_n(G) = |\mathrm{Hom}(G, \mathrm{Sym}(n))|$.
- $t_n(G)$ denotes the number of homomorphisms from G into $\mathrm{Sym}(n)$ having transitive image.
- The cyclic group of order r is denoted C_r.

Proposition 14.1.2 *Let G be a group. Then*

$$a_n(G) = \frac{t_n(G)}{(n-1)!} \tag{14.1}$$

$$= \frac{h_n(G)}{(n-1)!} - \sum_{k=1}^{n-1} \frac{h_{n-k}(G)}{(n-k)!} a_k(G). \tag{14.2}$$

If $G = G_1 * G_2 * \ldots * G_d$ is a free product, then of course $h_n(G) = \prod_{i=1}^{d} h_n(G_i)$. Theorem 14.1.1 follows on taking $G_i = C_\infty$ for each i, so $h_n(G_i) = n!$ for each i. Another case of special interest is the *modular group* $\mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$. The sequences $h_n(C_2)$ and $h_n(C_3)$ satisfy recurrence relations, from which one can deduce a recurrence for $a_n(\mathrm{PSL}_2(\mathbb{Z}))$ of the following form:

Theorem 14.1.3 [Godsil, Imrich & Razen 1989] *Let $G = \mathrm{PSL}_2(\mathbb{Z})$. Then $a_1(G) = a_2(G) = 1$, $a_3(G) = 4$, $a_4(G) = 8$, $a_5(G) = 5$, $a_6(G) = 22$, and for each $n \geq 6$*

$$\begin{aligned}(n^4 - 2n^3 - n^2 + 3n + 1)a_{n+1}(G) = \\ (n^3 - 6n^2 + 5n + 1)a_n(G) + (n^3 - 3n^2 + 8n - 5)a_{n-1}(G) \\ + (3n^4 - 8n^3 + 8n - 8)a_{n-2}(G) + (2n^4 - 7n^3 + 10n^2 - gn + 2)a_{n-3}(G) \\ + 3(n^2 - 5n + 6)a_{n-4}(G) + (n^5 - 7n^4 - 11n^3 + 8n^2 - 1gn + 12)a_{n-5}(G).\end{aligned}$$

We remark that the existence of such a recursive formula for $a_n(G)$ is somewhat surprising: note that a subgroup of index n is not contained in any subgroup of index $n - i$ if $i < \frac{n}{2}$. It is probably rather a rare occurrence: for example, such a sequence cannot have growth type strictly between polynomial and exponential. It would be interesting to determine for what other kind of groups G the sequence $(a_n(G))$ can satisfy a recurrence relation with polynomial coefficients.

Anyway, it seems that the actual numbers $a_n(\mathrm{PSL}_2(\mathbb{Z}))$ have attracted considerable attention. Tables of values have been published by the American National Bureau of Standards [Newman 1976a]. For example

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

As for free groups, most permutation representations of $G = \mathrm{PSL}_2(\mathbb{Z})$ are transitive [Newman 1976b] and hence

$$t_n(G) \sim h_n(G),$$
$$a_n(G) \sim h_n(C_2)h_n(C_3)/(n-1)!$$

This may be combined with the following asymptotic estimates:

Proposition 14.1.4 [Moser & Wyman 1955] *For each prime p,*

$$h_n(C_p) \sim K_p \exp\left(\frac{p-1}{p} n(\ln n - 1) + n^{1/p}\right)$$

where

$$K_p = \begin{cases} p^{-1/2} & (p \neq 2) \\ 2^{-1/2}e^{-1/4} & (p = 2) \end{cases}.$$

Applying this for $p = 2$ and $p = 3$ [Newman 1976b] obtained

Proposition 14.1.5

$$a_n(\mathrm{PSL}_2(\mathbb{Z})) \sim \left(12\pi e^{1/2}\right)^{-1/2} \exp\left(\frac{n}{6}(\ln n - 1) + n^{1/2} + n^{1/3} + \frac{1}{2}\ln n\right).$$

Of course, once again we see that the growth of all subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ is much faster than that of the congruence subgroups (as described in Chapter 6).

14.2 Free products of finite groups

For a group G, let us write $b_0(G) = 1$ and for $n \geq 1$ set

$$b_n(G) = \frac{h_n(G)}{n!}.$$

Consider the formal power series

$$A(X) = A_G(X) = \sum_{n=1}^{\infty} a_n(G)X^n,$$
$$B(X) = B_G(X) = \sum_{n=0}^{\infty} b_n(G)X^n.$$

Now (14.2) reads

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

which is equivalent to the formal power series identity

$$XB'(X) = A(X)B(X).$$

Thus

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

(where of course log here denotes the usual formal series inverse to exp), and we can restate this as

Proposition 14.2.1

$$B(X) = \exp\int \frac{A(X)}{X}dX$$

This simple observation is the starting point of a deep theory, developed by Thomas Müller, which extends the results of Section 1 to more general free products of finite groups; all groups of that kind are virtually free.

Let's see for a moment what Proposition 14.2.1 says for the trivial group $G = \{1\}$. Now $a_1(G) = 1$ and $a_n(G) = 0$ for $n > 1$, while $h_n(G) = 1$ for every n, so $b_n(G) = 1/n!$. Thus in this case the proposition reads

$$\sum \frac{1}{n!}X^n = \exp\int \frac{X}{X}dX = \exp X.$$

Stirling's well-known formula asserts

$$n! \sim (2\pi)^{1/2}n^{n+1/2}e^{-n} \qquad \text{as} \quad n \to \infty.$$

For a more interesting example, let $G = C_p$ be a cyclic group of prime order p. Then $A(X) = X + X^p$. Note also that in general $\int(A(X)/X)dX = \sum_{n=1}^{\infty}\frac{a_n(G)}{n}X^n$ and so in this case $B(X) = \exp\left(X + \frac{1}{p}X^p\right)$. Now for each n,

$$b_n(G) = \frac{1 + \tau_p(n)}{n!}$$

where $\tau_p(n)$ denotes the number of elements of order p in $\mathrm{Sym}(n)$, and so we have

Proposition 14.2.2

$$\sum_{n=1}^{\infty}\frac{1 + \tau_p(n)}{n!}X^n = \exp\left(X + \frac{1}{p}X^p\right).$$

This lovely proposition is of independent combinatorial interest, and results of this type have been proved by direct methods in several places (see the *Notes).* Since $h_n(C_p) = 1 + \tau_p(n)$, we can now see Proposition 14.1.4 as an analogue of the Stirling formula.

Now let G be any group of finite order m. Putting

$$P(X) = P_G(X) = \sum_{d|m}\frac{a_d(G)}{d}X^d = \sum_{i=1}^{m}c_iX^i$$

we have

$$B_G(X) = 1 + \sum_{n=1}^{\infty} \frac{h_n(G)}{n!} X^n = \exp(P(X)).$$

The coefficients of $P(X)$ satisfy $c_1 \neq 0$ and $c_i = 0$ for $m/2 < i < m$. [Müller 1997], using methods of complex analysis, developed machinery which gives a detailed asymptotic expansion for $\exp(P(X))$ for such polynomials P. In this way he obtained an asymptotic expansion of $h_n(G) = |\mathrm{Hom}(G, S_n)|$ for every finite group G. Here is a corollary of his work:

Theorem 14.2.3 *Let G be a finite group of order m. Then*

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

where

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

Along the way Müller deduced the following curious phenomenon: if for two finite groups G and H we have $h_n(G) \sim h_n(H)$ as $n \to \infty$ then the two sequences must coincide. It is not difficult to show that there exist non-isomorphic groups for which the two sequences coincide. According to Proposition 14.1.2, it suffices to find G and H for which $a_k(H) = a_k(G)$ for every k. Examples of such pairs can be found in [Schmidt 1994], §5.6 (these examples have isomorphic subgroup lattices; in the case of p-groups G and H, this actually implies that $a_k(H) = a_k(G)$ for every k). Some pairs of infinite groups with this property will appear in Section 14.4 below.

We can now move in the other direction and apply the last theorem to counting subgroups in some infinite groups. Using the fact that h_n is multiplicative on free products, [Müller 1996] deduced

Theorem 14.2.4 *Let $G = G_1 * \cdots * G_s$ the free product of s finite groups of orders $m_1, \ldots, m_s$ respectively, where if $s = 2$ they are not both of order two. Then*

$$a_n(G) \sim L_G \Phi_G(n) \qquad (n \to \infty)$$

where

$$L_G = (2\pi m_1 \ldots m_s)^{-1/2} \exp\left(-\sum_{2|m_i} \frac{(a_{m/2}(G_i))^2}{2m_i} \right)$$

and

$$\Phi_G(n) = n^{-\chi(G)n} \exp\left(\chi(G)n + \sum_{i=1}^{s} \sum_{\substack{d|m_i \\ d<m_i}} \frac{a_d(G_i)}{d} n^{d/m_i} + \frac{1}{2} \ln n \right).$$

Here

$$\chi(G) = \frac{1-(m_1-1)\cdot\cdots\cdot(m_s-1)}{m_1\cdot\cdots\cdot m_s}$$

is the *Euler characteristic* of G.

Note that Proposition 14.1.4 is a very special case of Theorem 14.2.3 and Proposition 14.1.5 is a special case of Theorem 14.2.4. In fact, the full results of Müller are stronger even for the classical modular group, for which he showed:

$$a_n(\mathrm{PSL}_2(\mathbb{Z})) = (12\pi e^{1/2})^{-1/2} n^{n/6} \exp(1 + R(n) + O(n^{-4/3}))$$

where $R(n)$ is equal to

$$-n^{-1/6} - \frac{1}{6}n^{-1/3} - \frac{13}{24}n^{-1/2} - \frac{7}{36}n^{-2/3} + \frac{253}{240}n^{-5/6} - \frac{67963}{51840}n^{-1} - \frac{2449841}{362880}n^{-7/6}.$$

There has also been some interest in counting special subgroups of the modular group, for example the number of *free* subgroups of index n (these are precisely the torsion-free subgroups). More generally, every subgroup Δ of finite index in Γ is of the form $\underbrace{C_2 * \cdots * C_2}_{s} * \underbrace{C_3 * \cdots * C_3}_{t} * F_r$ where F_r is a free group on r generators. Say that Δ is of *type* (s,t,r) in this case. By comparing the Euler characteristics of the groups one can see that the index of a subgroup of type (s,t,r) is equal to $3s+4t+6(r-1)$, so for a given (s,t,r) there are only finitely many finite index subgroups of that type. The problem of determining the number of subgroups of a given type in $\mathrm{PSL}_2(\mathbb{Z})$ is discussed in [Müller (d)], where it is termed the *Poincaré problem*. More general results of this flavour are obtained in [Müller & Puchta (a)].

14.3 Modular Subgroup Arithmetic

Hall's recursive formula Theorem 14.1.1 easily implies by induction

Proposition 14.3.1 *$a_n(F_d)$ is odd for every d and every n.*

M. Grady and M. Newman have looked, more generally, at Hall's formula when taken modulo p. In each such case it becomes a linear recurrence relation of a fixed length with constant coefficients, and therefore defines a periodic sequence. For example for $d = 2$ and $p = 5$, the relation is

$$a_n \equiv 4a_{n-1} + 3a_{n-2} + 4a_{n-3} + a_{n-4} \pmod 5 \quad \text{for } n \geq 5$$

with initial values $a_1 \equiv 1$, $a_2 \equiv 3$, $a_3 \equiv 3$ and $a_4 \equiv 1$. The period of this sequence modulo 5 turns out to be 62. It is not at all clear for what kind of groups G the sequence $a_n(G)$ will be periodic modulo p, for every prime p or for some prime p. [Grady & Newman 1992] show that if G is the free product of at least two cyclic groups then $a_n(G)$ is periodic modulo p for every p; this paper has further results of a similar flavour.

Here is another suggestive observation. Since $x^{r+p-1} \equiv x^r \pmod{p}$ for every x, by Fermat's theorem, and $a_1(F_r) = 1$ for every r, it follows from Theorem 14.1.1 that

$$a_n(F_r) \equiv a_n(F_{r+p-1}) \pmod{p}$$

for every n. As $a_n(F_1) = 1$ for every n, we can deduce the following generalisation of Proposition 14.3.1:

Proposition 14.3.2 [Grady & Newman 1992] *Let p be a prime and suppose that $r \equiv 1 \pmod{p-1}$. Then*

$$a_n(F_r) \equiv 1 \pmod{p}$$

for all n.

Moving beyond free groups, we have

Theorem 14.3.3 [Stothers 1977] *$a_n(\mathrm{PSL}_2(\mathbb{Z}))$ is odd if and only if $n = 2^k - 3$ or $n = 2(2^k - 3)$ with $k \geq 2$.*

(This confirms a conjecture of C. R. Johnson.) Stothers's proof uses a different method. Put $\Gamma = \mathrm{PSL}_2(\mathbb{Z}) = \langle x, y \rangle$ where x has order 2 and y has order 3. To each subgroup H of index n in Γ one associates a directed graph whose vertices are the left cosets of H. A directed edge, coloured red, goes from u to v if $v = x \cdot u$, and a directed edge, coloured blue, goes from u to v if $v = y \cdot u$. Elements of Γ correspond to paths along the graph starting at H, and those which also end at H give the elements of H. The graph X so obtained has the following properties:

(a) each vertex has a blue loop, or is a vertex of precisely one blue triangle;

(b) each vertex has a red loop, or is an end of precisely one red edge;

(c) X is connected.

X has a distinguished vertex, the coset H, which we denote by 1. Two such directed coloured graphs satisfying (a), (b) and (c) are said to be *equivalent* if there is a colour-preserving isomorphism between them sending 1 to 1. It is not difficult to see that there is a one-to-one correspondence between the subgroups of index n in Γ and the equivalence classes of coloured graphs satisfying (a), (b) and (c). Thus questions about the number of subgroups are translated into problems of counting graphs.

A similar correspondence between finite-index subgroups and coloured graphs can in principle be established for every group with a given presentation. However, the problem of counting such graphs in general seems hopeless.

Following Stothers, other authors have studied the set

$$\pi(G) = \{n \in \mathbb{N} \mid a_n(G) \equiv 1 \pmod{2}\}.$$

As we have seen, $\pi(F_d) = \mathbb{N}$. [Grady & Newman 1992] showed that the same holds for the free product of at least four copies of any cyclic group.

[Müller (a)] studied $\pi(H_q)$ for the "Hecke groups" $H_q = C_2 * C_q$. Among other things he proved

Theorem 14.3.4 (i) *If q is even then $\pi(H_q) = \mathbb{N}$.*

(ii) *If q is odd then the following are equivalent:*

$$(a) : \pi(H_q) = \Lambda_q \cup 2\Lambda_q \quad \textit{where} \quad \Lambda_q = \left\{ \frac{2(q-1)^i - q}{q-2} \mid i \in \mathbb{N} \right\}$$

$$(b) : q \textit{ is a Fermat prime.}$$

(iii) *If q is odd and $q \geq 3$ then $\pi(H_q)$ is infinite.*

(iv) *If q_1 and q_2 are distinct odd integers ≥ 3 then $\pi(H_{q_1}) \neq \pi(H_{q_2})$.*

Note that (ii) is a far-reaching generalisation of Theorem 14.3.3. Altogether, the theorem gives a new characterisation of the Fermat primes!

Various other results and conjectures are given by the above mentioned authors, but it is difficult at this point to see the general picture. One of the difficulties is that (unlike most questions dealt in this book) divisibility properties of $a_n(G)$ can be severely affected when G is replaced by a commensurable group. [Müller (b)] has shown that if N is a normal subgroup of an arbitrary group G with G/N cyclic of order 2^r then

$$\pi(G) = 2^r \pi(N) \cup \bigcup_{\rho=0}^{r-1} 2^\rho \left(\pi(N) \cap (\mathbb{N} \setminus 2\mathbb{N}) \right).$$

He has also proved a result of similar flavour about the sets

$$\{ n \in \mathbb{N} \mid a_n(G) \equiv k \,(\mathrm{mod}\, p) \},$$

for arbitrary integers k and primes p, and used these to deduce congruence properties of $a_n(G)$ for certain free products G of finite groups. An analogous programme for one-relator groups is carried out in [Müller & Puchta (b)]. At this stage, the results, though quite deep, apply only to rather restricted classes of groups. But it seems that this is only the tip of the iceberg of a rich theory of "modular subgroup arithmetic".

14.4 Surface groups

Let us begin with some general observations about subgroup counting in one-relator groups. So let

$$G = \langle g_1, \ldots, g_d \,;\, w(g_1, \ldots, g_d) = 1 \rangle$$

be a one-relator group. The sequence $(a_n(G))$ is determined via Proposition 14.1.2 by the numbers

$$h_n(G) = |\mathrm{Hom}(G, \mathrm{Sym}(n))|.$$

It is evident that $h_n(G)$ is equal to the number of solutions in $\mathrm{Sym}(n)^{(d)}$ of the equation

$$w(x_1, \ldots, x_d) = 1.$$

Now the question of the number of solutions of an equation in a finite group has a long history: indeed it was one of the earliest applications by Frobenius of his new invention, character theory. To see why this should be, let us write, for a group H,

$$N_w(H,z) = \left|\left\{\mathbf{x} \in H^{(d)} \mid w(\mathbf{x}) = z\right\}\right|.$$

Thus

$$h_n(G) = N_w(\mathrm{Sym}(n), 1)$$

for each n.

The function $N_w = N_w(H,-)$ is a *class function*, i.e. constant on conjugacy classes. As the irreducible characters of G form a basis for the space of class functions on G, the function N_w can in principle be expressed as a linear combination of characters ("non-commutative Fourier analysis"). An elegant account of this procedure is given in §7.2 of the book [Serre 1992]. In general it is easier said than done; but there are cases where it can be done quite explicitly, and leads to sharp information about subgroup growth.

Before turning to our specific topic, we make two remarks.

(i) If two words w_1 and w_2 in F_d are in the same orbit of $\mathrm{Aut}(F_d)$ then $N_{w_1} = N_{w_2}$, so some complicated words can be replaced by simpler ones.

(ii) Suppose that $w = w_1 w_2$ where the supports of w_1 and w_2 are disjoint. Then

$$N_w = N_{w_1} * N_{w_2}$$

where $*$ denotes the convolution

$$(\phi * \psi)(z) = \sum_{y \in H} \phi(y)\psi(y^{-1}z).$$

From now on we focus on two famous sequences of one-relator groups; but it seems likely that the method should be applicable to other one-relator groups where the relator is a relatively simple word. Let Γ_g (resp. Γ_g^*) denote the fundamental group of a closed orientable (resp. non-orientable) surface of genus g (resp. $2g$), where $g \geq 1$. So Γ_g has the presentation

$$\Gamma_g = \left\langle x_1, \ldots, x_g, y_1, \ldots, y_g \ ; \ \prod_{i=1}^{g} [x_i, y_i] = 1 \right\rangle$$

and Γ_g^* has the presentation

$$\Gamma_g^* = \left\langle x_1, \ldots, x_g, y_1, \ldots, y_g \ ; \ \prod_{i=1}^{g} x_i^2 y_i^2 = 1 \right\rangle.$$

Several papers have been dedicated to counting the subgroups of finite index in Γ_g and Γ_g^*, according to various parameters. Most works have been motivated

by topological considerations and old questions of Hurwitz and Poincaré; these concern the number of covers of one sort or another of a closed Riemann surface. For example counting inequivalent covers of degree n amounts to counting conjugacy classes of index n subgroups, etc. For more on these questions we refer the reader to the survey article [Kwak & Lee 2001] and its bibliography. Here we shall concentrate on the question of counting all subgroups of index n.

Similar results, using the same methods, can be established for the fundamental groups of non-orientable surfaces of odd genus, too (and appear in the cited literature). We stick to the groups Γ_g^* because of a certain similarity to Γ_g, which will shortly become apparent.

It was probably [Mednykh 1979] who was the first to connect this question with the representation theory of the symmetric group $\mathrm{Sym}(n)$. We will follow the more recent (and far-reaching) presentation of [Puchta (a)] and [Müller & Puchta (a)].

For a positive integer k, we denote the set of irreducible characters of $\mathrm{Sym}(k)$ by $X(k)$. The fundamental result is

Theorem 14.4.1 *Let Γ be either Γ_g or Γ_g^*. Then*

$$h_n(\Gamma) = |\mathrm{Hom}(\Gamma, S_n)| = (n!)^{2g-1} \sum_{\chi \in X(k)} \frac{1}{\chi(1)^{2g-2}}.$$

Here is a striking consequence:

Corollary 14.4.2 [Mednykh 1988] *For every n, $a_n(\Gamma_g) = a_n(\Gamma_g^*)$.*

This follows immediately in view of Proposition 14.1.2. Thus Γ_g and Γ_g^* are "isospectral": that is, they have the same sequence $(a_n(\Gamma))$ and hence the same zeta-function (see Chapter 15 below). This is quite remarkable as the groups (and even their profinite completions) are not isomorphic. It would be of great interest to better understand what it means for groups to be isospectral, and very few examples of such groups with non-isomorphic profinite completions are known.

For $k \in \mathbb{N}$ and $t \in \mathbb{R}$ put

$$\beta_k(t) = (k!)^t \sum_{\chi \in X(k)} \chi(1)^{-t}.$$

Note that $\beta_k(0) = p(k)$, the number of partitions of k, since this is the number of conjugacy classes in $\mathrm{Sym}(k)$. Using this notation we can restate Theorem 14.4.1 in the concise form

$$h_n(\Gamma) = n! \beta_n(2g-2),$$

and the identity (14.2) in Proposition 14.1.2 now gives

$$a_n(\Gamma) = n\beta_n - \sum_{k=1}^{n-1} \beta_{n-k} a_k(\Gamma)$$

where $\beta_i = \beta_i(2g-2)$. Since $a_1(\Gamma) = 1$ we may deduce the following "explicit formula" by induction on n:

Corollary 14.4.3 [Mednykh 1979] *Let Γ denote one of Γ_g or Γ_g^*. Then*

$$a_n(\Gamma) = \sum_{s=1}^{n} (-1)^{s+1} \sum i_s \cdot \beta_{i_1}\beta_{i_2}\dots\beta_{i_s}$$

where $\beta_i = \beta_i(2g-2)$ for each i and the sum is over all ordered s-tuples $(i_1, \dots, i_s)$ of positive integers such that $i_1 + \dots + i_s = n$.

(Actually Mednykh gives a slightly different, but equivalent, formula.) Since $\Gamma_1 \cong \mathbb{Z}^2$ and $a_n(\mathbb{Z}^2)$ is easily seen to be $\sigma(n)$, the sum of the divisors of n, the special case $g = 1$ of this result reduces to the combinatorial identity

$$\sigma(n) = \sum_{s=1}^{n} (-1)^{s+1} \sum i_s \cdot p(i_1)\dots p(i_s).$$

To obtain an asymptotic estimate for the $a_n(\Gamma)$ we first need one for the character-sums $\beta_n(t)$; this is provided by

Proposition 14.4.4 [Müller & Puchta (a)] *For fixed $t \geq 1$,*

$$\sum_{\chi \in X(n)} \chi(1)^{-t} = 2 + O(n^{-t}) \quad (n \to \infty).$$

This means that the dominant terms of the sum come from the two one-dimensional representations of $\mathrm{Sym}(n)$. It implies that as long as $g \geq 2$,

$$\beta_n(2g-2) \sim 2(n!)^{2g-2} \qquad (n \to \infty)$$

Now just as for the free non-abelian groups, one can show that 'most' homomorphisms from Γ to $\mathrm{Sym}(n)$ have transitive image, so (for $g \geq 2$) we have

$$t_n(\Gamma) \sim h_n(\Gamma) = n!\beta_n(2g-2).$$

Together with (14.1) this gives

Theorem 14.4.5 *Let Γ be either Γ_g or Γ_g^*, where $g \geq 2$. Then*

$$a_n(\Gamma) \sim 2n(n!)^{2g-2}.$$

Recalling that $a_n(F_d) \sim n(n!)^{d-1}$ (Theorem 2.1) we see that

$$a_n(\Gamma) \sim 2a_n(F_{2g-1}).$$

This is a suggestive result: both Γ and F_{2g-1} are groups presented on $2g$ generators with one relation, and the value of a_n reflects the number of ways of

expressing the identity in $\mathrm{Sym}(n)$ as a value of the particular word defining that relation. Suppose that G is a d-generator 1-relator group and that

$$a_n(G) \sim c \cdot a_n(F_{d-1});$$

what are the possible values for the constant c?

Let us now sketch the proof of Theorem 14.4.1. For this we need first to determine the functions $N_{[x,y]}(\mathrm{Sym}(n), -)$ and $N_{x^2}(\mathrm{Sym}(n), -)$.

Proposition 14.4.6 (Frobenius, 1896) *Let H be a finite group. Then for $z \in H$,*

$$N_{[x,y]}(H, z) = |H| \sum \frac{\chi(z)}{\chi(1)}$$

summed over all irreducible characters of H.

The proof depends on the following general fact (see [Curtis & Reiner 1981], Prop. 9.33 or [Serre 1992], §7.2):

Lemma 14.4.7 *Let H be a finite group, C_1, C_2 conjugacy classes of H and $z \in H$. Then the number of solutions of the equation $x \cdot y = z$ with $x \in C_1$ and $y \in C_2$ equals*

$$\frac{|C_1||C_2|}{|H|} \sum \frac{\chi(C_1)\chi(C_2)\chi(z^{-1})}{\chi(1)},$$

summed over all irreducible characters of H.

Now $[x, y] = x^{-1}x^y$ so solutions of $[x, y] = z$ correspond to solutions of the equation $x^{-1} \cdot u = z$ where u is a conjugate of x. Given a conjugacy class C the number of solution of the second equation with $x \in C$ and $u \in C^{-1}$ is

$$\frac{|C||C^{-1}|}{|H|} \sum \frac{\chi(C)\chi(C^{-1})\chi(z^{-1})}{\chi(1)}.$$

Given one such solution (x, u), there are $|\mathrm{C}_G(x)| = |H| / |C|$ elements y such that $x^y = u$. Hence given C, the number of solutions of $[x, y] = z$ with $x \in C$ is

$$|C| \sum \frac{\chi(C)\chi(C^{-1})\chi(z^{-1})}{\chi(1)}$$

and summing over all classes C we get

$$\sum_{\chi} \left(\sum_{g \in H} \chi(g)\chi(g^{-1}) \right) \frac{\chi(z^{-1})}{\chi(1)} = |H| \sum \frac{\chi(z^{-1})}{\chi(1)}$$

since $\sum_{g \in H} \chi(g)\chi(g^{-1}) = |H|$ (the first orthogonality relation, [Curtis & Reiner 1981], Proposition 9.21). The proposition follows since $\chi(z^{-1})$ is the complex conjugate of $\chi(z)$ and the whole sum – being an integer! – is real.

The corresponding result for $w = x^2$ is a little harder to prove, and we refer the reader to [Isaacs 1976], Corollary 4.15:

Proposition 14.4.8 (Frobenius and Schur, 1906) *Let H be a finite group all of whose irreducible characters can be realized over $\mathbb{R}$. Then for $z \in H$,*

$$N_{x^2}(H, z) = \sum \chi(z)$$

summed over all irreducible characters of H.

Corollary 14.4.9 *With H as above,*

$$N_{x^2y^2}(H, z) = |H| \sum_{\chi} \frac{\chi(z)}{\chi(1)}.$$

Proof. According to remark (ii) above,

$$\begin{aligned} N_{x^2y^2}(H, z) &= \sum_{t \in H} N_{x^2}(H, t) N_{y^2}(H, t^{-1}z) \\ &= \sum_{t \in H} \sum_{\chi} \chi(t) \sum_{\chi'} \chi'(t^{-1}z) \\ &= \sum_{\chi, \chi'} \sum_{t \in H} \chi(t)\chi'(t^{-1}z) \\ &= |H| \sum_{\chi} \frac{\chi(z)}{\chi(1)} \end{aligned}$$

by the 'generalized orthogonality relation' (see e.g. [Isaacs 1976], Theorem 2.13). ■

Since all irreducible representations of $\mathrm{Sym}(n)$ can be realized over $\mathbb{Q}$, this applies to $H = \mathrm{Sym}(n)$. Thus for each n we have

$$N_{[x,y]}(\mathrm{Sym}(n), z) = N_{x^2y^2}(\mathrm{Sym}(n), z) = n! \sum_{\chi \in X(N)} \frac{\chi(z)}{\chi(1)}. \tag{14.3}$$

Let us denote this expression by $F_n(z)$. Applying (ii) again, we see that for $w = \prod_{i=1}^{g} [x_i, y_i]$ or $w = \prod_{i=1}^{g} x_i^2 y_i^2$,

$$N_w(\mathrm{Sym}(n), -) = \underbrace{F_n * F_n * \ldots * F_n}_{g} = F_n^{(*)^g}.$$

This already shows that Γ_g and Γ_g^* are isospectral, since $h_n(\Gamma_g) = h_n(\Gamma_g^*) = F_n^{(*)^g}(1)$.

To complete the proof of Theorem 14.4.1, it remains to show that

$$F_n^{(*)^g}(1) = n! \beta_n(2g - 2).$$

In fact we shall prove by induction on g that

$$F_n^{(*)^g}(z) = (n!)^{2g-1} \sum_{\chi \in X(n)} \frac{\chi(z)}{\chi(1)^{2g-1}};$$

this gives the result on putting $z = 1$.

When $g = 1$ this is (14.3). Suppose that $g > 1$. Then (arguing inductively)

$$\begin{aligned} F_n^{(*)^g}(z) &= \sum_{y \in \mathrm{Sym}(n)} F_n^{(*)^{g-1}}(y) F_n(y^{-1}z) \\ &= \sum_{y \in \mathrm{Sym}(n)} \left((n!)^{2g-3} \sum_{\chi \in X(n)} \frac{\chi(y)}{\chi(1)^{2g-3}} \cdot n! \sum_{\chi' \in X(N)} \frac{\chi'(y^{-1}z)}{\chi'(1)} \right) \\ &= (n!)^{2g-2} \sum_{\chi, \chi' \in X(n)} \frac{1}{\chi(1)^{2g-3}\chi'(1)} \sum_{y \in \mathrm{Sym}(n)} \chi(y)\chi'(y^{-1}z) \\ &= (n!)^{2g-2} \cdot n! \sum_{\chi \in X(n)} \frac{\chi(z)}{\chi(1)^{2g-1}}; \end{aligned}$$

the final equality applies the 'generalized orthogonality relation' as before. This completes the proof of Theorem 14.4.1.

To apply this method in studying the subgroup growth of other one-relator groups, one will need information about the number of solutions of other equations in $\mathrm{Sym}(n)$. Some results more general than the above are stated in the Exercises in §7.2 of [Serre 1992]. Another result of this type is

Theorem 14.4.10 [Kerber & Wagner 1980] *Let H be a finite group. For pre-assigned natural numbers $n_1, n_2, \ldots, n_k$, the number of solutions in H of the equation $x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k} = z$ is given by*

$$\frac{1}{|H|} \sum_{\chi} \left(\prod_{j=1}^{k} C_{\chi, n_j} \right) \frac{\chi(z^{-1})}{\chi(1)^{k-1}}$$

where

$$C_{\chi,n} = \sum_{y \in H} \chi(y^n).$$

We mention finally the recent work [Liskovets & Mednykh 2000]. This paper gives a formula for $a_n(\Theta_{g,e})$ where $\Theta_{g,e}$ is the fundamental group of an orientable S^1-bundle with Euler class e over a compact surface of genus g. This group has a presentation

$$\Theta_{g,e} = \left\langle a_1, \ldots, a_g, b_1, \ldots, b_g, h \; ; \; \prod_{i=1}^{g} [a_i, b_i] = h^e, \; [a_i, h] = [b_i, h] = 1 \, (\text{all } i) \right\rangle,$$

so it is a central extension of Γ_g. It is shown that

$$a_n(\Theta_{g,e}) = \sum_{\substack{m\ell = n \\ \ell^2 | n \cdot (e,n)}} a_m(\Gamma_g) \ell^{(2g-2)m+2}$$

(where (e, n) is the g.c.d. of e and n). The proof is algebraic. Similar results hold also for the other central extensions of surface groups.

Notes

For combinatorial results related to Proposition 14.2.2, see [**Chowla, Herstein & Moore 1951**], [**Chowla, Herstein & Scott 1952**], [**Moser & Wyman 1955**].

[**Müller 1996**] proves much more than the result we have stated as Theorem 14.2.4; on the one hand, his result allows also for infinite cyclic free factors, and on the other he gives a very explicit error term in the asymptotic expression for $a_n(G)$.

'Modular subgroup arithmetic' is developed in [**Grady & Newman 1992**], [**Grady & Newman 1994**], and the series of papers [**Müller (b)**], [**Müller (c)**], [**Müller (d)**], [**Müller & Puchta (b)**]. The survey article [**Müller (e)**] gives a full account of the present state of knowledge in this area.

The explicit formulas of §14.4 are due to [**Mednykh 1979**], [**Mednykh 1988**]. The asymptotic results are due to [**Puchta (a)**] and [**Müller & Puchta (a)**]; their results are more precise than those given here, with very strong bounds on the error terms.

Chapter 15

Zeta functions I: Nilpotent groups

In the previous chapter, the numbers $a_n(\Gamma)$ for a finitely generated group Γ were encoded via the generating function

$$A_\Gamma(X) = \sum a_n(\Gamma) X^n.$$

Another way to encode a sequence of numbers is via their associated Dirichlet series:

$$\zeta_\Gamma(s) = \sum a_n(\Gamma) n^{-s} = \sum_{H \leq \Gamma} |\Gamma : H|^{-s}.$$

This can be considered as a formal series, but if $a_n(\Gamma) = O(n^c)$ for some c, that is if Γ has polynomial subgroup growth, the series converges for complex numbers s such that $\mathfrak{Re}(s)$ is sufficiently large. More precisely, recalling that

$$\alpha(\Gamma) = \inf\{\alpha \mid s_n(\Gamma) = O(n^\alpha)\} = \limsup \frac{\log s_n(\Gamma)}{\log n},$$

we can say that $\zeta_\Gamma(s)$ converges for $\mathfrak{Re}(s) > \alpha(\Gamma)$ and defines a holomorphic function on this half plane (while ζ_Γ is divergent at $s = \alpha(\Gamma)$; both claims follow from elementary analysis). The analytic function $\zeta_\Gamma(s)$ is called the *zeta function* of Γ. This definition parallels the definition of the Dedekind zeta function of a number field, which encodes in exactly the same way the number of ideals of index n in a ring of algebraic integers.

Let's now assume in addition that the group Γ is *nilpotent*. Then $\zeta_\Gamma(s)$ has an *Euler product*, namely

$$\zeta_\Gamma(s) = \prod_p \zeta_{\Gamma,p}(s) \tag{15.1}$$

where the product runs over all primes p and

$$\zeta_{\Gamma,p}(s) = \sum_{i=0}^{\infty} a_{p^i}(\Gamma) p^{-is}.$$

The functions $\zeta_{\Gamma,p}(s)$ are called the *local zeta functions* of Γ, or just *local factors*. The identity (15.1) is a formal consequence of the fact that when Γ is a nilpotent group, the arithmetical function $a_n(\Gamma)$ is *multiplicative*, that is,

$$a_n(\Gamma) = \prod a_{p_j^{e(j)}}(\Gamma)$$

where $n = \prod p_j^{e(j)}$ is the factorisation of n with distinct primes p_j; this in turn follows easily from the fact that every finite nilpotent group is the direct product of its Sylow subgroups (see Proposition 1.4.4).

If $\Gamma = \mathbb{Z}$ then $a_n(\Gamma) = 1$ for every n, and $\zeta_\Gamma(s) = \sum n^{-s}$ is none other than the Riemann zeta function $\zeta(s)$, so the theory of zeta functions of nilpotent groups which we are going to discuss here may be seen as a non-commutative extension of classical analytic number theory.

More generally, let us consider $\Gamma = \mathbb{Z}^r$, the free abelian group of rank r. Here we have

Theorem 15.1 $\zeta_{\mathbb{Z}^r}(s) = \zeta(s) \cdot \zeta(s-1) \cdot \ldots \cdot \zeta(s-r+1)$.

We shall present *five* distinct proofs for this elementary, but suggestive, result (one of them has already appeared in Chapter 11).

Things begin to get more challenging – and unpredictable – when we turn to non-abelian groups. The smallest of these among torsion-free nilpotent groups is the 'discrete Heisenberg group', that is the free class-2 nilpotent group on 2 generators

$$\begin{aligned} F &= \langle x, y, z \,;\, z = [x,y],\, [z,x] = [z,y] = 1 \rangle \\ &\cong \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\} \leq \mathrm{GL}_3(\mathbb{Z}). \end{aligned}$$

Theorem 15.2 *Let F be the discrete Heisenberg group. Then*

$$\zeta_F(s) = \frac{\zeta(s)\zeta(s-1)\zeta(2s-2)\zeta(2s-3)}{\zeta(3s-3)}.$$

(Note that the right hand side is indeed a Dirichlet series since $\frac{1}{\zeta(s)} = \sum \mu(n) n^{-s}$ where μ is the Möbius function.)

When this result was discovered by Geoff Smith in the early 1980s, it encouraged the hope that the zeta function of every finitely generated nilpotent group might have such a nice expression (and hence, for example, a meromorphic continuation to the whole plane). This is by no means the case, however. The picture is more complicated and more subtle: we return to this below.

Section 1 examines the nature of the local zeta functions. We begin by showing how the local zeta function of $\mathbb{Z}^r$ may be re-interpreted as a certain p-adic integral. This integral is easy to evaluate explicitly, and leads to the first

proof of Theorem 15.1. (A brief explanation of p-adic integrals is given in the **p-adic integrals and logic** window.)

Now, the representation of $\zeta_{\Gamma,p}(s)$ as a p-adic integral is a procedure that can be applied quite generally, whenever Γ is a torsion-free finitely generated nilpotent group. When Γ is non-abelian the resulting integral is usually hard to evaluate explicitly; this can still be done in some very simple cases, and we do it for the Heisenberg group. We now come to a key observation: the integral representing $\zeta_{\Gamma,p}(s)$ is in any case the integral of a *definable function* over a *definable domain* of integration, in the sense of p-adic model theory. An important general theorem, due to to [Denef 1984], applies to all such integrals, yielding the following result:

Theorem 15.3 *Let Γ be a finitely generated torsion-free nilpotent group and p a prime. Then $\zeta_{\Gamma,p}(s)$ is a rational function over $\mathbb{Q}$ of p^{-s}.*

This theorem initiated the general theory of such group-theoretic zeta functions. Its meaning in terms of subgroup growth is quite concrete: thinking of $p^{-s} = X$ as a variable, we can interpret the theorem as asserting the power series identity

$$\sum_{i=0}^{\infty} a_{p^i}(\Gamma) X^i = \frac{\Phi(X)}{\Psi(X)}$$

where Φ and Ψ are polynomials over $\mathbb{Z}$, of degrees ℓ and k, say, respectively. Now multiplying out and equating coefficients we infer:

Corollary 15.4 *There exist positive integers $\ell = \ell(\Gamma, p)$ and $k = k(\Gamma, p)$ such that the sequence $\left(a_{p^i}(\Gamma)\right)_{i>\ell}$ satisfies a linear recurrence relation with constant coefficients over $\mathbb{Z}$ of length at most k.*

Both the Euler product (15.1) and Theorem 15.3 hold also for the 'normal zeta functions'

$$\zeta_{\Gamma}^{\triangleleft}(s), \ \zeta_{\Gamma,p}^{\triangleleft}(s)$$

which are defined analogously using $a_n^{\triangleleft}(\Gamma)$ in place of $a_n(\Gamma)$, with essentially the same proofs. Theorem 15.3 has been vastly generalized by [du Sautoy 1993], to the domain of all compact p-adic analytic groups; this is dealt with in the following chapter. One consequence of du Sautoy's theorem is that Theorem 15.3 applies to *all* finitely generated nilpotent groups, not just the torsion-free ones.

In Section 2 we digress to give four more proofs of Theorem 15.1. Each of these proofs generalizes in a different way, and some of them point in interesting new directions. Among these are (1) the topic of *zeta functions associated to algebraic groups*; the latter are in fact the 'true' generalisation of the Dedekind zeta functions; from our point of view, they arise when we study the growth of the number of subgroups H of Γ such that $\widehat{H} \cong \widehat{\Gamma}$. (2) The 'probabilistic zeta functions' introduced by Mann.

In Section 3 we turn to the 'global' zeta functions themselves. A better understanding of the analytic behaviour of $\zeta_\Gamma(S)$ depends on a more delicate analysis of the local factors $\zeta_{\Gamma,p}(s)$, in particular of their variation with p. The main results are as follows, where Γ denotes a finitely generated nilpotent group.

Theorem 15.5 *$\alpha(\Gamma)$ is a rational number.*

Theorem 15.6 *The function $\zeta_\Gamma(S)$ has a meromorphic analytic continuation to some open half-plane containing $\alpha(\Gamma)$.*

The significance of the latter theorem is that it allows one to apply a standard method of analytic number theory, a so-called *Tauberian theorem*, to deduce an asymptotic estimate for the subgroup growth. Combining Theorem 15.6 with [N], Corollary on p. 121, one deduces

Theorem 15.7 *There exist an integer $\beta \geq 0$ and a constant c such that*

$$s_n(\Gamma) \sim cn^\alpha (\ln n)^\beta$$

where $\alpha = \alpha(\Gamma) \in \mathbb{Q}$.

(Here, $\beta + 1$ is the order of the pole of $\zeta_\Gamma(S)$ at $s = \alpha(\Gamma)$). As before, these results all apply to the *normal subgroup* counting functions as well.

These deep theorems may be said to put the 'analytic number theory of nilpotent groups' firmly on the map. We cannot discuss the proofs in any detail, and confine ourselves to giving an outline of the main ideas. A more detailed account may be found in Chapter 9 of [NH]; for complete proofs the reader is referred to the original paper [du Sautoy and Grunewald 2000].

These proofs go deeply into algebraic geometry and algebraic number theory, and certainly represent the high point of the arithmetical theory of subgroup growth to date. They also shed some light, but only the first glimmerings, on some of the most intriguing problems that remain open. To conclude this introduction let us mention a few of these, together with what is at present known about them.

Problem 1 '*Uniformity*' In most cases where we have an explicit formula for the rational function representing $\zeta_{\Gamma,p}(S)$, it takes the form

$$\frac{P(p, p^{-s})}{Q(p, p^{-s})} \tag{15.2}$$

where P and Q are *two-variable* polynomials over $\mathbb{Z}$ that *do not depend on p*. In this case we say that $\zeta_{\Gamma,p}$ is *uniform in p*. A glance back at Theorems 15.1 and 15.2 will show that this is the case when Γ is either $\mathbb{Z}^r$ or the Heisenberg group, for example. Other examples, calculated in [Grunewald, Segal & Smith 1988], have the slightly weaker property that *finitely many* polynomials suffice to represent $\zeta_{\Gamma,p}(S)$ in this way, as p ranges over all primes, and it was suggested in [Grunewald, Segal & Smith 1988] that this might hold for all Γ. The proof

of Theorem 15.3 in [Grunewald, Segal & Smith 1988] actually showed that P and Q may be taken to have bounded degrees as p ranges over all primes; this implies in particular that the numbers $\ell(\Gamma, p)$ and $k = k(\Gamma, p)$ in Corollary 15.4 are independent of p.

In [du Sautoy 1994$_a$] it is proved that Q itself may be taken independent of p, indeed that it only depends on the Hirsch length of Γ. However, the suggestion as regards P has been refuted by [du Sautoy 2001], who shows how to encode an elliptic curve $\mathcal{C}$ over $\mathbb{Q}$ into the definition of a nilpotent group Γ in such a way that infinitely many different polynomials P are required, reflecting the ("wild") variation with the prime p of the number of points on $\mathcal{C}(\mathbb{F}_p)$. Specifically, to the curve

$$\mathcal{C} : Y^2 = X^3 - X$$

he associates the class-2 nilpotent group Γ generated by x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3 subject to the relations

$$\begin{aligned}
[x_1, x_4] &= [x_3, x_5] = y_3 \\
[x_1, x_5] &= [x_2, x_6] = [x_3, x_4] = y_1 \\
[x_1, x_6] &= [x_2, x_4] = y_2 \\
[x_i, x_j] &= 1 \,(\text{all other } i,\, j) \\
[x_i, y_j] &= [y_i, y_j] = 1 \,(\text{all } i,\, j),
\end{aligned}$$

and shows that for almost all primes p,

$$\zeta^{\triangleleft}_{\Gamma,p}(s) = R_1(p, p^{-s}) + |\mathcal{C}(\mathbb{F}_p)| \cdot R_2(p, p^{-s});$$

here R_1 and R_2 are (non-zero) rational functions.

It was also conjectured in [Grunewald, Segal & Smith 1988] that for a *relatively free* nilpotent group Γ, $\zeta_{\Gamma,p}$ is uniform in p (with perhaps finitely many exceptions for small primes). This was established in [Grunewald, Segal & Smith 1988] for free-nilpotent groups of class 2, and recently for all 2-generator free-nilpotent groups [du Sautoy & Grunewald (a)]. But the problem in general remains open.

Problem 2 '*Local functional equation*' In most cases that have been calculated explicitly, the numerator P in (15.2) has a curious symmetry property: the coefficients are 'symmetric about the middle'. In other words, there exist integers a and b such that

$$P(X, Y) = X^a Y^b P(X^{-1}, Y^{-1}).$$

No general explanation is known for this phenomenon (but see the discussion of the related function $\widehat{\zeta}_G$ in §15.2 below).

Problem 3 *Abscissa of convergence and analytic continuation.* This is really two problems.

(a) How does $\alpha(\Gamma)$ depend on the structure of Γ? The proof of Theorem 15.5 gives in principle an explicit procedure that may be applied to any given group Γ (f.g. nilpotent as always), but sheds little light on how the result reflects algebraic properties of Γ. Some relatively crude upper and lower bounds are given in [Grunewald, Segal & Smith 1988] and [Klopsch 2000].

(b) For which groups Γ does $\zeta_\Gamma(s)$ have a meromorphic continuation to the whole complex plane? This is the case for groups like $\mathbb{Z}^r$ and H, but there are groups Γ such that $\zeta_\Gamma(s)$ has a natural boundary. Here we have a subtle arithmetical property of a nilpotent group Γ: what does it mean in terms of the structure of Γ? The paper [du Sautoy & Grunewald 1998] studies an interesting variant of this question.

We can illustrate some of these phenomena with the following example, of a group that is barely more complicated than the Heisenberg group: the free class-two nilpotent group on three generators. For this group Γ, it is shown in [Grunewald, Segal & Smith 1988] that

$$\zeta^{\triangleleft}_{\Gamma,p}(s) = \frac{1 + p^{3-3s} + p^{4-3s} + p^{6-5s} + p^{7-5s} + p^{10-8s}}{(1-p^{-s})(1-p^{1-s})(1-p^{2-s})(1-p^{8-5s})(1-p^{9-6s})}$$

for every prime p. So in this case we have (1) 'uniformity' and (2) a 'local functional equation' (formally replacing p by p^{-1} has the effect of multiplying the expression by p^{10-6s}). But (3) the global function $\zeta^{\triangleleft}_\Gamma(s) = \prod_p \zeta^{\triangleleft}_{\Gamma,p}(s)$ does *not* have analytic continuation to $\mathbb{C}$; [du Sautoy (b)] shows that the line $\mathrm{Re}(s) = 7/5$ is a natural boundary.

To conclude with a quotation: "The [Dedekind] zeta function knows everything about the number field; we just have to prevail on it to tell us" [Swinnerton-Dyer 2001], page viii. The great edifice of algebraic number theory exists largely for that purpose. Results like Theorem 15.7 show that the analogy is not completely fanciful; in our non-commutative, group theoretic, context we have some foundation-stones, but there is plenty of building still to be done.

15.1 Local zeta functions as p-adic integrals

In this section, p will denote a fixed prime. The p-adic absolute value of $\lambda \in \mathbb{Z}_p$ is written

$$|\lambda| = p^{-f}$$

where $\lambda = p^f u$ and u is a p-adic unit. When talking about pro-p groups, we shall use 'generated' to mean 'topologically generated, and write $G = \langle S \rangle$ to mean that the set S generates G topologically.

For any nilpotent group Γ and all i we have $a_{p^i}(\Gamma) = a_{p^i}(\widehat{\Gamma}_p)$, so to study the p-local zeta function of Γ we may replace Γ by its pro-p completion.

Let us begin with $\Gamma = \mathbb{Z}^r$, in which case $\widehat{\Gamma}_p = \mathbb{Z}_p^r = G$, say. Each open subgroup H of G has a 'triangular' basis

$$\begin{array}{rcl} h_1 &=& (\lambda_{11} \quad \lambda_{12} \quad \quad \dots \quad \quad \dots \quad \lambda_{1r}) \\ h_2 &=& (0 \quad \lambda_{22} \quad \lambda_{23} \quad \dots \quad \dots \quad \lambda_{2r}) \\ \vdots & & \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ h_i &=& (0 \quad \dots \quad 0 \quad \lambda_{ii} \quad \quad \lambda_{ir}) \\ \vdots & & \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ h_r &=& (0 \quad \dots \quad \dots \quad \dots \quad 0 \quad \lambda_{rr}) \end{array} \tag{15.3}$$

An r-tuple $(h_1, \dots, h_r)$ of this form will be called a *good basis* for H.

Let e_i denote the ith standard basis vector in $G = \mathbb{Z}_p^r$, and put

$$G_i = \langle e_i, \dots, e_r \rangle \,, \;\; H_i = H \cap G_i.$$

Then $(h_1, \dots, h_r)$ is a good basis for H precisely when

$$H_i = \langle h_i \rangle + H_{i+1} \quad \text{for} \quad i = 1, \dots, r \tag{15.4}$$

For each i we have

$$\begin{aligned} |G_i : H_i| &= |G_i : G_{i+1} + H_i| \cdot |G_{i+1} : H_{i+1}| \\ &= |\lambda_{ii}|^{-1} \, |G_{i+1} : H_{i+1}| \,, \end{aligned} \tag{15.5}$$

since $G_i/(G_{i+1} + H_i) \cong \mathbb{Z}_p/\lambda_{ii}\mathbb{Z}_p = \mathbb{Z}_p/p^{f_i}\mathbb{Z}_p$ where λ_{ii} is p^{f_i} times a p-adic unit. It follows that

$$|G : H| = |G_1 : H_1| = \prod_{i=1}^{r} |\lambda_{ii}|^{-1} \tag{15.6}$$

whenever (15.3) is a good basis for H.

To each open subgroup H of G we associate the following set of upper-triangular matrices over $\mathbb{Z}_p$:

$$\mathcal{M}(H) = \left\{ \begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix} \mid (h_1, \dots, h_r) \text{ is a good basis for } H \right\}.$$

Writing μ for the normalized Haar measure on the additive group $\mathrm{Tr}(r, \mathbb{Z}_p) \cong \mathbb{Z}_p^{r(r+1)/2}$ of all of upper-triangular $r \times r$ matrices, we make the following key calculation:

Lemma 15.1.1 *$\mathcal{M}(H)$ is an open subset of $\mathrm{Tr}(r, \mathbb{Z}_p)$. Its measure is given by*

$$\mu(\mathcal{M}(H)) = (1 - p^{-1})^r \prod_{i=1}^{r} |\lambda_{ii}|^i,$$

where the $|\lambda_{ii}|$ are determined by (15.5).

Proof. Fix a generator g_i for H_i modulo H_{i+1}. From (15.4) we see that (h_i) is a good basis if and only if

$$h_i \in g_i \mathbb{Z}_p^* + H_{i+1}$$

for each i, so

$$\mathcal{M}(H) = (g_1 \mathbb{Z}_p^* + H_2) \times \cdots \times (g_r \mathbb{Z}_p^* + H_{r+1}).$$

This shows that $\mathcal{M}(H)$ is open, and that its measure is

$$\prod_{i=1}^{r} \mu\left(g_i \mathbb{Z}_p^* + H_{i+1}\right) \tag{15.7}$$

(using μ to denote the normalized measure on $\mathbb{Z}_p^j$ for every j, a slight abuse of notation).

Now write

$$g_i = (0, \ldots, 0, \lambda_{ii}, \ldots, \lambda_{ir}) = (0, \lambda_{ii}, \overline{\lambda})$$

say. Then as a subset of $\mathbb{Z}_p^{r-i+1} = \mathbb{Z}_p \times \mathbb{Z}_p^{r-i}$ we have

$$g_i \mathbb{Z}_p^* + H_{i+1} = \left\{(\lambda_{ii} v, v\overline{\lambda} + h) \mid v \in \mathbb{Z}_p^*,\ h \in H_{i+1}\right\}.$$

Now there exists n such that $p^n \mathbb{Z}_p^{r-i} \subseteq H_{i+1}$. Partitioning $\mathbb{Z}_p^*$ into (finitely many) additive cosets $U_j = v_j + p^n \mathbb{Z}_p$, we may write

$$g_i \mathbb{Z}_p^* + H_{i+1} = \bigcup_j ((\lambda_{ii} U_j) \times (v_j \overline{\lambda} + H_{i+1})).$$

The measure of this set is equal to

$$\begin{aligned}
\sum_j \mu(\lambda_{ii} U_j) \cdot \mu(v_j \overline{\lambda} + H_{i+1}) &= \mu\left(\bigcup_j (\lambda_{ii} U_j)\right) \cdot \mu(H_{i+1}) \\
&= \mu(\lambda_{ii} \mathbb{Z}_p^*) \cdot \mu(H_{i+1}) \\
&= (1 - p^{-1}) \left|\lambda_{ii}\right| \cdot \left|G_{i+1} : H_{i+1}\right|^{-1} \\
&= (1 - p^{-1}) \left|\lambda_{ii}\right| \cdot \prod_{j=i+1}^{r} \left|\lambda_{jj}\right| \\
&= (1 - p^{-1}) \prod_{j=i}^{r} \left|\lambda_{jj}\right|,
\end{aligned}$$

by (15.6) applied to $H_{i+1} \leq G_{i+1}$. Plugging this into (15.7) gives the result. ∎

Since the integral of a constant function over $\mathcal{M}(H)$ is just $\mu(\mathcal{M}(H))$ times the value of the function, we can rewrite the conclusion (introducing a formal variable s) in the following form:

$$|G:H|^{-s} = \frac{1}{(1-p^{-1})^r} \int\limits_{\mathcal{M}(H)} |\lambda_{11}|^{s-1} \cdot \ldots \cdot |\lambda_{rr}|^{s-r} d\mu.$$

As the sets $\mathcal{M}(H)$ are pairwise disjoint, we may sum over the countable collection of all open subgroups H of G and obtain

Proposition 15.1.2

$$\zeta_G(s) = \frac{1}{(1-p^{-1})^r} \int\limits_{\mathcal{M}} |\lambda_{11}|^{s-1} \cdot \ldots \cdot |\lambda_{rr}|^{s-r} \, d\mu$$

where $\mathcal{M} = \bigcup \{\mathcal{M}(H) \mid H \leq_o G\}$.

To evaluate this integral, we observe that $\mathcal{M}$ is equal to the set all upper triangular $r \times r$ matrices over $\mathbb{Z}_p$ with non-zero entries along the diagonal. Those with determinant zero form a set of measure zero and can therefore be ignored. Thus

$$\begin{aligned}
\zeta_{\mathbb{Z}_p^r}(s) &= \frac{1}{(1-p^{-1})^r} \int\limits_{\mathrm{Tr}(r,\mathbb{Z}_p)} |\lambda_{11}|^{s-1} \cdot \ldots \cdot |\lambda_{rr}|^{s-r} d\mu \\
&= \frac{1}{(1-p^{-1})^r} \prod_{i=1}^{r} \int\limits_{\mathbb{Z}_p} |\lambda_{ii}|^{s-i} d\mu \\
&= \prod_{i=0}^{r-1} (1-p^{i-s})^{-1}; \qquad (15.8)
\end{aligned}$$

the final step uses the formula

$$\int\limits_{\mathbb{Z}_p} |\lambda|^s d\mu = \frac{1-p^{-1}}{1-p^{-s-1}},$$

which is derived in the ***p*-adic integrals and logic** window.

With the Euler product (15.1) this completes the first proof of Theorem 15.1.

The formalism of this proof can be carried over whenever G is the pro-p completion of a torsion free finitely generated nilpotent group Γ. In this case, Γ has a central series $\Gamma = \Gamma_1 > \Gamma_2 > \cdots > \Gamma_r > \Gamma_{r+1} = 1$ with each factor Γ_i/Γ_{i+1} infinite cyclic. Choosing $x_1, \ldots, x_r$ so that $x_i\Gamma_{i+1}$ is a generator for Γ_i/Γ_{i+1}, we can express each element of Γ uniquely in the form

$$x = x_1^{a_1} \cdot \ldots \cdot x_r^{a_r}$$

with $a_1, \ldots, a_r \in \mathbb{Z}$. Such an r-tuple $(x_1, \ldots, x_r)$ is called a *Mal'cev basis for* Γ. P. Hall showed that when $(a_1, \ldots, a_r)$ are taken as the co-ordinates of x, the

group operations in Γ are given by polynomial functions with rational coefficients; this applies also to the power operation $x \mapsto x^n$, which is a polynomial function of $(a_1, \ldots, a_r)$ and n (see e.g. [Kargapolov & Merzljakov 1979], §17.2).

These polynomial functions, being integer-valued on the integers, can all be expressed as polynomials over $\mathbb{Z}$ in the binomial functions $\binom{X}{k}$. They can therefore be extended to polynomial functions on any 'binomial ring', in particular to $\mathbb{Z}_p$. Endowing the set $\mathbb{Z}_p^r$ with operations defined by these functions, we obtain a group

$$G = \Gamma^{\mathbb{Z}_p};$$

this is a pro-p group, having the central series $G = G_1 > G_2 > \cdots > G_r > G_{r+1} = 1$ where

$$\begin{aligned} G_i &= \Gamma_i^{\mathbb{Z}_p} \\ &= \left\langle x_i^{\mathbb{Z}_p} \right\rangle G_{i+1}. \end{aligned}$$

Sending $x \in \Gamma$ to its co-ordinate vector $(a_1, \ldots, a_r)$ identifies Γ with $\mathbb{Z}^r \subseteq \mathbb{Z}_p^r = G$, and it is not hard to verify that then G is the pro-p completion $\widehat{\Gamma}_p$. For later reference, we note the crucial facts that the group operations

$$(x, y) \mapsto xy, \ x \mapsto x^{-1} \qquad (x, y \in G)$$

and the power operation

$$(x, \lambda) \mapsto x^\lambda \qquad (x \in G, \ \lambda \in \mathbb{Z}_p)$$

are *polynomial functions* on $G \times G = \mathbb{Z}_p^{2r}$, $G = \mathbb{Z}_p^r$ and $G \times \mathbb{Z}_p = \mathbb{Z}_p^{r+1}$ respectively.

Now, simply changing additive to multiplicative notation, we define a *good basis* for an open subgroup H of G by the criterion (15.4). Then (15.5), (15.6) and Lemma 15.1.1 are still valid, with essentially the same proofs. The conclusion is that

Proposition 15.1.2 holds whenever G is the pro-p completion of torsion free finitely generated nilpotent group.

In general, it is not so easy to describe the set $\mathcal{M}$ for a non-abelian group G. When this can be done, it again leads to a complete evaluation of the local zeta function. By way of illustration, we apply it now to complete the

Proof of Theorem 15.2. The discrete Heisenberg group is

$$F = \langle x, y, z \mid [x, y] = z, \, [x, z] = [y, z] = 1 \rangle.$$

As Mal'cev basis we take (z, y, x), giving rise to the central series

$$G = G_1 = \langle x, y, z \rangle > G_2 = \langle y, z \rangle > G_1 = \langle z \rangle > G_0 = 1$$

in the pro-p completion $G = F^{\mathbb{Z}_p}$. We have to recognize the set $\mathcal{M}$ of upper-triangular matrices that represent good bases for open subgroups of G.

Now the upper-triangular matrix $A = (\lambda_{ij})$ belongs to $\mathcal{M}(H)$ if and only if the following three conditions are satisfied:

$$H = \left\langle x^{\lambda_{11}} y^{\lambda_{12}} z^{\lambda_{13}},\, y^{\lambda_{22}} z^{\lambda_{23}},\, z^{\lambda_{33}} \right\rangle \tag{i}$$

$$H \cap G_2 = \left\langle y^{\lambda_{22}} z^{\lambda_{23}},\, z^{\lambda_{33}} \right\rangle \tag{ii}$$

$$H \cap G_3 = \left\langle z^{\lambda_{33}} \right\rangle. \tag{iii}$$

Given the matrix A, take H to be the (closed) subgroup of G defined by (i); this is open if and only if $\lambda_{11} \cdot \lambda_{22} \cdot \lambda_{33} \neq 0$. Assuming this to be so, then (iii) is satisfied if and only if $\left\langle z^{\lambda_{33}} \right\rangle$ contains the commutator

$$[x^{\lambda_{11}} y^{\lambda_{12}} z^{\lambda_{13}},\, y^{\lambda_{12}} z^{\lambda_{23}}] = [x^{\lambda_{11}}, y^{\lambda_{22}}] = z^{\lambda_{11}\lambda_{22}},$$

which happens if and only if λ_{33} divides $\lambda_{11}\lambda_{22}$ in $\mathbb{Z}_p$. If condition (iii) is satisfied then one easily checks that (ii) also follows. We conclude that $\mathcal{M}$ is the set of all upper-triangular matrices A as above for which all λ_{ii} are non-zero and $\lambda_{33} \mid \lambda_{11}\lambda_{22}$.

We can now evaluate the integral giving $\zeta_{F,p}(s) = \zeta_G(s)$. Having already evaluated $\zeta_{\mathbb{Z}_p^3}(s)$, it is simpler in fact to integrate over the *complement* of $\mathcal{M}$ in $\mathrm{Tr}(3, \mathbb{Z}_p)$, namely the set

$$C(\mathcal{M}) \sim \bigcup_{a,b,c \geq 0} \begin{pmatrix} p^a\mathbb{Z}_p^* & \mathbb{Z}_p & \mathbb{Z}_p \\ 0 & p^b\mathbb{Z}_p^* & \mathbb{Z}_p \\ 0 & 0 & p^{a+b+c+1}\mathbb{Z}_p^* \end{pmatrix}$$

where $\sim$ indicates equality apart from the set of measure zero consisting of singular matrices. Noting that $\mu(p^n\mathbb{Z}_p^*) = p^{-n}(1-p^{-1})$ we find that

$$\begin{aligned}
(1-p^{-1})^{-3} \int_{C(\mathcal{M})} & |\lambda_{11}|^{s-1} |\lambda_{22}|^{s-2} |\lambda_{33}|^{s-3}\, d\mu \\
&= \sum_{a\geq 0}\sum_{b\geq 0}\sum_{c\geq 0} p^{-as} p^{-b(s-1)} p^{-(a+b+c+1)(s-2)} \\
&= \frac{p^{2-s}}{(1-p^{2-s})} \sum_a \sum_b p^{-a(2s-2)} p^{-b(2s-3)} \\
&= \frac{p^{2-s}}{(1-p^{2-s})(1-p^{2-2s})(1-p^{3-2s})}
\end{aligned}$$

(the transition from an integral to a geometric progression made here in the first step is illustrated in more detail in the window on **p-adic integrals and logic**). To obtain $\zeta_G(s)$ we have to subtract this from $(1-p^{-1})^{-3}$ times the corresponding integral over the whole of $\mathrm{Tr}(3, \mathbb{Z}_p)$, which is given in (15.8) above.

The result is

$$\frac{1}{(1-p^{-s})(1-p^{1-s})(1-p^{2-s})} - \frac{p^{2-s}}{(1-p^{2-s})(1-p^{2-2s})(1-p^{3-2s})}$$
$$= \frac{(1-p^{3-3s})}{(1-p^{-s})(1-p^{1-s})(1-p^{2-2s})(1-p^{2-3s})}. \tag{15.9}$$

With the Euler product formula this completes the proof.

We have given this calculation in some detail for several reasons.

Firstly, because the result is remarkable: it presents the zeta function of a non-commutative group as a simple closed formula in terms of the very classical Riemann zeta function – a result we had no right to expect in advance.

Secondly, to show how, in practice, one evaluates integrals of the type that arise in this context: namely by successively summing certain geometric progressions. In fact, a little thought about the definition of these p-adic integrals reveals that they are, in essence, a convenient formalism for handling just such geometric progressions. This makes Denef's rationality theorem seem less surprising: indeed, the main point of Denef's proof is to decompose the domain of integration into pieces on each of which the integral can actually be evaluated in this way (↬ **p-adic integrals and logic**).

Thirdly, to reveal the lucky accident that is responsible for the simple form of (15.9): while the *denominator* $(1-p^{-s})(1-p^{1-s})(1-p^{2-2s})(1-p^{2-3s})$ is predictable once we know the general shape of the integral, the fact that the *numerator* also looks like a local zeta-factor just comes from some lucky cancellations. As far as we know, there is no deeper explanation for this phenomenon, and it is *not* reproduced in the local zeta functions of (even slightly) more complicated groups. The denominator, on the other hand, does always take the form of a product $\prod(1-p^{a_i-b_is})$: see [du Sautoy 1994_a].

Let us return now to the general case of a torsion free finitely generated nilpotent group Γ. Proposition 15.1.2 represents $\zeta_{\Gamma,p}(s)$ quite explicitly as an integral. The only difficulty is the domain of integration $\mathcal{M}$. This is the set of all upper-triangular matrices with rows $h_i = (0,\dots,0,\lambda_{ii},\dots,\lambda_{ir}), i = 1,\dots,r$, which form good bases for open subgroups of $G = \widehat{\Gamma}_p$, when this is identified with $\mathbb{Z}_p^r$ as explained above.

Lemma 15.1.3 *An r-tuple $(h_1,\dots,h_r)$ is a good basis for some open subgroup of G if and only if*
(i) $\prod \lambda_{ii} \neq 0$ *and*
(ii) *for each pair $i \geq j$ there exist $\beta_{i,j+1},\dots,\beta_{i,r} \in \mathbb{Z}_p$ such that*

$$[h_i, h_j] = h_{j+1}^{\beta_{i,j+1}} \cdot \ldots \cdot h_r^{\beta_{i,r}}.$$

Proof. This is just the same as the argument used above for the special case of the Heisenberg group, if we note that condition (ii) expresses the requirement that $[h_i, h_j]$ should lie in the closed subgroup generated by $h_{j+1},\dots,h_r$. ■

Now comes a crucial observation: both conditions (i) and (ii) in this lemma can be expressed in the *first-order language of* $\mathbb{Z}_p$ ($\leadsto$ ***p*-adic integrals and logic**). This is clear for (i); for (ii) it depends on the fact both the group operations and the operation of taking powers (with a p-adic exponent) are given by *polynomials* with rational coefficients. This implies that each component of both the left-hand side and the right-hand side of the displayed equation in (ii) can be expressed as a polynomial in the components λ_{kl} of the vectors $h_i, \ldots, h_r$. Lemma 15.1.3 thus implies

Proposition 15.1.4 *The domain of integration $\mathcal{M}$ in Proposition 15.1.2 is a definable subset of* $\mathrm{Tr}(r, \mathbb{Z}_p)$.

Everything is now ready to apply the following theorem:

Theorem 15.1.5 [Denef 1984] *Let $\mathcal{M}$ be a definable subset of $\mathbb{Z}_p^m$ and let $h, k : \mathbb{Z}_p^m \to \mathbb{Z}_p$ be definable functions. Then*

$$\int_{\mathcal{M}} |h(x)|\,|k(x)|^s d\mu$$

is equal to a rational function over $\mathbb{Q}$ of p^{-s}.

(A function $h : \mathbb{Z}_p^m \to \mathbb{Z}_p$ is *definable* if its graph $\{(y, h(y)) \mid y \in \mathbb{Z}_p^m\}$ is a definable subset of $\mathbb{Z}_p^{m+1}$.) For some discussion of this fundamental result, see the ***p*-adic integrals and logic** window.

Theorem 15.3 now follows from this together with Propositions 15.1.2 and 15.1.4.

15.2 Alternative methods

We now describe some other proofs of Theorem 15.1. While most of them, in the end, come down to the same basic calculation, each illustrates a different approach to the problem of counting subgroups, and each can be generalized in its own way.

We recall the

Theorem

$$\zeta_{\mathbb{Z}^r}(s) = \zeta(s)\zeta(s-1)\ldots\zeta(s-r+1). \tag{15.10}$$

We first mention a corollary:

Corollary 15.2.1 *Let $\sigma(n)$ denote the sum of the divisors of n and $p(n)$ the number of partitions of n. Write $\Sigma(X) = \sum_{n=1}^{\infty} \sigma(n)X^n$ and $P(X) = 1 + \sum_{n=1}^{\infty} p(n)X^n$. Then*

$$\frac{\Sigma(X)}{X} = \frac{P'(X)}{P(X)}$$

Proof. In the notation of Chapter 14, we claim that $h_n(\mathbb{Z}^2) = p(n) \cdot n!$. Indeed, $\mathbb{Z}^2$ is the free abelian group on say x and y. The image of x in $\mathrm{Sym}(n)$ can be be any element of $\mathrm{Sym}(n)$. Once the image g of x is chosen, y can be mapped to any element of the centralizer $C(g)$ of g in $\mathrm{Sym}(n)$. Hence

$$h_n(\mathbb{Z}^2) = \sum_{g \in \mathrm{Sym}(n)} |C(g)| = \sum_{g \in \mathrm{Sym}(n)} \frac{|\mathrm{Sym}(n)|}{|[g]|}$$
$$= |\mathrm{Sym}(n)| \sum_{[g]} \frac{|[g]|}{|[g]|} = n!\, p(n)$$

where $[g]$ denotes the conjugacy class of g. Thus $b_n(\mathbb{Z}^2) = p(n)$ (notation of Section 14.2). On the other hand (15.10) says that $\zeta_{\mathbb{Z}^2}(s) = \zeta(s)\zeta(s-1) = (\sum 1 \cdot n^{-s})(\sum n \cdot n^{-s})$ which means that $a_n(\mathbb{Z}^2) = \sum_{d|n} 1 \cdot d = \sigma(n)$. Thus our corollary follows now from the discussion in Section 2 of Chapter 14. ■

This corollary is equivalent to the following well known partition identity

$$p(n) = \sum_{i=1}^{n} \frac{\sigma(i)}{n} p(m-i).$$

Just as happened in Chapter 14, the group theoretic approach gives a new proof for an old combinatorial identity. It will be be an interesting development if new identities can be found using subgroup-counting techniques.

Second proof of (15.10) [Grunewald, Segal & Smith 1988] This naive approach simply follows the proof that soluble groups of finite rank have polynomial subgroup growth; the easy structure of $\mathbb{Z}^r$ allows us to count subgroups exactly rather just estimate their number. Let $\Gamma = \mathbb{Z}^r$ and fix $Z < \Gamma$ with $Z \cong \mathbb{Z}$ and $\Gamma/Z \cong \mathbb{Z}^{r-1}$. To each pair (D, P) where $D \leq_f Z$ and $Z < P \leq_f \Gamma$ we associate the set

$$\mathcal{H}(D,P) = \{H \leq \Gamma \mid H \cap Z = D \ \text{ and } \ HZ = P\}.$$

Since P/Z is free abelian, the extension $Z/D \lhd P/D$ splits, and the number of complements is equal to

$$|\mathrm{Der}(P/Z, Z/D)| = |\mathrm{Hom}(P/Z, Z/D)| = |Z/D|^{r-1}$$

(see §1.3). So $|\mathcal{H}(D,P)| = |Z:D|^{r-1}$. Now every subgroup H of finite index in Γ belongs to precisely one of the sets $\mathcal{H}(D,P)$, and then

$$|\Gamma : H| = |\Gamma : P|\,|P : H| = |\Gamma : P|\,|Z : D|.$$

It follows that

$$\begin{aligned}\zeta_\Gamma(s) &= \sum_{P/Z\leq_f \Gamma/Z} \sum_{D\leq_f Z} \sum_{H\in\mathcal{H}(D,P)} |\Gamma : H|^{-s} \\ &= \sum_{P/Z\leq_f \Gamma/Z} |\Gamma : P|^{-s} \sum_{D\leq_f Z} |Z : D|^{-s} \, |\mathcal{H}(D,P)| \\ &= \sum_{P/Z\leq_f \Gamma/Z} |\Gamma/Z : P/Z|^{-s} \sum_{D\leq_f Z} |Z : D|^{r-1-s} \\ &= \zeta_{\Gamma/Z}(s)\zeta_Z(s-r+1).\end{aligned}$$

Since $\Gamma/Z \cong \mathbb{Z}^{r-1}$ and $Z \cong \mathbb{Z}$ our formula (15.10) now follows by induction on r.

The above proof is very explicit in the sense that we "construct" all subgroups of finite index in Γ from the subgroups of Z and Γ/Z. This method can be applied to some groups Γ that are nilpotent of class two, taking for Z the centre of Γ. However, we need to have some control over when the subgroup P/D actually splits over Z/D. The original determination of the zeta function of the Heisenberg group by [Smith 1983] used exactly this approach; with hindsight, one sees that the 'splitting conditions' amount to the same as the conditions that define the domain of integration in the proof given in the preceding section, while the 'summand' $|Z : D|^{-s} \, |\mathcal{H}(D,P)|$ corresponds to the integrand.

Third proof of (15.10) [Ilani 1989] This is an application of Hall's enumeration principle (↬ **Pro-p groups**). This says the following, where $\begin{bmatrix} d \\ t \end{bmatrix}$ denotes the number of subspaces of codimension t in $\mathbb{F}_p^d$:

Proposition 15.2.2 *Let G be a pro-p group, $\Phi = \Phi(G) = [G,G]G^p$ its Frattini subgroup and $d = d(G)$. For $1 \leq t \leq d$ let*

$$\left\{ K_{t,i} \mid i = 1, \ldots, \begin{bmatrix} d \\ t \end{bmatrix} \right\}$$

be the set of all subgroups K of G with $\Phi \leq K \leq G$ and $|G : K| = p^t$. Let $\mathcal{S}$ be a finite collection of proper subgroups of G and denote by $n(t,i)$ the number of $H \in \mathcal{S}$ such that $H \leq K_{t,i}$. Then

$$|\mathcal{S}| + \sum_{t=1}^{d} (-1)^t p^{t(t-1)/2} \sum_{i=1}^{\begin{bmatrix} d \\ t \end{bmatrix}} n(t,i) = 0.$$

Now take $G = \mathbb{Z}_p^r$ and let $\mathcal{S}$ be the set of all open subgroups of index p^n in G. Since each $K_{t,i} \cong G$ in this case, we have

$$n(t,i) = a_{p^{n-t}}(G)$$

for each t, hence the recursive formula

Corollary 15.2.3 *For $n \geq 1$,*

$$a_{p^n}(\mathbb{Z}_p^r) = \sum_{t=1}^{r} (-1)^{t+1} p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix} a_{p^{n-t}}(\mathbb{Z}_p^r).$$

Writing $c_n = a_{p^n}(\mathbb{Z}_p^r)$, with $c_n = 0$ for $n < 0$, and putting $f(X) = 1 + \sum_{n=1}^{\infty} c_n X^n$, .we can interpret this as a power series identity

$$f(X) - 1 = -\sum_{t=1}^{r} (-1)^t p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix} f(X) X^t.$$

Thus

$$\begin{aligned} f(X)^{-1} &= 1 + \sum_{t=1}^{r} (-1)^t p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix} X^t \\ &= (-1)^r p^{-r(r-1)/2} \sum_{j=0}^{r} (-1)^j p^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix} (p^{r-1}X)^{r-j} \end{aligned}$$

(putting $j = r - t$ and noting that $\begin{bmatrix} r \\ t \end{bmatrix} = \begin{bmatrix} r \\ j \end{bmatrix}$). Now the following identity was established in the course of proving Hall's principle (↬ **Pro-p groups**):

$$\prod_{j=0}^{r-1} (Y - p^j) = \sum_{j=0}^{r} (-1)^j p^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix} Y^{r-j}.$$

Putting $Y = p^{r-1}X$ we infer that

$$\begin{aligned} f(X)^{-1} &= (-1)^r p^{-r(r-1)/2} \prod_{j=0}^{r-1} (p^{r-1}X - p^j) \\ &= \prod_{j=0}^{r-1} (1 - p^{r-j-1}X). \end{aligned}$$

Thus

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

giving the Euler p-factor in (15.10).

This method of proof produces a recursive formula for $a_{p^n}(G)$. It works equally well for all pro-p groups G with the 'homogeneity' property that ζ_K depends only on the index of an open subgroup K in G. This is the case for the free pro-p groups, and we used the same method for these in Chapter 3. In fact, it is enough to assume that G has the following property: for every open subgroup H of G, $d(H) = f(|G : H|)$ depends only on the index of H in G. In this case G is said to be *f-indexed*, and the argument leading to Corollary 15.2.3 gives the following slightly surprising result:

Proposition 15.2.4 *If the pro-p group G is f-indexed then ζ_G is determined by the function f.*

Proof. One shows by induction on n that $a_{p^n}(G)$ depends only on f. Indeed, $a_{p^0}(G) = 1$, and if $n \geq 1$ then $a_{p^n}(G)$ is determined by the numbers $a_{p^{n-t}}(K)$ where $t \geq 1$ and K ranges over the subgroups $K_{t,i}$. Each $K_{t,i}$ is f_t-indexed, where $f_t(p^k) = f(p^{t+k})$ for all k, so inductively we may suppose that all the $a_{p^{n-t}}(K_{t,i})$ are determined by f_t, hence by f. Explicitly, $a_{p^n}(G) = a_{p^n}(f)$ where

$$a_{p^n}(f) = \sum_{t=1}^{r} (-1)^{t+1} p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix} a_{p^{n-t}}(f_t).$$

■

This applies for example to any extension G of $\mathbb{Z}_p$ by $\mathbb{Z}_p$, since clearly $d(H) = 2$ for every open subgroup H of G. The conclusion is that $\zeta_G = \zeta_{\mathbb{Z}_p^2}$; thus we obtain uncountably many pairwise non-isomorphic pro-p groups having the same zeta function. (Of these, however, only $\mathbb{Z}_p^2$ is nilpotent; it is not known if infinitely many f.g. nilpotent groups can have the same zeta function, nor even if two non-isomorphic torsion-free nilpotent pro-p groups can.)

The next proof differs from the others: instead of considering the subgroup structure of Γ it focuses on the structure of the *endomorphisms* of Γ. This approach, when generalized, leads to a rich theory that we mention below.

Fourth proof of (15.10) [Bushnell & Reiner 1980] Each finite index subgroup H of $\mathbb{Z}^r$ is of the form $H = \mathbb{Z}^r \cdot g$ where g is an integral $r \times r$ matrix of non-zero determinant, that is

$$g \in \mathrm{GL}_r^+(\mathbb{Q}) = \mathrm{M}_r(\mathbb{Z}) \cap \mathrm{GL}_r(\mathbb{Q}).$$

Further $\mathbb{Z}^r g_1 = \mathbb{Z}^r g_2$ if and only if $g_1 g_2^{-1} \in \mathrm{GL}_r(\mathbb{Z})$, and the index of $\mathbb{Z}^r g$ in $\mathbb{Z}^r$ is equal to $|\det(g)|$. Hence $\zeta_{\mathbb{Z}^r}(s) = \sum_g |\det(g)|^{-s}$ where g ranges over a complete set of representatives of the coset space $\mathrm{GL}_r(\mathbb{Z})\backslash\mathrm{GL}_r^+(\mathbb{Q})$. Such a set of coset representatives is given by the set T of integral upper-triangular matrices (a_{ij}) such that $a_{ij} = 0$ if $j > i$, $a_{ii} \geq 1$ for $i = 1, \ldots, r$ and $0 \leq a_{ij} < a_{jj}$ for $j < i$. (Of course, choosing a coset representative of this shape corresponds to choosing a good basis for the corresponding subgroup of $\mathbb{Z}^r$). The number of such matrices with given diagonal $(a_{11}, \ldots, a_{rr})$ is equal to $a_{22} a_{33}^2 \ldots a_{rr}^{r-1}$, while the determinant of each such matrix is $a_{11} a_{22} a_{33} \ldots a_{rr}$. Thus

$$\begin{aligned}
\zeta_{\mathbb{Z}^r}(s) &= \sum_{g \in T} |\det(g)|^{-s} \\
&= \sum_{a_{11}=1}^{\infty} \cdots \sum_{a_{rr}=1}^{\infty} a_{22}\, a_{33}^2 \ldots a_{rr}^{r-1} (a_{11} \ldots a_{rr})^{-s} \\
&= \left(\sum a_{11}^{-s}\right) \left(\sum a_{22}^{1-s}\right) \ldots \left(\sum a_{rr}^{r-1-s}\right) = \zeta(s)\zeta(s-1)\ldots\zeta(s-r+1).
\end{aligned}$$

If we try to generalize this proof to a wider class of groups we won't learn much about the corresponding zeta functions, since usually there are subgroups of finite index in Γ that are not isomorphic to Γ (in fact if Γ is nilpotent then it *must* be free abelian), and there is no such semi-group which takes the role of $\mathrm{GL}_r(\mathbb{Q}) \cap \mathrm{M}_r(\mathbb{Z})$ in the above proof. However, we do obtain information about the numbers $a_n^{\mathrm{iso}}(\Gamma)$ of subgroups of index n that are *isomorphic* to Γ. [Grunewald, Segal & Smith 1988] introduced the function

$$\zeta_\Gamma^{\mathrm{iso}}(s) = \sum a_n^{\mathrm{iso}}(\Gamma) n^{-s}$$

and calculated it for certain nilpotent groups Γ (of course $\zeta_\Gamma^{\mathrm{iso}} = \zeta_\Gamma$ when Γ is free abelian). Just as above, $\zeta_\Gamma^{\mathrm{iso}}(s)$ can in general be expressed as a sum over the cosets of $\mathrm{Aut}(\Gamma)$ in the semigroup $\mathrm{End}(\Gamma)$. However, this function is not usually very nice: for example it does not have an Euler product. As explained in the above-mentioned paper, $\zeta_\Gamma^{\mathrm{iso}}(s)$ is analogous the the zeta function of the principal ideal class in a number field.

A much better function appears if instead of the finitely generated nilpotent group Γ we consider its profinite completion $\widehat{\Gamma}$. Then

$$\widehat{\zeta}_\Gamma(s) := \zeta_{\widehat{\Gamma}}^{\mathrm{iso}}(s) = \prod_p \zeta_{\widehat{\Gamma}_p}^{\mathrm{iso}}(s)$$

does have an Euler product decomposition; it counts the number of subgroups H of index n in Γ such that $\widehat{H} \cong \widehat{\Gamma}$. The local factors are again rational functions of p^{-s}, and can be expressed as suitable p-adic integrals:

$$\begin{aligned} \zeta_{\widehat{\Gamma}_p}^{\mathrm{iso}}(s) &= \sum_{\mathbf{A}(\mathbb{Z}_p)\backslash \mathbf{A}^+(\mathbb{Q}_p)} |\det(g)|_p^s \\ &= \int_{\mathbf{A}^+(\mathbb{Q}_p)} \nu(\mathbf{A}(\mathbb{Z}_p)g)^{-1} \cdot |\det(g)|_p^s d\nu \end{aligned} \tag{15.11}$$

where $\mathbf{A}$ is a linear algebraic group such that $\mathbf{A}(\mathbb{Z}_p) \cong \mathrm{Aut}(\widehat{\Gamma}_p)$, $\mathbf{A}^+(\mathbb{Q}_p) = \mathrm{M}_r(\mathbb{Z}_p) \cap \mathbf{A}(\mathbb{Q}_p)$, and ν is a (multiplicative) Haar measure on $\mathbf{A}_r(\mathbb{Q}_p)$. The formula (15.11) in fact associates a 'local zeta function' $\zeta_{\mathbf{A},p}$ to any linear algebraic group $\mathbf{A}$, and such zeta functions have received a considerable amount of attention; see [Grunewald, Segal & Smith 1988], [du Sautoy & Lubotzky 1996], [du Sautoy (c)]. For example, when $\mathbf{A} = \mathcal{R}_{k/\mathbb{Q}}(\mathrm{GL}_1)$ is the multiplicative group of a number field k then $\zeta_{\mathbf{A},p}$ is exactly the product of the Euler $\mathfrak{p}$-factors of the Dedekind zeta function of k over primes $\mathfrak{p}$ dividing p. Following [Igusa 1989], [du Sautoy & Lubotzky 1996] establish both 'uniformity' and a 'local functional equation' for the functions $\zeta_{\mathbf{A},p}$, for an extensive class of algebraic groups $\mathbf{A}$; the latter is connected with certain symmetries in the associated root system.

Fifth proof of (15.10) [Mann 1996] We gave this in detail in Chapter 11, Section 11.5. It depends on two observations: the first is that the probability $P(G,k)$ that a random k-tuple in a pro-p group G generates G is given by

$$P(G,k) = \prod_{j=0}^{d-1}(1-p^{j-k})$$

where $d = d(G)$. The second is that a random k-tuple generates an open subgroup of G with probability 1 if k is big enough, provided G has polynomial subgroup growth.

The key fact now is that every open subgroup H of $\mathbb{Z}_p^r = G$ is isomorphic to G, hence satisfies $P(H,k) = P(G,k)$. Since the probability that a k-tuple in G generates H is $|G:H|^{-k} P(H,k)$, we may combine the above observations and deduce

$$\begin{aligned} 1 = \sum_{H \leq_o G} |G:H|^{-k} P(H,k) &= \zeta_G(k) P(G,k) \qquad (15.12) \\ &= \zeta_G(k) \prod_{j=0}^{d-1}(1-p^{j-k}). \end{aligned}$$

This holds for all large integers k, so using the identity theorem for power series we may infer that

$$\zeta_{\mathbb{Z}^r,p}(s) = \zeta_G(s) = \prod_{j=0}^{r-1}(1-p^{j-s})^{-1},$$

the desired Euler factor in (15.10).

An attractive feature of the method is that it seems to require hardly any calculation, and provides a satisfying conceptual explanation of the formula $\prod_{j=0}^{r-1}(1-p^{j-s})^{-1}$. Like the third proof, above, this approach may be useful when G is a pro-p group that is f-indexed for some function f, in which case $P(H,k)$ depends only on k and $|G:H|$ when H is open in G.

Avinoam Mann had the idea of using the equation (15.12) to *define* a new zeta function, for any profinite group G such that $P(G,k) > 0$ when k is large (that is, any PFG group, in the language of chapter 11). He conjectures that there should exist an analytic function $\zeta_G^{\mathrm{prob}}(s)$, 'naturally' associated to G, such that

$$\zeta_G^{\mathrm{prob}}(k) = P(G,k)^{-1} \quad \text{for all large } k \in \mathbb{N}.$$

The paper [Mann 1996] explains how ζ_G^{prob} is a subtle form of generating function for the growth of subgroups that are 'maximal intersections', and discusses some interesting cases. In particular, it is shown that when G is a finitely generated *prosoluble* group then ζ_G^{prob} really exists, that it has an Euler product, and that the p-local factor is rational in p^{-s} if G is virtually pro-(p-nilpotent). Thus for prosoluble groups G, the function $\zeta_G^{\mathrm{prob}}(s)$ is 'better' than $\zeta_G(s)$ in two respects: the latter does not usually have an Euler product, and it is only defined (convergent on a non-empty half-plane) when G has finite rank. There is a far-reaching theory here waiting to be discovered.

15.3 The zeta function of a nilpotent group

In this section we sketch some of the ideas behind Theorems 15.5 and 15.6. We shall be brief; a much fuller survey is given in Chapter 9 of [NH].

To find out more about the global zeta function ζ_Γ of a f.g. nilpotent group Γ, one has to analyse the local factors $\zeta_{\Gamma,p}$ in greater detail. Recall that in order to express $\zeta_{\Gamma,p}$ as an integral, we identified $\widehat{\Gamma}_p$ with $\mathbb{Z}_p^r$ by using a Mal'cev basis: the domain of integration $\mathcal{M} \subseteq \mathrm{Tr}(r, \mathbb{Z}_p)$ is then defined by some first-order conditions coming from the commutator operation in $\widehat{\Gamma}_p$. These conditions can become very complicated. Now there is another way to identify $\widehat{\Gamma}_p$ with $\mathbb{Z}_p^r$, arising from Lie theory, namely via the mapping log from $\widehat{\Gamma}_p$ to its Lie algebra ('co-ordinates of the first kind' as opposed to the 'co-ordinates of the second kind' that we introduced first). It turns out that in these new co-ordinates the definition of $\mathcal{M}$ is much cleaner.

Let us assume for simplicity that Γ is torsion-free. Then Γ may be identified with a subgroup of the upper unitriangular group $\mathrm{Tr}_1(m, \mathbb{Z})$ for some m, and the mapping

$$g \mapsto \log g = \sum_{n=1}^{m} \frac{(-1)^{n-1}}{n} (g-1)^n$$

sends Γ into the set $\mathrm{Tr}_0(m, \mathbb{Q})$ of upper-triangular matrices over $\mathbb{Q}$ with zero diagonal. This is a Lie algebra, with the operation $[a, b] = ab - ba$. The subset $\log \Gamma$ is not usually a Lie subring, or even an additive subgroup, of this Lie algebra; but there is a subgroup Γ_0 of finite index in Γ such that $L = \log \Gamma_0$ is indeed a Lie ring, and $L \cong \mathbb{Z}^r$ where r is the Hirsch length of Γ (for all this, see [Sg], Chapter 6). Moreover, it is shown in [Grunewald, Segal & Smith 1988] that for almost all primes p,

$$a_{p^n}(\Gamma) = a_{p^n}(L) \quad \text{for all } n,$$

where $a_{p^n}(L)$ is the number of Lie subrings of index p^n in L. Thus for such primes, we can determine the local zeta functions of Γ by studying instead the local zeta functions of L.

Now fix a prime p and identify $L \otimes \mathbb{Z}_p$ with $\mathbb{Z}_p^r$ by choosing a $\mathbb{Z}$-basis for L. The proof of Proposition 15.1.2 in Section 1, above, shows that

$$\zeta_{L,p}(s) = \frac{1}{(1-p^{-1})^r} \int_{\mathcal{M}} |\lambda_{11}|^{s-1} \cdot \ldots \cdot |\lambda_{rr}|^{s-r} \, d\mu$$

where $\mathcal{M}$ is now the subset of $\mathrm{Tr}(r, \mathbb{Z}_p)$ defined by a certain collection of *bilinear* equations, which express the requirement that the linear span of the rows of the matrix (λ_{ij}) be closed under the Lie bracket.

The upshot is that $\zeta_{L,p}(s)$ is given by what Grunewald and du Sautoy call a *cone integral*. The definition is as follows. Let $\mathcal{D} = (f_i, g_i \mid i = 1, \ldots, l)$ be a family of m-variable polynomials over $\mathbb{Q}$, and let $\psi_{\mathcal{D}}(\mathbf{x})$ be the statement

$$v(f_i(\mathbf{x})) \leq v(g_i(\mathbf{x})) \quad \text{for} \quad 1 \leq i \leq l,$$

where for a given prime p, one interprets v as the p-adic valuation. Put

$$V_p(\mathcal{D}) = \left\{ \mathbf{x} \in \mathbb{Z}_p^m \mid \psi_{\mathcal{D}}(\mathbf{x}) \text{ holds} \right\}.$$

The set $\mathcal{D}$ is called a set of *cone integral data*, and the *cone integral* defined by $\mathcal{D}$ is then

$$Z_D(s,p) = \int_{V_p(\mathcal{D})} |f_0(\mathbf{x})|_p \, |g_0(\mathbf{x})|_p^s \, d\mu$$

where as before μ is the normalized Haar measure on $\mathbb{Z}_p^m$.

We can now state

Proposition 15.3.1 *Let $L \cong \mathbb{Z}^r$ be a Lie ring. Then there is a set of cone integral data $\mathcal{D}$ such that*

$$\zeta_{L,p}(s) = a_{p,0}^{-1} Z_{\mathcal{D}}(s,p)$$

for all primes p, where each $a_{p,0} = Z_{\mathcal{D}}(\infty, p)$ is a non-zero constant.

It is important to note that the defining conditions coming from $\mathcal{D}$ are independent of the prime p.

Now the main result of [du Sautoy & Grunewald 2000] is

Theorem 15.3.2 *Let $\mathcal{D}$ be a set of cone integral data, and put*

$$Z_{\mathcal{D}}(s) = \prod_p a_{p,0}^{-1} Z_{\mathcal{D}}(s,p),$$

the product over all primes p. Then

(i) *$Z_D(s)$ is equal to a Dirichlet series with rational abscissa of convergence, α;*

(ii) *the function $Z_D(s)$ has a meromorphic continuation to the half-plane $\mathrm{Re}(s) > \alpha - \delta$ for some $\delta > 0$.*

From the above discussion we see that if Γ is any finitely generated nilpotent group, then $\zeta_\Gamma(s)$ differs from $Z_{\mathcal{D}}(s)$ in at most finitely many Euler factors. With some more work to deal with these 'bad' factors, one can then deduce Theorems 15.5 and 15.6 from Theorem 15.3.2.

The proof of this theorem has three main ingredients. The following sketch is not expected to be really comprehensible on its own; it is just meant to give an impression of the general circle of ideas.

(1) Using Denef's method of evaluating p-adic integrals by an explicit resolution of singularities, it is shown that for almost all primes p,

$$Z_{\mathcal{D}}(s,p) = a_{p,0} + \sum_{I \in \mathcal{S}} c_p(I) P_I(p, p^{-s}) \tag{15.13}$$

where $\mathcal{S}$ is a certain finite collection of (Boolean combinations of) algebraic varieties defined over $\mathbb{Z}$, $c_p(I)$ denotes the number of $\mathbb{F}_p$-points on the reduction

modulo p of I, and each $P_I(X,Y)$ is a rational function of two variables over $\mathbb{Q}$, of a simple and explicit form. This very interesting result shows that the question of 'uniformity' for our local zeta functions as the prime varies is intimately related to the corresponding question for the numbers $c_p(I)$; this links the group-theoretic zeta function in an explicit way to the Weil zeta functions of certain algebraic varieties.

(2) Using the Lang-Weil estimate for the numbers of points on varieties over finite fields, together with (15.13), including the explicit form of the functions $P_I(X,Y)$, it is shown that $a_{p,0}^{-1} Z_{\mathcal{D}}(s,p)$ can be determined to a good approximation in terms of expressions like

$$1 + l_p(U) \frac{p^{-s}}{1-p^{-s}}, \tag{15.14}$$

where U runs over certain irreducible $\mathbb{Q}$-varieties and $l_p(U)$ encodes the number of *absolutely irreducible* components of the reduction modulo p of U.

(3) Now the absolutely irreducible components over $\mathbb{Q}$ of the varities U that arise in (2) are all defined over some finite Galois extension field K of $\mathbb{Q}$, and the Galois group permutes these components, according to some permutation representation ρ. To these data is associated an *Artin L-function* $L(s,\rho,K/\mathbb{Q})$. The final step is to show that

$$\frac{\prod_p \left(1 + l_p(U) \frac{p^{-s}}{1-p^{-s}}\right)}{L(s,\rho,K/\mathbb{Q})}$$

is finite for all $s > 1-\delta$, for some $\delta > 0$.

The classical work of Artin shows that $L(s,\rho,K/\mathbb{Q})$ has a meromorphic continuation to the left of $\mathrm{Re}(s) = 1$. The same therefore holds for Euler products of factors like (15.14), and this when fed back into Step (2) is enough to establish (ii) in Theorem 15.3.2. The proof of (i) is a little simpler: it is possible to determine the abscissa of convergence of $\prod_p a_{p,0}^{-1} Z_{\mathcal{D}}(s,p)$ directly from the formula (15.13), with the help of the Lang-Weil estimates.

This analysis has an interesting moral. While the local factors of our zeta function in general vary wildly with the prime, as do the solution-numbers $c_p(I)$, the analytic behaviour of the global zeta function mimics that of a classical Artin L-function, whose own Euler factors vary quite uniformly with the prime - that is, they take only finitely many distinct forms depending on the decomposition of the prime in the number field. Thus the uniformity proposal of [Grunewald, Segal & Smith 1988] mentioned in the introductory section, while false as stated, is sort of true in an asymptotic sense.

Note, finally, that Proposition 15.3.1 makes no mention of nilpotency: it applies to any Lie ring over $\mathbb{Z}$, in fact to *any* $\mathbb{Z}$-algebra structure (not necessarily Lie or associative) on $\mathbb{Z}^r$; and the local version applies similarly to any $\mathbb{Z}_p$-algebra structure on $\mathbb{Z}_p^r$. It follows that the corresponding local zeta functions

are rational in p^{-s}. All the problems mentioned in the introduction apply equally in this new context, and equally little is known about them. A particularly interesting project is to investigate these rational functions for the 'simple' Lie algebras such as $\mathfrak{sl}(d,\mathbb{Z})$; a first step in this direction is taken in [Ilani 1999], [du Sautoy 2000] and [du Sautoy & Taylor], where it is shown that for $L = \mathfrak{sl}(2,\mathbb{Z})$,

$$\zeta_L(s) = \zeta(s)\zeta(s-1)\zeta(2s-1)\zeta(2s-2)\prod_{p\neq 2}(1-p^{1-3s})\cdot(1+3\cdot 2^{1-2s}-2^{3-3s}).$$

Notes

Most of the sources have been mentioned in the main text; here is a résumé.

The definition of the zeta function for a torsion-free f.g. nilpotent group, the Euler product, and the rationality of the local factors were given in [**Grunewald, Segal & Smith 1988**]. This paper also considers (a) zeta functions of rings, showing that ζ_G and ζ_L differ in at most finitely many local factors when L is the Lie ring associated to a nilpotent group G; (b) zeta functions associated to algebraic groups.

These latter zeta functions are studied in depth by [**du Sautoy & Lubotzky 1996**], who establish 'uniformity' and a local functional equation in many cases, generalizing fundamental work of [**Igusa 1989**]. A sequel by du Sautoy is in preparation.

Theorems 15.5, 15.6 and 15.7 are due to [**du Sautoy & Grunewald 2000**].

The following works determine the zeta functions for various specific classes of groups and/or rings: [**Ilani 1989**], [**du Sautoy 2000**], [**du Sautoy, McDermott & Smith 1999**], [**du Sautoy & Taylor**], [**Klopsch (b)**], [**Taylor 2001**]. A general approach to constructing nilpotent groups whose zeta functions are related to elliptic curves is developed in the recent works [**du Sautoy (a)**], [**Griffin 2002**] and [**Voll 2002**]; the latter work of Voll also establishes a number of cases of 'uniformity' and of local functional equations.

More theoretical developments are to be found in a series of forthcoming papers of du Sautoy and of du Sautoy & Grunewald. For further references see the survey articles [**du Sautoy & Segal 2000**], which appears in [**NH**], and [**du Sautoy (d)**]. The final section of the latter presents most of the local zeta functions for which an explicit formula is known.

A different kind of generating function can be associated to the family of finite index subgroups of a group. For a finitely generated group G, [**Larsen (2001)**] defines

$$Z(G,s) = \sum e(n)n^{-s}$$

where $e(n)$ is 1 if G has a subgroup of index n and 0 otherwise. Larsen shows that the abscissa of convergence of this series is equal to $1/d$ where d is the smallest possible dimension of the Zariski closure of some linear representation of G with infinite image (if no such representation exists then the abscissa is zero).

Chapter 16

Zeta functions II: p-adic analytic groups

As we saw in the last chapter, the arithmetic of subgroup growth in a finitely generated nilpotent group Γ can be studied 'locally': on the one hand, the sequence $(a_n(\Gamma))$ is determined in a simple way by the numbers $a_{p^j}(\Gamma)$ (for all prime-powers p^j); on the other hand, for each fixed prime p the sequence $(a_{p^j}(\Gamma))$ satisfies a linear recurrence relation: in other words, the *local zeta function*

$$\zeta_{\Gamma,p}(s) = \sum_{j=0}^{\infty} \frac{a_{p^j}(\Gamma)}{p^s}$$

is a rational function in the variable p^{-s}. The first, 'global', property is a special feature of nilpotent (or more generally pronilpotent) groups. The second, 'local', one, however, holds in much greater generality. In this chapter we give a brief account of the results, some of the ideas behind them, and some remarkable applications to the enumeration and classification of finite p-groups. For more information, see the detailed survey article [du Sautoy & Segal 2000] and the original papers [du Sautoy 1993], [du Sautoy 2000].

The common theme underlying all the results of this chapter is the subgroup growth of *compact p-adic analytic groups*. We recall that a topological group is compact and p-adic analytic if and only if (i) it is a profinite group of finite rank and (ii) it is virtually a pro-p group; this holds if and only if it contains an open subgroup that is a uniform pro-p group. For the definition and properties of these groups, see the **Pro-p groups** window. The first main theorem is

Theorem 16.1 *Let G be a compact p-adic analytic group. Then $\zeta_{G,p}(s)$ and $\zeta^{\triangleleft}_{G,p}(s)$ are rational functions over $\mathbb{Q}$ of p^{-s}.*

If Γ is an abstract group then the pro-p completion $G = \widehat{\Gamma}_p$ of Γ has finite rank if and only if Γ has finite upper p-rank. Since $a_{p^j}(G) = a^{\triangleleft\triangleleft}_{p^j}(\Gamma)$, the

theorem implies that $\zeta^{\triangleleft\triangleleft}_{\Gamma,p}(s) = \zeta_{G,p}(s)$ is rational in p^{-s} provided Γ has finite upper p-rank. With a little more work it is also possible to deduce

Corollary 16.2 *Let Γ be a group with finite upper p-rank. Then $\zeta_{\Gamma,p}(s)$ and $\zeta^{\triangleleft}_{\Gamma,p}(s)$ are rational functions over $\mathbb{Q}$ of p^{-s}.*

Of course, compact p-adic analytic groups arise in other ways; Theorem 16.1 raises the interesting challenge of determining the rational functions associated to groups such as the congruence subgroups of $\mathrm{SL}_d(\mathbb{Z}_p)$, which are very far from nilpotent. Beyond the case of $\mathrm{SL}_2(\mathbb{Z}_p)$ this project is still wide open.

In order to prove Theorem 16.1, du Sautoy established a very general rationality theorem for integrals defined over a uniform pro-p group. This is explained in Section 1; it depends on work of Denef and van den Dries in 'analytic' p-adic model theory. The deduction of Theorem 16.1 and Corollary 16.2 is given in Section 2.

du Sautoy's rationality theorem is so general that it can be applied not only to the familiar subgroup-counting zeta functions, in the spirit of Chapter 15, but also to various 'modified' zeta functions. For example, one can encode in such a zeta function the number of orbits, under some acting group, of subgroups of index p^j in G that satisfy some 'definable' condition. This method has wide scope, and we describe some of its applications in Sections 3 and 4.

Higman and Sims showed in the 1960s that the number of (isomorphism types of) groups of order p^n is about $p^{(2/27)n^3}$, and we have seen in Chapter 3 that for a fixed d, the number of *d-generator* groups of order p^n grows like $p^{\gamma n^2}$ (where γ depends on d). Now let

$$f(n, p, c, d)$$

denote the number of d-generator groups of order p^n and *nilpotency class at most c* (up to isomorphism). This number is certainly bounded above by $a^{\triangleleft}_{p^n}(F)$ where F is the free nilpotent-of-class-c pro-p group on d generators, hence it is at most *polynomial* in p^n (because F is a pro-p group of finite rank).

Theorem 16.3 *For fixed c, d and p and sufficiently large n, the function $n \mapsto f(n, p, c, d)$ satisfies a linear recurrence relation over $\mathbb{Z}$.*

A major inroad into the classification of finite p-groups has been the beautiful coclass theory, developed by Leedham-Green, Newman and others. A group of order p^n has *coclass* r when its nilpotency class is $n - r$. Let

$$c(n, p, r)$$

denote the number of groups of order p^n and coclass r (up to isomorphism). This number is also polynomially bounded in terms of p^n (this is not at all obvious!), and we have the analogous

Theorem 16.4 *For fixed r and p and sufficiently large n, the function $n \mapsto c(n,p,r)$ satisfies a linear recurrence relation over $\mathbb{Z}$.*

These are very striking results: the class of finite p-groups has traditionally been considered too 'wild' for classification, yet here we see very regular patterns, established by model-theoretic methods applied in a subgroup-growth context.

The next result is even more striking; to explain it we need to recall the main conclusion of coclass theory. This says that for each fixed prime p and natural number r, almost all finite p-groups of coclass r can be arranged into finitely many 'families'. Each family is represented by a rooted tree that contains exactly one infinite path (the 'trunk'). Each vertex of the tree represents one group, and there is an edge from G to H if and only if there is an epimorphism from G onto H with central kernel of order p. For accounts of this theory, see [Leedham-Green & McKay 2000] and [DDMS], Chapter 10. Now, extensive computer calculations by Newman and O'Brien for the case $p = 2$ led them to some delicate conjectures about the shape of these trees. One of these is

Conjecture P ($p = 2$) Each of the trees of coclass-r 2-groups is eventually periodic, with period dividing 2^{r-1}.

This means the following. Let $\mathfrak{T}$ be a tree with trunk $(P_0, P_1, \ldots, P_n, \ldots)$; removing the edge between P_{n-1} and P_n divides $\mathfrak{T}$ into two connected components, one finite and one infinite. The infinite one is denoted $\mathfrak{T}_n$. The conjecture asserts that for all sufficiently large n, the trees $\mathfrak{T}_n$ and $\mathfrak{T}_{n+2^{r-1}}$ are isomorphic.

It is known that this periodicity fails for primes $p \neq 2$. However, there is a modified version. For a natural number m, let $\mathfrak{T}[m]$ denote the subtree of $\mathfrak{T}$ consisting of all vertices of $\mathfrak{T}$ having distance at most m from the trunk (and the corresponding edges); so $\mathfrak{T}[m]$ is a 'pruned' version of $\mathfrak{T}$. It is known that when $p = 2$ there exists a finite m such that $\mathfrak{T} = \mathfrak{T}[m]$; hence the following theorem, valid for all primes, implies the qualitative statement of Conjecture P (though not the actual period):

Theorem 16.5 *Let $\mathfrak{T}$ be one of the infinite rooted trees of p-groups of a fixed coclass, and let $m \in \mathbb{N}$. Then the tree $\mathfrak{T}[m]$ is eventually periodic.*

All of these theorems about finite p-groups are proved by establishing the rationality of suitable 'modified' local zeta functions. du Sautoy has also established some results of a 'global' flavour, by showing that the generating Dirichlet series for the function $f(n,p,c,d)$ can be represented as a *cone integral*, in the sense of Chapter 15, Section 3. We shall not go into this further, but state one of the conclusions:

Theorem 16.6 *Let $g(n,c,d)$ denote the number of isomorphism types of d-generator nilpotent groups of class at most c and order at most n. Then for fixed c and d,*

$$g(n,c,d) \sim \gamma n^{\alpha} (\log n)^{\beta}$$

as $n \to \infty$, for some real $\gamma > 0$, rational $\alpha > 0$ and integer $\beta \geq 0$.

The theory of cone integrals also sheds some light on the question of how $f(n,p,c,d)$ varies with the prime p, for fixed c, d and n, a problem raised by Higman in 1960; see [du Sautoy 2000].

These results represent a new kind of application for the arithmetic theory of subgroup growth, one that shows great promise for the future.

16.1 Integration on pro-p groups

In this section we consider a *uniform pro-p group* G. Writing $G = G_1 > \Phi(G) = G_2 > G_3 > \ldots$ for the lower central p-series of G, this means that (i) G/G^p is abelian (G/G^4 is abelian if $p = 2$) and (ii) each of the factors G_i/G_{i+1} is elementary abelian of rank d ($\rightsquigarrow$ **Pro-p groups**). For $g \in G$, define

$$\omega(g) = n \text{ if } g \in G_n \setminus G_{n+1}$$
$$\omega(1) = \infty.$$

The first-order language $\mathcal{L}_G$ has two sorts of variables: those of sort x, interpreted as elements of G, and those of sort λ, interpreted as elements of $\mathbb{Z}_p$; function symbols x^{-1}, $x \cdot y$, x^λ, and $\phi_\alpha(x)$ ($\alpha \in \mathbb{N}$), the latter to be interpreted as certain fixed automorphisms of G; a binary relation symbol interpreted as $\omega(x) \geq \omega(y)$; and constant symbols of the first sort, representing fixed elements of G. A subset $\mathcal{M}$ of $G^{(r)}$ is *definable* if there is a formula $\kappa(x_1, \ldots, x_r)$ of $\mathcal{L}_G$, containing exactly r free variables of the first sort, such that

$$\mathcal{M} = \{(g_1, \ldots, g_r) \mid \kappa(g_1, \ldots, g_r) \text{ is true}\}.$$

A function $\psi : G^{(r)} \to G$ is definable if its graph $\{(\mathbf{g}, \psi(\mathbf{g})) \mid \mathbf{g} \in G^{(r)}\}$ is a definable subset of $G^{(r+1)}$. Finally, a function $f : G^{(r)} \to \mathbb{Z}$ is said to be *simple* if there exist definable functions $\psi_1, \ldots, \psi_m : G^{(r)} \to G$ and integers $a_1, \ldots, a_m$ such that

$$f(g_1, \ldots, g_r) = \sum_{i=1}^{m} a_i \omega(\psi_i(g_1, \ldots, g_r))$$

for all $g_1, \ldots, g_r \in G$.

We can now state du Sautoy's rationality theorem:

Theorem 16.1.1 *Let G be a uniform pro-p group, let $\mathcal{M}$ be a definable subset of $G^{(r)}$ and let $h, k : G^{(r)} \to \mathbb{Z}$ be simple functions. Then*

$$Z(h,k,\mathcal{M},s) = \int_{\mathcal{M}} p^{-sh(x)} p^{-k(x)} d\mu(x)$$

is equal to a rational function over $\mathbb{Q}$ of p^{-s}.

Here, μ denotes the normalized Haar measure on $G^{(r)}$. The theorem is proved by introducing p-adic co-ordinates on G, translating everything into the 'analytic' language of $\mathbb{Q}_p$ introduced by [Denef & van den Dries 1988], and then applying their correponding rationality theorem ($\rightsquigarrow$ **p-adic integrals and logic**,

Theorem 3). The possibility of making this translation depends on Lazard's theory, which implies that the group operations (including the taking of p-adic powers) can be expressed in terms of suitable power series; see [DDMS].

16.2 Counting subgroups in a p-adic analytic group

Now let G be a compact p-adic analytic group. Then G has an open characteristic subgroup G_1 that is a uniform pro-p group, of dimension d, say ($\rightarrowtail$ **Pro-p groups**). Write G_i for the ith term of the lower p-central series of G_1. In order to count the open subgroups of G, we want to associate to each such subgroup a 'good basis', in the spirit of Chapter 15, Section 1.

Fix a subgroup K of p-power index in G with $K \geq G_1$, and fix a transversal $\{y_1 = 1, y_2, \ldots, y_l\}$ to the right cosets of G_1 in K. Let H be an open subgroup of G such that $G_1 H = K$, and put $H_i = H \cap G_i$ for each i. Since H is open, there exists m such that $H_m = G_m$. We start by defining a *good basis* for H_1: this is a d-tuple $(h_1, \ldots, h_d)$ in G_1 such that

$$\omega(h_1) \leq \omega(h_2) \leq \ldots \leq \omega(h_d),$$

and such that for each $n \leq m$ the set

$$\left\{ h_i^{p^{n-\omega(h_i)}} G_{n+1} \mid 1 \leq i \leq d,\ \omega(h_i) \leq n \right\}$$

is a basis for the $\mathbb{F}_p$-vector space $H_n G_{n+1}/G_{n+1}$. Now a tuple $(h_1, \ldots, h_d, t_1, \ldots, t_l) \in G_1^{(d+l)}$ is called a *basis* for H if

(i) $(h_1, \ldots, h_d)$ is a good basis for H_1, and

(ii) $\{t_1 y_1, t_2 y_2, \ldots, t_l y_l\}$ is a transversal to the right cosets of H_1 in H.

Let $\mathcal{M}(H_1)$ denote the set of all good bases for H_1, and $\mathcal{K}(H)$ the set of all bases for H. Then

$$\mu(\mathcal{K}(H)) = |G_1 : H_1|^{-l}\, \mu(\mathcal{M}(H_1))$$

where μ denotes the normalized Haar measure on G_1 (because each t_i in (ii) can vary over exactly one left coset of H_1 in G_1). The measure of $\mathcal{M}(H_1)$ depends on just how the index $|G_1 : H_1|$ splits up into its factors $|G_i : H_i G_{i+1}|$; this is encoded by a certain partition $P = P_{H_1}$ of d, and the result is

$$\mu(\mathcal{M}(H_1)) = q_P \cdot p^{d^2 + \sum (1-2i)\omega(h_i)}$$

where $q_P = \prod_{t \in P} \prod_{j=1}^{t} (1 - p^{-j})$, and $(h_1, \ldots, h_d)$ is any element of $\mathcal{M}(H_1)$. Also

$$\begin{aligned} |G_1 : H_1| &= \prod_{i=1}^{m} |G_i : H_i G_{i+1}| \\ &= p^{d - \omega(h_1) - \cdots - \omega(h_d)}. \end{aligned}$$

Now let $\mathcal{H}_{K,P}$ denote the set of all open subgroups H of G such that (a) $G_1H = K$ and (b) the partition P_{H_1} is equal to P. There are finitely many possibilities for K and for P, and

$$\zeta_{G,p}(s) = \sum_{K,P} \sum_{H \in \mathcal{H}_{K,P}} |G : H|^{-s}.$$

Put

$$\mathcal{K}_{K,P} = \bigcup_{H \in \mathcal{H}_{K,P}} \mathcal{K}(H).$$

Then $\sum_{H \in \mathcal{H}_{K,P}} |G : H|^{-s}$ is equal to $|G : K|^{-s}$ times

$$\begin{aligned}
&\sum |G_1 : H_1|^{-s} \, \mu(\mathcal{K}(H))^{-1} \int_{\mathcal{K}(H)} d\mu \\
&= \int_{\mathcal{K}_{K,P}} \mu(\mathcal{K}(H))^{-1} \cdot p^{(\omega(h_1)+\cdots+\omega(h_d)-d)s} d\mu \\
&= q_P^{-1} \int_{\mathcal{K}_{K,P}} p^{(d-\omega(h_1)-\cdots-\omega(h_d))l} p^{\sum (2i-1)\omega(h_i)-d^2} p^{(\omega(h_1)+\cdots+\omega(h_d)-d)s} d\mu \\
&= q_P^{-1} p^{dl-d^2-ds} \cdot Z(h, k, \mathcal{K}_{K,P}, s)
\end{aligned}$$

in the notation of the previous section, where h and k are certain *simple functions*. The essential point now is that each of the sets $\mathcal{K}_{K,P}$ is *definable* as a subset of $G_1^{(d+l)}$, in the language $\mathcal{L}_{G_1}$. It follows by Theorem 16.1.1 that each $Z(h, k, \mathcal{K}_{K,P}, s)$ is a rational function of p^{-s}. Therefore so is $\zeta_{G,p}(s)$.

More generally, let $\mathcal{X}$ be a subset of the set of all open subgroups of p-power index in G. We say that $\mathcal{X}$ is *definable* if each of the sets

$$\mathcal{K}_{K,P}^{\mathcal{X}} = \bigcup_{H \in \mathcal{H}_{K,P} \cap \mathcal{X}} \mathcal{K}(H)$$

is definable; this will hold if membership of $\mathcal{X}$ for an open subgroup H can be expressed as a statement in $\mathcal{L}_{G_1}$, applied to any basis for H. In this case, the above argument yields the conclusion that

$$\zeta_{G,p}^{\mathcal{X}}(s) = \sum_{H \in \mathcal{X}} |G : H|^{-s}$$

is a rational function of p^{-s}. This applies in particular when $\mathcal{X}$ is the family of all open *normal* subgroups of p-power index in G, showing that $\zeta_{G,p}^{\triangleleft}(s)$ is a rational function. This concludes our sketch of the proof of Theorem 16.1.

To deduce Corollary 16.2, let Γ be a group of finite upper p-rank; assume without loss of generality that Γ is residually finite. By the *Remark* in Section 5

of Chapter 5, Γ has a normal subgroup Γ_0 of finite index such that every finite quotient of Γ_0 has a normal p-complement. Now let

$$G = \varprojlim \{\Gamma/N \mid N \lhd \Gamma,\ N \leq \Gamma_0 \text{ and } \Gamma_0/N \text{ is a finite } p\text{-group}\}. \qquad (16.1)$$

Thus G is a profinite group, and it is easy to see that the closure in G of Γ_0 is the pro-p completion of Γ_0. Hence G is virtually a pro-p group of finite rank, hence a p-adic analytic group. Moreover, if H is a subgroup of p-power index in Γ then $H \cap \Gamma_0$ contains one of the normal subgroups N in (16.1), which implies that $\left|G : \overline{H}\right| = |\Gamma : H|$ where $\overline{H}$ denotes the closure of H in G. Thus $H \mapsto \overline{H}$ is an index-preserving bijection between the family of all subgroups of p-power index in Γ and the family of all open subgroups of p-power index in G, and it follows that

$$\zeta_{\Gamma,p}(s) = \zeta_{G,p}(s),\ \zeta^{\lhd}_{\Gamma,p}(s) = \zeta^{\lhd}_{G,p}(s)$$

(note that $H \lhd \Gamma$ if and only if $\overline{H} \lhd G$).

16.3 Counting orbits

We keep the notation of the last section, so G is a compact p-adic analytic group, and let A denote some fixed group of automorphisms of G. Now let $\mathcal{X}$ be a definable and A-invariant family of open subgroups of G, and let $b_{p^n}(\mathcal{X}/A)$ denote the number of orbits under the action of A on

$$\{H \in \mathcal{X} \mid |G : H| = p^n\}.$$

The following generalizes Theorem 16.1:

Theorem 16.3.1 *The function*

$$\zeta_{\mathcal{X}/A}(s) = \sum_{n=0}^{\infty} b_{p^n}(\mathcal{X}/A)p^{-ns}$$

is a rational function over $\mathbb{Q}$ of p^{-s}.

For example, taking A to be the group of all inner automorphisms of G and $\mathcal{X}$ to be the set of all open subgroups of G, we deduce that the number of *conjugacy classes* of open subgroups of index p^n in G satisfies a linear recurrence relation, for sufficiently large n. On the other hand, taking $A = \mathrm{Aut}(G)$, we shall see in the following section how this can be applied to the enumeration of isomorphism types of finite p-groups.

The proof of Theorem 16.3.1 depends on the fact that $\mathrm{Aut}(G)$ is itself again a compact p-adic analytic group ([DDMS], Chapter 5). It is easy to see that the numbers $b_{p^n}(\mathcal{X}/A)$ are unchanged if we replace $A \leq \mathrm{Aut}(G)$ by its closure in $\mathrm{Aut}(G)$, so we may assume that A is in fact closed; then A is also a compact p-adic analytic group. Thus A contains an open normal uniform pro-p subgroup

A_1; we may choose A_1 and the characteristic open uniform subgroup G_1 of G so that

$$\mathfrak{G} = G_1 \rtimes A_1$$

is a uniform pro-p group. Now

$$\begin{aligned}\sum b_{p^n}(\mathcal{X}/A)p^{-ns} &= \sum_{H\in\mathcal{X}} |G:H|^{-s} \cdot |A : \mathrm{N}_A(H)|^{-1} \\ &= \sum_{H,X} |A:X|^{-1}\,|G:H|^{-s}\end{aligned}$$

where the second sum ranges over pairs (H, X) where $H \in \mathcal{X}$ and $X = \mathrm{N}_A(H) \leq A$. The heart of the proof now consists in showing that this sum can be interpreted as a finite sum of integrals over subsets of $\mathfrak{G}^{(m)}$, where the domain of integration is definable in the language $\mathcal{L}_{\mathfrak{G}}$ and the integrand involves simple functions in the sense of $\mathcal{L}_{\mathfrak{G}}$. The theorem is thus reduced to an application of Theorem 16.1.1.

16.4 Counting p-groups

The link between subgroup growth and the enumeration of finite groups is provided by the following elementary fact:

Proposition 16.4.1 ([FJ], Prop. 15.31) *Let $\mathcal{C}$ be a class of finite groups closed under taking subgroups, quotients and direct products, and let F be a free pro-$\mathcal{C}$ group. Let M, N be open normal subgroups of F. Then $F/M \cong F/N$ if and only if there exists an automorphism ψ of F such that $\psi(M) = N$.*

For our first application, take $\mathcal{C}$ to be the class of finite p-groups of nilpotency class at most c, and let F be the free pro-$\mathcal{C}$ group on d generators. Then every d-generator finite p-group of class at most c appears as a quotient F/N, and the proposition shows that the number $f(n, p, c, d)$ of isomorphism classes of such groups of order p^n is equal to the number $b_{p^n}(\mathcal{X}/A)$ of orbits of $A = \mathrm{Aut}(F)$ acting on the set $\{H \in \mathcal{X} \mid |G : H| = p^n\}$, where now $\mathcal{X}$ denotes the set of all open normal subgroups in F. Also F is a pro-p group of finite rank (↬ **Pro-p groups**). Applying Theorem 16.3.1 we deduce that

$$\sum_{n=0}^{\infty} f(n, p, c, d)p^{-ns}$$

is a rational function of p^{-s}, and Theorem 16.3 follows.

If we want to enumerate groups of fixed *coclass*, we come up against the problem that there is no corresponding relatively-free profinite group. However, the following theorem, the main result of coclass theory, goes some way to saving the situation:

Proposition 16.4.2 [Leedham-Green 1994], [Shalev 1994] *For each prime p and integer $r \geq 1$ there exists $h = h(p, r)$ such that every finite p-group of coclass r contains a normal subgroup of index at most p^h that is nilpotent of class 2 (abelian if $p = 2$).*

Suppose now that P is a finite group of coclass r and order p^n. Then $|\gamma_i(P) : \gamma_{i+1}(P)| \geq p$ for $1 \leq i \leq n - r$, so $|\gamma_2(P)| \geq p^{n-r-1}$ and hence $|P : \gamma_2(P)| \leq p^{r+1}$. Therefore $d(P) \leq r + 1$, and so P is an image of the free pro-p group F on $r + 1$ generators. Also, the proposition implies that

$$\gamma_3(\gamma_h(P)P^{p^h}) = 1. \tag{16.2}$$

Putting

$$U = F/\gamma_3\left(\gamma_h(F)F^{p^h}\right),$$

we see that every finite p-group of coclass r is isomorphic to a quotient of U. Now U is a free pro-$\mathcal{C}$ group where $\mathcal{C}$ is the class of all finite p-groups P satisfying (16.2), and it is easy to see that U is a pro-p group of finite rank. However, not all the finite images of U have coclass r; let $\mathcal{X}$ denote the set of those open normal subgroups N of U such that the coclass of U/N is exactly r. Then just as before we see that the number $c(n, p, r)$ of isomorphism classes of groups of order p^n and coclass r is equal to $b_{p^n}(\mathcal{X}/A)$ where $A = \mathrm{Aut}(U)$.

Applying Theorem 16.3.1, we may deduce that the function

$$\sum_{n=0}^{\infty} c(n, p, r)p^{-ns}$$

is rational in p^{-s}, *provided* we can show that the family $\mathcal{X}$ of open normal subgoups of U is *definable*. This of course requires more work; the key fact here is that one can determine whether a group P has coclass r in a uniformly bounded number of steps, because of the following result:

Proposition 16.4.3 [Shalev 1994] *Let P be a finite p-group. Then P has coclass r if and only if $P/\gamma_f(P)$ has coclass r, where $f = 2p^r$ if p is odd, $f = 2^{r+3}$ if $p = 2$.*

This concludes our sketch of the proof of Theorem 16.4.

The proof of Theorem 16.5, regarding the shape of a tree, is naturally more subtle. Again, this comes down to establishing the rationality of a certain generating function, one that encodes the number of subgroups in $\mathcal{X}$ that belong to a 'twig' of each specified shape: the *twigs* are the connected components that remain when the trunk is deleted from the tree. The periodicity of the ('pruned') tree is then deduced with the help of the following elementary lemma:

Lemma 16.4.4 *Let (c_n) be a sequence where each c_n is either 0 or 1. If the sequence satisfies a linear recurrence relation, then it is eventually periodic.*

For details, see [du Sautoy & Segal 2000] and [du Sautoy 2000].

Notes

Again, we have mentioned most of the sources in the main text.

Theorem 16.1 and the material of §§16.1, 16.2 are from [**du Sautoy 1993**].

The remaining main theorems, and the material of §§16.1, 16.2, are from [**du Sautoy 2000**]; see also the announcement [**du Sautoy 1999**].

[**Ilani 1999**] determines zeta functions associated to the group $\mathrm{SL}_2(\mathbb{Z}_p)$. The zeta functions associated to various Lie rings over $\mathbb{Z}_p$ are determined in [**Klopsch (b)**] and [**Taylor 2001**].

Window: Finite group theory

In this window, all groups are assumed finite. Here we collect a number of results that play a significant role in the book (further material of an elementary nature that we sometimes take for granted is easily available in textbooks such as [H], [R] and [A]).

1 Hall subgroups and Sylow bases

(See [R], Chapter 9 or [H], Chapter VI.)

A subgroup H of a group G is a *Hall π-subgroup* (where π is a set of primes) if $|H|$ is a product of primes in π and $|G : H|$ is divisible by no prime in π. When p is a prime, a Hall p'-subgroup is called a *p-complement* (where p' denotes the the set of all primes distinct from p).

Theorem 16.4.5 (P. Hall) *The following are equivalent for a group G.*

(i) G is soluble;

(ii) G has a p-complement for every prime p dividing $|G|$;

(iii) G has a Hall π-subgroup for every set of primes π;

(iv) for every set of primes π, every π-subgroup of G is contained in a Hall π-subgroup, and all Hall π-subgroups are conjugate in G.

Let p_i $(i = 1, \ldots, k)$ be the prime factors of $|G|$ and suppose that G has a p_i-complement Q_i for each i. Then

$$P_i = \bigcap_{j \neq i} Q_j$$

is a Sylow p_i-subgroup of G for each i, and $P_i P_j = P_j P_i$ for each pair (i, j). Such a system of pairwise permutable Sylow subgroups (one for each prime factor of $|G|$) is called a *Sylow basis* of G. The first statement of the next theorem follows from the last theorem:

Theorem 16.4.6 *Let G be a soluble group. Then G possesses a Sylow basis. Moreover, all Sylow bases are conjugate in G.*

The second statement means that if (P_i) and (P_i^*) are two Sylow bases, then there exists $g \in G$ such that $P_i^* = P_i^g$ for each i (assuming of course that P_i and P_i^* correspond to the same prime). A subgroup H of G is said to *reduce* into a Sylow basis (P_i) if $H \cap P_i$ is a Sylow subgroup of H for each i.

Corollary 16.4.7 *If G is soluble with Sylow basis (P_i) and $H \leq G$ then some conjugate of H reduces into (P_i).*

Proof. Let $p_1, \ldots, p_k$ be as above. For each i let H_i be a p_i-complement of H, and $Q_i \geq H_i$ a p_i-complement of G. Then the $P_i^* = \bigcap_{j \neq i} Q_j$ form a Sylow basis of G and for each i it is clear that $H \cap P_i^*$ is a Sylow subgroup of H. If g is such that $P_i^* = P_i^g$ for each i then $H^{g^{-1}}$ reduces into (P_i). ■

2 Carter subgroups

(See [R] Chapter 9 or [H] Chapter VI.)

A *Carter subgroup* of a group G is a nilpotent subgroup C such that $\mathrm{N}_G(C) = C$.

Theorem 16.4.8 (R. W. Carter) *Let G be a soluble group. Then*

(i) G possesses Carter subgroups, and they are all conjugate.

(ii) Let C be a Carter subgroup of G and let $C \leq H \leq G$. If $N \lhd H$ and H/N is nilpotent then $H = NC$.

Corollary 16.4.9 *Suppose that G has a chain of normal subgroups $1 = N_0 < N_1 < \ldots < N_l = G$ such that N_i/N_{i-1} is nilpotent for each i. Then*

$$G = C_1 \cdot C_2 \cdot \ldots \cdot C_l$$

where C_i is a Carter subgroup of N_i for each i.

3 The Fitting subgroup

This is the unique maximal nilpotent normal subgroup $\mathrm{Fit}(G)$ of a group G (Fitting proved that a product of nilpotent normal subgroups is nilpotent, so $\mathrm{Fit}(G)$ exists). A frequently used and well known fact is that *in a finite soluble group, the Fitting subgroup contains its centraliser*. The following lemma is a little sharper:

Lemma 16.4.10 *Let G be a finite soluble group. Then G has a normal subgroup N such that*

$$[N, N] \leq \mathrm{Z}(N) = \mathrm{C}_G(N).$$

Proof. Let A be maximal among abelian normal subgroups of G, and put $C = \mathrm{C}_G(A)$. If $C = A$ take $N = A$. If not, then C/A is a non-trivial normal

subgroup of G/A, hence contains a non-trivial abelian normal subgroup N/A of G/A, and we choose a maximal such N. Then

$$C \geq \mathrm{C}_G(N) \geq \mathrm{Z}(N) = A \geq [N, N],$$

by the maximality of A. Suppose that $\mathrm{C}_G(N) \neq A$. Then $\mathrm{C}_G(N)/A$ contains a non-trivial abelian normal subgroup D/A of G/A. Then $D \cap N \leq \mathrm{Z}(N)$ so in fact $D \cap N = A$; therefore $DN/A = D/A \times N/A$ is abelian, contradicting the maximality of N. It follows that $\mathrm{C}_G(N) = A = \mathrm{Z}(N)$ and the proof is complete.

■

(The finiteness of G is not really necessary here: we can use Zorn's Lemma instead.)

Theorem 16.4.11 *If G is a soluble group then*

$$|G| \leq |\mathrm{Fit}(G)|^4 .$$

Proof. Put $F = \mathrm{Fit}(G)$ and let $\Phi(F)$ be the Frattini subgroup of F. Then $F/\Phi(F) \cong \bigoplus V_p$ where for each prime p, $V_p = F/F'F^p$ is an $\mathbb{F}_p[G]$-module via conjugation. Let W_p denote the completely reducible $\mathbb{F}_p[G]$-module obtained by forming the direct sum of the $\mathbb{F}_p[G]$-composition factors of V_p, and let K_p be the kernel of the action of G on W_p. According to the theorem of Pálfy and Wolf (↬ **Permutation groups**) we have

$$|G/K_p| \leq |W_p|^3 = |V_p|^3 .$$

Now put $K = \bigcap_p K_p$. Then K acts nilpotently on each V_p, hence it acts nilpotently on $F/\Phi(F)$, and hence it acts nilpotently on F (an elementary property of nilpotent groups). Therefore $K/\mathrm{C}_K(F)$ is nilpotent, and as $\mathrm{C}_K(F) \leq \mathrm{C}_G(F) \leq F$ it follows that K is nilpotent. Thus $K = F$ and so

$$|G| = |K|\,|G/K| \leq |F| \cdot \prod_p |V_p|^3 = |F|\,|F/\Phi(F)|^3 \leq |F|^4 .$$

■

The *Fitting length* (or *Fitting height*) of a soluble group G is the least integer h such that $\mathrm{Fit}^{(h)}(G) = G$, where $\mathrm{Fit}^{(1)}(G) = \mathrm{Fit}(G)$ and $\mathrm{Fit}^{(i+1)}(G)/\mathrm{Fit}^{(i)}(G) = \mathrm{Fit}(G/\mathrm{Fit}^{(i)}(G))$; this is clearly the minimal length of a chain of normal subgroups from 1 to G with nilpotent factors. Corollary 16.4.9 thus shows that G is equal to a product of h nilpotent subgroups.

4 The generalised Fitting subgroup

(See [A], §31.)

This plays the role of the Fitting subgroup in non-soluble groups. A group S is *quasi-simple* if S is perfect (i.e. $S = S'$) and $S/\mathrm{Z}(S)$ is simple. The *layer* of G is the characteristic subgroup $E(G)$ generated by all the quasi-simple subnormal subgroups of G. The *generalised Fitting subgroup* of G is

$$F^*(G) = E(G)\mathrm{Fit}(G).$$

Proposition 16.4.12 *Let G be a finite group, $E = E(G)$ and $F^* = F^*(G)$. Then*

$$\begin{aligned} \mathrm{C}_G(E/Z(E) &= \mathrm{C}_G(E), \\ \mathrm{C}_G(F^*) &= \mathrm{Z}(F^*), \end{aligned}$$

and if R is a soluble normal subgroup of G then

$$[E, R] = 1.$$

5 Tate's theorem

(See [H] Chapter IV, Satz 4.7.)

A group G is *p-nilpotent if* G has a normal p-complement, so G is an extension of a normal p'-subgroup by a p-group. Several sufficient conditions for p-nilpotency are provided by transfer arguments. The important one for us is the following, due to John Tate:

Theorem 16.4.13 *Let G be a group with a normal subgroup N and a Sylow p-subgroup P. If $P \cap N \leq \Phi(P)$ then N is p-nilpotent.*

Write $\overline{P} = P/(P \cap N)$. Now $P/\Phi(P)$ is a d-dimensional vector space over $\mathbb{F}_p$ where $d = d(P)$; so if $P \cap N$ is not contained in $\Phi(P)$ then

$$d(\overline{P}) = \dim(\overline{P}/\Phi(\overline{P})) < \dim(P/\Phi(P)) = d(P).$$

Hence the

Corollary 16.4.14 *Let G, N and P be as above. If $d(PN/N) = d(P)$ then N is p-nilpotent.*

This result is useful in combination with the **Odd order theorem**: this says that every group of odd order is soluble, and hence implies that *every 2-nilpotent group is soluble.*

6 Rank and p-rank

The following was proved for soluble groups in [Kovács 1968], and for all finite groups (using CFSG) by [Lucchini 1989] and [Guralnick 1989]:

Theorem 16.4.15 *If every Sylow subgroup of G can be generated by d elements then $d(G) \leq d + 1$.*

Now recall that $\mathrm{rk}(G) = \sup\{d(H) \mid H \leq G\}$ and $\mathrm{r}_p(G) = \mathrm{rk}(P)$ where p is a Sylow p-subgroup of G. Applying the theorem to arbitrary subgroups of a group G we deduce

Corollary 16.4.16

$$\mathrm{rk}(G) \leq 1 + \max_{p||G|} \mathrm{r}_p(G).$$

A related result uses soluble subgroups instead of Sylow subgroups:

Theorem 16.4.17 [Aschbacher & Guralnick 1982] *Let G be a group. Then there exist a soluble subgroup H and an element g of G such that $\langle H, H^g \rangle = G$.*

7 Schur multiplier

(See [H] Chapter V, §§23-25 or [A], §33.)

The multiplier of a group G is $M(G) = H^2(G, \mathbb{C}^*) \cong H_2(G, \mathbb{Z})$, a finite abelian group whose exponent e satisfies $e^2 \mid |G|$.

If G is *perfect*, that is $G = G'$, then G has a unique *universal covering group* $\widetilde{G}$. This is a perfect central extension of G by $M(G)$ and *every perfect central extension of G is a quotient of $\widetilde{G}$*. In particular, if

$$1 \to A \to Y \to G \to 1$$

is a central extension of G with $Y = Y'$ then A is an image of $M(G)$.

If G and H are perfect groups then $M(G \times H) \cong M(G) \times M(H)$ (in general there is an extra 'correction term' $(G/G') \otimes (H/H')$).

If P is a Sylow p-subgroup of G then the p-component of $M(G)$ is isomorphic to a subgroup of $M(P)$.

The following is an application of the theory of powerful p-groups (see below):

Theorem 16.4.18 [Lubotzky & Mann 1987] *Let G be a p-group of rank r. Then*

$$\mathrm{rk}(M(G)) \leq r(r-1)/2 + r^2(\lceil \log r \rceil + \varepsilon)$$

where $\varepsilon = 0$ if p is odd, $\varepsilon = 1$ if $p = 2$.

8 Powerful p-groups

This theory is due to [Lubotzky & Mann 1987]; for a detailed exposition see [DDMS], Chapter 2. A p-group G is said to be *powerful* if G/G^p is abelian (when $p \neq 2$) or G/G^4 is abelian (when $p = 2$). Powerful groups resemble abelian groups in several respects; for example,

Theorem 16.4.19 *Let G be a powerful p-group. Then*

(i) $\mathrm{rk}(G) = d(G)$;

(ii) *if $G = \langle x_1, \ldots, x_d \rangle$ then $G = \langle x_1 \rangle \langle x_2 \rangle \ldots \langle x_d \rangle$ is a product of d cyclic subgroups.*

Part (i) implies that if G is powerful then

$$\dim_{\mathbb{F}_p}(H/\Phi(H)) = d(H) \leq d(G) = \dim_{\mathbb{F}_p}(G/\Phi(G))$$

for every subgroup H of G.

Corollary 16.4.20 *If G is a powerful p-group of exponent p^h then $|G| \leq p^{hd(G)}$.*

Write $\Phi^0(G) = G$ and for $i \geq 1$ set $\Phi^i(G) = \Phi(\Phi^{i-1}(G))$.

Theorem 16.4.21 ([DDMS] Chapter 2, Exercise 6) *Let G be a p-group, put $G_i = \Phi^i(G)$ and let*

$$s = \max_{i \geq 0} d(G_i),$$
$$m = \lceil \log s \rceil + \varepsilon$$

where $\varepsilon = 0$ if p is odd, $\varepsilon = 1$ if $p = 2$. Then
(i) G_m is powerful;
(ii) $|G : G_m| \leq p^{ms}$.

Since

$$s \leq \max\{d(N) \mid N \lhd G\} \leq \mathrm{rk}(G)$$

this implies

Corollary 16.4.22 *If G is a p-group of rank r then G contains a powerful characteristic subgroup of index at most $p^{r(1+\lceil \log r \rceil)}$.*

Corollary 16.4.23 *Let G be a p-group. If $d(N) \leq k$ for every normal subgroup N of G then*

$$\mathrm{rk}(G) \leq k(2 + \lceil \log k \rceil).$$

For if $H \leq G$ then $d(H \cap G_m) \leq d(G_m) \leq k$ by Theorem 16.4.19, while for each $i \leq m$ we have

$$d\left((H \cap G_{i-1})/(H \cap G_i)\right) \leq d(G_{i-1}/G_i) \leq k$$

since G_{i-1}/G_i is elementary abelian.

Combining Corollary 16.4.22 with Corollary 16.4.20 we deduce

Corollary 16.4.24 *If G is a p-group of rank r and exponent p^h then*

$$|G| \leq p^{r(1+\lceil \log r \rceil + h)}.$$

This has an application to arbitrary finite groups:

Proposition 16.4.25 *Let G be a finite group of rank r and exponent m. Then*

$$|G| \mid m^{r(3+\log r)}.$$

Indeed, if $m = \prod p^{e(p)}$ and P is a Sylow p-subgroup of G then $|P| = p^{n(p)}$ where

$$n(p) \leq r(1 + \lceil \log r \rceil + e(p)) \leq e(p)r(3 + \log r),$$

and the result follows since $|G| = \prod p^{n(p)}$.

The theory of powerful p-groups has important applications to pro-p groups (↬ **pro-p groups**).

9 GL_n and $\mathrm{Sym}(n)$

If p is a prime, the p-part of $n!$ is at most $p^{[(n-1)/(p-1)]}$, so this is an upper bound for the order of any p-subgroup of $\mathrm{Sym}(n)$. It follows that

$$\mathrm{r}_p(\mathrm{Sym}(n)) \leq \frac{n-1}{p-1}.$$

With Corollary 16.4.16 this implies that the rank of $\mathrm{Sym}(n)$ is at most n. However, an elementary argument due to [Jerrum 1986] yields the better bound

Theorem 16.4.26 *The rank of* $\mathrm{Sym}(n)$ *is at most* $n-1$.

(See [Cameron 1999], § 1.14. The best bound (for $n \geq 4$) is actually $[n/2]$, due to [Mciver & Neumann 1987].)

In the other direction it is easy to see that

$$\mathrm{rk}(\mathrm{Alt}(n)) \geq (n-3)/2;$$

indeed, $\mathrm{Alt}(n)$ contains a direct product of $[n/4]$ Klein four-groups, which is elementary abelian of rank $2 \cdot [n/4]$.

If $n = a_1 + \cdots + a_k$ then by the GM-AM inequality we have

$$\prod a_i \leq (n/k)^k \leq 2^n.$$

It follows that *the maximal order of any element in* $\mathrm{Sym}(n)$ *is at most* 2^n. We can also bound the *exponent* $\exp(\mathrm{Sym}(n))$ of $\mathrm{Sym}(n)$. If p is a prime then the maximal order of a p-element in $\mathrm{Sym}(n)$ is at most $p^{e(p)}$ where $e(p) = \left[\log_p n\right]$. Hence

$$\exp(\mathrm{Sym}(n)) = \prod_{p \leq n} p^{e(p)} \leq n^{\pi(n)} \leq n^{A(n/\ln n)} = e^{An}$$

where $\pi(n)$ denotes the number of primes below n and A is a constant (slightly greater than 1), by the Prime Number Theorem. [Hanson 1972] shows that in fact 3^n is an upper bound. Note that $\prod_{p \leq n} p^{e(p)} = e^{\psi(n)}$, where ψ is the number-theoretic function defined in [HW], §22.1. It follows by [HW] Theorem 434, a version of the Prime Number Theorem, that

$$\ln(\exp(\mathrm{Sym}(n))) \sim n$$

as $n \to \infty$.

Now we consider the group $G = \mathrm{GL}_n(\mathbb{F}_q)$ where $q = p^e$ for a prime p. A Sylow p-subgroup of G is the group of upper uni-triangular matrices, which has order

$$q^{n(n-1)/2}$$

and hence rank at most $en(n-1)/2$. If l is a prime other than p and H is a Sylow l-subgroup of G then H is monomial (see [We], Chapter 1); that is,

H is conjugate over the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_q$ to a group of monomial matrices. Thus there is a homomorphism $\theta : H \to \mathrm{Sym}(n)$ such that $\ker\theta$ is diagonalisable. Then $\ker\theta$ is an abelian group of rank at most n (since every finite subgroup of $\overline{\mathbb{F}}_p^*$ is cyclic), while $H/\ker\theta$ has rank at most $(n-1)/(l-1)$. Thus we have

Theorem 16.4.27 *Let $G = \mathrm{GL}_n(\mathbb{F}_q)$ where $q = p^e$. Then*

$$\mathrm{r}_p(G) \le en(n-1)/2,$$
$$\mathrm{r}_l(G) \le n + \frac{n-1}{l-1} \le 2n-1$$

for primes $l \ne p$.

With Corollary 16.4.16 this gives

Corollary 16.4.28 *The rank of $\mathrm{GL}_n(\mathbb{F}_{p^e})$ is at most $1 + en(n-1)/2 < en^2/2$ if $n \ge 5$ or $e \ge 2$, and at most 7 otherwise.*

Again, this is not the best bound. (For $p \ne 2$ and $e = 1$, [Pyber 1993] gives $n^2/4$.)

It it easy to see that a diagonalisable subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ has order at most $q^n - 1$. Since an l-subgroup of $\mathrm{Sym}(n)$ has order at most $l^{(n-1)/(l-1)} \le 2^{n-1}$, the above argument also gives

Proposition 16.4.29 *If l is a prime and $l \nmid q$ then a Sylow l-subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ has order less than $(2q)^n$.*

If $g \in \mathrm{GL}_n(\mathbb{F}_q)$ is unipotent then

$$g^{p^f} - 1 = (g-1)^{p^f} = 0$$

as long as $p^f \ge n$. Hence the order of g is less than pn. In any case, the eigenvalues of g lie in $\mathbb{F}_{q^n}^*$, so if g is semisimple then its order divides $q^n - 1$. It follows that the order of any element of $\mathrm{GL}_n(\mathbb{F}_q)$ is bounded above by $pn(q^n-1)$. In fact the correct bound is $q^n - 1$ [Horoshevskii 1974].

Window: Finite simple groups

In a statistical sense, the simple groups (by which we mean, in this window, *non-abelian finite* simple groups) are quite rare: the Godfather of the subject has likened them to fossils, occasionally found buried among the composition factors of a general finite group [Thompson 1984]. The analogy includes the suggestion that they are *hard*: excavating with primitive tools may uncover some general features of a group, but will usually not reveal the deeper secrets of structure hidden within the simple factors. Prosaically, what this means is that when simple groups are present, one can only get so far with elementary group-theoretic arguments and then one gets stuck.

A revolutionary change in the nature of group theory occurred around 1980, after two or three decades of extraordinary work. This was the complete *classification of the simple groups*, which we shall refer to as **CFSG**. Many hitherto intractable problems can now be solved by a more or less standard two-stage procedure: (1) the problem is reduced to a specific question about simple groups, and (2) one answers the question by examining the known list of simple groups. Either stage may of course be difficult – but we are no longer stuck in quite the same way. Some of the main results in this book, such as the PSG theorem, testify to the remarkably wide scope of this philosophy – and show that, far from bringing group theory to an end, CFSG may open the doors to unexpected new vistas.

The *proof* of CFSG is so long (estimated at 15,000 pages) and fragmented that some mathematicians are doubtful about accepting the result as definitive. Unwilling to be ejected from the paradise created for us by Thompson, Gorenstein, Aschbacher and their co-workers, we trust that such doubts will eventually be laid to rest. The proof is being systematised and re-written in a series of books by Gorenstein, Lyons and Solomon; a careful explanation of its present status is given in the introduction to the first volume of the series [**Gorenstein, Lyons & Solomon 2000**].

As an extra 'safety net', it should be mentioned that most results in infinite group theory that depend on CFSG are robust to the extent that the occurrence of just *finitely many* presently unknown simple groups would not invalidate their proof.

1 The list

For the statement of the classification theorem, and more or less detailed accounts of the proof, see [**G**], [**Gorenstein, Lyons & Solomon 2000**], [**A**]. For the construction and properties of groups of Lie type see [**C**], [**Carter 1985**], [**St**]. A comprehensive (if rather indigestible) reference for properties of all the simple groups is [**GLS**].

The starting point for the classification was the celebrated **Odd order theorem:**

Theorem 16.4.1 [Feit & Thompson 1963] *Every group of odd order is soluble.*

This is of course equivalent to the statement that *every finite simple group has even order.*

The finite simple groups comprise two infinite families and 26 sporadic groups. The infinite families are

(1) the alternating groups $\mathrm{Alt}(n)$ for $n \geq 5$;

(2) the groups of Lie type.

The simple groups of Lie type are the adjoint *Chevalley groups* $X_l(q)$ and the *twisted Chevalley groups* ${}^tX_l(q)$ Here X_l denotes one of the connected Dynkin diagrams A_l ($l \geq 1$), B_l ($l \geq 2$), C_l ($l \geq 3$), D_l ($l \geq 4$), E_6, E_7, E_8, F_4, G_2; $q = p^e$ denotes a prime-power; and t is 2 or 3. The twisted groups only exist for certain of the diagrams and certain values of l, t and q:

$$
\begin{array}{l}
{}^2A_l(q),\ {}^2D_l(q),\ {}^2E_6(q), \\
{}^3D_4(q) \\
{}^2B_2(2^m),\ {}^2F_4(2^m),\ {}^2G_2(3^m)\ \ (m\ \ \text{odd}).
\end{array}
$$

The groups ${}^*X_l(q)$ are simple except for a few very small values of l and q; for almost all of these the derived group is simple, and these are usually included among the 'simple groups of Lie type' ($*$ means 1, 2 or 3 where ${}^1X_l(q) = X_l(q)$). However, up to isomorphism, all these 'derived' simple groups of Lie type also occur as 'adjoint groups' ${}^*X_l(q)$, with the one exception ${}^2F_4(2)'$ (the 'Tits group'), and to simplify some statements we shall count this group as an honorary 'sporadic'.

In general, $X_l(q)$ is the group of $\mathbb{F}_q$-rational points of the corresponding simple (split, adjoint) algebraic group, and ${}^tX_l(q)$ the subgroup of fixed points in $X_l(q^t)$ of a certain automorphism of order t. Many groups of Lie type are

classical groups:

$$\begin{aligned} A_l(q) &= \mathrm{PSL}(l+1, \mathbb{F}_q) \\ B_l(q) &= \mathrm{P}\Omega(2l+1, \mathbb{F}_q) \\ C_l(q) &= \mathrm{PSp}(2l, \mathbb{F}_q) \\ D_l(q) &= \mathrm{P}\Omega^+(2l, \mathbb{F}_q) \\ {}^2A_l(q) &= \mathrm{PSU}(l+1, \mathbb{F}_q) \\ {}^2D_l(q) &= \mathrm{P}\Omega^-(2l, \mathbb{F}_q). \end{aligned}$$

The others are called *exceptional groups*.

The parameter l is the *Lie rank* (or 'untwisted rank').

With 9 small exceptions, the simple groups of Lie type and the alternating groups are all pairwise non-isomorphic, except that $B_l(2^n) \cong C_l(2^n)$ for all l and n.

The **order** of ${}^tX_l(q)$ is given by a certain polynomial in q; these are listed in Table I of [**GLS**], for example. The same table also gives the orders of the sporadic groups. This table shows that $|A_2(4)| = |A_3(2)|$ and $|B_l(q)| = |C_l(q)|$ for all l and q. It is true (but by no means self-evident!) that these are the only cases of non-isomorphic simple groups whose orders coincide. Thus

- *For each integer n there are are most* two *non-isomorphic simple groups of order n.*

Moreover,

- *If S and T are simple and $|S|^a = |T|^b$ for integers a and b then $|S| = |T|$.*

These and many other interesting facts about the orders of simple groups are established in [**Kimmerle, Lyons, Sandling & Teague 1990**], following work of Artin and Tits.

Theoretical formulas for the order are given in [**C**], [**A**] and [**St**], §§9, 11. Writing $\dim(X_l)$ for the dimension of the simple Lie algebra of type X_l (see table (16.1) below), we have

Proposition 16.4.2 *Let $G = {}^tX_l(q)$ be simple of Lie type and put $d = \dim(X_l)$. Then*

$$|G| = q^d(1 + o(1))$$

and if G is untwisted then

$$|G| < q^d.$$

(Here $o(1)$ means a number that tends to 0 as $q \to \infty$.)

A group G is *quasi-simple* if G is perfect (i.e. $G = [G, G]$) and $G/\mathrm{Z}(G)$ is simple. Each simple group G of Lie type ${}^tX_l(q)$ has a 'universal' version $\widetilde{G} = {}^t\widetilde{X}_l(q)$ such that $\widetilde{G}/\mathrm{Z}(\widetilde{G}) \cong G$. If G is simple then $\widetilde{G}$ is quasi-simple.

2 Generators

Theorem 16.4.3 [Aschbacher & Guralnick 1984] *Every simple group can be generated by* 2 *elements.*

This was established for the groups of Lie type by [**Steinberg 1962**]. In fact, 'most' pairs of elements in a simple group S generate S, in the sense that

$$1 - \frac{|X|}{|S|^2} \to 0$$

as $|S| \to \infty$ where $X = \{(x, y) \in S \times S \mid \langle x, y\rangle = S\}$; this conjecture of Dixon was finally proved by [**Liebeck & Shalev 1995**] following work of Dixon, Babai and Kantor & Lubotzky.

3 Subgroups

Let $G = {}^*X_l(q)$ be a group of Lie type, Δ the associated Dynkin diagram. (In the twisted case, Δ is a quotient graph of the diagram X_l by the appropriate symmetry). To each subset of Δ there corresponds a conjugacy class of *parabolic subgroups* of G. In particular, suppose that Δ' is a connected subgraph of Δ. Then Δ' is again a Dynkin diagram X', and the corresponding parabolic subgroup contains a quasi-simple group of type $X'(q)$, that is, a perfect central extension of the simple group $X'(q)$. Applying this to the classical groups we deduce

Proposition 16.4.4 *Let $G = {}^*X_l(q)$ be a classical group. Then G contains a subgroup isomorphic to* $(\mathrm{P})\mathrm{SL}(m, \mathbb{F}_q)$*, and hence* $\mathrm{Alt}(m)$ *is a section of G, where $m \geq 1 + l/2$.*

Here by $(\mathrm{P})\mathrm{SL}(m, \mathbb{F}_q)$ we mean a group of the form $\mathrm{SL}(m, \mathbb{F}_q)/N$ where $1 \leq N \leq \mathrm{Z}(\mathrm{SL}(m, \mathbb{F}_q))$.

If $q = p^e$ it follows that G contains an elementary abelian p-subgroup of rank $\left[\frac{m}{2}\right]^2 e \geq l^2 e/4$, corresponding to the group of upper unitriangular matrices in $\mathrm{SL}(m, \mathbb{F}_q)$ having non-zero entries only in the top right-hand $\left[\frac{m}{2}\right] \times \left[\frac{m}{2}\right]$ corner. This implies

Corollary 16.4.5 *Let $G = {}^*X_l(p^e)$ be a group of Lie type. Then*

$$\begin{aligned} l^2 e &\leq 4\mathrm{rk}(G) \quad \textit{if } G \textit{ is of classical type} \\ l &\leq 8 \textit{ and } e \leq \mathrm{rk}(G) \quad \textit{if } G \textit{ is of exceptional type.} \end{aligned}$$

The second claim holds because, in any case, G contains a copy of the additive group of $\mathbb{F}_q$. (Recall that $\mathrm{rk}(G)$ denotes the maximum of $d(H)$ over all subgroups of a group G, *not* the Lie rank. To avoid confusion, in this window we shall refer to $\mathrm{rk}(G)$ as the *Prüfer rank*.)

4 Representations

Each (adjoint) Chevalley group may be constructed as a group of automorphisms of the corresponding Lie algebra. The dimension of this Lie algebra is given in terms of the Lie rank l by the following table (see [Jacobson 1962], Chapter IV):

A_l	B_l	C_l	D_l	E_6	E_7	E_8	F_4	G_2
$l(l+2)$	$l(2l+1)$	$l(2l+1)$	$l(2l-1)$	78	133	248	52	14

(16.1)

Hence if $G = X_l(q)$ is an untwisted simple group of Lie type then

$$G \leq \mathrm{SL}_n(\mathbb{F}_q) \leq \mathrm{SL}_{ne}(\mathbb{F}_p)$$

where $n \leq \max\{2l^2 + l,\ 248\}$ and $q = p^e$. If $G = {}^tX_l(q)$ is a twisted group then $G \leq X_l(q^t)$, where $t = 2$ except for the case of ${}^3D_4$. Thus we have (crudely) part (i) of

Proposition 16.4.6 *Let $G = {}^*X_l(q)$ be a simple group of Lie type, where $q = p^e$. Then* (i)

$$G \leq \mathrm{SL}_n(\mathbb{F}_q) \leq \mathrm{SL}_{ne}(\mathbb{F}_p)$$

where $n = \max\{5l^2,\ 248\}$;

(ii) *if G is a classical group then*

$$G \leq \mathrm{PSL}_{2l+1}(\mathbb{F}_q).$$

Of course, (ii) follows from the table in Section 1. Since the Prüfer rank of $\mathrm{GL}_d(\mathbb{F}_{p^e})$ is at most $\max\{ed^2/2,\ 7\}$ (↬ **Finite group theory**), this implies

Proposition 16.4.7 *Let G be as above. Then*

$$\mathrm{rk}(G) \leq \max\{(2l+1)^2\frac{e}{2},\ Ne\}$$

where $N = 248^2/2$.

Combining this with Corollary 16.4.5 we deduce

Corollary 16.4.8 *There exists a function f such that*

$$\max\{e,\ l/4\} \leq \mathrm{rk}({}^*X_l(p^e)) \leq f(l, e)$$

for every prime p.

Thus a collection of simple groups of Lie type has bounded Prüfer ranks if and only if it has bounded Lie ranks and bounded field degrees.

The minimal degree of a faithful linear representation of a simple group of Lie type is generally less than the crude bound given in Proposition 16.4.6. A lower bound for this follows from

Proposition 16.4.9 *Let G be a classical group of Lie rank l. If G is a section of $\mathrm{GL}_n(F)$ for some finite field F then*

$$n \geq \frac{l-4}{3}.$$

This follows from Proposition 16.4.4 together with

Proposition 16.4.10 ([DM], Theorem 5.7A) *If $\mathrm{Alt}(k)$ is a section of $\mathrm{GL}_n(F)$ for some finite field F then*

$$n \geq \frac{2k-6}{3}.$$

(The bound $(2k-4)/3$ given in [DM] is slightly too weak.)

The minimal degree of a faithful *permutation representation* of a simple group G is equal to the minimal index of a proper subgroup. In the case of a classical group $G = X_l(q)$ the smallest permutation representation is generally speaking given by the natural action of the group on the points of the corresponding $(d-1)$-dimensional projective space, where d is $l+1$, $2l$ or $2l+1$ (see Section 1). The minimal degree is therefore

$$\frac{q^{d+1}-1}{q-1} > q^{l+1}.$$

In general we have

Proposition 16.4.11 ([Kleidman & Liebeck 1990], **5.2.2**) *Let G be a simple group of Lie type of Lie rank l. Then every proper subgroup M of G satisfies*

$$|G : M| \geq |G|^{c(l)}$$

where $c(l)$ is a positive constant depending only on l.

5 Automorphisms

Let $G = {}^*X_l(p^e)$ be a simple group of (adjoint) Lie type. Every automorphism of G is a product (in the stated order) of an inner automorphism, a 'diagonal automorphism', a 'field automorphism' and a 'graph automorphism'; these are defined in [**C**], [**St**]. See also [**GLS**] §2.5. It follows that $\mathrm{Aut}(G)$ has a chain of normal subgroups

$$\mathrm{Inn}(G) \leq D \leq DF \leq \mathrm{Aut}(G)$$

such that

- $\mathrm{Inn}(G) \cong G$
- $D/\mathrm{Inn}(G)$ is a finite group isomorphic to the centre of the universal group ${}^*\widetilde{X}_l(p^e)$, an abelian group of rank at most 2, order dividing 3, 4 or $l+1$ and exponent dividing $p^e \pm 1$

- F is a cyclic group of order dividing e and $DF/D \leq \mathrm{Z}(\mathrm{Aut}(G)/D)$
- $\mathrm{Aut}(G)/DF$ is 1, cyclic of order 2 or isomorphic to Sym(3).

Writing $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ we have

Proposition 16.4.12 *Let $G = {}^*X_l(p^e)$ be a simple group of Lie type. Then $\mathrm{Out}(G)$ is soluble of derived length at most 3 and*

$$|\mathrm{Out}(G)| \leq 6e \cdot \max\{(l+1),\, 4\}.$$

Combined with Proposition 16.4.6 this implies

Corollary 16.4.13 *Let $G = {}^*X_l(p^e)$ be a simple group of Lie type. Then*

$$\mathrm{Aut}(G) \leq \mathrm{SL}_n(\mathbb{F}_p)$$

where $n = 6e^2 \cdot \max\{(l+1),\, 4\} \cdot \max\{5l^2,\, 248\}$.

Regarding the remaining simple groups, we have

Proposition 16.4.14 *Let G be an alternating or sporadic simple group. Then $|\mathrm{Out}(G)| \leq 2$ unless $G = \mathrm{Alt}(6)$ in which case $|\mathrm{Out}(G)| = 4$.*

6 Schur multipliers

The multipliers of all finite simple groups are given in [**G**], Table 4.1 (based largely on work of Schur, Steinberg and Griess.) From this table one reads off the following.

1) If G is simple then $M(G)$ has rank at most 2.

2) If G is not of the form $A_l(q)$ or ${}^2A_l(q)$ then $M(G)$ has exponent dividing 12.

3) If $G = A_l(q)$ then $M(G)$ is cyclic of order $\gcd(l+1, q-1)$ unless the pair (l, q) is one of five small exceptions; in each of these cases $M(G)$ has exponent dividing 12 and order dividing 48.

4) If $G = {}^2A_l(q)$ then $M(G)$ is cyclic of order $\gcd(l+1, q+1)$ unless the pair (l, q) is one of three small exceptions; in each of these cases $M(G)$ has exponent dividing 12 and order dividing 36.

5) Apart from a finite number of pairs (l, q), the 'universal' group of Lie type ${}^t\widetilde{X}_l(q)$ is the universal central extension of the simple group $G = {}^tX_l(q)$; that is, the centre of ${}^t\widetilde{X}_l(q)$ is isomorphic to $M(G)$, which is a p'-group (see [**G**], §4.15A).

It follows from (1) that $H^2(G, \mathbb{F}_p)$ has dimension at most 2 for every prime p (because $H^2(G, \mathbb{F}_p)$ is the cokernel of the mapping $M(G) \to M(G)$ given by multiplication by p).

7 An elementary proof

We stated above that there are no more than two simple groups of any given order. The only known proof of this fact depends on the classification, and it may be of interest to record an elementary direct proof of the following (ridiculously weak!) bound, which will suffice for some of our applications. It is due to L. Pyber and A. Shalev (unpublished).

Proposition 16.4.15 *here is an absolute constant c such that for each positive integer n, the number of simple groups of order n is at most c^n.*

Proof. Fix a large integer n. Let G be a simple group of order n. We consider two cases.

Case 1. Where G has a proper subgroup of order at least $(\log n)^2$. Then $G \leq \mathrm{Sym}(m)$ where $m = [n/(\log n)^2]$. Also G can be generated by at most $\log n$ elements, so there are at most

$$(m!)^{\log n} < (n^{n/(\log n)^2})^{\log n} = 2^n$$

possibilities for G.

Case 2. Where every proper subgroup of G has order less than $(\log n)^2$. We claim that then n has a prime divisor $p > \frac{1}{8}\log n$. Accepting the claim for now, let P be a subgroup of G of order p and let M be a maximal subgroup containing P. Put $m = |M|$ and $k = m/p$. The length of any chain of subgroups refining $1 < P \leq M < G$ is at most $2 + \log k$, so G can be generated by $[2 + \log k]$ elements. Also $G \leq \mathrm{Sym}(n/m)$, so the number of possibilities for G is at most

$$((n/m)!)^{2+\log k} < n^{(n/m)(2+\log k)} = 2^r$$

where

$$r = \frac{n \log n \cdot (2 + \log k)}{pk} \leq 16n.$$

It remains to establish the *claim*. Suppose that all prime factors of n are bounded above by $x = \frac{1}{8}\log n$. The number of these prime factors is then at most

$$\pi(x) \leq (2 + o(1))\frac{x}{\log x} \leq 3\frac{x}{\log x}$$

if n is large enough, by an easy weak form of the Prime Number Theorem (↬ **Prime numbers**). On the other hand, since each Sylow subgroup of G has order less than $(\log n)^2$ we have

$$n = |G| < (\log n)^{2\pi(x)}.$$

Therefore

$$\begin{aligned} \log n &< 2\pi(x) \log\log n \\ &\leq 2 \cdot 3 \cdot \frac{\log n}{8(\log\log n - 3)} \cdot \log\log n, \end{aligned}$$

a contradiction if n is large. The claim follows, and this completes the proof. ∎

Window: Permutation groups

In this Window, all groups are finite unless otherwise stated.

1 Primitive groups

A permutation group acting on a set Ω is *primitive* if it preserves no partition of Ω apart from the trivial ones $\{\Omega\}$ and $\{\{\alpha\} \mid \alpha \in \Omega\}$. A subgroup G of $\mathrm{Sym}(n)$ is called a *proper primitive group if* G is primitive and G does not contain $\mathrm{Alt}(n)$. To obtain a useful classification of proper primitive groups is a longstanding goal of permutation group theory, recently brought much closer with the help of CFSG: see [Cameron 1981]. We shall need

Theorem 16.4.1 *Let $G \leq \mathrm{Sym}(n)$ be a proper primitive group. Then*

$$|G| \leq \frac{n!}{\lceil n/2 \rceil !}, \tag{16.1}$$

$$|G| \leq 3^n, \tag{16.2}$$

$$|G| \leq n^{c\sqrt{n}} \tag{16.3}$$

where c is an absolute constant; and

$$|G| \leq 2^{n-1} \text{ unless } G \text{ is one of 24 known exceptions.} \tag{16.4}$$

(16.1) was proved by Bochert in 1889; see [DM], Theorem 3.3B. (16.2) and (16.4) are due to [Maróti]; these depend on CFSG. (The slightly weaker bound $|G| \leq 4^n$ due to [Praeger & Saxl 1980] does not; nor does the better bound $n^{c\sqrt{n}\log n}$ obtained by L. Babai, see [DM] §5.3). (16.3) follows from [Cameron 1981], Theorem 6.1; this also depends on CFSG.

2 Groups with restricted sections

A *section* of a group G is a factor A/B where $B \lhd A \leq G$. Of course, A/B is a *composition factor* of G if, in addition, A/B is simple and A is subnormal in G. It is a *chief factor* if $B \lhd G$ and A/B is a minimal normal subgroup of G/B.

We consider the following classes of groups, where k denotes a positive integer constant.

$G \in \mathcal{C}_k$ if no section of G is isomorphic to $\mathrm{Alt}(k+1)$

$G \in \mathcal{C}_k^{\triangleleft}$ if no composition factor of G is isomorphic to $\mathrm{Alt}(n)$ for any $n > k$

$G \in \mathcal{B}_k$ if $G \in \mathcal{C}_k^{\triangleleft}$ and no composition factor of G is isomorphic to a classical finite simple group of degree exceeding k (here by *degree* we mean the degree of the natural projective representation)

$G \in \mathcal{R}_k$ if $\mathrm{rk}(M) \leq k$ for every non-abelian composition factor M of G

$G \in \mathcal{R}'_k$ if $G \in \mathcal{B}_k$ and for every composition factor of G which is a simple group of Lie type $X_l(\mathbb{F}_{p^e})$, the field degree e satisfies $e \leq k$.

Remarks (i) The classes $\mathcal{C}_k$ are closed under taking subgroups, quotients and extensions. Conversely, any class of finite groups with this property, other than the class of all finite groups, is necessarily contained in $\mathcal{C}_k$ for some k. Similarly, each of the classes $\mathcal{C}_k^{\triangleleft}, \mathcal{B}_k$, $\mathcal{R}_k$ and $\mathcal{R}'_k$ is closed under taking *normal* subgroups, quotients and extensions.

(ii) Let G be an infinite group. Then either G involves every finite group as an upper section, or else every finite quotient of G lies in $\mathcal{C}_k$ for some fixed k; in particular, if (in the latter case) G is a profinite group then G is a pro-$\mathcal{C}_k$ group.

(iii) Let $\mathcal{S}_0$ denote the set of sporadic simple groups; for $\beta \in \mathbb{N}$ let $\mathcal{A}(\beta)$ denote the set of alternating groups $\mathrm{Alt}(n)$ with $5 \leq n \leq \beta$ and $\mathcal{X}(\beta)$ the set of simple groups of Lie type $X_l(p^e)$ (untwisted or twisted) where the Lie rank l and the field degree e are both $\leq \beta$. Then

$$\mathcal{S}_0 \cup \mathcal{A}(\beta) \cup \mathcal{X}(\beta) \subseteq \mathcal{R}'_k$$

where $k = 2\beta + 1$. On the other hand, it follows from CFSG that every simple group in $\mathcal{R}'_k$ belongs to $\mathcal{S}_0 \cup \mathcal{A}(\beta) \cup \mathcal{X}(\beta)$ where $\beta = \max\{8, k\}$. (A classical group of Lie rank l has degree at least $l+1$ and at most $2l+1$, while a group of exceptional Lie type has Lie rank at most 8) (↬ **Finite simple groups**).

Proposition 16.4.2 *For each k there exists k' such that*

$$\mathcal{C}_k \subseteq \mathcal{B}_{k'} \quad \textit{and } \mathcal{B}_k \subseteq \mathcal{C}_{k'} \tag{16.5}$$

$$\mathcal{R}_k \subseteq \mathcal{R}'_{k'} \quad \textit{and} \quad \mathcal{R}'_k \subseteq \mathcal{R}_{k'}. \tag{16.6}$$

Also $\mathcal{C}_k \subseteq \mathcal{C}_k^{\triangleleft}$ and $\mathcal{R}'_k \subseteq \mathcal{B}_k$.

Proof. The final statement is obvious.

Note that every simple section of G is a section of some composition factor of G. Now suppose that C is classical finite simple group of degree n. If $\mathrm{Alt}(k+1)$ is a section of C then $n \geq (2k-4)/3$, by [DM], Theorem 5.7A (↬ **Finite simple groups**, Prop. 10). On the other hand, C contains a copy of $(\mathrm{P})\mathrm{SL}_m(F)$ for

some field F, where $m \geq (n+3)/4$, hence C does have $\mathrm{Alt}(m)$ as a section ($\looparrowright$ **Finite simple groups**). It is now easy to deduce (16.5).

To prove (16.6) it suffices, in view of CFSG, to observe (a) that $(n-3)/2 \leq \mathrm{rk}(\mathrm{Alt}(n)) \leq n-1$ ($\looparrowright$ **Finite group theory**), (b) that if $C = X_l(\mathbb{F}_{p^e})$ then both l and e are bounded above in terms of $\mathrm{rk}(C)$, and $\mathrm{rk}(C)$ is bounded above by a function of l and e ($\looparrowright$ **Finite simple groups**). ■

While the class $\mathcal{B}_k$ is not closed under taking subgroups, the above proposition gives

Corollary 16.4.3 *For each k there exists k'' such that if $G \in \mathcal{B}_k$ then every section of G belongs to $\mathcal{B}_{k''}$.*

The class $\mathcal{B}_k$ was introduced in the seminal paper [Babai, Cameron & Pálfy 1982]. The main results of that paper are the next two theorems, where f_1, $f_2, \ldots$ denote certain arithmetical functions. (This paper considers groups whose composition factors are the *known* simple groups in $\mathcal{B}_k$, and with this proviso the proofs do not depend on CFSG; the results as stated here do rely on CFSG.)

Theorem 16.4.4 *If G is a primitive permutation group of degree n and $G \in \mathcal{B}_k$ then*

$$|G| \leq n^{f_1(k)}.$$

Theorem 16.4.5 *If V is a finite vector space and $G \in \mathcal{B}_k$ is a completely reducible subgroup of $\mathrm{GL}(V)$ then*

$$|G| \leq |V|^{f_2(k)}.$$

Theorem 16.4.4 may be deduced from a more recent result of [Gluck, Seress & Shalev 1998], which shows that if $G \in \mathcal{B}_k$ is a primitive subgroup of $\mathrm{Sym}(\Omega)$, then Ω contains a subset Δ of cardinality at most Ak^2 such that the pointwise stabiliser of Δ in G is $\{1\}$ (i.e. Δ is a *base* for G); here A is some absolute constant, and it follows easily that then

$$|G| \leq n^{|\Delta|} \leq n^{Ak^2}.$$

(Liebeck and Shalev have since improved the former result to $|\Delta| \leq Ak$; this implies an earlier result of Pyber that f_1 may even be taken to be a *linear* function of k.)

Of course each class $\mathcal{B}_k$ contains the finite soluble groups. For these we can give explicit bounds, due to Pálfy and Wolf:

Theorem 16.4.6 *(*[Manz & Wolf 1993], Theorem 3.5) *If V is a finite vector space and G is a completely reducible soluble subgroup of $\mathrm{GL}(V)$ then*

$$|G| < \frac{1}{2}|V|^{9/4}.$$

Theorem 16.4.7 *(*[Manz & Wolf 1993], Corollary 3.6) *If G is a primitive soluble subgroup of* $\mathrm{Sym}(n)$ *then*

$$|G| < \frac{1}{2}n^{13/4}.$$

Permutation groups in the class $\mathcal{C}_k^{\lhd}$ also have bounded orders. The next result was originally proved with a slightly weaker bound in [Babai, Cameron & Pálfy 1982]; the present form is due to [Maróti] (and for $k \geq 9$ to A. Mann, independently):

Theorem 16.4.8 *Let $G \leq \mathrm{Sym}(n)$. If $G \in \mathcal{C}_k^{\lhd}$, where $k \geq 4$, then*

$$|G| \leq \mu^{n-1}$$

where

$$\mu = k!^{1/(k-1)}.$$

Proof. This is clear if $n \leq k$. Suppose that $n > k$ and argue by induction on n. Note that $\mu \geq 4!^{1/3} > 2$.

Case 1. Suppose that G is primitive. Since $k < n$, the group G does not contain $\mathrm{Alt}(n)$; Theorem 16.4.1 (16.4) now shows that $|G| \leq 2^{n-1} < \mu^{n-1}$ unless G is one of the 24 known exceptions listed in [Maróti]; for these the claim can be checked case by case.

Case 2. Suppose that G is imprimitive. Then G preserves a system of blocks of sizes $r_1, \ldots, r_s$, say, where $r_i < n$, $s < n$ and $r_1 + \cdots + r_s = n$. The action of G on the set of blocks gives a homomorphism $\phi : G \to \mathrm{Sym}(s)$ with kernel K, say. Let K_i denote the group of permutations induced by K on the ith block. Then $K_i \leq \mathrm{Sym}(r_i)$ for each i, and the inductive hypothesis gives $|K_i| \leq \mu^{r_i - 1}$, while $|\phi(G)| \leq \mu^{s-1}$. It follows that

$$|G| \leq \prod_{i=1}^{s} |K_i| \cdot |\phi(G)| \leq \mu^{\sum (r_i - 1)} \mu^{(s-1)} = \mu^{n-1}.$$

■

The constant μ given here is *best possible*, as shown by the iterated permutational wreath product of k^r copies of $\mathrm{Sym}(k)$, a permutation group of degree $n = k^{r+1}$ and order $k!^{(n-1)/(k-1)}$. This observation is also due to Maróti.

Taking $k = 4$ we deduce

Corollary 16.4.9 *If G is a soluble subgroup of* $\mathrm{Sym}(n)$ *then $|G| \leq \mu^{n-1}$ where $\mu = (24)^{1/3}$.*

This was obtained earlier by Dixon (see [DM], Theorem 5.8B)

One connection with subgroup growth (by no means the only one) is manifested in the following way. Let H be a subgroup of G. The *normal core* of H in G is

$$\mathrm{core}_G(H) = \bigcap_{g \in G} H^g;$$

this is the biggest normal subgroup of G contained in H. Similarly, the *subnormal core* of H is

$$\mathrm{core}_{\mathrm{sn}G}(H) = \langle K \lhd\lhd G \mid K \leq H \rangle ;$$

by a classical theorem of Wielandt (see [R], **13.1.8**) this is the biggest subnormal subgroup of G contained in H. The following result is from an unpublished manuscript of L. Pyber and A. Shalev.

Proposition 16.4.10 (L. Pyber & A. Shalev) *Let $\mathcal{X}$ be a family of finite groups.*

(i) there exists k such that $\mathcal{X} \subseteq \mathcal{C}_k^{\lhd}$ if and only if there exists c such that

$$|G : \mathrm{core}_G(H)| \leq c^{|G:H|} \tag{16.7}$$

for every $G \in \mathcal{X}$ and every $H \leq G$ ('exponential core condition').

(ii) there exists k such that $\mathcal{X} \subseteq \mathcal{B}_k$ if and only if there exists c such that

$$|G : \mathrm{core}_{\mathrm{sn}G}(H)| \leq |G : H|^c \tag{16.8}$$

for every $G \in \mathcal{X}$ and every $H \leq G$ ('polynomial subnormal core condition').

Proof. (i) Suppose that $G \in \mathcal{C}_k^{\lhd}$; we may assume that $k \geq 6$. Let $H < G$ with $|G : H| = n$. Then the action of G on the right cosets of H gives a permutation representation $G \to \mathrm{Sym}(n)$ with kernel $\mathrm{core}_G(H)$, and it follows by Theorem 16.4.8 that

$$|G : \mathrm{core}_G(H)| \leq \mu^{n-1};$$

so (16.7) holds with $c = k$ (since $\mu \leq k$).

Conversely, suppose that (16.7) holds, and that G has a composition factor isomorphic to $S = \mathrm{Alt}(m)$, where $m \geq 7$. Let $N \lhd G$ be maximal such that S is a composition factor of G/N, and write $\overline{G} = G/N$. Then $\overline{G}$ has a unique minimal normal subgroup $M = S_1 \times \cdots \times S_r$ where $S_i \cong S$ for each i, and $\mathrm{C}_{\overline{G}}(M) = 1$. Let U be a subgroup of index m in S_1, put $L = \mathrm{N}_{\overline{G}}(S_1)$ and $H = \mathrm{N}_L(U)$. Since G permutes $S_1, \ldots, S_r$ transitively, $\left|\overline{G} : L\right| = r$, and since every subgroup of index m in $\mathrm{Alt}(m)$ is a point-stabiliser (this holds because $m \geq 7$) we have $|L : H| \leq m$. Thus

$$\left|\overline{G} : H\right| \leq mr.$$

On the other hand, $H \cap S_1 = U < S_1$, so H does not contain M and it follows that $\mathrm{core}_{\overline{G}}(H) = 1$. Of course, (16.7) still holds with $\overline{G}$ in place of G, giving

$$\left(\frac{m!}{2}\right)^r \leq \left|\overline{G}\right| = \left|\overline{G} : \mathrm{core}_{\overline{G}}(H)\right| \leq c^{|\overline{G}:H|} \leq c^{mr}.$$

Hence $m^{m/2} \leq m! \leq 2c^m$ and so $m \leq 2c^2$. It follows that $G \in \mathcal{C}_k^{\lhd}$ where $k = \max\{6, \lceil 2c^2 \rceil\}$.

(ii) Suppose that $G \in \mathcal{B}_k$, and let $H < G$ with $|G : H| = n$. We claim that (16.8) holds with $c = f_1(k)$. Replacing G by $G/\mathrm{core}_G(H)$, we may assume that G is a subgroup of $\mathrm{Sym}(n)$ and that H is the stabiliser of 1, say.

Case 1. Suppose that G is primitive. Then $|G| \leq n^c$ by Theorem 16.4.4, and the result is immediate.

Case 2. Suppose that G is not primitive. The action of G on a minimal system of imprimitivity gives a homomorphism $\theta : G \to \mathrm{Sym}(r)$, where $1 < r < n$ and $\theta(G)$ is a primitive subgroup of $\mathrm{Sym}(r)$. As above, $|\theta(G)| \leq r^c$. Put $K = \ker\theta$. Then $H \cap K$ is the stabiliser of 1 in K, so $|K : H \cap K|$ is the length of the K-orbit of 1, which is at most the size of a block, namely n/r. Making the natural inductive hypothesis, we may suppose that $H \cap K$ contains a subnormal subgroup L of K with $|K : L| \leq (n/r)^c$. But then L is subnormal in G so

$$\begin{aligned} |G : \mathrm{core}_{\mathrm{sn}G}(H)| \leq |G : L| &= |G : K|\,|K : L| \\ &\leq r^c(n/r)^c = n^c. \end{aligned}$$

The proof of the converse is similar in spirit to the corresponding part of (i), but more complicated, and we omit the details. (The result in this direction will not be needed in this book). ■

Corollary 16.4.11 *Let G be a transitive subgroup of* $\mathrm{Sym}(n)$. *If $G \in \mathcal{B}_k$ then the exponent of G is at most n^c, where $c = f_1(k)$.*

Proof. Let H be a point stabiliser in G. By (ii), H contains a subnormal subgroup U of G with $n^c \geq |G : U| = t$, say. Then $G^t \leq U$, so $G^t \leq \mathrm{core}_G(H) = 1$. (The proof of (ii) gives $c = f_1(k)$.) ■

Let $cf(G)$ denote the *product of the orders of all the composition factors of* G (each isomorphism type being counted once). The following result, due to L. Pyber, is a slight variation of one in [Segal 1996$_b$]:

Proposition 16.4.12 *Let G be a transitive subgroup of* $\mathrm{Sym}(n)$. *If $G \in \mathcal{B}_k$ then $cf(G)$ is at most n^c, where $c = f_1(k)$.*

Proof. If G is primitive this is clear from Theorem 16.4.4. Otherwise, G permutes transitively a set of r blocks, each of size b, where $r < n$, $b < n$ and $br = n$. Let N be the kernel of this action. Provided the blocks are chosen as small as possible, N induces equivalent transitive permutation groups on the blocks. So N is a subdirect product of copies of some transitive subgroup $T \leq \mathrm{Sym}(b)$, and $T \in \mathcal{B}_k$. Inductively, we may suppose that $cf(G/N) \leq r^c$ and $cf(T) \leq b^c$. The result follows since $cf(N) = cf(T)$, $cf(G) \leq cf(N) \cdot cf(G/N)$ and $br = n$. ■

The next result gives an upper bound for the size of primitive groups under weaker hypotheses than that of Theorem 16.4.4. It may be deduced from [Cameron 1981], Theorem 6.1.

Theorem 16.4.13 *Let H be a primitive subgroup of* $\mathrm{Sym}(n)$*. If $H \in \mathcal{C}_k^{\triangleleft}$ then $|H| \leq n^{c \log n}$ where c is a constant depending on k.*

Corollary 16.4.14 *Let G be a transitive subgroup of* $\mathrm{Sym}(n)$*. If $G \in \mathcal{C}_k^{\triangleleft}$ then the exponent of G is at most $n^{c \log n}$.*

Proof. If G is primitive this follows from the theorem. If not, then G permutes transitively a set of k blocks, each of size n/k, where $1 < k < n$. Let N be the kernel of this action. Provided the blocks are chosen as small as possible, N induces equivalent transitive permutation groups on the blocks. Inductively we may suppose that these permutation groups have (the same) exponent at most $(n/k)^{c \log(n/k)}$, and that G/N has exponent at most $k^{c \log k}$. The result follows since

$$k^{c \log k} \cdot (n/k)^{c \log(n/k)} \leq n^{c \log n}.$$

■

The next result applies to classes such as $\mathcal{C}_k$:

Theorem 16.4.15 ([Borovik, Pyber & Shalev 1996], Thm 1.2) *Let $\mathcal{C}$ be a class of finite groups that is closed under taking subgroups, quotients and extensions, contains all finite soluble groups but does not contain all finite groups. Then there is a constant c (depending on $\mathcal{C}$) such that for every n, the maximal transitive $\mathcal{C}$-subgroups of* $\mathrm{Sym}(n)$ *lie in at most n^c conjugacy classes in* $\mathrm{Sym}(n)$*.*

Finally we have the following bound for the number of conjugacy classes of primitive groups:

Theorem 16.4.16 ([Pyber & Shalev 1996], Thm 1.) *There is an absolute constant c such that, for each n, the group* $\mathrm{Sym}(n)$ *has at most $n^{c \log n}$ conjugacy classes of primitive subgroups.*

The last four theorems all depend on CFSG. The proofs involve detailed information on the subgroup structure of finite simple groups and powerful techniques of permutation group theory; we cannot go into them here.

3 Subgroups of alternating groups

For sets $\Delta \subseteq \Omega$ we make the convention that $\mathrm{Alt}(\Delta)$ is identified with the pointwise stabiliser in $\mathrm{Alt}(\Omega)$ of $\Omega \setminus \Delta$.

Definition Let Ω be a finite set. A *standard subgroup* of $\mathrm{Sym}(\Omega)$ is a subgroup of the form

$$\mathrm{Alt}(\Omega_1) \times \cdots \times \mathrm{Alt}(\Omega_r)$$

where $\Omega_1, \ldots, \Omega_r$ are disjoint subsets of Ω of cardinality at least 5. We allow $r = 0$, corresponding to the identity subgroup.

The following theorem is the key to counting subgroups in products of finite alternating groups.

Theorem 16.4.17 [Pyber (b)] *Let Ω be a finite set and S a standard subgroup of* $\mathrm{Sym}(\Omega)$*. Then each subgroup H of S contains a standard subgroup H_* of* $\mathrm{Sym}(\Omega)$ *such that*

$$|S : H_*| \leq |S : H|^5 . \tag{16.9}$$

Note that (16.9) is equivalent to

$$|H : H_*| \leq |S : H|^4 . \tag{16.10}$$

We sketch the proof, which is basically a dévissage to Bochert's theorem. The first reduction is to

Proposition 16.4.18 *Let $H < \mathrm{Sym}(n)$ where $n \geq 5$. Then H contains a standard subgroup H_* of* $\mathrm{Sym}(n)$ *such that*

$$|H : H_*| \leq |\mathrm{Sym}(n) : H|^3 . \tag{16.11}$$

Let us assume this for now and deduce Theorem 16.4.17. So let

$$H < S = \mathrm{Alt}(\Omega_1) \times \cdots \times \mathrm{Alt}(\Omega_r)$$

where $|\Omega_i| \geq 5$ for each i. Put $A = \mathrm{Alt}(\Omega_1)$ and $B = \mathrm{Alt}(\Omega_2) \times \cdots \times \mathrm{Alt}(\Omega_r)$.

Suppose first that $r = 1$, so $S = \mathrm{Alt}(n)$, $n \geq 5$. The proposition gives a standard subgroup H_* of H such that $|H : H_*| \leq (2\,|S : H|)^3 = 8\,|S : H|^3$; this implies (16.10) unless $n < 8$. If $5 \leq n \leq 7$ then

$$|H| \leq \frac{1}{2}(n-1)! < n^4 \leq |S : H|^4 ,$$

and we take $H_* = 1$.

Now suppose that $r > 1$. Then $S = A \times B$. Let X, Y denote the projections of H into A and B and put $D_A = H \cap A$, $D_B = H \cap B$. Note that $D_A \lhd X$, $D_B \lhd Y$ and

$$|X|\,|D_B| = |H| = |Y|\,|D_A| .$$

Inductively we may suppose that there exist standard groups $X_* \leq X$ and $Y_* \leq Y$ such that $|X : X_*| \leq |A : X|^4$ and $|Y : Y_*| \leq |B : Y|^4$. Put

$$H_* = (H \cap X_*)(H \cap Y_*) = (D_A \cap X_*) \times (D_B \cap Y_*).$$

Since any normal subgroup of a standard group is standard (because $\mathrm{Alt}(k)$ is simple for $k \geq 5$), we see that H_* is a standard group. Moreover, since $H \leq X \times Y$,

$$\begin{aligned} |H : H_*| &\leq |X : X_*|\,|X_* : D_A \cap X_*| \cdot |Y : Y_*|\,|Y_* : D_B \cap Y_*| \\ &\leq \frac{|A|^4}{|X|^4} \cdot \frac{|X|}{|D_A|} \cdot \frac{|B|^4}{|Y|^4} \cdot \frac{|Y|}{|D_B|} \\ &= \frac{|S|^4}{|XY|^3\,|H|} \leq |S : H|^4 . \end{aligned} \tag{16.12}$$

This completes the reduction, and it remains to prove Proposition 16.4.18. Write $S = \mathrm{Sym}(\Omega)$ and put $n = |\Omega|$. Note that (16.11) is equivalent to

$$|H|^4 \leq (n!)^3 |H_*| . \tag{16.13}$$

Case 1. Where $H < S$ is primitive. This is the heart of the proof. If $H = \mathrm{Alt}(n)$ we take $H_* = H$. Otherwise, H is a proper primitive group, and Bochert's result Theorem 16.4.1(1) shows that $|S : H| \geq \lceil n/2 \rceil !$. It is easy to see that then

$$|S : H|^4 \geq n! = |S| ,$$

so we may take $H_* = 1$.

Case 2. Where H is transitive but imprimitive. Then H preserves a partition of Ω into blocks $\Omega_1, \ldots, \Omega_s$ each of size r, say, where $rs = n$ and $1 < r < n$. Let

$$K = \ker(H \to \mathrm{Sym}(s))$$

be the kernel of the permutation action of H on the set $\{\Omega_1, \ldots, \Omega_s\}$ and let $P_i \leq \mathrm{Sym}(\Omega_i)$ be the group induced by K on Ω_i. Then the P_i are conjugate under H and H is contained in the permutational wreath product $P \wr \mathrm{Sym}(s)$ where $P = P_1$; so

$$|H| \leq |P^s| \, s! \leq (r!)^s s!.$$

Choosing r as small as possible we ensure that P is a primitive subgroup of $\mathrm{Sym}(\Omega_1) = \mathrm{Sym}(r)$. We will repeatedly use the elementary estimate

$$(r!)^s (s!)^r \leq n!.$$

Subcase 2.1: where $2 \leq r \leq 4$. In this case we have

$$|H|^4 \leq (r!)^{4s} (s!)^4 \leq (n!)^3$$

(an easy estimate if $s \geq 3$, a direct calculation when $s = 2$). So $H_* = 1$ will do.

Assume henceforth that $r \geq 5$, and put

$$Q = \mathrm{Alt}(\Omega_1) \times \cdots \times \mathrm{Alt}(\Omega_s).$$

Subcase 2.2: where P is a proper primitive subgroup of $\mathrm{Sym}(\Omega_1)$. Applying Bochert's theorem to P we find that $|H|^4 \leq (n!)^3$ by a calculation similar to the preceding subcase. Take $H_* = 1$ in this case.

Subcase 2.3: where $K \geq Q$. Put $H_* = Q$. A simple calculation shows that (16.13) holds in this case.

Subcase 2.4: where K does not contain Q but $P_i \geq \mathrm{Alt}(\Omega_i)$ for each i. Then $K \cap P_i = 1$ for each i. The following is a nice exercise:

Lemma 16.4.19 *Let $N \leq Q = A_1 \times \cdots \times A_s$ where the A_i are isomorphic finite simple groups. Suppose that N projects onto each direct factor A_i but $N \not\geq A_i$ for each i. Then $|N| \leq |Q|^{1/2}$.*

(cf. [Cameron 1999], Exercise 4.3). Applying this to $K \cap Q$ we infer that $|K \cap Q| \leq |Q|^{1/2}$ and hence that

$$|K| \leq 2^s \, |K \cap Q| \leq 2^s (r!/2)^{s/2}.$$

A short calculation using $|H| \leq s! \, |K|$ now yields $|H|^4 \leq (n!)^3$, and we take $H_* = 1$ in this case.

Case 3: where H is intransitive. Then $H \leq A \times B$ where $A = \mathrm{Sym}(\Omega_1)$, $B = \mathrm{Sym}(\Omega_2)$ and $\Omega = \Omega_1 \cup \Omega_2$ is a non-trivial partition of Ω. Put $r = |\Omega_1|$ and $s = |\Omega_2| = n - r$, and suppose that $r \leq s$. As above, let X, Y denote the projections of H into A and B and put $D_A = H \cap A$, $D_B = H \cap B$. Note that $|S : H| \geq |S : AB| = \binom{n}{r}$.

Subcase 3.1: where $s \leq 4$. One verifies directly that $\binom{n}{r}^4 > n!$, whence

$$|H| \leq r!s! < \binom{n}{r}^3 \leq |S : H|^3 .$$

Take $H_* = 1$.

Subcase 3.2: where $r \leq 4 < s$. Suppose that $D_B < B$. Inductively we may suppose that D_B contains a standard subgroup T such that $|D_B : T| \leq |B : D_B|^3$. In this case we put $H_* = T$. Then

$$\begin{aligned} |H : H_*| &\leq |H : D_B| \, |B : D_B|^3 \\ &\leq |A| \cdot |AB : H|^3 \\ &\leq r! \binom{n}{r}^{-3} |S : H|^3 \leq \frac{24}{125} |S : H|^3 . \end{aligned}$$

If $D_B = B$ we take $H_* = \mathrm{Alt}(\Omega_1)$ and get $|H : H_*| \leq 48 < |S : H|$.

Subcase 3.3: where $s \geq r \geq 5$. Suppose that $X < A$ and $Y < B$. Inductively we find standard subgroups $X_* \leq X$ and $Y_* \leq Y$ such that $|X : X_*| \leq |A : X|^3$ and $|Y : Y_*| \leq |B : Y|^3$. Put

$$H_* = (H \cap X_*)(H \cap Y_*) = (D_A \cap X_*) \times (D_B \cap Y_*).$$

As in (16.12), above, we then have

$$|H : H_*| \leq |AB : H|^3 \leq \binom{n}{r}^{-3} |S : H|^3 .$$

If $X = A$ or $Y = B$, replace H by the inverse image in H of $\mathrm{Alt}(\Omega_1) \times \mathrm{Alt}(\Omega_2)$. This introduces a factor of at most 4^4 in the last equation. In any case, $|H : H_*| \leq |S : H|^3$.

This completes the proof.

Window: Profinite groups

For background on profinite groups we recommend Wilson's book [Wi] and the book of Ribes and Zalesskii [RZ], where detailed proofs and generalisations can be found for the results stated below. For pro-p groups a convenient source is the book of Dixon, du Sautoy, Mann and Segal [DDMS].

Let us recall some definitions and elementary properties.

Let $\mathcal{C}$ be a class of finite groups. We assume throughout that $\mathcal{C}$ is closed under taking normal subgroups, quotient groups and finite subdirect products, and that $\mathcal{C}$ contains a non-trivial group. A *pro-$\mathcal{C}$ group* is the inverse limit of an inverse system of epimorphisms of groups in $\mathcal{C}$. When $\mathcal{C}$ is the class of all finite groups a pro-$\mathcal{C}$ group is called a *profinite group*. This is a compact Hausdorff topological group whose open subgroups form a base for the neighbourhoods of 1 (and a subgroup is open if and only if it is closed and of finite index). In general, a profinite group G is a pro-$\mathcal{C}$ group if and only if $G/N \in \mathcal{C}$ for every open normal subgroup N of G. When $\mathcal{C}$ is the class of all finite p-groups for a fixed prime p (respectively, all finite nilpotent groups, or all finite soluble groups), a pro-$\mathcal{C}$ group is called a *pro-p group* (resp. a *pronilpotent* group, a *prosoluble* group).

In the context of profinite groups, one commonly uses 'subgroup' to mean 'closed subgroup', and 'generating set' to mean 'topological generating set'; in particular, a profinite group is said to be *finitely generated* if it is *topologically* generated by a finite subset (note that an infinite profinite group can never be finitely generated as an 'abstract' group, since it is necessarily uncountable). Also 'homomorphism' normally means 'continuous homomorphism'. The profinite group G can be generated by d elements if and only if G is the inverse limit of finite d-generator groups, and this holds if and only if G/N is a d-generator group for every open normal subgroup N of G.

1 Completions

Let Γ be a finitely generated group. The *pro-$\mathcal{C}$ topology* on Γ is defined by taking as a fundamental system of neighborhoods of the identity the collection of all normal subgroups N of Γ such that $\Gamma/N \in \mathcal{C}$. A subgroup H is then open in Γ if and only if H contains a normal subgroup N of Γ such that $\Gamma/N \in \mathcal{C}$ (this implies that H has finite index in Γ). We can complete Γ with respect to this

topology to get

$$\widehat{\Gamma}_{\mathcal{C}} = \varprojlim \{\Gamma/N \mid N \lhd \Gamma \text{ and } \Gamma/N \in \mathcal{C}\};$$

this is the *pro-$\mathcal{C}$ completion* of Γ (it is denoted $\Gamma_{\widehat{\mathcal{C}}}$ in [RZ]). It has a natural topology, making it into a pro-$\mathcal{C}$ group, inherited from the product topology on

$$\prod \{\Gamma/N \mid N \lhd \Gamma \text{ and } \Gamma/N \in \mathcal{C}\}$$

where each of the finite groups Γ/N is given the discrete topology. There is a natural homomorphism (continuous w.r.t. the pro-$\mathcal{C}$ topology)

$$i : \Gamma \to \widehat{\Gamma}_{\mathcal{C}}$$

given by $i(\gamma) = \lim(\gamma N)$. The kernel of i is the *$\mathcal{C}$-residual* of Γ, that is the intersection of all $N \lhd \Gamma$ such that $\Gamma/N \in \mathcal{C}$. In particular, i is injective if and only if Γ is residually-$\mathcal{C}$, that is, if the $\mathcal{C}$-residual of Γ is equal to 1.

If $\mathcal{C} = \{\text{all finite groups}\}$ we write $\widehat{\Gamma}_{\mathcal{C}} = \widehat{\Gamma}$: this is the *profinite completion* of Γ; if $\mathcal{C} = \{\text{all finite } p\text{-groups}\}$ we write $\widehat{\Gamma}_{\mathcal{C}} = \widehat{\Gamma}_p$: this is the *pro-$p$ completion* of Γ (also sometimes denoted $\Gamma_{\widehat{p}}$; the authors disagree as to which notation is preferable).

Proposition 16.4.1 The universal property*: the pair $(\widehat{\Gamma}_{\mathcal{C}}, i)$ is characterized by the following: $i(\Gamma)$ is a dense subgroup of $\widehat{\Gamma}_{\mathcal{C}}$, and for every pro-$\mathcal{C}$ group P and every continuous (relative to the pro-$\mathcal{C}$ topology) homomorphism $\varphi : \Gamma \to P$ there exists a (necessarily unique) continuous homomorphism $\varphi_* : \widehat{\Gamma}_{\mathcal{C}} \to P$ such that $\varphi_* \circ i = \varphi$. Moreover, this holds if it holds for every continuous homomorphism φ from Γ to a (*finite*) group $P \in \mathcal{C}$.*

If $\mathcal{C}_1 \subseteq \mathcal{C}_2$ then $\widehat{\Gamma}_{\mathcal{C}_1}$ is the maximal pro-$\mathcal{C}_1$ quotient of $\widehat{\Gamma}_{\mathcal{C}_2}$.

Note that if $\mathcal{C}$ is closed under taking subgroups, then every homomorphism $\Gamma \to P$ is continuous.

When the group Γ is residually-$\mathcal{C}$, we normally identify Γ with its image under i in $\widehat{\Gamma}_{\mathcal{C}}$.

Corollary 16.4.2 *Let $N \lhd \Gamma$. Then the quotient mapping $\Gamma \to \Gamma/N$ induces an isomorphism*

$$\widehat{\Gamma}_{\mathcal{C}}/\overline{N} \xrightarrow{\simeq} \widehat{(\Gamma/N)}_{\mathcal{C}}$$

where $\overline{N}$ denotes the closure of $i(N)$ in $\widehat{\Gamma}_{\mathcal{C}}$.

Proof. N is contained in the kernel of the composed homomorphism $\Gamma \to \widehat{\Gamma}_{\mathcal{C}} \to \widehat{\Gamma}_{\mathcal{C}}/\overline{N}$ so we have an induced homomorphism $\Gamma/N \to \widehat{\Gamma}_{\mathcal{C}}/\overline{N}$. This in turn induces a homomorphism $\alpha : \widehat{(\Gamma/N)}_{\mathcal{C}} \to \widehat{\Gamma}_{\mathcal{C}}/\overline{N}$. On the other hand, $\Gamma \to \Gamma/N$ induces a homomorphism $\widehat{\Gamma}_{\mathcal{C}} \to \widehat{(\Gamma/N)}_{\mathcal{C}}$ whose kernel contains $\overline{N}$, giving $\beta : \widehat{\Gamma}_{\mathcal{C}}/\overline{N} \xrightarrow{\simeq} \widehat{(\Gamma/N)}_{\mathcal{C}}$. It is easy to see that α and β are mutual inverses. ■

Proposition 16.4.3 *Suppose that Γ is residually-$\mathcal{C}$. Then there is a one-to-one correspondence between the set $\mathcal{X}$ of all subgroups of Γ that are open in the pro-$\mathcal{C}$ topology of Γ and the set $\mathcal{Y}$ of all open subgroups of $\widehat{\Gamma}_{\mathcal{C}}$, given by*

$$X \mapsto \overline{X} \qquad (H \in \mathcal{X})$$
$$Y \mapsto Y \cap \Gamma \qquad (Y \in \mathcal{Y})$$

where $\overline{X}$ denotes the closure of X in $\widehat{\Gamma}_{\mathcal{C}}$. Moreover,

$$|\Gamma : X| = \left|\widehat{\Gamma}_{\mathcal{C}} : \overline{X}\right|.$$

This shows that the number

$$a_n(\widehat{\Gamma}_{\mathcal{C}})$$

of open subgroups of index n in $\widehat{\Gamma}_{\mathcal{C}}$ is equal to the number of subgroups of index n in Γ that are open in the pro-$\mathcal{C}$ topology. For example, we have $a_n(\widehat{\Gamma}) = a_n(\Gamma)$ for each n, while $a_n(\widehat{\Gamma}_p)$ is equal to the number of *subnormal* subgroups of index n in Γ when n is a power of the prime p. Though quite elementary this observation is fundamental for this book, and we sketch the proof.

Write $G = \widehat{\Gamma}_{\mathcal{C}}$, and let N be a normal subgroup of Γ such that $\Gamma/N \in \mathcal{C}$. Then Γ/N is a pro-$\mathcal{C}$ group so the residue-class mapping $\varphi : \Gamma \to \Gamma/N$ induces a homomorphism $\varphi_* : G \to \Gamma/N$ such that $\varphi_*|_\Gamma = \varphi$. Thus writing $\widetilde{N} = \ker \varphi_*$ we have $\widetilde{N} \cap \Gamma = N$; also $\widetilde{N}$ is open in G (being a closed subgroup of finite index), and as Γ is dense in G it follows that $\widetilde{N}$ is exactly the closure $\overline{N}$ of N in G and that $\overline{N}\Gamma = G$. Thus Γ/N is naturally isomorphic to $G/\overline{N}$, and the assignment $X \mapsto X\overline{N}$ is an index-preserving bijection from the set of subgroups X of Γ with $N \leq X$ to the set of all subgroups Y of G with $Y \geq \overline{N}$. It is clear that if $Y = X\overline{N}$ then $Y \cap \Gamma = X$ and that Y is the closure of X in G. All the claims of the proposition follow easily from this.

We emphasise that subgroup growth questions about profinite groups always refer to the number of *open* subgroups of a given index; it is not known whether a finitely generated profinite group can have subgroups of finite index that are not open. (This cannot happen in pro-p groups – see [DDMS], Chapter 1 – nor more generally in prosoluble groups [Segal 2000]).

Proposition 16.4.4 *Assume (additionally) that the class $\mathcal{C}$ is closed under taking subgroups and extensions. Suppose that Γ is residually-$\mathcal{C}$ and that $X \leq \Gamma$ is open in the pro-$\mathcal{C}$ topology. Then the closure of X in $\widehat{\Gamma}_{\mathcal{C}}$ is isomorphic to $\widehat{X}_{\mathcal{C}}$.*

Proof. Suppose $M \lhd X$ is such that $M/X \in \mathcal{C}$. Let M_0 be the Γ-core of M (the intersection of all Γ-conjugates of M); then $X/M_0 \in \mathcal{C}$, being a finite subdirect product of copies of X/M. Also there exists $N \lhd \Gamma$ with $N \leq X$ such that $\Gamma/N \in \mathcal{C}$. Now put $D = M_0 \cap N$. The hypotheses on $\mathcal{C}$ imply that $\Gamma/D \in \mathcal{C}$. From the proof of Proposition 16.4.3 we have

$$\overline{X} = X\overline{D},\ \overline{X} \cap \Gamma = X \ \text{ and } \ X \cap \overline{D} = \Gamma \cap \overline{D} = D.$$

Thus the quotient map $X \to X/D$ lifts to the quotient map $\overline{X} \to \overline{X}/\overline{D}$, and it follows that the quotient map $X \to X/M$ lifts to a homomorphism from $\overline{X}$ onto $\overline{X}/M\overline{D} \cong X/M$.

This shows that the inclusion mapping $X \to \overline{X}$ has the universal property with respect to continuous homomorphisms from X into $\mathcal{C}$-groups, and the result follows from Proposition 16.4.1. ■

2 Free profinite groups

Let r be a positive integer and let $F = F_r$ be the free group on the set $X = \{x_1, \ldots, x_r\}$. The pro-$\mathcal{C}$ completion $\widehat{F}_{\mathcal{C}}$ of F is the *free pro-$\mathcal{C}$ group on r generators.* That is, the mapping

$$j = i|_X : X \to \widehat{F}_{\mathcal{C}}$$

has the universal property: for every pro-$\mathcal{C}$ group G and every map φ from the set X to G there is a unique continuous homomorphism $\tilde{\varphi} : \widehat{F}_{\mathcal{C}} \to G$ such that $\tilde{\varphi} \circ j = \varphi$.

Proposition 16.4.5 *Assume (additionally) that the class $\mathcal{C}$ is closed under taking subgroups and extensions. Let $F = F_r$.*

(i) *Let T be a subgroup of F that is open in the pro-$\mathcal{C}$ topology, with $|F : T| = l$. Then the closure $\overline{T}$ of T in $\widehat{F}_{\mathcal{C}}$ is a free pro-$\mathcal{C}$ group on $1+l(r-1)$ generators.*

(ii) *Let Y be an open subgroup of index l in $\widehat{F}_{\mathcal{C}}$. Then Y is a free pro-$\mathcal{C}$ group on $1 + l(r-1)$ generators.*

It is known (see for example [RZ], Proposition 3.3.15) that F is residually-$\mathcal{C}$. The proposition then follows from Propositions 16.4.1 and 16.4.4, in view of the Nielsen-Schreier Theorem (see [R], Theorem 6.1.1) which shows that X is a free group on $1 + l(r-1)$ generators. But a warning is needed here: the proof of Proposition 16.4.4 used crucially the fact that $\mathcal{C}$ is closed under extensions. (In fact we gave the proof to stress this point!) If $\mathcal{C}$ is the class of nilpotent groups, for example, which is not extension closed, then Proposition 16.4.5 fails to hold. Indeed, $\widehat{F}_{\mathcal{C}}$ is then the Cartesian product of its Sylow pro-p subgroups $\widehat{F}_p$, over all primes p; so $\widehat{F}_{\mathcal{C}}$ has an open subgroup of prime index q which takes the form

$$\prod_{p \neq q} \widehat{F}_p \times \widehat{F^*}_q$$

where F^* is free on $1+q(r-1)$ generators; this group is neither free pro-nilpotent on r generators nor on $1 + q(r-1)$ generators.

For most purposes, it is safe to assume that we are dealing with a class $\mathcal{C}$ that has all the desirable closure properties mentioned above; however, we will also be interested in group classes defined by restrictions on *composition factors*: such classes are not in general closed under taking subgroups, so a little care is sometimes necessary.

Warning The definition of a free pro-$\mathcal{C}$ group on an *infinite* set of generators has to be slightly modified: see [Wi] §5.1 or [RZ] §3.3. We shall not be needing this.

3 Profinite presentations

We assume throughout this section that the class $\mathcal{C}$ is closed under subgroups, quotients and extensions. Let $F = \widehat{F}_{\mathcal{C}}$ be the free pro-$\mathcal{C}$ group on the finite set $X = \{x_1, \ldots, x_d\}$, and let K be a closed normal subgroup of F. Suppose that K is generated as a closed normal subgroup of F by a subset Y (that is, K is generated topologically by the conjugates of all elements of Y). We write

$$F/K = \langle X; Y \rangle .$$

It is natural to interpret this as the pro-$\mathcal{C}$ group generated by X subject to the 'relations' Y, but we have to extend the language of 'group words' in the following way. If $w \in F$ and H is a pro-$\mathcal{C}$ group containing elements $h_1, \ldots, h_d$, the expression

$$w(h_1, \ldots, h_d)$$

denotes the element $\varphi(w) \in H$ where $\varphi : F \to H$ is the unique homomorphism $F \to H$ sending x_i to h_i for $i = 1, \ldots, d$. It is now clear that $\langle X; Y \rangle$ has the usual universal property: if G is any pro-$\mathcal{C}$ group generated by d elements $g_1, \ldots, g_d$ such that

$$w(g_1, \ldots, g_d) = 1 \quad \text{for all } w \in Y,$$

then there exists a unique epimorphism $\pi : \langle X; Y \rangle \to G$ with $\pi(x_i K) = g_i$ for $i = 1, \ldots, d$.

In particular, if this π is an *isomorphism* we say that G is generated by $\{g_1, \ldots, g_d\}$ subject to the relations $\{w(g_1, \ldots, g_d) \mid w \in Y\}$, and write

$$G = \langle g_1, \ldots, g_d; Y \rangle .$$

This is called a pro-$\mathcal{C}$ presentation of G (it is usual also to say that G has a pro-$\mathcal{C}$ presentation $\langle X; Y \rangle$ if X is a set bijective with $\{g_1, \ldots, g_d\}$).

Proposition 16.4.6 *Suppose that $G = \widehat{\Gamma}_{\mathcal{C}}$ where Γ is a finitely generated (abstract) group. If*

$$\Gamma = \langle X; Y \rangle$$

is a presentation for Γ (in the usual sense), where X is finite, then

$$G = \langle X; Y \rangle$$

is a pro-$\mathcal{C}$ presentation for G.

Proof. Let Φ be the free (abstract) group on X and N the normal closure of Y in Φ. By Corollary 16.4.2 we have

$$\widehat{\Phi}_{\mathcal{C}}/\overline{N} \cong \widehat{(\Phi/N)}_{\mathcal{C}} \cong \widehat{\Gamma}_{\mathcal{C}} = G.$$

The result follows since $\widehat{\Phi}_{\mathcal{C}}$ is the free pro-$\mathcal{C}$ group on X and $\overline{N}$ is the closed normal subgroup generated by (the image of) Y. ■

It follows that if a *finite* group $\Gamma \in \mathcal{C}$ has a presentation with d generators and r relations, then it has such a pro-$\mathcal{C}$ presentation. Whether the *converse* is true, however, is a long-standing open problem, both for $\mathcal{C}$ the class of all finite groups and for $\mathcal{C}$ the class of finite p-groups (the problem is whether a set of r 'infinite' relations, i.e. profinite ones, can be replaced by a set of r ordinary finite relations).

For the remainder of this section, we take $\mathcal{C}$ to be the class of all finite groups, and consider profinite presentations of a *finite* group G. Let F be the free profinite group on a set X of d generators and suppose that

$$G = F/N = \langle X;\, R\rangle$$

where now N is an open normal subgroup of F, generated as a normal subgroup by the set R. Write $N' = \overline{[N,N]}$ for the closure of the derived group of N. Then G acts by conjugation on the abelian group N/N', and the resulting G-module is called the *relation module* of the associated presentation. For each prime p, we put $N(p) = N'N^p$, and call $N/N(p)$ the *mod p relation module*.

For any G-module M let $d_G(M)$ denote the minimal number of module generators required by M. It is obvious that

$$d_G(N/N(p)) \le d_G(N/N') \le |R|$$

for each prime p. In Chapter 2, §2.3 we show that in fact there exists a set of relations R with

$$|R| = \max_p d_G(N/N(p))$$

(this is essentially Proposition 2.8 of [Gruenberg 1976]). Thus to determine the minimal number of (profinite!) relations needed to define G, it suffices to find the numbers $d_G(N/N(p))$. Remarkably, this information is contained in the represenation theory of G. The following result is due to [Gruenberg 1976]; see also [Lubotzky 2001] for the case where G is profinite (not necessarily finite).

Let $\mathcal{S}$ denote the set of all simple $\mathbb{F}_p[G]$-modules, and for $M \in \mathcal{S}$ put

$$\xi_M = 0 \ \text{ if } \ M \cong \mathbb{F}_p$$
$$\xi_M = 1 \ \text{ if } \ M \ncong \mathbb{F}_p.$$

Then Gruenberg's formula is as follows:

Proposition 16.4.7

$$d_G(N/N(p)) = \max_{M\in\mathcal{S}} \left\{ \left\lceil \frac{\dim H^2(G,M) - \dim H^1(G,M)}{\dim M} \right\rceil - \xi_M \right\} + d. \quad (16.1)$$

(If $p \nmid |G|$, this formula reduces to $d_G(N/N(p)) = d$, a result obtained earlier by Gaschütz.)

Now fix $M \in \mathcal{S}$. Then $E = \mathrm{Hom}_G(M, M)$ is a finite field extension of $\mathbb{F}_p$, and both $H^1(G, M)$ and $H^2(G, M)$ have a natural structure as E-modules. Put

$$\begin{aligned} e_M &= (E : \mathbb{F}_p) \\ r_M &= \dim_E(M) \\ s_M &= \dim_E H^1(G, M) \\ t_M &= \dim_E H^2(G, M). \end{aligned}$$

Let $\ell(M)$ be the maximal integer such that $M^{\ell(M)}$ is a quotient module of $N/N(p)$; then

$$\mathrm{Hom}_G(N, M) = \mathrm{Hom}_G(N/N(p), M) \cong E^{\ell(M)}.$$

Now the key step is

Lemma 16.4.8 *For each $M \in \mathcal{S}$,*

$$\ell(M) = r_M(d - \xi_M) - s_M + t_M.$$

Proof. Considering M as an F-module, we have the 5-term exact sequence corresponding to the extension $1 \to N \to F \to G \to 1$:

$$0 \to H^1(G, M^N) \to H^1(F, M) \to H^1(N, M)^G \to H^2(G, M^N) \to H^2(F, M) \qquad (*)$$

(see [RZ] Corollary 7.2.5).

Now as M is trivial as an N-module,

$$H^1(N, M)^G = \mathrm{Hom}_G(N, M) \cong E^{\ell(M)}.$$

Also

$$\begin{aligned} \dim_{\mathbb{F}_p} H^1(F, M) &= \begin{cases} d \cdot \dim_{\mathbb{F}_p} M & \text{if } M \text{ is the trivial } G\text{-module} \\ (d-1)\dim_{\mathbb{F}_p} M & \text{if } M \text{ is non-trivial} \end{cases} \\ &= (d - \xi_M) e_M r_M; \end{aligned}$$

while since $M^N = M$ we have

$$\begin{aligned} \dim_{\mathbb{F}_p} H^1(G, M^N) &= e_M s_M, \\ \dim_{\mathbb{F}_p} H^2(G, M^N) &= e_M t_M. \end{aligned}$$

Note finally that $H^2(F, M) = 0$ because F is free. Putting this information into $(*)$ gives

$$e_M s_M - (d - \xi_M) e_M r_M + e_M \ell(M) - e_M t_M = 0.$$

The lemma follows. ∎

Note now that

(i) M^{r_M} is the maximal direct power of M which appears as a quotient of $\mathbb{F}_p[G]$. Indeed, if M occurs r' times then

$$M \cong \mathrm{Hom}_{\mathbb{F}_p[G]}(\mathbb{F}_p[G], M) \cong \mathrm{Hom}_{\mathbb{F}_p[G]}(M, M)^{r'} = E^{r'};$$

(ii) $d_G(M^{\ell(M)})$ is equal to the smallest integer k such that $M^{\ell(M)}$ appears as quotient of $\mathbb{F}_p[G]^k$.

Together these imply that

$$d_G(M^{\ell(M)}) = \left\lceil \frac{\ell(M)}{r_M} \right\rceil.$$

An elementary argument shows that

$$d_G(N/N(p)) = \max_{M \in \mathcal{S}} d_G(M^{\ell(M)}).$$

Using the formula for $\ell(M)$ given in the lemma we deduce finally that

$$d_G(N/N(p)) = \max_{M \in \mathcal{S}} \left\lceil \frac{\ell(M)}{r_M} \right\rceil = \max_{M \in \mathcal{S}} \left(\left\lceil \frac{t_M - s_M}{r_M} \right\rceil - \xi_M + d \right).$$

This completes the proof of Proposition 16.4.7.

Window: Pro-p groups

A pro-p group is an inverse limit of finite p-groups, or equivalently it is a profinite group (↬ **Profinite groups**) in which every open subgroup has index a power of p ; here p denotes a prime, kept fixed throughout. It is important to note that a non-trivial profinite group can be a pro-p group for *at most one* prime p (otherwise the only open subgroup is the whole group).

We consider only closed subgroups and continuous homomorphisms; so $\langle X\rangle$ denotes the closed subgroup generated by a subset X in a pro-p group G, $G' = [G,G]$ the closure of the derived group, and G^{p^n} the closed subgroup generated by all x^{p^n}, $x \in G$. As usual, $d(G)$ denotes the minimal cardinality of a (topological) generating set for G.

The *lower central p-series of a* pro-p group G is defined by

$$P_1(G) = G$$
$$P_n(G) = [P_{n-1}(G), P_{n-1}(G)]P_{n-1}(G)^p \quad (n > 1).$$

The *modular dimension series* or *Jennings-Zassenhaus series* is defined by

$$D_1(G) = G$$
$$D_n(G) = \prod_{i+j=n} [D_i(G), D_j(G)] \cdot D_{\lceil n/p\rceil}(G)^p \quad (n > 1).$$

The material of the first two sections can all be found in [DDMS] and/or in [Wi].

1 Generators and relations

Let G be a pro-p group. The *Frattini subgroup* $\Phi(G)$ of G is the intersection of all maximal (open) subgroups of G. Every maximal subgroup of G is normal and of index p, (because the same is true for finite p-groups), and so contains $G'G^p$. Therefore $\Phi(G) \geq G'G^p$. On the other hand, $G'G^p$ is an intersection of open normal subgroups N of G; for each such N the group G/N is a finite elementary abelian p-group and satisfies $\Phi(G/N) = 1$. Therefore $\Phi(G) \leq \bigcap N$, and we have

Proposition 16.4.1 *If G is a pro-p group then $\Phi(G) = G'G^p$.*

It follows that *if $\theta : G \to H$ is an epimorphism of pro-p groups then*

$$\theta(\Phi(G)) = \Phi(H). \tag{16.1}$$

A subset X of G generates G if and only if $X \not\subseteq M$ for every maximal subgroup M; this holds for X if and only if it holds for $\Phi(G) \cup X$. Consequently $G = \langle X \rangle$ if and only if $G = \langle X \rangle \Phi(G)$. Considering $G/\Phi(G)$ as a vector space over $\mathbb{F}_p$, we deduce that G is finitely generated if and only if $G/\Phi(G)$ is finite-dimensional, in which case

$$d(G) = \dim_{\mathbb{F}_p}(G/\Phi(G)).$$

This fact makes pro-p groups much easier to manage than profinite groups in general. Here is one application (for generalities on profinite presentations see the **Profinite groups** window).

Proposition 16.4.2 *Suppose that the pro-p group G has a finite pro-p presentation $G = \langle X; R \rangle$. Then G has a pro-p presentation $\langle Y; S \rangle$ such that*

$$|Y| = d(G),\ |S| = |R| - (|X| - d(G)).$$

Proof. Let F be the free pro-p group on the set X. We are given an epimorphism $\theta : F \to G$ with kernel $\langle R^F \rangle$. This induces an epimorphism $\phi : F/\Phi(F) \to G/\Phi(G)$, and it follows from (16.1) that $\ker \phi = \langle R^F \rangle \Phi(F) = \langle R \rangle \Phi(F)$. Let $r_1, \ldots, r_k \in R$ be such that $\{r_1\Phi(F), \ldots, r_k\Phi(F)\}$ is a basis for $\langle R \rangle \Phi(F)/\Phi(F)$, and extend this to a basis $\{r_1\Phi(F), \ldots, r_k\Phi(F), s_1\Phi(F), \ldots, s_n\Phi(F)\}$ of $F/\Phi(F)$. Then

$$\begin{aligned} n &= \dim_{\mathbb{F}_p}(G/\Phi(G)) = d(G), \\ k &= d(F) - n = |X| - d(G). \end{aligned}$$

Now put $R_0 = \{r_1, \ldots, r_k\}$ and let N be the normal closure of R_0 in F. It is easy to see from the universal property that $F/N = \widetilde{F}$ is the free pro-p group on the set $Y = \{s_1N, \ldots, s_nN\}$, and θ induces an epimorphism $\theta^* : \widetilde{F} \to G$. Moreover,

$$\ker \theta^* = \langle R^F \rangle N/N = \left\langle S^{\widetilde{F}} \right\rangle$$

where S is the image of $R \setminus R_0$ in $\widetilde{F}$. The result follows since $|S| \leq |R| - k$ (if this inequality is strict we may just repeat some relators). ■

It is plausible to suppose that a pro-p group $G = \langle X; R \rangle$ must be large if $|R|$ is small compared with $|X|$. The celebrated theorem of Golod and Shafarevich asserts that if $|X| = d(G)$ and $|R| < |X|^2/4$ then G must be infinite; recently, [Zelmanov 2000] has proved that under these conditions, G must in fact contain a *non-abelian free pro-p subgroup*. Here we prove the very easy

Lemma 16.4.3 *Suppose that the pro-p group G has a finite pro-p presentation $G = \langle X; R \rangle$. If $|R| < |X|$ then G has an infinite abelian quotient.*

Proof. We have $G \cong F/N$ where F is the free pro-p group on d generators and N is generated by the conjugates of $x_1, \ldots, x_r$, say, where $r = |R| < |X| = d$. Then $G/G' \cong F/NF'$. Now $F/F' \cong \mathbb{Z}_p^d$ and NF'/F' is generated by the $r < d$ elements $x_i F'$. Since every $\mathbb{Z}_p$-submodule of finite index in $\mathbb{Z}_p^d$ is isomorphic to $\mathbb{Z}_p^d$ it follows that NF' has infinite index in F. ■

The same argument applied to the abstract free group on d generators gives

Lemma 16.4.4 *Every finite presentation of a finite group needs at least as many relators as generators.*

2 Pro-p groups of finite rank

The *rank* of a profinite group G is

$$\begin{aligned} \mathrm{rk}(G) &= \sup\{d(H) \mid H \leq_o G\} \\ &= \sup\{d(H) \mid H \text{ is a closed subgroup of } G\}. \end{aligned}$$

The following portmanteau theorem summarises much of the book [DDMS]; for detailed references see [DDMS], Interlude A. The results are due mainly to [Lazard 1965] and [Lubotzky & Mann 1987].

Theorem 16.4.5 *For a pro-p group G the following are equivalent:*

a *G has finite rank;*

b *G has the structure of a p-adic analytic group;*

c *G is isomorphic to a closed subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$ for some d;*

d *G is finitely generated and virtually powerful;*

e *G is virtually uniform;*

f *G is finitely generated and for some n, or for infinitely many n, $D_n(G) = D_{n+1}(G)$;*

g *G has PSG, or PIG, or is boundedly generated.*

Of these, (b) is mentioned mainly for interest, and will only be used in Chapter 16. PSG means 'polynomial subgroup growth': that this is equivalent to finite rank for pro-p groups is proved in Chapter 4 of this book. The conditions PIG ('polynomial index growth') and 'bounded generation' are discussed in Chapter 12.

To say that G is *powerful* means that G/G^p is abelian (if p is odd), that G/G^4 is abelian (if $p = 2$); this is equivalent to saying that G is the inverse limit of a system of *powerful finite p-groups* with all maps surjective (↬ **Finite group theory**). G is *uniform* if G is powerful and

$$d(G) = \dim_{\mathbb{F}_p}(P_n(G)/P_{n+1}(G)) < \infty \text{ for all } n \geq 1.$$

This holds if and only if G is f.g., powerful and torsion-free ([DDMS], Chapter 4).

If G is f.g. and powerful then for each $n > 1$,

$$P_n(G) = G^{p^{n-1}} = \left\{ g^{p^{n-1}} \mid g \in G \right\} = \Phi(P_{n-1}(G)).$$

If G is a pro-p group of finite rank then there exists d such that $d(H) = d$ for every open uniform subgroup H of G. This number d is called the *dimension* of G and is denoted $\dim(G)$. This is equal to the dimension of G as a p-adic analytic group. Evidently

$$\dim(G) \leq \mathrm{rk}(G).$$

If G is *powerful* then we also have

$$\mathrm{rk}(G) = d(G).$$

In particular, if G is *uniform* then $\mathrm{rk}(G) = \dim(G)$, so every subgroup of G can be generated by $\dim(G)$ elements. As one would expect, dimension is additive on extensions:

Proposition 16.4.6 ([DDMS], Theorem 4.8) *Let G be a pro-p group of finite rank and N a closed normal subgroup of G. Then*

$$\dim(G) = \dim(N) + \dim(G/N).$$

The next result in the case of finite p-groups is discussed in the window on **Finite group theory**. For the proof see [DDMS], Corollary 3.14:

Proposition 16.4.7 *Let G be a pro-p group and r a positive integer. If every open subgroup of G contains an open normal subgroup N of G with $d(N) \leq r$ then G has finite rank.*

Now let us examine the implication (c) $\Longrightarrow$ (a) in Theorem 5 more closely. Fix a positive integer d and for $i \geq 1$ let

$$\Gamma(i) = \mathrm{GL}_d^i(\mathbb{Z}_p) = \left\{ g \in \mathrm{GL}_d(\mathbb{Z}_p) \mid g \equiv 1_d \,(\mathrm{mod}\, p^i) \right\}$$
$$\Delta(i) = \mathrm{SL}_d^i(\mathbb{Z}_p) = \left\{ g \in \mathrm{SL}_d(\mathbb{Z}_p) \mid g \equiv 1_d \,(\mathrm{mod}\, p^i) \right\}.$$

Thus $\Gamma(i)$ is the kernel of the residue map $\mathrm{GL}_d(\mathbb{Z}_p) \to \mathrm{GL}_d(\mathbb{Z}_p/p^i\mathbb{Z}_p)$, and similarly for $\Delta(i)$ (these are 'principal congruence subgroups modulo p^i'). The following is proved in [DDMS], Chapter 5:

Proposition 16.4.8 *Let $i \geq 1$ if p is odd, $i \geq 2$ if $p = 2$. Then $\Gamma(i)$ is a uniform pro-p group of dimension d^2.*

We now deduce

Corollary 16.4.9 *(i) Suppose that* $p \neq 2$. *Then* $\mathrm{rk}(\Delta(1)) = d^2 - 1$.
(ii) Suppose that $p = 2$. *Then* $\mathrm{rk}(\Gamma(1)) \leq 2d^2$ *and* $\mathrm{rk}(\Delta(1)) \leq 2d^2 - 1$.

Proof. (i) The mapping $g \mapsto \det g$ is a homomorphism from $\Gamma(1)$ into the multiplicative group $U = 1 + p\mathbb{Z}_p \subseteq \mathbb{Z}_p^*$, with kernel $\Delta(1)$ and nontrivial image. Now $U \cong \mathbb{Z}_p$ (by the logarithm map, or apply the proposition with $d = 1$). Therefore $\Gamma(1)/\Delta(1) \cong \mathbb{Z}_p$. The claim follows because dim is additive on extensions ([DDMS] Theorem 4.8).

(ii) Write $V = \mathbb{Z}_2^{(d)}$. Then $\Gamma(1)/\Gamma(2)$ acts faithfully on $V/4V$ and trivially on both $V/2V$ and $2V/4V$. The mapping $g \mapsto g - 1$ therefore induces an injective homorphism from $\Gamma(1)/\Gamma(2)$ into $\mathrm{Hom}(V/2V, 2V/4V) \cong \mathbb{F}_2^{(d^2)}$. Since rank is (obviously) sub-additive on extensions it follows that $\mathrm{rk}(\Gamma(1)) \leq \mathrm{rk}(\Gamma(2)) + d^2 = 2d^2$.

The argument of (i) shows similarly that $\mathrm{rk}(\Delta(2)) = d^2 - 1$. As $\Delta(1)/\Delta(2)$ is isomorphic to a subgroup of $\Gamma(1)/\Gamma(2)$ it follows as before that $\mathrm{rk}(\Delta(1)) \leq \mathrm{rk}(\Delta(2)) + d^2 = 2d^2 - 1$. ■

For a more direct argument, see the proof of [Wi], Lemma 8.3.3.

3 Linear pro-p groups over local fields

In this section, K will denote a local field of positive characteristic ℓ. The ring of integers of K is denoted $\mathcal{O}_K$.

Proposition 16.4.10 *Suppose that* $G \leq \mathrm{GL}_m(K)$ *is a pro-p group where* $p \neq \ell$. *Then* G *is finite.*

Proof. Since G is compact, it can be conjugated into $\mathrm{GL}_m(\mathcal{O}_K)$. Since this is virtually a pro-ℓ group, it follows that G has a subgroup H of finite index that is both a pro-p group and a pro-ℓ group. Since $p \neq \ell$ this forces $H = 1$. ■

The following major theorem describes the structure of compact subgroups in general:

Theorem 16.4.11 ([Pink 1998], Corollary 0.5) *Let* G *be a compact subgroup of* $\mathrm{GL}_m(K)$. *Then there exist closed normal subgroups* $L_3 \leq L_2 \leq L_1$ *of* G *such that:*
(1) G/L_1 *is finite;*
(2) L_1/L_2 *is abelian of finite exponent;*
(3) if L_2/L_3 *is infinite, there exist a local field* E *of characteristic* ℓ, *a connected adjoint semi-simple algebraic group* H *over* E *with universal covering* $\pi\colon \tilde{H} \to H$, *and an open compact subgroup* $\Delta \subseteq \tilde{H}(E)$, *such that* L_2/L_3 *is isomorphic as topological group to* $\pi(\Delta)$;
(4) L_3 *is a soluble group of derived length at most* m.

Corollary 16.4.12 *Suppose that* $G \leq \mathrm{GL}_m(K)$ *is a pro-p group of finite rank. Then* G *is virtually abelian.*

Proof. By Proposition 16.4.10 we may assume that $p = \ell$. It is easy to see that now G/L_2 is finite. We claim that L_2/L_3 is also finite. Suppose not. Then L_2/L_3 is a pro-p group of finite rank which is isomorphic to an open compact subgroup Δ of a semi-simple group H over a characteristic-p local field E. But this is impossible. Indeed, E is isomorphic to $\mathbb{F}_q((t))$ for some $q = p^k$, and Δ is commensurable to $H(\mathbb{F}_q[[t]]) = P$, say. The congruence subgroups

$$P_n = \ker(H(\mathbb{F}_q[[t]]) \to H(\mathbb{F}_q[[t]]/(t^n)))$$

satisfy $[P_n, P_n]P_n^p \leq P_{2n}$ and $|P_n : P_{2n}| \geq p^n$ for all n. Thus P_n/P_{2n} is an elementary abelian p-group of rank at least n. It follows that P, and therefore also Δ, has infinite rank as a pro-p group, and so cannot be isomorphic to L_2/L_3. (One could also deduce the same conclusion from [Pink 1998], Corollary 0.3, which shows that if two open compact subgroups of simple algebraic groups over local fields are isomorphic, then the fields are the same, and the algebraic groups are isomorphic.)

We conclude that L_3 is of finite index in G, so G is virtually soluble. By the Lie-Kolchin-Mal'cev theorem (↬ **Linear groups**), G has a unipotent normal subgroup U such that G/U is virtually abelian, and we may take U to be closed in G. Then U is a pro-p group of finite rank and has exponent dividing p^m, so U is finite. As G is residually finite it follows that G is virtually abelian as claimed. ■

Remark The ranks of torsion-free abelian subgroups pro-p subgroups of $\mathrm{GL}_m(K)$ are not bounded. Even $\mathrm{GL}_1(\mathbb{F}_p[[t]])$ contains free abelian pro-p subgroups of arbitrarily large rank: for example, for every set of primes $\{q_1, \ldots, q_l\}$, the elements $\{1 + t^{q_i} \mid i = 1, \ldots, l\}$ generate a free abelian pro-p group of rank l.

A more elaborate application of Pink's theorem leads to

Theorem 16.4.13 [Barnea & Larsen 1999] *The group* $\mathrm{GL}_m(K)$ *contains no free non-abelian pro-p subgroup.*

4 Automorphisms of finite p-groups

Proposition 16.4.14 *Let A be a finite abelian p-group of rank r. Then the p-rank of* $\mathrm{Aut}(A)$ *is at most* $\frac{1}{2}(3r^2 - r)$ *if p is odd,* $\frac{1}{2}(5r^2 - r)$ *if $p = 2$.*

Proof. Let $V = \mathbb{Z}_p^{(r)}$ and identify A with a quotient $\mathbb{Z}_p$-module V/K of V. Let Γ be the stabiliser of K in $\mathrm{Aut}_{\mathbb{Z}_p}(V)$. Since V is a free $\mathbb{Z}_p$-module every automorphism α of A lifts to a $\mathbb{Z}_p$-endomorphism α^* of V; each such α^* is surjective since $V = K + V\alpha^*$ and $K \leq Vp$, hence α^* is also injective, so in fact $\alpha^* \in \Gamma$. It follows that the natural mapping from Γ to $\mathrm{Aut}(A)$ is surjective, and hence that

$$\mathrm{r}_p(\mathrm{Aut}(A)) \leq \mathrm{ur}_p(\Gamma) \leq \mathrm{ur}_p(\mathrm{Aut}_{\mathbb{Z}_p}(V)).$$

Now $\mathrm{Aut}_{\mathbb{Z}_p}(V) = \mathrm{GL}_r(\mathbb{Z}_p)$. Using Proposition 7 or Corollary 16.4.9 we have

$$\begin{aligned}\mathrm{ur}_p(\mathrm{GL}_r(\mathbb{Z}_p)) &\leq \mathrm{rk}(\mathrm{GL}_r^1(\mathbb{Z}_p)) + \mathrm{r}_p(\mathrm{GL}_r(\mathbb{F}_p)) \\ &\leq \varepsilon r^2 + r(r-1)/2,\end{aligned}$$

where $\mathrm{GL}_r^1(\mathbb{Z}_p)$ is the first congruence subgroup in $\mathrm{GL}_r(\mathbb{Z}_p)$ and $\varepsilon = 1$ if p is odd, $\varepsilon = 2$ if $p = 2$ (for the p-rank of $\mathrm{GL}_r(\mathbb{F}_p)$ see the window on **Finite group theory**). The result follows.

For a direct proof, see [Wi], Lemma 8.3.3. ■

Lemma 16.4.15 *Let G be a finite p-group and $P \lhd G$. Let A be maximal among the normal abelian subgroups of G contained in P. Then $\mathrm{C}_P(A) = A$.*

Proof. Suppose $\mathrm{C}_P(A) > A$. Then $\mathrm{C}_P(A)$ contains an element $z \notin A$ such that zA is in the centre of G/A. But then $A\langle z\rangle$ is abelian and normal in G, contradicting the maximality of A. ■

Proposition 16.4.16 *Let P be a finite p-group of rank r and Q a p-subgroup of $\mathrm{Aut}(P)$. Then the rank of Q is at most $\frac{1}{2}(5r^2 - r)$ if p is odd, at most $\frac{1}{2}(7r^2 - r)$ if $p = 2$.*

Proof. Put $G = P \rtimes Q$. Let $A \lhd G$ be as in the lemma, and put $C = \mathrm{C}_G(A)$. Then $[P, C] \leq C \cap P = A$, so $C/\mathrm{C}_C(P)$ embeds into $\mathrm{Der}(P/A, A)$ via

$$c \mapsto (h \mapsto [h, c]).$$

Since $Q \cap \mathrm{C}_C(P) = 1$ it follows that

$$Q \cap C \hookrightarrow \mathrm{Der}(P/A, A) \hookrightarrow A^{(r)}.$$

Thus $\mathrm{rk}(Q \cap C) \leq r^2$.

Proposition 16.4.14 shows that the rank of any p-subgroup of $\mathrm{Aut}(A)$ is at most

$$\frac{3r^2 - r}{2} \quad (p \neq 2), \qquad \frac{5r^2 - r}{2} \quad (p = 2).$$

Since $Q/(Q \cap C)$ acts faithfully on A this is an upper bound for $\mathrm{rk}(Q/(Q \cap C))$, and the result follows since

$$\mathrm{rk}(Q) \leq \mathrm{rk}(Q \cap C) + \mathrm{rk}(Q/(Q \cap C)).$$

■

(A weaker bound is given in [Segal & Shalev 1997], Lemma 2.1.)

5 Hall's enumeration principle

This is a form of the inclusion-exclusion argument in combinatorics particularly adapted to counting sets of subgroups in p-groups.

For integers $r \geq t \geq 0$ we write

$$\begin{bmatrix} r \\ t \end{bmatrix} = \frac{(p^r-1)(p^{r-1}-1)\dots(p^{r-t+1}-1)}{(p^t-1)(p^{t-1}-1)\dots(p-1)} = \begin{bmatrix} r \\ r-t \end{bmatrix};$$

this is the number of subspaces of dimension (or codimension) t in the vector space $\mathbb{F}_p^r$.

We begin with two lemmas.

Lemma 16.4.17

$$\begin{bmatrix} r+1 \\ t \end{bmatrix} = \begin{bmatrix} r \\ t \end{bmatrix} + p^{r-t+1}\begin{bmatrix} r \\ t-1 \end{bmatrix}.$$

This is immediate from the defining formula; we prefer to see it as an exercise in counting subspaces. Let $V = \mathbb{F}_p^{r+1} > U \cong \mathbb{F}_p$. For each subspace W/U of codimension $t-1$ in V/U there are precisely p^{r-t+1} complements to U in W, giving altogether $p^{r-t+1}\begin{bmatrix} r \\ t-1 \end{bmatrix}$ subspaces of codimension t in V; the remaining subspaces of this codimension in V all contain U, and there are $\begin{bmatrix} r \\ t \end{bmatrix}$ of them.

Lemma 16.4.18 *The following identity holds:*

$$\prod_{t=0}^{r-1}(X-p^t) = \sum_{t=0}^{r}(-1)^t p^{t(t-1)/2}\begin{bmatrix} r \\ t \end{bmatrix} X^{r-t} \tag{16.2}$$

Proof. Let $F(r,X)$ denote the polynomial on the right-hand side of this identity. It is easy to see that $F(1,X) = X-1$. Now let $r \geq 1$ and suppose that $F(r,X) = \prod_{t=0}^{r-1}(X-p^t)$.

Now consider the coefficient of X^{r+1-t} in $F(r,X)(X-p^r)$. For $t \geq 1$ this is equal to

$$(-1)^t p^{t(t-1)/2}\begin{bmatrix} r \\ t \end{bmatrix} - p^r \cdot (-1)^{t-1} p^{(t-1)(t-2)/2}\begin{bmatrix} r \\ t-1 \end{bmatrix}$$
$$= (-1)^t p^{t(t-1)/2}\begin{bmatrix} r+1 \\ t \end{bmatrix}$$

by Lemma 16.4.17; for $t = 0$ it is equal to 1. In either case this is the coefficient of X^{r+1-t} in $F(r+1,X)$, so we have $F(r,X)(X-p^r) = F(r+1,X)$ and the lemma follows by induction. ■

We can now state the main result, due to [Hall 1934]; he considered finite p-groups but the proof is the same:

Proposition 16.4.19 *Let G be a pro-p group, $\Phi = \Phi(G) = [G,G]G^p$ its Frattini subgroup and $d = d(G)$. For $1 \leq t \leq r$ let*

$$\left\{ K_{t,i} \mid i = 1, \dots, \begin{bmatrix} d \\ t \end{bmatrix} \right\}$$

be the set of all subgroups K of G with $\Phi \leq K \leq G$ and $|G:K| = p^t$. Let $\mathcal{S}$ be a finite collection of proper subgroups of G and denote by $n(t,i)$ the number of $H \in \mathcal{S}$ such that $H \leq K_{t,i}$. Then

$$|\mathcal{S}| + \sum_{t=1}^{d} (-1)^t p^{t(t-1)/2} \sum_{i=1}^{\begin{bmatrix} d \\ t \end{bmatrix}} n(t,i) = 0. \tag{16.3}$$

Proof. For $H \in \mathcal{S}$, put $\delta_H(t,i) = 1$ if $H \leq K_{t,i}$, $\delta_H(t,i) = 0$ otherwise. The left-hand side of (16.3) is then equal to to sum over all $H \in \mathcal{S}$ of the expressions

$$1 + \sum_{t=1}^{d} (-1)^t p^{t(t-1)/2} \sum_{i=1}^{\begin{bmatrix} d \\ t \end{bmatrix}} \delta_H(t,i). \tag{16.4}$$

Fix such an H and let L be the intersection of all the $K_{t,i}$ that contain H. Then $L \geq \Phi$ and $|G:L| = p^r$ for some $r \geq 1$. Now $\delta_H(t,i) = 1$ just when $K_{t,i} \geq L$, and for each t with $1 \leq t \leq r$ there are precisely $\begin{bmatrix} r \\ t \end{bmatrix}$ such $K_{t,i}$; consequently (16.4) is equal to

$$1 + \sum_{t=1}^{r} (-1)^t p^{t(t-1)/2} \begin{bmatrix} r \\ t \end{bmatrix} = \prod_{t=0}^{r-1} (1 - p^t) = 0,$$

as we see on substituting $X = 1$ in Lemma 16.4.18. ■

Window: Soluble groups

1 Nilpotent groups

Most of the following is quite elementary and can be found in [Sg], Chapter 1 or [R], Chapter 5.

Proposition 16.4.1 *Let G be a group and $G_i = \gamma_i(G)$ for each i. Then for each $i > 1$ the commutator induces an epimorphism of abelian groups*

$$G_{i-1}/G_i \otimes_{\mathbb{Z}} G/G' \to G_i/G_{i+1}.$$

Consequently,
(i) if G_k/G_{k+1} is π-torsion for some set of primes π, or has exponent dividing m, then G_i/G_{i+1} has the same property for each $i \geq k$;
(ii) if $\mathrm{rk}(G/G') = r$ then $\mathrm{rk}(G/G_{k+1}) \leq r + r^2 + \cdots + r^k$. Hence if G is nilpotent and G/G' has finite rank then G has finite rank;
(iii) if a group Γ acts on G and

$$[G, \underbrace{\Gamma, \ldots, \Gamma}_{n}] \leq G_2$$

then for each $i \geq 1$

$$[G_i, \underbrace{\Gamma, \ldots, \Gamma}_{in}] \leq G_{i+1}.$$

Proposition 16.4.2 *Let G be a finitely generated nilpotent group.*
(i) G is residually finite.
(ii) The elements of finite order in G form a finite subgroup $\tau(G)$ and $G/\tau(G)$ is torsion free.
(iii) If G is torsion-free then G is residually a finite p-group for every prime p. If G is not torsion-free then G is residually a finite nilpotent π-group where $\pi = \pi(G)$ is the finite set of primes p such that G contains an element of order p.
(iv) $G/\tau(G)$ has a central series of finite length h with infinite cyclic factors. Here $h = h(G)$ is an invariant of G, the Hirsch length.
(v) For each prime p, the pro-p completion $\widehat{G}_p$ has finite rank. If $p \notin \pi(G)$ then

$\widehat{G}_p$ is a torsion-free pro-p group and

$$\mathrm{rk}(\widehat{G}_p) = \dim(\widehat{G}_p) = h(G).$$

(vi) For every prime p,

$$\mathrm{rk}(\widehat{G}_p) = \mathrm{ur}_p(G).$$

Part (vi) holds because if $\overline{G}$ is any finite quotient of G then each Sylow subgroup of $\overline{G}$ is a direct factor. Evidently $\mathrm{ur}_p(G) \leq \mathrm{r}_p(\tau(G)) + h(G)$, which is finite.

Suppose that G is torsion-free. Then G has a central subgroup $Z \cong \mathbb{Z}$ such that G/Z is torsion-free with Hirsch length $h-1$. By (ii) applied to the group G/Z^{p^n} we see that Z^{p^n} is closed in the pro-p topology of G, for each n, from which it follows easily that the sequence

$$1 \to \widehat{Z}_p \to \widehat{G}_p \to \widehat{(G/Z)}_p \to 1$$

is exact. It follows that $\widehat{G}_p$ is a torsion-free pro-p group of dimension

$$h = h(G) \geq \mathrm{ur}_p(G) = \mathrm{rk}(\widehat{G}_p).$$

This is then an equality since $\mathrm{rk}(P) \geq \dim(P)$ for any pro-p group P of finite rank ($\looparrowright$ **pro-p groups**). Part (v) now follows since $\widehat{G}_p = \widehat{(G/\tau(G))}_p$ whenever $p \notin \pi(G)$

Proposition 16.4.3 'Stability groups' *Let G be a group and Γ a subgroup of* $\mathrm{Aut}(G)$*. Suppose that*

$$1 = G_0 \leq G_1 \leq \ldots \leq G_k = G$$

is a chain of normal subgroups of G such that $[G_i, \Gamma] \leq G_{i-1}$ for $1 \leq i \leq k$. Then
(i) $\gamma_k(\Gamma) = 1$;
(ii) *if $k = 2$ then Γ embeds in* $\mathrm{Der}(G/G_1, \mathrm{Z}(G_1))$ *via*

$$\gamma \mapsto (gG_1 \mapsto [g, \gamma]).$$

2 Soluble groups of finite rank

These were studied by A. I. Mal'cev around 1950 and then by D. J. S. Robinson and Wehrfritz around 1970. Many of the assertions below are proved in [R2], sections 9.3 and 10.3.

Following [We], we denote by

$$\mathfrak{S}_t$$

the class of soluble groups of finite rank that are *virtually torsion-free*.

The following is proved in [We], pages 25-26:

Proposition 16.4.4 *Let G be an $\mathfrak{S}_t$ group. Then G is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{Q})$ for some n.*

With the Lie-Kolchin-Mal'cev theorem (↬ **Linear groups**) this implies that every $\mathfrak{S}_t$ group is virtually nilpotent-by-abelian; in fact, since a diagonalisable linear group over (a finite extension of) $\mathbb{Q}$ has finite rank if and only if it is finitely generated, we can deduce (cf. [R2], Theorem 10.33)

Proposition 16.4.5 *If G is an $\mathfrak{S}_t$ group then G has a nilpotent normal subgroup N such that G/N is virtually free abelian of finite rank.*

A soluble group G is *minimax* if there is a finite chain

$$1 = G_0 \leq G_1 \leq \ldots \leq G_k = G \tag{16.1}$$

of normal subgroups of G such that each factor G_i/G_{i-1} is an abelian minimax group; an abelian group A is *minimax* if A contains a subgroup B such that

(i) B is finitely generated

(ii) A/B is the direct product finitely many groups of type C_{p^∞} (for various primes p). The set of primes p that occur is called $\mathrm{spec}(A)$.

For any set of primes π write

$$\mathbb{Q}_\pi = \mathbb{Z}[\frac{1}{p} \mid p \in \pi].$$

A torsion-free abelian group A is minimax if and only if A is isomorphic to a subgroup of $\mathbb{Q}_\pi^{(r)}$ for some finite r and some finite set of primes π; the smallest such set is then $\mathrm{spec}(A)$. If G is as above, one defines

$$\mathrm{spec}(G) = \bigcup_{i=1}^{k} \mathrm{spec}(G_i/G_{i-1}).$$

This is a finite set of primes.

More generally, if G is virtually an $\mathfrak{S}_t$ group then there is a set π of primes and a chain (16.1) of normal subgroups of G such that $G_i/G_{i-1} \hookrightarrow \mathbb{Q}_\pi^{(r_i)}$ for $i = 1, \ldots, k-1$ and G/G_{k-1} is finite. The smallest such set π (which may be infinite in general) is called $\mathrm{spec}(G)$, and G is virtually minimax if and only if π is finite. The proof of Proposition 16.4.4 shows that G is a linear group over the ring $\mathbb{Q}_\pi$. Conversely, it follows from the Lie-Kolchin-Mal'cev theorem that if π is finite then every soluble linear group over $\mathbb{Q}_\pi$ belongs to $\mathfrak{S}_t$, and is a minimax group (this depends also on the S-units theorem of Dirichlet).

Proposition 16.4.6 *A soluble minimax group G is residually finite if and only if it is virtually torsion-free.*

In one direction this follows from the preceding remark, since if π is a finite set of primes then the group $\mathrm{GL}_n(\mathbb{Q}_\pi)$ is residually finite, because the finitely generated ring $\mathbb{Q}_\pi$ is residually finite. In the other direction, it follows from [R2], Theorem 10.33 which shows that a residually finite soluble minimax group is virtually nilpotent-by-(free abelian of finite rank); while if N is a nilpotent minimax group with torsion subgroup T then T is finite if it is residually finite (cf. [R2], Theorem 10.23).

Both the classes of soluble minimax groups and of $\mathfrak{S}_t$ groups are closed under taking extensions. The first is obvious from the definition; the second follows from

Lemma 16.4.7 *Let G be a soluble group of finite rank. Then $G \in \mathfrak{S}_t$ if and only if G has no infinite periodic normal subgroup.*

This follows from [R2], Theorem 9.39.3 and Lemma 9.34. Together with the preceding proposition it easily implies

Proposition 16.4.8 *The class of residually finite virtually soluble groups of finite rank is extension-closed.*

Finally, the important result of Robinson:

Theorem 16.4.9 ([R2], Theorem 10.38) *Every finitely generated soluble group of finite rank is a minimax group.*

In [Robinson 1975] this is generalised, to show that every finitely generated soluble group having finite sectional p-rank for each prime p is a minimax group.

To summarise some of the main conclusions:

Theorem 16.4.10 *Let $\mathfrak{X}$ denote the class of finitely generated residually finite virtually soluble groups of finite rank.*

(1) A finitely generated group G belongs to $\mathfrak{X}$ if and only if G is virtually soluble and linear over $\mathbb{Q}_\pi$ for some finite set of primes π.

(2) A finitely generated group G belongs to $\mathfrak{X}$ if and only if G is virtually a torsion-free soluble minimax group.

(3) The class $\mathfrak{X}$ is extension-closed.

Now let $G \in \mathfrak{S}_t$. The sum of the torsion-free ranks of the abelian factors G_i/G_{i-1} in a series like (16.1) is an invariant $h(G)$ called the *Hirsch length* of G. This can be detected in suitable pro-p completions:

Proposition 16.4.11 *Let $G \in \mathfrak{S}_t$ be residually finite, and let p be a prime. Then $\widehat{G}_p$ is a pro-p group of finite rank and dimension at most $h(G)$. If $p \notin \mathrm{spec}(G)$ then G has a normal subgroup H of finite index such that $\dim(\widehat{H}_p) = h(G)$.*

Proof. G has an abelian normal subgroup A such that G/A is again a residually finite $\mathfrak{S}_t$ group and A is isomorphic to a subgroup of $\mathbb{Q}_\pi^{(r)}$, where $\pi \subseteq \mathrm{spec}(G)$, $r = \mathrm{rk}(A) > 0$ and $h(G) = r + h(G/A)$. We have an exact sequence

$$1 \to \overline{A} \to \widehat{G}_p \to \widehat{(G/A)}_p \to 1 \tag{16.2}$$

where $\overline{A}$ denotes the closure of A in $\widehat{G}_p$. Now $\overline{A}$ is an image of $\widehat{A}_p$ and $\widehat{A}_p \cong \mathbb{Z}_p^{(s)}$ for some $s \leq r$; moreover $s = r$ if $p \notin \pi$. Since the rank is subadditive and the dimension is additive on extensions of pro-p groups, and $\dim(\mathbb{Z}_p) = 1$, (↬ **Pro-p groups**), the first claim of the proposition follows by induction on $h(G)$.

For the second claim, let $H = \bigcap \mathrm{C}_G(M)$ where M ranges over all the normal sections of G that are elementary abelian p-groups; since G has finite rank m, say, we have $G/\mathrm{C}_G(M) \hookrightarrow \mathrm{GL}_m(\mathbb{F}_p)$ for each such M, and as G is soluble of finite rank it follows that G/H is finite. We claim that $\dim(\widehat{H}_p) = h(G)$.

Replacing G by H in (16.2) and arguing by induction, it suffices now to show that if $\overline{A}$ is the closure of A in $\widehat{H}_p$ then $\overline{A} \cong \widehat{A}_p$. This holds provided the pro-p topology on H induces that on A. A base for the neighbourhoods of 1 in the latter topology is the family of subgroups A^{p^n}, $n \in \mathbb{N}$, so it remains to show that for each n there exists a normal subgroup K_n of finite p-power index in H such that $A^{p^n} = A \cap K_n$.

By Proposition 16.4.8 the quotient G/A^{p^n} is residually finite, so there exists a normal subgroup N of finite index in G with $A \cap N = A^{p^n}$. Now put $K/(N \cap H) = O_{p'}(H/(N \cap H))$. Evidently $K \cap A = A^{p^n}$. We claim that H/K is a p-group. To see this, put $P/K = O_p(H/K)$. If $P < H$ then there exists a normal subgroup Q/P of H/P with $Q \leq H$ and $1 \neq Q/P$ an abelian q-group for some prime $q \neq p$. The definition of H ensures that H acts nilpotently on P/K, so Q/K is a nilpotent group, hence has a unique Sylow q-subgroup Q_0/K. But $Q_0/(N \cap H)$ is a normal p'-subgroup of $H/(N \cap H)$ and $Q_0 > K$, contradicting the definition of K. It follows that $H/K = P/K$ is a p-group, as claimed. This completes the proof. ■

Remark. It is not hard to see that the converse of the final statement is also true, in the sense that if $p \in \mathrm{spec}(G)$ then $\dim(\widehat{H}_p) < h(G)$ for every subgroup H of finite index in G.

3 Finitely generated metabelian groups

In the 1950s Philip Hall obtained some deep results about the structure of finitely generated soluble groups by generalising facts from commutative algebra to the case of certain non-commutative group rings. When dealing with metabelian groups, it is enough to apply Hall's methodology and the original commutative algebra. (For Hall's results, which include everything we need, see [R], Sections 15.3-15.5.)

Throughout this section, G denotes a finitely generated metabelian group. Thus G has an abelian normal subgroup A such that G/A is also abelian. The

conjugation action of G on A induces an action of G/A on A, whereby A may be considered a module for the group ring $\mathbb{Z}(G/A) = R$. Thus R is a *finitely generated commutative ring*.

Lemma 16.4.12 *A is finitely generated as an R-module.*

Proof. Let $\theta : F \to G$ be a presentation of G where F is a finitely generated free group, and put $N = \theta^{-1}(A)$. Then F/N is abelian, hence finitely presented, and it follows that N is generated as a normal subgroup of F by finitely many elements $x_1, \ldots, x_m$. Their images $\theta(x_1), \ldots, \theta(x_m)$ then generate A as a normal subgoup of G, hence as an R-module. ■

As R is a Noetherian ring by Hilbert's basis theorem, we deduce

Proposition 16.4.13 *A is a Noetherian R-module.*

Next, we need

Lemma 16.4.14 *A is residually finite as an R-module.*

Proof. Let $0 \neq a \in A$ and let N be a submodule of A maximal subject to $a \notin N$; it will suffice to show that A/N is finite. So replacing A by A/N, we reduce to the case where every non-zero submodule of A contains a. Let I be a maximal ideal of R containing the annihilator of a, and write

$$AI^\infty = \bigcap_{n=1}^{\infty} AI^n.$$

According to Krull's intersection theorem ([AM], Theorem 10.17) there exists $r \in I$ such that $AI^\infty(1 - r) = 0$.

Suppose that $AI^n \neq 0$ for each n. Then $a \in AI^\infty$, so $1 - r \in \mathrm{ann}_R(a) \subseteq I$, which is impossible since $r \in I$. Therefore $AI^n = 0$ for some n. Now R/I is a finite field (see below) and each factor I^j/I^{j+1} is a finitely generated R/I-module, so the ring R/I^n is finite. Therefore so is the finitely generated R/I^n-module A. ■

Remark We quoted the fact that R/I is a finite if I is a maximal ideal of R. This follows from a form of Hilbert's Nullstellensatz: *if k is a field, E is a finitely generated k-algebra, and E is a field then E is a finite extension of k* (see [AM], Cor. 5.24). To conclude that $R/I = E$ is *finite*, we also need to know that the prime field k of R/I is finite; this may be deduced from the 'generic freeness lemma', [E], Theorem 4.14.

We can now deduce

Proposition 16.4.15 *The group G is residually finite.*

Proof. Suppose first that A is finite, and put $K = \mathrm{C}_G(A)$. Then $[K, K] \leq K \cap A \leq \mathrm{Z}(K)$ so K is nilpotent. Also K has finite index in G, so K is finitely generated. Therefore K is residually finite (see Section 1 above), and hence so is G.

The general case follows from the preceding lemma, which shows that the normal subgroups N of G with $N \leq A$ and N/A finite intersect in 1. ■

A similar argument gives

Proposition 16.4.16 (B. Wehrfritz; see also [Segal 1974]) *G has a normal subgroup G_0 of finite index such that G_0 is residually nilpotent.*

Proof. It suffices to show that $AI^\infty = 0$ for some ideal I of finite index in R; indeed, the inverse image G_0 in G of $(G/A) \cap (1 + I)$ satisfies

$$\gamma_{n+1}(G_0) \leq AI^n$$

for each n, so G_0 is residually nilpotent if $AI^\infty = 0$, and G/G_0 is isomorphic to a subgroup of the unit group in the finite ring R/I.

Let us call A 'good' if such an ideal exists. Suppose now that A is not good. Then A has a submodule D maximal with the property that A/D is not good, and in order to arrive at a contradiction we may factor out D and suppose that every proper quotient module of A is good. Let I be a maximal ideal of R containing the annihilator of A. As before we find $r \in I$ such that $AI^\infty(1 - r) = 0$. By the Artin-Rees Lemma ([AM], Chapter 10) there exists m such that

$$A(1 - r)^m \cap AI^\infty \subseteq AI^\infty(1 - r) = 0.$$

Since $r \in I$ we cannot have $(1 - r)^m \in I$, so $0 \neq A(1 - r)^m = B$, say. Then A/B is good, so there exists an ideal J of finite index in R with $AJ^\infty \subseteq B$. But then $K = J \cap I$ has finite index in R and $AK^\infty \subseteq B \cap AI^\infty = 0$, so A is good, a contradiction. ■

The next result is a special case of Grothendieck's 'generic freeness lemma', see [E], Theorem 4.14. Actually, Hall's non-commutative "generalisation" probably came first; his proof is given in [R], **15.4.3**.

Proposition 16.4.17 *The group A contains a free abelian subgroup F such that A/F is a π-group for some finite set of primes π.*

Hall proved this as a step towards his proof of residual finiteness. For our purposes, its importance lies in the following consequence:

Corollary 16.4.18 *For almost all primes p,*

$$\mathrm{rk}(F) \leq \mathrm{ur}_p(G) \leq \mathrm{rk}(F) + \mathrm{rk}(G/A).$$

This follows because if $p \notin \pi$ then

$$A/A^p \cong F/F^p,$$

and $\mathrm{rk}(A/A^p) \leq \mathrm{ur}_p(G)$ since G/A^p is residually finite, while $\mathrm{rk}(F/F^p) = \mathrm{rk}(F)$.

Window: Linear groups

Here we collect mostly standard material about group-theoretic properties of linear groups, most of which appear in Wehrfritz's book [We]. Some deeper results relating to strong approximation are discussed in the window of that name.

Throughout, F denotes a field with algebraic closure $\overline{F}$, and n is a positive integer. The subgroup of upper-triangular matrices in $\mathrm{GL}_n(F)$ is denoted $\mathrm{Tr}(n,F)$ and the subgroup of upper uni-triangular matrices is denoted $\mathrm{Tr}_1(n,F)$.

G denotes a subgroup of $\mathrm{GL}_n(F)$.

1 Soluble groups

The basic result is

Theorem 16.4.1 (Lie, Kolchin) *If G is soluble and connected in the Zariski topology then G is triangularizable, that is, there exists $x \in \mathrm{GL}_n(\overline{F})$ such that $x^{-1}Gx \leq \mathrm{Tr}(n,\overline{F})$.*

See [We], Chapter 5. This implies that any soluble G has a normal subgroup of finite index that is triangularizable; this index can be effectively bounded:

Theorem 16.4.2 (Mal'cev) *There is a function f such that every soluble subgroup of $\mathrm{GL}_n(F)$ has a triangularizable normal subgroup of index at most $f(n)$.*

See [We], Chapter 5. It is important to note that $f(n)$ depends only on n and not on the field F.

Since $\mathrm{Tr}_1(n,F)$ is nilpotent of class $n-1$ and $\mathrm{Tr}(n,F)/\mathrm{Tr}_1(n,F)$ is abelian, this implies

Theorem 16.4.3 (Zassenhaus) *There is a function g such that every soluble subgroup of $\mathrm{GL}_n(F)$ has derived length at most $g(n)$.*

2 Jordan's theorem

Theorem 16.4.4 (C. Jordan, 1878) *If $\mathrm{char}(F) = 0$ and G is finite then G has an abelian normal subgroup of index at most $j(n)$, where $j(n)$ depends only on n.*

See [Curtis & Reiner 1981] (or [Ra], Theorem 8.29 for a more general result). This has an important extension:

Theorem 16.4.5 (Platonov) *If* $\mathrm{char}(F) = 0$ *and* G *is virtually soluble then* G *has a soluble normal subgroup of index at most* $j(n)$.

See [We], Corollary 10.11.

3 Monomial groups

A matrix in $\mathrm{GL}_n(F)$ is *monomial* if it has exactly one non-zero entry in each row and each column. These form a subgroup $\mathrm{Mon}(n, F)$, which is the semi-direct product of the diagonal group by the group of permutation matrices; thus

$$\mathrm{Mon}(n, F) \cong (F^*)^n \rtimes \mathrm{Sym}(n).$$

Proposition 16.4.6 *If* G *is completely reducible and nilpotent then there exists* $x \in \mathrm{GL}_n(\overline{F})$ *such that* $x^{-1}Gx \leq \mathrm{Mon}(n, \overline{F})$.

This follows from [We], Theorem 1.14. It applies in particular when G is a finite nilpotent group and $\mathrm{char}(F) \nmid |G|$, by Maschke's theorem. Since every finite subgroup of $\overline{F}^*$ is cyclic, we deduce

Corollary 16.4.7 *If* G *is finite and nilpotent and* $\mathrm{char}(F) \nmid |G|$ *then* G *is an extension of an abelian group of rank at most* n *by some subgroup of* $\mathrm{Sym}(n)$.

4 Finitely generated groups

If G is finitely generated then $G \leq \mathrm{GL}_n(R)$ where R is some finitely generated subring of F. For each (proper) ideal I of R, let

$$G(I) = G \cap (1_n + M_n(I))$$

denote the kernel of the natural projection $\mathrm{GL}_n(R) \to \mathrm{GL}_n(R/I)$. Thus if I has finite index in R then $G(I)$ is a normal subgroup of finite index in G. We now quote some facts from commutative algebra:

(i) Every maximal ideal of R has finite index (↬ **Soluble groups**, §3, **Remark).**

(ii) $\mathrm{Jac}(R) = \bigcap\{M \mid M \text{ is a maximal ideal of } R\} = 0$ ([AM], Chap. 5, Exercise 24).

(iii) For each proper ideal I of R, $\bigcap_{j=1}^{\infty} I^j = 0$ ([AM], Corollary 10.18).

From (ii) it follows that the subgroups $G(M)$ as M ranges over maximal ideals intersect in 1, and with (i) this gives

Proposition 16.4.8 (Mal'cev) *If G is finitely generated then G is residually finite, indeed residually (linear of degree n over finite fields).*

This result has a sort of converse: see the **Linearity conditions** window.

Now fix one maximal ideal M. Then R/M is a finite field, of characteristic p say, and it is easy to see that for each i, M^i/M^{i+1} is a finite (additive) group of exponent p. If $i \geq 1$ and $x \in G(M^i)$ then $(x-1)^p$ and $p(x-1)$ are both $\equiv 0$ modulo M^{i+1}, and it follows that $x^p \in G(M^{i+1})$. Thus $G(M^i)/G(M^{i+1})$ has exponent (dividing) p, and so $G(M)/G(M^j)$ is a finite p-group for each $j \geq 1$. With (iii) this gives the first claim in

Proposition 16.4.9 *If G is finitely generated then G has a normal subgroup of finite index which is residually a finite p-group, for some prime p, where $p = \mathrm{char}(F)$ if $\mathrm{char}(F) \neq 0$.*

If $\mathrm{char}(F) = 0$, this holds for all but finitely many primes p.

The final claim follows from the fact that $pR = R$ for only finitely many primes p, by 'generic freeness' ([E] Theorem 14.4). One half of the 'Lubotzky linearity criterion' asserts (in the characteristic zero case) that, for almost all primes p, G is virtually residually a finite p-group of *bounded rank*; this is discussed in the **Linearity conditions** window.

Since any element of finite order in a group that is residually a p-group must have p-power order, we see that $G(M_1) \cap G(M_2)$ is torsion free if $\mathrm{char}(R/M_1) \neq \mathrm{char}(R/M_2)$. Hence

Corollary 16.4.10 *If G is finitely generated and $\mathrm{char}(F) = 0$ then G is virtually torsion-free.*

5 Lang's theorem

A subgroup $\mathbf{G}$ of $\mathrm{GL}_n(\overline{F})$ that is closed in the Zariski topology is called a *linear algebraic group*. If the ideal of polynomials in $X_{11}, \ldots, X_{nn}$ that vanish on $\mathbf{G}$ can be generated by polynomials with coefficients in F then $\mathbf{G}$ is said to be *defined over F*, or an *F-group*. When F is perfect (for example, finite), a necessary and sufficient condition for $\mathbf{G}$ to be defined over F is the 'Galois criterion':

$$x \in \mathbf{G} \Longleftrightarrow x^\sigma \in \mathbf{G} \quad \text{for every } \sigma \in \mathrm{Gal}(\overline{F}/F)$$

([B] AG Theorem 14.4).

For any subring R of $\overline{F}$ one writes

$$\mathbf{G}(R) = \mathbf{G} \cap \mathrm{GL}_n(R).$$

In particular $\mathbf{G}(F)$ is the group of F-rational points of $\mathbf{G}$. One says that $\mathbf{G}$ is *connected* if it is connected in the Zariski topology. For further definitions and more details, see for example the books of Borel [B] or Humphreys [Hm].

In this section we asume that F is a *finite* field of size q. Let ϕ be the automorphism of $\overline{F}$ given by $\phi(x) = x^q$ $(x \in \overline{F})$, so F is the fixed-point set of ϕ. We assume that $\mathbf{G}$ is an F-group, and extend the map ϕ to $\mathbf{G}$ by applying it to each matrix entry. Then $\mathbf{G}(F)$ is exactly the fixed-point set of ϕ in $\mathbf{G}$.

Theorem 16.4.11 (Lang) *If* $\mathbf{G}$ *is connected then the mapping*

$$\sigma : \mathbf{G} \to \mathbf{G};\ x \mapsto \phi(x) \cdot x^{-1}$$

is surjective.

For the proof, see [B] §16.

A *Borel subgroup* of $\mathbf{G}$ is a maximal closed connected soluble subgroup of $\mathbf{G}$. A fundamental property of Borel subgroups is that they are all conjugate in $\mathbf{G}$ ([B] §11.1). If $\mathbf{G}$ has a Borel subgroup that is defined over F then $\mathbf{G}$ is said to be *quasi-split*.

Corollary 16.4.12 *If* $\mathbf{G}$ *is connected then* $\mathbf{G}$ *is quasi-split.*

Proof. Let B be a Borel subgroup of $\mathbf{G}$. Then $\phi(B)$ is another one so there exists $x \in \mathbf{G}$ such that $x^{-1}Bx = \phi(B)$. By Lang's theorem we have $x^{-1} = \phi(y) \cdot y^{-1}$ for some $y \in \mathbf{G}$. Put $C = y^{-1}By$. Then

$$\begin{aligned}\phi(C) &= \phi(y)^{-1}\phi(B)\phi(y) \\ &= \phi(y)^{-1} \cdot x^{-1}Bx \cdot \phi(y) \\ &= y^{-1}By = C.\end{aligned}$$

Now each element c of C has entries in some finite Galois extension of F, so if $\sigma \in \mathrm{Gal}(\overline{F}/F)$ then $c^\sigma = \phi^t(c)$ for some t, hence $c^\sigma \in C$. It follows by the 'Galois criterion' that C is defined over F. ■

Any closed subgroup of $\mathbf{G}$ that contains a Borel subgroup is called *parabolic* ([B] §11). The combinatorics of parabolic subgroups hold the key to the structure of a semisimple group; however the result we need here is the following, a special case of [B] Theorem 20.6:

Proposition 16.4.13 *Suppose that* $\mathbf{G}$ *is semisimple and connected. If* $\mathbf{G}$ *has a proper parabolic subgroup defined over* F *then* $\mathbf{G}$ *contains a non-trivial* F*-split torus.*

An F-split torus is a closed subgroup T that is isomorphic over F (as an algebraic group) to a product of copies of the multiplicative group $\overline{F}^*$. In particular, the group of F-rational points $T(F)$ is isomorphic to $(F^*)^{(m)}$ for some m. Combining the last two result we deduce:

Proposition 16.4.14 *If* $\mathbf{G}$ *is semisimple and connected then* $\mathbf{G}(F)$ *contains a copy of the group* F^*.

Window: Linearity conditions for infinite groups

1 Variations on Mal'cev's local theorem

It was a fundamental discovery of Mal'cev that for groups, the property of being linear of (fixed) degree n is of 'finite character'. From the metamathematical point of view, his observation was that this property can be expressed in a suitable first-order language; algebraically, what it means is that a group G is linear of degree n if and only if for every finite subset S of G there exists a degree-n linear representation ρ of $\langle S \rangle$ which separates S, i.e. such that $|\rho(S)| = |S|$. This sounds rather like saying that G is locally residually (linear of degree n), but is in fact stronger: a direct product of infinitely many elementary abelian groups of distinct prime exponents and unbounded ranks is residually linear of degree 1 but has no faithful linear representation over any field. If we make the additional assumption that G is *finitely generated*, however, then results like Mal'cev's obtain under the weaker hypothesis; this observation is due to [Wilson 1991_b]. The following proof is based on an idea that we learned from J. D. Dixon.

Notation

$$\mathcal{L}(n, R)$$

denotes the class of all linear groups of degree n over the ring R; for p a prime or 0,

$$\mathcal{L}(n, p) = \bigcup \{\mathcal{L}(n, F) \mid F \text{ a field of characteristic } p\}$$
$$\mathcal{L}(n) = \bigcup \{\mathcal{L}(n, F) \mid F \text{ a field}\}.$$

Let $n \in \mathbb{N}$, fixed throughout the following discussion, and let G be a group. Let S denote one of the rings

$$\mathbb{Z},\ \mathbb{F}_p \ \text{ or } \ \mathbb{Q};$$

by an *S-field* we mean a field that is an S-algebra, in other words any field if $S = \mathbb{Z}$, a field of characteristic p if $S = \mathbb{F}_p$, a field of characteristic zero if $S = \mathbb{Q}$.

Consider the polynomial ring

$$A = A(G) = S[X_{ij}(g) \mid i, j = 1, \ldots, n;\ g \in G]$$

where the $X_{ij}(g)$ are independent indeterminates. Let I be the ideal of A generated by the elements

$$E_{ij} = X_{ij}(1) - \delta_{ij} \qquad (\text{all } i, j)$$

$$P_{ij}(g, h) = X_{ij}(gh) - \sum_{k=1}^{n} X_{ik}(g)X_{kj}(h) \qquad (\text{all } i, j, \quad \text{all } g, h \in G),$$

and write $\overline{A} = A/I$. Then for each S-field F we have a $1-1$ correspondence

$$\mathrm{Hom}(G, \mathrm{GL}_n(F)) \to \mathrm{Hom}_{S\text{-alg}}(\overline{A}, F), \tag{16.1}$$

such that $\theta : G \to \mathrm{GL}_n(F)$ corresponds to $\theta^{\cdot} : \overline{A} \to F$ where $\overline{X_{ij}(g)}\theta^{\cdot} = (g\theta)_{ij}$ for all i, j and g (so $\overline{A}$ is the co-ordinate ring of the 'variety of n-dimensional representations' of G).

Now let $\{Y_{ij}(g) \mid i, j = 1, \ldots, n;\ g \in G \setminus \{1\}\}$ be a new set of indeterminates and put

$$B = B(G) = A[Y_{ij}(g) \mid i, j = 1, \ldots, n;\ g \in G \setminus \{1\}],$$

$$\overline{B} = \overline{B}(G) = B/IB.$$

For $1 \neq g \in G$ put

$$N(g) = 1 - \sum_{k,l=1}^{n} (X_{kl}(g) - \delta_{kl})Y_{kl}(g) \in B.$$

Suppose that $\theta : G \to \mathrm{GL}_n(F)$ corresponds to $\theta^{\cdot} : \overline{A} \to F$. Then for $1 \neq g \in G$ we have $g\theta \neq 1$ if and only if $\overline{X_{ij}(g)}\theta^{\cdot} \neq \delta_{ij}$ for some pair (i, j). In this case, we can extend $\theta^{\cdot}$ to a homomorphism $\theta^* : \overline{B} \to F$ such that $\overline{N(g)}\theta^* = 0$ by mapping

$$Y_{kl}(g) \mapsto \begin{cases} (\overline{X_{ij}(g)}\theta^{\cdot} - \delta_{ij})^{-1} & \text{for } (k, l) = (i, j) \\ 0 & \text{for } (k, l) \neq (i, j) \end{cases}$$

and for $h \neq g$ mapping each $Y_{kl}(h)$ to an arbitrary element of F. Conversely, if $\theta^* : \overline{B} \to F$ is any homomorphism that extends $\theta^{\cdot}$ and satisfies $\overline{N(g)}\theta^* = 0$, then $\overline{X_{kl}(g)}\theta^{\cdot} = \overline{X_{kl}(g)}\theta^* \neq \delta_{kl}$ for some pair (k, l), and so $g\theta \neq 1$.

It follows that for any given subset T of $G \setminus \{1\}$, the existence of a representation $\theta : G \to \mathrm{GL}_n(F)$ with $T \cap \ker\theta = \emptyset$ is equivalent to the existence of an algebra homomorphism $\theta^* : \overline{B} \to F$ with $\overline{N(g)} \in \ker\theta^*$ for all $g \in T$.

Putting

$$\mathcal{L} = \begin{cases} \mathcal{L}(n) & \text{if } S = \mathbb{Z} \\ \mathcal{L}(n,p) & \text{if } S = \mathbb{F}_p \\ \mathcal{L}(n,0) & \text{if } S = \mathbb{Q} \end{cases},$$

we can state

Theorem 16.4.1 (Mal'cev) *Let G be a group. Then $G \in \mathcal{L}$ if and only if for every finite subset T of G there exists a linear representation $\theta : \langle T \rangle \to \mathrm{GL}_n(F)$, where F is an S-field, such that $t\theta \neq 1$ for all $t \in T \setminus \{1\}$.*

Proof. We only have to prove the 'if' statement. Let J be the ideal of B generated by the set $\{N(g) \mid 1 \neq g \in G\}$. If $\overline{J} \neq \overline{B}$ then $\overline{J}$ is contained in a maximal ideal M of $\overline{B}$, and the residue mapping $\theta^* : \overline{B} \to \overline{B}/M = F$ satisfies $\overline{N(g)} \in \ker \theta^*$ for all $g \in G \setminus \{1\}$. It follows by the above discussion (taking $T = G \setminus \{1\}$) that the corresponding representation $\theta : G \to \mathrm{GL}_n(F)$ is faithful, so in this case $G \in \mathcal{L}$.

Suppose that $\overline{J} = \overline{B}$. Then $1 \in IB + J$ and we can write

$$1 = \sum U_{ij} E_{ij} + \sum_{g,h \in T} V_{ij}(g,h) P_{ij}(g,h) + \sum_{t \in T \setminus \{1\}} W(t) N(t) \tag{16.2}$$

for some finite subset T of G and suitable elements U_{ij}, $V_{ij}(g,h), W(g) \in B$. There is a finite subset $T' \supseteq T$ of G such that each of these elements lies in the subring $B(H)$ of B where $H = \langle T' \rangle$. By hypothesis, there exists a representation $\theta : H \to \mathrm{GL}_n(F)$, for some S-field F, such that $t\theta \neq 1$ for all $t \in T' \setminus \{1\}$. The corresponding homomorphism $\theta^* : \overline{B}(H) \to F$ then satisfies $\overline{N(t)}\theta^* = 0$ for each $t \in T' \setminus \{1\}$; applying θ^* to the image of equation (16.2) in $\overline{B}(H)$ now yields the contradiction $1 = 1\theta^* = 0$.

This completes the proof. ■

Assume next that $G = \langle g_1, \ldots, g_d \rangle$ is finitely generated. Then so is the S-algebra

$$\overline{A} = A/I,$$

namely by the elements $\overline{X_{ij}(g_k)}$, $\overline{X_{ij}(g_k^{-1})}$ for $i, j = 1, \ldots, n$ and $k = 1, \ldots, d$. It follows that $\overline{A}$ has only finitely many minimal prime ideals, $P_1, \ldots, P_m$ say. Denote by E_k the field of fractions of the integral domain $\overline{A}/P_k$. If $\theta : G \to \mathrm{GL}_n(F)$ is a representation of G in an S-field F then $\theta^* : \overline{A} \to F$ factors through $\overline{A}/P_k$ for some k; it follows that θ factors through

$$\begin{aligned} \pi_k : G &\to \mathrm{GL}_n(\overline{A}/P_k) \leq \mathrm{GL}_n(E_k) \\ g &\mapsto (\overline{X_{ij}(g)} + P_k). \end{aligned}$$

Hence if $g \in G$ and $g\theta \neq 1$ then $g\pi_k \neq 1$ for some k, and so $g\pi \neq 1$ where

$$\pi = (\pi_1, \ldots, \pi_m) : G \to \mathrm{GL}_n(E_1) \times \cdots \times \mathrm{GL}_n(E_m).$$

Suppose now that G is residually in $\mathcal{L}$. Then for each element $g \neq 1$ in G there exists a representation θ as above with $g\theta \neq 1$, and then $g\pi \neq 1$. Thus $\ker \pi = 1$ and so π embeds G into $\mathrm{GL}_n(E_1) \times \cdots \times \mathrm{GL}_n(E_m)$.

If $S = \mathbb{F}_p$ or $S = \mathbb{Q}$ then each E_k is an extension field of S; in this case there exists an extension field E of S that contains $E_1, \ldots, E_m$, and $\mathrm{GL}_n(E_1) \times \cdots \times \mathrm{GL}_n(E_m) \leq \mathrm{GL}_{mn}(E)$. Thus we have established the first two parts of

Theorem 16.4.2 *Let G be a finitely generated group.*
(i) If G is residually in $\mathcal{L}(n)$ then G is a subdirect product of finitely many linear groups of degree n.
(ii) Let p be a prime or zero. If G is residually in $\mathcal{L}(n, p)$ then G is in $\mathcal{L}(mn, p)$ for some m.
(iii) Let (F_α) be a family of fields such that for each prime p only finitely many of the F_α have characteristic p, and these are all finite. Suppose that G admits representations $\theta_\alpha : G \to \mathrm{GL}_n(F_\alpha)$ such that $\bigcap_\alpha \ker \theta_\alpha = 1$. Then $G \in \mathcal{L}(n', 0)$ for some n'.

To prove (iii), we take $S = \mathbb{Z}$, and suppose that $E_1, \ldots, E_r$ have characteristic 0 while the rest have positive characteristic. We embed the E_k for $1 \leq k \leq r$ in a common field E of characteristic zero, and write

$$\pi_0 = (\pi_1, \ldots, \pi_r) : G \to \mathrm{GL}_n(E_1) \times \cdots \times \mathrm{GL}_n(E_m) \leq \mathrm{GL}_{rn}(E).$$

Let $\mathcal{X} = \{\alpha \mid \mathrm{char} F_\alpha \neq 0\}$, and put

$$K = \bigcap_{\alpha \in \mathcal{X}} \ker \theta_\alpha$$

(if $\mathcal{X}$ is empty, $K = G$). Suppose $1 \neq g \in K$. Then $g\theta_\alpha \neq 1$ for some $\alpha \notin \mathcal{X}$. Now $\theta_\alpha : \overline{A} \to F_\alpha$ factors through $\overline{A}/P_k$ for some k, and then

$$\mathrm{char} E_k = \mathrm{char} F_\alpha = 0,$$

so $k \leq r$. Since θ factors through π_k it follows that $g\pi_0 \neq 1$. Thus

$$K \cap \ker \pi_0 = 1,$$

and G embeds in $G/K \times G\pi_0$.

Now the hypotheses imply that G/K is finite, of order f say. Then G/K embeds in $\mathrm{GL}_f(E)$ and G embeds in $\mathrm{GL}_f(E) \times \mathrm{GL}_{rn}(E) \leq \mathrm{GL}_{n'}(E)$ where $n' = f + rn$. This completes the proof.

(A quicker way to prove (i) and (ii) is to observe that G maps injectively into $\mathrm{GL}_n(R)$ where R is a finitely generated subring of a Cartesian product of S-fields; see [Wilson 1991_b], [Lubotzky, Mann and Segal 1993]. We have chosen the present approach via representation rings to emphasize the relationship with Mal'cev's local theorem.)

We shall apply this result to groups satisfying the following condition:

Definition A group G has *restricted upper chief factors* if there is a finite upper bound to $\mathrm{rk}(M)$ as M ranges over all the non-abelian upper chief factors of G.

Corollary 16.4.3 *Let G be a finitely generated group with restricted upper chief factors. Then there is an exact sequence*

$$1 \to D \to G \to \mathrm{GL}_n(F)$$

where F is a field of characteristic zero and the closure of D in $\widehat{G}$ is prosoluble.

The stated property of D amounts to saying that $D/(N \cap D)$ is soluble for every normal subgroup N of finite index in G.

Proof. Let $\mathcal{M}$ be the set of (G-isomorphism types of) non-abelian upper chief factors of G, and put

$$D = \bigcap_{M \in \mathcal{M}} \mathrm{C}_G(M).$$

If $N \lhd_{\mathrm{f}} G$ then by considering a chief series of G/N through DN/N we see at once that $D/(N \cap D) \cong DN/N$ is soluble; so D has the stated property.

Let $\mathcal{M}_0$ denote the subset of $\mathcal{M}$ consisting of groups that are products of sporadic or alternating groups, and for each prime p let $\mathcal{M}_p$ denote the set of those members of $\mathcal{M}$ that are products of simple groups of Lie type in characteristic p. Since by hypothesis $\mathcal{M}$ consists of groups of bounded rank, we see that for each p, prime or zero, the set $\mathcal{M}_p$ contains only finitely many non-isomorphic groups; as G is finitely generated there is only a finite number of possible G-actions on each of these groups, and it follows that each of the sets $\mathcal{M}_p$ is finite.

Now according to Corollaries 13 and 8 in the **Finite simple groups** window, there exists f, independent of p, such that $\mathrm{Aut}(M) \leq \mathrm{GL}_f(\mathbb{F}_p)$ for every $M \in \mathcal{M}_p$ if p is a prime; and this holds also for $p = 0$ if we write $\mathbb{F}_0 = \mathbb{Q}$ and take $f \geq \max\{|\mathrm{Aut}(M)| \mid M \in \mathcal{M}_0\}$.

Since $\mathrm{C}_G(M)$ is the kernel of the natural map $G \to \mathrm{Aut}(M)$, part (iii) of Theorem 16.4.2 now applies to show that G/D is a linear group in characteristic zero. ■

2 Groups that are residually of bounded rank

The following useful analogue to Theorem 16.4.2 has a slightly different hypothesis and a slightly weaker conclusion.

Theorem 16.4.4 [Segal 1996_a] *Let G be a finitely generated group. Suppose that G is residually (finite soluble of rank $\leq r$), where r is finite. Then G has a nilpotent normal subgroup D such that G/D is a subdirect product of finitely many linear groups over fields.*

Proof Let G/K be a finite soluble quotient of G. Then G/K has a normal subgroup N/K which is nilpotent of class at most 2 and satisfies $\mathrm{C}_G(N/K) \leq N$ ($\looparrowright$ **Finite group theory**). Put $E_K = N/N'K$

Claim: If $H \lhd G$ and $[E_K, {}_k\, H] = 1$ then $\gamma_{6k}H \leq K$.

To see this, write $\overline{N} = N/K$ and observe that

$$\begin{aligned}[\overline{N}, {}_k\, H] \leq \overline{N}' &\Longrightarrow [\overline{N}', {}_{2k}\, H] \leq \gamma_3\overline{N} = 1\\ &\Longrightarrow [\overline{N}, {}_{3k}\, H] = 1\\ &\Longrightarrow \gamma_{3k}H \leq \mathrm{C}_G(\overline{N}) \leq N\\ &\Longrightarrow \gamma_{6k}H \leq [N, {}_{3k}\, H] \leq K\end{aligned}$$

($\looparrowright$ **Soluble groups**).

Now for some finite r, G has a family $\mathcal{S}$ of normal subgroups, intersecting in the identity, such that G/K is finite and soluble of rank at most r for each $K \in \mathcal{S}$. For $K \in \mathcal{S}$ let E_K be the section of G/K indicated above, and write Z for the Cartesian product of all the abelian groups E_K. Then Z is an r-generator module for the ring $R = \mathbb{Z}^{\mathcal{S}}$, on which G acts by R-module automorphisms. Since G is finitely generated, there exist a finitely generated subring S of R and an r-generator S-submodule M of Z such that $MG = M$ and $MR = Z$.

Since S is a commutative Noetherian ring, M contains a finite chain of fully invariant S-submodules

$$0 = M_0 < M_1 < \ldots < M_k = M$$

such that, for each j, M_j/M_{j-1} is a finitely generated torsion-free S/P_j-module, where $P_j = \mathrm{ann}_S(M_j/M_{j-1})$ is a prime ideal of S (see e.g. [We], Lemma 13.2). Put $Q_j = \mathrm{C}_G(M_j/M_{j-1})$, and suppose that M_j/M_{j-1} can be generated by r_j elements as an S/P_j-module. Then the action of G embeds G/Q_j in

$$\mathrm{Aut}_{S/P_j}(M_j/M_{j-1}) \leq \mathrm{GL}_{r_j}(F_j)$$

where F_j is the field of fractions of S/P_j.

Put $D = Q_1 \cap \ldots \cap Q_k$. Then

$$Z(D-1)^k = M(D-1)^k R = 0.$$

It follows that $[E_K, {}_k\, D] = 1$ for every $K \in \mathcal{S}$. By the initial *Claim*, this implies that

$$\gamma_{6k}D \leq \bigcap \mathcal{S} = 1.$$

The theorem follows since

$$G/D \hookrightarrow G/Q_1 \times \cdots \times G/Q_k \hookrightarrow \prod_{j=1}^{k} \mathrm{GL}_{r_j}(F_j).$$

Corollary 16.4.5 (of the proof) *Let G be as in Theorem 16.4.4. If every finite quotient of G is soluble, then G is virtually nilpotent-by-abelian.*

Proof Suppose now that every finite quotient of G is soluble. Let $1 \leq j \leq k$, put $S_j = S/P_j$ and $V_j = M_j/M_{j-1}$. If L is a maximal ideal of S_j then G induces on V_j/V_jL a finite linear group of degree at most r_j. It follows by Mal'cev's theorem (↬ **Linear groups**) that G has a normal subgroup H, of finite index bounded by a function of r_j, such that H' acts unipotently on V_j/V_jL. Since G is finitely generated, we can choose $H = H_j$, say, independently of L, and then have

$$V_j(H_j' - 1)^{r_j} \subseteq \bigcap_L V_jL = 0$$

(the final equality follows easily from the facts that V_j is torsion-free and finitely generated and the Jacobson radical of S_j is zero).

Now let $T = \bigcap_{j=1}^k H_j$ and put $s = r_1 + \cdots + r_k$. Then $M(T' - 1)^s = 0$. As above, this implies that $\gamma_{6s}(T') = 1$, and the result follows since G/T is finite.

3 Applications of Ado's theorem

Ado's theorem asserts that every finite-dimensional Lie algebra over a field of characteristic zero has a faithful linear representation. If the Lie algebra is associated to an analytic group, this gives rise to a linear representation of the group, which may not be faithful in general; however, for a compact p-adic analytic group we do indeed obtain a faithful representation for some open subgroup, which can be induced up to a faithful representation of the whole group. Since these groups include the pro-p groups of finite rank, we have

Theorem 16.4.6 *Let G be a pro-p group of finite rank. Then G is isomorphic to a closed subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ for some n.*

For details of the proof, see [DDMS], Section 7.3. An important consequence is

Theorem 16.4.7 'Lubotzky linearity criterion' [Lubotzky 1988] *Let Γ be a finitely generated group. Then $\Gamma \in \mathcal{L}(n, 0)$ for some n if and only if there exist a prime p and an integer r such that Γ has a filtration by normal subgroups (Γ_i) such that Γ/Γ_1 is finite, Γ_1/Γ_i is a finite p-group of rank $\leq r$ for each $i \geq 1$, and $\bigcap_{i=1}^\infty \Gamma_i = 1$.*

To prove the 'if' statement, observe that Γ_1 embeds in

$$G = \varprojlim \Gamma_1/\Gamma_i.$$

Now G is a pro-p group of rank at most r, hence linear over $\mathbb{Q}_p$ by Theorem 16.4.6. Therefore so is Γ_1, and the induced representation of Γ is a faithful linear representation over $\mathbb{Q}_p$. For the converse, see [Lubotzky 1988] or [DDMS], Interlude B (in fact the converse holds in a stronger form: if Γ is linear in characteristic zero then a filtration of the stated kind exists for almost all primes p).

All this applies to groups that are virtually residually p-groups. In some circumstances this can be generalised.

Theorem 16.4.8 *Let Γ be a finitely generated residually nilpotent group. If the pro-p completion $\widehat{\Gamma}_p$ has finite rank for every prime p then $\Gamma \in \mathcal{L}(n,0)$ for some n.*

This will follow from Theorem 16.4.6 once we have established the following lemma:

Lemma 16.4.9 *Let Γ be a finitely generated residually nilpotent group. Suppose that, for some prime p, the pro-p completion $\widehat{\Gamma}_p$ has finite rank. Then there exists a finite set π of primes such that the natural map*

$$\Gamma \to \prod_{\ell \in \pi} \widehat{\Gamma}_\ell$$

is injective.

Indeed, the hypotheses of Theorem 16.4.8 then imply that $\widehat{\Gamma}_\ell \hookrightarrow \mathrm{GL}_{n(\ell)(}(\mathbb{Z}_\ell)$ for each $\ell \in \pi$, so Γ embeds into

$$\prod_{\ell \in \pi} \mathrm{GL}_{n(\ell)(}(\mathbb{Z}_\ell) \leq \mathrm{GL}_n(\mathbb{C})$$

where $n = \sum_{\ell \in \pi} n(\ell)$.

Proof of Lemma 16.4.9 Suppose that Λ is a torsion-free nilpotent quotient of Γ. Then $\widehat{\Lambda}_p$ is an image of $\widehat{\Gamma}_p$, so $\dim(\widehat{\Lambda}_p) \leq \dim(\widehat{\Gamma}_p)$. Now $\dim(\widehat{\Lambda}_p)$ is equal to the Hirsch length $h(\Lambda)$ of Λ, so we have

$$h(\Lambda) \leq \dim(\widehat{\Gamma}_p).$$

We may therefore choose a normal subgroup T of Γ such that Γ/T is torsion-free and nilpotent of maximal possible Hirsch length. Then $\gamma_n(\Gamma) \leq T$ and $T/\gamma_n(\Gamma)$ is finite, for every n exceeding the nilpotency class of Γ/T (↬ **Soluble groups**). It follows that $T/[T,\Gamma]$ is finite, of order m, say.

Let $q \nmid m$ be a prime, and suppose that $Q \lhd \Gamma$ has finite index a power of q. Then $T = (T \cap Q)[T,\Gamma]$, and as $\Gamma/(T \cap Q)$ is nilpotent it follows that $T = (T \cap Q) \leq Q$. Hence T is contained in the kernel $\Gamma(q)$, say, of the natural homomorphism $\Gamma \to \widehat{\Gamma}_q$. On the other hand, $T \geq \Gamma(q)$ because Γ/T is residually a finite q-group (Gruenberg's theorem, ↬ **Soluble groups**).

Thus $\Gamma(q) = T$ for every prime $q \nmid m$. Choose one such prime q and let π be the set of prime divisors of m together with q. The kernel of the natural map $\Gamma \to \prod_{\ell \in \pi} \widehat{\Gamma}_\ell$ is then

$$\bigcap_{\ell \in \pi} \Gamma(\ell) = T \cap \bigcap_{\ell \mid m} \Gamma(\ell) = \bigcap_{\text{all primes } \ell} \Gamma(\ell) = 1,$$

since Γ is residually nilpotent. The result follows.

Window: Strong approximation for linear groups

The original Strong Approximation Theorem, commonly attributed to the ancient Chinese, says that $\mathbb{Z}$ is dense in the profinite group $\prod_p \mathbb{Z}_p$. An analogous formulation is valid for the additive group of an algebraic number field. Such a group may be viewed as the $\mathbb{Q}$-rational points of a linear algebraic group over $\mathbb{Q}$, and one is led to consider the question of strong approximation in linear groups.

In group-theoretic terms, the question is this: given a subgroup Λ of $\mathrm{GL}_n(\mathbb{Z})$, what is the image $\pi_m(\Lambda)$ of Λ in $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$, for arbitrary values of m? Obviously, if Λ is contained in a proper algebraic subgroup $\mathbf{G}$ of GL_n then $\pi_m(\Lambda)$ must be contained in the corresponding subgroup $G(\mathbb{Z}/m\mathbb{Z})$. One says that Λ has the *strong approximation property* if this is the only obstacle to solving congruences in Λ; more precisely (and slightly more generally), let us make the following definition, where for a set of primes S we put

$$\mathbb{Z}_S = \mathbb{Z}[p^{-1} \mid p \in S].$$

Definition Let S be a finite set of primes, Λ a subgroup of $\mathrm{GL}_n(\mathbb{Z}_S)$ and $\mathbf{G}$ the Zariski-closure of Λ in GL_n. Then Λ has *strong approximation* w.r.t. S if Λ is dense in the profinite group

$$\mathbf{G}(\widehat{\mathbb{Z}_S}) = \prod_{p \notin S} \mathbf{G}(\mathbb{Z}_p).$$

In other words, the closure of Λ in the Zariski topology on $\mathbf{G}(\widehat{\mathbb{Z}_S})$ is the same as its closure in the *congruence topology*. On the face of it this may seem a rather technical matter; but the consequences are far-reaching. Indeed, when Λ has strong approximation we see that $\pi_m(\Lambda) = \mathbf{G}(\mathbb{Z}/m\mathbb{Z})$ whenever m is divisible by no prime in S. A lot is known about the finite groups $\mathbf{G}(\mathbb{Z}/m\mathbb{Z})$ when $\mathbf{G}$ is an algebraic group, and we may infer that Λ has this large collection of well-understood finite images, a matter of special interest to us in the context of this book.

The 'classical' Strong Approximation Theorem for algebraic groups gives sufficient (and necessary) conditions under which an S-arithmetic group $\mathbf{G}(\mathbb{Z}_S)$ in an algebraic group $\mathbf{G}$ has strong approximation in the above sense. Although deep and fundamental, this result is not entirely unexpected, because it applies essentially to algebraic groups that are in a sense generated by copies of the additive group. It was a remarkable discovery of Nori, Weisfeiler and others in the 1980s that similar results can be obtained for quite general linear groups. We shall state a particular case of their results in Section 1, and show there how it can be reduced to a certain theorem about finite linear groups. In Section 2 we outline three different approaches to the proof of this theorem (but stop well short of proving it in full). In the final section we briefly discuss a recent generalisation due to Pink, applicable to fields of arbitrary characteristic.

Our main application is presented in Section 3. Sometimes referred to as 'Lubotzky's alternative', this is the following theorem: *for a finitely generated linear group Γ over a field of characteristic zero, one of the following holds*:

(a) Γ *is virtually soluble,* or

(b) *there exist a simply-connected simple algebraic group $\mathbf{G}$ over $\mathbb{Q}$, a finite set of primes S such that $\mathbf{G}(\mathbb{Z}_S)$ is infinite, and a representation $\rho : \Gamma_0 \to \mathbf{G}(\mathbb{Z}_S)$, where Γ_0 is a normal subgroup of finite index in Γ, such that $\rho(\Gamma_0)$ is dense in $\mathbf{G}(\widehat{\mathbb{Z}_S})$.*

In particular, in case (b) it follows that Γ_0 *maps onto $\mathbf{G}(\mathbb{F}_p)$ for almost all primes p.*

A few other applications are discussed along the way.

1 A variant of the Strong Approximation Theorem

For definitions and background on algebraic groups, the reader is referred to [B] and [PR]. By a *linear algebraic group over* $\mathbb{Q}$ we mean a Zariski-closed subgroup $\mathbf{G}$ of $\mathrm{GL}_n = \mathrm{GL}_n(\mathbb{C})$ defined by some finite set of polynomial equations over $\mathbb{Q}$. Taking these equations to have $\mathbb{Z}$-coefficients, we may interpret them in any ring R, and then $\mathbf{G}(R)$ denotes the solution-set of these equations in $\mathrm{GL}_n(R)$. This is 'usually' a group, equal to the R-rational points of the group scheme $\mathbf{G}$. We shall leave aside such delicate foundational questions; when R is a domain of characteristic zero it may be embedded in $\mathbb{C}$, and then $\mathbf{G}(R) = \mathbf{G} \cap \mathrm{GL}_n(R)$; for the case $R = \mathbb{F}_p$ see the remarks following Corollary 3 below.

Let $\mathbf{G}$ be a connected, simply connected $\mathbb{Q}$-simple linear algebraic group defined over $\mathbb{Q}$, with a given embedding in GL_n. Let S be a finite set of primes. The S-arithmetic subgroup $\mathbf{G}(\mathbb{Z}_S)$ of $\mathbf{G}$ is infinite if and only if at least one of the groups $\mathbf{G}(\mathbb{Q}_p)$ for $p \in S \cup \{\infty\}$ is non-compact (here $\mathbb{Q}_\infty = \mathbb{R}$); in one direction this is easy to see, because $\mathbf{G}(\mathbb{Z}_S)$ sits 'diagonally' as a discrete subgroup in $\prod_{p \in S \cup \{\infty\}} \mathbf{G}(\mathbb{Q}_p)$. Under these conditions we have

Theorem 16.4.1 ([PR] Theorem 7.12) ***Strong Approximation Theorem for S-arithmetic groups:*** *Provided $\mathbf{G}(\mathbb{Z}_S)$ is infinite, it is dense in $\mathbf{G}(\widehat{\mathbb{Z}_S})$.*

This is equivalent to the statement

$$\mathbf{G}(\mathbb{Q}) \text{ is dense in } \mathbf{G}(\mathbb{A}_S),$$

where $\mathbb{A}_S$ denotes the ring of *S-adeles*; see [PR], §7.1. The same holds, with appropriate definitions, if $\mathbb{Q}$ is replaced by any algebraic number field.

We remark that some, but not all, of the hypotheses are necessary here: the conclusion holds if $\mathbf{G}$ is either semi-simple or unipotent, but not in general if $\mathbf{G}$ is an algebraic torus. But it is necessary that $\mathbf{G}(\mathbb{Q}_p)$ be non-compact for at least one $p \in S \cup \{\infty\}$, and that $\mathbf{G}$ be simply connected; a brief explanation of the latter requirement is given in §4.

The main result we are going to discuss is

Theorem 16.4.2 ***Strong Approximation Theorem for linear groups:*** *Let Λ be a Zariski-dense subgroup of $\mathbf{G}$ with $\Lambda \leq \mathbf{G}(\mathbb{Z}_S)$. Then the closure of Λ in $\mathbf{G}(\widehat{\mathbb{Z}_S})$ is open (hence of finite index) in $\mathbf{G}(\widehat{\mathbb{Z}_S})$.*

Several remarks are in order. First of all, since Λ is Zariski-dense in $\mathbf{G}$ it is certainly infinite, so the non-compactness condition mentioned above is automatically satisfied. Secondly, the conclusion is equivalent to the statement that the closure of Λ in the S-arithmetic group $\mathbf{G}(\mathbb{Z}_S)$ with respect to the congruence topology is of finite index in $\mathbf{G}(\mathbb{Z}_S)$; this is the topology induced on $\mathbf{G}(\mathbb{Z}_S)$ as a subspace of $\mathbf{G}(\widehat{\mathbb{Z}_S})$, and has a base for the neighbourhoods of 1 consisting of the *S-congruence subgroups* $\ker(\mathbf{G}(\mathbb{Z}_S) \to \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z}))$, where m ranges over integers not divisible by any prime in S. This follows from Theorem 1. Finally, to say that the closure $\overline{\Lambda}$ of Λ is open in $\mathbf{G}(\widehat{\mathbb{Z}_S})$ implies in particular that $\overline{\Lambda}$ contains

$$\mathbf{G}(\widehat{\mathbb{Z}_{S_1}}) = \prod_{p \notin S_1} \mathbf{G}(\mathbb{Z}_p)$$

for some finite set of primes S_1 containing S, hence that Λ actually has the strong approximation property w.r.t. S_1. Now if Λ is merely assumed to be a finitely generated subgroup of $\mathbf{G}(\mathbb{Q})$ then there exists a finite set S such that $\Lambda \leq \mathbf{G}(\mathbb{Z}_S)$, and enlarging S to S_1 as above we infer

Corollary 16.4.3 *Let Λ be a finitely generated Zariski-dense subgroup of $\mathbf{G}(\mathbb{Q})$. Then there exists a finite set of primes S such that Λ is dense in $\mathbf{G}(\widehat{\mathbb{Z}_S})$. In particular, for almost all primes p we have*

$$\pi_p(\Lambda) = \mathbf{G}(\mathbb{F}_p).$$

The final statement needs a word of explanation. For almost all primes p, the equations defining the algebraic group $\mathbf{G}$ can be reduced modulo p to give

a connected, semisimple algebraic subgroup of GL_n defined over $\mathbb{F}_p$, that we still denote by $\mathbf{G}$, and (for almost all p) one has $\pi_p(\mathbf{G}(\mathbb{Z}_p)) = \mathbf{G}(\mathbb{F}_p)$; see [PR], Proposition 3.20. Our claim therefore follows from the fact that $\pi_p(\Lambda) = \pi_p(\mathbf{G}(\mathbb{Z}_p))$ for almost all p.

This corollary, which suffices for some (though not all) applications, is a little easier to derive than the full strength of Theorem 16.4.2; it does not depend on Lemmas 16.4.4 and 16.4.5 below (they have other uses, however, and Corollary 16.4.6 is important in its own right).

We now outline the proof of Theorem 2. We explain the reduction to Proposition 16.4.7, below, in some detail, as it is not easily accessible in the literature; our approach is based on the unpublished manuscript [Nori (a)], where a considerably more general theorem is established. A complete published proof is available in [Weisfeiler 1984]; Weisfeiler's result is also much more general as he works over an arbitrary field (the somewhat easier theorem of [Mathews, Vaserstein & Weisfeiler 1984] does not quite cover our case as it deals with an absolutely simple $\mathbb{Q}$-group). A still more general theorem is proved by [Pink 2000] (see §4 below).

The $\mathbb{Q}$-simple group $\mathbf{G}$ may be identified with the restriction of scalars

$$\mathfrak{R}_{k/\mathbb{Q}}\mathbf{H}$$

of some absolutely simple k-group H, where k is a finite Galois extension of $\mathbb{Q}$. Then

$$\mathbf{G}(\mathbb{Q}) = \mathbf{H}(k)$$

and for each prime p we have

$$\mathbf{G}(\mathbb{Q}_p) = \prod_{i=1}^{f} \mathbf{H}(k_{\mathfrak{p}(i)})$$

where $k \otimes \mathbb{Q}_p = \prod_{i=1}^{f} k_{\mathfrak{p}(i)}$ (and $f = f(p)$ depends on p). We denote the Lie algebra of $\mathbf{G}$ by L; then $L(\mathbb{Q})$ is a simple module for $\mathbf{G}(\mathbb{Q})$ under the adjoint representation. In general, $L(\mathbb{Q}_p)$ is not simple for $\mathbf{G}(\mathbb{Q}_p)$, but it is semisimple and may be identified with

$$\bigoplus_{i=1}^{f} L_{\mathbf{H}}(k_{\mathfrak{p}(i)})$$

where $L_{\mathbf{H}}$ is the Lie algebra of $\mathbf{H}$; each summand $L_{\mathbf{H}}(k_{\mathfrak{p}(i)})$ is a minimal ideal and a minimal $\mathbf{G}(\mathbb{Q}_p)$-invariant subspace. For almost all p, the analogous decomposition is valid 'modulo p': that is,

$$\mathbf{G}(\mathbb{F}_p) = \prod_{i=1}^{f} \mathbf{H}(\mathcal{O}/\mathfrak{p}(i)), \tag{16.1}$$

$$L(\mathbb{F}_p) = \bigoplus_{i=1}^{f} L_{\mathbf{H}}(\mathcal{O}/\mathfrak{p}(i)) \tag{16.2}$$

($\mathcal{O}$ being the ring of integers of k). As $\mathbf{H}$ is an absolutely simple group, $L_{\mathbf{H}}(k)$ is absolutely irreducible as a $k[\mathbf{H}(k)]$-module, so $\mathrm{Ad}\mathbf{H}(k)$ spans $\mathrm{End}_k(L_{\mathbf{H}}(k))$; it follows that $\mathrm{Ad}\mathbf{H}(\mathcal{O}/\mathfrak{p})$ spans $\mathrm{End}_{\mathcal{O}/\mathfrak{p}}(L_{\mathbf{H}}(\mathcal{O}/\mathfrak{p}))$ for almost all primes $\mathfrak{p}$ of $\mathcal{O}$, in which case $L_{\mathbf{H}}(\mathcal{O}/\mathfrak{p})$ is irreducible for $\mathbf{H}(\mathcal{O}/\mathfrak{p})$. This implies that, for almost all primes p, (16.2) is a decomposition of $L(\mathbb{F}_p)$ into minimal ideals.

Lemma 16.4.4 *For every prime $p \notin S$ the closure of Λ in $\mathbf{G}(\mathbb{Z}_p)$ is open.*

Proof. (Sketch) Write P for the closure of Λ in $\mathbf{G}(\mathbb{Z}_p)$. Then P is a closed subgroup of the p-adic analytic group $\mathbf{G}(\mathbb{Z}_p)$, and the Lie algebra $L(P)$ of P is a subalgebra of the Lie algebra of $\mathbf{G}(\mathbb{Z}_p)$, which is $L(\mathbb{Q}_p)$ (see [DDMS], Chapter 9). Since Λ is Zariski-dense in $\mathbf{G}(\mathbb{Q}_p)$, the subalgebra $L(P)$ is invariant under the adjoint action of $\mathbf{G}(\mathbb{Q}_p)$, hence is an ideal in $L(\mathbb{Q}_p)$. Therefore $L(P)$ is equal to the sum of some of the $L_{\mathbf{H}}(k_{\mathfrak{p}(i)})$. Now since $\Lambda \leq \mathbf{G}(\mathbb{Q})$ it follows that the projections of Λ into each of the $\mathbf{H}(k_{\mathfrak{p}(i)})$ are isomorphic, and this implies that the projections of $L(P)$ into each of the summands $L_{\mathbf{H}}(k_{\mathfrak{p}(i)})$ are isomorphic. It follows that if $L(P) \neq 0$ then $L(P)$ is the sum of all the $L_{\mathbf{H}}(k_{\mathfrak{p}(i)})$, that is, $L(P) = L(\mathbb{Q}_p)$.

If $L(P) = 0$ then P is finite, which is clearly not the case. Therefore $L(P) = L(\mathbb{Q}_p)$, which implies that P is open in $\mathbf{G}(\mathbb{Z}_p)$ as claimed. ■

Lemma 16.4.5 *For almost all primes p, the Frattini subgroup of $\mathbf{G}(\mathbb{Z}_p)$ is*

$$N_p = \ker(\pi_p : \mathbf{G}(\mathbb{Z}_p) \to \mathbf{G}(\mathbb{F}_p)).$$

Proof. (sketch) For large enough primes p, the residue map π_p maps $\mathbf{G}(\mathbb{Z}_p)$ onto $\mathbf{G}(\mathbb{F}_p)$. Let G_i denote the kernel of the map $\mathbf{G}(\mathbb{Z}_p) \to \mathbf{G}(\mathbb{Z}_p/p^i\mathbb{Z}_p)$, so $N_p = G_1$. When $m \geq 1$, the mapping

$$1 + p^m x \mapsto x (\mathrm{mod}\, p)$$

induces an injective group homomorphism $\theta_m : G_m/G_{m+1} \to \mathrm{M}_n(\mathbb{F}_p)$; and the mapping

$$g \mapsto g^p$$

induces a homomorphism $P_m : G_m/G_{m+1} \to G_{m+1}/G_{m+2}$. It is easy to verify that the triangle

$$\begin{array}{ccc} G_m/G_{m+1} & \xrightarrow{P_m} & G_{m+1}/G_{m+2} \\ & {\scriptstyle\theta_m}\searrow \quad \swarrow{\scriptstyle\theta_{m+1}} & \\ & \mathrm{M}_n(\mathbb{F}_p) & \end{array}$$

commutes. Now $\mathbf{G}$ is defined as an algebraic subgroup of GL_n by polynomial equations in the matrix entries, and the Lie algebra L of $\mathbf{G}$ is defined as a subspace of M_n by the linear parts of these equations (taking the identity matrix as origin of co-ordinates). When p is large, we may reduce these equations

modulo p, and find that $L(\mathbb{F}_p)$ is exactly the image of θ_m; this holds for each $m \geq 1$. It follows in particular that θ_m and θ_{m+1} have the same image, and hence that P_m is an isomorphism.

This implies that $G_{m+1} = G_m^p G_{m+2}$ for each $m \geq 1$, and hence that for any k we have

$$G_2 = G_1^p G_k.$$

Since the G_k form a base for the neighbourhoods of 1 in the pro-p group G_1, and G_1/G_2 is abelian, this shows that G_2 is the closure of $G_1^p[G_1, G_1]$ in G_1, which is exactly the Frattini subgroup of G_1.

The lemma will follow, therefore, once we show that G_1/G_2 is the Frattini subgroup of G_0/G_2 where $G_0 = \mathbf{G}(\mathbb{Z}_p)$. Now if p is large enough, it follows from the structure theory that $L(\mathbb{F}_p)$ is spanned by elements of the form $\log x$ where x is an element of order p in $G(\mathbb{F}_p)$ (see [Nori 1987]; here, log is defined by the formula (16.3) in the following section). Using the identity

$$p^{-1}\binom{p}{j} \equiv \frac{(-1)^{j-1}}{j} \pmod{p} \qquad (1 \leq j \leq p-1),$$

we can see that if $x \in G_0$ satisfies $x^p \in G_1$, then

$$\theta_1(x^p G_2) = \log \overline{x}$$

where $\overline{x} = \pi_p(x) \in \mathbf{G}(\mathbb{F}_p)$. It follows from the preceding paragraph that G_1/G_2 is generated by elements of the form $x^p G_2$ with $x \in G_0$. If M/G_2 is a maximal subgroup of G_0/G_2 and M does not contain G_1, then $G_1 M = G_0$; but if $x \in G_0$ satisfies $x^p \in G_1$ and $x \equiv y \pmod{G_1}$ with $y \in M$, then $x^p \equiv y^p \pmod{G_2}$ lies in M, and so G_1 is contained in M, a contradiction. Thus every maximal subgroup of G_0/G_2 contains G_1/G_2, and the lemma follows. ■

Along the way we have shown that for each $m \geq 1$, the closure of G_m^p in the p-adic topology (which is the same as the pro-p topology of G_1) is equal to G_{m+1}; as G_m/G_{m+1} is an elementary abelian p-group of rank $\dim(\mathbf{G})$, we have

Corollary 16.4.6 *For almost all p, the group N_p is a uniform pro-p group of dimension equal to $\dim(\mathbf{G})$, and the lower central p-series of N_p is given by*

$$P_i(N_p) = \ker\left(\mathbf{G}(\mathbb{Z}_p) \to \mathbf{G}(\mathbb{Z}_p/p^i\mathbb{Z}_p)\right).$$

($\looparrowright$ **Pro-p groups**. Recall that in a uniform pro-p group N of dimension d, $P_{i+1}(N)$ is equal to the Frattini subgroup of $P_i(N)$ and $|P_{i+1}(N) : P_i(N)| = p^d$ for each $i \geq 1$.)

The main step in the proof is the following proposition; here we write

$$\sigma_i : \mathbf{G}(\mathbb{F}_p) \to \mathbf{H}(\mathcal{O}/\mathfrak{p}(i)) \quad \text{and}$$
$$\sigma_i : L(\mathbb{F}_p) \to L_{\mathbf{H}}(\mathcal{O}/\mathfrak{p}(i))$$

for the projection maps in (16.1) and (16.2).

Proposition 16.4.7 *For all sufficiently large primes p the following holds. If X is a subgroup of $\mathbf{G}(\mathbb{F}_p)$ such that*
(a) *for $i = 1, \ldots, f(p)$ the order of $\sigma_i(X)$ is divisible by p, and*
(b) *every X-invariant Lie subalgebra of $L(\mathbb{F}_p)$ is an ideal,*
then $X = \mathbf{G}(\mathbb{F}_p)$.

We discuss the proof of Proposition 16.4.7 in the following section. Assuming this result for now, we may deduce

Lemma 16.4.8 *For almost all primes p, Λ is dense in $\mathbf{G}(\mathbb{Z}_p)$.*

Proof. We claim that for almost all primes p, the group $X = \pi_p(\Lambda)$ satisfies the hypotheses of Proposition 16.4.7. Suppose that hypothesis (a) is false for infinitely many primes. Then there is an infinite set $\mathcal{Q}$ of primes of $\mathcal{O}$ such that for each $\mathfrak{p} \in \mathcal{Q}$,

$$\pi_{\mathfrak{p}}(\Lambda) = \sigma_i \pi_p(\Lambda) \leq \mathrm{GL}_n(\mathbb{F}_p)$$

is a group of order coprime to p (where $\mathfrak{p}$ is the ith prime divisor of the rational prime p). By Jordan's theorem (↬ **Linear groups**) there exists m, depending only on n, such that each such $\pi_{\mathfrak{p}}(\Lambda)$ has an abelian normal subgroup of index dividing m. It follows that

$$\begin{aligned}[\Lambda^m, \Lambda^m] &\subseteq \bigcap_{\mathfrak{p} \in \mathcal{Q}} \ker \pi_{\mathfrak{p}} \\ &= 1\end{aligned}$$

since $\mathcal{Q}$ is infinite (here we are identifying $\mathbf{G}(\mathbb{Z}_S)$ with $\mathbf{H}(\mathcal{O}_{\widetilde{S}})$ where $\widetilde{S}$ denotes the set of prime divisors in $\mathcal{O}$ of primes in S). Since Λ is Zariski-dense in $\mathbf{G}$ this implies that $[\mathbf{G}^m, \mathbf{G}^m] = 1$, which is false since $\mathbf{G}$ is a $\mathbb{Q}$-simple algebraic group. This contradiction shows that condition (a) in Proposition 16.4.7 must hold for almost all primes.

Since $L_{\mathbf{H}}(k)$ is absolutely irreducible for $\mathbf{H}(k)$ and Λ is Zariski-dense in $\mathbf{H}(k)$, it is also absolutely irreducible for Λ. Therefore $\mathrm{Ad}(\Lambda)$ spans $\mathrm{End}_k(L_{\mathbf{H}}(k))$; it follows that for almost all primes $\mathfrak{p}$ of $\mathcal{O}$, $\mathrm{Ad}\pi_{\mathfrak{p}}(\Lambda)$ spans $\mathrm{End}_{\mathcal{O}/\mathfrak{p}}(L_{\mathbf{H}}(\mathcal{O}/\mathfrak{p}))$ and hence that the $\mathcal{O}/\mathfrak{p}$-module $L_{\mathbf{H}}(\mathcal{O}/\mathfrak{p})$ is irreducible for $\pi_{\mathfrak{p}}(\Lambda)$. Thus for almost all primes p, the decomposition (16.2) expresses $L(\mathbb{F}_p)$ as a direct sum of simple $\pi_p(\Lambda)$-modules. As each summand is an ideal of $L(\mathbb{F}_p)$ this shows that (b) holds for each such p.

To complete the proof of the lemma, let $\overline{\Lambda}$ denote the closure of Λ in $\mathbf{G}(\mathbb{Z}_p)$. Proposition 16.4.7 shows that

$$\pi_p(\overline{\Lambda}) = \pi_p(\Lambda) = \mathbf{G}(\mathbb{F}_p) = \pi_p \mathbf{G}(\mathbb{Z}_p)$$

for almost all primes p. For each such p we then have

$$\mathbf{G}(\mathbb{Z}_p) = N_p \overline{\Lambda},$$

and it follows by Lemma 16.4.5 that $\overline{\Lambda} = \mathbf{G}(\mathbb{Z}_p)$. ■

It is now easy to complete the

Proof of Theorem 2 Let Y be the closure of Λ in $\mathbf{G}(\widehat{\mathbb{Z}_S}) = \prod_{p\notin S}\mathbf{G}(\mathbb{Z}_p)$, and let Y_p denote the closure of Λ in $\mathbf{G}(\mathbb{Z}_p)$. Thus Y_p is the projection of Y into $\mathbf{G}(\mathbb{Z}_p)$. Lemmas 16.4.8 and 16.4.4 imply that $\prod_{p\notin S} Y_p$ is open in $\mathbf{G}(\widehat{\mathbb{Z}_S})$, so it suffices to show that Y is open in the product $\prod_{p\notin S} Y_p$. Now if P is a product of pro-p groups for distinct primes p, then a closed subgroup of P that projects onto each factor must be the whole of P (because the same is true for products of finite p-groups). It follows that Y certainly contains the product

$$\prod_{p\notin S}(Y_p\cap N_p) = \prod_{p\notin T} N_p \times \prod_{p\in T\setminus S}(Y_p\cap N_p)$$

for some finite set of primes $T\supseteq S$, and we may choose T so that for each $p\notin T$, (i) $Y_p = \mathbf{G}(\mathbb{Z}_p)$ and (ii) $Y_p/N_p \cong \mathbf{G}(\mathbb{F}_p)$ is a finite semisimple group. Then $\prod_{p\notin T} Y_p/N_p$ is a product of pairwise non-isomorphic finite semisimple groups; as Y projects onto each factor in this product it follows that Y projects onto $\prod_{p\notin T} Y_p$. On the other hand, $\prod_{p\in T\setminus S}(Y_p\cap N_p)$ has finite index in $\prod_{p\in T\setminus S} Y_p$. Together these imply that Y is open in $\prod_{p\notin S} Y_p$ as required.

We conclude this section with the following somewhat surprising application of the preceding arguments:

Theorem 16.4.9 *Let $\mathbf{G}$ be a connected, simply-connected simple algebraic group defined over $\mathbb{Q}$. Then there exists a finite set of primes S with the following property: if A is a subset of $\mathbf{G}(\mathbb{Z}_S)$ such that for one prime p not in S the image of A in $\mathbf{G}(\mathbb{F}_p)$ generates $\mathbf{G}(\mathbb{F}_p)$, then the image of A in $\mathbf{G}(\mathbb{F}_q)$ generates $\mathbf{G}(\mathbb{F}_q)$ for almost all primes q.*

Proof. Let S be the set of 'bad' primes for Lemma 16.4.5, let Λ be the subgroup generated by $A\subseteq\mathbf{G}(\mathbb{Z}_S)$, and suppose that $\pi_p(\Lambda) = \mathbf{G}(\mathbb{F}_p)$ for some $p\notin S$. Since $\ker\pi_p$ is the Frattini subgroup of $\mathbf{G}(\mathbb{Z}_p)$ it follows that Λ is dense in $\mathbf{G}(\mathbb{Z}_p)$, in the congruence (p-adic) topology. As the congruence topology is finer than the Zariski topology this implies that Λ is Zariski-dense in $\mathbf{G}(\mathbb{Z}_p)$, and hence also in $\mathbf{G}$. Lemma 16.4.8 now shows that Λ is (q-adically) dense in $\mathbf{G}(\mathbb{Z}_q)$ for almost all primes q. For each such q we then have $\pi_q(\Lambda) = \pi_q\mathbf{G}(\mathbb{Z}_q)$, and the result follows since $\pi_q\mathbf{G}(\mathbb{Z}_q) = \mathbf{G}(\mathbb{F}_q)$ for almost all q. ■

2 Subgroups of $\mathrm{SL}_n(\mathbb{F}_p)$.

All the main results depend on Proposition 16.4.7, stated in the preceding section. We shall not attempt to prove this in full; unfortunately, moreover, it does not appear explicitly in the literature, but only in the unpublished manuscript [Nori (a)]. However, different versions of this important result have been proved in [Nori 1987], [Mathews, Vaserstein & Weisfeiler 1984], [Weisfeiler 1984] and [Hrushovskii & Pillay 1995], and we would like to illustrate three quite different

ways of approaching the proof. To this end, we shall concentrate on the special case where G is the algebraic group SL_n; all the key ideas appear already in this case.

Since SL_n is absolutely simple, the statement reduces to

Theorem 16.4.10 *Fix $n \geq 2$. For all sufficiently large primes p the following holds. If X is a subgroup of $\mathrm{SL}_n(\mathbb{F}_p)$ such that*
(a) *the order of X is divisible by p, and*
(b) $\mathfrak{sl}_n(\mathbb{F}_p)$ *is irreducible as an X-module under conjugation in the matrix ring, then $X = \mathrm{SL}_n(\mathbb{F}_p)$.*

First proof (in the spirit of) [Matthews, Vaserstein & Weisfeiler 1984], [Weisfeiler 1984]: *using the classification of finite simple groups.*

If $X < \mathrm{SL}_n(\mathbb{F}_p) = \mathrm{SL}(V)$, then X is contained in some maximal subgroup L of $\mathrm{SL}(V)$. The maximal subgroups of (most) finite simple groups have been classified (and CFSG is needed, even when one comes to classify the maximal subgroups of a known family of groups such as $\mathrm{SL}_n(\mathbb{F}_p)$). According to a fundamental result of [Aschbacher 1984], every such maximal subgroup L is one of the following nine cases:

C_1**:** The stabilizer of a subspace of V, or of a pair of subspaces V_1, V_2 such that $\dim V_1 + \dim V_2 = n$ and either $V_1 \subseteq V_2$ or $V = V_1 \oplus V_2$.

C_2**:** The stabilizer of a direct sum decomposition $V = \oplus V_i$ for V_i of the same dimension.

C_3**:** The stabilizer of a field extension of $\mathbb{F}_p$ whose degree is a prime dividing n.

C_4**:** The stabilizer of a tensor product decomposition $V = V_1 \otimes V_2$.

C_5**:** The centralizer of a field automorphism.

C_6**:** The normalizer of a symplectic-type r-group for a prime $r \neq p$ (in an irreducible representation).

C_7**:** The stabilizer of a tensor product decomposition $V = \bigotimes V_i$ for V_i of the same dimension.

C_8**:** A classical subgroup embedded as usual.

C_9**:** $L = \mathrm{N}_G(S)$, where S is a nonabelian simple subgroup of $\mathrm{PSL}(V)$ such that $S \leq L \leq \mathrm{Aut}(S)$, and the universal cover $\widetilde{S}$ of S acts absolutely irreducibly on V. (Here $\widetilde{S}$ is the largest perfect group which, modulo its center, is isomorphic to S.)

Now, one can see that in the first eight cases, the maximal subgroup L is inside a proper connected algebraic subgroup of SL_n and therefore has an invariant subspace in the Lie algebra $\mathfrak{sl}_n$ of SL_n, thus its action on $\mathfrak{sl}_n$ is not irreducible and so L cannot contain X. The more difficult case to handle is (as usual) C_9. In this case L is the normalizer of a finite simple group S. If S is an alternating group then the order of S is bounded by some number depending only on n, because $\mathrm{Alt}(k)$ is not a section of $\mathrm{SL}_n(F)$ for any field F if $k > (3n+6)/2$ ($\leadsto$ **Finite simple groups**). Since $X \leq L \leq \mathrm{Aut}(S)$, the order of X is bounded if S is an alternating or sporadic group, and hence that $p \nmid |X|$ provided p is large enough.

We may therefore suppose that S is of Lie type, say $S = Y(\mathbb{F}_{r^e})$ where r is a prime. Suppose first that $r \neq p$. Both e and the Lie rank of Y are bounded in terms of n ($\leadsto$ **Finite simple groups**). Now S contains a non-trivial split torus T (Lang's theorem, $\leadsto$ **Linear groups**), and T normalises a non-trivial unipotent r-subgroup R. If r is large (relative to the Lie rank of Y) then R is elementary abelian, and $\left|\mathrm{N}_{\mathrm{SL}_n(\mathbb{F}_p)}(R) : R\right| \leq n!$ (exercise!); consequently $|T| \leq n!$. Since $|T| \geq r-1$ it follows that r is bounded in terms of n. We conclude that $|S| = |Y(\mathbb{F}_{r^e})|$ is bounded by a number depending only on n, and as above we deduce that $p \nmid |X|$ if p is large.

In the remaining case, $S = Y(\mathbb{F}_{p^e})$ is a simple group of the "right" characteristic. By Steinberg's theory (see [St]), the representation of S in $\mathrm{SL}(V)$ is a tensor product of representations obtained by applying the Frobenius automorphism of $\mathbb{F}_{p^e}$ (maybe several times) and then an algebraic representation of Y. It follows that S is contained in a proper connected algebraic subgroup of SL; therefore so is its normalizer and hence X cannot act irreducibly on $\mathfrak{sl}_n(\mathbb{F}_p)$. This completes the proof (the original proofs given by Weisfeiler, Matthews *et al.*, predating Aschbacher's theorem, used some more direct consequences of CFSG).

Second proof [Nori 1987]: *using algebraic geometry over finite fields*

For a subgroup X of $\mathrm{SL}_n(\mathbb{F}_p)$ we denote by X^+ the subgroup of X generated by the elements of order p. Note that if $p > n$, then every element of p-power order in $\mathrm{SL}_n(\mathbb{F}_p)$ actually has order p, so in this case $X^+ = O^{p'}(X)$ contains the Sylow p-subgroups of X.

For each element x in X of order p, let

$$U_x = \{\exp(t \log x) \mid t \in \widetilde{\mathbb{F}_p}\} \leq \mathrm{SL}_n(\widetilde{\mathbb{F}_p}),$$

where $\widetilde{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$; here

$$\log x = -\sum_{i=1}^{p-1} \frac{(1-x)^i}{i}, \tag{16.3}$$

$$\exp z = \sum_{i=0}^{p-1} \frac{z^i}{i!} \tag{16.4}$$

for matrices x and z in $M_n(\widetilde{\mathbb{F}_p})$ satisfying $x^p = 1,\ z^p = 0$, and U_x is an algebraic (one-parameter) subgroup of SL_n.

Let $\widetilde{X}$ be the (connected) algebraic subgroup of SL_n generated by $\{U_x \mid x \in X,\ x^p = 1\}$. Nori's key result states that *if p is large enough with respect to n, then $X^+ = \widetilde{X}(\mathbb{F}_p)^+$*. Now, it follows from the structure theory that (if p is large enough then) $\widetilde{X}(\mathbb{F}_p) = \widetilde{X}(\mathbb{F}_p)^+$; thus in fact $X^+ = \widetilde{X}(\mathbb{F}_p)$. In other words, *$X^+$ can be realized as the group of $\mathbb{F}_p$-rational points of the connected algebraic group $\widetilde{X}$*. This result now implies Theorem 16.4.10. Indeed, since X normalises $\widetilde{X}$ it preserves the Lie algebra $L_{\widetilde{X}}$ of $\widetilde{X}$; it follows that $L_{\widetilde{X}}(\mathbb{F}_p) = \mathfrak{sl}_n(\mathbb{F}_p)$ and hence that $\widetilde{X} = \mathrm{SL}_n$. Thus $X \geq X^+ = \mathrm{SL}_n(\mathbb{F}_p)$

Nori's proof rests on a detailed analysis of the relation between groups and their Lie algebras in the characteristic p case. He establishes a one to one correspondence between nilpotently-generated Lie subalgebras of $M_n(\mathbb{F}_p)$ and unipotently-generated subgroups of $\mathrm{SL}_n(\mathbb{F}_p)$, provided $p >> n$.

Third proof [Hrushovskii & Pillay 1995]: *using model theory.*

A field F is said to be *pseudo algebraically closed* (PAC, for short) if every irreducible variety defined over F contains an F-rational point. By Hilbert's Nullstellensatz, algebraically closed fields are PAC, but there are many others (see [FJ]). Important examples of PAC fields are the *pseudo-finite fields*. These are the fields E whose elementary theory is equal to the theory of almost all finite fields: this means that a first-order sentence is true in E if and only if it is true in almost every finite field. If one takes an infinite set of primes $\{p_i\}_{i\in I}$ then a non-principal ultraproduct of $\{\mathbb{F}_{p_i}\}_{i\in I}$ provides an example of such a field. Such an E is indeed PAC: If V is an irreducible variety defined over E, then it gives rise to such varieties V_F over almost every finite field F. It follows from the Lang-Weil estimates on the number of points in varieties over finite fields that $V_F(F) \neq \emptyset$ for sufficiently large F, and by elementary equivalence we see that $V(E) \neq \emptyset$.

Hrushowski and Pillay studied "definable" subgroups and subsets of $\mathrm{GL}_n(F)$, i.e. subsets which can be defined by first-order statements. They have developed a theory of such subsets which parallels the theory of Zariski-closed subsets. One of their fundamental results is as follows [Hrushovskii & Pillay 1994], Prop. 2.1: *let X be the subgroup of $\mathrm{GL}_n(F)$ generated by a family of Zariski-irreducible definable subsets. Then* (i) *H is definable* and (ii) *H has finite index in its Zariski closure in* $\mathrm{GL}_n(F)$. Let us see now how this may be applied to the proof of Theorem 16.4.10. Suppose that the Theorem does not hold. Then there is an infinite sequence of primes $\{p_i\}_{i\in I}$ and proper subgroups $H_i \leq \mathrm{SL}_n(\mathbb{F}_{p_i})$ such that each H_i acts irreducibly on $\mathfrak{sl}_n(\mathbb{F}_{p_i})$ and has order divisible by p_i. Let's take a (nonprincipal) ultraproduct of these structures. Then F, the ultraproduct of the $\mathbb{F}_{p_i}$, is a pseudo-finite field, and the corresponding ultraproduct of the $\{H_i\}_{i\in I}$ is a subgroup H of $\mathrm{SL}_n(F)$. We first show that H is Zariski-dense in $\mathrm{SL}_n(F)$. Otherwise, its Zariski closure $\overline{H}$, an algebraic group over F, would have an invariant proper Lie subalgebra in $\mathfrak{sl}_n(F)$. By the elementary equivalence,

this would imply that H_i has an invariant proper Lie subalgebra in $\mathfrak{sl}_n(\mathbb{F}_{p_i})$ for almost all $i \in I$, contrary to hypothesis. A similar argument implies that H contains a unipotent element: if not, then H_i has order coprime to p_i for almost all $i \in I$, again contradicting the hypothesis.

Suppose y is a unipotent element of H. Then the set $U_y = \{\exp(t \log y) \mid t \in F\}$ is a subgroup of H. Indeed, for any $p_i > n$, any unipotent element x of $\mathrm{GL}_n(\mathbb{F}_{p_i})$ has order p_i, and

$$\{\exp(t \log x) \mid t \in \mathbb{F}_{p_i}\} = \left\{x^j \mid 0 \leq j \leq p-1\right\}$$

is exactly the subgroup generated by x inside H_i. If y is the image of (x_i) in the ultraproduct H it follows that U_y is a subgroup of H (here, log and exp are defined componentwise, by the formulae (16.3) and (16.4) above).

Now for each unipotent element $y \in H$, U_y is a definable Zariski-irreducible subgroup of $\mathrm{SL}_n(F)$. Let H_0 be the subgroup of H generated by all such U_y. The theorem stated above shows that H_0 has finite index in its Zariski closure $\overline{H_0}$. As H_0 is normalized by H which is Zariski-dense in $\mathrm{SL}_n(F)$, it follows that $\overline{H_0}$ is normal in $\mathrm{SL}_n(F)$. Therefore $\overline{H_0}$, and its finite-index subgroup H_0, are both equal to $\mathrm{SL}_n(F)$. This now implies that $H_i = \mathrm{SL}_n(\mathbb{F}_{p_i})$ for almost all i, the final contradiction that completes the proof.

We end this section by mentioning that in recent years, various strong results on subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$ have been obtained. Most notable is the work of Larsen and Pink who established the following general structure theorem, which can be used as an 'elementary' alternative to CFSG in certain arguments:

Theorem 16.4.11 [Larsen & Pink] *Let H be a finite subgroup of $\mathrm{GL}_n(F)$, where F is a field of characteristic $p > 0$. Then G has normal subgroups $G_3 < G_2 < G_1$ such that*
1) $|G/G_1|$ is bounded as a function of n;
2) G_1/G_2 is a direct product of at most $\frac{n}{2}$ simple groups of Lie type defined over fields of characteristic p;
3) G_2/G_3 is abelian of order prime to p, and
4) G_3 is a finite p-group.

3 The 'Lubotzky alternative'

On the face of it, the strong approximation theorem is only about subgroups of S-arithmetic groups, but in fact it has profound applications to finitely generated linear groups. Most of these are derived via the following theorem, which Mann has kindly dubbed "Lubotzky's Alternative", in analogy with the well-known "Tits Alternative".

The Tits alternative asserts that a finitely generated linear group Γ either is virtually solvable or else contains a non-abelian free group. It means that either Γ is small ("virtually solvable") or else Γ contains a large ("free") subgroup. One of its main applications is the dichotomy: linear groups are either of polynomial

word growth or of exponential word growth. The Lubotzky alternative asserts that either Γ is small (virtually solvable) or else Γ has large finite quotients ("$\mathbf{G}(\mathbb{F}_p)$ for almost all primes p"). Its main application is the dichotomy: linear groups of polynomial subgroup growth are virtually soluble, and if the subgroup growth is not polynomial then it grows at least as fast as $n^{\log n}$ (see Chapters 5 and 8). It appeared in this role in [Lubotzky and Mann 1991].

Theorem 16.4.12 *Let G be a finitely generated linear group over a field of characteristic zero. Then one of the following holds:*
(a) G is virtually soluble,
(b) there exist a connected, simply connected simple algebraic group $\mathfrak{S}$ over $\mathbb{Q}$, a finite set of primes S such that $\mathfrak{S}(\mathbb{Z}_S)$ is infinite, and a subgroup G_1 of finite index in G such that the profinite group $\mathfrak{S}(\widehat{\mathbb{Z}_S})$ is an image of $\widehat{G}_1$.

In finitary terms, the meaning of (b) is that *every congruence quotient of $\mathfrak{S}(\mathbb{Z}_S)$ appears as a quotient of G_1* (this is equivalent to (b) by the Strong Approximation Theorem). It may also be important to know something more about the simple algebraic group $\mathfrak{S}$ (for example, in Chapter 8 when we try to count *normal* subgroups of finite index in a linear group). We return to this question below, after discussing the proof of Theorem 16.4.12.

The theorem is proved in a sequence of reductions. For the first, we recall that a *specialisation* of a group $G \leq \mathrm{GL}_n(F)$ into $\mathrm{GL}_n(k)$, where k is a field, means the homomorphism $\phi^* : G \to \mathrm{GL}_n(k)$ induced by some ring homomorphism ϕ from R into k where R is a subring of F that contains the entries of all matrices in G.

Proposition 16.4.13 *Let G be finitely generated subgroup of $\mathrm{GL}_n(F)$, where F is a field of characteristic zero. If G is not virtually soluble then there exist an algebraic number field k and a specialisation ϕ^* of G into $\mathrm{GL}_n(k)$ such that $\phi^*(G)$ is not virtually soluble.*

Proof. Let f and m be positive integers, provided by the Platonov-Zassenhaus theorem, such that every virtually soluble linear group of degree n over a field of characteristic zero is (soluble of derived length $\leq f$) by (finite of order $\leq m$) (↬ **Linear groups**). Since G is finitely generated, its subgroups of index at most m intersect in a normal subgroup G_1 of finite index in G. Let K be the fth term of the derived series of G_1; since G is not virtually soluble we know that $K \neq 1$. Choose an element $g \neq 1$ of K, an entry $g_{ij} \neq \delta_{ij}$ of the matrix g, and put $z = g_{ij} - \delta_{ij}$.

Now let R be a finitely generated $\mathbb{Q}$-subalgebra of F such that $G \leq \mathrm{GL}_n(R)$. Since the maximal ideals of R intersect in 0 ([E], Theorem 4.19), there exist a field k and a $\mathbb{Q}$-algebra epimorphism $\phi : R \to k$ such that $\phi(z) \neq 0$. The group homomorphism $\phi^* : G \to \mathrm{GL}_n(k)$ induced by ϕ then satisfies $\phi^*(z) \neq 1$, so we have $\phi^*(K) \neq 1$. From the definition of K it now follows that $\phi^*(G)$ is not virtually soluble.

Since the field k is finitely generated as a $\mathbb{Q}$-algebra, the 'Weak Nullstellensatz' ([E], Theorem 4.19 or [AM], Prop. 7.9) shows that is a finite extension of $\mathbb{Q}$, that is, an algebraic number field. ∎

Thus to prove Theorem 16.4.12, we may replace the original group G by its image under a suitable specialisation, and so assume that $G \leq \mathrm{GL}_n(k)$ where $(k:\mathbb{Q}) = d$ is finite. Since $\mathrm{GL}_n(k) \leq \mathrm{GL}_{dn}(\mathbb{Q})$, we may further replace n by dn and F by $\mathbb{Q}$.

Changing notation, we henceforth assume that $G \leq \mathrm{GL}_n(\mathbb{Q})$.

Second reduction Let G^0 be the connected component of 1 in the Zariski topology of G (induced from the Zariski topology on $\mathrm{GL}_n(\mathbb{Q})$). Then $G^0 \lhd_{\mathrm{f}} G$, so replacing G by G^0 we may assume that in fact G *is Zariski-connected*. Now let $\mathfrak{G}$ be the Zariski-closure of G in $\mathrm{GL}_n(\mathbb{C})$. Thus $\mathfrak{G}$ is a connected linear algebraic group defined over $\mathbb{Q}$. Also $\mathfrak{G}$ is not soluble; hence there exist a connected $\mathbb{Q}$-simple algebraic group $\mathfrak{S}$ defined over $\mathbb{Q}$ and a $\mathbb{Q}$-rational epimorphism $\rho : \mathfrak{G} \to \mathfrak{S}$. Since G is Zariski-dense in $\mathfrak{G}$ it follows that $\rho(G)$ is Zariski-dense in $\mathfrak{S}$; and we have $\rho(G) \leq \mathfrak{S}(\mathbb{Q})$.

Replacing G by its image $\rho(G)$, we may therefore assume that G *is Zariski-dense in the connected* $\mathbb{Q}$*-simple algebraic group* $\mathfrak{S}$.

Third reduction Let $\pi : \widetilde{\mathfrak{S}} \to \mathfrak{S}$ be the universal cover of $\mathfrak{S}$. Thus $\widetilde{\mathfrak{S}}$ is a simple simply connected algebraic group over $\mathbb{Q}$ and π is a $\mathbb{Q}$-rational morphism. Moreover, $\ker\pi$ *is finite* and

$$\mathfrak{S}(\mathbb{Q})/\pi(\widetilde{\mathfrak{S}}(\mathbb{Q})) = E, \text{ say}$$

is an abelian group of finite exponent. Indeed, $\ker\pi$ is the (finite) centre $\mathcal{Z}$ of $\widetilde{\mathfrak{S}}$ and E embeds into $H^1(\mathbb{Q}, \mathcal{Z})$ by the exact sequence of Galois cohomology (see [PR], §2.2); we recall the simple proof in Lemma 16.4.14 below. Let us continue now with our reduction, and put

$$H = \widetilde{\mathfrak{S}}(\mathbb{Q}) \cap \pi^{-1}(G).$$

Then

$$G/\pi(H) = G/(G \cap \pi(\widetilde{\mathfrak{S}}(\mathbb{Q})) \hookrightarrow E,$$

so $G/\pi(H)$ is finite because G is finitely generated. Hence $\pi(H)$ is finitely generated also, and as $\ker\pi$ is finite it follows that H is finitely generated. Therefore $H \leq \widetilde{\mathfrak{S}}(\mathbb{Z}_S)$ for some finite set of primes S. Since $\widetilde{\mathfrak{S}}(\mathbb{Z}_S) \leq \mathrm{GL}_m(\mathbb{Z}_S)$ for some m this implies in particular that H is residually finite; hence there exists $H_1 \lhd_{\mathrm{f}} H$ with $H_1 \cap \ker\pi = 1$. We now have

$$H_1 \cong \pi(H_1) \leq_{\mathrm{f}} G.$$

We claim that H_1 is Zariski dense in $\widetilde{\mathfrak{S}}$. Indeed, writing $\mathfrak{H}$ for the Zariski-closure of H_1 in $\widetilde{\mathfrak{S}}$, we have $\pi(H_1) \leq \pi(\mathfrak{H}) \leq \mathfrak{S}$; but $\pi(\mathfrak{H})$ is Zariski-closed in $\mathfrak{S}$, while the Zariski-closure of $\pi(H_1)$ has finite index in the Zariski-closure of G which is $\mathfrak{S}$. As $\mathfrak{S}$ is connected it follows that $\pi(\mathfrak{H}) = \mathfrak{S}$. Therefore $\widetilde{\mathfrak{S}} = \mathfrak{H}\cdot\ker\pi$. Since $\ker\pi$ is finite and $\widetilde{\mathfrak{S}}$ is connected this implies that $\widetilde{\mathfrak{S}} = \mathfrak{H}$ as claimed.

Replacing G by H_1, we may now therefore assume that *the simple algebraic group $\mathfrak{S}$ is simply connected, and that $G \leq \mathfrak{S}(\mathbb{Z}_S)$ for some finite set of primes S.*

Conclusion Now Theorem 16.4.2 shows that the closure $\overline{G}$ of G in the profinite group

$$\mathfrak{S}(\widehat{\mathbb{Z}_S}) = \prod_{p \notin S} \mathfrak{S}(\mathbb{Z}_p)$$

is an open subgroup of $\mathfrak{S}(\widehat{\mathbb{Z}_S})$. This implies that $\overline{G}$ contains a subgroup of the form

$$\prod_{p \notin S_1} \mathfrak{S}(\mathbb{Z}_p) \times \prod_{p \in S_1 \setminus S} \{1\}$$

where $S_1 \supseteq S$ is still some finite set of primes, and hence that G is in fact dense in $\mathfrak{S}(\widehat{\mathbb{Z}_{S_1}}) = \prod_{p \notin S_1} \mathfrak{S}(\mathbb{Z}_p)$. Replacing S by S_1 we may as well suppose that G is dense in $\mathfrak{S}(\widehat{\mathbb{Z}_S})$.

In that case, $\mathfrak{S}(\widehat{\mathbb{Z}_S})$ is the completion of G relative to the congruence topology, which is coarser than the profinite topology; so $\mathfrak{S}(\widehat{\mathbb{Z}_S})$ is a homomorphic image of $\widehat{G}$ and the proof is complete.

It remains to prove

Lemma 16.4.14 *Let $\mathfrak{S}$ be a semisimple algebraic group defined over $\mathbb{Q}$, and $\pi : \widetilde{\mathfrak{S}} \to \mathfrak{S}$ its universal covering. Then*

$$\frac{\mathfrak{S}(\mathbb{Q})}{\pi(\widetilde{\mathfrak{S}}(\mathbb{Q}))}$$

is an abelian group with finite exponent dividing the order of the center of $\widetilde{\mathfrak{S}}$.

Example. A typical example is $\mathfrak{S} = \mathrm{PGL}_2$, $\widetilde{\mathfrak{S}} = \mathrm{SL}_2$ and

$$\frac{\mathfrak{S}(\mathbb{Q})}{\pi(\widetilde{\mathfrak{S}}(\mathbb{Q}))} \cong \frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2} \cong \bigoplus_{i=1}^{\infty} \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

Proof. The map $\pi : \widetilde{\mathfrak{S}} \to \mathfrak{S}$ is surjective with a finite central kernel Z of order m, say. Let $L = \pi^{-1}(\mathfrak{S}(\mathbb{Q}))$ and $M = \widetilde{\mathfrak{S}}(\mathbb{Q})$. The Galois group $\mathcal{G} = \mathrm{Gal}(\widetilde{\mathbb{Q}}/\mathbb{Q})$ acts on L and M is precisely the set of fixed points. Moreover, for every $x \in L$ and $\sigma \in \mathcal{G}$ we have $x^{-1}\sigma(x) \in Z$. This implies that $\sigma[x, y] = [x, y]$ for every $\sigma \in \mathcal{G}$ and $x, y \in L$. It follows that $[x, y] \in M$ for all $x, y \in L$. Now let $x \in L$. Then $\sigma(x) = xz$ for some $z = z(\sigma, x)$ in Z, and then $\sigma(x^m) = x^m z^m = x^m$. This shows that x^m is in M. Thus

$$M \geq [L, L]L^m$$

and the lemma follows since $\mathfrak{S}(\mathbb{Q})/\pi(\widetilde{\mathfrak{S}}(\mathbb{Q}))$ is a quotient of L/M. ∎

We promised to say more about the simple group $\mathfrak{S}$. Looking back at the above proof of Theorem 16.4.12, we see that $\mathfrak{S}$ appears as (a covering group of) one of the simple components of $\mathfrak{G}^0$ where $\mathfrak{G}$ is the Zariski closure of $\phi^*(G)$; and we are free to choose any one of these simple components. Is there any way to keep some control over the group $\mathfrak{G}$?

Proposition 16.4.15 *Let G be finitely generated subgroup of $\mathrm{GL}_n(F)$, where F is a field of characteristic zero. Let $\mathbf{G}$ be the Zariski closure of G in $\mathrm{GL}_n(\mathbb{C})$. Then there exist an algebraic number field k, a normal subgroup G_1 of finite index in G, and a specialisation ϕ^* of G_1 into $\mathrm{GL}_n(k)$ such that the Zariski closure of $\phi^*(G_1)$ is isomorphic to $\mathbf{G}^0$.*

Here $\mathbf{G}^0$ denotes the identity component of $\mathbf{G}$.

Using this, it is possible to strengthen the statement of Theorem 16.4.12: under the hypotheses of that theorem, *suppose that the Zariski closure of G has a simple composition factor* $\mathbf{T}$. Then $\mathbf{T}$ is a product of absolutely simple groups, each isomorphic over $\mathbb{C}$ to a simple algebraic group $\mathbf{S}$; and *the simple group $\mathfrak{S}$ in the conclusion of the theorem may be taken to be $\mathbb{C}$-isomorphic to a product of copies of* $\mathbf{S}$.

We omit the details of the proof, which needs some care over fields of definition, but sketch now the proof of Proposition 16.4.15. A slightly different formulation, valid in all characteristics, is proved in [Larsen & Lubotzky] and stated in the following section.

There is a finitely generated subring A of F such that (i) $G \leq \mathrm{GL}_n(A)$ and (ii) the algebraic group $\mathbf{G}$ is defined by equations with coefficients in A. There exists a prime p (in fact infinitely many) such that A can be embedded in $\mathbb{Z}_p$ ([Cassels 1986], Chapter 5); and $\mathbb{Z}_p$ may be embedded in $\mathbb{C}$. We may then suppose that

$$G \leq \mathrm{GL}_n(A) \leq \mathrm{GL}_n(\mathbb{Z}_p) \leq \mathrm{GL}_n(\mathbb{C}),$$

and the Zariski closure of G in $\mathrm{GL}_n(\mathbb{C})$ is still $\mathbf{G}$. Replacing G by a suitable subgroup of finite index, we may suppose that (i) $G \leq \mathrm{GL}_n^1(\mathbb{Z}_p)$, the principal congruence subgroup modulo p, and (ii) the algebraic group $\mathbf{G}$ is connected.

The idea now is to think of a specialisation of G_1 as a *deformation* of the given representation $G_1 \to \mathrm{GL}_n^1(\mathbb{Z}_p)$. Say $G = \langle g_1, \ldots, g_d \rangle$, and let M be the closure of G in the pro-p group $\mathrm{GL}_n^1(\mathbb{Z}_p)$. Then M is a finitely generated pro-p group, so its Frattini subgroup $\Phi(M)$ is open (↬ **Pro-p groups**). Since the algebraic numbers in $\mathbb{Z}_p$ are dense in $\mathbb{Z}_p$, there exist homomorphisms $\phi : A \to \mathbb{Z}_p$ arbitrarily close to the inclusion $A \hookrightarrow \mathbb{Z}_p$ such that $\phi(A)$ is contained in the algebraic closure of $\mathbb{Q}$ in $\mathbb{Z}_p$ (this is not obvious: it depends on the fact that if an equation $f(X) = 0$ over $\mathbb{Z}_p$ has a solution $\xi \in \mathbb{Z}_p$, then for every polynomial f_1 sufficiently close to f, the equation $f_1(X) = 0$ also has a solution in $\mathbb{Z}_p$, moreover one that is close to ξ). We may therefore find such a homomorphism ϕ for which $\phi^*(g_i) \equiv g_i \pmod{\Phi(M)}$ for $i = 1, \ldots, d$. Since $g_1, \ldots, g_d$ generate M topologically, so do $\phi^*(g_1), \ldots, \phi^*(g_d)$. Thus $\phi^*(G)$ is (topologically) dense in M. Now if H is any dense subgroup of M and $\mathbf{H}$ is the Zariski closure of H then $\mathbf{H}(\mathbb{Z}_p)$ is a closed subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ containing H, so $\mathbf{H}(\mathbb{Z}_p) \geq M \geq H$

and so $\mathbf{H}$ is the Zariski closure of M. Applying this to $H = G$ and to $H = \phi^*(G)$ we deduce that $\phi^*(G)$ has the same Zariski closure as G. This completes the proof; for k we take the finite extension field of $\mathbb{Q}$ generated by the finitely generated ring $\phi(A)$.

We conclude this section with a few applications.

Theorem 16.4.16 *Let Γ be a finitely generated linear group over a field of characteristic zero. If Γ is not virtually soluble then, for every prime p, the Sylow pro-p subgroups of the profinite completion $\widehat{\Gamma}$ of Γ are not finitely generated.*

Before proving this we deduce a couple of corollaries.

Corollary 16.4.17 *Let Γ be a finitely generated linear group over a field of characteristic zero. If Γ is infinite then Γ has a subgroup of index divisible by d for every integer $d \neq 0$.*

Proof. It is easy to see that the conclusion equivalent to the assertion that for every prime p, the Sylow pro-p subgroups of $\hat{\Gamma}$ are infinite. This follows from the Theorem if Γ is not virtually solvable, while if Γ is virtually solvable then Γ has a finite-index subgroup which maps onto $\mathbb{Z}$. ■

Corollary 16.4.18 *Let Γ be a finitely generated linear group over a field of characteristic zero. If Γ has finite upper p-rank for at least one prime p then Γ is virtually soluble.*

Indeed this is a formal consequence of the theorem since the upper p-rank of Γ is by definition the rank of a Sylow pro-p subgroup P of $\widehat{\Gamma}$, hence an upper bound for the number of generators required by P.

Remark If $p = 2$, this can be proved by a quite different route, namely using Theorem 4 of chapter 5. It is interesting to compare it with Theorem 2 of Chapter 5, which asserts that a finitely generated residually finite group of finite upper rank is virtually soluble: finite upper rank implies a (uniform) finite bound for the upper p-ranks for *all* primes p, and this much stronger hypothesis is necessary if we don't assume linearity (for examples see Chapter 13, Section 4).

Proof of Theorem 16.4.16. Replacing Γ by a suitable subgroup of finite index, we may suppose by the Lubotzky alternative that $\widehat{\Gamma}$ maps onto $\prod_{q \notin S} \mathfrak{S}(\mathbb{F}_q)$ where $\mathfrak{S}$ and S are as in Theorem 16.4.12. It suffices therefore to prove that the Sylow pro-p subgroups of this product are not finitely generated.

Fixing the prime p, it will suffice to show that there are infinitely many primes q for which $p \mid |\mathfrak{S}(\mathbb{F}_q)|$. Now, by Lang's Theorem (↬ **Linear groups**) the group $\mathfrak{S}$ is quasi-split over $\mathbb{F}_q$ and therefore contains a one-dimensional split torus; so $\mathfrak{S}(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{F}_q^*$ which is of order $q - 1$. By Dirichlet's Theorem (↬ **Primes**) there are infinitely many primes q with $q \equiv 1 (\mathrm{mod}\, p)$. The theorem follows as then $p \mid |\mathfrak{S}(\mathbb{F}_q)|$ for each such q.

Remark. While the Lubotzky alternative has to be formulated slightly differently in positive characteristic, all the applications in this section hold also in that case. See §4 below.

4 Strong approximation in positive characteristic

"Morally" the Strong Approximation Theorem holds also for linear groups over fields of positive characteristic; but it needs to be properly formulated, and this is not quite a straightforward matter.

Recall that in the 'classical' (characteristic zero) situation, one hypothesis of the Strong Approximation Theorem is that the algebraic group $\mathbf{G}$ be *simply connected*. If $\mathbf{G}$ is not simply connected, there is a proper isogeny $\varphi : \widetilde{\mathbf{G}} \to \mathbf{G}$. Then $\Gamma = \mathbf{G}(\mathbb{Z}_S) = \varphi(\widetilde{\mathbf{G}}(\mathbb{Z}_S))$ for some finite set of primes S, and the closure of Γ in $\mathbf{G}(\widehat{\mathbb{Z}_S})$ is contained in $\varphi(\widetilde{\mathbf{G}}(\widehat{\mathbb{Z}_S}))$ which has infinite index in $\mathbf{G}(\widehat{\mathbb{Z}_S})$ (see [PR] §7.4 for details). When the characteristic p is positive, a similar obstacle arises even if the group is simply connected. Consider for example the group $\Gamma_1 = \mathrm{SL}_d(\mathbb{F}_p[t^p])$, a subgroup of the arithmetic group $\Gamma_0 = \mathrm{SL}_d(\mathbb{F}_p[t])$. Like the latter, Γ_1 is Zariski dense in SL_d; but its (congruence) closure in the congruence completion $\mathrm{SL}_d(\widehat{\mathbb{F}_p[t]})$ is far from open. To see this, note that a single local factor of $\mathrm{SL}_d(\widehat{\mathbb{F}_p[t]})$ looks like $\mathrm{SL}_d(\mathbb{F}_q[[x]])$ where q is a power of p and x is a uniformising parameter, while the closure $\overline{\Gamma_1}$of Γ_1 in such a factor consists of matrices all of whose entries are pth powers; so $\overline{\Gamma_1} \leq \mathrm{SL}_d(\mathbb{F}_q[[x^p]])$, a subgroup of infinite index in $\mathrm{SL}_d(\mathbb{F}_q[[x]])$.

This is just a 'formal' counterexample, in that Γ_1 is isomorphic to Γ_0, which does have the strong approximation property. However, a more delicate problem can occur when p is 2 or 3 and $\mathbf{G}$ is a simple algebraic group possessing roots of two distinct lengths whose ratio is $\sqrt{p}$ (this happens for $p = 2$ and $\mathbf{G}$ of type B_n, C_n or F_4 and for $p = 3$ and $\mathbf{G}$ of type G_2). In such cases, there is a so-called 'non-standard isogeny' $\varphi : \mathbf{G} \to \mathbf{G}^\sharp$ where $\mathbf{G}^\sharp$ is another simple algebraic group, and we can play a game similar to the above taking for Γ_1 the image under φ of an arithmetic group in $\mathbf{G}$; in this case Γ_1 need not be isomorphic to any arithmetic group in $\mathbf{G}^\sharp$. (These isogenies are responsible for the 'twisted groups' of Suzuki and Ree.)

Thus if strong approximation is to hold at all, it must be formulated rather carefully. A suitable formulation was found by Pink, and we present here a slight variation of this. Let $\mathbf{G}$ be a connected simple *adjoint* algebraic group defined over a global field k, and let Γ be a finitely generated Zariski-dense subgroup of $\mathbf{G}(k)$. The triple $(k, \mathbf{G}, \Gamma)$ is said to be *minimal* if whenever $(k', \mathbf{G}', \Gamma')$ is another such triple with k' a global subfield of k, and $\varphi : \mathbf{G}' \to \mathbf{G}$ is an isogeny with $\varphi(\Gamma') = \Gamma$, then $k' = k$ and φ is an isomorphism. Pink proves that for any such triple $(k, \mathbf{G}, \Gamma)$ there exists a minimal one $(k', \mathbf{G}', \Gamma')$ such that $\mathbf{G}'$ is isogenous to $\mathbf{G}$ and Γ' is commensurable to Γ.

Now let $(k, \mathbf{G}, \Gamma)$ be a minimal triple and let $\pi : \widetilde{\mathbf{G}} \to \mathbf{G}$ denote the universal cover of $\mathbf{G}$, so $\widetilde{\mathbf{G}}$ is simply-connected. Put $\Gamma^* = \widetilde{\mathbf{G}}(k) \cap \pi^{-1}(\pi(\Gamma))$.

Theorem 16.4.19 [Pink 2000] *Let $(k, \mathbf{G}, \Gamma)$ be a minimal triple, and let S be a finite set of primes of $\mathcal{O} = \mathcal{O}_k$ such that $\Gamma^* \leq \widetilde{\mathbf{G}}(\mathcal{O}_S)$. Then the closure of Γ^* in $\widetilde{\mathbf{G}}(\widehat{\mathcal{O}_S})$ is open.*

If we start with an arbitrary triple $(k_0, \mathbf{G}_0, \Gamma_0)$, then replace it with a minimal one $(k, \mathbf{G}, \Gamma)$ as above, then the resulting Γ^* will be commensurable with the original group Γ_0; hence the group-theoretic applications discussed in the preceding sections remain valid, with suitable adjustments, also in characteristic p. However we need also the following analogue of Proposition 16.4.15, which is of some independent interest:

Theorem 16.4.20 [Larsen & Lubotzky] *Let F be an arbitrary field and let Γ be a finitely generated subgroup of $\mathrm{GL}_n(F)$. Suppose that the Zariski closure $\mathbf{G}$ of Γ is a connected absolutely simple algebraic group. Then there exist a global field k and a specialisation $\psi : \Gamma \to \mathrm{GL}_n(k)$ such that the Zariski closure of $\psi(\Gamma)$ in GL_n is isomorphic to $\mathbf{G}$.*

Using this and Pink's theorem, one can deduce a version of Lubotzky's alternative valid in all characteristics (here $\overline{k}$ denotes the separable closure of k):

Theorem 16.4.21 *Let G be a finitely generated linear group over a field of characteristic p. Then one of the following holds:*
(a) G is virtually soluble,
(b) there exist a global field k of characteristic p, a connected, simply connected simple algebraic group $\mathfrak{S}$ over k, a finite set of primes S of the ring of integers $\mathcal{O}$ of k such that $\mathfrak{S}(\mathcal{O}_S)$ is infinite, and a subgroup G_1 of finite index in G such that the profinite group $\mathfrak{S}(\widehat{\mathcal{O}_S})$ is an image of $\widehat{G}_1$. Moreover, $\mathfrak{S}$ may be chosen to be $\overline{k}$-isomorphic to $\mathbf{T}^{(l)}$ for some l, where $\mathbf{T}$ is any of the simple components of the Zariski closure of G.

Window: Primes

The problems discussed in this book bring us quite often to counting congruence subgroups in an arithmetic group $\Gamma = G(\mathbb{Z})$ and that leads to counting primes. One may note that if G is the one-dimensional unipotent algebraic group G_a, then $G(\mathbb{Z}) = \mathbb{Z}$ and counting primes is actually counting maximal subgroups in this $G(\mathbb{Z})$. So the whole content of this book can be considered as a generalization of the counting problems studied in analytic number theory. From this point of view, one may see our subject of subgroup growth as a chapter of "non-commutative analytic number theory".

1 The Prime Number Theorem

For a real number $x > 1$, let $\pi(x)$ denote the number of primes not exceeding x and $\vartheta(x) = \sum_{p \le x} \ln p$. (Throughout, the variable p is supposed to range over primes.) The main result of classical analytic number theory is

Theorem 16.4.1 PNT (Hadamard, de la Vallée Poussin)

$$\pi(x) \sim \frac{x}{\ln x}.$$

That is, $\pi(x)/(x/\ln x)$ tends to 1 as $x \to \infty$. This is proved in [HW], Chapter XXII. It is a relatively elementary fact ([HW] Theorem 420) that

$$\vartheta(x) \sim \pi(x) \ln x,$$

so an equivalent formulation of PNT is

$$\vartheta(x) \sim x. \tag{16.1}$$

Another equivalent form ([HW], Theorem 9) is

$$p_n \sim n \ln n \tag{16.2}$$

where p_n denotes the nth prime.

Much effort has been devoted to estimating the error term $E(x) = \vartheta(x) - x$ in the PNT. It is known that the Riemann Hypotheses (RH) is equivalent (!) to the assertion: $E(x) = O_\varepsilon(x^{\frac{1}{2}+\varepsilon})$ for every $\varepsilon > 0$. Moreover if one assumes RH, then actually $E(x) = O\left(x^{1/2}(\ln x)^2\right)$.

Estimation of $\pi(x)$ is crucially needed in the proof of the PSG Theorem (see Chapter 5); actually for this theorem the following weaker estimate suffices:

Proposition 16.4.2 (Chebyshef, 1852)

$$\pi(x) \asymp \frac{x}{\ln x} \quad \textit{as } x \to \infty.$$

The proof goes essentially as follows: Assume x is an integer. It is easy to see that the highest power of a prime p which divides $x!$ is $\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \left[\frac{x}{p^3}\right] + \cdots$ where $[t]$ denotes the greatest integer less than or equal to t. It immediately follows that $x! = \prod_{p \le x} p^{[x/p]+[x/p^2]+\cdots}$ and so

$$\ln(x!) = \sum_{p \le x} \left(\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \left[\frac{x}{p^3}\right] + \cdots \right) \ln(p).$$

Now $\ln(x!)$ is asymptotic to $x \ln(x)$ by Stirling's formula, and, since squares, cubes, $\cdots$ of primes are comparatively rare, and $\left[\frac{x}{p}\right]$ is almost the same as $\frac{x}{p}$, one can infer that

$$x \sum_{p \le x} \frac{\ln(p)}{p} = x \ln(x) + O(x);$$

from this one can deduce that $\pi(x)$ is of order $\frac{x}{\ln x}$. For details, see [HW], ch. XXII. An explicit easy upper bound, obtained by combining Theorems 415 and 420 of [HW], is

$$\pi(x) \le (2 + o(1)) \frac{x}{\log x}$$

(recall that $\log x$ denotes the logarithm to base 2).

The following useful estimates are easily derived from (16.2):

Corollary 16.4.3 *If n is divisible by exactly m distinct primes then*

$$m = O\left(\frac{\ln n}{\ln \ln n}\right).$$

Corollary 16.4.4 *If n is the product of the first m primes then*

$$\ln n = O(m \ln m).$$

For certain purposes we shall also need a much more elementary result, known as 'Bertrand's postulate'. For the proof see [HW], Theorem 418 or [PB], Chapter 1:

Theorem 16.4.5 *For each positive integer n there exists a prime p with $n < p \le 2n$.*

2 Arithmetic progressions and the Bombieri-Vinogradov theorem

For the more precise counting of congruence subgroups in arithmetic groups presented in Chapter 6, we need to count primes in arithmetic progressions, together with good estimates for the error term.

To this end, let a and q be relatively prime integers with $q > 0$. Let

$$\begin{aligned}\mathcal{P}(x;q,a) &= \{p \le x \mid p \equiv a \,(\mathrm{mod}\, q)\}\,,\\ \pi(x;q,a) &= |\mathcal{P}(x;q,a)|\,,\\ \vartheta(x;q,a) &= \sum_{p\in\mathcal{P}(x;q,a)} \ln p.\end{aligned}$$

The classic theorem of Dirichlet, proved in 1837, asserts that if $\gcd(q,a) = 1$ then there are infinitely many primes congruent to $a \,(\mathrm{mod}\, q)$, that is, $\pi(x;q,a) \to \infty$ as $x \to \infty$. In fact, these primes are 'equally distributed' in the following sense:

Theorem 16.4.6 *Assume that* $\gcd(q,a) = 1$. *Then*

$$\begin{aligned}\pi(x;q,a) &\sim \frac{1}{\phi(q)} \cdot \frac{x}{\ln x},\\ \vartheta(x;q,a) &\sim \frac{\vartheta(x)}{\phi(q)} \sim \frac{x}{\phi(q)}.\end{aligned}$$

Here ϕ denotes the Euler function. For the proof, see for example [N], Theorem 3.11. Below we shall see how it may be deduced from a more general result, Chebotarev's theorem.

However, we also need an estimate for the error term

$$E(x;q,a) = \vartheta(x;q,a) - \frac{x}{\phi(q)}.$$

Assuming the generalized Riemann Hypothesis, one can prove that if $q \le x$ then

$$\max_{(a,q)=1} E(x;q,a) \le Cx^{1/2}(\ln x)^2$$

for some absolute constant C.

[Bombieri 1965] proved *unconditionally* that this holds "on the average" (a slightly weaker version was proved independently by Vinogradov). See also [Davenport 2000]. Precisely, we have

Theorem 16.4.7 (Bombieri's Theorem) *Let* $A > 0$ *be fixed. Then there exists a constant* $c(A) > 0$ *such that*

$$\sum_{q\le \frac{\sqrt{x}}{(\ln x)^A}} \max_{y\le x} \max_{(a,q)=1} |E(y;q,a)| \le c(A)\frac{x}{(\ln x)^{A-5}}.$$

Thus the "average error" is $O(x^{\frac{1}{2}}(\ln x)^5)$, which as remarked above does imply RH "in the average". We will need to use it in the following way.

Definition. Let x be a large positive real number. A *Bombieri prime*, w.r.t. x, is a prime q for which $\max\limits_{y\le x}|E(y;q,1)| \le \frac{x}{\phi(q)\ln x}$. If q is a Bombieri prime, w.r.t. x, we call the set $\mathcal{P}(x;q,1)$ a *Bombieri set* w.r.t. x and denote it for short by $\mathcal{P}(x;q)$.

Lemma 16.4.8 *Fix $0<\rho<\frac{1}{2}$. Then for x sufficiently large, there exists at least one Bombieri prime q lying in the interval $\left[\frac{x^\rho}{\ln x}, x^\rho\right]$.*

Proof. Assume not, then for all primes q in the interval $\frac{x^\rho}{\ln x} \le q \le x^\rho$, $\max\limits_{y\le x}|E(y;q,1)| > \frac{x}{\phi(q)\ln x}$. In view of the trivial inequality $\phi(q) = q-1 < q$, it immediately follows that

$$\begin{aligned}\sum_{\frac{x^\rho}{\ln x}\le q\le x^\rho} \max_{y\le x}|E(y;q,1)| &> \frac{x}{\ln x}\sum_{\frac{x^\rho}{\ln x}<q<x^\rho}\frac{1}{q}\\ &> \frac{x}{2\rho}\frac{\ln\ln x}{(\ln x)^2}\end{aligned}$$

provided x is sufficiently large (the sums ranging over primes q); the last inequality follows from the well known asymptotic formula for the partial sum of the reciprocals of the primes

$$\sum_{q\le y}\frac{1}{q} = \ln\ln y + b + O\left(\frac{1}{\ln y}\right)$$

when b is an absolute constant.

This contradicts Bombieri's Theorem with $A \ge 7$, provided x is sufficiently large. ■

Corollary 16.4.9 *Let q be a Bombieri prime with respect to x. Then for x sufficiently large,*

$$\left|\pi(x;q,1) - \frac{x}{\phi(q)\ln x}\right| \le 3\left(\frac{x}{\phi(q)(\ln x)^2}\right).$$

Proof. We have

$$\begin{aligned}\sum_{p\in\mathcal{P}(x,q)} 1 &= \sum_{n=2}^{x}\frac{\vartheta(n;q,1)-\vartheta(n-1;q,1)}{\ln n} =\\ &= \sum_{n=2}^{x}\vartheta(n;q,1)\left(\frac{1}{\ln(n)}-\frac{1}{\ln(n+1)}\right)+\frac{\vartheta(x;q,1)}{\ln(x+1)}\\ &= \sum_{n=2}^{x}\vartheta(n;q,1)\frac{\ln(1+\frac{1}{n})}{\ln n\ln(n+1)}+\frac{\vartheta(x;q,1)}{\ln x}-\vartheta(x;q,1)\left(\frac{1}{\ln x}-\frac{1}{\ln(x+1)}\right).\end{aligned}$$

By the defining property of a Bombieri set, we have the estimate $|\vartheta(n;q,1) - \frac{n}{\phi(q)}| \leq \frac{x}{\phi(q)\ln x}$, for $n \leq x$. It follows easily that

$$\left| \sum_{p\in\mathcal{P}(x,q)} 1 - \frac{\vartheta(x;q,1)}{\ln x} \right| \leq \sum_{n=2}^{x} \vartheta(n;q,1)\frac{1}{n\cdot(\ln n)^2} + \vartheta(x;q,1)\left(\frac{1}{\ln x} - \frac{1}{\ln(x+1)}\right)$$
$$\leq 3\left(\frac{x}{\phi(q)(\ln x)^2}\right).$$

■

3 Global fields and Chebotarev's theorem

By a 'gobal field' one understands either an algebraic number field (finite extension of $\mathbb{Q}$) or a finite extension of the rational function field $\mathbb{F}_p(t)$ for some prime p (a function field). The *ring of integers* $\mathcal{O}_k$ of a global field k is the integral closure of $\mathbb{Z}$ (in the first case) or of $\mathbb{F}_p[t]$ (in the second case). There are several equivalent concepts of 'prime of k'. The 'infinite primes' are equivalence classes of archimedean valuations of k; the 'finite primes' are equivalence classes of non-archimedean valuations of k, or the non-zero prime ideals of $\mathcal{O}_k$. We stick with the latter interpretation; the *norm of a prime* $\mathfrak{p}$ is

$$N\mathfrak{p} = |\mathcal{O}_k/\mathfrak{p}|\,.$$

The Prime Ideal Theorem for global fields is

Theorem 16.4.10 *Let $\pi(x)$ denote the number of prime ideals $\mathfrak{p}$ of $\mathcal{O}_k$ with $N\mathfrak{p} \leq x$. Then*

$$\pi(x) \sim \frac{x}{\ln x}.$$

The proof for algebraic number fields may be found in [Cassels & Fröhlich 1968], Chapter VIII §2, or [Lang 1970], Chapter 15, §5. For the function field case see [Reichardt 1936].

There is also a far-reaching generalisation of Dirichlet's theorem. Let L be a finite Galois extension of the global field k, with Galois group G. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_k$. Provided $\mathfrak{p}$ is unramified (which holds for almost all primes), there is a unique element

$$\sigma = \left[\frac{L/k}{\mathfrak{P}}\right] \in G$$

such that $x^\sigma \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}}$ for every $x \in \mathcal{O}_L$. This is called the *Frobenius symbol*. The primes $\mathfrak{P}$ such that $\mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p}$ for a given $\mathfrak{p}$ form a single orbit under G, and their Frobenius symbols form a single conjugacy class in G; this is denoted $\left(\frac{L/k}{\mathfrak{p}}\right)$ and is called the *Artin symbol*. The important theorem of Chebotarev asserts that the primes of k are equally distributed according to their Artin symbol; that is,

Theorem 16.4.11 (Chebotarev) *Let $\mathcal{C}$ be a conjugacy class in G, and denote by $\pi_{\mathcal{C}}(x)$ the number of prime ideals $\mathfrak{p}$ of $\mathcal{O}_k$ such that $N\mathfrak{p} \leq x$ and $\left(\frac{L/k}{\mathfrak{p}}\right) = \mathcal{C}$. Then*

$$\pi_{\mathcal{C}}(x) \sim \frac{|\mathcal{C}|}{|G|} \cdot \frac{x}{\ln x}.$$

A special case most often used in applications is when $\mathcal{C} = \{1\}$: the primes $\mathfrak{p}$ such that $\left(\frac{L/k}{\mathfrak{p}}\right) = \{1\}$ are precisely those that split completely in L, and the theorem asserts that these have density $1/|G| = 1/(L:k)$.

The theorem was originally proved (like Dirichlet's theorem on arithmetic progressions) in a weaker form, namely as a statement about the *Dirichlet density* of the set of primes in question. A set of primes $\mathcal{S}$ has Dirichlet density δ if

$$\frac{\sum_{\mathfrak{p}\in\mathcal{S}}(N\mathfrak{p})^{-s}}{\sum_{\text{all }\mathfrak{p}}(N\mathfrak{p})^{-s}}$$

tends to the limit δ as $s \to 1^+$. It is easy to see that if $\delta > 0$ then $\mathcal{S}$ is infinite. However, what one really wants to know is the 'natural density' of $\mathcal{S}$, namely the limit as $x \to \infty$ (if it exists) of

$$\frac{|\{\mathfrak{p} \in \mathcal{S} : N\mathfrak{p} \leq x\}|}{|\{\mathfrak{p} \text{ prime} : N\mathfrak{p} \leq x\}|}.$$

It turns out that if either density exists then so does the other, and they are equal; this is an application of the Tauberian theorem of Ikehara and Delange (cf. [Koch 1997], Theorem 1.113, [Lang 1970], Chapter 15). Bearing this in mind, the proof of Chebotarev's theorem may be found in [FJ], Chapter 5.

Let us show how Dirichlet's theorem appears as a special case (cf. [FJ], Chapter 5). Let q, a be integers without common factor. Let ζ be a primitive qth root of unity, $k = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta)$. For each integer b coprime to q there exists $\gamma(b) \in \mathrm{Gal}(L/k)$ such that $\zeta^{\gamma(b)} = \zeta^b$. If $p \nmid q$ is a prime then $\gamma(p)$ is the Frobenius automorphism corresponding to (any prime of L lying over) p. Clearly $p \equiv a \pmod{q}$ if and only if $\gamma(p) = \gamma(a)$; thus the density of the set of all such primes p is equal to $1/|\mathrm{Gal}(L/k)| = 1/\phi(q)$, as required (note that $\mathrm{Gal}(L/k) \cong \mathbb{Z}/q\mathbb{Z}$ is abelian in this case, so the conjugacy class of $\gamma(a)$ has just one element).

Window: Probability

We require very little in the way of probability theory, but the probabilistic terminology is suggestive; in particular it makes sense of what would otherwise seem a purely technical piece of measure-theoretic manipulation. For an accessible and rigorous introduction to the theory, see for example [Renyi 1970].

Let P be a set with a positive, countably-additive measure μ such that $\mu(P) = 1$ (a 'probability space'). The measurable subsets of P are called *events*, and the *probability* of an event X is $\mu(X)$. Two events X and Y are *independent* if

$$\mu(X \cap Y) = \mu(X)\mu(Y).$$

We prove two results, which go together by the name of the **Borel-Cantelli Lemma**. A slightly stronger form is proved in [Renyi 1970], Chapter VII §5. Both concern a sequence $(X_n)_{n\in\mathbb{N}}$ of events, and the associated event

$$X_\infty = \bigcap_{n\in\mathbb{N}} \left(\bigcup_{k=n}^{\infty} X_k \right).$$

An element x lies in X_∞ if and only if x belongs to infinitely many of the X_n, so X_∞ is interpreted as the event "infinitely many of the events X_n happen". The Borel-Cantelli Lemma (under some conditions) determines the probability of X_∞, once the probabilities of the individual events X_n are given.

Fix the notation

$$p_n = \mu(X_n)$$
$$p_\infty = \mu(X_\infty),$$

and for $X \subseteq P$ write $\overline{X} = P \setminus X$.

Proposition 16.4.1 *If the series $\sum_{n=1}^{\infty} p_n$ is convergent then $p_\infty = 0$.*

Proof. Let $\varepsilon > 0$. Then there exists n such that $\sum_{k=n}^{\infty} p_k < \varepsilon$. Since $X_\infty \subseteq \bigcup_{k=n}^{\infty} X_k$ we have

$$\begin{aligned} 0 \leq p_\infty = \mu(X_\infty) &\leq \mu\left(\bigcup_{k=n}^{\infty} X_k \right) \\ &\leq \sum_{k=n}^{\infty} \mu(X_k) = \sum_{k=n}^{\infty} p_k < \varepsilon. \end{aligned}$$

The result follows. ■

Proposition 16.4.2 *Assume that the events X_n are pairwise independent. If the series $\sum_{n=1}^{\infty} p_n$ is divergent then $p_\infty = 1$.*

The proof of this direction needs a little more preparation. For any measurable function f on P, define

$$E(f) = \int_P f,$$
$$D^2(f) = \int_P (f(x) - E(f))^2 dx;$$

$E(f)$ is the *expectation* of f and $D^2(f)$ is the *variance* of f. Now for each n let $\alpha_n : P \to \{0, 1\}$ be the characteristic function of X_n, so $\alpha_n(x) = 1$ for $x \in X_n$, $\alpha_n(x) = 0$ for $x \in \overline{X_n}$. Note that

$$p_n = \mu(X_n) = \int_P \alpha_n.$$

Define

$$F_n(x) = \sum_{k=1}^{n} (\alpha_k(x) - p_k),$$

and note that

$$E(F_n) = 0.$$

We assume henceforth that the events X_n are *pairwise independent*.

Lemma 16.4.3 *For each n we have*

$$D^2(F_n) = \sum_{k=1}^{n} p_k(1 - p_k).$$

Proof. Since $E(F_n) = 0$ we have

$$\begin{aligned} D^2(F_n) &= \int_P \left(\sum_{k=1}^{n} (\alpha_k(x) - p_k) \right)^2 dx \\ &= \sum_{k=1}^{n} \int_P (\alpha_k(x) - p_k)^2 dx + \sum_{l \neq k} \int_P (\alpha_k(x) - p_k)(\alpha_l(x) - p_l) dx. \end{aligned}$$

Now $\alpha_k(x) - p_k$ takes the value $1 - p_k$ on X_k and the value $-p_k$ on $\overline{X_k}$. So

$$\int_P (\alpha_k(x) - p_k)^2 dx = p_k(1 - p_k)^2 + (1 - p_k)p_k^2 = p_k(1 - p_k).$$

Similarly, for $k \neq l$ the function $(\alpha_k(x) - p_k)(\alpha_l(x) - p_l)$ takes the values

$$\begin{array}{ccc} -(1-p_k)p_l & \text{on} & X_k \setminus X_l \\ -p_k(1-p_l) & \text{on} & X_l \setminus X_k \\ (1-p_k)(1-p_l) & \text{on} & X_k \cap X_l \\ p_k p_l & \text{on} & \overline{X_k \cup X_l} \end{array}.$$

Since $\mu(X_k \cap X_l) = p_k p_l$, these four sets have measure $p_k(1-p_l)$, $p_l(1-p_k)$, $p_k p_l$ and $1 - p_k - p_l + p_k p_l = (1-p_k)(1-p_l)$ respectively. Putting these together we find that

$$\int_P (\alpha_k(x) - p_k)(\alpha_l(x) - p_l)dx = 0.$$

The lemma follows. ■

The next lemma is known as *Chebyshef's inequality*:

Lemma 16.4.4 *Let f be a measurable function on P. For $\lambda > 1$ put*

$$B_\lambda = \left\{x \in P \mid (f(x) - E(f))^2 > \lambda D^2(f)\right\}.$$

Then

$$\mu(B_\lambda) \leq \lambda^{-1}.$$

Proof. If $D^2(f) = 0$ then $f(x) = E(f)$ identically and $\mu(B_\lambda) = 0$. Suppose that $D^2(f) \neq 0$. Then

$$\begin{aligned} D^2(f) &= \int_P (f(x) - E(f))^2 dx \\ &\geq \int_{B_\lambda} (f(x) - E(f))^2 dx \\ &\geq \mu(B_\lambda) \cdot \lambda D^2(f), \end{aligned}$$

and the result follows. ■

Proof of Proposition 16.4.2. For each n let

$$Y_n = \left\{x \in P \mid F_n(x) < -\frac{1}{2}\sum_{k=1}^n p_k\right\}.$$

Then each $x \in Y_n$ satisfies

$$\begin{aligned} (F_n(x) - E(F_n))^2 &> \frac{1}{4}\left(\sum_{k=1}^n p_k\right)^2 \\ &= \lambda D^2(F_n) \end{aligned}$$

where

$$\lambda = \frac{\left(\sum_{k=1}^n p_k\right)^2}{4D^2(F_n)} = \frac{\left(\sum_{k=1}^n p_k\right)^2}{4\sum_{k=1}^n p_k(1-p_k)} \geq \frac{\sum_{k=1}^n p_k}{4}$$

since $p_k(1-p_k) \leq p_k$ for each k.

It follows by Lemma 16.4.4 that

$$\mu(Y_n) < 4\left(\sum_{k=1}^{n} p_k\right)^{-1}.$$

As the series $\sum_{k=1}^{\infty} p_k$ is divergent, there exists an increasing sequence $(n(j))_{j\in\mathbb{N}}$ such that

$$\mu(Y_{n(j)}) \leq 2^{-j}$$

for each j. Putting $Z_j = Y_{n(j)}$ we may now apply Proposition 16.4.1 to deduce that $\mu(Z_\infty) = 0$.

To conclude the proof, it will therefore suffice now to verify that $\overline{X_\infty} \subseteq Z_\infty$. Suppose then that $x \in \overline{X_\infty}$. Then for some n we have $x \notin \bigcup_{k=n}^{\infty} X_k$, whence $\alpha_k(x) = 0$ for all $k \geq n$. For each $m \geq n$ we then have

$$F_m(x) + \sum_{k=1}^{m} p_k = \sum_{k=1}^{m} \alpha_k(x) = \sum_{k=1}^{n} \alpha_k(x) \leq n.$$

Since this is less than $\frac{1}{2}\sum_{k=1}^{m} p_k$ if m is large enough, we see that $x \in Y_m$ for all sufficiently large m, and so $x \in Z_\infty$. The proposition follows.

Window: p-adic integrals and logic

1 Results

We consider integrals of $\mathbb{R}_{\geq 0}$-valued functions over subsets of $\mathbb{Q}_p^m$, with respect to the Haar measure μ (always normalised so that $\mu(\mathbb{Z}_p^m) = 1$). The functions and subsets considered will always be easily seen to be measurable, which means that the integral is well defined, as a non-negative real number or ∞ (see for example [Royden 1964], Chapter 11).

In practice, we evaluate integrals by interpreting them as series. Thus if $\phi : V \to \mathbb{R}_{>0}$ takes only countably many values c_n we have

$$\int_V \phi d\mu = \sum_n c_n \cdot \mu(\phi^{-1}(c_n)) \in \mathbb{R} \cup \{\infty\}$$

The fibres $\phi^{-1}(c_n)$ will usually be the intersection of a closed set with an open set, hence measurable. The series either diverges to $+\infty$ or else converges absolutely, so the order of summation is immaterial.

The p-adic absolute value of $\lambda \in \mathbb{Q}_p$ is written

$$|\lambda| = p^{-v(\lambda)}$$

where $v(\lambda)$ is the exact power of p that divides λ (i.e. $p^{-v(\lambda)} \cdot \lambda \in \mathbb{Z}_p^*$ if $\lambda \neq 0$; one puts $v(0) = \infty$ and $|0| = 0$).

In general, s will denote a real variable, assumed when convenient to be large and positive.

The following is in a sense the typical example:

Lemma 16.4.1

$$\int_{\mathbb{Z}_p} |x|^s \, d\mu = \frac{1 - p^{-1}}{1 - p^{-1-s}}.$$

Proof. Let $U_n = p^n\mathbb{Z}_p \setminus p^{n+1}\mathbb{Z}_p$. This consists of $p - 1$ cosets of $p^{n+1}\mathbb{Z}_p$ (out of a possible total of p^{n+1}), so $\mu(U_n) = (p-1)p^{-(n+1)}$. Since the measure

of $\{0\}$ is zero we have

$$\int_{\mathbb{Z}_p} |x|^s \, d\mu = \sum_{n=0}^{\infty} \int_{U_n} |x|^s \, d\mu = \sum_{n=0}^{\infty} p^{-ns} \mu(U_n) = p^{-1}(p-1) \sum_{n=0}^{\infty} p^{-n(s+1)},$$

a geometric progression with the stated sum. ■

The *first order language* L of $\mathbb{Q}_p$ consists of the usual logical symbols (including the quantifiers $\forall$, $\exists$), symbols for variables, a constant symbol for each element of $\mathbb{Q}_p$, binary operation symbols $+$, $\cdot$, and relation symbols $=$, $|$ (where $x \mid y$ is interpreted as $v(x) \leq v(y)$). By a *formula of* L we mean a 'meaningful' expression constructed using only these symbols. A subset V of $\mathbb{Q}_p^m$ is *definable* if there is a formula $\varphi(x_1, \ldots, x_m)$ of L, containing exactly m free variables x_i, such that

$$V = \left\{ \mathbf{x} \in \mathbb{Q}_p^m \mid \varphi(\mathbf{x}) \text{ is true} \right\}.$$

Theorem 16.4.2 [Denef 1984] *Let $V \subseteq \mathbb{Z}_p^m$ be a definable subset of $\mathbb{Q}_p^m$ and let h, k be polynomials in m variables over $\mathbb{Z}_p$. Then there exist polynomials P and Q over $\mathbb{Q}$ such that*

$$\int_V |h(x)| \, |k(x)|^s \, d\mu = \frac{P(p^{-s})}{Q(p^{-s})}$$

for all large positive $s \in \mathbb{R}$.

Denef's statement has only $|k(x)|^s$ in the integrand, but his proof works as well with the extra factor $|h(x)|$. On the other hand, he also proves a more general form of the theorem, in which k is allowed to be any *definable* function, that is one whose graph is a definable subset of $\mathbb{Q}_p^m \times \mathbb{Q}_p = \mathbb{Q}_p^{m+1}$. The proof shows that the polynomial Q can always be taken to be of the form

$$Q(T) = \prod (1 - p^{\alpha_i} T^{\beta_i}) \tag{16.1}$$

where α_i and β_i are non-negative integers. An outline of this proof is given in the following section.

The integral on the left can be written as a sum

$$\sum_{n=0}^{\infty} a_n p^{-ns} = S(p^{-s}),$$

say, where S is a power series. It follows from the theorem that $Q(T)S(T) = P(T)$ holds for all T in some interval $[0, \varepsilon]$ where $\varepsilon > 0$. This implies that $Q(T)S(T) = P(T)$ is an *identity of formal power series*; that is, we may consider s as a dummy and determine the coefficients a_n recursively from this identity.

A further refinement of Denef's theorem was obtained by [Macintyre 1990]. He shows that if h and k are defined independently of the prime p (for example,

if they are polynomials over $\mathbb{Z}$), and the domain V is also defined independently of p, then the degrees of P and Q are *bounded* independently of p. More explicit information about the variation of P and Q with p has been obtained in certain cases by [du Sautoy & Grunewald 2000] (see also our Chapter 15, Section 3).

A powerful generalisation of Denef's theorem was obtained by Denef and van den Dries:

Theorem 16.4.3 [Denef & van den Dries 1988] *Let $V \subseteq \mathbb{Z}_p^m$ be a subanalytic set and let h, $k : \mathbb{Z}_p^m \to \mathbb{Z}_p$ be analytic functions. Then there exist polynomials P and Q over $\mathbb{Q}$ such that*

$$\int_V |h(x)|\,|k(x)|^s\,d\mu = \frac{P(p^{-s})}{Q(p^{-s})}$$

for all large positive $s \in \mathbb{R}$.

A function on $\mathbb{Z}_p^m$ is called *analytic* if locally it can be defined by convergent power series. We won't define 'subanalytic set', but note that these include the sets definable in a certain first-order language for $\mathbb{Q}_p$ that includes function symbols for functions defined by power series. This is just what is needed for the applications to p-adic analytic groups discussed in Chapter 16.

As above, the polynomial Q may be taken of the form (16.1). The formal structure of the proof is similar to that of Denef's theorem; the hard work goes into setting up the 'analytic' theory which makes the argument possible, and we shall say no more about this.

2 A peek inside the black box

The key to Denef's theorem is the fact that the logic of $\mathbb{Q}_p$ admits *quantifier elimination*, in a suitable sense. This means that any formula can be replaced by a formula without quantifiers, and hence that any definable set can be built out of sets that have a particularly simple form. The precise result is as follows:

Theorem 16.4.4 [Macintyre 1976] *A subset of $\mathbb{Q}_p^m$ is definable if and only if it is a Boolean combination of sets of the following types:*

$$\{\mathbf{x} \in \mathbb{Q}_p^m \mid f(\mathbf{x}) = 0\} \tag{I}$$

$$\{\mathbf{x} \in \mathbb{Q}_p^m \mid g(\mathbf{x}) \mid f(\mathbf{x})\} \tag{II}$$

$$\{\mathbf{x} \in \mathbb{Q}_p^m \mid (\exists y \in \mathbb{Q}_p)\ .\, f(\mathbf{x}) = y^n\} \tag{III}$$

where f, g are nonzero polynomials in m variables over $\mathbb{Z}_p$ and $n \geq 2$ is a natural number.

A *Boolean combination* means a set obtained by forming (finitely many) unions, complements and intersections.

A simple lemma in [Denef 1984] shows that any set of type (I) or (II) is also of type (III) (exercise for the reader!). Now if V is a Boolean combination of sets V_i then an integral over V is a finite linear combination, with coefficients ± 1, of integrals over sets of the form $V_{i_1} \cap \ldots \cap V_{i_k}$. So it suffices in Denef's theorem to consider the case where V is defined by finitely many conditions of the form

$$P(g_j(\mathbf{x}); n_j) : g_j(\mathbf{x}) \text{ is an } n_j\text{th power}$$

where $g_j \in \mathbb{Z}_p[T]$ and $2 \leq n_j \in \mathbb{N}$.

The next, and hardest, step is to show that V can be further decomposed into finitely many compact, open pieces on each of which all the polynomials g_j and the functions h, k appearing in the integrand can be replaced by *monomials*. We shall come back to this below, but first let us see how it is used.

Suppose, then, that V is the set of all $\mathbf{x} \in \mathbf{a} + p^e\mathbb{Z}_p^m$ such that $P(g_j(\mathbf{x}); n_j)$ holds $(j = 1, \ldots, q)$, where each $g_j(\mathbf{x})$ is a *monomial*. Let n be a common multiple of $n_1, \ldots, n_q$. If each x_i is replaced by $z_i^n x_i$ with $z_i \in \mathbb{Q}_p^*$ then the validity of $P(g_j(\mathbf{x}); n_j)$ is unaffected. Since $(\mathbb{Q}_p^*)^n \cap \mathbb{Z}_p^*$ has finite index in $\mathbb{Z}_p^*$, it follows that V is partitioned into finitely many subsets of the form

$$\left\{\mathbf{x} \in \mathbf{a} + p^e\mathbb{Z}_p^m \mid P(\lambda_i^{-1}x_i; n) \text{ for } i = 1, \ldots, m\right\}.$$

We may therefore suppose that V is just this set. If h and k are also monomials then

$$|h(\mathbf{x})|\,|k(\mathbf{x})|^s = p^{e_0}\prod_{i=1}^{m}|x_i|^{c_i s + b_i}$$

where c_i and b_i are non-negative integers, and

$$\int_V |h(\mathbf{x})|\,|k(\mathbf{x})|^s\,d\mu = p^{e_0}\prod_{i=1}^{m}\left(\int_{V_i}|x_i|^{c_i s+b_i}\,d\mu(x_i)\right)$$

where

$$V_i = \left\{y \in a_i + p^e\mathbb{Z}_p \mid P(\lambda_i^{-1}y; n)\right\}.$$

Let us fix i and evaluate the corresponding integral. Putting $U(k) = \left(p^k\mathbb{Z}_p \setminus p^{k+1}\mathbb{Z}_p\right) \cap V_i$, we have

$$\begin{aligned} J(i) = \int_{V_i}|x_i|^{c_i s+b_i}\,d\mu(x_i) &= \sum_{k=0}^{\infty}\int_{U(k)}|y|^{c_i s+b_i}\,d\mu \\ &= \sum_{k=0}^{\infty}p^{-k(c_i s+b_i)}\mu(U(k)). \end{aligned}$$

Suppose first that $a_i \notin p^e\mathbb{Z}_p$. Then $|y| = |a_i| = p^{-f}$, say, for every $y \in V_i$. In this case $U(k)$ is empty for $k \neq f$, so

$$J(i) = Ap^{-f(c_i s+b_i)}$$

where $A = \mu(V_i)$.

Suppose next that $a_i \in p^e\mathbb{Z}_p$. Then we may as well take $a_i = 0$. Say $\lambda_i = p^g u$ where $u \in \mathbb{Z}_p^*$. Then $y \in U(k)$ if and only if (i) $k \geq e$ and (ii) $y = p^k v$ where $v \in \mathbb{Z}_p^*$ and

$$p^k v = p^g u \cdot p^{nl} w^n$$

for some integer l and some $w \in \mathbb{Z}_p^*$. Hence $U(k) = \emptyset$ unless $k \geq e$ and $k \equiv g \,(\mathrm{mod}\, n)$, in which case $U(k) = p^k u \cdot \left(\mathbb{Z}_p^*\right)^n$. So putting $B = \mu(u \cdot \left(\mathbb{Z}_p^*\right)^n)$ we have $\mu(U(k)) = p^{-k}B$, and

$$\begin{aligned} J(i) &= \sum_{k \in K} p^{-k(c_i s + b_i + 1)} B \\ &= B \frac{p^{-e'(c_i s + b_i + 1)}}{1 - p^{-n(c_i s + b_i + 1)}}, \end{aligned}$$

where K is the set of $k \geq e$ with $k \equiv g \,(\mathrm{mod}\, n)$ and e' is the smallest number in K.

Thus

$$\int_V |h(\mathbf{x})| \, |k(\mathbf{x})|^s \, d\mu = p^{e_0} \prod_{i=1}^{m} J(i) = \frac{P(p^{-s})}{Q(p^{-s})}$$

where P is a polynomial and $Q(T)$ is a product of factors of the type $(1 - p^c T)$. This is precisely the claim of Denef's theorem, and it makes clear why the result takes the form that it does.

The heart of the proof lies in the reduction to this special case (where everything is a monomial). Denef gives two different ways of achieving this reduction. The first appeals to Hironaka's theorem on the *resolution of singularities*. Applied to the hypersurface defined by the polynomial $h \cdot k \cdot \prod g_j$, this shows that locally, co-ordinates can be found in terms of which each of the individual polynomials in question can be expressed as a monomial. The use of this 'black box' has the advantage of giving a relatively quick and easy proof of the general existence theorem. The disadvantage is that it relies on deep and massive work in algebraic geometry. However, in specific cases it can be carried out effectively, giving an explicit rational function as the value of the integral. This was used to good effect by du [Sautoy & Grunewald 2000], as reported in Chapter 15.

Denef's alternative proof is more complicated, but more elementary, and avoids resolution of singularities. Instead, it takes advantage of the 'grainy' structure of $\mathbb{Z}_p$ as expressed in the so-called *cell decomposition theorem*. This approach, which makes essential use of the quantifier elimination theorem, has the advantage that it can be applied to any *definable functions*, not just polynomials: the idea is to show that if f is definable then $\mathbb{Z}_p^m$ can be decomposed into 'cells' on which $|f|$ is the same as $|r|^{1/e}$ for some *rational function* r and some $e \in \mathbb{N}$; a cell is something like a rectangle. This approach is developed further in [Macintyre 1990], whose 'uniform cell decomposition' is the basis for his proof that the numerator and denominator in Denef's theorem have bounded degrees, independently of the prime. It is worth consulting the introduction to Macintyre's paper for a clear and detailed review of Denef's argument.

Open problems

Most of the following problems have been mentioned, explicitly or implicitly, earlier. Problems that seem to us of particular interest are marked $*$.

1 'Growth spectrum'

The broad question of what subgroup growth types occur is answered in Chapter 13, but as soon as we begin to restrict either the class of groups or the kind of subgroups the problem is very much open. Here is a brief summary of what is known, together with some indications of what remains to be discovered.

Note that the definition of 'growth type' allows one group to have growth type f for many distinct functions f. When referring to the 'spectrum of growth types', what we mean really is the set of *equivalence classes* of growth types, where f is equivalent to g when $\log f \asymp \log g$. All groups are assumed to be finitely generated (abstract or profinite).

1.1 Subgroup growth types

All groups: full spectrum from n to n^n, except possibly between $n^{(\log\log n)^k}$ ($k \in \mathbb{N}$) and $n^{\log n}$ (see chapter 13).

Problems: (a) Fill this gap;

(b) What about *strict* growth types? (the construction of Chapter 13 already gives all strict types between $n^{\log n}$ and n^n).

Residually nilpotent groups: there is a gap between n and $n^{\log n/\log\log n}$ (see Chapter 8). The only types known to occur apart from n and n^n are

$$n^{\log n/\log\log n},\ n^{\log n} \tag{16.1}$$

$$2^{n^\gamma}\ (\gamma = 1/d \text{ or } 1-1/d \text{ with } d \in \mathbb{N}). \tag{16.2}$$

(See Chapters 6 and 9.)

Problems: (a) What other types occur?

(b) Are there further gaps?

(c) Is the spectrum uncountable?

(d) Does type 2^{n^γ} occur for every rational $\gamma \in (0,1)$? (See §9.3.)

Linear groups and **soluble residually nilpotent groups**. Here the gaps are wider, from n to $n^{\log n}$ for linear groups in positive characteristic, from n to 2^{n^γ} ($\gamma > 0$ arbitrarily small) for soluble res. nilpotent groups (see Chapters 8 and 9).

Problems: (a) and (b) as above. (c) for soluble res. nilpotent groups. (d) for *metabelian* groups.

Soluble groups: The maximal growth type is 2^n (see Chapter 3); the only known ones beyond PSG are those in (16.2).

Problems: (a*) Is there a gap above PSG?

(b*) Is the spectrum uncountable?

Countable classes: there are only countably many f.g. linear groups, f.g. metabelian groups, finitely presented groups.

Problem: in each case, the spectrum is countable – describe it!

Pro-p groups: The maximal growth type is 2^n; there is a gap from n to $n^{\log n}$. The known growth types are n, $n^{\log n}$ and types as in (16.2) (see Chapter 4 and §9.3).

Problems: (a*) Are there other gaps?

(b*) What other growth types occur?

(c*) Is the spectrum uncountable?

1.2. Finer growth invariants

PSG groups: there are two invariants, $\alpha(G) = \limsup \frac{\log s_n(G)}{\log n}$ and $\deg(G) = \limsup \frac{\log a_n(G)}{\log n}$. It is known that $\deg(G)$ cannot lie in $(1, 3/2)$ and that $\alpha(G)$ cannot lie in $(1,2)$ ([Shalev 1997$_b$], [Shalev 1999$_a$]).

Problems: (a*) Are there further gaps in the spectrum of α or deg ?

(b*) Is $\alpha(G) \in \mathbb{Q}$ for every f.g. PSG group? Describe the spectrum of possible values (it is a countable set!)

(c) Find the supremum of the numbers ξ such that $\alpha(G) \geq (\xi + o(1)) \cdot h(G)$ for all f.g. PSG groups. (It is known that $3 - 2\sqrt{2} \leq \xi \leq 1$: see §5.6.)

See also problem (a) in §3 below.

Nilpotent groups: It is known that $\alpha(G) \in \mathbb{Q}$ (see Chapter 15).

*Problem**: What is the spectrum of $\alpha(G)$ for f.g. nilpotent groups G? (The only known values are in $\mathbb{N} \cup \{5/2, 7/2\}$).

Pro-p groups: If $s_n(G) \leq n^{c \log_p n}$ for all n where $c < 1/8$ then G has PSG (see Chapter 4).

Problems:

(a) What is the best bound for c? (it is known to lie between $1/8$ and $1/2$).

(b) If G does not have PSG, does G have *strict* growth type at least f, for some function f that is faster than polynomial (and independent of G)?

(c) Determine $\alpha(G)$ for $G = \mathrm{SL}_d^1(\mathbb{Z}_p)$ (see also 'local zeta functions below).

(d) Find the supremum of the numbers ξ such that $\alpha(G) \geq (\xi + o(1)) \cdot \dim G$ for all pro-p groups G of finite rank. (It is known that $3 - 2\sqrt{2} \leq \xi \leq 1$: see §4.1.)

1.3. Subnormal subgroup growth types

Finitely generated abstract groups: The fastest subnormal growth type is 2^n (see Chaper 2). The only known types faster than polynomial are those in (16.2), achieved by metabelian groups (see Chapter 9), $n^{\log n}$ (arithmetic groups in positive characteristic) and $n^{\log n/(\log\log n)^2}$ (some arithmetic groups in characteristic zero) (see Chapter 6: for arithmetic groups with the CSP, the subnormal growth can be estimated in a similar way to the normal subgroup growth).

Problems: (a*) is the spectrum uncountable?

(b*) Are there gaps?

F.g. profinite groups: All the subgroup growth types achieved by pro-p groups (listed above) are in fact *subnormal* subgroup growth types.

Problem: Are there any other subnormal growth types in profinite groups, beyond these and the ones listed just above?

1.4. Normal subgroup growth types

The fastest normal growth type is $n^{\log n}$ (Chapter 2). The only known types faster than polynomial are $n^{\log n}$ and $n^{\log n/(\log\log n)^2}$ (certain arithmetic groups) and a countable infinite sequence of types $n^{(\log n)^\varepsilon}$ with $1/3 \leq \varepsilon < 1$ (metabelian groups) (see Chapters 6 and 9).

Problems: (a*) is the spectrum uncountable?

(b*) Are there gaps?

(c*), (d*): The same questions for f.g. pro-p groups.

Problem: Investigate the possible normal and subnormal growth rates where these are very slow (less than linear); the examples of Chapter 13 have this property.

1.5. Maximal subgroup growth types of finitely generated groups

The examples of §13.2 exhibit the full spectrum of maximal subgroup growth types between $n^{\log n}$ and n^n. Pyber can extend this down to $n^{\log n/\log\log n}$.

*Problem**: Is there a gap between n and this latter type (or some smaller gap)?

2 Normal subgroup growth in pro-p groups and metabelian groups

Problems:

(a*) Characterise the f.g. pro-p groups with polynomial normal subgroup growth. (The metabelian ones are characterised in §9.4.)

(b) Let F be the free pro-p group on $d \geq 2$ generators. Then $\log_p a^{\lhd}_{p^k}(F)$ lies between $(c_1 - \epsilon)k^2$ and $(c_2 + \epsilon)k^2$ for large k, where $c_1 = (d-1)^2/4d$ and $c_2 = (d-1)/2$ (see Chapter 3). Does $k^{-2}\log_p a^{\lhd}_{p^k}(F)$ tend to a limit as $k \to \infty$? If so, what is it?

(c) Let G be a f.g. metabelian group or metabelian pro-p group. Then

$$2 - 2/k + o(n) \leq \frac{\log\log s^{\lhd}_n(G)}{\log\log n} \leq 2 - 1/k + o(n)$$

where $k = \kappa(G)$ (see Chapter 9). Does the middle expression tend to a limit as $n \to \infty$? If so, what is it?

3 The degree of f.g. nilpotent groups

Problems: (a*) Determine $\alpha(G)$ in terms of structural invariants of the f.g. nilpotent group G.

(b) It is known that

$$h(G) \geq \alpha(G) \geq (3 - 2\sqrt{2})h(G)$$

(this is slightly stronger than Proposition 5.6.6 which applies to all f.g. PSG groups). Is the constant on the right best possible?

4 Finite extensions

Let H be a normal subgroup of finite index in a group G.

Problems: (a*) If G has polynomial *normal* subgroup growth, does H also? (cf. §1.11.)

(b*) Same for polynomial *maximal* subgroup growth (cf. Chapter 11).

5 Soluble groups

All the results giving lower bounds for the subgroup growth of f.g. soluble groups or prosoluble groups are obtained by counting *subnormal* subgroups.

Questions: Let G be such a group. (a*) Is the subnormal subgroup growth type of G the same as the subgroup growth type?

(b*) If G has PSG, is $\alpha^{\triangleleft\triangleleft}(G) = \alpha(G)$?

6 Isospectral groups

Groups G and H are said to be *isospectral* if $a_n(G) = a_n(H)$ for every n. This is equivalent to saying that they have identical zeta functions (see Chapter 15). Evidently this holds if $\widehat{G} \cong \widehat{H}$, but this sufficient condition is not necessary: it is shown in Chapter 14 that for each g, the orientable surface group of genus g and the unorientable surface group of genus $2g$ are isospectral.

In general, nothing seems to be known about the structural implications of this relation. To determine what it means for two groups to be isospectral is one of the fundamental problems in the theory of subgroup growth. Here are some specific questions:

(a) If G and H are isospectral groups, do they have the same normal, subnormal or maximal subgroup growth types?

(b) If G and H are isospectral torsion-free finitely generated nilpotent groups, must they have isomorphic profinite completions?

(c) Can there be infinitely many non-isomorphic isospectral torsion-free finitely generated nilpotent groups? (A fundamental theorem of Pickel shows that there are only finitely many such groups with a given profinite completion – see [Sg], Chapter 10).

7 Congruence subgroups, lattices in Lie groups

Question:* Let Γ be a finitely generated just-infinite linear group over a field of characteristic zero, with subgroup growth of type $n^{\log n/\log\log n}$. Does it follow that Γ is isomorphic to an S-arithmetic group? (cf. problem 8(d)

below. See [Lubotzky & Venkataramana] for another algebraic characterization of arithmetic groups, and [Bass & Lubotzky 2000] for a counterexample to Platonov's conjectural characterization.)

Problem:* Determine the congruence subgroup growth type of arithmetic groups in simple algebraic groups of type A_1 and C_l over global fields of characteristic 2. (See Chapter 6.)

Problems:* Prove the '*generalised congruence subgroup conjecture*' for an irreducible lattice Γ in a characteristic-zero semisimple group H (see Chapter 7). It is of particular interest to establish

(a) If Γ is non-arithmetic then Γ has subgroup growth of type at least $n^{\log n}$.

(b) if Δ is another irreducible lattice in H then Δ and Γ have the same subgroup growth type. Same problem in positive characteristic, assuming Γ and Δ are finitely generated (see Chapter 7.)

Problems: (a*) If Γ is an arithmetic group (in a simple algebraic group) in characteristic zero then

$$\frac{\log c_n(\Gamma)}{(\log n/\log\log n)^2} \tag{16.3}$$

is bounded above and below by positive constants (Chapter 6). Does this ratio tend to a limit as $n \to \infty$? If so, what is it? The answer is known only for $\Gamma = \mathrm{SL}_2(\mathcal{O})$; for this and a precise conjecture in the general case, see §6.1 and [Goldfeld, Lubotzky & Pyber].

(b*) Similar questions in characteristic $p \neq 0$, for the ratio

$$\frac{\log c_n(\Gamma)}{(\log n)^2}.$$

(c*) Is there an absolute upper bound, independent of the simple algebraic group $\mathbf{G}$, for this ratio, when $\Gamma = \mathbf{G}(\mathcal{O}_k)$, k is a global field of characteristic $p \neq 0$? (See [Abért, Nikolov & Szegedy] for a step in this direction).

8 Other growth conditions

PIG means 'polynomial index growth' (see Chapter 12). BG means 'boundedly generated': G is BG if G is equal to the product of finitely many cyclic or procyclic subgroups.

Problems:

(a) Are there uncountably many residually finite boundedly generated groups?

(b) If G is a f.g. residually finite group, does $\widehat{G}$ BG imply that G is BG?

(c*) Is every residually finite BG group G linear? Is G linear if we assume additionally that every subgroup of finite index has finite abelianisation? (H. Bass; see [Abért, Lubotzky & Pyber] for more on this question.)

(d*) Is every just-infinite BG linear group isomorphic to an S-arithmetic group?

(e) Does every *soluble* f.g. residually finite group with PIG have finite rank? (Yes if it is also residually nilpotent: see Chapter 12.)

(f) Does every f.g. group with PIG have subgroup growth type at most $n^{\log n}$, or polynomial maximal subgroup growth? (Theorem 12.4 gives the weaker upper bounds $n^{(\log n)^2}$, $n^{\log n}$ respectively.)

(g*) Let G be a f.g. group with $\mathrm{ur}_p(G)$ finite for every prime p. Must G have finite rank? (If this holds for soluble groups G it implies a gap in the subgroup growth spectrum for these groups; see Chapter 9, *Notes*.)

9 Zeta functions

This area is largely uncharted territory, waiting to be explored in many directions. For some promising beginnings, see the papers by du Sautoy in the bibliography, as well as Chapter 15. Here we mention a small sample of problems. Several specific conjectures are stated in the comprehensive survey article [du Sautoy (d)].

Problems:

(a*) "Uniformity". Let G be a f.g. free group in the variety of nilpotent groups of a given class. Prove that

$$\zeta_{G,p}(s) = R(p, p^{-s}) \tag{16.4}$$

for almost all primes p, where R is a rational function in two variables over $\mathbb{Q}$. Same for $\zeta^{\triangleleft}_{G,p}(s)$.

(b*) For which f.g. nilpotent groups G is it the case that the local zeta functions $\zeta_{G,p}(s)$ (or $\zeta^{\triangleleft}_{G,p}(s)$) satisfy a 'local functional equation'

$$R(X^{-1}, Y^{-1}) = X^a Y^b R(X, Y),$$

where R is given by (16.4)? Find an explanation for this phenomenon where it is known to occur. (For many examples, see [du Sautoy (d)], §5.)

(c*) Determine $\zeta_{G,p}$ for $G = \mathrm{SL}^1_d(\mathbb{Z}_p)$, or ζ_L for the associated Lie algebra $L = \mathfrak{sl}_d(\mathbb{Z}_p)$, where $d > 2$ (for $d = 2$, see [du Sautoy 2000], [du Sautoy & Taylor]).

(d*) Find a definition for Mann's 'probabilistic zeta function', and study its properties (see §15.2, and [Mann 1996] for more details).

Bibliography

Some background books

[A] M. Aschbacher, *Finite group theory,* Cambridge Studies in Advanced Maths. **10**, Cambridge Univ. Press, Cambridge, 1988.

[AM] M. F. Atiyah & I. G. Macdonald, *Introduction to commutative algebra,* Addison Wesley, Reading, Mass., 1969.

[B] A. Borel, *Linear algebraic groups,* 2nd ed., Graduate Texts in Math. **126**, Springer-Verlag, New York, 1991.

[C] R. W. Carter, *Simple groups of Lie type,* Wiley, London, 1972.

[DDMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann & D. Segal, *Analytic pro-p Groups*, 2nd edition, Cambridge Studies in Advanced Maths. **61**, Cambridge Univ. Press, Cambridge, 1999.

[DM] J. D. Dixon & B. Mortimer, *Permutation groups,* Graduate texts in Math. **163**, Springer, New York, 1996

[E] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry,* Graduate texts in Math. **150**, Springer, New York, 1995

[FJ] M. D. Fried & M. Jarden, *Field arithmetic*, Ergebnisse der Math. (3) **11**, Springer-Verlag, Berlin–Heidelberg, 1986.

[G] D. Gorenstein, *Finite simple groups*, Plenum Press, New York, 1982.

[GLS] D. Gorenstein, R. Lyons & R. Solomon, *The classification of the finite simple groups, No. 3.* Math. Surveys and Monographs **40.3**, Amer. Math. Soc., Providence, Rhode Island, 1998.

[H] B Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[HB] B Huppert & N. Blackburn, *Finite groups II*, Springer-Verlag, Berlin – Heidelberg, 1982.

[Hm] J. Humphreys, *Linear algebraic groups,* Graduate Texts in Math. **21**, Springer-Verlag, New York, 1975.

[HW] G. H. Hardy & E. M. Wright, *An introduction to the theory of numbers,* 5th edn., Oxford Univ. Press, Oxford, 1983.

[M] G. A. Margulis, *Discrete subgroups of semisimple Lie groups.* Ergebnisse der Math. (3) **17**. Springer-Verlag, Berlin, 1991.

[N] W. Narkiewicz, *Number theory,* World Scientific Publ. co., 1983.

[NH] M. P. F. du Sautoy, D. Segal & A. Shalev (ed.), *New horizons in pro-p groups,* Progress in Math. **184**, Birkhäuser Boston, 2000.

[PB] M. Aigner & G. M. Ziegler, *Proofs from THE BOOK*, 2nd. ed., Springer-Verlag, Berlin – Heidelberg, 2001.

[PR] V. P. Platonov & A. S. Rapinchuk, *Algebraic groups and number theory*, Academic Press, San Diego, 1994.

[R] D. J. S. Robinson, *A course in the theory of groups,* Graduate Texts in Math. **80**, Springer-Verlag, New York, 1982.

[R1] D. J. S. Robinson, *Finiteness conditions and generalized soluble groups 1,* Ergebnisse der Math. **62**. Springer-Verlag, Berlin, 1972.

[R2] D. J. S. Robinson, *Finiteness conditions and generalized soluble groups 2,* Ergebnisse der Math. **63**. Springer-Verlag, Berlin, 1972.

[Ra] M. S. Raghunathan, *Discrete subgroups of Lie groups*, Ergebnisse der Math. **68**, Springer-Verlag, Berlin–Heidelberg–New York, 1972.

[RZ] L. Ribes & P. A. Zalesskii, *Profinite groups,* Ergebnisse der Math. (3) **40**, Springer-Verlag, Berlin – Heidelberg – New York, 2000.

[Sg] D. Segal, *Polycyclic groups*, Cambridge Univ. Press, Cambridge, 1983.

[Sr] J.-P. Serre, *Trees*, Springer-Verlag, Berlin–Heidelberg–New York, 1980.

[St] R. Steinberg, *Lectures on Chevalley groups,* Yale University, 1967.

[We] B. A. F. Wehrfritz, *Infinite linear groups*, Ergebnisse der Math. **76**, Springer-Verlag, Berlin, 1973.

[Wi] J. S. Wilson, *Profinite groups*, Londin Math. Soc. Monographs (n.s.) **19**, Clarendon Press, Oxford, 1998.

General bibliography

M. Abért, A. Lubotzky & L. Pyber, Bounded generation and linear groups, *Intl. J. Algebra and Computation*, to appear.

M. Abért, N. Nikolov & B. Szegedy, Congruence subgroup growth of arithmetic groups in positive characteristic, *Duke Math. J.*., to appear

M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514.

M. Aschbacher & R. Guralnick, Solvable generation of groups and Sylow subgroups of the lower central series, *J. Algebra* **77** (1982), 189-201.

M. Aschbacher & R. Guralnick, Some applications of the first cohomology group, *J. Algebra* **90** (1984), 446-460.

L. Babai, P. J. Cameron & P. P. Pálfy, On the orders of primitive groups with restricted nonabelian composition factors, *J. Algebra* **79** (1982), 161-168.

L. Babai, A. J. Goodman, W. M. Kantor, E. M. Luks & P. P. Palfy, Short presentations for finite groups, *J. Algebra* **194** (1997), 79–112.

A. Balog, L. Pyber & A. Mann, Polynomial index growth groups, *Intl. J. Algebra and Computation* **10** (2000), 773-782.

Y. Barnea & R. Guralnick, Subgroup growth of some pro-p groups, *Proc. Amer. Math. Soc.*, **130** (2002), 653-659.

Y. Barnea & M. Larsen, A non-abelian free pro-p group is not linear over a local field, *J. Algebra* **214** (1999), 338-341.

H. Bass, K-theory and stable algebra, *Publ. Math. IHES* **22** (1964), 5-60.

H. Bass & A. Lubotzky, Non-arithmetic super-rigid groups: counterexamples to Platonov's conjecture, *Annals of Math.* **151** (2000), 1151-1173.

H. Bass & A. Lubotzky, *Tree lattices.* Progress in Mathematics **176**. Birkhäuser Boston, Boston, 2001.

H. Bass, J. Milnor & 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.

M. Bhattacharjee, The probability of generating certain profinite groups by two elements, *Israel J. Math.* **86** (1994), 311-329.

E. Bombieri, On the large sieve, *Mathematika* **12** (1965), 201–225.

A. Borovik, L. Pyber & A. Shalev, Maximal subgroups in finite and profinite groups, *Trans. Amer. Math. Soc.* **348** (1996), 3745-3761.

M. Burger, T. Gelander, A. Lubotzky & S. Mozes, Countng hyperbolic manifolds, *GAFA Journal*, to appear.

M. Burger & S. Mozes, Lattices in products of trees. *Publ. Math. IHES* **92** (2000), 151–194.

C. Bushnell & I. Reiner, Zeta functions of arithmetic orders and Solomon's conjectures, *Math. Zeit.* **173** (1980), 135-161.

L. M. Butler, Subgroup lattices and symmetric functions, *Memoirs Amer. Math. Soc.* **112** (1994).

P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1-22.

P. J. Cameron, *Permutation groups,* London Math. Soc. Student Texts **45**, Cambridge Univ.Press, Cambridge, 1999.

S. Carlip, Spacetime foam and the cosmological constant, *Phys. Rev. Lett.* **79** (1997), 4071-4074.

S. Carlip, Dominant topologies in Euclidean quantum gravity, *Class. Quant. Grav.* **15** (1998), 2629-2638.

J. W. S. Cassels, *Local fields*, London Math. Soc. Student Texts **3**, Cambridge Univ.Press, Cambridge, 1986.

J. W. S. Cassels & A. Fröhlich, *Algebraic number theory*, Academic Press, New York, 1968.

S. Chowla, I. N. Herstein & K. Moore, On recursions connected with symmetric groups I, *Canad. J. Math.* **3** (1951), 328–334.

S. Chowla, I. N. Herstein and W. R. Scott, The solutions of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk* **25** (1952), 29–31.

L. Clozel,On the cohomology of Kottwitz's arithmetic varieties. *Duke Math. J.* **72** (1993), 757–795.

D. Cooper, D. D. Long & A. W. Reid, Essential closed surfaces in bounded 3-manifolds. *J. Amer. Math. Soc.* **10** (1997), 553–563.

K. Corlette, Archimedean superrigidity and hyperbolic geometry. *Ann. of Math.* (2) **135** (1992), 165–182.

C. Curtis and I. Reiner, *Methods of Representation Theory*, Wiley Interscience, New York, 1981.

H. Davenport, *Multiplicative number theory*, 3d edn. Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 2000.

P. Deligne & D. G. Mostow, *Commensurabilities among lattices in* PU$(1, n)$. Annals of Math. Studies **132**, Princeton University Press, Princeton, 1993.

J. Denef, The rationality of the Poincaré series associated to the p-adic points on a variety, *Invent. Math.* **77** (1984), 1-23.

J. Denef & L. van den Dries, p-adic and real subanalytic sets, *Annals of Math.* **128** (1988), 79-138.

I. M. S. Dey, Schreier systems in free products, *Proc. Glasgow Math. Soc.* **7** (1965), 61-79.

J. D. Dixon, The Fitting subgroup of a linear solvable group, *J. Austral. Math. Soc.* **7** (1967), 417-424.

J. D. Dixon, The probability of generating the symmetric group, *Math. Zeit.* **110** (1969), 199-205.

M. P. F. du Sautoy, Finitely generated groups, p-adic analytic groups and Poincaré series, *Annals of Math* **137** (1993), 639-670.

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

M. P. F. du Sautoy, Counting congruence subgroups in arithmetic groups, *Bull. London Math. Soc.* **26** (1994_b), 255-262.

M. P. F. du Sautoy, Mersenne primes, irrationality and counting subgroups, *Bull. London Math. Soc.* **29** (1997), 285-294.

M. P. F. du Sautoy, Zeta functions and counting finite p-groups, *Electronic Research Announcements Amer. Math. Soc.* **5** (1999), 112-122.

M. P. F. du Sautoy, Counting p-groups and nilpotent groups, *Publ. Math. IHES* **92** (2000), 63-112.

M. P. F. du Sautoy, A nilpotent group and its elliptic curve: non-uniformity of local zeta functions of groups, *Israel J. Math.***126** (2001), 269-288.

M. P. F. du Sautoy, Counting subgroups in nilpotent groups and points on elliptic curves, *J. reine angew. Math.,* to appear. (a)

M. P. F. du Sautoy, Natural boundaries for zeta functions of groups, in preparation. (b)

M. P. F. du Sautoy, Functional equations and uniformity for local zeta functions of algebraic groups, in preparation. (c)

M. P. F. du Sautoy, Zeta functions of groups: the quest for order versus the flight from ennui, in *Groups St. Andrews/Oxford 2001*, LMS Lect. note series, Cambridge Univ. Press, Cambridge, to appear. (d)

M. P. F. du Sautoy & F. J. Grunewald, Zeta functions of classical groups and their friendly ghosts, *C. R. Acad. Sci. Paris* Sér. I math. **327** (1998), 1-6.

M. P. F. du Sautoy & F. J. Grunewald, Analytic properties of Euler products of Igusa-type zeta functions and subgroup growth of nilpotent groups, *C. R. Acad. Sci. Paris* Sér. I math. **329** (1999), 351-356.

M. P. F. du Sautoy & F. J. Grunewald, Analytic properties of zeta functions and subgroup growth, *Annals of Math.* **152** (2000), 793-833.

M. P. F. du Sautoy & F. J. Grunewald, Zeta functions of groups: zeros and friendly ghosts, *Amer. J. Math.* **124** (2000), 1-48.

M. P. F. du Sautoy & F. J. Grunewald, Uniformity for zeta functions of two-generator free nilpotent groups, in preparation. (a)

M. P. F. du Sautoy & A. Lubotzky, Functional equations and uniformity for local zeta functions of nilpotent groups, *Amer. J. Math.* **118** (1996), 39-90.

M. P. F. du Sautoy, J. J. McDermott & G. C. Smith, Zeta functions of crystallographic groups and analytic continuation, *Proc. London Math. Soc.* (3) **79** (1999), 511-534.

M. P. F. du Sautoy and D. Segal, Zeta functions of groups, in *New Horizons in pro-p Groups*, Progress in Math. **184**, Birkhäuser Boston, 2000.

M. P. F. du Sautoy and G. L. Taylor, The zeta function of $\mathfrak{sl}_2$ and resolution of singularities, in preparation.

D. B. A. Epstein, Finite presentations of groups and 3-manifolds. *Quart. J. Math. Oxford* Ser. (2) **12** (1961), 205–212.

W. Feit & J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775-1029.

T. Gelander, Counting locally symmetric manifolds, preprint.

D. Gluck, Á. Seress & A. Shalev, Bases for primitive permutation groups and a conjecture of Babai, *J. Algebra* **199** (1998), 367-378.

D. Goldfeld, A. Lubotzky & L. Pyber, Counting congruence subgroups, in preparation

C. Godsil, W. Imrich and R. Razen, *On the number of subgroups of given index in the modular group*, Monatsh. Math. **87** (1989), 273–280.

D. Gorenstein, R. Lyons & R. Solomon, *The classification of the finite simple groups,* No. 1. 2nd ed., Math. Surveys and Monographs **40.1**, Amer. Math. Soc. , Providence, Rhode Island, 2000.

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

M. Grady & M. Newman, Residue periodicity in subgroup counting function for free products, *Contemp. Math.* **166** (1994), 265-273.

C. Griffin, *Subgroups of infinite groups: interactions between number theory and group theory*, Ph.D. thesis, University of Nottingham, 2002.

R. I. Grigorchuk, Just infinite branch groups, *New horizons in pro-p groups,* Chap. 4, Progress in Math. **184**, Birkhäuser, Boston, 2000.

M. Gromov & I. Piatetskii-Shapiro, Nonarithmetic groups in Lobachevsky spaces. *Publ. Math. IHES* **66** (1988), 93–103.

M. Gromov & R. Schoen, Harmonic maps into singular spaces and p-adic superrigidity for lattices in groups of rank one. *Publ. Math. IHES* **76** (1992), 165–246.

K. W. Gruenberg, *Relation modules of finite groups,* CBMS regional conf. series in math. **25**, Amer. Math. Soc., Providence, Rhode Island, 1976.

F. J. Grunewald, J. Elstrodt & J. Mennicke, *Groups acting on hyperbolic space. Harmonic analysis and number theory.* Springer-Verlag, Berlin, 1998.

F. J. Grunewald & G. Noskov, Largeness of certain hyperbolic lattices, manuscript.

F. J. Grunewald & J. Schwermer, Free nonabelian quotients of SL_2 over orders of imaginary quadratic numberfields. *J. Algebra* **69** (1981), 298–304.

F. J. Grunewald, D. Segal & G. C. Smith, Subgroups of finite index in nilpotent groups, *Invent. Math.* **93** (1988), 185-223.

R. M. Guralnick, On the number of generators of a finite group, *Archiv der Math.* **53** (1989), 521-523.

P. Hall, A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.* **30** (1934), 29-95.

M. Hall, Subgroups of finite index in free groups, *Canadian J. Math.* **1** (1949), 187-190.

D. Hanson, On the product of the primes, *Canadian Math. Bull.* **15** (1972), 33-37.

G. M. D. Hogeweij, Almost-classical Lie algebras, I, *Nederl. Akad. Wetensch. Indag. Math.* **44** (1982), 441-452.

D. Holt, On the second cohomology group of a finite group, *Proc. London Math. Soc.* **55** (1987), 22-36.

M. V. Horoshevskii, On automorphisms of finite groups (Russian), *Mat. Sbornik* **93** (1974), 576-587.

E. Hrushovskii & A. Pillay, Groups definable in local fields and pseudo-finite fields, *Israel J. Math.* **85** (1994), 203-262.

E. Hrushovskii & A. Pillay, Definable subgroups of algebraic groups over finite fields, *J. reine angew. Math.* **462** (1995), 69-91.

A. Hulpke & A. Seress, Short presentations for three-dimensional unitary groups, *J. Algebra* **245** (2001), 719–729.

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

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

I. Ilani, Zeta functions related to the group $\mathrm{SL}_2(\mathbb{Z}_p)$, *Israel J. Math.* **109** (1999), 157-172.

I. M. Isaacs, *Character theory of finite groups,* Academic Press, New York–San Francisco–London, 1976.

M. Jarden, Roots of unity over large algebraic fields, *Math. Annalen* **213** (1975), 109-127.

M. R. Jerrum, A compact representation for permutation groups, *J. Algorithms* **7** (1986), 60-78.

G. A. Jones, Congruence and non-congruence subgroups of the modular group: a survey, *Proc. Groups St. Andrews 1985*, LMS Lect. note series **121**, pp. 223-234, Cambridge Univ. Press, Cambridge, 1986.

W. M. Kantor, Some topics in asymptotic group theory, *Groups, combinatorics and geometry*, LMS Lect. note series **165**, pp. 403-421, Cambridge Univ. Press, Cambridge, 1992.

W. M. Kantor & A. Lubotzky, The probability of generating a finite classical group, *Geom. Ded.* **36** (1990), 67-87.

M. I. Kargapolov & Ju. I. Merzljakov, *Fundamentals of the theory of groups,* Graduate texts. in maths. **62**, Springer-Verlag, New York Heidelberg Berlin, 1979.

A. Kerber & B. Wagner, Gleichungen in endlichen Gruppen, *Arch. Math. (Basel)* **35** (1980), 252-262.

W. Kimmerle, R. Lyons, R. Sandling & D. N. Teague, Composition factors from the group ring and Artin's theorem on orders of simple groups, *Proc. London Math. Soc.* (3) **60** (1990), 89-122.

P. B. Kleidman & M. W. Liebeck, *The subgroup structure of the finite classical groups,* London Math. Soc. Lect. Note Ser. **129**, Cambridge Univ. Press, Cambridge, 1990.

B. Klopsch, Linear bounds for the degree of subgroup growth in terms of the Hirsch length, *Bull. London Math. Soc.* **32** (2000), 403-408.

B. Klopsch, Pro-p groups with linear subgroup growth, to appear. (a)

B. Klopsch, The zeta function of the $\mathbb{Z}_p$ Lie algebra $\mathfrak{sl}_1(\delta_p)$, preprint. (b)

B. Klopsch, Enumerating finite groups without abelian composition factors, preprint. (c)

H. Koch, *Algebraic number theory*, Springer-Verlag, Berlin – Heidelberg, 1997.

L. G. Kovács, On finite soluble groups, *Math. Zeit.* **103** (1968), 37-39.

J. H. Kwak & J. Lee, Enumeration of graph coverings, surface branched coverings and related group theory, *Combinatorial & Computational Mathematics; Present and Future*, eds. S. Hong, J. H. Kwak, K. H. Kim & F. W. Roush, pp. 97–161, World-Scientific, Singapore 2001.

S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.

M. Larsen, How often is $84(g-1)$ achieved? *Israel J. Math.* **126** (2001), 1–16.

M. Larsen & A.Lubotzky, Normal subgroup growth of linear groups: the $(G_2,\ F_4,\ E_8)$ theorem, preprint.

M. Larsen & R. Pink, Finite subgroups of algebraic groups, preprint

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

C. R. Leedham-Green, The structure of finite p-groups, *J. London Math. Soc.* **50** (1994), 49-67.

C. R. Leedham-Green & S. McKay, On the classification of p-groups and pro-p groups, *New Horizons in pro-p groups*, pp. 55-74, Progress in Math. **184**, Birkhäuser Boston, 2000.

J-S. Li & J. J. Millson, On the first Betti number of a hyperbolic manifold with an arithmetic fundamental group. *Duke Math. J.* **71** (1993), 365–401.

M. W. Liebeck & L. Pyber, Finite linear groups and bounded generation, *Duke Math. J.* **107** (2001), 159-171.

M. W. Liebeck & A. Shalev, The probability of generating a finite simple group, *Geom. Ded.* **56** (1995), 103-113.

V. Liskovets and A. Mednykh, Enumeration of subgroups in fundamental groups of orientable circle bundles over surfaces, *Comm. in Algebra* **28** (2000), 1717–1738.

A. Lubotzky, Group presentation, p-adic analytic groups and lattices in $\mathrm{SL}_2(\mathbb{C})$. *Ann. of Math.* (2) **118** (1983), 115–130.

A. Lubotzky, Dimension function for discrete groups, in *Groups St Andrews 1985*, LMS Lect. note series **121**, pp. 254-262, Cambridge Univ. Press, Cambridge, 1986.

A. Lubotzky, A group-theoretic characterization of linear groups, *J. Algebra* **113** (1988), 207-214.

A. Lubotzky, Lattices in rank one Lie groups over local fields. *Geom. Funct. Anal.* **1** (1991), 406–431.

A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995_a), 267-295.

A. Lubotzky, Subgroup growth, *Proc. ICM 1994*, Birkhäuser, Basel, 1995_b, pp. 309-317.

A. Lubotzky, Counting finite-index subgroups, in *Groups Galway/St Andrews 1993*, LMS lect. notes **212**, pp. 368-404, Cambridge Univ. Press, Cambridge, 1995_c.

A. Lubotzky, Eigenvalues of the Laplacian, the first Betti number and the congruence subgroup problem. *Ann. of Math.* (2) **144** (1996_a), 441–452.

A. Lubotzky, Free quotients and the first Betti number of some hyperbolic manifolds. *Transform. Groups* **1** (1996_b), 71–82.

A. Lubotzky, Enumerating boundedly generated finite groups, *J. Algebra* **238** (2001), 194-199.

A. Lubotzky, The expected number of random elements to generate a finite group, to appear, (a).

A. Lubotzky & A. Mann, Powerful p-groups. I: Finite groups; II: p-adic analytic groups, *J. Algebra* **105** (1987), 484-505, 506-515.

A. Lubotzky & A. Mann, Residually finite groups of finite rank, *Math. Proc. Cambridge Philos. Soc.* **106** (1989), 385-388.

A. Lubotzky & A. Mann, On groups of polynomial subgroup growth, *Invent. Math.* **104** (1991), 521-533.

A. Lubotzky, A. Mann & D. Segal, Finitely generated groups of polynomial subgroup growth, *Israel J. Math.* **82** (1993), 363-371.

A. Lubotzky, L. Pyber & A. Shalev, Discrete groups of slow subgroup growth, *Israel J. Math.* **96** (1996), 399-418.

A. Lubotzky & A, Shalev, On some Λ-analytic pro-p groups, *Israel J. Math.* **85** (1994), 307-337.

A. Lubotzky & T. N. Venkataramana, A group theoretical characterisation of S-arithmetic groups in higher rank semisimple Lie groups, *Geom. Dedicata* **90** (2002), 1-28.

A. Lucchini, A bound on the number of generators of a finite group, *Archiv der Math.* **53** (1989), 313-317.

A. Lucchini & F. Morini, On the probability of generating finite groups with a unique minimal normal subgroup, *Pacific J. Math.* **203** (2002), 429-440.

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

A. J. Macintyre, Rationality of p-adic Poincaré series: uniformity in p, *Annals Pure Applied Logic* **49** (1990), 31-74.

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

A. Mann, Positively finitely generated groups, *Forum Math.* **8** (1996), 429-459.

A. Mann, Enumerating finite groups and their defining relations, *J. Group Theory* **1** (1998), 59-64.

A. Mann, Subgroup growth in pro-p groups, in *New Horizons in pro-p Groups*, eds. du Sautoy, Segal and Shalev, Progress in Math. **184**, Birkhäuser, Boston, 2000.

A. Mann: Enumerating finite groups and their defining relations, II, in preparation. (a)

A. Mann, Some applications of probability in group theory, *Groups: geometric and combinatorial aspects*, eds. H. Helling & T. W. Müller (to appear). (b)

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

A. Mann and D. Segal, Subgroup growth: some current developments, in *Infinite Groups 94*, eds. de Giovanni and Newell, W. de Gruyter 1995

A. Mann & A. Shalev, Simple groups, maximal subgroups and probabilistic aspects of profinite groups, *Israel J. Math.* **96** (1996), 449-468.

A. McIver & P. M. Neumann, Enumerating finite groups, *Quarterly J. Math. Oxford* (2) **38** (1987), 473-488.

O. Manz & T. R. Wolf, *Representations of solvable groups*, LMS Lect. note series **185**, Cambridge Univ. Press, Cambridge, 1993.

A. Maróti, On the orders of primitive groups, *J. Algebra*, to appear.

C. R. Matthews, L. N. Vaserstein & B. Weisfeiler, Congruence properties of Zariski-dense subgroups, *Proc. London Math. Soc.* **48** (1984), 514-532.

A. D. Mednykh, On unramified coverings of compact Riemann surfaces, *Soviet Math. Doklady.* **20** (1979), 85–88.

A. D. Mednykh, On the number of subgroups in the fundamental group of a closed surface, *Comm. in Algebra* **16** (1988), 2137-2148.

J. J. Millson, On the first Betti number of a constant negatively curved manifold. *Ann. of Math.* (2) **104** (1976), 235–247.

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

T. W. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* **44** (1991), 75-94.

T. W. Müller, Subgroup growth of free products, *Invent. Math.* **126** (1996), 111-131.

T. W. Müller, Finite group actions and asymptotic expansion of $e^{P(z)}$, *Combinatorica* **17** (1997_a), 523-554.

T. W. Müller, Combinatorial classification of finitely generated virtually free groups. *J. Algebra* **195** (1997_b), 285–29.

T. W. Müller, Parity patterns in Hecke groups and Fermat primes, preprint. (a)

T. W. Müller, Modular subgroup arithmetic and a theorem of P. Hall, *Bull. London Math. Soc.*, to appear. (b)

T. W. Müller, Modular subgroup arithmetic in free products, preprint. (c)

T. W. Müller, Poincaré's problem for free products, in preparation. (d)

T. W. Müller, Modular subgroup arithmetic – the state of the art, to appear. (e)

T. W. Müller and J.-C. Puchta, Character theory of symmetric groups and subgroup growth, *J. London Math. Soc.*, to appear. (a)

T. W. Müller and J.-C. Puchta, Parity patterns in one-relator groups, *J. Group Theory*, to appear. (b)

B. H. Neumann, Some remarks on infinite groups, *J. London Math. Soc.* **12** (1937), 120-127.

P. M. Neumann, An enumeration theorem for finite groups, *Quarterly J. Math.* (2) **30** (1969), 395-401.

P. M. Neumann, Some questions of Edjvet and Pride about infinite groups, *Illinois J. Math.* **30** (1986), 301-316.

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

M. Nori, Subgroups of $\mathrm{SL}_n(\mathbb{Z}_p)$, unpublished manuscript. (a)

M. Nori, On subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$, *Invent. Math.* **88** (1987), 257-275.

P. P. Pálfy, A polynomial bound for the orders of primitive solvable groups, *J. Algebra* **77** (1982), 127-137.

R. Pink, Compact subgroups of linear algebraic groups, *J. Algebra* **206** (1998), 438-504.

R. Pink, Strong approximation for Zariski-dense subgroups over arbitrary global fields, *Comment. Math. Helv.* **75** (2000), 608-643.

V. P. Platonov & A. S. Rapinchuk, Abstract characterizations of arithmetic groups with the congruence property. (Russian) *Dokl. Akad. Nauk SSSR* **319** (1991), 1322–1327; translation in *Soviet Math. Dokl.* **44** (1992), 342–347.

V. P. Platonov & A. S. Rapinchuk, Abstract properties of S-arithmetic groups and the congruence problem. (Russian) *Izv. Ross. Akad. Nauk Ser. Mat.* **56** (1992), 483–508; translation in *Russian Acad. Sci. Izv. Math.* **40** (1993), 455–476

C. E. Praeger & J. Saxl, On the order of primitive permutation groups, *Bull. London Math. Soc.* **12** (1980), 303-307.

J.-C. Puchta, Groups with multiplicative subgroup growth, *Israel J. math.* **122** (2001), 149-156.

J.-C. Puchta, The subgroup growth of some one-relator-groups, preprint (a).

L. Pyber, Asymptotic results for permutation groups, *DIMACS series in discrete maths. and computer sci.* **11** (1993), 197-219.

L. Pyber, Group enumeration and where it leads us, *Proc. European Math. Congress, Budapest,* 1996.

L. Pyber, Asymptotic results for simple groups and some applications, *DIMACS series in discrete maths. and computer. sci.* **28** (1997), 309-327.

L. Pyber, Bounded generation and subgroup growth, *Bull. London Math. Soc.,* **34** (2000), 55-60.

L. Pyber, Maximal subgroups, growth functions and Dixon-type theorems, in preparation. (a)

L. Pyber, Groups of intermediate subgroup growth and a problem of Grothendieck, to appear. (b)

L. Pyber and A. Shalev, Groups with super-exponential subgroup growth, *Combinatorica* **16** (1996), 527-533.

L. Pyber and A. Shalev, Asymptotic results for primitive permutation groups, *J. Algebra* **188** (1997), 103-124.

A. S. Rapinchuk, The congruence subgroup problem. *Algebra, K-theory, groups, and education* (New York, 1997), 175–188, *Contemp. Math.* **243**, Amer. Math. Soc., Providence, RI, 1999.

A. S. Rapinchuk, Representations of groups of finite width. (Russian) *Dokl. Akad. Nauk SSSR* **315** (1990_a), 536–540; translation in *Soviet Math. Dokl.* **42** (1991), 816–820

A. S. Rapinchuk, The congruence subgroup problem for arithmetic groups of bounded generation. (Russian) *Dokl. Akad. Nauk SSSR* **314** (1990_b),1327–1331; translation in *Soviet Math. Dokl.* **42** (1991), 664–668

H. Reichardt, Der Primdivisorsatz für algebraische Funktionenkörper über einem endlichen Konstantenkörper, *Math. Zeit.* **40** (1936), 713-719.

A. Renyi, *Probability Theory*, North-Holland, Amsterdam, 1970.

A. Reznikov & P. Moree, Three-manifold subgroup growth, homology of coverings and simplicial volume. *Asian J. Math.* **1** (1997), 764–768.

D. J. S. Robinson, On the cohomology of soluble groups of finite rank, *J. Pure and Applied Algebra* **6** (1975), 155-164.

J. D. Rogawski, *Automorphic representations of unitary groups in three variables.* Annals of Mathematics Studies **123**. Princeton University Press, Princeton, NJ, 1990.

H. Royden, *Real Analysis,* Macmillan, New York, 1963.

R. Schmidt, *Subgroup lattices of groups*, de Gruyter Expositions in Mathematics **14**. Walter de Gruyter & Co., Berlin, 1994.

D. Segal, A residual property of finitely generated abelian-by-nilpotent groups, *J. Algebra* **32** (1974), 389-399.

D. Segal, Subgroups of finite index in soluble groups I, in *Groups St Andrews 1985*, LMS Lect. note series **121**, pp. 307-314, Cambridge Univ. Press, Cambridge, 1986_a.

D. Segal, Subgroups of finite index in soluble groups II, in *Groups St Andrews 1985*, LMS Lect. note series **121**, pp. 315-319, Cambridge Univ. Press, Cambridge, 1986_b

D. Segal, Residually finite groups, in *Groups–Canberra 1989,* ed. L. G. Kovács. Lect. notes in Maths. **1456**, Springer-Verlag, Berlin, 1990.

D. Segal, A footnote on residually finite groups, *Israel J. Math.* **94** (1996_a), 1-5.

D. Segal, Variations on polynomial subgroup growth, *Israel J. Math.* **94** (1996_b), 7-19.

D. Segal, On the growth of ideals and submodules, *J. London Math. Soc.* (2) **56** (1997), 245-263.

D. Segal, Closed subgroups of profinite groups, *Proc. London Math. Soc.* (3) **81** (2000_a), 29-54.

D. Segal, On modules of finite upper rank, *Trans. Amer. Math. Soc.* **353** (2000_b), 391-410.

D. Segal, The finite images of finitely generated groups, *Proc. London Math. Soc.* (3) **82** (2001), 597-613.

D. Segal, On the finite images of infinite groups, *Groups: geometric and combinatorial aspects*, eds. H. Helling & T. W. Müller (to appear)(a).

D. Segal & A. Shalev, Groups with fractionally exponential subgroup growth, *J. Pure Applied Algebra* **88** (1993), 205-223

D. Segal & A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math. Soc.*(2) **55** (1997), 320-334

Y. Segev, On finite homomorphic images of the multiplicative group of a division algebra. *Ann. of Math.* (2) **149** (1999), 219–251.

J.-P. Serre, Le problème des groupes de congruence pour SL_2. *Annals of Math.* (2) **92** (1970), 489–527.

J.-P. Serre, *Topics in Galois theory,* Research notes in math. **1**, Jones and Bartlett, Boston – London, 1992.

A. Shalev, Growth functions, p-adic analytic groups and groups of finite coclass, *J. London Math. Soc.* **46** (1992), 111-122

A. Shalev, The structure of finite p-groups: effective proof of the coclass conjectures, *Invent. Math.* **115** (1994), 315-345.

A. Shalev, Subgroup growth and sieve methods, *Proc. London Math. Soc.*(3) **74** (1997_a), 335-359

A. Shalev, Groups whose subgroup growth is less than linear, *Internat. J. Algebra Comput.* **7** (1997_b), 77-91.

A. Shalev, Simple groups, permutation groups and probabliity, *Proc. Intl. Conf. Math. Berlin, 1998*, vol. II, Berlin, 1998, pp. 129-137.

A. Shalev, On the degree of groups of polynomial subgroup growth, *Trans. Amer. Math. Soc.* **351** (1999_a), 3793-3822.

A. Shalev, Probabilistic group theory, *Groups St. Andrews 1997 in Bath II*, London Math. Soc. LNS **261**, pp. 648-678. Cambridge Univ.Press, Cambridge, 1999_b.

G. C. Smith, *Zeta functions of torsion-free finitely generated nilpotent groups*, PhD thesis, University of Manchester Institute of Science and Technology, 1983.

R. P. Steinberg, Generators for simple groups, *Canad. J. Math.* **14** (1962), 277-183.

H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory,* London Math. Soc. Student Texts **50**, Cambridge Univ.Press, Cambridge, 2001.

O. I. Tavgen, Bounded generation of Chevalley groups over rings of algebraic S-integers, *Math. USSR Izvestiya* **36** (1991), 101-128.

G. L. Taylor, *Zeta functions of algebras and resolution of singularities*, PhD thesis, University of Cambridge, 2001.

J. G. Thompson, Finite non-solvable groups, *Group Theory: Essays for Philip Hall,* pp. 1-12, eds. K. W. Gruenberg & J. E. Roseblade, Academic Press, London, 1984.

J. Tits, Reductive groups over local fields, Automorphic forms, representations and L-functions, *Proc. Symposia Pure Math.* **33**, pp. 29-69, Amer. Math. Soc., Providence, Rhode Island, 1979.

M. R. Vaughan-Lee & E. Zelmanov, Bounds in the restricted Burnside problem, *J. Austral. Math. Soc.* (A) **67** (1999), 261-271.

È. B. Vinberg & O. V. Shvartsman, Discrete groups of motions of spaces of constant curvature. *Geometry, II*, 139–248, *Encyclopaedia Math. Sci.* **29**, Springer, Berlin, 1993.

C. Voll, *Zeta functions of groups and enumeration in Bruhat-Tits buildings,* Ph.D. thesis, University of Cambridge, 2002.

H. C. Wang, Topics on totally discontinuous groups, *Symmetric Spaces,* eds. W. Boothby & G. Weiss, Marcel Dekker, 1972, 460-487.

B. Weisfeiler, Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups, *Annals of Math.* **120** (1984), 271-315.

J. S. Wilson, Groups satisfying the maximal condition for normal subgroups, *Math. Zeit.* **118** (1970), 107-114.

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

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

K. Wohlfahrt, Über einen Satz von Dey und die Modulgruppe, *Archiv der Math.* **29** (1977), 455-457.

E. I. Zelmanov, On the restricted Burnside problem, *Proc. Internl. Congress Math. Kyoto, 1990*, Math. Soc. Japan, Tokyo, 1991, pp. 395–402.

E. I. Zelmanov, On groups satisfying the Golod-Shafarevich condition, in *New Horizons in pro-p Groups*, eds. du Sautoy, Segal and Shalev, Progress in Math. **184**, Birkhäuser Boston, 2000.