Editor's introduction

From a purely algebraic point of view, there is not a lot one can say about infinite groups in general. Traditionally, these have been studied to good effect in combination with topology or geometry. These lectures represent an introduction to some recent developments that arise out of looking at infinite groups from a point of view inspired – in a general sense – by number theory; specifically the interaction between 'local' and 'global', where by 'local' properties of a group G, in this context, one means the properties of its finite quotients, or equivalently properties of its profinite completion $\widehat{G}$. The second chapter directly addresses the interplay between certain finitely generated groups and their finite images. The other two chapters are more specifically 'local' in emphasis: Chapter I concerns the algebraic structure of certain pro-p groups, while Chapter III introduces a way of studying the rich arithmetical data encoded in certain infinite groups and related structures.

A motivating example for all of the above is the question of 'subgroup growth'. Say G has $s_n(G)$ subgroups of index at most n for each n; the function $n \mapsto s_n(G)$ is the *subgroup growth function* of G, and is finite-valued if we assume that G is finitely generated. Now we can ask (inspired perhaps by Gromov's celebrated *polynomial growth theorem*): what does it mean for the global structure of a finitely generated group if its subgroup growth function is (bounded by a) polynomial? To approach a question of this kind, we need to show that if G is in some sense very big, or very complicated, then G must have a lot of finite quotients that can be more or less well understood. If G is a finitely generated *linear group*, there is a natural family of such quotients provided by the *congruence subgroups*. The theory of 'strong approximation' gives remarkably good information about these; this is the topic of Chapter II.

The point of 'local–global' results in number theory is that the 'local' situation is usually easier to understand. In group theory, we can similarly make things easier by restricting attention to p-groups: there is only one finite simple p-group! To an infinite group G we can associate its pro-p completion $\widehat{G}_p$, which is the inverse limit of the finite p-group quotients of G. If these finite p-quotients are suitably 'small' (for example, if G has polynomial subgroup growth), then – wonderfully! – $\widehat{G}_p$ turns out to have the structure of a (p-adic) Lie group. This has manifold consequences; in particular, $\widehat{G}_p$ is a linear group. Thus the natural map from G into $\widehat{G}_p$ provides a linear representation of G, and the whole technology of linear groups (including the methods of Chapter II) can be applied. Of course, p-adic Lie groups arise in many other situations. Chapter I presents an elementary introduction to the topic, from a group-theoretic perspective.

Given a group G, we can also study the arithmetic of the sequence $(s_n(G))$, or of other sequences associated to G in a similar spirit (such as the *representation growth* function). If G is not 'too big' – finitely generated and nilpotent, say, or arithmetic, or p-adic analytic – these sequences have amazing properties. This is the topic of Chapter III, which introduces the *zeta functions* attached to certain groups and rings. This is a subject still in its infancy: while many striking results have been obtained, many tantalising questions remain.

The three chapters can be read independently of one another, though there are occasional cross-references; for a quick introduction to p-adic numbers and profinite groups see Sections 2–5 of Chapter I. Each chapter has its own introduction; the following remarks are more by way of general motivation.

Analytic pro-p groups

If we want to study the finite images of a group like $\mathrm{SL}_n(\mathbb{Z})$ from a 'local' point of view, we may focus on those of the form $\mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z})$ for a fixed prime p. The inverse limit of this system is the group $\mathrm{SL}_n(\mathbb{Z}_p)$ (where $\mathbb{Z}_p$ is the ring of *p-adic integers*). This is the prototype of a (compact) *p-adic analytic group*. As one would hope, its structure is more transparent than that of the original arithmetic group $\mathrm{SL}_n(\mathbb{Z})$. In particular, it has an open (finite-index) normal subgroup which is a pro-p group of finite rank. In general, one obtains such a pro-p group as an inverse limit of finite p-groups of uniformly bounded ranks; Chapter I presents some of the rich structural theory that exists for these groups. This material belongs in every group-theorist's toolbox.

The chapter introduces the concept of pro-p groups, as inverse limits of finite p-groups. It then develops in more detail the theory of pro-p groups of finite rank – in this context, the *rank* of a group G can be defined as the largest dimension (over $\mathbb{F}_p$) of an elementary abelian section of G. If this is finite, it turns out that G (or at least a suitable subgroup of finite index) carries the structure of a *Lie algebra* over the p-adic integers $\mathbb{Z}_p$, of the same (*finite*) dimension. Thus certain questions about the non-commutative group G can be approached with the help of linear methods.

One consequence is that a pro-p group G of finite rank has the structure of an *analytic group* over $\mathbb{Q}_p$. The more analytic aspects of the theory are not explored in depth in this chapter; a fuller account may be found in the book [APG]. Here it is pointed out that a p-adic analytic pro-p group is the same thing as a closed (in the p-adic topology) subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$, for some n, a fact that has useful applications as mentioned above.

The Lie theory is applied to good effect in studying the *finite* representations of these groups; the *Kirillov orbit method* relates these to the adjoint action of the group on its Lie algebra, and leads to remarkable results concerning the 'representation growth' functions. These in turn can be applied, in a local–global spirit, to the representation growth of arithmetic groups: a topic touched on in Chapters I and III, and the subject of much ongoing research.

Chapter I has some overlap with the book [APG], to which it may serve as an introduction; it also pursues in some depth topics not covered by that book – these include saturable pro-p groups, potent filtrations, and the Kirillov orbit method.

Strong approximation

If one wants to study linear groups, one needs to have some basic familiarity with the theory of linear algebraic groups. One purpose of Chapter II is to provide a brief overview of some of the essential features of this theory – at least enough so that the newcomer can make sense of, and appreciate the value of, the 'strong approximation' results that form the main focus.

In algebraic number theory, the Strong Approximation Theorem is a slightly beefed-up version of the Chinese Remainder Theorem, which says that if $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ are (finitely many) pairwise coprime ideals in a ring of algebraic integers $\mathfrak{o}$, then the natural map from $\mathfrak{o}$ into $\mathfrak{o}/\mathfrak{a}_1 \times \cdots \times \mathfrak{o}/\mathfrak{a}_s$ is surjective. A much deeper fact is that an analogous statement is true for certain non-commutative matrix groups (arithmetic groups). The general setup is explained in Chapter II; as a typical example, we have: if $q_1, \ldots, q_s$ are pairwise coprime integers, then the natural map $\pi : \mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/q_1\mathbb{Z}) \times \cdots \times \mathrm{SL}_n(\mathbb{Z}/q_s\mathbb{Z})$ is surjective.

This theory is satisfying, and in a sense not surprising ($\mathrm{SL}_n(\mathbb{Z})$ is generated by elementary subgroups that look like $\mathbb{Z}$, to which the Chinese Remainder Theorem may be applied; the proof for other arithmetic groups is much harder). A truly remarkable generalisation was discovered in the 1980s by Madhav Nori and Boris Weisfeiler. This applies to linear groups that may be far from arithmetic; for example, if Γ is *any* Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Z})$, then the restriction of π to Γ is still surjective, as long as $q_1, \ldots, q_s$ avoid some finite set of possibly bad primes. In general, the theorem applies to any linear group Γ (over a ring $\mathbb{Z}[1/m]$ for some m) such that the Zariski-closure G of Γ is simple as an algebraic group over $\mathbb{Q}$: it ensures that Γ has an infinite family of readily identifiable finite images, namely the groups $G(\mathbb{Z}/q\mathbb{Z})$ for many integers q.

The necessary technical language (algebraic groups, Zariski topology) is all explained in this chapter, which goes on to describe some powerful and straightforward applications to finitely generated linear groups in general. These are encapsulated in the so-called 'Lubotzky alternative', which implies the following: if Γ is a finitely generated linear group over a field of characteristic 0, then *either* Γ is virtually soluble *or* Γ has a subgroup Δ of finite index such that Δ has infinitely many finite quotients of the form $G(\mathbb{F}_{p^e})$, simple groups of a fixed Lie type over finite fields, with p ranging over almost all primes and e bounded.

The Lubotzky alternative is a key tool for attacking questions of the following kind (and was indeed motivated by them): what global constraints follow for a finitely generated group G if the finite images of G are in some sense 'small', or in some sense 'grow slowly'? Such investigations are expounded in Chapters 5 and 12 of the book [SG]; results include the characterisation of finitely generated residually finite groups of finite upper rank, or with polynomial subgroup growth, as those which are virtually soluble of finite rank. The point in each case is that if G is not virtually soluble, then G must have finite images that are 'too big', or grow too fast.

This methodology has been used in a number of other ways (see Chapter II, Section 6.4). It also belongs in the toolbox of anyone seriously studying finitely generated residually finite groups.

Zeta functions

To each finitely generated group G we may associate the numerical sequence (a_n) where $a_n = a_n(G)$ is the number of subgroups of index (exactly) n in G. It is traditional in number theory to represent such a sequence by a 'generating function'. If the a_n grow at most polynomially with n (i.e. if G has *polynomial subgroup growth*), it may be a good idea to take for this the Dirichlet series

$$\zeta_G(s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

This is a priori a formal expression in which s is an indeterminate, but the polynomial growth condition implies (and is equivalent to) the fact that $\zeta_G(s)$ converges if s is a complex number lying in some non-empty right half-plane, and defines there an analytic function of s. A familiar example is where G is the infinite cyclic group, in which case ζ_G is the Riemann zeta function $\zeta(s)$. Of course, the sequence – $a_n = 1$ for all n – encoded by $\zeta(s)$ does not in itself seem very challenging. However, if instead of $\mathbb{Z}$ we consider the ring of integers $\mathfrak{o}$ in an algebraic number field k and let a_n denote the number of ideals of index (i.e. *norm*) n in $\mathfrak{o}$, the resulting Dirichlet series is then the Dedekind zeta function ζ_k; over a century of algebraic and analytic number theory has shown how the analysis of ζ_k reveals deep properties of the number field k.

The number-theoretic zeta functions have many excellent properties, such as an Euler product, analytic continuation, functional equations. It would be too much to expect all of these to obtain if we start from an essentially non-commutative object like a finitely generated (non-abelian) group. However, for certain kinds of group the associated zeta functions turn out to have some remarkable properties: for example, if G is nilpotent then ζ_G does have an Euler product. This is not so surprising; more remarkably, the 'local factor' at a prime p is a *rational function* in the parameter p^{-s} (recall that the p-local factor of the Riemann zeta function is $1/(1 - p^{-s})$). We can then seek more detailed information about these rational functions: are they all the same (as in Riemann's case)? What other properties do they have? It turns out that the Dedekind zeta functions are not quite an adequate model: more relevant are the Hasse–Weil zeta functions associated to algebraic varieties.

Various zeta functions of this general nature can be associated to various kinds of groups and rings. Chapter III introduces some of these, and presents methods used for analysing them. The non-commutative nature of the input means that, in all but the simplest cases, the explicit calculation of the functions is very hard. Many remarkable results have nonetheless been achieved. Among the most remarkable is the widespread occurrence of so-called 'local functional equations'. This was quite unexpected, remaining for a long time no more than a collection of experimental observations. It reveals deep hidden arithmetical symmetries in apparently innocuous algebraic structures (partly related to – though not a simple consequence of – the Weil conjectures).

Chapter III is perhaps the most technically demanding part of the book: it serves as an introduction to a rich field of research that is only beginning to reveal its mysteries. Less technical – and less up-to-date – discussions of these topics can be found in Chapter 9 of [NH] and Chapters 15 and 16 of [SG].

References for Chapter

[APG] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups, 2nd edn*, Cambridge University Press, 1999.

[NH] M. P. F. du Sautoy, D. Segal and A. Shalev (eds.), *New horizons in pro-p groups*, Birkhäuser, Boston MA, 2000.

[SG] A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser, Basel, 2003.

Chapter I

An introduction to compact p-adic Lie groups

by Benjamin Klopsch

1 Introduction

The theory of Lie groups is highly developed and of relevance in many parts of contemporary mathematics and theoretical physics. Loosely speaking, a Lie group is a group with the additional structure of a real differentiable manifold, given by local coordinate systems, such that the group operations are smooth functions.

Historically, the study of Lie groups, over the real and complex numbers, arose toward the end of the 19th century, from the analysis of continuous symmetries of differential equations by the mathematician Sophus Lie and others. Around the middle of the 20th century, mathematicians such as Armand Borel and Claude Chevalley found that many of the foundational results concerning Lie groups could be developed completely algebraically, giving rise to the theory of algebraic groups defined over arbitrary fields. This insight opened the way for entirely new directions of investigation. Much of the theory of p-adic Lie groups was developed in the 1960s by mathematicians such as Nicolas Bourbaki, Michel Lazard and Jean-Pierre Serre. Since then the study of p-adic Lie groups and analogues of Lie groups over adele rings has largely been motivated by questions from number theory, e.g. regarding automorphic forms and Galois representations. More recently, p-adic Lie groups have also become a key tool in infinite group theory.

Throughout, let p be a prime. The real numbers $\mathbb{R}$ form a completion of the rational numbers $\mathbb{Q}$. Similarly, the field of p-adic numbers $\mathbb{Q}_p$ is obtained by completing $\mathbb{Q}$, albeit with respect to a different, non-archimedean notion of distance. One can define analytic functions over $\mathbb{Q}_p$ and p-adic manifolds, just as over $\mathbb{R}$. A p-adic Lie group, or p-adic analytic group, is a Lie group whose local coordinate systems are p-adic valued rather than real valued. Given such a group, the usual apparatus of Lie theory is available; but one needs to keep in mind that the underlying geometry is rather different, i.e. non-archimedean.

Based on [6, Historical Note, VII], we give some indication of the early history of p-adic Lie theory. The first p-adic Lie groups were encountered by Kurt Hensel at the beginning of the 20th century. He was interested in the local isomorphisms between the additive and the multiplicative groups of $\mathbb{Q}_p$, via the exponential and logarithm maps. More general commutative p-adic Lie groups appeared in the works of André Weil and Élisabeth Lutz on elliptic curves in the 1930s. Subsequent investigations of abelian varieties by Claude Chabauty suggested that the local theory of Lie groups could be applied with little change to the p-adic setting. In 1942, this was made explicit by Robert Hooke, a student of Chevalley; see [19]. Until the beginning of the 1960s, p-adic Lie theory continued to be of interest mainly to arithmeticians and algebraic geometers.

The crucial turning point came in 1962, when Jean-Pierre Serre was prompted by a question of John Tate to consider the cohomology of a closed subgroup of the p-adic Lie group $\mathrm{GL}_2(\mathbb{Z}_p)$. His work led him to propose to Michel Lazard a general programme of comparing the cohomology of p-adic Lie groups to the cohomology of associated Lie algebras.[1] In addition to his cohomological results, Lazard's great achievement in [39] was to show that the class of p-adic Lie groups admits a fairly straightforward group-theoretic characterisation, thereby solving the p-adic analogue of Hilbert's fifth problem.

The upshot of Lazard's characterisation and its later interpretation in terms of powerful groups and groups of finite rank, as described in [10], is that one can study and utilise compact p-adic Lie groups without ever imposing any analytic machinery. Instead, one can construct internally, by group-theoretic means, the key features and invariants of such groups, e.g. their dimensions as Lie groups. This truly algebraic nature of p-adic Lie groups explains to a certain degree their continuing relevance and usefulness in infinite group theory throughout the last three decades; e.g. see [10] and the references given therein.

It is very natural to ask to what extent this success story also translates to groups which are analytic over local fields of positive characteristic or, more generally, pro-p domains of higher Krull dimension. Here our understanding is still much less complete; cf. [10, Ch. 13] and [25].

Aims and scope

The aim of the present notes is to provide an accessible introduction to compact p-adic Lie groups from a group-theoretic point of view. We also discuss the relation between p-adic analytic pro-p groups, other classes of profinite groups and abstract groups. The text is based on a series of five lectures delivered during a short course for graduate students at the University of Oxford in 2007. I have tried to preserve the basic structure and informal style of the original lectures, while adding slightly more detail and appropriate references in places. The series

[1] We are grateful to Prof. Serre for providing this historical information.

of exercises which I include are essentially the ones given during the course, and one of their key purposes is to explore topics which branch off from the main thread of narration. Readers of these notes who are subsequently interested in a more detailed account of the theory of p-adic analytic pro-p groups will naturally turn to the book [10], by Dixon, du Sautoy, Mann and Segal, and the other books listed as main references below.

Content and organisation

The notes are organised as follows.

Section 2 provides a short account of prerequisites from group theory, algebra and number theory. The main topics discussed are: nilpotent groups, finite p-groups, Lie rings, Lie methods in group theory, absolute values, p-adic numbers and integers. The section ends with a preview of what p-adic analytic groups are. The short Section 3 provides a summary of basic notions and facts from point-set topology. Section 4 contains the first series of exercises.

Section 5 introduces powerful finite p-groups and profinite groups (as Galois groups, inverse limits, profinite completions and topological groups). It goes on to describe pro-p groups, powerful pro-p groups and pro-p groups of finite rank. The latter are precisely the pro-p groups which admit the structure of a p-adic analytic group. The second series of exercises is collected in Section 6.

Section 7 describes uniformly powerful pro-p groups and the powerful $\mathbb{Z}_p$-Lie lattices associated to them. Both directions, the limit process which yields a Lie lattice from a Lie group and the transition from a Lie lattice to a Lie group via the Hausdorff formula are explained.

Section 8 starts with a concrete example, the group $\mathrm{GL}_d(\mathbb{Z}_p)$ and its principal congruence subgroups. It then moves on to discuss just-infinite pro-p groups, saturable pro-p groups and the Lie correspondence between subgroups of saturable pro-p groups and Lie sublattices of the associated $\mathbb{Z}_p$-Lie lattice. The third and last series of exercises is collected in Section 9.

Section 10 provides a taste of current research on complex irreducible representations of compact p-adic Lie groups. It introduces the Kirillov orbit method and illustrates its use in the study of representation zeta functions.

References

The following books, which can be regarded as our main references, cover some of the selected material in greater detail. They also address many related and more advanced topics.

J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, Cambridge University Press, 1999.

E. I. Khukhro, *p-automorphisms of finite p-groups*, Cambridge University Press, 1998.

G. Klaas, C. R. Leedham-Green and W. Plesken, *Linear pro-p-groups of finite width*, Springer Verlag, 1997.

C. R. Leedham-Green and S. McKay, *The structure of groups of prime power order*, Oxford University Press, 2002.

J. S. Wilson, *Profinite groups*, Oxford University Press, 1998.

The original source for much of the theory of p-adic analytic groups is Lazard's seminal paper 'Groupes analytiques p-adiques', Inst. Hautes Études Scientifiques, *Publ. Math.* 26, 389–603 (1965).

Throughout the text I have aimed to give reasonably complete, but not exhaustive references to the literature. A guiding principal for my choices has been to select economically a mixture of classical and modern references which are suitable for a newcomer to the subject. More complete references can be found in the books listed above. Each section of the present notes, except for the short Section 3, ends with a few selected suggestions for further reading.

Acknowledgements

In preparing the original course and these notes, I made considerable use of several of the main references listed above, in particular the first book. I also included key results from selected research articles and preprints. Originality I can claim, in a limited sense, with regard to the overall exposition. I am grateful to Dan Segal, Christopher Voll and the anonymous referees for their comments on earlier versions of this text. Given the informal style of the notes I made a fair, but perhaps not entirely systematical effort to attribute results to their respective authors; I apologise for any shortcomings of this light approach.

2 From finite p-groups to compact p-adic Lie groups

In this section, we provide a short account of various basic concepts from group theory and number theory, and we introduce some key notation. After discussing finite p-groups, Lie methods and p-adic integers, we state a hands-on version of Lazard's characterisation of compact p-adic Lie groups.

A useful, general reference for the group-theoretic notions and facts, appearing in this section, is Robinson's introductory text [51].

2.1 Nilpotent groups

Let G be a group and let $x, y \in G$. The *conjugate* of x by y is $x^y = y^{-1}xy$. Conjugation provides a natural action of G on itself; indeed, it induces a homomorphism from G into its automorphism group $\mathrm{Aut}(G)$. The kernel of this homomorphism, which constitutes a normal subgroup of G, is called the *centre* of G and denoted by $\mathrm{Z}(G)$. The *upper central series* of G is the ascending series of normal subgroups

$$1 = \mathrm{Z}_0(G) \leq \mathrm{Z}_1(G) \leq \ldots, \quad \text{where } \mathrm{Z}_{i+1}(G)/\,\mathrm{Z}_i(G) = \mathrm{Z}(G/\,\mathrm{Z}_i(G)).$$

By and large, we will be interested in filtrations of a group G which start at the top, such as the lower central series which we describe next. The *commutator* of x with y is $[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$. The subgroup generated by all commutators is called the *commutator subgroup* of G and denoted by $[G, G]$. This notation is easily adapted to a more general situation: if $H, K \leq G$, then we write $[H, K]$ to denote the subgroup of G which is generated by all commutators $[h, k]$ with $h \in H$ and $k \in K$. The group $[G, G]$ can be characterised as the smallest normal subgroup of G such that the corresponding quotient is abelian. The *lower central series* of G is the descending series of normal subgroups

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \ldots, \quad \text{where } \gamma_{i+1}(G) = [\gamma_i(G), G].$$

A basic property of this sequence is that $[\gamma_i(G), \gamma_j(G)] \subseteq \gamma_{i+j}(G)$ for all $i, j \in \mathbb{N}$.

The group G is said to be *nilpotent* if its lower central series terminates in the trivial group 1 after finitely many steps; in this case, the nilpotency class of G is the smallest non-negative integer c such that $\gamma_{c+1}(G) = 1$. It can be shown that for any group G and for any natural number c the lower central series of G terminates in 1 after c steps if and only if the upper central series of G terminates in G after c steps; see [51, §5.1.9].

Nilpotent groups can be thought of as close relatives of abelian groups. Nevertheless, the study of finite nilpotent groups can become exceedingly difficult from a purely group-theoretic point of view. In fact, a finite group is nilpotent if and only if for each prime p it has a unique Sylow p-subgroup. Equivalently, a finite group is nilpotent if and only if it decomposes as a direct product of finite p-groups; see [51, §5.2.4]. Whereas finite abelian groups are completely classified, the theory of finite p-groups remains an active area of research with many open problems.

Of particular interest in finite group theory is the information that can be gained about a group G from its Sylow p-subgroups – which, as indicated, are nilpotent – and their normalisers. This direction, called *local group theory*, played a critical role in the classification of finite simple groups. For instance, relating the representation theory of a finite group G to the representation theory of the normalisers of p-subgroups of G is currently an attractive field of research; a lot of recent work is focused around the McKay conjecture and generalisations thereof, e.g. see [46].

2.2 Finite p-groups

A *p-group* is a torsion group in which every element has p-power order. Accordingly, finite p-groups are precisely the groups of p-power order. We implicitly stated above that every finite p-group is nilpotent. This fact can easily be proved