Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

789

James E. Humphreys

Arithmetic Groups

Springer-Verlag
Berlin Heidelberg New York

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

I. LOCALLY COMPACT GROUPS AND FIELDS

Here we shall review briefly the approach to local fields based on the use of Haar measure, together with the construction of the adele ring of a number field. For a full treatment of these matters, the reader can consult Chapter I of Weil [2].

§1. Haar measure

For the standard results mentioned below, see Halmos [1, Chapter XI] or Bourbaki [3, Chapter 7].

1.1 Existence and uniqueness

Let G be a locally compact topological group (each element of G has a compact neighborhood, or equivalently, the identity element e does). G acts on itself by left and right translations

$$\lambda_x : g \longmapsto xg$$
$$\rho_x : g \longmapsto gx^{-1}$$

(here the inverse insures that we get a homomorphism $x \longmapsto \rho_x$ of G into the group of homeomorphisms of the space G).

Define a left (resp. right) Haar measure μ on G to be a nonzero Borel measure invariant under all left (resp. right) translations. This means, by definition, that μ is nonzero, all Borel sets are measurable, $\mu(C) < \infty$ for C compact, and $\mu(\lambda_x M) = \mu(M)$ (resp. $\mu(\rho_x M) = \mu(M)$) for $x \in G$, $M \subset G$ measurable.

Remarks and examples.

(1) If μ is a left Haar measure on G, $\hat{\mu}$ is a right Haar measure, where $\hat{\mu}(X) = \mu(X^{-1})$ for all measurable X^{-1}. (Check!)

(2) If μ is a left Haar measure on G, $c \in \mathbb{R}^{>0}$, then $c\mu$ is again such (so Haar measure, if it exists, cannot be absolutely unique).

(3) If G is abelian, left Haar measure = right Haar measure.

(4) $G = \mathbb{R}$ or $\mathbb{C}$ (additive group): Lebesgue measure is a Haar measure.

(5) On finite products, the product measure is again a Haar measure (for example, on $\mathbb{R}^n$ or $\mathbb{C}^n$).

(6) On the multiplicative group $\mathbb{R}^{>0}$, dx/x is a Haar measure. (Verify this by integrating functions of compact support.)

(7) G may have essentially distinct left and right Haar measures. (See Halmos, p. 256, for the standard example.)

THEOREM. *Let G be locally compact. Then G has a left (hence also a right) Haar measure, and (up to a positive multiple) only one.*

Haar proved the existence part for G having a countable basis of open sets (1933). Later von Neumann proved uniqueness for compact G. The general case was completed by Weil and von Neumann.

Exercise. G locally compact, μ (left) Haar measure.

(a) G is discrete iff $\mu(\{e\}) > 0$.

(b) G is compact iff $\mu(G) < \infty$.

When G is compact, one frequently (but not always) normalizes μ so that $\mu(G) = 1$.

1.2 Module of an automorphism

The uniqueness part of Theorem 1.1 is more useful than may appear at first. Let G be locally compact, with left Haar measure μ. Aut G denotes the group of automorphisms of G (as topological group).

If $\phi \in \text{Aut } G$, and $X \subset G$ with $\phi(X)$ measurable, set $\nu(X) = \mu(\phi(X))$. Since ϕ preserves Borel sets and compact sets, it is very easy to see that ν is again a left Haar measure on G. By uniqueness, $\nu = (\text{mod}_G\, \phi)\mu$, where $\text{mod}_G\, \phi \in \mathbb{R}^{>0}$ (and this number is independent of the original choice of μ, again by uniqueness). Call $\text{mod}_G\, \phi$ the (left) *module of* ϕ.

Example. Let $\phi = \mathrm{Int}\ x : g \mapsto xgx^{-1}$ $(x \in G)$. Here write $\mathrm{mod}_G\ \phi = \Delta_G(x)$, so $\Delta_G: G \to \mathbb{R}^{>0}$ is a function, called the module of G. If $\Delta_G = 1$, call G unimodular (this means that left Haar measure on G is also right Haar measure).

Exercises and examples.

(a) We could also have defined a right module of ϕ. Prove that this equals $\mathrm{mod}_G\ \phi$.

(b) $\mathrm{mod}_G\ \phi \cdot \mathrm{mod}_G\ \psi = \mathrm{mod}_G(\phi \circ \psi)$.

(c) An abelian group is unimodular.

(d) Any automorphism of a discrete or compact group has module 1, so such groups are unimodular.

(e) Any semisimple or nilpotent Lie group is unimodular.

Besides the example $\phi = \mathrm{Int}\ x$, another sort of automorphism and its module will arise in §2 when we discuss locally compact fields.

1.3 Homogeneous spaces

THEOREM. Let G be locally compact, H a closed subgroup of G. Then there exists a G-invariant nonzero Borel measure on the homogeneous space G/H iff the function Δ_G, restricted to H, equals Δ_H; in this case, such a measure is unique up to a positive multiple.

When G is abelian, or G is semisimple and H discrete, etc., the hypothesis will be fulfilled. It is cases like these that will occupy us later.

§2. Local and global fields

Here and in subsequent sections we are following the approach of Cassels [1] (cf. also Weil [2, Part I], Lang [1, Chapter VII], Goldstein [1, Part 1]).

2.1 Classification theorem

By global field we mean either a number field (finite extension of $\mathbb{Q}$) or a function field (finite extension of $\mathbb{F}_q(t)$, t transcendental).

By local field we mean the completion of a global field with respect to an archimedean or discrete (always rank 1 for our purposes) nonarchimedean valuation. $\mathbb{Q}$ has the completions $\mathbb{R}$ and $\mathbb{Q}_p$ (for primes p in $\mathbb{Z}$) ; $\mathbb{F}_q(t)$ has completions (all nonarchimedean) isomorphic to the field $\mathbb{F}_q((t))$ of formal power series. To get all local fields we just take all finite extensions of the fields just named. (Finite separable extensions will actually suffice.) Some authors do not regard $\mathbb{R}$ or $\mathbb{C}$ as local fields. Also, some authors allow more general coefficients for function fields. However, our definitions are the appropriate ones in the present context, as the following well known theorem shows.

THEOREM. *Let K be a (non-discrete) locally compact topological field. Then K is a local field, in the above sense.*

Outline of proof.

(1) If $\alpha \in K^*$, multiplication by α is obviously an automorphism of the (additive) locally compact group K, so its module (see 1.2) is defined. We denote it $\mathrm{mod}_K(\alpha)$ and set $\mathrm{mod}_K(0) = 0$. This function $\mathrm{mod}_K : K \to \mathbb{R}^{\geqslant 0}$ is our candidate for a valuation on K.

(2) It must be seen that mod_K actually is a valuation (since square of absolute value occurs for $\mathbb{C}$, one must define "valuation" appropriately: cf. Cassels, §1). The multiplicative property is obvious. To see whether mod_K is archimedean or not one looks at the prime field ($\mathbb{Q}$ or $\mathbb{F}_p$) and studies the various possibilities.

(3) Local compactness of K implies completeness in the metric topology defined by mod_K; in particular, K contains a copy of the appropriate completion of its prime field ($\mathbb{R}$, $\mathbb{Q}_p$, $\mathbb{F}_p((t))$). Local compactness also forces K to be finite dimensional over this subfield, which finishes the proof.

Exercise. It will be seen shortly that local fields are indeed locally compact. Compute mod_K explicitly, e.g., for

$\mathbb{R}$: usual absolute value

$\mathbb{C}$: square of usual absolute value

$\mathbb{Q}_p$: $p^{-\mathrm{ord}_p(\alpha)}$ (see Appendix).

This singles out for each local field a normalized valuation, which we will always use.

Exercise. K a local field, mod_K as above, μ = Haar measure on K (additive group). Then $\frac{1}{\mathrm{mod}_K}\,\mu$ defines a Haar measure on K^*. (Cf. 1.1, example (6)).

2.2 Structure of local fields

Let K_v be a local field, as defined above, with valuation $|\ |_v$. We assume the reader is familiar with the basic algebraic properties of K_v; since the topological structure of $\mathbb{R}$, $\mathbb{C}$ is sufficiently known, we require v to be nonarchimedean. So K_v is a completion of a number field or function field at a "finite place"; for some facts about the former case (of main interest to us) see the Appendix below.

$O_v = \{\alpha \in K_v \mid |\alpha|_v \le 1\}$ is called the ring of local integers, and is a principal ideal domain (PID). It has a unique maximal ideal $P_v = \{\alpha \in K_v \mid |\alpha|_v < 1\}$, which is generated by an element π_v of the underlying global field K with maximum value < 1. The residue field $k_v = O_v/P_v$ is well known to be finite. (For $K_v = \mathbb{Q}_p$, these objects are $\mathbb{Z}_p$, $p\,\mathbb{Z}_p$, $\pm p$, $\mathbb{F}_p$.) In the following theorem we list those topological properties of local fields which will be of importance to us.

THEOREM. Let K_v be a local field, v nonarchimedean. Then O_v is an open (hence also closed) subgroup of the (additive) group K_v; O_v is the unique maximal compact subring of K_v; and K_v is a (non-discrete) locally compact field.

Proof sketch.

(1) The neighborhood $|\alpha|_v < \varepsilon$ $(\varepsilon > 0)$ of 0 in K_v always contains a sufficiently large power of the "prime" π_v, so the topology is non-discrete.

(2) P_v is obviously an open subgroup of K_v; since k_v is finite, P_v has finite index in O_v, which is therefore a finite union of open cosets.

(3) That O_v is compact follows from the fact that it is closed, along with the general principle (exercise): A subset of K_v is relatively compact (i.e., has compact closure) iff it is bounded relative to $|\ |_v$.

(4) Any subring of K_v containing an element α with $|\alpha|_v > 1$ (i.e., α not in O_v) contains all powers of α and hence is not bounded. In particular, O_v is the unique maximal compact subring of K_v.

(5) O_v is a compact neighborhood of the identity in K_v, so K_v is locally compact.

Since $\mathbb{R}$ and $\mathbb{C}$ are well known to be locally compact, we obtain the converse of Theorem 2.1: All local fields are (non-discrete) locally compact fields.

Appendix: Review of number fields and completions

(a) Besides the usual (archimedean) absolute value $|\alpha|_\infty = |\alpha|$, $\mathbb{Q}$ has a p-adic valuation for each prime p: If $\alpha \in \mathbb{Q}$, write

$$\alpha = p^{\mathrm{ord}_p(\alpha)} \frac{\beta}{\gamma}$$

where β, γ are integers relatively prime to p, and $\mathrm{ord}_p(\alpha) \in \mathbb{Z}$.
Define

$$|\alpha|_p = (\tfrac{1}{p})^{\mathrm{ord}_p(\alpha)} \quad , \quad |0|_p = 0 \quad .$$

(We could replace $1/p$ by anything strictly between 0 and 1, without changing the metric topology, but Haar measure yields this normalized choice: see 2.1.)

It is obvious that:

$$\mathbb{Z} = \{\alpha \in \mathbb{Q} \mid |\alpha|_p \leq 1 \text{ for all primes } p\}$$

and

$$\alpha \in \mathbb{Q}^* \text{ implies } |\alpha|_p \leq 1 \text{ for almost all } p,$$

hence $|\alpha|_p = 1$ for almost all p.

(b) Let K be a number field, of degree n over $\mathbb{Q}$. There are n distinct embeddings of K into $\mathbb{C}$, r of them <u>real</u> (with image in $\mathbb{R}$) and the remaining $2s$ <u>imaginary</u>, s pairs of complex conjugate embeddings. (In the literature, the usual notation is r_1, r_2 rather than r,s.) Denote these $\sigma_1,\ldots,\sigma_r$ and $\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s$, respectively. Combining each σ_i with ordinary absolute value yields an archimedean valuation on K, extending $|\ |_\infty$; each pair τ_i, $\overline{\tau}_i$, combined with the square of ordinary absolute value on $\mathbb{C}$, yields another such. The resulting $r+s$ valuations exhaust the extensions of $|\ |_\infty$ to K, and may be called <u>infinite</u> valuations.

On the other hand, each p-adic valuation $|\ |_p$ on $\mathbb{Q}$ extends in at least one (and at most n) ways to K; the resulting <u>finite</u> valuations $|\ |_v$ correspond precisely to the prime ideals dividing (p) in the ring O_K of elements of K integral over $\mathbb{Z}$, the <u>ring of integers of</u> K.

These exhaust the archimedean and discrete nonarchimedean valuations of K. It is well known that $O_K = \bigcap_{v \text{ finite}} O_v$ (defined below) $= \{\alpha \in K \mid |\alpha|_v \leq 1$ for all finite $v\}$. Moreover, if $x \in K^*$, $|\alpha|_v \leq 1$ for almost all v (hence $|\alpha|_v = 1$ for almost all v).

(c) K (as above) has an integral basis over $\mathbb{Q}$, i.e., a basis $\{\omega_1, \ldots, \omega_n\}$ consisting of elements of O_K, such that $O_K = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$. (O_K is a free $\mathbb{Z}$-module of rank n, as are all fractional ideals $\neq 0$ in K.) With notation as above, the <u>discriminant</u> D_K of K is defined to be the square of

$$\det \begin{pmatrix} \sigma_1\omega_1 & \cdots & \sigma_r\omega & \tau_1\omega_1 \cdots & \tau_s\omega_1 & \bar{\tau}_1\omega_1 & \cdots & \bar{\tau}_s\omega_1 \\ \vdots & & & & & \vdots & & \\ \sigma_1\omega_n & \cdots & \sigma_r\omega_n & \tau_1\omega_n \cdots & \tau_s\omega_n & \bar{\tau}_1\omega_n & \cdots & \bar{\tau}_s\omega_n \end{pmatrix}$$

This number is a (positive or negative) rational integer, <u>nonzero</u> because $K/\mathbb{Q}$ is separable (cf. Cassels, Appendix B). (<u>Exercise</u>. The sign of D_K is $(-1)^s$.)

(d) K as above. If v is infinite, and we complete K in the metric topology of $|\ |_v$, we get $K_v = \mathbb{R}$ (v real) or $\mathbb{C}$(v imaginary). Moreover, $|\ |_v$ extends uniquely to K_v. Similarly, if v is finite we get a completion K_v (written $\mathbb{Q}_p$ for $K = \mathbb{Q}$, v = p-adic valuation). Let O_v = ring of local integers $= \{\alpha \in K_v \mid |\alpha|_v \leq 1\}$ and P_v = unique maximal ideal of $O_v = \{\alpha \in K_v \mid |\alpha_v| < 1\}$. For some $\pi_v \in O_K$ such that $|\pi_v|_v$ is maximal < 1 (π_v is unique up to units), $P_v = \pi_v O_v$. Moreover, $k_v = O_v/P_v$ is <u>finite</u> ($\cong \mathbb{F}_q$ if q is the "norm" of the prime in O_K which defines v). If Σ is a set of coset representatives for k_v, we can express $\alpha \in K_v$ uniquely as a Laurent series in powers of π_v with coefficients in Σ. (O_v consists of the ordinary power series.)

§3. Adele ring of a global field

In the 1930's Chevalley invented ideles (see §7 below); the additive version (adeles, or valuation vectors) is now widely used as well. Essentially, adeles provide a formalism for studying simultaneously all completions K_v (v finite or infinite) of a global field K, cf. Robert [1]. Tate's thesis, for example, exploits the possibilities of this formalism in the direction of Fourier analysis. In this section we merely introduce the basic notions, following Cassels [1, §13-14] (cf. also Tate [1, §3].)

3.1 Restricted topological products

Let X_λ $(\lambda \in \Lambda)$ be a collection of topological spaces, with open subsets Y_λ defined for almost all λ. Let X consist of all elements $(x_\lambda) \in \prod_{\lambda \in \Lambda} X_\lambda$ satisfying: $x_\lambda \in Y_\lambda$ for almost all λ. Topologize X by taking as basic open sets all products $\prod_{\lambda \in \Lambda} Z_\lambda$, where Z_λ is open in X_λ and $Z_\lambda = Y_\lambda$ for almost all λ. Call X (with this topology) the restricted topological product of the X_λ with respect to the Y_λ.

If $S \subset \Lambda$ is finite, and includes all λ for which Y_λ is not defined, let

$$X(S) = \prod_{\lambda \in S} X_\lambda \times \prod_{\lambda \notin S} Y_\lambda$$

with the product topology. A moment's thought shows that X is the union of the various open subsets $X(S)$, and indeed the topology of X is uniquely specified by the requirement that each $X(S)$ (with its product topology) be open in X. (X is the direct limit of the $X(S)$.)

LEMMA. *If X_λ is locally compact, and Y_λ is compact whenever defined, then X is locally compact.*