London Mathematical Society
Lecture Note Series 157

Analytic pro-*p* Groups

J. D. Dixon, M. P. F. du Sautoy, A. Mann
and D. Segal

CAMBRIDGE UNIVERSITY PRESS

London Mathematical Society Lecture Note Series, 157

Analytic pro-*p* Groups

J.D. Dixon
Carleton University
M.P.F. du Sautoy
All Souls College, Oxford
A. Mann
Hebrew University
D. Segal
All Souls College, Oxford

The right of the University of Cambridge to print and sell all manner of books was granted by Henry VIII in 1534. The University has printed and published continuously since 1584.

CAMBRIDGE UNIVERSITY PRESS
Cambridge
New York Port Chester Melbourne Sydney

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011–4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1991

Printed in Great Britain at the University Press, Cambridge

Library of Congress cataloguing in publication data available

British Library cataloguing in publication data available

ISBN 0 521 39580 1

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor J.W.S. Cassels, Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, 16 Mill Lane, Cambridge CB2 1SB, England

The books in the series listed below are available from booksellers, or, in case of difficulty, from Cambridge University Press.

34 Representation theory of Lie groups, M.F. ATIYAH *et al*
36 Homological group theory, C.T.C. WALL (ed)
39 Affine sets and affine groups, D.G. NORTHCOTT
40 Introduction to H_p spaces, P.J. KOOSIS
46 p-adic analysis: a short course on recent work, N. KOBLITZ
49 Finite geometries and designs, P. CAMERON, J.W.P. HIRSCHFELD & D.R. HUGHES (eds)
50 Commutator calculus and groups of homotopy classes, H.J. BAUES
57 Techniques of geometric topology, R.A. FENN
59 Applicable differential geometry, M. CRAMPIN & F.A.E. PIRANI
62 Economics for mathematicians, J.W.S. CASSELS
66 Several complex variables and complex manifolds II, M.J. FIELD
69 Representation theory, I.M. GELFAND *et al*
74 Symmetric designs: an algebraic approach, E.S. LANDER
76 Spectral theory of linear differential operators and comparison algebras, H.O. CORDES
77 Isolated singular points on complete intersections, E.J.N. LOOIJENGA
78 A primer on Riemann surfaces, A.F. BEARDON
79 Probability, statistics and analysis, J.F.C. KINGMAN & G.E.H. REUTER (eds)
80 Introduction to the representation theory of compact and locally compact groups, A. ROBERT
81 Skew fields, P.K. DRAXL
82 Surveys in combinatorics, E.K. LLOYD (ed)
83 Homogeneous structures on Riemannian manifolds, F. TRICERRI & L. VANHECKE
86 Topological topics, I.M. JAMES (ed)
87 Surveys in set theory, A.R.D. MATHIAS (ed)
88 FPF ring theory, C. FAITH & S. PAGE
89 An F-space sampler, N.J. KALTON, N.T. PECK & J.W. ROBERTS
90 Polytopes and symmetry, S.A. ROBERTSON
91 Classgroups of group rings, M.J. TAYLOR
92 Representation of rings over skew fields, A.H. SCHOFIELD
93 Aspects of topology, I.M. JAMES & E.H. KRONHEIMER (eds)
94 Representations of general linear groups, G.D. JAMES
95 Low-dimensional topology 1982, R.A. FENN (ed)
96 Diophantine equations over function fields, R.C. MASON
97 Varieties of constructive mathematics, D.S. BRIDGES & F. RICHMAN
98 Localization in Noetherian rings, A.V. JATEGAONKAR
99 Methods of differential geometry in algebraic topology, M. KAROUBI & C. LERUSTE
100 Stopping time techniques for analysts and probabilists, L. EGGHE
101 Groups and geometry, ROGER C. LYNDON
103 Surveys in combinatorics 1985, I. ANDERSON (ed)
104 Elliptic structures on 3-manifolds, C.B. THOMAS
105 A local spectral theory for closed operators, I. ERDELYI & WANG SHENGWANG
106 Syzygies, E.G. EVANS & P. GRIFFITH

107 Compactification of Siegel moduli schemes, C-L. CHAI
108 Some topics in graph theory, H.P. YAP
109 Diophantine analysis, J. LOXTON & A. VAN DER POORTEN (eds)
110 An introduction to surreal numbers, H. GONSHOR
111 Analytical and geometric aspects of hyperbolic space, D.B.A.EPSTEIN (ed)
113 Lectures on the asymptotic theory of ideals, D. REES
114 Lectures on Bochner-Riesz means, K.M. DAVIS & Y-C. CHANG
115 An introduction to independence for analysts, H.G. DALES & W.H. WOODIN
116 Representations of algebras, P.J. WEBB (ed)
117 Homotopy theory, E. REES & J.D.S. JONES (eds)
118 Skew linear groups, M. SHIRVANI & B. WEHRFRITZ
119 Triangulated categories in the representation theory of finite-dimensional algebras, D. HAPPEL
121 Proceedings of *Groups - St Andrews 1985*, E. ROBERTSON & C. CAMPBELL (eds)
122 Non-classical continuum mechanics, R.J. KNOPS & A.A. LACEY (eds)
124 Lie groupoids and Lie algebroids in differential geometry, K. MACKENZIE
125 Commutator theory for congruence modular varieties, R. FREESE & R. MCKENZIE
126 Van der Corput's method of exponential sums, S.W. GRAHAM & G. KOLESNIK
127 New directions in dynamical systems, T.J. BEDFORD & J.W. SWIFT (eds)
128 Descriptive set theory and the structure of sets of uniqueness, A.S. KECHRIS & A. LOUVEAU
129 The subgroup structure of the finite classical groups, P.B. KLEIDMAN & M.W.LIEBECK
130 Model theory and modules, M. PREST
131 Algebraic, extremal & metric combinatorics, M-M. DEZA, P. FRANKL & I.G. ROSENBERG (eds)
132 Whitehead groups of finite groups, ROBERT OLIVER
133 Linear algebraic monoids, MOHAN S. PUTCHA
134 Number theory and dynamical systems, M. DODSON & J. VICKERS (eds)
135 Operator algebras and applications, 1, D. EVANS & M. TAKESAKI (eds)
136 Operator algebras and applications, 2, D. EVANS & M. TAKESAKI (eds)
137 Analysis at Urbana, I, E. BERKSON, T. PECK, & J. UHL (eds)
138 Analysis at Urbana, II, E. BERKSON, T. PECK, & J. UHL (eds)
139 Advances in homotopy theory, S. SALAMON, B. STEER & W. SUTHERLAND (eds)
140 Geometric aspects of Banach spaces, E.M. PEINADOR and A. RODES (eds)
141 Surveys in combinatorics 1989, J. SIEMONS (ed)
142 The geometry of jet bundles, D.J. SAUNDERS
143 The ergodic theory of discrete groups, PETER J. NICHOLLS
144 Introduction to uniform spaces, I.M. JAMES
145 Homological questions in local algebra, JAN R. STROOKER
146 Cohen-Macaulay modules over Cohen-Macaulay rings, Y. YOSHINO
147 Continuous and discrete modules, S.H. MOHAMED & B.J. MÜLLER
148 Helices and vector bundles, A.N. RUDAKOV et al
149 Solitons, nonlinear evolution equations and inverse scattering, M.A. ABLOWITZ & P.A. CLARKSON
150 Geometry of low-dimensional manifolds 1, S. DONALDSON & C.B. THOMAS (eds)
151 Geometry of low-dimensional manifolds 2, S. DONALDSON & C.B. THOMAS (eds)
152 Oligomorphic permutation groups, P. CAMERON
153 L-functions and arithmetic, J. COATES & M.J. TAYLOR (eds)
154 Number theory and cryptography, J. LOXTON (ed)
155 Classification theories of polarized varieties, TAKAO FUJITA
156 Twistors in mathematics and physics, T.N. BAILEY & R.J. BASTON (eds)
157 Analytic pro-*p* groups, J.D. DIXON, M.P.F. DU SAUTOY, A. MANN & D. SEGAL
158 Geometry of Banach spaces, P.F.X. MÜLLER & W. SCHACHERMAYER (eds)
159 Groups St Andrews 1989 Volume 1, C.M. CAMPBELL & E.F. ROBERTSON (eds)
160 Groups St Andrews 1989 Volume 2, C.M. CAMPBELL & E.F. ROBERTSON (eds)
161 Lectures on Block Theory, BURKHARD KÜLSHAMMER

Acknowledgements

Our first debt is to *Alex Lubotzky*: his remarkable successes in the application of pro-p groups to problems in group theory have made it necessary for group theorists to come to terms with "pro-p" methods, and this book is the outcome of our own attempts in this direction.

Luis Ribes kindly read the earlier chapters of the book, and we thank him for several suggestions which saved us from errors and obscurities. The short proof of Theorem 2.9 is due to *Andrea Caranti*, and we thank him for permission to include it. We are very grateful to *Aner Shalev* for a number of useful hints, and for allowing us to include several of his unpublished results, on the characterisation of pro-p groups of finite rank and on pro-p groups of finite co-class; and to *Steve Donkin* and *Charles Leedham-Green* for explaining to us their results on pro-p groups of finite co-class, and giving us access to their unpublished notes.

We are grateful to the American Mathematical Society for permission to reproduce Appendix C, which first appeared in the *Bulletin of the American Mathematical Society*.

Thanks to David Tranah of Cambridge University Press, and to the skilful typists in Cambridge, for their patience and efficiency in turning a sequence of fragments into an elegant volume of TEX. The authors collectively would also like to thank the two of their number in Oxford for undertaking the final editing and production of the manuscript.

The first and third named authors would like to thank the Mathematical Institute in Oxford for its hospitality during the initial stages of this project.

CONTENTS

INTERLUDE

PART II : *Analytic groups*

INTRODUCTION

And the end of all our exploring
Will be to arrive where we started
And know the place for the first time.
T. S. Eliot, *Little Gidding*

This book has its origin in a seminar held at All Souls College, Oxford, in the Spring of 1989. The aim of the seminar was to work through Michel Lazard's paper *Groupes analytiques p-adiques*, at least far enough to understand the proof of "Lubotzky's linearity criterion" (Lubotzky (1988)). In fact, Lubotzky's proof combined Lazard's characterisation of p-adic analytic groups with some recent results of Lubotzky and Mann (1987b) on "powerful" pro-p groups. We found that by reversing the historical order of development, and starting with powerful pro-p groups, we could reconstruct most of the group-theoretic consequences of Lazard's theory without having to introduce any "analytic" machinery. This was a comforting insight for us (as group theorists), and gave us the confidence to go on and develop what we hope is a fairly straightforward account of the theory of p-adic analytic groups.

The book is divided (like Gaul) into three parts. Parts I and II are essentially linear in structure. The point of view in Part I is group-theoretic; in Part II, more machinery is introduced, such as normed algebras and formal power series. Between Parts I and II is an *Interlude* (Chapter 6): this consists of a series of more or less independent digressions, describing applications of the results to various aspects of group theory. The reader with a particular interest in one of these aspects might want to turn first to the relevant section of Chapter 6, and then follow up the references therein to earlier (and occasionally) later chapters. On the other hand, someone seeking an introduction to p-adic Lie groups could omit the Interlude, without disturbing the logical structure of the account.

We now outline the contents in more detail. *Part I* is an account of pro-p groups of finite rank. **Chapter 1** is a leisurely introduction to profinite groups and pro-p groups, starting from first principles. **Chapter 2** is about finite p-groups. A finite p-group G is defined to be *powerful* if

G/G^p is abelian (if p is odd; the case $p = 2$ is slightly different). The key results established in this chapter are due to Lubotzky and Mann (1987a): *(i) if G is powerful and can be generated by d elements, then every subgroup of G can be generated by d elements;* and *(ii) if G is a p-group and every subgroup of G can be generated by d elements, then G has a powerful normal subgroup of index at most $p^{d(\log(d)+2)}$* (log to the base 2). **Chapter 3** returns to profinite groups. Here the *rank* of a profinite group is defined, in several equivalent ways. Defining a pro-p group G to be powerful if $G/\overline{G^p}$ is abelian (where $\overline{}$ denotes closure, and the proviso regarding $p = 2$ still applies), we deduce from the above results that *a pro-p group has finite rank if and only if it has a powerful finitely generated subgroup of finite index* (Lubotzky and Mann (1987b)). This is then used to give several aternative characterisations for pro-p groups of finite rank. **Chapter 4** continues with the deeper investigation of finitely generated powerful pro-p groups. These groups, being "abelian modulo p", are in many ways rather like abelian groups. In particular, each such group contains a normal subgroup of finite index which is "uniform"; we shall not define this here, but note that the uniform pro-p groups are exactly those studied by Lazard under the name "groupes p-saturables". Following an exercise in Lazard (1965), we show that a *uniform pro-p group G has in a natural way the structure of a finitely generated free $\mathbb{Z}_p$-module*, which we denote $(G, +)$ (here $\mathbb{Z}_p$ denotes the ring of p-adic integers). (Defining an additional operation "bracket" on this module, we also indicate how $(G, +)$ can be turned into a Lie algebra over $\mathbb{Z}_p$: this is the first hint of a connection with Lie groups.) It follows that the automorphism group of G has a faithful linear representation over $\mathbb{Z}_p$, and hence that G itself is "linear modulo its centre". Part I concludes with **Chapter 5**. Here we study the most familiar p-adic analytic group, namely $\mathrm{GL}_d(\mathbb{Z}_p)$, and show quite explicitly that a suitable congruence subgroup is a uniform pro-p group. Together with the results of Chapter 4, this is used to show that *the automorphism group of any pro-p group of finite rank is itself virtually* (i.e. up to finite index) *a pro-p group of finite rank.*

The *Interlude* presents a variety of applications of the results obtained in Part I (with occasional reference to results proved in Part II). Although the six sections are to some extent independent of each other, they are too short to make separate chapters, and we have put them all together into **Chapter 6.** §**6.1** is devoted to *Lubotzky's group-theoretic criterion for a finitely generated group to have a faithful linear representation in characteristic zero*, and some variations on the same theme. (While the proof of these results in their full glory depends on a forward reference to Chapter 8, we remark that for certain group-theoretic applications, such as those in §6.2, a linear representation with abelian kernel is good enough, and the results in Chapter 4 suffice.) The next two sections are intended to illustrate the power of such "linearity criteria" as a tool for attacking purely group-theoretic problems. §**6.2** outlines the proofs of some recent results concerning residually finite groups subject to additional finiteness conditions; among them, the fact that *every residually finite group of finite rank is virtually locally soluble* (Lubotzky and Mann (1989), and the fact that *a finitely generated residually finite group has polynomial subgroup growth if and only if it is virtually soluble of finite rank* (Lubotzky, Mann and Segal(a)). §**6.3** gives an elementary proof, for the special case of residually nilpotent groups, of Gromov's Theorem that a finitely generated group of polynomial growth is a linear group (the idea of using p-adic analytic groups in this context was first used by Grigorchuk (1989), to prove a stronger result).

§**6.4**, which is independent of §6.1, gives an outline of Leedham-Green and Newman's (1980) programme for classifying finite p-groups by *co-class*. We present a complete proof of Leedham-Green's theorem that *every pro-p group of finite co-class has finite rank*, based on results from Chapter 3; we also show that *both the rank and the index of a uniform normal subgroup are bounded above by a function of the co-class*, for an infinite pro-p group of finite co-class.

The last two sections of Chapter 6 are also independent of the preceding ones. §**6.5** extends the *Golod-Šafarevič* inequality, concerning the minimal number of relations needed to present a finite p-group, to the case of pro-p groups of finite rank; a corresponding result is then derived for certain abstract groups, including all finitely generated nilpotent groups. In §**6.6** we indicate how the Golod-Šafarevič inequality for pro-p groups can be used to prove that certain discrete subgroups in $\mathrm{SL}_2(\mathbb{C})$ cannot have the *congruence subgroup property.* The results of §6.5 and §6.6 are due to Lubotzky (1983).

A different kind of group-theoretic application is described in **Appendix C**, where we have reprinted an announcement recently published by one of the authors. This is concerned with the rationality of certain Poincaré series, associated with the functions $n \mapsto a_n(G)$, where $a_n(G)$ denotes the number of subgroups of index n in a group G. (Though the author of Appendix C uses the terminology of Lazard (1965), the relevant results about pro-p groups can all be found in Chapter 4 and Chapter 9 of this book.)

At this point we should mention an important early application of Lazard's theory: the proof by Bass, Milnor and Serre (1967) that *every representation of* $\mathrm{SL}_n(\mathbb{Z})$ *is a polynomial representation, provided* $n \geq 3$. It would have taken us too far afield to give this proof in Chapter 6, but it is worth remarking that some of the essential ingredients are explained in this book: §6.6 shows that the pro-p completion of an arithmetic group with the congruence subgroup property has finite rank; and it is shown in Chapter 10 that every homomorphism between such groups arises from a homomorphism between the associated Lie algebras.

Although *Part II* is headed "Analytic groups", these do not appear as such until Chapter 9. **Chapter 7** is utilitarian, giving definitions and elementary results about complete normed $\mathbb{Q}_p$-algebras which are needed later. **Chapter 8**, loosely based on Lazard (1965), forms the backbone of Part II. In it, we show how to define a norm on the group algebra $\mathbb{Q}_p[G]$ of a uniform pro-p group G, in a way that respects both the p-adic topology on $\mathbb{Q}_p$ and the pro-p topology on G. The completion $\hat{A}$ of this algebra with respect to the norm serves two purposes. On the one hand, an argument using the binomial expansion of terms in $\hat{A}$ is used to show that the group operations in G are given by *analytic functions* with respect to a natural co-ordinate system on G, previously introduced in Chapter 4. On the other hand, $\hat{A}$ serves as the co-domain for the *logarithm* mapping $\log : G \to \hat{A}$. We show that $\log(G)$ is a $\mathbb{Z}_p$-Lie subalgebra of the commutation Lie algebra on $\hat{A}$, isomorphic via log to the Lie algebra $(G, +)$ defined intrinsically in Chapter 4 (in fact, the proof simultaneously establishes that $(G, +)$ satisfies the Jacobi identity, and that $\log(G)$ is closed with respect to the operation of commutation). An appeal to *Ado's Theorem*, in conjunction with the *Campbell-Hausdorff formula*, then shows that G has a faithful linear representation over $\mathbb{Q}_p$; it follows that *every pro-p group of finite rank has a faithful linear representation.*

p-adic analytic groups are defined in **Chapter 9**. Although we introduce p-adic manifolds, only a bare minimum of theory is developed (in contrast to Serre (1965), for example, there is no mention of differentials). Using the results of Chapter 8, it is shown that a *pro-p group has a p-adic analytic structure if and ony if it has finite rank*, and, more generally, that *every p-adic analytic group has an open subgroup which is a pro-p group of finite rank.* These major results are due to Lazard (1965), except that he refers to finitely generated virtually powerful pro-p groups where we have "pro-p groups of finite rank".

Chapter 10 is concerned with some of the "global" properties of p-adic analytic groups. The first main result here is that *every continuous homomorphism between p-adic analytic groups is an analytic homomorphism*, from which it follows that *the analytic structure of a p-adic analytic group is determined by its topological group structure.* Next, it is shown that *closed subgroups, quotients and extensions of p-adic analytic groups are again p-adic analytic*; these results now follow quite easily from the corresponding properties of pro-p groups of finite rank. The chapter concludes by establishing the equivalence of the category of p-adic analytic groups (modulo "local isomorphism") with the category of finite-dimensional Lie algebras over $\mathbb{Q}_p$.

The *Campbell-Hausdorff formula*, mentioned in connection with Chapter 8, also plays an essential role in Chapter 10. A self-contained (if rather *ad hoc*) proof of this is given in **Appendix A. Appendix B** contains the proofs of some elementary facts about topological groups, used in Chapter 10.

A topic which we have omitted altogether is the cohomology of analytic pro-p groups; this is the subject of Lazard (1965), Chapter V.

Survey articles covering various aspects of the book's material are du Sautoy (a), Mann (b) and Segal (1990).

For the sake of euphony, we have titled the book "Analytic pro-p groups"; a more correct title would be "p-Adic analytic pro-p groups". Analytic groups over other fields also deserve consideration; a Lie group in the usual sense (over $\mathbb{R}$ or $\mathbb{C}$) cannot be a pro-p group (except in the trivial, discrete, case), but some extremely interesting pro-p groups arise as analytic groups over fields of characteristic p: for example, suitable congruence subgroups in $\mathrm{SL}_n(\mathbb{F}_p[[t]])$. The theory of such groups poses some exciting challenges: they will have to be faced in a different book.

Sources

Most of the results in the book are not original. Much of Chapter 1 is "folklore"; the important Theorem 1.17 is due to Serre (unpublished). Chapter 2 is based in Lubotzky and Mann (1987a). Chapter 3 is mostly based on Lubotzky and Mann (1987b), with some new material. In Chapter 4, some of the results are due to Lazard (1965), and some are new. The material of Chapter 5 is presumably known, though we do not have a specific reference.

Chapter 6 contains references for the results discussed there. The proof in §6.3 is new; the proofs in §6.4 are based on unpublished work of Leedham-Green, Donkin, Shalev and Mann.

Part II, as a whole, is a re-working of material from Lazard (1965), with help from Serre (1965) and Bourbaki (1989).

Notation

$\overline{X}$	closure of X
$\subseteq$	subset
$\subseteq_O$, $\subseteq_C$	open subset, closed subset
$\leq$	subgroup
$\leq_O$, $\leq_C$	open subgroup, closed subgroup
$<$	proper subgroup
$<_O$, $<_C$	open proper subgroup, closed proper subgroup
$\triangleleft$	normal subgroup
$\triangleleft_O$, $\triangleleft_C$	open normal subgroup, closed normal subgroup
$\langle X \rangle$	group generated by X
$\mathrm{Z}(G)$	centre of G
$\Phi(G)$	Frattini subgroup of G
$\mathrm{Aut}(G)$	automorphism group of G
$K[G]$	group ring of G over K
$\mathrm{C}_G(X)$	centraliser of X in G
$A \times B$	direct product of A and B
$A \rtimes B$	semidirect product of A by B
$A^{(n)}$	n-fold direct power of A
$A \oplus B$	direct sum of A and B
A^n	direct sum of n copies of (additive group) A
$\mathrm{d}(G)$	minimal number of generators of G
$\mathrm{d_p}(G)$	minimal number of generators of $G/[G,G]G^p$
$\mathrm{rk}(G)$	rank of G
$\mathrm{ur}(G)$	upper rank of G
$\dim(V)$	dimension of V
$v(x) = v_p(x)$	p-adic valuation of x
$\lvert x \rvert = \lvert x \rvert_p$	p-adic absolute value of x
$[x]$	least integer $\geq x$
$\lambda(r)$	defined by $2^{\lambda(r)-1} < r \leq 2^{\lambda(r)}$

GL_n	$n \times n$ general linear group
U_n	$n \times n$ upper uni-triangular matrix group
M_n	$n \times n$ matrix ring
1_n	$n \times n$ identity matrix
$\mathbb{C}$	complex numbers
$\mathbb{R}$	real numbers
$\mathbb{Q}$	rational numbers
$\mathbb{Z}$	integers
$\mathbb{N}$	non-negative integers
$\mathbb{Z}_p$	p-adic integers
$\mathbb{Q}_p$	p-adic numbers
$\mathbb{F}_q$	finite field of size q

$x^y = y^{-1}xy$

$[x, y] = x^{-1}x^y$, or $-x + xy$ if x is in a module acted on by y

$[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$

$[x, {}_n y] = [x, y, \ldots, y]$, with n occurrences of y

$[A, B] = \langle\{[x, y] \mid x \in A,\ y \in B\}\rangle$

$[A_1, \ldots, A_n] = [[A_1, \ldots, A_{n-1}], A_n]$

$[A, {}_n B] = [A, B, \ldots, B]$, with n occurrences of B

$X^{\{n\}} = \{x^n \mid x \in X\}$

$G^n = \langle G^{\{n\}}\rangle$ (if G is a multiplicative group)

$\gamma_1(G) = G,\ \gamma_n(G) = [\gamma_{n-1}(G), G]$

$P_1(G) = G,\ P_n(G) = \overline{[P_{n-1}(G), G]P_{n-1}(G)^p}$