

# 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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to the publisher, the amount of the fee to be determined by agreement with the publisher.

© by Springer-Verlag Berlin Heidelberg 1980  
Printed in Germany

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,  $\mathbf{Z}$  in  $\mathbf{R}$ ,  $GL(n, \mathbf{Z})$  in  $GL(n, \mathbf{R})$ ,  $SL(n, \mathbf{Z})$  in  $SL(n, \mathbf{R})$ . 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 adèles 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.,  $\mathbf{Z}$  in  $\mathbf{R}$ , or the ring of integers  $O_K$  of a number field  $K$  inside  $\mathbf{R}^n$  ( $n$  the degree of  $K$  over  $\mathbf{Q}$ ), where a fundamental domain corresponds to a parallelotope determined by an integral basis of  $K$  over  $\mathbf{Q}$ . In the framework of adèles 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  $GL(n, \mathbf{Z})$  in  $GL(n, \mathbf{R})$  and deduces, for example, the finite presentability of  $GL(n, \mathbf{Z})$  or  $SL(n, \mathbf{Z})$ . 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  $SL(n, \mathbf{Z})$ ) the approach of Matsumoto [1] to the Congruence Subgroup Problem,

via central extensions and "Steinberg symbols". Here adèles 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

I.	LOCALLY COMPACT GROUPS AND FIELDS	
	1. Haar measure	
	1.1 Existence and uniqueness . . . . .	1
	1.2 Module of an automorphism . . . . .	2
	1.3 Homogeneous spaces . . . . .	3
	2. Local and global fields	
	2.1 Classification theorem . . . . .	4
	2.2 Structure of local fields . . . . .	5
	Appendix: Review of number fields and completions . .	6
	3. Adele ring of a global field	
	3.1 Restricted topological products . . . . .	9
	3.2 Adeles . . . . .	10
II.	THE ADDITIVE GROUP	
	4. The quotient $\mathbb{A}_K/K$	
	4.1 The space $K_\infty$ . . . . .	11
	4.2 Fundamental domain for $K$ in $\mathbb{A}_K$ . . . . .	13
	4.3 Product formula . . . . .	14
	5. Volume of fundamental domain	
	5.1 Normalized Haar measure . . . . .	15
	5.2 Volume calculation . . . . .	16
	5.3 Application: Fields of discriminant $\neq 1$ . . . .	16
	6. Strong approximation	
	6.1 Chinese Remainder Theorem . . . . .	18
	6.2 An important lemma . . . . .	19
	6.3 Main theorem . . . . .	20
III.	THE MULTIPLICATIVE GROUP	
	7. Ideles	
	7.1 Idele topology . . . . .	21
	7.2 Special ideles . . . . .	22
	8. Compactness theorem	
	8.1 Compactness of $J_K^0/K^*$ . . . . .	24
	8.2 Applications: Class number and units of $K$ . .	25
	8.3 Fundamental domain . . . . .	28
IV.	$GL_n$ AND $SL_n$ (OVER $\mathbb{R}$ )	
	9. Example: The modular group . . . . .	29
	10. Siegel sets in $GL(n, \mathbb{R})$	
	10.1 Iwasawa decomposition . . . . .	31
	10.2 Siegel sets . . . . .	33
	10.3 Minimum principle . . . . .	34

11.	Applications	
11.1	Siegel sets in $SL(n, \mathbb{R})$	36
11.2	Reduction of positive definite quadratic forms	39
12.	BN-pairs	
12.1	Axioms and Bruhat decomposition	41
12.2	Parabolic subgroups	43
12.3	Conjugates of B by W	46
12.4	Complements for $GL_n$	51
13.	Siegel property (and applications)	
13.1	Siegel sets revisited	53
13.2	Fundamental sets and Siegel property	56
13.3	Proof of Harish-Chandra's theorem	58
13.4	Finite presentation of $\Gamma$	61
13.5	Corners and arithmetic groups	64
V.	$GL_n$ AND $SL_n$ (p-ADIC AND ADELIC GROUPS)	
14.	Adelic groups	
14.1	Adelization of a linear group	65
14.2	Class number	66
14.3	Strong approximation	68
14.4	Reduction theory	70
15.	$SL_2$ (over p-adic fields)	
15.1	Infinite dihedral group	71
15.2	Lattices in $K^2$	72
15.3	BN-pair in G	73
15.4	Building attached to BN-pair	77
15.5	Ihara's theorem; maximal compact subgroups	78
	Appendix: Graphs and free groups	81
VI.	THE CONGRUENCE SUBGROUP PROBLEM	
16.	Reformulation of the problem	
16.1	Topological groups	85
16.2	Subgroup topologies on $SL(n, \mathbb{Q})$ and $SL(n, \mathbb{Z})$	86
16.3	Review of topology	88
16.4	Profinite groups	90
16.5	Completions of topological groups	92
16.6	The congruence kernel	97
17.	The congruence kernel of $SL(n, \mathbb{Z})$	
17.1	Some consequences of the invariant factor theorem	98
17.2	Congruence subgroups and q-elementary subgroups	100
17.3	A finiteness lemma	103
17.4	Proof of the theorem	104

17.5	The congruence kernel . . . . .	106
17.6	Universal property of the extension . . . . .	108
18.	The Steinberg group	
18.1	Generators and relations . . . . .	109
18.2	The upper unitriangular group . . . . .	110
18.3	The monomial group . . . . .	111
18.4	Steinberg symbols . . . . .	112
18.5	Determination of $A$ . . . . .	114
18.6	Determination of $\text{Ker } \phi$ . . . . .	115
18.7	Universal property . . . . .	116
18.8	Properties of Steinberg symbols . . . . .	119
19.	Matsumoto's theorem	
19.1	Central extensions and cocycles . . . . .	121
19.2	Statement of the theorem . . . . .	123
19.3	The diagonal group . . . . .	124
19.4	An auxiliary construction . . . . .	124
19.5	The monomial group . . . . .	129
19.6	Conclusion of the proof . . . . .	132
19.7	The big cell . . . . .	136
19.8	The topological case . . . . .	137
20.	Moore's theory	
20.1	Topological Steinberg symbols . . . . .	140
20.2	Local and global theorems . . . . .	142
20.3	Central extensions of locally compact groups . . . . .	143
20.4	The fundamental group in the local case . . . . .	144
20.5	Restricted products . . . . .	145
20.6	Relative coverings . . . . .	146
20.7	The congruence kernel revisited . . . . .	148
	SUGGESTIONS FOR FURTHER READING . . . . .	149
	REFERENCES . . . . .	151
	INDEX . . . . .	157