Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

789

James E. Humphreys

Arithmetic Groups

Springer-Verlag
Berlin Heidelberg New York 1980

Author

James E. Humphreys
Department of Mathematics & Statistics
GRC Tower
University of Massachusetts
Amherst, MA 01003
USA

AMS Subject Classifications (1980): 10D07, 20G25, 20G30, 20G35, 20H05, 22E40

ISBN 3-540-09972-7 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-09972-7 Springer-Verlag New York Heidelberg Berlin

Library of Congress Cataloging in Publication Data. Humphreys, James E. Arithmetic groups. (Lecture notes in mathematics ; 789) Bibliography: p. Includes index. 1. Linear algebraic groups. 2. Lie groups. I. Title. II. Series: Lecture notes in mathematics (Berlin) ; 789. QA3.L28. no. 789. [QA171]. 510s [512'.2] 80-12922

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2141/3140-543210

PREFACE

An arithmetic group is (approximately) a discrete subgroup of a Lie group defined by arithmetic properties - for example, $\mathbb{Z}$ in $\mathbb{R}$, $GL(n,\mathbb{Z})$ in $GL(n,\mathbb{R})$, $SL(n,\mathbb{Z})$ in $SL(n,\mathbb{R})$. Such groups arise in a wide variety of contexts: modular functions, Fourier analysis, integral equivalence of quadratic forms, locally symmetric spaces, etc. In these notes I have attempted to develop in an elementary way several of the underlying themes, illustrated by specific groups such as those just mentioned. While no special knowledge of Lie groups or algebraic groups is needed to appreciate these particular examples, I have emphasized methods which carry over to a more general setting. None of the theorems presented here is new. But by adopting an elementary approach I hope to make the literature (notably Borel [5] and Matsumoto [1]) appear somewhat less formidable.

Chapters I - III formulate some familiar number theory in the setting of locally compact abelian groups and discrete subgroups (following Cassels [1], cf. Weil [2] and Goldstein [1]). Here the relevant groups are the additive group and the multiplicative group, taken over local and global fields - or over the ring of adeles of a global field. One basic theme is the construction of a good fundamental domain for a discrete group inside a locally compact group, e.g., $\mathbb{Z}$ in $\mathbb{R}$, or the ring of integers O_K of a number field K inside $\mathbb{R}^n$ (n the degree of K over $\mathbb{Q}$), where a fundamental domain corresponds to a parallelotope determined by an integral basis of K over $\mathbb{Q}$. In the framework of adeles or ideles such fundamental domains have nice arithmetic interpretations. Another basic theme is strong approximation. These introductory chapters are not intended to be a first course in number theory, so the proofs of a few well known theorems are just sketched.

Chapters IV and V deal with general linear and special linear groups, emphasizing "reduction theory" in the spirit of Borel [5]. Here one encounters approximations to fundamental domains (called "Siegel sets") for $GL(n,\mathbb{Z})$ in $GL(n,\mathbb{R})$ and deduces, for example, the finite presentability of $GL(n,\mathbb{Z})$ or $SL(n,\mathbb{Z})$. The BN-pair (Tits system) and Iwasawa decomposition are used heavily here. There is also a brief introduction to adelic and p-adic groups.

Finally, Chapter VI recounts (in the special case of $SL(n,\mathbb{Z})$) the approach of Matsumoto [1] to the Congruence Subgroup Problem, via central extensions and " Steinberg symbols". Here adeles and strong approximation play a key role, along with the Bruhat decomposition already treated in IV. Matsumoto's group-theoretic arguments, done in detail, lead ultimately to the deep arithmetic results of Moore [1], which can only be summarized here. (It is only fair to point out that $SL(n,\mathbb{Z})$ can be handled in a more self-contained way, cf. Bass, Lazard, Serre [1], Mennicke [1], and unpublished lectures of Steinberg. Special linear and symplectic groups over other rings of integers can also be handled more directly, cf. Bass, Milnor, Serre [1]. My objective has been to indicate the most general setting in which the Congruence Subgroup Problem has so far been investigated; in this generality it has not been completely solved.)

The various chapters can be read almost independently, if the reader is willing to follow up a few references. I have tried to make the notation locally (if not always globally) consistent. Standard symbols such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are used, along with $\mathbb{R}^{>0}$ (resp. $\mathbb{R}^{\geq 0}$) for the set of positive (resp. nonnegative) reals. If K is a field, K^* denotes its multiplicative group.

Chapters I - V are a revision of notes published some years ago by the Courant Institute. Chapter VI is based partly on a course I gave at the University of Massachusetts; class notes written up by the students were of great help to me. I am grateful to the National Science Foundation for research support, and to Peg Bombardier for her help in typing the manuscript.

J.E. Humphreys

CONTENTS