

Introduction to Arithmetic Groups

Preliminary version (February 27, 2003)

Send comments to dwitte@math.okstate.edu

Dave Witte Morris

DEPARTMENT OF MATHEMATICS
OKLAHOMA STATE UNIVERSITY
STILLWATER, OKLAHOMA 74078, USA

E-mail address: dwitte@math.okstate.edu, <http://www.math.okstate.edu/~dwitte>

Copyright © 2001, 2002, 2003 Dave Witte Morris. All rights reserved.

Permission to make copies of these lecture notes for educational or scientific use, including multiple copies for classroom or seminar teaching, is granted (without fee), provided that any fees charged for the copies are only sufficient to recover the reasonable copying costs, and that all copies include this title page and its copyright notice. Specific written permission of the author is required to reproduce or distribute this book (in whole or in part) for profit or commercial advantage.

Acknowledgments

In writing this book, I have benefited from the comments and suggestions of many colleagues, including Marc Burger, Indira Chatterjee, Alessandra Iozzi, Anders Karlsson, Sean Keel, Nicolas Monod, Hee Oh, Yehuda Shalom, Shmuel Weinberger, Barak Weiss, and Kevin Whyte.

I have also benefited greatly from discussions with Scot Adams, S.G. Dani, Benson Farb, G.A. Margulis, Gopal Prasad, M.S. Raghunathan, T. N. Venkataramana, and Robert J. Zimmer. They (and others) may note that some of the comments they made to me over the years have been reproduced here almost verbatim.

I would like to thank É. Ghys, D. Gaboriau and the other members of the École Normale Supérieure de Lyon for the stimulating conversations and invitation to speak that were the impetus for this work, and B. Farb, A. Eskin and the other members of the University of Chicago mathematics department for encouraging me to write this introduction, for the opportunity to lecture from it, and for providing a stimulating audience.

I am grateful to ENS–Lyon, the University of Bielefeld, the Isaac Newton Institute for Mathematical Sciences, and the Tata Institute for Fundamental Research for their warm hospitality while various of the chapters were being written. The preparation of this manuscript was partially supported by a research grant from the National Science Foundation (DMS–0100438).

List of Chapters

(Only 1–11, 25, and App. I are available so far)

Acknowledgments	iii
Chapter 1. What is a Locally Symmetric Space?	1
Chapter 2. Geometer's Introduction to $\mathbb{R}$ -rank and $\mathbb{Q}$ -rank	14
Chapter 3. Introduction to Semisimple Lie Groups	19
Chapter 4. Some of the Structure of Semisimple Lie Groups	32
Chapter 5. Basic Properties of Lattices	44
Chapter 6. What is an Arithmetic Lattice?	68
Chapter 7. Examples of Lattices	88
Chapter 8. Real Rank	112
Chapter 9. $\mathbb{Q}$ -Rank	121
Chapter 10. Arithmetic Lattices in Classical Groups	135
Chapter 11. Central division algebras over number fields	164
Chapter 12. Galois Cohomology and $\mathbb{Q}$ -Forms	173
Chapter 13. Lattices of Extremal $\mathbb{Q}$ -rank	175
Chapter 14. Fundamental Domain for $G/G_{\mathbb{Z}}$	179
Chapter 15. Arithmetic Subgroups are Lattices	181
Chapter 16. Zassenhaus Neighborhood	182
Chapter 17. Rigidity, Strong Rigidity and Superrigidity	183
Chapter 18. Root Systems	189

Chapter 19.	Basic Properties of Semisimple Algebraic k -Groups	193
Chapter 20.	Amenability vs. Kazhdan's Property (T)	194
Chapter 21.	Introduction to Ergodic Theory	200
Chapter 22.	Proof of the Margulis Superrigidity Theorem	204
Chapter 23.	Normal Subgroups of Higher-Rank Lattices	207
Chapter 24.	Cohomology of Arithmetic Lattices	216
Chapter 25.	Actions on the Circle	218
Appendix I.	Assumed Background	250
	List of Notation	262
	Index	263

Contents

Acknowledgments	iii
Chapter 1. What is a Locally Symmetric Space?	1
§1A. Symmetric spaces	1
§1B. How to construct a symmetric space	3
§1C. Locally symmetric spaces	6
§1D. Notes	9
§1E. References	10
Exercises	10
Chapter 2. Geometer's Introduction to $\mathbb{R}$ -rank and $\mathbb{Q}$ -rank	14
§2A. Rank and real rank	14
§2B. $\mathbb{Q}$ -rank	15
§2C. Notes	18
§2D. References	18
Exercises	18
Chapter 3. Introduction to Semisimple Lie Groups	19
§3A. The standing assumptions	19
§3B. Isogenies	19
§3C. What is a semisimple Lie group?	20
§3D. The simple Lie groups	22
§3E. Which classical groups are isogenous?	24
§3F. Notes	28
§3G. References	28
Exercises	28
Chapter 4. Some of the Structure of Semisimple Lie Groups	32
§4A. G is almost Zariski closed	32
§4B. Real Jordan decomposition	34

§4C.	Jacobson-Morosov Lemma	35
§4D.	Maximal compact subgroups and the Iwasawa decomposition	35
§4E.	Cartan involution and Cartan decomposition	36
§4F.	The image of the exponential map	36
§4G.	Parabolic subgroups	37
§4H.	The normalizer of G	39
§4I.	Fundamental group and center of G	40
§4J.	Notes	40
§4K.	References	40
	Exercises	41
Chapter 5.	Basic Properties of Lattices	44
§5A.	Definition	44
§5B.	Commensurability	46
§5C.	Irreducible lattices	47
§5D.	Unbounded subsets of $\Gamma \backslash G$	48
§5E.	Intersection of Γ with other subgroups of G	50
§5F.	Borel Density Theorem and some consequences	51
§5G.	Proof of the Borel Density Theorem	52
§5H.	Γ is finitely presented	54
§5I.	Γ has a torsion-free subgroup of finite index	56
§5J.	Γ has a nonabelian free subgroup	59
§5K.	Notes	62
§5L.	References	63
	Exercises	63
Chapter 6.	What is an Arithmetic Lattice?	68
§6A.	Definition of arithmetic lattices	68
§6B.	Margulis Arithmeticity Theorem	71
§6C.	Commensurability criterion for arithmeticity	73
§6D.	Why superrigidity implies arithmeticity	73
§6E.	Unipotent elements of $G_{\mathbb{Z}}$: the Godement Compactness Criterion	75
§6F.	How to make an arithmetic lattice	76
§6G.	Restriction of scalars	78
§6H.	Notes	83
§6I.	References	83
	Exercises	84
Chapter 7.	Examples of Lattices	88
§7A.	Arithmetic lattices in $\mathrm{SL}(2, \mathbb{R})$	88
§7B.	Teichmüller space and moduli space of lattices in $\mathrm{SL}(2, \mathbb{R})$	91
§7C.	Arithmetic lattices in $\mathrm{SO}(1, n)$	92

§7D.	Some nonarithmetic lattices in $\mathrm{SO}(1, n)$	94
§7E.	Noncocompact lattices in $\mathrm{SL}(3, \mathbb{R})$	101
§7F.	Cocompact lattices in $\mathrm{SL}(3, \mathbb{R})$	103
§7G.	Lattices in $\mathrm{SL}(n, \mathbb{R})$	106
§7H.	Quaternion algebras over a field F	107
§7I.	Notes	108
§7J.	References	108
	Exercises	108
Chapter 8.	Real Rank	112
§8A.	$\mathbb{R}$ -split tori	112
§8B.	Definition of real rank	113
§8C.	Relation to geometry	114
§8D.	Parabolic subgroups	115
§8E.	Groups of real rank zero	115
§8F.	Groups of real rank one	116
§8G.	Groups of higher real rank	118
§8H.	Notes	120
§8I.	References	120
	Exercises	120
Chapter 9.	$\mathbb{Q}$ -Rank	121
§9A.	$\mathbb{Q}$ -split tori	121
§9B.	$\mathbb{Q}$ -rank of an arithmetic lattice	122
§9C.	Isogenies over $\mathbb{Q}$	124
§9D.	$\mathbb{Q}$ -rank of any lattice	125
§9E.	The possible $\mathbb{Q}$ -ranks	125
§9F.	Lattices of $\mathbb{Q}$ -rank zero	126
§9G.	Lattices of $\mathbb{Q}$ -rank one	128
§9H.	Lattices of higher $\mathbb{Q}$ -rank	128
§9I.	Parabolic $\mathbb{Q}$ -subgroups	129
§9J.	The large-scale geometry of $\Gamma \backslash X$	131
§9K.	Notes	133
§9L.	References	133
	Exercises	134
Chapter 10.	Arithmetic Lattices in Classical Groups	135
§10A.	Complexification of G	135
§10B.	Calculating the complexification of G	137
§10C.	Cocompact lattices in some classical groups	139
§10D.	Isotypic classical groups have irreducible lattices	141
§10E.	What is a central division algebra over F ?	146

§10F. What is an absolutely simple group?	148
§10G. Absolutely simple classical groups	149
§10H. The Lie group corresponding to each F -group	151
§10I. The arithmetic lattices in classical groups	152
§10J. What are the possible Hermitian forms?	154
§10K. Notes	160
§10L. References	160
Exercises	160
Chapter 11. Central division algebras over number fields	164
§11A. How to construct central division algebras over number fields	164
§11B. The Brauer group	167
§11C. Division algebras are cyclic	169
§11D. Simple algebras are matrix algebras	170
§11E. Cohomological approach to division algebras	171
§11F. Notes	172
§11G. References	172
Exercises	172
Chapter 12. Galois Cohomology and $\mathbb{Q}$ -Forms	173
§12A. Using Galois Cohomology to find the F -forms of classical groups	173
§12B. The Tits Classification	174
§12C. Inner forms and outer forms	174
§12D. Quasi-split groups	174
§12E. References	174
Exercises	174
Chapter 13. Lattices of Extremal $\mathbb{Q}$ -rank	175
§13A. Construction using Galois cohomology	175
§13B. Explicit construction of the Lie algebra	176
§13C. Notes	178
§13D. References	178
Exercises	178
Chapter 14. Fundamental Domain for $G/G_{\mathbb{Z}}$	179
§14A. Godement Criterion for compactness of $H/H_{\mathbb{Z}}$	179
§14B. Dirichlet's Unit Theorem	179
§14C. Reduction theory: a weak fundamental domain for $G/G_{\mathbb{Z}}$	179
§14D. Large-scale geometry of $\Gamma \backslash X$	180
§14E. References	180
Exercises	180
Chapter 15. Arithmetic Subgroups are Lattices	181

§15A. $G/G_{\mathbb{Z}}$ has finite volume	181
§15B. Divergent sequences in $G/G_{\mathbb{Z}}$	181
§15C. Proof of Godement's Criterion	181
§15D. References	181
Exercises	181
Chapter 16. Zassenhaus Neighborhood	182
§16A. Zassenhaus neighborhood	182
§16B. Lower bound on $\text{vol}(\Gamma \backslash G)$	182
§16C. Existence of maximal lattices	182
§16D. Noncocompact lattices have unipotent elements	182
§16E. Weak fundamental domain for G/Γ	182
§16F. References	182
Exercises	182
Chapter 17. Rigidity, Strong Rigidity and Superrigidity	183
§17A. Deformations of Γ	183
§17B. Representation Varieties	183
§17C. Mostow Rigidity Theorem	183
§17D. Proof of the Mostow Rigidity Theorem	184
§17E. Quasi-isometry rigidity	184
§17F. Margulis Superrigidity Theorem	185
§17G. Homomorphisms into compact groups	187
§17H. Geometric superrigidity	187
§17I. A nonarithmetic superrigid group	187
§17J. Notes	187
§17K. References	188
Chapter 18. Root Systems	189
§18A. Roots of complex Lie algebras	189
§18B. Definition of roots	189
§18C. Classification of semisimple Lie algebras over $\mathbb{C}$	190
§18D. Dynkin diagrams	190
§18E. The root system BC_n	191
§18F. Real roots	191
§18G. $\mathbb{Q}$ -roots	191
§18H. Notes	192
§18I. References	192
Exercises	192
Chapter 19. Basic Properties of Semisimple Algebraic k -Groups	193
§19A. Kneser-Tits Conjecture	193
§19B. BN -pairs	193

§19C. Tits building	193
§19D. Normal subgroups of $G_{\mathbb{Q}}$	193
§19E. Connected unipotent subgroups are Zariski closed	193
§19F. References	193
Exercises	193
Chapter 20. Amenability vs. Kazhdan's Property (T)	194
§20A. Amenability	194
§20B. Kazhdan's property (T)	196
§20C. Notes	198
§20D. References	199
Chapter 21. Introduction to Ergodic Theory	200
§21A. Ergodicity vs. tameness	200
§21B. Ergodic components	200
§21C. Mean Ergodic Theorem	200
§21D. Pointwise Ergodic Theorem	200
§21E. Multiplicative Ergodic Theorem	200
§21F. Moore Ergodicity Theorem	200
§21G. Ergodic actions as a generalization of closed subgroups	203
§21H. Cocycle Superrigidity Theorem	203
§21I. Entropy and topological entropy	203
§21J. Lyapunov exponents and Bernoulli shifts	203
§21K. References	203
Exercises	203
Chapter 22. Proof of the Margulis Superrigidity Theorem	204
§22A. The Zariski closure of $\rho(\Gamma)$	204
§22B. Measurable equivariant map on the boundary	204
§22C. Action on the space of probability measures	205
§22D. Stabilizers of probability measures	205
§22E. Actions on function spaces	205
§22F. Equivariant maps are rational	205
§22G. Notes	206
Chapter 23. Normal Subgroups of Higher-Rank Lattices	207
§23A. Γ is almost simple	207
§23B. Γ -equivariant measurable quotients of G/P	208
§23C. Unipotent generators	208
§23D. The Congruence Subgroup Property	211
§23E. Lattices with no torsion-free subgroup of finite index	212
§23F. Bounded generation	212
§23G. Almost-normal subgroups	213

§23H. Conjugation-invariant subsemigroups	214
§23I. Counterexamples in real rank one	214
§23J. Notes	214
§23K. References	214
Exercises	215
Chapter 24. Cohomology of Arithmetic Lattices	216
§24A. Cohomology	216
§24B. Hodge theory and deRham cohomology	216
§24C. Cohomology vanishing for higher-rank lattices	216
§24D. Relation of cohomology to rigidity	216
§24E. Rigidity and arithmeticity	216
§24F. Hermitian symmetric spaces and infinite fundamental groups	216
§24G. Lattices in semisimple groups with infinite center	217
§24H. Bounded cohomology	217
§24I. Notes	217
Chapter 25. Actions on the Circle	218
§25A. Overview	218
§25B. Algebraic reformulation of the conjecture	220
§25C. Continuous actions on the circle	221
§25D. Smooth actions of Kazhdan groups on the circle	224
§25E. The Reeb-Thurston Stability Theorem	227
§25F. Existence of a finite orbit	228
§25G. Complements	233
§25H. Notes	240
§25I. References	241
Exercises	243
Appendix I. Assumed Background	250
§I.A. Riemannian manifolds	250
§I.B. Geodesics	250
§I.C. Lie groups	252
§I.D. Galois theory and field extensions	256
§I.E. Algebraic numbers and transcendental numbers	257
§I.F. Polynomial rings and the Nullstellensatz	258
§I.G. Eisenstein Criterion	259
§I.H. Notes	260
§I.I. References	260
Exercises	261
List of Notation	262
Index	263

What is a Locally Symmetric Space?

In this chapter, we give a geometric introduction to the notion of a symmetric space or a locally symmetric space, and explain the central role played by simple Lie groups and their lattice subgroups. This material is not a prerequisite for reading any of the later chapters, except Chap. 2; it is intended to provide a geometric motivation for the study of lattices in semisimple Lie groups, which is the main topic of the rest of the book.

1A. Symmetric spaces

The nicest Riemannian manifolds are homogeneous. This means that every point looks exactly like every other point.

(1.1) **Definition.** A Riemannian manifold X is a *homogeneous space* if its isometry group $\text{Isom}(X)$ acts transitively. That is, for every $x, y \in X$, there is an isometry ϕ of X , such that $\phi(x) = y$.

(1.2) **Example.** Here are some elementary examples of (simply connected) homogeneous spaces.

- The round sphere $S^n = \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}$. Rotations are the only orientation-preserving isometries of S^n , so $\text{Isom}(S^n)^\circ = \text{SO}(n+1)$. Any point on S^n can be rotated to any other point, so S^n is homogeneous.
- Euclidean space $\mathbb{R}^n$. Any orientation-preserving isometry of $\mathbb{R}^n$ is a combination of a translation and a rotation, so $\text{Isom}(\mathbb{R}^n)^\circ = \text{SO}(n) \ltimes \mathbb{R}^n$. Any point in $\mathbb{R}^n$ can be translated to any other point, so $\mathbb{R}^n$ is homogeneous.
- The hyperbolic plane $\mathfrak{H}^2 = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$, where the inner product on $T_z \mathfrak{H}^2$ is given by

$$\langle u \mid v \rangle_{\mathfrak{H}^2} = \frac{1}{4(\text{Im } z)^2} \langle u \mid v \rangle_{\mathbb{R}^2}.$$

One may show that $\text{Isom}(\mathfrak{H}^2)^\circ$ is isomorphic to $\text{PSL}(2, \mathbb{R})^\circ = \text{SL}(2, \mathbb{R})/\{\pm 1\}$, by noting that $\text{SL}(2, \mathbb{R})$ acts on $\mathfrak{H}^2$ by linear-fractional transformations $z \mapsto (az + b)/(cz + d)$, and confirming, by calculation, that these linear-fractional transformations preserve the hyperbolic metric.

- Hyperbolic space $\mathfrak{H}^n = \{x \in \mathbb{R}^n \mid x_n > 0\}$, where the inner product on $T_x \mathfrak{H}^n$ is given by

$$\langle u \mid v \rangle_{\mathfrak{H}^n} = \frac{1}{4x_n^2} \langle u \mid v \rangle_{\mathbb{R}^n}.$$

It is not difficult to see that $\mathfrak{H}^n$ is homogeneous (see Exer. 1:1). One can also show that that the group $\text{Isom}(\mathfrak{H}^n)^\circ$ is isomorphic to $\text{SO}(1, n)^\circ$ (see Exer. 1:4).

- A cartesian product of any combination of the above (see Exer. 1:6).

(1.3) **Definition.** Let $\phi: X \rightarrow X$.

- We may say that ϕ is *involutive* (or that ϕ is an *involution*) if $\phi^2 = \text{Id}$.
- A *fixed point* of ϕ is a point $p \in X$, such that $\phi(p) = p$.
- A fixed point p of ϕ is *isolated* if there is a neighborhood U of p , such that p is the only fixed point of ϕ that is contained in U .

Besides an isometry taking x to y , each of the above spaces also has a nice involutive isometry that fixes x .

- Define $\phi_1: S^n \rightarrow S^n$ by

$$\phi_1(x_1, \dots, x_{n+1}) = (-x_1, \dots, -x_n, x_{n+1}).$$

Then ϕ_1 is an isometry of S^n , such that ϕ_1 has only two fixed points: namely, e_{n+1} and $-e_{n+1}$, where $e_{n+1} = (0, 0, \dots, 0, 1)$. Thus, e_{n+1} is an isolated fixed point of ϕ_1 .

- Define $\phi_2: \mathbb{R}^n \rightarrow \mathbb{R}^n$ by $\phi_2(x) = -x$. Then ϕ_2 is an isometry of $\mathbb{R}^n$, such that 0 is the only fixed point of ϕ_1 .
- Define $\phi_3: \mathfrak{H}^2 \rightarrow \mathfrak{H}^2$ by $\phi_3(z) = -1/z$. Then i is the only fixed point of ϕ_3 .
- There are involutive isometries of $\mathfrak{H}^n$ that have a unique fixed point (see Exer. 1:3), but they are somewhat difficult to describe in the upper-half-space model that we are using.

The existence of such an isometry is the additional condition that is required to be a symmetric space.

(1.4) **Definition.** A Riemannian manifold X is a *symmetric space* if

- 1) X is connected;
- 2) X is homogeneous; and
- 3) there is an involutive isometry ϕ of X , such that ϕ has at least one isolated fixed point.

(1.5) **Remark.** If X is a symmetric space, then all points of X are essentially the same, so, for each $x \in X$ (not only for *some* $x \in X$), there is an isometry ϕ of X , such that $\phi^2 = \text{Id}$ and x is an isolated fixed point of ϕ (see Exer. 1:9). Conversely, if Condition (3) is replaced with this stronger assumption, then Condition (2) can be omitted (see Exer. 1:10).

We constructed examples of involutive isometries of S^n , $\mathbb{R}^n$, and $\mathfrak{H}^n$ that have an isolated fixed point. The following proposition shows that no choice was involved: the involutive isometry with a given isolated fixed point p is unique, if it exists. Furthermore, in the exponential coordinates at p , the involution must simply be the map $x \mapsto -x$.

(1.6) **Proposition.** Suppose ϕ is an involutive isometry of a Riemannian manifold X , and suppose p is an isolated fixed point of ϕ . Then

- 1) $d\phi_p = -\text{Id}$; and
- 2) for every geodesic γ with $\gamma(0) = p$, we have $\phi(\gamma(t)) = \gamma(-t)$, for all $t \in \mathbb{R}$.

Proof. (1) From the Chain Rule, and the fact that $\phi(p) = p$, we have

$$d(\phi^2)_p = d\phi_{\phi(p)} \circ d\phi_p = (d\phi_p)^2.$$

Also, because $\phi^2 = \text{Id}$, we know that $d(\phi^2)_p = d\text{Id}_p = \text{Id}$. We conclude that $(d\phi_p)^2 = \text{Id}$; thus, the linear transformation $d\phi_p: T_pX \rightarrow T_pX$ satisfies the polynomial equation $x^2 - 1 = 0$.

Suppose $d\phi_p \neq -\text{Id}$. (This will lead to a contradiction.) Since the polynomial $x^2 - 1$ has no repeated roots, we know that $d\phi_p$ is diagonalizable. Furthermore, because 1 and -1 are the only roots of $x^2 - 1$, we know that 1 and -1 are the only possible eigenvalues of $d\phi_p$. Thus, because $d\phi_p \neq -\text{Id}$, we conclude that 1 is an eigenvalue; so we may choose some nonzero $v \in T_pX$, such that $d\phi_p(v) = v$. Let γ be the geodesic with $\gamma(0) = p$ and $\gamma'(0) = v$. Then, because ϕ is an isometry, we know that $\phi \circ \gamma$ is also a geodesic. We have

$$(\phi \circ \gamma)(0) = \phi(\gamma(0)) = \phi(p) = p = \gamma(0)$$

and

$$(\phi \circ \gamma)'(0) = d\phi_{\gamma(0)}(\gamma'(0)) = d\phi_p(v) = v = \gamma'(0).$$

Since a geodesic is uniquely determined by prescribing its initial position and its initial velocity, we conclude that $\phi \circ \gamma = \gamma$. Therefore, $\phi(\gamma(t)) = \gamma(t)$, so $\gamma(t)$ is a fixed point of ϕ , for every t . This contradicts the fact that the fixed point $p = \gamma(0)$ is isolated.

(2) Define $\bar{\gamma}(t) = \gamma(-t)$, so $\bar{\gamma}$ is a geodesic. Because ϕ is an isometry, we know that $\phi \circ \gamma$ is also a geodesic. We have

$$(\phi \circ \gamma)(0) = \phi(\gamma(0)) = \phi(p) = p = \bar{\gamma}(0)$$

and, from (1),

$$(\phi \circ \gamma)'(0) = d\phi_{\gamma(0)}(\gamma'(0)) = -\gamma'(0) = \bar{\gamma}'(0).$$

Since a geodesic is uniquely determined by prescribing its initial position and its initial velocity, we conclude that $\phi \circ \gamma = \bar{\gamma}$, as desired. $\square$

(1.7) **Definition.** Let M be a Riemannian manifold, and let $p \in M$. Fix a star-shaped, symmetric neighborhood V of 0 in T_pM , such that the exponential map $\exp_p$ maps V diffeomorphically onto a neighborhood U of p in M (see I.8). The *geodesic symmetry* at p is the diffeomorphism τ of U defined by

$$\tau(\exp_p(v)) = \exp_p(-v),$$

for all $v \in V$.

In other words, for each geodesic γ in M , such that $\gamma(0) = p$, and for all $t \in \mathbb{R}$, such that $t\gamma'(0) \in V$, we have $\tau(\gamma(t)) = \gamma(-t)$.

(1.8) **Note.** The geodesic symmetry τ is a local diffeomorphism, but, for most manifolds M , it is *not* a local isometry (cf. 1.18).

In this terminology, the preceding proposition shows that if an involutive isometry ϕ has a certain point p as an isolated fixed point, then, locally, ϕ must agree with the geodesic symmetry at p . This has the following easy consequence, which is the motivation for the term *symmetric space*.

(1.9) **Corollary.** A connected Riemannian manifold M is a symmetric space if and only if, for each $p \in M$, the geodesic symmetry at p extends to an isometry of M .

1B. How to construct a symmetric space

In this section, we describe how Lie groups are used to construct symmetric spaces. Let us begin by recalling the well-known group-theoretic structure of any homogeneous space.

Suppose X is a connected homogeneous space, and let $G = \text{Isom}(X)^\circ$. Because $\text{Isom}(X)$ is transitive on X , and X is connected, we see that G is transitive on X (see Exer. 1:12), so we may

identify X with the coset space G/K , where K is the stabilizer of some point in X . Note that K is compact (see Exer. 1:13).

Conversely, if K is any compact subgroup of any Lie group G , then there is a G -invariant Riemannian metric on G/K (see Exer. 1:15), so G/K (with this metric) is a homogeneous space. (For any closed subgroup H of G , the group G acts transitively on the manifold G/H , by diffeomorphisms. However, when H is not compact, G usually does not act by isometries of any Riemannian metric on G/H , so there is no reason to expect G/H to be a homogeneous space in the sense of Defn. 1.1.)

(1.10) **Example.**

- 1) For $X = S^n$, we have $G = \mathrm{SO}(n+1)$, and we may let $K = \mathrm{Stab}_G(e_{n+1}) = \mathrm{SO}(n)$, so $S^n = \mathrm{SO}(n+1)/\mathrm{SO}(n)$. Note that, letting σ be the diagonal matrix

$$\sigma = \mathrm{diag}(-1, -1, \dots, -1, 1),$$

we have $\sigma^2 = \mathrm{Id}$, and $K = C_G(\sigma)$ is the centralizer of σ in G .

- 2) For $X = \mathbb{R}^n$, we have $G = \mathrm{SO}(n) \ltimes \mathbb{R}^n$, and we may let $K = \mathrm{Stab}_G(0) = \mathrm{SO}(n)$, so $\mathbb{R}^n = (\mathrm{SO}(n) \ltimes \mathbb{R}^n)/\mathrm{SO}(n)$. Note that the map $\sigma: (k, v) \mapsto (k, -v)$ is an automorphism of G , such that $\sigma^2 = \mathrm{Id}$, and

$$C_G(\sigma) = \{g \in G \mid \sigma(g) = g\} = K.$$

- 3) For $X = \mathfrak{H}^2$, we have $G \approx \mathrm{SL}(2, \mathbb{R})$, and we may let $K = \mathrm{Stab}_G(i) \approx \mathrm{SO}(2)$, so $\mathfrak{H}^2 = \mathrm{SL}(2, \mathbb{R})/\mathrm{SO}(2)$.
- 4) For $X = \mathfrak{H}^n$, we have $G = \mathrm{SO}(1, n)^\circ$, and we may take $K = \mathrm{SO}(n)$ (see Exer. 1:5). Note that, letting σ be the diagonal matrix $(1, -1, -1, \dots, -1)$, we have $\sigma^2 = \mathrm{Id}$, and $K = C_G(\sigma)$.

Thus, in each of these cases, there is an automorphism σ of G , such that K is the centralizer of σ . The following proposition shows, in general, that a slightly weaker condition makes G/K symmetric, not just homogeneous.

(1.11) **Proposition.** *Let*

- G be a connected Lie group;
- K be a compact subgroup of G ; and
- σ be an involutive automorphism of G , such that K is an open subgroup of $C_G(\sigma)$.

Then G/K can be given the structure of a symmetric space, such that the map $\tau(gK) = \sigma(g)K$ is an involutive isometry of G/K with eK as an isolated fixed point.

Proof. To simplify the proof slightly, let us assume that $K = C_G(\sigma)$ (see Exer. 1:16).

Because K is compact, we know there is a G -invariant Riemannian metric on G/K (see Exer. 1:15). Then, because $\langle \tau \rangle$ is finite, and normalizes G , it is not difficult to see that we may assume this metric is also τ -invariant (see Exer. 1:17). (This conclusion can also be reached by letting $G^+ = \langle \sigma \rangle \ltimes G$ and $K^+ = \langle \sigma \rangle \ltimes K$, so K^+ is a compact subgroup of G^+ , such that $G^+/K^+ = G/K$.) Thus, τ is an involutive isometry of G/K .

Suppose gK is a fixed point of τ , with $g \approx e$. Then $\sigma(g) \in gK$, so we may write $\sigma(g) = gk$, for some $k \in K$. Since σ centralizes k (and σ is an automorphism), we have

$$\sigma^2(g) = \sigma(\sigma(g)) = \sigma(gk) = \sigma(g)\sigma(k) = (gk)(k) = gk^2.$$

On the other hand, we know $\sigma^2(g) = g$ (because σ is involutive), so we conclude that $k^2 = e$.

Since $g \approx e$, and $\sigma(e) = e$, we have $\sigma(g) \approx g$, so $k = g^{-1}\sigma(g) \approx e$. Since $k^2 = e$, we conclude that $k = e$. (There is a neighborhood U of e in G , such that, for every $u \in U \setminus \{e\}$, we have $u^2 \neq e$.) Therefore $\sigma(g) = gk = ge = g$, so $g \in C_G(\sigma) = K$; thus, $gK = eK$. $\square$

Conversely, for any symmetric space X , there exist G , K , and σ as in Prop. 1.11, such that X is isometric to G/K (see Exer. 1:18).

(1.12) **Example.** Let $G = \mathrm{SL}(n, \mathbb{R})$, $K = \mathrm{SO}(n)$, and define $\sigma(g) = (g^{-1})^T$ (the transpose-inverse). Then $\sigma^2 = 1$ and $C_G(\sigma) = K$, so the theorem implies that G/K is a symmetric space. Let us describe this space somewhat more concretely.

Recall that any real symmetric matrix A can be diagonalized over $\mathbb{R}$. In particular, all of its eigenvalues are real. If all the eigenvalues of A are strictly positive, then we say that A is *positive definite*.

Let

$$X = \{ A \in \mathrm{SL}(n, \mathbb{R}) \mid A \text{ is symmetric and positive definite} \},$$

and define $\alpha: G \times X \rightarrow X$ by $\alpha(g, x) = gxg^T$. Then:

- a) α defines an action of G on X ; that is, we have $\alpha(gh, x) = \alpha(g, \alpha(h, x))$ for all $g, h \in G$ and $x \in X$.
- b) In this action, we have $K = \mathrm{Stab}_G(\mathrm{Id})$, so X may be identified with G/K .
- c) $T_{\mathrm{Id}}X = \{ u \in \mathrm{Mat}_{n \times n}(\mathbb{R}) \mid u \text{ is symmetric and } \mathrm{trace}(u) = 0 \}$. (By definition, we have $X \subset \mathrm{SL}(n, \mathbb{R})$. The condition $\mathrm{trace}(u) = 0$ comes from the restriction $\det(A) = 1$.)
- d) The inner product $\langle u \mid v \rangle = \mathrm{trace}(uv)$ on $T_{\mathrm{Id}}X$ is K -invariant, so it may be extended to a G -invariant Riemannian metric on X .
- e) The map $\tau: X \rightarrow X$, defined by $\tau(A) = A^{-1}$, is an involutive isometry of X , such that $\tau(\alpha(g, x)) = \sigma(g)\tau(x)$ for all $g \in G$ and $x \in X$.

(1.13) **Example.** Other examples of symmetric spaces are:

- $\mathrm{SL}(n, \mathbb{C})/\mathrm{SU}(n)$; and
- $\mathrm{SO}(p, q)^\circ/(\mathrm{SO}(p) \times \mathrm{SO}(q))$.

These are special cases of the following corollary of Prop. 1.11.

(1.14) **Definition.** A symmetric space X is *irreducible* if its universal cover is not isometric to any nontrivial product $X_1 \times X_2$.

(1.15) **Proposition.** Let G be a connected, noncompact, simple Lie group with finite center. Then G has a maximal compact subgroup K (which is unique up to conjugacy), and G/K is a simply connected, noncompact, irreducible symmetric space that has semi-negative curvature and is not flat.

Conversely, any noncompact, non-flat, irreducible symmetric space is of the form G/K , where G is a connected, noncompact, simple Lie group with trivial center, and K is a maximal compact subgroup of G .

(1.16) **Remark.** Let K be a compact subgroup of a connected, simple Lie group G with finite center, such that G/K is a symmetric space (cf. 1.11). The proposition shows that if G is not compact, then K must be a maximal compact subgroup of G , which is essentially unique.

On the other hand, if G is compact, then the subgroup K may not be unique, and may not be maximal. For example, both $\mathrm{SO}(n)/\mathrm{SO}(n-1)$ and $\mathrm{SO}(n)/\{e\}$ are symmetric spaces. The former

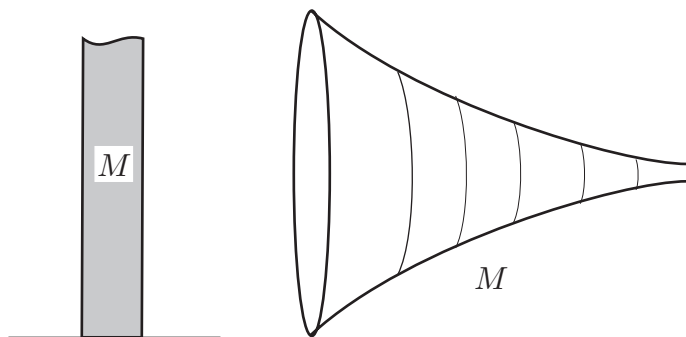


Figure 1.1. The (two-way infinite) cusp M .

is a round sphere, which has already been mentioned. The latter is a special case of the fact that every connected, compact Lie group is a symmetric space (see Exer. 1:21).

É. Cartan obtained a complete list of all the symmetric spaces (both compact and noncompact) by finding all of the simple Lie groups G , and determining which compact subgroups K can arise in Prop. 1.11.

1C. Locally symmetric spaces

The gist of the following definition is that a locally symmetric space is a Riemannian manifold that is locally isometric to a symmetric space; that is, every point has a neighborhood that is isometric to an open subset of some symmetric space.

(1.17) **Definition.** A (complete) Riemannian manifold M is *locally symmetric* if its universal cover is a symmetric space. In other words, there is a symmetric space X , and a group Γ of isometries of X , such that

- 1) Γ acts freely and properly discontinuously on X ; and
- 2) M is isometric to $\Gamma \backslash X$.

(1.18) **Remark.** In a symmetric space, the geodesic symmetry $\gamma(t) \mapsto \gamma(-t)$ at any point extends to an isometry of the entire manifold (see 1.9). In a locally symmetric space, the geodesic symmetry τ at any point is an isometry on its domain, but it may not be possible to extend τ to an isometry that is well-defined on the entire manifold; that is, the geodesic symmetry is only a *local* isometry. That is the origin of the term *locally symmetric*.

(1.19) **Example.** Define $g: \mathfrak{H}^2 \rightarrow \mathfrak{H}^2$ by $g(z) = z + 1$, let $\Gamma = \langle g \rangle$, and let $M = \Gamma \backslash \mathfrak{H}^2$. Then (obviously) M is locally symmetric.

However, M is not symmetric. We provide several different geometric proofs of this fact, in order to illustrate the important distinction between symmetric spaces and locally symmetric spaces. (It can also be proved group-theoretically (see Exer. 1:23).) The manifold M is a cusp (see Fig. 1.1).

- 1) Any point far out in the cusp lies on a short loop that is not null-homotopic, but points at the other end do not lie on such a loop. Thus, M is not homogeneous, so it cannot be symmetric.
- 2) The geodesic symmetry performs a 180° rotation. Thus, if it is a well-defined diffeomorphism of M , it must interchange the two ends of the cusp. However, one end is thin, and the other end is (very!) wide, so no isometry can interchange these two ends. Thus, the geodesic symmetry (at any point) is not an isometry, so M is not symmetric.

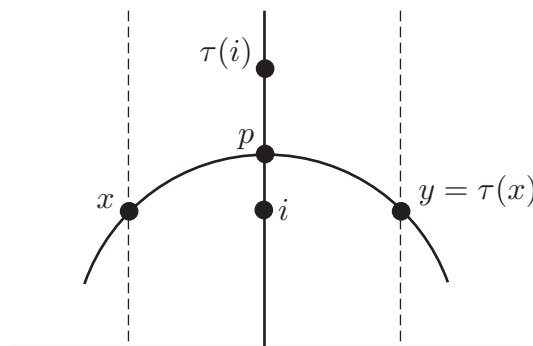


Figure 1.2. The geodesic symmetry τ at p .

- 3) Let us show, directly, that the geodesic symmetry at some point $p \in \mathfrak{H}^2$ does not factor through to a well-defined map on $\Gamma \backslash \mathfrak{H}^2 = M$.
- Let $x = -1 + i$ and $y = 1 + i$, and let $p \in i\mathbb{R}$ be the midpoint of the geodesic segment joining x and y (see Fig. 1.2).
 - Let τ be the geodesic symmetry at p . Then $\tau(x) = y = 1 + i$.
 - Because the imaginary axis is a geodesic, we have $\tau(i) = ai$, for some $a > 1$.
 - Now $i = x + 1 = g(x)$, so x and i represent the same point in M . However, $\tau(i) - \tau(x) = -1 + (a - 1)i$ is not an integer (it is not even real), so $\tau(x)$ and $\tau(i)$ do **not** represent the same point in M . Thus, τ does not factor through to a well-defined map on M .

(1.20) **Remark.**

- 1) Some authors do not require M to be complete in their definition of a locally symmetric space. This would allow the universal cover of M to be an open subset of a symmetric space, instead of the entire symmetric space.
- 2) A more intrinsic (but more advanced) definition is that a complete, connected Riemannian manifold M is *locally symmetric* if and only if the curvature tensor of M is invariant under all parallel translations, and M is complete.

Any complete, connected manifold of constant negative curvature is a locally symmetric space, for (after normalizing the curvature to be -1) the universal cover of such a manifold is $\mathfrak{H}^n$. As a generalization of this, we are interested in locally symmetric spaces M whose universal cover $\widetilde{M}$ is of *noncompact type*, with no flat factors; that is, such that each irreducible factor of $\widetilde{M}$ is noncompact (and not flat). From Prop. 1.15, we see, in this case, that M can be written in the form $M = \Gamma \backslash G/K$, where $G = G_1 \times \cdots \times G_n$ is a product of noncompact simple Lie groups, K is a maximal compact subgroup of G , and Γ is a discrete subgroup of G .

A topologist may like M to be compact, but it turns out that a very interesting theory is obtained by making the weaker assumption that M has finite volume. Thus, the subgroup Γ should be chosen so that $\Gamma \backslash G/K$ has finite volume. Because $\Gamma \backslash G$ is a principal K -bundle over $\Gamma \backslash G/K$, and K has finite measure, it is not difficult to see, from Fubini's Theorem, that $\Gamma \backslash G$ has finite volume (see Exer. 1:27). This leads to the following definition.

(1.21) **Definition.** A discrete subgroup Γ of G is a *lattice* if $\Gamma \backslash G$ has finite volume.

(As a special case, note that if Γ is discrete and $\Gamma \backslash G$ is compact, then Γ is a lattice in G , because any compact Riemannian manifold obviously has finite volume.)

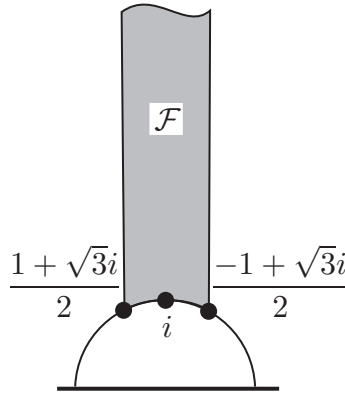


Figure 1.3. A fundamental domain $\mathcal{F}$ for $\mathrm{SL}(2, \mathbb{Z})$ in $\mathrm{SL}(2, \mathbb{R})$.

(1.22) **Example.** $\mathrm{SL}(2, \mathbb{Z})$ is a lattice in $\mathrm{SL}(2, \mathbb{R})$. To see this, let

$$(1.23) \quad \mathcal{F} = \{ z \in \mathfrak{H}^2 \mid |z| \geq 1 \text{ and } -1/2 \leq \operatorname{Re} z \leq 1/2 \}$$

(see Fig. 1.3). It is well known (though not obvious) that $\mathcal{F}$ is a fundamental domain for the action of $\mathrm{SL}(2, \mathbb{Z})$ on $\mathfrak{H}^2$ (see Exers. 1:28 and 1:29); it therefore suffices to show that $\mathcal{F}$ has finite volume, or, more precisely, finite hyperbolic area.

The hyperbolic area dA of an infinitesimal rectangle is the product of its hyperbolic length and its hyperbolic width. If the Euclidean length is dx and the Euclidean width is dy , and the rectangle is located at the point $x + iy$, then, by definition of the hyperbolic metric, the hyperbolic length is $(dx)/(2y)$ and the hyperbolic width is $(dy)/(2y)$. Thus,

$$dA = \frac{dx \, dy}{4y^2}.$$

Since $\operatorname{Im} z \geq \sqrt{3}/2$ for all $z \in \mathcal{F}$, we have

$$\operatorname{vol}(\mathcal{F}) = \int_{x+iy \in \mathcal{F}} dA \leq \int_{\sqrt{3}/2}^{\infty} \int_{-1/2}^{1/2} \frac{dx \, dy}{4y^2} = \frac{1}{4} \int_{\sqrt{3}/2}^{\infty} \frac{1}{y^2} \, dy < \infty.$$

Unfortunately, $\mathrm{SL}(2, \mathbb{Z}) \backslash \mathfrak{H}^2$ is not a locally symmetric space, because $\mathrm{SL}(2, \mathbb{Z})$ does not act freely on $\mathfrak{H}^2$ (so the quotient space is not a Riemannian manifold). However, there are finite-index subgroups of $\mathrm{SL}(2, \mathbb{Z})$ that do act freely (cf. 5.60), and these provide interesting locally symmetric spaces.

Calculations similar to (but more complicated than) Eg. 1.22 show:

- $\mathrm{SL}(n, \mathbb{Z})$ is a lattice in $\mathrm{SL}(n, \mathbb{R})$, and
- $\mathrm{SO}(p, q) \cap \mathrm{SL}(n, \mathbb{Z})$ is a lattice in $\mathrm{SO}(p, q)$.

As in the example of $\mathrm{SL}(2, \mathbb{Z}) \backslash \mathfrak{H}^2$, the hard part is to find a fundamental domain for $\Gamma \backslash G$ (or an appropriate approximation of a fundamental domain); then it is not difficult to see that its volume is finite. These are special cases of the following general theorem, which implies that every simple Lie group has a lattice.

(1.24) **Theorem** (Arithmetic subgroups are lattices). *Assume*

- $G = G_1 \times \cdots \times G_m$ is a product of simple Lie groups,
- $G \subset \mathrm{SL}(\ell, \mathbb{R})$, and
- $G \cap \mathrm{SL}(\ell, \mathbb{Q})$ is dense in G .

Then $G_{\mathbb{Z}} = G \cap \mathrm{SL}(\ell, \mathbb{Z})$ is a lattice in G .

Lattices constructed by taking the integer points of G in this way are said to be *arithmetic*. (For most simple Lie groups, these are the only lattices (see 6.21).) If ℓ is large, then there is more than one way to embed G in $\mathrm{SL}(\ell, \mathbb{R})$, and we will see that different embeddings can lead to quite different intersections with $\mathrm{SL}(\ell, \mathbb{Z})$. By taking an appropriate embedding of G in some $\mathrm{SL}(\ell, \mathbb{R})$, we will show that every noncompact, simple Lie group has a lattice Γ , such that $\Gamma \backslash G$ is compact. By taking a different embedding, we will construct a different lattice Γ' , such that $\Gamma' \backslash G$ is not compact.

We will also see some of the ways that the algebraic properties of Γ influence the geometry of the corresponding locally symmetric space M . The following important theorem implies that every geometric property of M is faithfully reflected in some group-theoretic property of Γ . For example, we will see how to tell, just by looking at Γ , whether M is compact or not. (One of the many algebraic characterizations is that M is compact if and only if there is a finite-index, torsion-free subgroup Γ' of Γ , such that the group cohomology $\mathcal{H}^n(\Gamma'; \mathbb{Z})$ is finitely generated as an abelian group, for each n .) More generally, we will see how group-theoretic properties of Γ influence the large-scale structure of M .

(1.25) **Theorem** (Mostow Rigidity Theorem). *Let M_1 and M_2 be finite-volume locally symmetric spaces, such that*

- $\pi_1(M_1) \cong \pi_1(M_2)$, and
- *the universal covers of M_1 and M_2 are neither compact, nor flat, nor reducible.*

Then (modulo a normalizing scalar multiple) M_1 is isometric to M_2 , unless $\dim M_1 = 2$.

In fact, any homotopy equivalence is homotopic to an isometry (modulo a normalizing scalar multiple).

(1.26) **Definition.** A locally symmetric space is *irreducible* if no *finite* cover of M can be written as a nontrivial cartesian product $M_1 \times M_2$.

It is important to note that the universal cover of an irreducible locally symmetric space need not be an irreducible symmetric space. In other words, there can be lattices in $G_1 \times \cdots \times G_n$ that are not of the form $\Gamma_1 \times \cdots \times \Gamma_n$ (see §10D).

Theorem 1.25 can be generalized to the case where only M_1 , rather than the universal cover of M_1 , is irreducible. However, one must strengthen the hypotheses correspondingly: it suffices to assume that no irreducible factor of M_1 or M_2 is either compact or flat or 2-dimensional. The conclusion is also weaker: rather than a single normalizing scalar, there can be a different scalar on each irreducible factor of the universal cover.

1D. Notes

Either of Helgason's books [Hel1, Hel2] is a good reference for the geometric material on symmetric spaces and locally symmetric spaces, the connection with simple Lie groups, and much more. Lattices are the main topic of Raghunathan's book [Rag].

Theorem 1.24 is a result of Borel and Harish-Chandra [B-HC]. We will prove it in Chap. 15.

Theorem 1.25 combines work of G.D. Mostow [Mos], G. Prasad [Pra], and G. A. Margulis [Mar]. We will discuss it in Chap. 17.

Example 1.22 appears in many number theory texts. Our hints for Exers. 1:28 and 1:29 are taken from [P-R, Prop. 4.4, pp. 181–182].

1E. References

- [B–HC] A. Borel and Harish-Chandra: Arithmetic subgroups of algebraic groups, *Ann. Math.* (2) 75 (1962) 485–535.
- [Hel1] S. Helgason: *Differential Geometry and Symmetric Spaces*. American Mathematical Society, Providence, RI, 1962. ISBN 0-8218-2735-9
- [Hel2] S. Helgason: *Differential Geometry, Lie Groups, and Symmetric Spaces*. Academic Press, New York, 1978. (A revised edition is coming soon from the American Mathematical Society.)
- [Mar] G. A. Margulis: Discrete groups of motions of manifolds of non-positive curvature, *Amer. Math. Soc. Translations*, 109 (1977) 33–45.
- [Mos] G. D. Mostow: *Strong Rigidity of Locally Symmetric Spaces*. Princeton Univ. Press, Princeton, 1973.
- [P–R] V. Platonov and A. Rapinchuk: *Algebraic Groups and Number Theory*. Academic Press, Boston, 1994.
- [Pra] G. Prasad: Strong rigidity of $\mathbb{Q}$ -rank 1 lattices, *Invent. Math.* 21 (1973) 255–286. MR 52:5875
- [Rag] M. S. Raghunathan: *Discrete Subgroups of Lie Groups*. Springer, Berlin Heidelberg New York, 1972.

Exercises

- 1:1) Show that $\mathfrak{H}^n$ is homogeneous. [*Hint*: For any $t \in \mathbb{R}^+$, the dilation $x \mapsto tx$ is an isometry of $\mathfrak{H}^n$. Also, for any $v \in \mathbb{R}^{n-1}$, the translation $x \mapsto x + v$ is an isometry of $\mathfrak{H}^n$.]
- 1:2) Let $B^n = \{x \in \mathbb{R}^n \mid \|x\| < 1\}$ be the open unit ball in $\mathbb{R}^n$, equip $T_x B^n$ with the inner product

$$\langle u \mid v \rangle_{B^n} = \frac{1}{(1 - \|x\|^2)^2} \langle u \mid v \rangle_{\mathbb{R}^n},$$

and let $e_n = (0, 0, \dots, 0, 1) \in \mathbb{R}^n$. Show that the map $\phi: B^n \rightarrow \mathfrak{H}^n$ defined by

$$\phi(x) = \frac{x + e_n}{\|x + e_n\|^2} - \frac{1}{2}e_n$$

is an isometry from B_n onto $\mathfrak{H}^n$. (In geometric terms, ϕ is obtained by composing a translation with the inversion centered at the south pole of B^n .)

- 1:3) Show that $x \mapsto -x$ is an isometry of B^n (with respect to the Riemannian metric $\langle \cdot \mid \cdot \rangle_{B^n}$).
- 1:4) For $u, v \in \mathbb{R}^{n+1}$, define

$$\langle u \mid v \rangle_{1,n} = u_0 v_0 - \sum_{j=1}^n u_j v_j.$$

(Note that, for convenience, we start our numbering of the coordinates at 0, rather than at 1.) Let

$$X_{1,n}^+ = \{x \in \mathbb{R}^{n+1} \mid \langle x \mid x \rangle_{1,n} = 1, x_0 > 0\},$$

so $X_{1,n}^+$ is one sheet of a 2-sheeted hyperboloid. Equip $T_x X_{1,n}^+$ with the inner product obtained by restricting $\langle \cdot \mid \cdot \rangle_{1,n}$ to this subspace.

- (a) Show that the bijection $\psi: B^n \rightarrow X_{1,n}^+$ defined by

$$\psi(x) = \frac{1}{1 - \|x\|^2}(1, x)$$

is an isometry. (Note that this implies that the restriction of $\langle \cdot | \cdot \rangle_{1,n}$ to $T_x X_{1,n}^+$ is positive definite, even though $\langle \cdot | \cdot \rangle_{1,n}$ is not positive definite on all of $\mathbb{R}^{n+1}$.)

- (b) Show $\mathrm{SO}(1, n)^\circ$ acts transitively on $X_{1,n}^+$ by isometries.

- 1:5) For $G = \mathrm{SO}(1, n)^\circ = \mathrm{Isom}(\mathfrak{H}^n)^\circ$, show there is some $p \in \mathfrak{H}^n$, such that $\mathrm{Stab}_G(p) = \mathrm{SO}(n)$. [Hint: This is easy in the hyperboloid model $X_{1,n}^+$.]
- 1:6) Show that if $X_1, X_2, \dots, X_n$ are homogeneous spaces, then the cartesian product $X_1 \times X_2 \times \dots \times X_n$ is also homogeneous.
- 1:7) Show that every homogeneous space is *geodesically complete*. That is, for every geodesic segment $\gamma: (-\epsilon, \epsilon) \rightarrow X$, there is a doubly-infinite geodesic $\bar{\gamma}: \mathbb{R} \rightarrow X$, such that $\bar{\gamma}(t) = \gamma(t)$ for all $t \in (-\epsilon, \epsilon)$.
- 1:8) Show that if $X_1, \dots, X_n$ are symmetric spaces, then the cartesian product $X_1 \times X_2 \times \dots \times X_n$ is also a symmetric space.
- 1:9) Show that if X is a symmetric space, then, for each $x \in X$, there is an isometry ϕ of X , such that $\phi^2 = \mathrm{Id}$ and x is an isolated fixed point of ϕ .
- 1:10) Let X be a connected Riemannian manifold, and assume, for each $x \in X$, that there is an isometry ϕ of X , such that $\phi^2 = \mathrm{Id}$ and x is an isolated fixed point of ϕ . Show that X is homogenous, and conclude that X is a symmetric space.
- 1:11) Show that the real projective space $\mathbb{R}P^n$ (with the metric that makes its universal cover a round sphere) has an involutive isometry ϕ , such that ϕ has both an isolated fixed point, and a fixed point that is not isolated. Is $\mathbb{R}P^n$ a symmetric space?
- 1:12) Suppose a topological group G acts transitively (and continuously) on a connected topological space M . Show that the identity component G° is transitive on M .
- 1:13) Let H be a group of isometries of a Riemannian manifold M , and assume that H has a fixed point. (That is, there is a point $p \in M$, such that, for all $h \in H$, we have $hp = p$.) Use Prop. I.17 to show that the closure of H in $\mathrm{Isom}(M)$ is compact.
- 1:14) Let K be a compact group, and let $\rho: K \rightarrow \mathrm{GL}(n, \mathbb{R})$ be a continuous homomorphism. Show that there is a K -invariant inner product $\langle \cdot | \cdot \rangle_K$ on $\mathbb{R}^n$; that is, such that

$$\langle \rho(k)u | \rho(k)v \rangle_K = \langle u | v \rangle_K$$

for all $k \in K$ and all $u, v \in \mathbb{R}^n$. [Hint: Define

$$\langle u | v \rangle_K = \int_K \langle \rho(k)u | \rho(k)v \rangle d\mu(k),$$

where μ is a Haar measure on K .]

- 1:15) Let K be a compact subgroup of a Lie group G . Use Exer. 1:14 to show that there is a G -invariant Riemannian metric on G/K . [Hint: A G -invariant Riemannian metric on G/K is determined by the inner product it assigns to $T_{eK}(G/K)$.]
- 1:16) Complete the proof of Prop. 1.11, by removing the simplifying assumption that $K = C_G(\sigma)$.
- 1:17) Let F be a finite group of diffeomorphisms (not necessarily isometries) of a Riemannian manifold $(M, \langle \cdot | \cdot \rangle_x)$. Define a new inner product $\langle \cdot | \cdot \rangle'_x$ on each tangent space $T_x M$ by

$$\langle u | v \rangle'_x = \sum_{f \in F} \langle df_x(u) | df_x(v) \rangle_{f(x)}.$$

- (a) Show that the Riemannian metric $\langle \cdot | \cdot \rangle'$ on M is F -invariant.
- (b) Show that if G is a group of isometries of $(M, \langle \cdot | \cdot \rangle_x)$, and G is normalized by F , then $\langle \cdot | \cdot \rangle'$ is G -invariant.
- 1:18) For any symmetric space X , show that there exist G , K , and σ as in Proposition 1.11, such that X is isometric to G/K . [Hint: Suppose τ is an involutive isometry of X with an isolated fixed point p . Let $G = \text{Isom}(X)^\circ$ and $K = \text{Stab}_G(p)$. Define $\sigma(g) = \tau g \tau$. Show $K \subset C_G(\sigma)$ and, using the fact that p is isolated, show that K contains the identity component of $C_G(\sigma)$. Hence K is an open subgroup of $C_G(\sigma)$.]
- 1:19) Verify assertions (a), (b), (c), (d), and (e) of Eg. 1.12.
- 1:20) Show that if X is a connected homogeneous space, then $\text{Isom}(X)$ has only finitely many connected components.
- 1:21) Show that if G is compact, then there is a G -invariant Riemannian metric on G that makes G a symmetric space. [Hint: The involutive isometry is $g \mapsto g^{-1}$.]
- 1:22) Let
- X be a simply connected symmetric space,
 - $\Gamma \backslash X$ be a locally symmetric space whose universal cover is X (so Γ is a discrete group of isometries that acts freely and properly discontinuously on X), and
 - τ be an isometry of X .
- Show that τ factors through to a well-defined map on $\Gamma \backslash X$, then τ normalizes Γ (that is, $\tau^{-1} \gamma \tau \in \Gamma$, for every $\gamma \in \Gamma$).
- 1:23) Define $g: \mathfrak{H}^2 \rightarrow \mathfrak{H}^2$ by $g(z) = z + 1$.
- (a) Show that the geodesic symmetry τ at i is given by $\tau(z) = -1/z$.
- (b) Show that τ does not normalize $\langle g \rangle$.
- (c) Conclude that τ does not factor through to a well-defined map on $\langle g \rangle \backslash \mathfrak{H}^2$.
- 1:24) Let
- X be a simply connected symmetric space, and
 - $\Gamma \backslash X$ be a locally symmetric space whose universal cover is X (so Γ is a discrete group of isometries that acts freely and properly discontinuously on X), and
 - τ be an isometry of X .
- Show that X is homogeneous if and only if the normalizer $N_G(\Gamma)$ is transitive on X , where $G = \text{Isom}(X)$.
- 1:25) Let $M = \Gamma \backslash G/K$ be a locally symmetric space, and assume that G has no compact factors. Show that if $N_G(\Gamma)/\Gamma$ is finite, then $\text{Isom}(M)$ is finite.
- 1:26) Show that if K is any compact subgroup of a Lie group G , then there is a unique (up to a scalar multiple) G -invariant Borel measure ν on G/K , such that $\nu(C) < \infty$, for every compact subset C of G/K .
- 1:27) Let
- K be a compact subgroup of a Lie group G , and
 - Γ be a discrete subgroup of G that acts freely on G/K .
- Show that $\Gamma \backslash G$ has finite volume if and only if $\Gamma \backslash G/K$ has finite volume.
- 1:28) Let $\Gamma = \text{SL}(2, \mathbb{Z})$, and define $\mathcal{F} \subset \mathfrak{H}^2$ as in (1.23). Show, for each $p \in \mathfrak{H}^2$, that there is some $\gamma \in \Gamma$ with $\gamma(p) \in \mathcal{F}$. [Hint: If $\text{Im } \gamma(p) \leq \text{Im } p$ for all $\gamma \in \Gamma$, and $-1/2 \leq \text{Re } p \leq 1/2$, then $p \in \mathcal{F}$.]
- 1:29) Let $\Gamma = \text{SL}(2, \mathbb{Z})$, and define $\mathcal{F} \subset \mathfrak{H}^2$ as in (1.23). Show, for $z, w \in \mathcal{F}$, that if there exists $\gamma \in \Gamma$ with $\gamma(z) = w$, then either $z = w$ or $z, w \in \partial \mathcal{F}$. [Hint: Assume $\text{Im } w \leq z$. Then

$|\gamma_{2,1}z + \gamma_{2,2}| \leq 1$. Hence $|\gamma_{2,1}| \in \{0, 1\}$. If $|\gamma_{2,1}| = 1$ and $\gamma_{2,2} \neq 0$, then $|\operatorname{Re} z| = 1/2$, so $z \in \partial\mathcal{F}$. If $|\gamma_{2,1}| = 1$ and $\gamma_{2,2} = 0$, then $w = (az - 1)/z$. Since $|\operatorname{Re}(1/z)| \leq |\operatorname{Re} z| \leq 1/2$, and $|\operatorname{Re} w| \leq 1/2$, we see that either $\operatorname{Re} z = 1/2$ or $w = -1/z$.]

Geometer's Introduction to $\mathbb{R}$ -rank and $\mathbb{Q}$ -rank

This chapter, like the previous one, is motivational. It is not a prerequisite for later chapters.

2A. Rank and real rank

Let X be a Riemannian symmetric space. (That is, for each point $p \in X$, there is an isometry ϕ of X , such that the derivative $d\phi_p$ is $-\text{Id}$ on the tangent space T_pX .) For example, X could be a Euclidean space $\mathbb{R}^n$, or a round sphere S^n , or a hyperbolic space $\mathfrak{H}^n$, or a product of any combination of these.

As is well known, the rank of X is a natural number that describes part of the geometry of X , namely, the dimension of a maximal flat.

(2.1) **Definition.** A *flat* in X is a connected, totally geodesic, flat submanifold in X .

(2.2) **Definition.** $\text{rank}(X)$ is the largest natural number r , such that X contains an r -dimensional flat.

Let us assume that X has no flat factors. (That is, the universal cover of X is not isometric to a product of the form $Y \times \mathbb{R}^n$. Mostly, we will be interested in the case where X also does not have any compact factors.)

Let $G = \text{Isom}(X)^\circ$. Thus, G acts transitively on X , and there is a compact subgroup K of G , such that $X = G/K$. Because X has no flat factors, G is a connected, semisimple, real Lie group with trivial center (see §1B). (We remark that G is isomorphic to a closed subgroup of $\text{SL}(\ell, \mathbb{R})$, for some ℓ .)

The real rank can be understood similarly. It is an invariant of G that is defined algebraically, but it has the following geometric interpretation.

(2.3) **Theorem.** $\mathbb{R}\text{-rank}(G)$ is the largest natural number r , such that X contains a closed, **simply connected**, r -dimensional flat.

For example, if X is compact, then every closed, totally geodesic, flat subspace of X must be a torus, not $\mathbb{R}^n$, so $\mathbb{R}\text{-rank}(G) = 0$. On the other hand, if X is not compact, then X has unbounded

geodesics (for example, if X is irreducible, then every geodesic goes to infinity), so $\mathbb{R}\text{-rank}(G) \geq 1$. Therefore:

$$\mathbb{R}\text{-rank}(G) = 0 \quad \Leftrightarrow \quad X \text{ is compact.}$$

Thus, there is a huge difference between $\mathbb{R}\text{-rank}(G) = 0$ and $\mathbb{R}\text{-rank}(G) > 0$, because no one would mistake a compact space for a noncompact one.

(2.4) **Remark.** We have $\mathbb{R}\text{-rank}(G) = \text{rank}(X)$ if and only if X has no compact factors.

There is also an important difference between $\mathbb{R}\text{-rank}(G) = 1$ and $\mathbb{R}\text{-rank}(G) > 1$. The following proposition is an important example of this.

(2.5) **Definition.** X is *two-point homogeneous* if, whenever (x_1, x_2) and (y_1, y_2) are two pairs of points in X with $d(x_1, x_2) = d(y_1, y_2)$, there is an isometry g of X with $g(x_1) = y_1$ and $g(x_2) = y_2$.

If $\mathbb{R}\text{-rank}(G) > 1$, then there exist maximal flats H_1 and H_2 that intersect nontrivially. On the other hand, there also exist some pairs x_1, x_2 , such that $\{x_1, x_2\}$ is not contained in the intersection of any two (distinct) maximal flats. This establishes one direction of the following result.

(2.6) **Proposition.** *Assume X is noncompact and irreducible. The symmetric space X is two-point homogeneous if and only if $\mathbb{R}\text{-rank}(G) = 1$.*

The following is an infinitesimal version of this result.

(2.7) **Proposition.** *Assume X is noncompact and irreducible. The group G acts transitively on the set of unit tangent vectors of X if and only if $\mathbb{R}\text{-rank}(G) = 1$.*

(2.8) **Corollary.** $\mathbb{R}\text{-rank}(\text{SO}(1, n)) = 1$.

Proof. For $G = \text{SO}(1, n)$, we have $X = \mathfrak{H}^n$. The stabilizer $\text{SO}(n)$ of a point in $\mathfrak{H}^n$ acts transitively on the unit tangent vectors at that point. So G acts transitively on the unit tangent vectors of X . $\square$

More generally, $\mathbb{R}\text{-rank}(\text{SO}(m, n)) = \min\{m, n\}$. Also, $\mathbb{R}\text{-rank}(\text{SL}(n, \mathbb{R})) = n - 1$. Although perhaps not clear geometrically, these will be very easy to calculate from the algebraic definition.

For every n , there is a difference between $\mathbb{R}\text{-rank}(G) = n$ and $\mathbb{R}\text{-rank}(G) > n$, but this difference is less important as n grows larger: the three main cases are $\mathbb{R}\text{-rank}(G) = 0$, $\mathbb{R}\text{-rank}(G) = 1$, and $\mathbb{R}\text{-rank}(G) \geq 2$. (This is analogous to the situation with smoothness assumptions: countless theorems require a function to be C^0 or C^1 or C^2 , but far fewer theorems require a function to be, say, C^7 , rather than only C^6 .)

2B. $\mathbb{Q}$ -rank

Now let $\Gamma \backslash X$ be a locally symmetric space modeled on X , and assume that $\Gamma \backslash X$ has finite volume. Thus, Γ is a (torsion-free) discrete subgroup of G , such that $\Gamma \backslash G$ has finite volume; in short, Γ is a *lattice* in G .

Real rank has the following interesting implication for the geometry of $\Gamma \backslash X$:

(2.9) **Proposition.** *Assume X has no compact factors.*

- 1) *There is a dense geodesic in $\Gamma \backslash X$.*
- 2) *The geodesic flow on the unit tangent bundle $T^1(\Gamma \backslash X)$ has a dense orbit if and only if $\mathbb{R}\text{-rank}(G) = 1$.*



Figure 2.1. Looking at a compact manifold from farther and farther away.

The real rank depends only on X , so it is not affected by the choice of a particular lattice Γ . We now describe an analogous algebraically defined invariant, $\mathbb{Q}$ -rank(Γ), that does depend on Γ , and thus distinguishes between some of the various locally homogeneous spaces that are modeled on X . We will mention some of the geometric implications of $\mathbb{Q}$ -rank, leaving a more detailed discussion to later chapters.

(2.10) **Theorem.** $\mathbb{Q}$ -rank(Γ) is the smallest natural number r , for which there exists collection of finitely many (closed, simply connected) r -dimensional flats, such that all of $\Gamma \backslash X$ is within a bounded distance of the union of these flats.

(2.11) **Open Problem.** Is it true that $\mathbb{Q}$ -rank(Γ) is the largest natural number r , such that $\Gamma \backslash X$ contains a closed, simply connected, r -dimensional flat?

(2.12) **Remark.** Although not entirely obvious from Thm. 2.10, it is true that $\mathbb{Q}$ -rank(Γ) always exists (and is finite). Then it is clear that $0 \leq \mathbb{Q}$ -rank(Γ) $\leq \mathbb{R}$ -rank(G). The extreme values are always attained: there are lattices Γ_c and Γ_s in G with $\mathbb{Q}$ -rank(Γ_c) = 0 and $\mathbb{Q}$ -rank(Γ_s) = $\mathbb{R}$ -rank(G). So it is perhaps surprising that there may be gaps in between (see 9.20).

(2.13) **Example.** From the algebraic definition, which will appear in Chap. 9, it is easy to calculate

$$\mathbb{Q}\text{-rank}(\mathrm{SO}(m, n)_{\mathbb{Z}}) = \min\{m, n\} = \mathbb{R}\text{-rank}(\mathrm{SO}(m, n))$$

and

$$\mathbb{Q}\text{-rank}(\mathrm{SL}(n, \mathbb{Z})) = n - 1 = \mathbb{R}\text{-rank}(\mathrm{SL}(n, \mathbb{R})).$$

As for $\mathbb{R}$ -rank, the biggest difference is between spaces where the invariant is zero and those where it is nonzero, because this is again the distinction between a compact space and a noncompact one.

(2.14) **Theorem.** $\mathbb{Q}$ -rank(Γ) = 0 if and only if $\Gamma \backslash X$ is compact.

Theorem 2.10 implies that the $\mathbb{Q}$ -rank of Γ is directly reflected in the large-scale geometry of $\Gamma \backslash X$, described by the tangent cone at infinity. Intuitively, the tangent cone at ∞ of a metric space is obtained by looking at it from a large distance. For example, if $\Gamma \backslash X$ is compact, then, as we move farther away, the manifold appears smaller and smaller (see Fig. 2.1). In the limit, the manifold shrinks to a point.

An intuitive understanding is entirely sufficient for our purposes here, but, for the interested reader, we provide a more formal definition.

(2.15) **Definition.** The *tangent cone at infinity* of a metric space (M, d) is the limit space

$$\lim_{\epsilon \rightarrow 0^+} ((M, \epsilon d), p),$$

if the limit exists. Here, p is an arbitrary (but fixed!) point of M , and the limit is with respect to Gromov's Hausdorff distance. (Roughly speaking, a large ball around p in $(M, \epsilon d)$ is δ -close to being isometric to a large ball around a certain (fixed) point p_0 in the limit space (M_0, d_0) .)

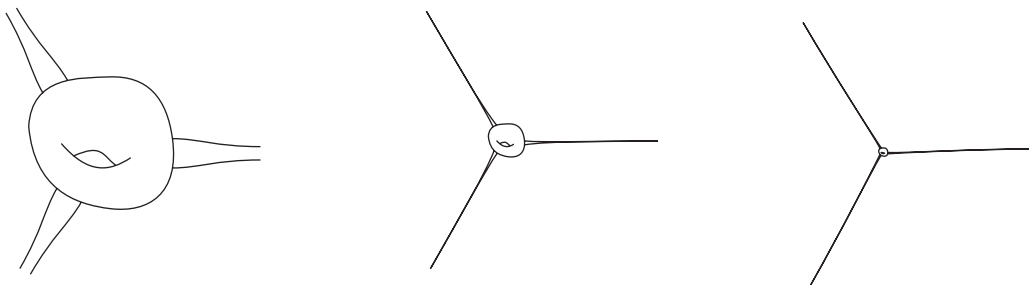


Figure 2.2. Looking at a manifold with cusps from farther and farther away.

(2.16) **Example.**

- 1) If $\Gamma \backslash X$ is compact, then the tangent cone at infinity of $\Gamma \backslash X$ is a point (see Fig. 2.1), which is a 0-dimensional simplicial complex. This 0-dimensionality is a geometric manifestation of the fact that $\mathbb{Q}\text{-rank}(\Gamma) = 0$.
- 2) If $\mathbb{R}\text{-rank}(G) = 1$, and $\Gamma \backslash X$ is not compact, then, as is well known, $\Gamma \backslash X$ has finitely many cusps. The tangent cone at infinity of a cusp is a ray, so the tangent cone at infinity of $\Gamma \backslash X$ is a “star” of finitely many rays emanating from a single vertex (see Fig. 2.2). Thus, the tangent cone at infinity of $\Gamma \backslash X$ is a 1-dimensional simplicial complex. This manifests the fact that $\mathbb{Q}\text{-rank}(\Gamma) = 1$.

(2.17) **Theorem.** *The tangent cone at infinity of $\Gamma \backslash X$ is a simplicial complex whose dimension is $\mathbb{Q}\text{-rank}(\Gamma)$.*

(2.18) **Example.** Let $G = \mathrm{SL}(3, \mathbb{R})$ and $\Gamma = \mathrm{SL}(3, \mathbb{Z})$. From Thm. 2.17, we see that the tangent cone at infinity of $\Gamma \backslash G/K$ is a 2-dimensional simplicial complex. In fact, it turns out to be (isometric to) the sector

$$\left\{ (x, y) \in \mathbb{R}^2 \mid 0 \leq y \leq \frac{\sqrt{3}}{2}x \right\}.$$

(It is not a coincidence that this sector is a Weyl chamber of the Lie algebra $\mathfrak{sl}(3, \mathbb{R})$.)

(2.19) **Remark.**

- If $\mathbb{Q}\text{-rank} \Gamma = 1$, then the tangent cone at infinity of $\Gamma \backslash X$ is a star of finitely many rays emanating from the origin (cf. 2). Note that this intersects the unit sphere in finitely many points.
- In general, if $\mathbb{Q}\text{-rank} \Gamma = k$, then the unit sphere contains a certain simplicial complex $\mathcal{T}_\Gamma$ of dimension $k - 1$, such that the tangent cone at infinity of $\Gamma \backslash X$ is the union of all the rays emanating from the origin that pass through $\mathcal{T}_\Gamma$.
- For $\Gamma = \mathrm{SL}(3, \mathbb{Z})$, the simplicial complex $\mathcal{T}_\Gamma$ is a single edge (cf. 2.18). In general, the Tits building $\mathcal{T}_G$ is a certain simplicial complex defined from the parabolic $\mathbb{Q}$ -subgroups of G , and $\mathcal{T}_\Gamma$ can be obtained from $\mathcal{T}_G$ by modding out the action of Γ .

The $\mathbb{Q}$ -rank is also directly reflected in the cohomology of $\Gamma \backslash X$. Namely, let c be the cohomological dimension of $\Gamma \backslash X$. Because $\Gamma \backslash X$ is a manifold of dimension $\dim X$, we have $c = \dim X$ if and only if $\Gamma \backslash X$ is compact. So the deficiency $\dim X - c$ is, in some sense, a measure of how far $\Gamma \backslash X$ is from being compact. This measure is precisely $\mathbb{Q}\text{-rank}(\Gamma)$.

(2.20) **Theorem.** *Assume X has no compact factors. Then the cohomological dimension of $\Gamma \backslash X$ is $(\dim X) - (\mathbb{Q}\text{-rank}(\Gamma))$.*

2C. Notes

Helgason's book [Hel2] provides a thorough discussion of rank and $\mathbb{R}$ -rank.

A version of Problem 2.11, and substantial progress toward an affirmative answer, can be found in [T–W].

If Γ is arithmetic, Theorem 2.14 was proved by Borel and Harish-Chandra [B–HC] and, independently, by Mostow and Tamagawa [M–T]. For non-arithmetic lattices, we will take this theorem as part of the *definition* of $\mathbb{Q}$ -rank.

A more precise version of Thm. 2.17 (providing a more precise description of the geometry of the simplicial complex) was proved by Hattori [Hat]. Theorem 2.20 is due to Borel and Serre [B–S].

2D. References

- [B–HC] A. Borel and Harish-Chandra: Arithmetic subgroups of algebraic groups. *Ann. Math.* (2) 75 (1962) 485–535.
- [B–S] A. Borel and J. P. Serre: Corners and arithmetic groups, *Comment. Math. Helvetici* 48 (1973) 436–491.
- [Hat] T. Hattori: Asymptotic geometry of arithmetic quotients of symmetric spaces. *Math. Z.* 222 (1996) 247–277. MR **98d**:53061
- [Hel2] S. Helgason: *Differential Geometry, Lie Groups, and Symmetric Spaces*. Academic Press, New York, 1978. (A revised edition is coming soon from the American Mathematical Society.)
- [M–T] G. D. Mostow and T. Tamagawa: On the compactness of arithmetically defined homogeneous spaces, *Ann. Math.* 76 (1961) 446–463.
- [T–W] G. Tomanov and B. Weiss: Closed orbits for actions of maximal tori on homogeneous spaces (preprint, 2001).

Exercises

- 2:1) Show $\mathbb{R}\text{-rank}(G_1 \times G_2) = \mathbb{R}\text{-rank } G_1 + \mathbb{R}\text{-rank } G_2$.
- 2:2) Assume $\mathbb{R}\text{-rank } G = 1$. Show X is irreducible if and only if X has no compact factors.
- 2:3) Show that if X is reducible, then X is *not* two-point homogeneous. (Do not assume the fact about maximal flats that was mentioned, without proof, before Prop. 2.6.)
- 2:4) Prove, directly from Thm. 2.11, that if $\Gamma \backslash X$ is compact, then $\mathbb{Q}\text{-rank}(\Gamma) = 0$.

Introduction to Semisimple Lie Groups

The main topic of this book is the study of a lattice Γ in a semisimple Lie group G . Without losing any of the main ideas, the reader may assume, throughout, that G is either $\mathrm{SL}(n, \mathbb{R})$ or $\mathrm{SO}(m, n)^\circ$ (or a product of these groups). Much of the material is of interest even in the special case $G = \mathrm{SO}(1, n)^\circ$.

See §3C below for the definition of “semisimple.”

3A. The standing assumptions

Throughout this book:

- 1) G is a connected, real, semisimple Lie group with finite center; and
- 2) Γ is a lattice in G (see Defn. 5.8).

Similar restrictions apply to the symbols $G_1, G_2, G', \Gamma_1, \Gamma_2, \Gamma'$, etc.

Geometers interested in the locally symmetric space $\Gamma \backslash G/K$ usually place additional restrictions on G and Γ :

- Geometers assume that the center of G is trivial, for otherwise G does not act *faithfully* as a group of isometries of the symmetric space G/K .
- Geometers assume that Γ is torsion-free (that is, that Γ has no nontrivial elements of finite order), for otherwise Γ does not act freely on G/K .

3B. Isogenies

We usually wish to ignore the minor differences that come from taking finite covers, so let us recall the following definition.

(3.1) **Definition.** Two Lie groups H_1 and H_2 (with only finitely many connected components) are *isogenous* if there exists a connected Lie group $\overline{H}$, such that $\overline{H}$ finitely covers both H_1° and H_2° . (Or, equivalently, if there exists a connected Lie group $\underline{H}$, such that $\underline{H}$ is finitely covered by each of H_1° and H_2° .) This is an equivalence relation.

Note that (for G_1 and G_2 as in 3A(1)), G_1 is isogenous to G_2 if and only if $\text{Ad } G_1 \cong \text{Ad } G_2$; equivalently, G_1 and G_2 are *locally isomorphic*, that is, the Lie algebras $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are isomorphic.

3C. What is a semisimple Lie group?

Recall that an abstract group is *simple* if it has no nontrivial, proper, normal subgroups. For Lie groups, we relax this to allow normal subgroups that are discrete (except that the one-dimensional abelian groups $\mathbb{R}$ and $\mathbb{T}$ are not considered to be simple).

(3.2) **Definition.** G is *simple* if G has no nontrivial, connected, closed, proper, normal subgroups, and G is not abelian.

(3.3) **Example.** $G = \text{SL}(n, \mathbb{R})$ is a simple Lie group. If n is even, then $\{\pm \text{Id}\}$ is a subgroup of G , and it is normal, but, because this subgroup is not connected, it does not disqualify G from being simple as a Lie group.

(3.4) **Other terminology.** Some authors say that $\text{SL}(n, \mathbb{R})$ is *almost simple*, and reserve the term “simple” for groups that have no (closed) normal subgroups at all, not even finite ones.

Although Defn. 3.2 only refers to *closed* normal subgroups, it turns out that, except for the center, there are no normal subgroups at all.

(3.5) **Theorem.** *If G is simple, then G has no infinite, proper, normal subgroups. More precisely, every proper, normal subgroup of G is contained in $Z(G)$.*

In particular, if G is simple, and $Z(G) = e$, then G is simple as an abstract group.

(3.6) **Definition.** G is *semisimple* if it is isogenous to a direct product of simple Lie groups. That is, G is isogenous to $G_1 \times \cdots \times G_r$, where each G_i is simple.

(3.7) **Remark.** Semisimple groups have no nontrivial (continuous) homomorphisms to $\mathbb{R}^+$ (see Exer. 3:3), so any semisimple group is unimodular.

A semisimple group, unlike a simple group, may have connected, normal subgroups (such as the simple factors G_i). However, these normal subgroups cannot be abelian (see Exer. 3:1). The converse is a major theorem in the structure theory of Lie groups:

(3.8) **Theorem.** *A connected Lie group H is semisimple if and only if it has no nontrivial, connected, abelian, normal subgroups.*

(3.9) **Remark.** A connected Lie group R is *solvable* if every nontrivial quotient of R has a nontrivial, connected, abelian, normal subgroup. (For example, abelian groups are solvable.) One can show that any connected Lie group H has a unique maximal connected, closed, solvable, normal subgroup. It is called the *radical* of H , and is denoted $\text{Rad } H$. Our statement of Thm. 3.8 is equivalent to the more usual statement that H is semisimple if and only if $\text{Rad } H$ is trivial (see Exer. 3:4).

(3.10) **Remark.** The center $Z(G)$ is finite, so G is isogenous to $G/Z(G)$. Also, the kernel of the adjoint representation is $Z(G)$, so $G/Z(G)$ is isomorphic to a group of matrices; that is, $G/Z(G)$ is linear. Thus, G is isogenous to a linear group, so there is usually no harm in assuming that G itself is linear.

(3.11) **Definition.** G is *linear* if G is isomorphic to a group of matrices; more precisely, G is isomorphic to a closed subgroup of $\text{SL}(\ell, \mathbb{R})$, for some ℓ .

The following result makes it easy to see that the classical groups, such as $\text{SL}(n, \mathbb{R})$, $\text{SO}(m, n)$, and $\text{SU}(m, n)$, are semisimple (except a few abelian groups in small dimensions).

(3.12) **Definition.** A subgroup H of $\mathrm{GL}(\ell, \mathbb{R})$ (or $\mathrm{GL}(\ell, \mathbb{C})$) is *irreducible* if there are no nontrivial, proper, H -invariant subspaces of $\mathbb{R}^\ell$ (or $\mathbb{C}^\ell$, respectively).

(3.13) **Example.** $\mathrm{SL}(\ell, \mathbb{R})$ is an irreducible subgroup of $\mathrm{SL}(\ell, \mathbb{C})$ (see Exer. 3:7).

(3.14) **Warning.** In a different context, the adjective “irreducible” can have a completely different meaning when it is applied to a group. For example, saying that a lattice is irreducible (as in Defn. 5.23) has nothing to do with Defn. 3.12.

(3.15) **Remark.** If H is a subgroup of $\mathrm{GL}(\ell, \mathbb{C})$ that is *not* irreducible (that is, if H is *reducible*), then, after a change of basis, we have

$$H \subset \begin{pmatrix} \mathrm{GL}(k, \mathbb{C}) & * \\ 0 & \mathrm{GL}(n-k, \mathbb{C}) \end{pmatrix},$$

for some k with $1 \leq k \leq n-1$.

Similarly for $\mathrm{GL}(\ell, \mathbb{R})$.

(3.16) **Corollary.** If H is a nonabelian, closed, connected, irreducible subgroup of $\mathrm{SL}(\ell, \mathbb{C})$, then H is semisimple.

Proof. Suppose A is a connected, abelian, normal subgroup of H . For each function $w: A \rightarrow \mathbb{C}^\times$, let

$$V_w = \{v \in \mathbb{C}^\ell \mid \forall a \in A, a(v) = w(a)v\}.$$

That is, a nonzero vector v belongs to V_w if

- v is an eigenvector for every element of A , and
- the corresponding eigenvalue for each element of a is the number that is specified by the function w .

Of course, $0 \in V_w$ for every function w ; let $W = \{w \mid V_w \neq 0\}$. (This is called the set of *weights* of A on $\mathbb{C}^\ell$.)

Each element of a has an eigenvector (because $\mathbb{C}$ is algebraically closed), and the elements of A all commute with each other, so there is a common eigenvector for the elements of A . Therefore, $W \neq \emptyset$. From the usual argument that the eigenspaces of any linear transformation are linearly independent, one can show that the subspaces $\{V_w \mid w \in W\}$ are linearly independent. Hence, W is finite.

For $w \in W$ and $h \in H$, a straightforward calculation shows that $hV_w = V_{h(w)}$, where $(h(w))(a) = w(h^{-1}ah)$. That is, H permutes the subspaces $\{V_w\}_{w \in W}$. Because H is connected and W is finite, this implies $hV_w = V_w$ for each w ; that is, V_w is an H -invariant subspace of $\mathbb{C}^\ell$. Since H is irreducible, we conclude that $V_w = \mathbb{C}^\ell$.

Now, for any $a \in A$, the conclusion of the preceding paragraph implies that $a(v) = w(a)v$, for all $v \in \mathbb{C}^\ell$. Thus, a is a scalar matrix.

Since $\det a = 1$, this scalar is an ℓ^{th} root of unity. So A is a subgroup of the group of ℓ^{th} roots of unity, which is finite. Since A is connected, we conclude that $A = \{e\}$, as desired. $\square$

Here is another useful characterization of semisimple groups.

(3.17) **Corollary.** Let H be a closed, connected subgroup of $\mathrm{SL}(\ell, \mathbb{C})$. If

- the center $Z(H)$ is finite; and
- $H^* = H$ (where $*$ denotes the “adjoint,” or conjugate-transpose);

then H is semisimple.

Proof. Let A be a connected, normal subgroup of H . Because $H^* = H$, it is not difficult to show that H is *completely reducible*: there is a direct sum decomposition $\mathbb{C}^\ell = \bigoplus_{j=1}^r V_j$, such that $H|_{V_j}$ is irreducible, for each j (see Exer. 3:10).

The proof of Cor. 3.16 (everything except the final paragraph) shows that $A|_{V_j}$ consists of scalar multiples of the identity, for each j . Hence $A \subset Z(H)$. Since A is connected, but (by assumption) $Z(H)$ is finite, we conclude that A is trivial. $\square$

(3.18) **Remark.** There is a converse: if G is semisimple (and connected), then G is conjugate to a subgroup H , such that $H^* = H$. However, this is more difficult to prove.

3D. The simple Lie groups

(3.19) **Definition.** G is a *classical group* if it is isogenous to the direct product of any collection of the groups constructed in Egs. 3.22 and 3.23 below. That is, each simple factor of G is either a special linear group or the isometry group of a bilinear or Hermitian form, over $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$ (where $\mathbb{H}$ is the algebra of quaternions). See Exers. 3:18, 3:21, and 3:22.

(3.20) **Warning.** Contrary to the usage of some authors, we do not require a form to be positive-definite in order to be called “Hermitian.”

(3.21) **Notation.** For natural numbers m and n , let

- $I_{m,n}$ be the $(m+n) \times (m+n)$ diagonal matrix whose diagonal entries are m 1’s followed by n -1’s;
- g^T denote the transpose of the matrix g , and
- g^* denote the adjoint (that is, the conjugate-transpose) of g .

(3.22) **Example.**

- 1) The *special linear group* $\mathrm{SL}(n, \mathbb{R})$ is a simple Lie group (if $n \geq 2$). It is connected.
- 2) *Special orthogonal group.* Let

$$\mathrm{SO}(m, n) = \{ g \in \mathrm{SL}(m+n, \mathbb{R}) \mid g^T I_{m,n} g = I_{m,n} \}.$$

Then $\mathrm{SO}(m, n)$ is semisimple if $m+n \geq 3$, and is simple if either $m+n = 3$ or $m+n \geq 5$. However, $\mathrm{SO}(m+n)$ is not connected unless either $m = 0$ or $n = 0$ (cf. Exers. 3:19 and 3:20); otherwise, it has exactly two components. We use $\mathrm{SO}(n)$ to denote $\mathrm{SO}(n, 0)$ (or $\mathrm{SO}(0, n)$, which is the same group).

- 3) *Special unitary group.* Let

$$\mathrm{SU}(m, n) = \{ g \in \mathrm{SL}(m+n, \mathbb{C}) \mid g^* I_{m,n} g = I_{m,n} \}.$$

Then $\mathrm{SU}(m, n)$ is simple if $m+n \geq 2$. It is connected. We use $\mathrm{SU}(n)$ to denote $\mathrm{SU}(n, 0)$ (or $\mathrm{SU}(0, n)$).

- 4) *Symplectic group.* Let

$$J_{2m} = \begin{pmatrix} 0 & \mathrm{Id}_{m \times m} \\ -\mathrm{Id}_{m \times m} & 0 \end{pmatrix} \in \mathrm{GL}(2m, \mathbb{R})$$

(where $\mathrm{Id}_{m \times m}$ denotes the $m \times m$ identity matrix), and let

$$\mathrm{Sp}(2m, \mathbb{R}) = \{ g \in \mathrm{SL}(2m, \mathbb{R}) \mid g^T J_{2m} g = J_{2m} \}.$$

Then $\mathrm{Sp}(2m, \mathbb{R})$ is simple if $m \geq 2$. It is connected.

(3.23) **Example.** One may construct additional simple groups, by replacing the field $\mathbb{R}$ with the field $\mathbb{C}$ of complex numbers or the division ring $\mathbb{H}$ of quaternions in the above examples:

- 1) *Complex and quaternionic special linear groups:* $\mathrm{SL}(n, \mathbb{C})$ and $\mathrm{SL}(n, \mathbb{H})$ are simple Lie groups (if $n \geq 2$). Each is connected.

Note: The noncommutativity of $\mathbb{H}$ causes some difficulty in defining the determinant of a quaternionic matrix. To avoid this problem, we define the *reduced norm* of a quaternionic $n \times n$ matrix g to be the determinant of the $2n \times 2n$ complex matrix obtained by identifying $\mathbb{H}^n$ with $\mathbb{C}^{2n}$. Then, by definition, g belongs to $\mathrm{SL}(n, \mathbb{H})$ if and only if its reduced norm is 1. It turns out that the reduced norm of a quaternionic matrix is always a semipositive (or, in other words, nonnegative) real number.

- 2) *Complex and quaternionic special orthogonal groups:*

$$\mathrm{SO}(n, \mathbb{C}) = \{ g \in \mathrm{SL}(n, \mathbb{C}) \mid g^T \mathrm{Id} g = \mathrm{Id} \}$$

and

$$\mathrm{SO}(n, \mathbb{H}) = \{ g \in \mathrm{SL}(n, \mathbb{H}) \mid \tau_r(g^T) \mathrm{Id} g = \mathrm{Id} \},$$

where τ_r is the antiinvolution on $\mathbb{H}$ defined by

$$\tau_r(a_0 + a_1i + a_2j + a_3k) = a_0 + a_1i - a_2j + a_3k.$$

(Note that $\tau_r(ab) = \tau_r(b) \tau_r(a)$ (see Exer. 3:23); τ_r is included in the definition of $\mathrm{SO}(n, \mathbb{H})$ in order to compensate for the noncommutativity of $\mathbb{H}$ (see Exer. 3:25).)

- 3) *Complex symplectic group:* Let

$$\mathrm{Sp}(2m, \mathbb{C}) = \{ g \in \mathrm{SL}(2m, \mathbb{C}) \mid g^T J_{2m} g = J_{2m} \}.$$

- 4) *symplectic unitary group* Symplectic unitary groups: Let

$$\mathrm{Sp}(m, n) = \{ g \in \mathrm{SL}(m+n, \mathbb{H}) \mid g^* I_{m,n} g = I_{m,n} \}.$$

We use $\mathrm{Sp}(n)$ to denote $\mathrm{Sp}(n, 0)$ (or $\mathrm{Sp}(0, n)$).

(3.24) **Other terminology.** Some authors use

- $\mathrm{SU}^*(2n)$ to denote $\mathrm{SL}(n, \mathbb{H})$ and
- $\mathrm{SO}^*(2n)$ to denote $\mathrm{SO}(n, \mathbb{H})$.

(3.25) **Remark.** $\mathrm{SL}(2, \mathbb{R})$ is the smallest connected, noncompact, simple Lie group; it is contained (up to isogeny) in any other.

- $\mathrm{SL}(n, \mathbb{R})$, $\mathrm{SL}(n, \mathbb{C})$, and $\mathrm{SL}(n, \mathbb{H})$ all contain $\mathrm{SL}(2, \mathbb{R})$.
- If $\mathrm{SO}(m, n)$ is semisimple and not compact, then $\min\{m, n\} \geq 1$ and $\max\{m, n\} \geq 2$, so $\mathrm{SO}(1, 2) \subset \mathrm{SO}(m, n)$.
- If $\mathrm{SU}(m, n)$ is not compact, then $\min\{m, n\} \geq 1$, so $\mathrm{SU}(1, 1) \subset \mathrm{SU}(m, n)$.
- If $\mathrm{Sp}(m, n)$ is not compact, then $\min\{m, n\} \geq 1$, so $\mathrm{Sp}(1, 1) \subset \mathrm{Sp}(m, n)$.

Note that $\mathrm{SO}(1, 2)$ and $\mathrm{SU}(1, 1)$ are isogenous to $\mathrm{SL}(2, \mathbb{R})$ (see 3.31(1b)); and $\mathrm{Sp}(1, 1)$ is isogenous to $\mathrm{SO}(1, 4)$ (see 3.31(2b)), which contains $\mathrm{SO}(1, 2)$.

(3.26) **Remark.** There is some redundancy in the above lists. (For example, $\mathrm{SL}(2, \mathbb{R})$, $\mathrm{SU}(1, 1)$, $\mathrm{SO}(1, 2)$, and $\mathrm{Sp}(2, \mathbb{R})$ are isogenous to each other (see 3.31(1b)).) A complete list of these redundancies is given in §3E below.

(3.27) **Remark.** This notation for the classical groups, although common, is not universal. In particular, the group $\mathrm{SO}(n, \mathbb{H})$ is sometimes denoted $\mathrm{SO}^*(2n)$, the group $\mathrm{SL}(n, \mathbb{H})$ is sometimes denoted $\mathrm{SU}^*(2n)$, and the group $\mathrm{Sp}(2m, \mathbb{R})$ is sometimes denoted $\mathrm{Sp}(m, \mathbb{R})$.

The classical groups are just examples, so one would expect there to be many other (more exotic) simple Lie groups. Amazingly, that is not the case:

(3.28) **Theorem** (É. Cartan). *Any connected, simple Lie group with finite center is isogenous to either*

- 1) *a classical group; or*
- 2) *one of the finitely many exceptional groups.*

3E. Which classical groups are isogenous?

(3.29) **Notation.** For reasons that will be more clear later (see Prop. 3.35 and Chap. 18), the classical simple groups are collected into four infinite families: each classical group is of *type* A_n , B_n , C_n , or D_n , for some $n \geq 1$. See Fig. 3.1.

Similarly, the exceptional groups are of type E_6 , E_7 , E_8 , F_4 , or G_2 . We will have nothing in particular to say about exceptional groups, but let us mention that there are 22 different isogeny classes of exceptional simple groups (with finite center). Of these,

- 6 are of type E_6 ;
- 5 are of type E_7 ;
- 4 are of type E_8 ;
- 4 are of type F_4 ; and
- 3 are of type G_2 .

Three of the groups of each type (in particular, all of the groups of type G_2) are easy to account for: each type includes a compact group, a complex group, and an $\mathbb{R}$ -split group. The 4th group of type F_4 is the only exceptional group that will play any role in this book (cf. 8.25).

(3.30) **Remark.** Note that half of the orthogonal groups are of type B_n , and the other half are of type D_n . Although this may not seem natural, there are good reasons to divide the orthogonal groups into two classes: orthogonal groups in odd dimensions behave very differently than orthogonal groups in even dimensions. For example, ℓ is even if and only if $\mathrm{SO}(\ell)$ has an outer automorphism (cf. Exer. 3:27).

(3.31) **Remark.** Groups of different type are never isogenous, except:

- 1) Any group of type B_1 or C_1 is isogenous to a group of type A_1 (and vice versa). Namely:
 - (a) $\mathrm{SO}(3)$ and $\mathrm{Sp}(1)$ are isogenous to $\mathrm{SL}(1, \mathbb{H})$ and $\mathrm{SU}(2)$ (see Exer. 3:28);
 - (b) $\mathrm{SO}(1, 2)$ and $\mathrm{Sp}(2, \mathbb{R})$ are isogenous to $\mathrm{SL}(2, \mathbb{R})$ and $\mathrm{SU}(1, 1)$ (see Exers. 3:29, 3:30 and 3:31);
 - (c) $\mathrm{SO}(3, \mathbb{C})$ and $\mathrm{Sp}(2, \mathbb{C})$ are isogenous to $\mathrm{SL}(2, \mathbb{C})$ (see Exer. 3:32).
- 2) Any group of type C_2 is isogenous to a group of type B_2 (and vice versa). Namely:
 - (a) $\mathrm{Sp}(2)$ is isogenous to $\mathrm{SO}(5)$;
 - (b) $\mathrm{Sp}(1, 1)$ is isogenous to $\mathrm{SO}(1, 4)$;
 - (c) $\mathrm{Sp}(4, \mathbb{R})$ is isogenous to $\mathrm{SO}(2, 3)$; and
 - (d) $\mathrm{Sp}(4, \mathbb{C})$ is isogenous to $\mathrm{SO}(5, \mathbb{C})$.

type	G	restrictions	$\mathbb{R}$ -rank(G)	maximal compact subgroup K	$\dim G$
A_n	$\mathrm{SL}(n+1, \mathbb{R})$		n	$\mathrm{SO}(n+1)$	$n^2 + 2n$
	$\mathrm{SL}(n+1, \mathbb{C})$		n	$\mathrm{SU}(n+1)$	$2n^2 + 4n$
	$\mathrm{SL}(\frac{n+1}{2}, \mathbb{H})$	n odd	$(n-1)/2$	$\mathrm{Sp}((n+1)/2)$	$n^2 + 2n$
	$\mathrm{SU}(p, q)$	$p+q = n+1$	$\min\{p, q\}$	$\mathrm{S}(\mathrm{U}(p) \times \mathrm{U}(q))$	$n^2 + 2n$
B_n	$\mathrm{SO}(p, q)$	$p+q = 2n+1$	$\min\{p, q\}$	$\mathrm{S}(\mathrm{O}(p) \times \mathrm{O}(q))$	$2n^2 + n$
	$\mathrm{SO}(2n+1, \mathbb{C})$		n	$\mathrm{SO}(2n+1)$	$4n^2 + 2n$
C_n	$\mathrm{Sp}(p, q)$	$p+q = n$	$\min\{p, q\}$	$\mathrm{Sp}(p) \times \mathrm{Sp}(q)$	$2n^2 + n$
	$\mathrm{Sp}(2n, \mathbb{R})$		n	$\mathrm{U}(n)$	$2n^2 + n$
	$\mathrm{Sp}(2n, \mathbb{C})$		n	$\mathrm{Sp}(n)$	$4n^2 + 2n$
D_n	$\mathrm{SO}(p, q)$	$p+q = 2n$	$\min\{p, q\}$	$\mathrm{S}(\mathrm{O}(p) \times \mathrm{O}(q))$	$2n^2 - n$
	$\mathrm{SO}(2n, \mathbb{C})$		n	$\mathrm{SO}(2n)$	$4n^2 - 2n$
	$\mathrm{SO}(n, \mathbb{H})$		$\lfloor n/2 \rfloor$	$\mathrm{U}(n)$	$2n^2 - n$

Figure 3.1. Basic information about each classical group (for $n \geq 1$).

- 3) Any group of type D_2 is isogenous to either a group of type A_1 (or B_1 or C_1) or the direct product of two groups of type A_1 (or B_1 or C_1). Namely:
- (a) $\mathrm{SO}(4)$ is isogenous to $\mathrm{SU}(2) \times \mathrm{SU}(2)$, $\mathrm{SO}(3) \times \mathrm{SO}(3)$, and $\mathrm{Sp}(1) \times \mathrm{Sp}(1)$ (see Exer. 3:33);
 - (b) $\mathrm{SO}(1, 3)$ is isogenous to $\mathrm{SL}(2, \mathbb{C})$, $\mathrm{SO}(3, \mathbb{C})$, and $\mathrm{Sp}(2, \mathbb{C})$ (see Exer. 3:34);
 - (c) $\mathrm{SO}(2, 2)$ is isogenous to $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$, $\mathrm{SO}(1, 2) \times \mathrm{SO}(1, 2)$, and $\mathrm{Sp}(2, \mathbb{R}) \times \mathrm{Sp}(2, \mathbb{R})$ (see Exer. 3:35);
 - (d) $\mathrm{SO}(4, \mathbb{C})$ is isogenous to $\mathrm{SL}(2, \mathbb{C}) \times \mathrm{SL}(2, \mathbb{C})$, $\mathrm{SO}(3, \mathbb{C}) \times \mathrm{SO}(3, \mathbb{C})$, and $\mathrm{Sp}(2, \mathbb{C}) \times \mathrm{Sp}(2, \mathbb{C})$ (see Exer. 3:36); and
 - (e) $\mathrm{SO}(2, \mathbb{H})$ is isogenous to $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SU}(2)$ (see Exer. 3:37).
- 4) Any group of type D_3 is isogenous to a group of type A_3 (and vice versa). Namely:
- (a) $\mathrm{SO}(6)$ is isogenous to $\mathrm{SU}(4)$;
 - (b) $\mathrm{SO}(1, 5)$ is isogenous to $\mathrm{SL}(2, \mathbb{H})$;
 - (c) $\mathrm{SO}(2, 4)$ is isogenous to $\mathrm{SU}(2, 2)$;
 - (d) $\mathrm{SO}(3, 3)$ is isogenous to $\mathrm{SL}(4, \mathbb{R})$ (see Exer. 3:38);
 - (e) $\mathrm{SO}(6, \mathbb{C})$ is isogenous to $\mathrm{SL}(4, \mathbb{C})$;
 - (f) $\mathrm{SO}(3, \mathbb{H})$ is isogenous to $\mathrm{SU}(1, 3)$.

We see, from Rem. 3.31, that the types B_1 , C_1 , C_2 , D_2 , and D_3 are redundant. Furthermore, groups of type D_1 are abelian, not semisimple. Thus, we have the following proposition.

(3.32) **Proposition.** *If G is simple, then G is isogenous to a group that is of type*

- 1) A_n , with $n \geq 1$; or
- 2) B_n , with $n \geq 2$; or

- 3) C_n , with $n \geq 3$; or
- 4) D_n , with $n \geq 4$; or
- 5) E_6, E_7, E_8, F_4 , or G_2 .

Furthermore, under these restrictions on n , this type is uniquely determined by the isogeny class of G .

(3.33) **Proposition.** *Under the restrictions on n given in Prop. 3.32, the only redundancies in the list of groups G in Fig. 3.1 are:*

- 1) $\mathrm{SL}(1, \mathbb{H})$ is isogenous to $\mathrm{SU}(2)$;
- 2) $\mathrm{SU}(1, 1)$ is isogenous to $\mathrm{SL}(2, \mathbb{R})$;
- 3) $\mathrm{SO}(4, \mathbb{H})$ is isogenous to $\mathrm{SO}(2, 6)$;
- 4) $\mathrm{SO}(p, q) \cong \mathrm{SO}(q, p)$;
- 5) $\mathrm{SU}(p, q) \cong \mathrm{SU}(q, p)$; and
- 6) $\mathrm{Sp}(p, q) \cong \mathrm{Sp}(q, p)$.

Let us close this section with some justification of the above remarks.

(3.34) **Notation.** As will be explained in §10A, G has a well-defined *complexification* $G \otimes \mathbb{C}$, obtained by replacing real numbers with complex numbers. (In terms of the Lie algebra $\mathfrak{g}$, we simply tensor $\mathfrak{g}$ with $\mathbb{C}$.) For example,

- $\mathrm{SL}(n, \mathbb{R}) \otimes \mathbb{C} = \mathrm{SL}(n, \mathbb{C})$,
- $\mathrm{SO}(m, n) \otimes \mathbb{C} = \mathrm{SO}(m + n, \mathbb{C})$, and
- $\mathrm{SL}(n, \mathbb{C}) \otimes \mathbb{C} = \mathrm{SL}(n, \mathbb{C}) \times \mathrm{SL}(n, \mathbb{C})$.

(3.35) **Proposition.** *Two simple Lie groups G_1 and G_2 are of the same type (under the restrictions on n given in Prop. 3.32) if and only if either*

- $G_1 \otimes \mathbb{C}$ is isogenous to $G_2 \otimes \mathbb{C}$, or
- $G_1 \otimes \mathbb{C}$ is isogenous to G_2 , or
- G_1 is isogenous to $G_2 \otimes \mathbb{C}$.

Proof. There is (up to isogeny) only one *complex* group of each type (see Fig. 3.2). One can verify, under the given restrictions on n , that none of these complex groups are isogenous to any of the others. (For the classical cases A_n, B_n, C_n, D_n , it is not too difficult to establish this directly. In any case, one can use the theory of roots: the conclusion follows from the observation that none of the Dynkin diagrams are isomorphic (see Fig. 18.1).) Note that if G is complex, then $G \otimes \mathbb{C}$ is isomorphic to $G \times G$.

If G is a *real* (non-complex) simple group, then $G \otimes \mathbb{C}$ is a complex simple group, so it is isogenous to one of the groups in Fig. 3.2. It is easy to verify, by inspection of Fig. 3.1, that G and $G \otimes \mathbb{C}$ have the same type. (Indeed, this is precisely the criterion that led to the groupings in Fig. 3.1.)

Thus, when G_1 and G_2 are either both real or both complex, we see that G_1 and G_2 have the same type if and only if $G_1 \otimes \mathbb{C}$ is isogenous to $G_2 \otimes \mathbb{C}$. On the other hand, when G_1 is real and G_2 is complex, we see that G_1 and G_2 have the same type if and only if $G_1 \otimes \mathbb{C}$ is isogenous to G_2 . $\square$

This has the following consequence, which is the starting point of Rem. 3.31.

type	complex group	restriction on n
A_n	$\mathrm{SL}(n+1, \mathbb{C})$	$n \geq 1$
B_n	$\mathrm{SO}(2n+1, \mathbb{C})$	$n \geq 2$
C_n	$\mathrm{Sp}(2n, \mathbb{C})$	$n \geq 3$
D_n	$\mathrm{SO}(2n, \mathbb{C})$	$n \geq 4$
E_n	$E_n(\mathbb{C})$	$n \in \{6, 7, 8\}$
F_n	$F_4(\mathbb{C})$	$n = 4$
G_n	$G_2(\mathbb{C})$	$n = 2$

Figure 3.2. The complex group of each type.

(3.36) **Corollary.** *If G_1 and G_2 are simple Lie groups that are isogenous, then G_1 and G_2 have the same type (under the restrictions on n given in Prop. 3.32).*

Proof of Prop. 3.33. Suppose G_1 and G_2 are two of the groups listed in Fig. 3.1, with the restrictions on n given in Prop. 3.32. Assume that G_1 is isogenous to G_2 .

From Cor. 3.36, we know that G_1 and G_2 have the same type.

We may assume that neither G_1 nor G_2 is complex. (Otherwise, they must both be complex. Since Fig. 3.1 lists only one complex group of each type, we conclude that $G_1 = G_2$, as desired.)

The rest of the proof is based heavily on the observation that $\mathbb{R}\text{-rank}(G_1) = \mathbb{R}\text{-rank}(G_2)$ (see Chap. 8 for a discussion of real rank, and see Fig. 3.1 for a record of the real rank of each classical group). For $\mathrm{SO}(p, q)$, $\mathrm{SU}(p, q)$, and $\mathrm{Sp}(p, q)$, we always assume that $p \leq q$ (see (4), (5), and (6) of Prop. 3.33).

Case 1. Assume G_1 and G_2 are of type A_n , for some $n \geq 1$. Let us assume $n > 1$ (see Exer. 3:39). The groups $\mathrm{SL}(n+1, \mathbb{R})$ and $\mathrm{SU}(p, n+1-p)$ all have different real ranks, so no one is isogenous to any of the others. Thus, we may assume that $G_1 = \mathrm{SL}(\frac{n+1}{2}, \mathbb{H})$ (which implies that n is odd). Then $0 < \mathbb{R}\text{-rank}(G_1) < n$ (recall that $n > 1$), so we must have $G_2 = \mathrm{SU}(p, q)$, for some p and q with $1 \leq p \leq q$. Now the maximal compact subgroup of G_1 is $\mathrm{Sp}(n)$, which is simple, but the maximal compact subgroup of G_2 is

$$\mathrm{S}(\mathrm{U}(p) \times \mathrm{U}(q)) \approx \mathrm{U}(1) \times \mathrm{SU}(p) \times \mathrm{SU}(q),$$

which is not simple. This is a contradiction.

Case 2. Assume G_1 and G_2 are of type B_n , for some $n \geq 2$. The groups $\mathrm{SO}(p, 2n+1-p)$ all have different real ranks, so none are isogenous.

Case 3. Assume G_1 and G_2 are of type C_n , for some $n \geq 3$. The groups $\mathrm{Sp}(2n, \mathbb{R})$ and $\mathrm{Sp}(p, n-p)$ all have different real ranks, so none are isogenous.

Case 4. Assume G_1 and G_2 are of type D_n , for some $n \geq 4$. The groups $\mathrm{SO}(p, 2n-p)$ all have different real ranks, so none are isogenous. Thus, we may assume that $G_1 = \mathrm{SO}(n, \mathbb{H})$ (and that $G_2 = \mathrm{SO}(p, q)^\circ$). The maximal compact subgroup of G_1 is $\mathrm{U}(n)$, which is isogenous to $\mathrm{U}(1) \times \mathrm{SU}(n)$. Since the maximal compact subgroup of G_2 is $\mathrm{SO}(p) \times \mathrm{SO}(q)$, we conclude that $p = 2$, and that $\mathrm{SU}(n)$ is isogenous to $\mathrm{SO}(2n-2)$.

Now $\mathrm{SU}(n)$ is of type A_{n-1} , and $\mathrm{SO}(2n-2)$ is of type D_{n-1} . Therefore, Cor. 3.36 implies that $n-1 \leq 3$, so $n = 4$. (Recall that, by assumption, we have $n \geq 4$.) Hence, Conclusion 3.33(3) applies. $\square$

3F. Notes

Most of the material of this chapter can be found in Helgason's book [Hel2]. However, we do not follow Helgason's notation for some of the classical groups (see 3.24).

Isogenies are discussed in texts, such as [Bor4], on algebraic groups and in the book of Platonov and Rapinchuk [P-R]. Remark 3.17 was proved by Mostow [Mos1].

The classification of real simple Lie groups (Thm. 3.28 and Props. 3.32 and 3.33) was obtained by É. Cartan [Car]. (The intervening decades have led to enormous simplifications in the proof.) There are two main steps. First, one classifies the complex semisimple Lie algebras. (This appears in standard texts on Lie algebras, such as [Hum1].) Then, one finds all of the real forms of each complex Lie algebra. For the classical case, this appears in the book of Platonov and Rapinchuk [P-R, §2.3] (based on an approach of Weil [Wei] that leads directly to orthogonal, unitary, and symplectic groups, and that applies over other fields of characteristic zero). For the general case (including exceptional groups), see Helgason's book [Hel2, Chap. 10]. The lists of isogenies in Rem. 3.31 and Prop. 3.33 are largely copied from there [Hel2, §10.6.4, pp. 519–520].

Helgason's book [Hel2, §10.2, pp. 447–451] proves that all of the classical simple groups except $SO(p, q)$ are connected. For a geometric proof of 3.31(2c), see [Hel2, §10.A.2, p. 521].

3G. References

- [Bor4] A. Borel: *Linear Algebraic Groups*, 2nd ed., Springer, New York, 1991.
- [Car] É. Cartan: Les groupes réels simples finis et continus, *Ann. Sci. École Norm. Sup.* 31 (1914) 263–355.
- [Hel2] S. Helgason: *Differential Geometry, Lie Groups, and Symmetric Spaces*. Academic Press, New York, 1978. (A revised edition is coming soon from the American Mathematical Society.)
- [Hum1] J. E. Humphreys: *Introduction to Lie Algebras and Representation Theory*. Springer, Berlin Heidelberg New York, 1972.
- [Mos1] G. D. Mostow: Self adjoint groups, *Ann. Math.* 62 (1955) 44–55.
- [P-R] V. Platonov and A. Rapinchuk: *Algebraic Groups and Number Theory*. Academic Press, Boston, 1994.
- [Var] V. S. Varadarajan: *Lie Groups, Lie Algebras, and their Representations*. Springer, Berlin Heidelberg New York, 1984.
- [Wei] A. Weil: Algebras with involution and the classical groups, *J. Indian Math. Soc.* 24 (1960) 589–623.

Exercises

- 3:1) Prove ($\Rightarrow$) of Thm. 3.8.
- 3:2) Show that if G is semisimple, and N is any closed, normal subgroup of G , then G/N is semisimple.
- 3:3) (a) Show that if $\phi: G \rightarrow A$ is a continuous homomorphism, and A is abelian, then ϕ is trivial.
(b) Show that $[G, G] = G$.
- 3:4) Show that a connected Lie group H is semisimple if and only if H has no nontrivial, connected, solvable, normal subgroups. [*Hint*: If R is a solvable, normal subgroup of H , then $[R, R]$ is also normal in H , and $R/[R, R]$ is an abelian, normal subgroup of $H/[R, R]$.]

- 3:5) Suppose N is a connected, closed, normal subgroup of $G = G_1 \times \cdots \times G_r$, where each G_i is simple. Show that there is a subset S of $\{1, \dots, r\}$, such that $N = \prod_{i \in S} G_i$.
- 3:6) Suppose N is a connected, closed, normal subgroup of G . Show that there is a connected, closed, normal subgroup H of G , such that G is isogenous to $N \times H$.
- 3:7) Show that no nontrivial, proper $\mathbb{C}$ -subspace of $\mathbb{C}^\ell$ is invariant under $\mathrm{SL}(\ell, \mathbb{R})$. [Hint: Suppose $v, w \in \mathbb{R}^\ell$, not both 0. Either there exists $g \in \mathrm{SL}(\ell, \mathbb{R})$ with $g(v + iw) = v - iw$, or there exists nonzero $\lambda \in \mathbb{C}$ with $\lambda(v + iw) \in \mathbb{R}^\ell$.]
- 3:8) Give an example of a nonabelian, closed, connected, irreducible subgroup of $\mathrm{SL}(\ell, \mathbb{R})$, such that H is not semisimple. [Hint: $\mathrm{U}(2)$ is an irreducible subgroup of $\mathrm{SO}(4)$.]
- 3:9) Suppose $H \subset \mathrm{SL}(\ell, \mathbb{C})$. Show that H is completely reducible if and only if, for every H -invariant subspace W of $\mathbb{C}^\ell$, there is an H -invariant subspace W' of $\mathbb{C}^\ell$, such that $\mathbb{C}^\ell = W \oplus W'$. [Hint: ($\Rightarrow$) If $W' = V_1 \oplus \cdots \oplus V_s$, and $W' \cap W = \{0\}$, but $(W' \oplus V_j) \cap W \neq \{0\}$ for every $j > s$, then $W' + W = \mathbb{C}^\ell$. ($\Rightarrow$) Let W be a maximal subspace that is a direct sum of irreducibles, and let V be a minimal H -invariant subspace of W' . Then $W \oplus V$ contradicts the maximality of W .]
- 3:10) Suppose $H = H^* \subset \mathrm{SL}(\ell, \mathbb{C})$.
- (a) Show that if W is an H -invariant subspace of $\mathbb{C}^\ell$, then the orthogonal complement $W^\perp$ is also H -invariant.
 - (b) Show that H is completely reducible.
- 3:11) For $A \in \mathrm{GL}(\ell, \mathbb{C})$, define

$$\mathrm{SU}(A) = \{g \in \mathrm{SL}(\ell, \mathbb{C}) \mid g^* A g = A\}.$$

Show that if $A^2 = \pm \mathrm{Id}$, then $\mathrm{SU}(A)^* = \mathrm{SU}(A)$. [Hint: For $g \in \mathrm{SU}(A)$, we have $A = (g^*)^{-1} A g^{-1}$. Taking inverses of both sides, and noting that $A^{-1} = \pm A$, conclude that $g^* \in \mathrm{SU}(A)$.]

- 3:12) For $A \in \mathrm{GL}(\ell, \mathbb{R})$, define

$$\mathrm{SO}(A) = \{g \in \mathrm{SL}(\ell, \mathbb{C}) \mid g^T A g = A\}.$$

Show that if $A^2 = \pm \mathrm{Id}$, then $\mathrm{SO}(A)^T = \mathrm{SO}(A)^* = \mathrm{SO}(A)$. [Hint: The argument of Exer. 3:11 shows that $\mathrm{SO}(A)^T = \mathrm{SO}(A)$. Since $A \in \mathrm{GL}(\ell, \mathbb{R})$, it is easy to see that $\mathrm{SO}(A)$ is also closed under complex conjugation.]

- 3:13) Let B be a symmetric, invertible $\ell \times \ell$ real matrix. Define

$$\mathrm{SO}(B; \mathbb{R}) = \{g \in \mathrm{SL}(\ell, \mathbb{R}) \mid g^T B g = B\}.$$

Show $\mathrm{SO}(B; \mathbb{R}) \cong \mathrm{SO}(m, n)$, for some m, n .

- 3:14) Let B be a Hermitian, invertible $\ell \times \ell$ matrix. Define

$$\mathrm{SU}(B) = \{g \in \mathrm{SL}(\ell, \mathbb{C}) \mid g^* B g = B\}.$$

Show $\mathrm{SU}(B) \cong \mathrm{SU}(m, n)$, for some m, n .

- 3:15) Let B be a skew-symmetric, invertible $\ell \times \ell$ real matrix. Define

$$\mathrm{Sp}(B; \mathbb{R}) = \{g \in \mathrm{SL}(\ell, \mathbb{R}) \mid g^T B g = B\}.$$

Show ℓ is even, and $\mathrm{Sp}(B; \mathbb{R}) \cong \mathrm{Sp}(\ell, \mathbb{R})$.

- 3:16) Let $B \in \mathrm{GL}(\ell, \mathbb{H})$, such that $\tau_r(B^T) = B$. Define

$$\mathrm{SU}(B; \mathbb{H}, \tau_r) = \{g \in \mathrm{SL}(\ell, \mathbb{H}) \mid \tau_r(g^T) B g = B\}.$$

Show $\mathrm{SU}(B; \mathbb{H}, \tau_r) \cong \mathrm{SO}(\ell, \mathbb{H})$.

3:17) Let $B \in \mathrm{GL}(\ell, \mathbb{H})$, such that $\tau_c(B^T) = B$. Define

$$\mathrm{SU}(B; \mathbb{H}, \tau_c) = \{g \in \mathrm{SL}(\ell, \mathbb{H}) \mid \tau_c(g^T)Bg = B\}.$$

Show $\mathrm{SU}(B; \mathbb{H}, \tau_c) \cong \mathrm{Sp}(m, n)$, for some m, n .

3:18) Define a symmetric bilinear form $\langle \cdot \mid \cdot \rangle_{\mathbb{R}^{m,n}}$ on $\mathbb{R}^{m+n}$ by

$$\langle x \mid y \rangle_{\mathbb{R}^{m,n}} = \sum_{i=1}^m x_i y_i - \sum_{i=1}^n x_{m+i} y_{m+i}.$$

Show that

$$\mathrm{SO}(m, n) = \{g \in \mathrm{SL}(m+n, \mathbb{R}) \mid \forall x, y \in \mathbb{R}^{m+n}, \langle gx \mid gy \rangle_{\mathbb{R}^{m,n}} = \langle x \mid y \rangle_{\mathbb{R}^{m,n}}\}.$$

[Hint: $\langle x \mid y \rangle_{\mathbb{R}^{m,n}} = x^T I_{m,n} y$.]

3:19) Show that $\mathrm{SO}(1, n)$ is not connected. [Hint: The subset $X_{1,n}^+$ of $\mathbb{R}^{n+1}$ (as in Exer. 1:4) is invariant under $\mathrm{SO}(1, n)^\circ$, but there is some $g \in \mathrm{SO}(1, n)$, such that $gX_{1,n}^+ = -X_{1,n}^+ \neq X_{1,n}^+$.]

3:20) Show that $\mathrm{SO}(m, n)$ is not connected if $m, n > 0$. [Hint: Assume $m \leq n$, and let $\pi: \mathbb{R}^{m+n} \rightarrow \mathbb{R}^m$ be projection onto the first m coordinates. For any m -dimensional, totally isotropic subspace L of $\mathbb{R}^{m+n}$, the linear map $\pi|_L$ is a bijection onto $\mathbb{R}^m$. Show $f(g) = \det(\pi \circ g \circ (\pi|_L)^{-1})$ is a continuous, surjective function from $\mathrm{SO}(m, n)$ to $\{\pm 1\}$.]

3:21) Define a Hermitian form $\langle \cdot \mid \cdot \rangle_{\mathbb{C}^{m,n}}$ on $\mathbb{C}^{m+n}$ by

$$\langle x \mid y \rangle_{\mathbb{C}^{m,n}} = \sum_{i=1}^m x_i \overline{y_i} - \sum_{i=1}^n x_{m+i} \overline{y_{m+i}}.$$

(When $n = 0$, this is the usual Hermitian inner product on $\mathbb{C}^m$.) Show that

$$\mathrm{SU}(m, n) = \{g \in \mathrm{SL}(m+n, \mathbb{C}) \mid \forall x, y \in \mathbb{C}^{m+n}, \langle gx \mid gy \rangle_{\mathbb{C}^{m,n}} = \langle x \mid y \rangle_{\mathbb{C}^{m,n}}\}.$$

3:22) Define a skew-symmetric bilinear form $\langle \cdot \mid \cdot \rangle_{\mathrm{Sp}}$ on $\mathbb{R}^{2m}$ by

$$\langle x \mid y \rangle_{\mathrm{Sp}} = \sum_{i=1}^m (x_i y_{m+i} - x_{m+i} y_i).$$

Show that

$$\mathrm{Sp}(2m, \mathbb{R}) = \{g \in \mathrm{SL}(2m, \mathbb{R}) \mid \forall x, y \in \mathbb{R}^{2m}, \langle gx \mid gy \rangle_{\mathrm{Sp}} = \langle x \mid y \rangle_{\mathrm{Sp}}\}.$$

3:23) In the notation of Eg. 3.23, show that $\tau_r(ab) = \tau_r(b) \tau_r(a)$ for all $a, b \in \mathbb{H}$. [Hint: Calculate explicitly, or note that $\tau_r(x) = jxj^{-1}$.]

3:24) Give an example of two matrices $g, h \in \mathrm{SL}(n, \mathbb{H})$, such that $(gh)^T \neq h^T g^T$ and $(gh)^T \neq g^T h^T$.

3:25) For $g, h \in \mathrm{Mat}_{n \times n}(\mathbb{H})$, show that $\tau_r((gh)^T) = \tau_r(h^T) \tau_r(g^T)$.

3:26) Show that $\mathrm{SO}(n, \mathbb{H})$ is a subgroup of $\mathrm{SL}(n, \mathbb{H})$.

3:27) For any $g \in \mathrm{O}(\ell)$, the map $\phi_g: \mathrm{SO}(\ell) \rightarrow \mathrm{SO}(\ell)$, defined by $\phi_g(x) = gxg^{-1}$, is an automorphism of $\mathrm{SO}(n)$. Show that ℓ is odd if and only if, for every $g \in \mathrm{O}(\ell)$, there exists $h \in \mathrm{SO}(\ell)$, such that $\phi_h = \phi_g$.

3:28) Show that $\mathrm{SO}(3)$, $\mathrm{Sp}(1)$, $\mathrm{SL}(1, \mathbb{H})$, and $\mathrm{SU}(2)$ are isogenous to each other. [Hint: Let $\mathbb{H}^*$ be the group of unit quaternions. Then $\mathrm{Sp}(1)$ and $\mathrm{SL}(1, \mathbb{H})$ are naturally isomorphic to $\mathbb{H}^*$. For any $g \in \mathbb{H}^*$, define $T_g: \mathbb{H} \rightarrow \mathbb{H}$ by $T_g(x) = xg^{-1}$; then, after identifying $\mathbb{H}$ with $\mathbb{C}^2$, the linear map T_g is unitary. Let

$$V = \{v \in \mathbb{H} \mid \mathrm{Re} v = 0\}.$$

For $g \in \mathbb{H}^*$, define $S_g: V \rightarrow V$ by $S_g(v) = gvg^{-1}$; then, after identifying V with $\mathbb{R}^3$, the linear map S_g is orthogonal.]

- 3:29) Show that $\mathrm{Sp}(2, \mathbb{R}) = \mathrm{SL}(2, \mathbb{R})$ and $\mathrm{Sp}(2, \mathbb{C}) = \mathrm{SL}(2, \mathbb{C})$. (These pairs of groups are actually equal, not just isogenous.)
- 3:30) Show that $\mathrm{SU}(1, 1)$ is isogenous to $\mathrm{SL}(2, \mathbb{R})$. (In fact, these two groups are isomorphic, not just isogenous.) [Hint: For the usual action of $\mathrm{SL}(2, \mathbb{C})$ on $\mathbb{C} \cup \{\infty\}$ by linear-fractional transformations, we have

$$\mathrm{PSL}(2, \mathbb{R})^\circ = \{g \in \mathrm{PSL}(2, \mathbb{C}) \mid g(\mathbb{R} \cup \infty) = \mathbb{R} \cup \infty\}^\circ$$

and

$$\mathrm{PSU}(1, 1) = \{g \in \mathrm{PSL}(2, \mathbb{C}) \mid g(\mathbb{T}) = \mathbb{T}\}^\circ$$

where $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. Hence, if $h \in \mathrm{PSL}(2, \mathbb{C})$ with $h(\mathbb{R} \cup \infty) = \mathbb{T}$, then $h \mathrm{PSL}(2, \mathbb{R}) h^{-1} = \mathrm{PSU}(1, 1)$.]

- 3:31) Show that $\mathrm{SL}(2, \mathbb{R})$ is isogenous to $\mathrm{SO}(1, 2)$. [Hint: The Killing form $K(A, B) = \mathrm{trace}(AB)$ is a symmetric bilinear form of signature $(2, 1)$ on the Lie algebra of $\mathrm{SL}(2, \mathbb{R})$. It is invariant under the adjoint representation.]
- 3:32) Show that $\mathrm{SO}(3, \mathbb{C})$, $\mathrm{Sp}(2, \mathbb{C})$, and $\mathrm{SL}(2, \mathbb{C})$ are isogenous to each other. [Hint: Complexify Rem. 3.31(1a) or 3.31(1b).]
- 3:33) Show that $\mathrm{SO}(4)$ is isogenous to $\mathrm{SU}(2) \times \mathrm{SU}(2)$. [Hint: Let $\mathbb{H}^*$ be the group of unit quaternions. For any $g, h \in \mathbb{H}^*$, define $T_{g,h}: \mathbb{H} \rightarrow \mathbb{H}$ by $T_{g,h}(x) = g x h^{-1}$; then, after identifying $\mathbb{H}$ with $\mathbb{R}^4$, the linear map $T_{g,h}$ is orthogonal.]
- 3:34) Show that $\mathrm{SO}(1, 3)$ is isogenous to $\mathrm{SL}(2, \mathbb{C})$. [Hint: Let V be the real vector space of 2×2 skew-adjoint matrices. For any $g \in \mathrm{SL}(2, \mathbb{C})$ and $v \in V$, define $T_g(v) = g v g^*$. The determinant is a form of signature $(1, 3)$ on V that is preserved by T_g .]
- 3:35) Show that $\mathrm{SO}(2, 2)$ is isogenous to $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$. [Hint: The map $(g, h, T) \mapsto g T h^{-1}$ defines a representation of $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$ on $\mathrm{Mat}_{2 \times 2}(\mathbb{R})$. The determinant is an invariant quadratic form of signature $(2, 2)$.]
- 3:36) Prove 3.31(3d). [Hint: Complexify a known isogeny.]
- 3:37) Show that $\mathrm{SO}(2, \mathbb{H})$ is isogenous to $\mathrm{SU}(1, 1) \times \mathrm{SU}(2)$. [Hint: Let $\phi: \mathbb{C} \rightarrow \mathbb{H}$ be the embedding defined by $\phi(i) = j$. Then $\mathrm{SO}(2, \mathbb{H})$ contains

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \phi(\mathrm{SU}(1, 1)) \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}^{-1}$$

and $\phi(\mathrm{SU}(2))$.]

- 3:38) Show that $\mathrm{SO}(3, 3)$ is isogenous to $\mathrm{SL}(4, \mathbb{R})$. [Hint: Let $V = \mathbb{R}^4 \wedge \mathbb{R}^4$. Then $V \wedge V \cong (\mathbb{R}^4)^{\wedge 4} \cong \mathbb{R}$, so there is a natural bilinear form on V . It is symmetric, of signature $(3, 3)$.]
- 3:39) Show that if

$$\{G_1, G_2\} \subset \{\mathrm{SL}(2, \mathbb{R}), \mathrm{SL}(1, \mathbb{H}), \mathrm{SU}(2), \mathrm{SU}(1, 1)\},$$

and G_1 is isogenous to G_2 , then either $G_1 = G_2$, or $\{G_1, G_2\} = \{\mathrm{SL}(2, \mathbb{R}), \mathrm{SU}(1, 1)\}$, or $\{G_1, G_2\} = \{\mathrm{SL}(1, \mathbb{H}), \mathrm{SU}(2)\}$.

Some of the Structure of Semisimple Lie Groups

This chapter is very preliminary!!! Many explanations are missing. More topics will be added as additional chapters are written.

The reader is encouraged to skip this chapter on a first reading, and refer back to it when necessary.

4A. G is almost Zariski closed

One may note that each of the classical groups has only finitely many connected components. This is a special case of the following much more general result.

(4.1) Definition.

- We use $\mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$ to denote the set of real polynomials in the ℓ^2 variables $\{x_{i,j} \mid 1 \leq i, j \leq \ell\}$.
- For any $Q \in \mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$, and any $g \in \text{Mat}_{\ell \times \ell}(\mathbb{C})$, we use $Q(g)$ to denote the value obtained by substituting the matrix entries $g_{i,j}$ into the variables $x_{i,j}$. For example, if $Q = x_{1,1}x_{2,2} - x_{1,2}x_{2,1}$, then $Q(g)$ is the determinant of the first principal 2×2 minor of g .
- For any subset $\mathcal{Q}$ of $\mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$, let

$$\text{Var}(\mathcal{Q}) = \{g \in \text{SL}(\ell, \mathbb{R}) \mid Q(g) = 0, \forall Q \in \mathcal{Q}\}.$$

This is the *variety* associated to $\mathcal{Q}$.

- A subset H of $\text{SL}(\ell, \mathbb{R})$ is *Zariski closed* if there is a subset $\mathcal{Q}$ of $\mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$, such that $H = \text{Var}(\mathcal{Q})$. (In the special case where H is a subgroup of $\text{SL}(\ell, \mathbb{R})$, we may also say that H is a *real algebraic group* or an *algebraic group that is defined over $\mathbb{R}$* .)
- The *Zariski closure* of a subset H of $\text{SL}(\ell, \mathbb{R})$ is the (unique) smallest Zariski closed subset of $\text{SL}(\ell, \mathbb{R})$ that contains H . The Zariski closure is sometimes denoted $\overline{H}$.

(4.2) Example.

- 1) $\text{SL}(\ell, \mathbb{R})$ is Zariski closed. Let $\mathcal{Q} = \emptyset$.
- 2) The group of diagonal matrices in $\text{SL}(\ell, \mathbb{R})$ is Zariski closed. Let $\mathcal{Q} = \{x_{i,j} \mid i \neq j\}$.

3) For any $A \in \mathrm{GL}(\ell, \mathbb{R})$, the centralizer of A is Zariski closed. Let

$$\mathcal{Q} = \left\{ \sum_{k=1}^{\ell} (x_{i,k} A_{k,j} - A_{i,k} x_{k,j}) \mid 1 \leq i, j \leq \ell \right\}.$$

4) If we identify $\mathrm{SL}(n, \mathbb{C})$ with a subgroup of $\mathrm{SL}(2n, \mathbb{R})$, by identifying $\mathbb{C}$ with $\mathbb{R}^2$, then $\mathrm{SL}(n, \mathbb{C})$ is Zariski closed, because it is the centralizer of T_i , the linear transformation in $\mathrm{GL}(2n, \mathbb{R})$ that corresponds to scalar multiplication by i .

5) The classical groups of Egs. 3.22 and 3.23 are Zariski closed (if we identify $\mathbb{C}$ with $\mathbb{R}^2$ and $\mathbb{H}$ with $\mathbb{R}^4$ where necessary).

(4.3) **Example.** Let

$$H = \left\{ \begin{pmatrix} e^{2t} & 0 & 0 \\ 0 & e^{-t} & t \\ 0 & 0 & e^{-t} \end{pmatrix} \mid t \in \mathbb{R} \right\} \subset \mathrm{SL}(3, \mathbb{R}).$$

Then H is a 1-dimensional subgroup that is not Zariski closed. Its Zariski closure is

$$\overline{H} = \left\{ \begin{pmatrix} a^2 & 0 & 0 \\ 0 & 1/a & t \\ 0 & 0 & 1/a \end{pmatrix} \mid \begin{array}{l} a \in \mathbb{R} \setminus \{0\}, \\ t \in \mathbb{R} \end{array} \right\} \subset \mathrm{SL}(3, \mathbb{R}).$$

The point here is that the exponential function is transcendental, not polynomial, so no polynomial can capture the relation that ties the diagonal entries to the off-diagonal entry in H . Thus, as far as polynomials are concerned, the diagonal entries are independent of the off-diagonal entry, as we see in the Zariski closure.

(4.4) **Remark.** If H is Zariski closed, then the set $\mathcal{Q}$ of Defn. 4.1 can be chosen to be finite (because the ring $\mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$ is Noetherian).

Everyone knows that a (nonzero) polynomial in one variable has only finitely many roots. The following important fact generalizes this observation to any collection of polynomials in any number of variables.

(4.5) **Theorem.** *Any Zariski closed subset of $\mathrm{SL}(\ell, \mathbb{R})$ has only finitely many components.*

(4.6) **Definition.** A closed subgroup H of $\mathrm{SL}(\ell, \mathbb{R})$ is *almost Zariski closed* if H has only finitely many components, and there is a Zariski closed subgroup H_1 of $\mathrm{SL}(\ell, \mathbb{R})$ (which also has only finitely many components, by Thm. 4.5), such that $H^\circ = H_1^\circ$. In other words, in the terminology of §5B, H is *commensurable* with a Zariski closed subgroup.

(4.7) **Example.**

- Let H be the group of diagonal matrices in $\mathrm{SL}(2, \mathbb{R})$. Then H is Zariski closed (see 4.2(2)), but H° is not: any polynomial that vanishes on the diagonal matrices with positive entries will also vanish on the diagonal matrices with negative entries. So H° is almost Zariski closed, but it is not Zariski closed.
- Let $G = \mathrm{SO}(1, 2)^\circ$. Then G is almost Zariski closed (because $\mathrm{SO}(1, 2)$ is Zariski closed), but G is not Zariski closed (see Exer. 4:3).

These examples are typical: H is almost Zariski closed if and only if it is a finite-index subgroup of its Zariski closure.

The following fact gives the Zariski closure a central role in the study of semisimple Lie groups.

(4.8) **Theorem.** *If $G \subset \mathrm{SL}(\ell, \mathbb{R})$, then G is almost Zariski closed.*

Proof. Let $\overline{G}$ be the Zariski closure of G . Then $\overline{G}$ is semisimple. (For example, if G is irreducible in $\mathrm{SL}(\ell, \mathbb{C})$, then $\overline{G}$ is also irreducible, so Cor. 3.16 implies that $\overline{G}^\circ$ is semisimple.)

Because G is connected, we know that the normalizer $N(G)$ is Zariski closed (see Exer. 4:5). Therefore $\overline{G} \subset N(G)$, so G is a normal subgroup of $\overline{G}$. Hence (up to isogeny), we have $\overline{G} = G \times H$, for some closed, normal subgroup H of $\overline{G}$ (see Exer. 3:6).

Then $G = C_{\overline{G}}(H)^\circ$ is almost Zariski closed (see 4.2(3)). $\square$

(4.9) **Warning.** Theorem 4.8 relies on our standing assumption that G is semisimple (see 4.3). (Actually, it suffices to know that, besides being connected, G is perfect; that is, $G = [G, G]$ is equal to its commutator subgroup.)

(4.10) **Other terminology.**

- Other authors use $\mathrm{GL}(\ell, \mathbb{R})$ in the definition of $\mathrm{Var}(\mathcal{Q})$, instead of $\mathrm{SL}(\ell, \mathbb{R})$. Our choice leads to no loss of generality, and simplifies the theory slightly. (In the GL theory, one should, for technical reasons, stipulate that the function $1/\det(g)$ is a polynomial. In our setting, $\det g$ is the constant function 1, so this is not an issue.)
- What we call $\mathrm{Var}(\mathcal{Q})$ is actually only the *real* points of the variety. Algebraic geometers usually consider the solutions in $\mathbb{C}$, rather than $\mathbb{R}$, but our preoccupation with real Lie groups leads to our emphasis on real points.

4B. Real Jordan decomposition

(4.11) **Definition.** Let $g \in \mathrm{GL}(n, \mathbb{R})$. We say that g is

- 1) *semisimple* if g is diagonalizable (over $\mathbb{C}$);
- 2) *hyperbolic* if
 - g is semisimple, and
 - every eigenvalue of g is real and positive;
- 3) *elliptic* if
 - g is semisimple, and
 - every eigenvalue of g is on the unit circle in $\mathbb{C}$;
- 4) *unipotent* (or *parabolic*) if 1 is the only eigenvalue of g over $\mathbb{C}$.

(4.12) **Remark.** A matrix g is semisimple if and only if the minimal polynomial of g has no repeated factors.

- 1) Because its eigenvalues are real, any hyperbolic g element is diagonalizable over $\mathbb{R}$. That is, there is some $h \in \mathrm{GL}(\ell, \mathbb{R})$, such that $h^{-1}gh$ is a diagonal matrix.
- 2) An element is elliptic if and only if it is contained in some compact subgroup of $\mathrm{GL}(\ell, \mathbb{R})$. In particular, if g has finite order (that is, if $g^n = \mathrm{Id}$ for some $n > 0$), then g is elliptic.
- 3) A matrix $g \in \mathrm{GL}(\ell, \mathbb{R})$ is unipotent if and only if the characteristic polynomial of g is $(x - 1)^\ell$. (That is, 1 is the only root of the characteristic polynomial, with multiplicity ℓ .) Another way of saying this is that g is unipotent if and only if $g - \mathrm{Id}$ is nilpotent (that is, if and only if $(g - \mathrm{Id})^n = 0$ for some $n \in \mathbb{N}$).

(4.13) **Definition.** Let $g \in G$. If $G \subset \mathrm{SL}(\ell, \mathbb{R})$, then Defn. 4.11 applies to g . The results of this chapter show that it is consistent to extend this definition as follows, without an assumption that G is embedded in $\mathrm{SL}(\ell, \mathbb{R})$.

We say that g is

- 1) *hyperbolic* if there is a one-parameter subgroup H of G , such that $g \in H$, and $\text{Ad } h$ is a hyperbolic element of $\text{SL}(\mathfrak{g})$, for every $h \in H$;
- 2) *elliptic* if g is contained in a compact subgroup of G ;
- 3) *unipotent* (or *parabolic*) if there is a one-parameter subgroup H of G , such that $g \in H$, and $\text{Ad } h$ is a unipotent element of $\text{SL}(\mathfrak{g})$, for every $h \in H$.

(4.14) **Proposition** (Real Jordan Decomposition). *Any element g of G can be written uniquely as the product $g = aku$ of three **commuting** elements a, k, u of G , such that a is hyperbolic, k is elliptic, and u is unipotent.*

(4.15) **Proposition.** *Let $\rho: G \rightarrow \text{SL}(n, \mathbb{R})$ be any (continuous) homomorphism, and let $g \in G$.*

- 1) *If g is hyperbolic, then $\rho(g)$ is hyperbolic.*
- 2) *If g is elliptic, then $\rho(g)$ is elliptic.*
- 3) *If g is unipotent, then $\rho(g)$ is unipotent.*

Proof. (1) Haven't written it yet!!!

(2) Let K be a compact subgroup of G that contains g . Then $\rho(g)$ is in the compact subgroup $\rho(K)$, so $\rho(g)$ is elliptic.

(3) Assume $G = \text{SL}(2, \mathbb{R})$ and $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. (Theorem 4.16 shows that there is no loss of generality in making this assumption.) Let $a = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix}$. Then $a^{-n}ga^n \rightarrow \text{Id}$, so $\rho(a)^{-n}\rho(g)\rho(a)^n \rightarrow \text{Id}$. Since similar matrices have the same characteristic polynomial, this implies that the characteristic polynomial of $\rho(g)$ is the same as the characteristic polynomial of Id , which is $(x - 1)^n$. So $\rho(g)$ is unipotent. $\square$

4C. Jacobson-Morosov Lemma

(4.16) **Theorem** (Jacobson-Morosov Lemma). *For every unipotent element u of G , there is a subgroup H of G isogenous to $\text{SL}(2, \mathbb{R})$, such that $u \in H$.*

*In fact, if $G \subset \text{SL}(\ell, \mathbb{C})$, and F is any subfield of $\mathbb{C}$, such that $u \in G \cap \text{SL}(\ell, F)$, then there is a **polynomial** homomorphism $\phi: \text{SL}(2, \mathbb{R}) \rightarrow G$, such that $\phi \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = u$ and ϕ is defined over F (so $\phi(\text{SL}(2, F)) \subset G \cap \text{SL}(\ell, F)$).*

4D. Maximal compact subgroups and the Iwasawa decomposition

(4.17) **Proposition.** *Every compact subgroup of G is contained in a maximal compact subgroup, and all maximal compact subgroups of G are conjugate.*

(4.18) **Theorem.** *Let*

- K be a maximal compact subgroup of G ,
- A be a maximal $\mathbb{R}$ -split torus of G (see Defn. 8.5), and
- N be a maximal unipotent subgroup of G ,

such that N is normalized by A . Then the map $K \times A \times N \rightarrow G$ defined by $(k, a, n) \mapsto kan$ is a diffeomorphism.

(4.19) **Corollary.** *If K is any maximal compact subgroup of G , then G is homeomorphic to the cartesian product $K \times \mathbb{R}^n$, for some n . In particular, K is connected, and G is simply connected if and only if K is simply connected.*

Proof. Choose K , A , and N as in Thm. 4.18. Since A is an $\mathbb{R}$ -split torus, and N is a connected, unipotent group, each of A and N is homeomorphic to some Euclidean space. So the desired conclusion follows from Thm. 4.18. $\square$

4E. Cartan involution and Cartan decomposition

(4.20) **Definition.** An involution σ of G is a *Cartan involution* if the fixed-point set

$$\{g \in G \mid \sigma(g) = g\}$$

is a maximal compact subgroup of G .

(4.21) **Theorem.** *If K is any maximal compact subgroup of G , then there is a Cartan involution σ of G , such that K is the fixed-point set of σ .*

(4.22) **Example.** For $G = \mathrm{SL}(n, \mathbb{R})$ and $K = \mathrm{SO}(n)$, let $\sigma(g) = (g^{-1})^T$ (the transpose-inverse).

(4.23) **Theorem** (Cartan Decomposition). *Suppose σ is a Cartan involution of G , with fixed point set K . If A is any maximal $\mathbb{R}$ -split torus of G , such that $\sigma(a) = a^{-1}$, for all $a \in A$, then $G = KAK$.*

(4.24) **Example.** For G , K , and σ as in Eg. 4.22, we may let A be the group of positive diagonal matrices.

4F. The image of the exponential map

(4.25) **Proposition.** *Let $g \in G$.*

- 1) *If g is either hyperbolic or unipotent, then there is a connected, closed, 1-dimensional, abelian subgroup H of G , such that $g \in H$.*
- 2) *If g is elliptic, then*
 - (a) *there is a connected, 1-dimensional, abelian subgroup H_1 of G , such that $g \in H_1$ (but H_1 may not be closed); and*
 - (b) *there is a connected, compact, abelian subgroup H_2 of G , such that $g \in H_2$ (but we may have $\dim H > 1$).*

(4.26) **Warning.** There may be elements of G that do not belong to any connected, abelian subgroup. For example, $g = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ does not belong to any connected, abelian subgroup of $\mathrm{SL}(2, \mathbb{R})$.

(4.27) **Proposition.** *Let $g \in G$. For some $n > 0$, there is a connected, 1-dimensional, abelian subgroup H of G , such that $g^n \in H$.*

If g is not elliptic, then any such subgroup H is closed.

(4.28) **Warning.** Proposition 4.27 requires our standing assumption that G has finite center. For example, let H be the universal cover of $\mathrm{SL}(2, \mathbb{R})$, so H has infinite center, and let $\tilde{g}$ be any lift of the element g of Warn. 4.26. Then, for every $n > 0$, no connected, abelian subgroup of H contains $\tilde{g}^n$.

4G. Parabolic subgroups

(4.29) **Definition.** A closed subgroup P of G is *parabolic* if there is a hyperbolic element a of G , such that

$$P = \left\{ g \in G \mid \limsup_{n \rightarrow \infty} \|a^{-n}ga^n\| < \infty \right\}.$$

(4.30) **Remark.** G is a parabolic subgroup of G (let $a = e$), but it is the *proper* parabolic subgroups that are most interesting.

(4.31) **Example.**

- Up to conjugacy, there is only one (proper) parabolic subgroup of $\mathrm{SL}(2, \mathbb{R})$, namely $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$.
(Take a diagonal matrix a with $a_{1,1} > a_{2,2} > 0$.)
- Up to conjugacy, there are 3 (proper) parabolic subgroups of $\mathrm{SL}(3, \mathbb{R})$, namely

$$\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}, \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{pmatrix}, \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

To verify that these three subgroups are parabolic, take a diagonal matrices a , b , and c with

- 1) $a_{1,1} > a_{2,2} > a_{3,3} > 0$;
 - 2) $b_{1,1} = b_{2,2} > b_{3,3} > 0$; and
 - 3) $c_{1,1} > c_{2,2} = c_{3,3} > 0$.
- Up to conjugacy, there is only one (proper) parabolic subgroup P of $\mathrm{SO}(1, n)$. It is easier to describe P if we replace $\mathrm{Id}_{m,n}$ with a different symmetric matrix of the same signature: let $G = \mathrm{SO}(B; \mathbb{R})^\circ$, for

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & \mathrm{Id}_{(n-1) \times (n-1)} & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Then G is conjugate to $\mathrm{SO}(1, n)^\circ$ (cf. Exer. 3:13), and a parabolic subgroup in G is

$$\left\{ \begin{pmatrix} t & * & * \\ 0 & \mathrm{SO}(n-1) & * \\ 0 & 0 & 1/t \end{pmatrix} \right\}.$$

The following result explains that a parabolic subgroup of a classical group is simply the stabilizer of a (certain kind of) flag. (For the general case, including exceptional groups, the theory of real roots gives a good understanding of the parabolic subgroups.)

(4.32) **Definition.** Let $\langle \cdot | \cdot \rangle$ be a bilinear or Hermitian form on a vector space V . A subspace W of V is *totally isotropic* if $\langle W | W \rangle = 0$.

(4.33) **Theorem.** 1) A subgroup P of $\mathrm{SL}(n, \mathbb{R})$ is parabolic if and only if there is a chain $V_0 \subset V_1 \subset \cdots \subset V_k$ of subspaces of $\mathbb{R}^n$, such that

$$P = \{ g \in \mathrm{SL}(n, \mathbb{R}) \mid \forall i, gV_i = V_i \}.$$

Similarly for $\mathrm{SL}(n, \mathbb{C})$ and $\mathrm{SL}(n, \mathbb{H})$, taking chains of subspaces in $\mathbb{C}^n$ and $\mathbb{H}^n$.

- 2) A subgroup P of $\mathrm{SO}(m, n)$ is parabolic if and only if there is a chain $V_0 \subset V_1 \subset \cdots \subset V_k$ of **totally isotropic** subspaces of $\mathbb{R}^{m+n}$ (with respect to the form $\langle \cdot | \cdot \rangle_{\mathbb{R}^{m,n}}$ of Exer. 3:18), such that

$$P = \{ g \in \mathrm{SO}(m, n) \mid \forall i, gV_i = V_i \}.$$

Similarly for $\mathrm{SO}(n, \mathbb{C})$, $\mathrm{SO}(n, \mathbb{H})$, $\mathrm{Sp}(2m, \mathbb{R})$, $\mathrm{Sp}(2m, \mathbb{C})$, $\mathrm{SU}(m, n)$ and $\mathrm{Sp}(m, n)$.

(4.34) **Definition.** A bilinear form $B(x, y)$ on a vector space V is *isotropic* if $B(v, v) = 0$, for some nonzero $v \in V$. Otherwise, $B(x, y)$ is *anisotropic*.

(4.35) **Proposition.** Let $B(x, y)$ be a symmetric, bilinear form on a finite-dimensional vector space V over any field F of characteristic 0. If B is nondegenerate, then V can be decomposed as an orthogonal direct sum $V = W_1 \oplus W_2$, such that

- 1) there is a basis $\mathcal{B}$ of W_1 , such that the matrix of $B|_{W_1}$, with respect to this basis, is block diagonal, with each block being the 2×2 matrix

$$(4.36) \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and

- 2) the restriction of B to W_2 is anisotropic.

Proof. We may assume there is some nonzero $v \in V$, with $B(v, v) = 0$. (Otherwise, let $W_1 = 0$ and $W_2 = V$.) Because B is nondegenerate, there is some $w \in V$ with $B(v, w) \neq 0$. Multiplying w by a scalar, we may assume $B(v, w) = 1$.

For $t \in F$, we have

$$B(v, w + tv) = B(v, w) + tB(v, v) = 1 + t \cdot 0 = 1$$

and

$$B(w + tv, w + tv) = B(w, w) + 2tB(v, w) + t^2B(v, v) = B(w, w) + 2t.$$

Thus, we may assume $B(w, w) = 0$ (by replacing w with $w + tv$, where $t = -B(w, w)/2$).

Now the matrix of $B|_{\langle v, w \rangle}$, with respect to the basis $\{v, w\}$, is the 2×2 matrix (4.36). By induction on $\dim V$, we may assume there is an appropriate basis $\mathcal{B}'$ for $\langle v, w \rangle^\perp$. Let $\mathcal{B} = \{v, w\} \cup \mathcal{B}'$. $\square$

(4.37) **Theorem** (Witt's Theorem). Let $B(x, y)$ be a nondegenerate, symmetric, bilinear form on a vector space V over any field F . If

- W_1 and W_2 are any subspaces of V , and
- $\sigma: W_1 \rightarrow W_2$ is any linear map, such that $B(\sigma(v), \sigma(w)) = B(v, w)$, for every $v, w \in W_1$,

then there is an isometry $\hat{\sigma}$ of V , such that $\hat{\sigma}(v) = v$, for every $v \in W_1$.

(4.38) **Definition.** The *unipotent radical* of a subgroup H of G is the (unique) maximal unipotent, normal subgroup of H .

(4.39) **Theorem** (Langlands Decomposition). If P is parabolic, then we may write P in the form $P = MAN$, where

- A is an $\mathbb{R}$ -split torus,
- $MA = C_G(A)$,
- $M/Z(M)$ is semisimple,
- $Z(M)$ is compact, and

- N is the unipotent radical of P .

For some $a \in A$, we have

$$N = \left\{ g \in G \mid \lim_{n \rightarrow \infty} a^{-n} g a^n = e \right\}.$$

(4.40) **Proposition.**

- 1) The minimal parabolic subgroups of G are conjugate to each other.
- 2) A parabolic subgroup P is minimal if and only if, in the Langlands decomposition of P , the subgroup A is a maximal $\mathbb{R}$ -split torus of G .
- 3) A parabolic subgroup P is minimal if and only if, in the Langlands decomposition of P , the subgroup M is compact.
- 4) A parabolic subgroup P is minimal if and only if the unipotent radical of P is a maximal unipotent subgroup of G .

(4.41) **Remark.** Maximal parabolic subgroups are usually *not* all conjugate to each other. For example, we see from Eg. 4.31 that there are two conjugacy classes of maximal parabolic subgroups of $\mathrm{SL}(3, \mathbb{R})$. For classical groups, a maximal parabolic subgroup is the stabilizer of a single subspace; parabolics corresponding to subspaces of different dimension are not conjugate.

(4.42) **Remark.** If P is parabolic, then G/P is compact. The converse does not hold. (For example, if $P = MAN$ is a minimal parabolic, then $G/(AN)$ is compact, but AN is not parabolic unless M is trivial.) However, passing to the complexification does yield the converse: P is parabolic if and only if $G_{\mathbb{C}}/P_{\mathbb{C}}$ is compact. Furthermore, P is parabolic if and only if $P_{\mathbb{C}}$ contains a maximal solvable subgroup (“Borel subgroup”) of $G_{\mathbb{C}}$.

(4.43) **Theorem (Tits).** If U is any unipotent subgroup of G , then there is a parabolic subgroup P of G , such that

- 1) U is contained in the unipotent radical of P , and
- 2) $N_G(U) \subset P$.

(4.44) **Corollary.** The maximal unipotent subgroups of G are precisely the unipotent radicals of the minimal parabolic subgroups of G .

(4.45) **Corollary.** All maximal unipotent subgroups of G are conjugate.

(4.46) **Corollary.** If P is a parabolic subgroup of G , then $N_G(P) = P$.

(4.47) **Proposition.** Let U be a unipotent subgroup of $\mathrm{SL}(\ell, \mathbb{R})$.

- 1) If U has only finitely many components, then U is connected, Zariski closed, and simply connected.
- 2) Let $\overline{U}$ be the Zariski closure of U . Then $\overline{U}/U$ is compact.
- 3) If U is connected, and Λ is any lattice in U , then Λ is Zariski dense in U .

(4.48) **Proposition.** Let H be a Lie group, such that H° is a noncompact, simple Lie group. The group H is connected if and only if H is generated by unipotent elements.

4H. The normalizer of G

It is not difficult to see that if $\phi \in \mathrm{Aut}(\mathfrak{g})$, then $\det \phi = \pm 1$, so $\mathrm{Aut}(\mathfrak{g}) \subset \mathrm{SL}^\pm(\mathfrak{g})$. We have defined Zariski closures only for subgroups of subgroups of $\mathrm{SL}(\ell, \mathbb{R})$, but the same definition works in $\mathrm{SL}^\pm(\ell, \mathbb{R})$.

(4.49) **Proposition.** $\text{Aut}(\mathfrak{g})$ is a Zariski closed subgroup of $\text{SL}^\pm(\mathfrak{g})$.

Proof. For fixed $v, w \in \mathfrak{g}$, the relation

$$\phi([v, w]) = [\phi(v), \phi(w)]$$

is a polynomial equation in the matrix entries of ϕ (with respect to a basis of $\mathfrak{g}$). □

(4.50) **Theorem.** We have $\text{Aut}(\mathfrak{g})^\circ = \text{Ad } G$.

(4.51) **Notation.**

- An automorphism of G is *inner* if it is of the form $x \mapsto gxg^{-1}$, for some $g \in G$.
- The inner automorphisms form a subgroup of $\text{Aut}(G)$, denoted $\text{Inn}(G)$.
- The *outer automorphism group* of G is $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$.

Should make a table listing $\text{Out}(G)$ for each of the classical groups!!!

(4.52) **Corollary.**

- 1) $\text{Out}(G)$ is finite.
- 2) If G is a subgroup of any connected Lie group H , then $N_H(G)^\circ = C_H(G)^\circ G$.

4I. Fundamental group and center of G

For reference, Fig. 4.1 lists the fundamental group and center of each classical group. Each of these groups is connected, except that $\text{SO}(p, q)$ has two components if $\min\{p, q\} \geq 1$ (see Exers. 3:20 and 4:13). Also, each of these groups is simple, except $\text{SO}(4)$, $\text{SO}(2, 2)$, $\text{SO}(4, \mathbb{C})$, and $\text{SO}(2, \mathbb{H})$ (see 3.31(4)). The center of each of these groups consists of scalar matrices.

4J. Notes

Not written yet!!!

The book of Platonov and Rapinchuk [P-R, Chap. 3] provides a good discussion of algebraic groups over $\mathbb{R}$ (and other local fields). Thm. 4.8 is in Hochschild's book [Hoc2, Thms. 8.3.2 and 8.3.3, pp. 112–113].

Prop. 4.14 can be found in [Hel2, Lem. IX.7.1, p. 430].

Prop. 4.17 and Thm. 4.19 were proved by Iwasawa [Iwa, Thm. 6]. They can also be found in Hochschild's book [Hoc1, Thm 15.3.1, pp. 180–181].

For Witt's Thm. (4.37), [P-R, p. 93] refers to [Bourbaki, *Algèbre Commutative*, Chap. 9, pp. 396–398]. Need to check this reference (and look for others)!!!

4K. References

- [Hel2] S. Helgason: *Differential Geometry, Lie Groups, and Symmetric Spaces*. Academic Press, New York, 1978. (A revised edition is coming soon from the American Mathematical Society.)
- [Hoc1] G. Hochschild: *The Structure of Lie Groups*. Holden-Day, San Francisco, 1965.
- [Hoc2] G. Hochschild: *Basic Theory of Algebraic Groups and Lie Algebras*. Springer, New York, 1981.

G	restrictions	$\pi_1(G^\circ) = \pi_1(K^\circ)$	$Z(G^\circ)$
$\mathrm{SL}(\ell, \mathbb{R})$	$\ell \geq 2$	$\begin{cases} \mathbb{Z} & \text{if } \ell = 2 \\ \mathbb{Z}_2 & \text{if } \ell > 2 \end{cases}$	$\begin{cases} 0 & \text{if } \ell \text{ is odd} \\ \mathbb{Z}_2 & \text{if } \ell \text{ is even} \end{cases}$
$\mathrm{SL}(\ell, \mathbb{C})$	$\ell \geq 2$	0	$\mathbb{Z}_\ell$
$\mathrm{SL}(\ell, \mathbb{H})$	$\ell \geq 1$	0	$\mathbb{Z}_2$
$\mathrm{SU}(p, q)$	$p + q \geq 2$	$\begin{cases} 0 & \text{if } \min\{p, q\} = 0 \\ \mathbb{Z} & \text{if } \min\{p, q\} > 0 \end{cases}$	$\mathbb{Z}_{p+q}$
$\mathrm{SO}(p, q)$	$p + q \geq 3$	$\begin{cases} 0 & \text{if } \min\{p, q\} = 0 \\ \mathbb{Z} & \text{if } \{p, q\} = \{1, 2\} \\ \mathbb{Z}_2 & \text{if } \begin{cases} \min\{p, q\} = 1 \text{ and} \\ \max\{p, q\} \geq 3 \end{cases} \\ \mathbb{Z} \oplus \mathbb{Z} & \text{if } p = q = 2 \\ \mathbb{Z} \oplus \mathbb{Z}_2 & \text{if } \begin{cases} \min\{p, q\} = 2 \text{ and} \\ \max\{p, q\} \geq 3 \end{cases} \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 & \text{if } \min\{p, q\} \geq 3 \end{cases}$	$\begin{cases} 0 & \text{if either } p \text{ or } q \text{ is odd} \\ \mathbb{Z}_2 & \text{if } p \text{ and } q \text{ are even} \end{cases}$
$\mathrm{SO}(\ell, \mathbb{C})$	$\ell \geq 3$	$\mathbb{Z}_2$	$\begin{cases} 0 & \text{if } \ell \text{ is odd} \\ \mathbb{Z}_2 & \text{if } \ell \text{ is even} \end{cases}$
$\mathrm{SO}(\ell, \mathbb{H})$	$\ell \geq 2$	$\mathbb{Z}$	$\mathbb{Z}_2$
$\mathrm{Sp}(p, q)$	$p + q \geq 1$	0	$\mathbb{Z}_2$
$\mathrm{Sp}(\ell, \mathbb{R})$	$\ell \geq 2$ even	$\mathbb{Z}$	$\mathbb{Z}_2$
$\mathrm{Sp}(\ell, \mathbb{C})$	$\ell \geq 2$ even	0	$\mathbb{Z}_2$

Figure 4.1. The fundamental group and center of each classical group. (We use $\mathbb{Z}_r$ to denote the cyclic group of order r .)

[Iwa] K. Iwasawa: On some types of topological groups, *Ann. Math.* 50 (1949) 507–558.

[P-R] V. Platonov and A. Rapinchuk: *Algebraic Groups and Number Theory*. Academic Press, Boston, 1994.

Exercises

4:1) Show that if $\overline{H}$ is the Zariski closure of a subgroup H of G , then $g\overline{H}g^{-1}$ is the Zariski closure of gHg^{-1} , for any $g \in G$.

4:2) Suppose G is a connected, Zariski closed subgroup of $\mathrm{SL}(\ell, \mathbb{R})$ and that $\mathcal{Q} \subset \mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$.

(a) Show that $G \cap \mathrm{Var}(\mathcal{Q})$ is a closed subset of G .

(b) Show that if $G \not\subset \mathrm{Var}(\mathcal{Q})$, then $G \cap \mathrm{Var}(\mathcal{Q})$ does not contain any nonempty open subset of G .

(c) Show that if $G \not\subset \mathrm{Var}(\mathcal{Q})$, then $G \cap \mathrm{Var}(\mathcal{Q})$ has measure zero, with respect to the Haar measure on G .

[Hint: Need to give some hints for this!!!]

4:3) Show that $\mathrm{SO}(1, 2)^\circ$ is not Zariski closed. [Hint: We have

$$\frac{1}{2} \begin{pmatrix} s + \frac{1}{s} & s - \frac{1}{s} & 0 \\ s - \frac{1}{s} & s + \frac{1}{s} & 0 \\ 0 & 0 & 2 \end{pmatrix} \in \mathrm{SO}(1, 2)^\circ \quad \Leftrightarrow \quad s > 0.$$

If a rational function $f: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}$ vanishes on $\mathbb{R}^+$, then it also vanishes on $\mathbb{R}^-$.]

4:4) Show, for any subspace V of $\mathbb{R}^\ell$, that

$$\text{Stab}_{\text{SL}(\ell, \mathbb{R})}(V) = \{g \in \text{SL}(\ell, \mathbb{R}) \mid gV = V\}$$

is Zariski closed.

4:5) Show that if H is a connected Lie subgroup of $\text{SL}(\ell, \mathbb{R})$, then the normalizer $N(H)$ is Zariski closed. [Hint: $g \in N(H)$ if and only if $ghg^{-1} = \mathfrak{h}$, where $\mathfrak{h} \subset \text{Mat}_{\ell \times \ell}(\mathbb{R})$ is the Lie algebra of H .]

4:6) A Zariski-closed subset of $\text{SL}(\ell, \mathbb{R})$ is *irreducible* if it cannot be written as the union of two Zariski-closed, proper subsets. Show that every Zariski-closed subset A of $\text{SL}(\ell, \mathbb{R})$ has a unique decomposition as an irredundant, finite union of irreducible, Zariski-closed subsets. (By irredundant, we mean that no one of the sets is contained in the union of the others.) [Hint: The ascending chain condition on ideals of $\mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$ implies the descending chain condition on Zariski-closed subsets, so A can be written as a finite union of irreducibles. To make the union irredundant, the irreducible subsets must be maximal.]

4:7) Let H be a connected subgroup of $\text{SL}(\ell, \mathbb{R})$. Show that if $H \subset A_1 \cup A_2$, where A_1 and A_2 are Zariski-closed subsets of $\text{SL}(\ell, \mathbb{R})$, then either $H \subset A_1$ or $H \subset A_2$. [Hint: The Zariski closure $\overline{H} = B_1 \cup \dots \cup B_r$ is an irredundant union of irreducible, Zariski-closed subsets (see Exer. 4:6). For $h \in H$, we have $\overline{H} = hB_1 \cup \dots \cup hB_r$, so uniqueness implies that h acts as a permutation of $\{B_j\}$. Because H is connected, conclude that $\overline{H} = B_1$ is irreducible.]

4:8) Show that:

- (a) Id is the only element of $\text{GL}(\ell, \mathbb{R})$ that is both semisimple and unipotent; and
- (b) Id is the only element of $\text{GL}(\ell, \mathbb{R})$ that is both hyperbolic and elliptic.

4:9) Show (without using Prop. 4.14) that the Jordan decomposition $g = aku$ is unique, if it exists.

4:10) Show that if $g \in \text{GL}(\ell, F)$, for some subfield F of $\mathbb{C}$, and $g = aku$ is the Jordan decomposition of g , then $a, k, u \in \text{GL}(\ell, F)$. [Hint: For any Galois automorphism of $\mathbb{C}$ over F , uniqueness of the Jordan decomposition implies that $\sigma(a) = a$, $\sigma(k) = k$, and $\sigma(u) = u$.]

4:11) Show that if $g = aku$ is the Jordan decomposition of g , and h is any element of G that commutes with g , then h commutes with a , k , and u . [Hint: $h^{-1}gh = (h^{-1}ah)(h^{-1}kh)(h^{-1}uh)$.]

4:12) This exercise constructs a simple Lie group that has finite center, but is not linear. Let $G = \text{SL}(2, \mathbb{R})$.

- (a) Show that $\text{SL}(2, \mathbb{C})$ is simply connected.
- (b) Show that the fundamental group $\pi_1(G)$ is infinite cyclic. [Hint: From the Iwasawa decomposition $G = KAN$, we know that G is homeomorphic to $\text{SO}(2) \times \mathbb{R}^2$.]
- (c) Show that G has a (unique) cover G_k of any degree k .
- (d) Show that if $\rho: G_k \rightarrow \text{SL}(n, \mathbb{R})$ is any finite-dimensional representation of G_k , then there is a homomorphism $\sigma_{\mathbb{C}}: \text{SL}(2, \mathbb{C}) \rightarrow \text{SL}(n, \mathbb{C})$, such that $\sigma_{\mathbb{C}} \circ \pi = \rho$, where $\pi: G_k \rightarrow G$ is the covering map. [Hint: By complexifying $d\rho$, we obtain a Lie algebra homomorphism $d\rho_{\mathbb{C}}: \mathfrak{sl}(2, \mathbb{C}) \rightarrow \mathfrak{sl}(n, \mathbb{C})$. Now use the fact that $\text{SL}(2, \mathbb{C})$ is simply connected.]
- (e) Show $\ker \pi \subset \ker \rho$.
- (f) Show that if $k > 1$, then G_k is not linear.

4:13) Show that $\text{SO}(m, n)$ is not connected if $m, n > 0$. [Hint: The maximal compact subgroup is not connected.]

4:14) Prove ($\Leftarrow$) of Prop. 4.48.

4:15) Use Prop. 4.48 to show that $\mathrm{SL}(n, \mathbb{R})$ is connected.

Basic Properties of Lattices

Three definitions are crucial: lattice subgroups (5.8), commensurable subgroups (5.17), and irreducible lattices (5.23) and (5.24). The rest of the material in this chapter may not be essential for a first reading, and can be referred back to when necessary. However, if the reader has no prior experience with lattices, then the basic properties discussed in §5A will probably be helpful.

5A. Definition

(5.1) **Lemma.** *If Λ is a discrete subgroup of G , then there is a Borel fundamental domain for Λ in G . That is, there is a Borel subset $\mathcal{F}$ of G , such that the natural map $\mathcal{F} \rightarrow \Lambda \backslash G$ defined by $g \mapsto \Lambda g$ is bijective.*

Proof. Because Λ is discrete, there is a nonempty, open subset U of G , such that $(UU^{-1}) \cap \Lambda = \{e\}$. Since G is second countable (or, if you prefer, since G is σ -compact), there is a sequence $\{g_n\}$ of elements of G , such that $\bigcup_{n=1}^{\infty} Ug_n = G$. Let

$$\mathcal{F} = \bigcup_{n=1}^{\infty} \left(Ug_n \setminus \bigcup_{i < n} \Lambda Ug_i \right).$$

Then $\mathcal{F}$ is a Borel fundamental domain for Λ in G (see Exer. 5:2). □

(5.2) **Proposition.** *Let Λ be a discrete subgroup of G , and let μ be Haar measure on G . There is a unique (up to a scalar multiple) σ -finite, G -invariant Borel measure ν on $\Lambda \backslash G$.*

1) *For any Borel fundamental domain $\mathcal{F}$, the measure ν can be defined by*

$$(5.3) \quad \nu(\Lambda \backslash A) = \mu(A \cap \mathcal{F}),$$

for every Borel set A in G , such that $\Lambda A = A$.

2) *Conversely, for $A \subset G$, we have*

$$(5.4) \quad \mu(A) = \int_{\Lambda \backslash G} \#(A \cap \Lambda x) d\nu(\Lambda x).$$

Proof. See Exers. 5:4 and 5:5 for (1) and (2). The uniqueness of ν follows from (2) and the uniqueness of the Haar measure μ . □

(5.5) **Remark.** We always assume that the G -invariant measure ν on $\Lambda \backslash G$ is normalized so that (5.3) and (5.4) hold.

(5.6) **Corollary.** Let Λ be a discrete subgroup of G , and let $\phi: G \rightarrow \Lambda \backslash G$ be the natural quotient map $\phi(g) = \Lambda g$. If A is a Borel subset of G , such that the restriction $\phi|_A$ is injective, then $\nu(\phi(A)) = \mu(A)$.

(5.7) **Remark.**

- 1) The Haar measure μ on G is given by a smooth volume form, so the associated measure ν on $\Lambda \backslash G$ is also given by a volume form. Thus, we say that $\Lambda \backslash G$ has *finite volume* if $\nu(\Lambda \backslash G) < \infty$.
- 2) The assumption that Λ is discrete cannot be eliminated from Prop. 5.2. It can, however, be weakened to the assumption that Λ is closed and unimodular (see Exer. 5:6).

(5.8) **Definition.** A subgroup Γ of G is a *lattice* in G if

- Γ is a discrete subgroup of G , and
- $\Gamma \backslash G$ has finite volume.

(5.9) **Proposition.** Let Λ be a discrete subgroup of G , and let μ be Haar measure on G . The following are equivalent:

- 1) Λ is a lattice in G .
- 2) There is a Borel fundamental domain $\mathcal{F}$ for Λ in G , such that $\mu(\mathcal{F}) < \infty$.
- 3) There is a Borel subset C of G , such that $\Lambda C = G$ and $\mu(C) < \infty$.

Proof. (1 $\Leftrightarrow$ 2) From 5.3, we have $\nu(\Lambda \backslash G) = \mu(\mathcal{F})$. Thus, $\Lambda \backslash G$ has finite volume if and only if $\mu(\mathcal{F}) < \infty$.

(2 $\Rightarrow$ 3) Obvious.

(3 $\Rightarrow$ 1) We have $C \cap \Lambda x \neq \emptyset$, for every $x \in G$, so, from 5.4, we see that

$$\nu(\Lambda \backslash G) = \int_{\Lambda \backslash G} 1 d\nu(\Lambda x) \leq \int_{\Lambda \backslash G} \#(C \cap \Lambda x) d\nu(\Lambda x) = \mu(C) < \infty.$$

□

(5.10) **Example.** As mentioned in Eg. 1.22, $\mathrm{SL}(2, \mathbb{Z})$ is a lattice in $\mathrm{SL}(2, \mathbb{R})$.

(5.11) **Definition.** A closed subgroup Λ of G is *cocompact* (or *uniform*) if $\Lambda \backslash G$ is compact.

(5.12) **Corollary.**

- 1) Any cocompact, discrete subgroup of G is a lattice.
- 2) Any finite-index subgroup of a lattice is a lattice.

Proof. Exercises 5:9 and 5:10.

□

(5.13) **Remark.** Lattices in G are our main interest, but we will occasionally encounter lattices in Lie groups H that are not semisimple. If H is unimodular, then all of the above results remain valid with H in the place of G . In contrast, if H is not unimodular, then Prop. 5.2 may fail: there may not exist an H -invariant Borel measure on $\Lambda \backslash H$. Instead, one sometimes obtains only a semi-invariant measure ν :

$$\nu(Ah) = \Delta(h^{-1}) \nu(A),$$

where Δ is the modular function of H (see Exer. 5:11). This is sufficient to determine whether $\Lambda \backslash H$ has finite volume or not, so Defn. 5.8 applies.

For completeness, let us specifically state the following concrete generalization of Defn. 5.8 (cf. 5.9).

(5.14) **Definition.** A subgroup Λ of a Lie group H is a *lattice* in H if

- Λ is a discrete subgroup of H , and
- there is a Borel subset C of H , such that $\Lambda C = H$ and $\mu(C) < \infty$, where μ is the left Haar measure on H .

(5.15) **Example.** $\mathbb{Z}^n$ is a cocompact lattice in $\mathbb{R}^n$.

(5.16) **Proposition.** If a Lie group H has a lattice, then H is unimodular.

Proof. Let $\mathcal{F}$ be a Borel fundamental domain for Λ in H , such that $\mu(\mathcal{F}) < \infty$. Define a σ -finite Borel measure ν on $\Lambda \backslash H$ by

$$\nu(\Lambda \backslash A) = \mu(A \cap \mathcal{F}),$$

for every Borel set A in H , such that $\Lambda A = A$. The proof of Prop. 5.2(1) shows that $\nu(\Lambda \backslash Ah^{-1}) = \Delta(h) \nu(\Lambda \backslash A)$ (see Exer. 5:11). Since $H = Hh^{-1}$, this implies that

$$\nu(\Lambda \backslash H) = \nu(\Lambda \backslash Hh^{-1}) = \Delta(h) \nu(\Lambda \backslash H).$$

Since $\Lambda \backslash H$ has finite volume, we conclude that $\Delta(h) = 1$, as desired. $\square$

5B. Commensurability

As already mentioned in §3B, we usually wish to ignore the minor differences that come from taking finite covers; thus, if Γ' is a finite-index subgroup of Γ , then we usually do not wish to distinguish between Γ and Γ' . The following definition describes the resulting equivalence relation.

(5.17) **Definition.** Subgroups Λ_1 and Λ_2 of a group H are *commensurable* if $\Lambda_1 \cap \Lambda_2$ is a finite-index subgroup of both Λ_1 and Λ_2 . This is an equivalence relation on the collection of all subgroups of H (see Exer. 5:12).

(5.18) **Example.** 1) Two cyclic subgroups $a\mathbb{Z}$ and $b\mathbb{Z}$ of $\mathbb{R}$ are commensurable if and only if a is a nonzero rational multiple of b ; thus, commensurability of subgroups generalizes the classical notion of commensurability of real numbers.

2) It is easy to see (for example, from Cor. 5.12(2) and Exer. 5:7) that any subgroup commensurable with a lattice is itself a lattice.

The normalizer of a subgroup is very important in group theory. Because we are ignoring finite groups, the following definition is natural in our context.

(5.19) **Definition.** An element g of G *commensurates* Γ if $g^{-1}\Gamma g$ is commensurable with Γ . Let

$$\text{Comm}_G(\Gamma) = \{g \in G \mid g \text{ commensurates } \Gamma\}.$$

This is called the *commensurator* of Γ (or the *commensurability subgroup* of Γ).

(5.20) **Remark.** The commensurator of Γ may be much larger than the normalizer of Γ . For example, let $G = \text{SL}(n, \mathbb{R})$ and $\Gamma = \text{SL}(n, \mathbb{Z})$. Then $N_G(\Gamma)$ is commensurable with Γ (see 5.43), but $\text{SL}(n, \mathbb{Q}) \subset \text{Comm}_G(\Gamma)$ (see Exer. 5:13), so $\text{Comm}_G(\Gamma)$ is dense in G , even though $N_G(\Gamma)$ is discrete. Thus, in this example (and, more generally, whenever Γ is “arithmetic”), $N_G(\Gamma)$ has infinite index in Γ .

On the other hand, if $G = \text{SO}(1, n)$, then it is known that there are examples in which Γ , $N_G(\Gamma)$, and $\text{Comm}_G(\Gamma)$ are commensurable with each other (see Exer. 6:11 and Cor. 7.35).

(5.21) **Definition.** We say that two groups Λ_1 and Λ_2 are *virtually isomorphic* if some finite-index subgroup of Λ_1 is isomorphic to some finite-index subgroup of Λ_2 .

Note that if Λ_1 and Λ_2 are commensurable, then they are virtually isomorphic, but not conversely.

(5.22) **Other terminology.** Abstract group theorists often use the word *commensurable* for what we are calling “virtually isomorphic.”

5C. Irreducible lattices

Note that $\Gamma_1 \times \Gamma_2$ is a lattice in $G_1 \times G_2$. A lattice that can be decomposed as a product of this type is said to be *reducible*.

(5.23) **Definition.** Γ is *irreducible* if ΓN is dense in G , for every noncompact, closed, normal subgroup N of G .

In particular, if G is either simple or compact, then every lattice in G is irreducible. Conversely, if G is neither simple nor compact, then not every lattice in G is irreducible. To see this, assume, for simplicity, that G has trivial center. Then we may write G as a nontrivial direct product $G = G_1 \times G_2$, where each of G_1 and G_2 is semisimple. If we let Γ_i be any lattice in G_i , for $i = 1, 2$, then $\Gamma_1 \times \Gamma_2$ is a reducible lattice in G .

The following proposition shows (under mild assumptions) that every lattice is essentially a product of irreducible lattices. Thus, the preceding example provides essentially the only way to construct reducible lattices, so most questions about lattices can be reduced to the irreducible case. Our proof relies on some results from later sections of this chapter, so it should be skipped on a first reading.

(5.24) **Proposition.** *Assume*

- G has trivial center and
- Γ projects densely into the maximal compact factor of G .

There is a direct-product decomposition $G = G_1 \times \cdots \times G_r$, such that Γ is commensurable with $\Gamma_1 \times \cdots \times \Gamma_r$, where $\Gamma_i = \Gamma \cap G_i$, and Γ_i is an irreducible lattice in G_i , for each i .

Proof. We may assume Γ is reducible (otherwise, let $r = 1$). Thus, there is some noncompact, connected, closed, normal subgroup N of G , such that $N\Gamma$ is *not* dense in G ; let H be the closure of $N\Gamma$, and let $H_1 = H^\circ$. Because $\Gamma \subset H$, we know that Γ normalizes H_1 , so H_1 is a normal subgroup of G (see 5.40 and Exer. 5:16).

Let $\Lambda_1 = H_1 \cap \Gamma$. By definition, H_1 is open in H , so $H_1\Gamma$ is also open in H . On the other hand, we have $N \subset H_1$, and $N\Gamma$ is dense in H (by the definition of H), so we must have $H_1\Gamma = H$. Therefore $H_1\Gamma$ is closed in G , so Λ_1 is a lattice in H_1 (see 5.38).

Because H_1 is normal in G and G is semisimple (with trivial center), there is a normal subgroup H_2 of G , such that $G = H_1 \times H_2$ (see Exer. 3:6). Let $\Lambda = H_1 \cap (H_2\Gamma)$ be the projection of Γ to H_1 . Now Γ normalizes Λ_1 , and H_2 centralizes Λ_1 , so Λ must normalize Λ_1 . Therefore Cor. 5.43 implies that Λ is discrete (hence closed), so $H_2\Gamma = \Lambda \times H_2$ is closed, so $\Lambda_2 = H_2 \cap \Gamma$ is a lattice in H_2 (see 5.38).

Because Λ_1 is a lattice in H_1 and Λ_2 is a lattice in H_2 , we know that $\Lambda_1 \times \Lambda_2$ is a lattice in $H_1 \times H_2 = G$. Thus, $\Lambda_1 \times \Lambda_2$ has finite index in Γ (see 5:7).

By induction on $\dim G$, we may write $H_1 = G_1 \times \cdots \times G_s$ and $H_2 = G_{s+1} \times \cdots \times G_r$, so that $\Gamma \cap G_i$ is an irreducible lattice in G_i , for each i . $\square$

These results can be restated in the following geometric terms.

(5.25) **Definition.** Recall that a locally symmetric space $\Gamma \backslash X$ is *irreducible* if there do not exist (nontrivial) locally symmetric spaces $\Gamma_1 \backslash X_1$ and $\Gamma_2 \backslash X_2$, such that the product $(\Gamma_1 \backslash X_1) \times (\Gamma_2 \backslash X_2)$ finitely covers $\Gamma \backslash X$.

The following is obvious by induction on $\dim X$.

(5.26) **Proposition.** *There are irreducible locally symmetric spaces $\Gamma_1 \backslash X_1, \dots, \Gamma_r \backslash X_r$, such that the product $(\Gamma_1 \backslash X_1) \times \cdots \times (\Gamma_r \backslash X_r)$ finitely covers $\Gamma \backslash X$.*

The following is a restatement of Prop. 5.24 (in the special case where G has no compact factors).

(5.27) **Proposition.** *Let M be an irreducible locally symmetric space, such that the universal cover X of M has no compact factors, and no flat factors. For any nontrivial cartesian product decomposition $X = X_1 \times X_2$ of X , the image of X_1 is dense in M .*

We will see in Prop. 6.44 that $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$ has an irreducible lattice (for example, a lattice isomorphic to $\mathrm{SL}(2, \mathbb{Z}[\sqrt{2}])$). More generally, Thm. 6.26 shows that if all the simple factors of G are of the same type (see 3.29), then G has an irreducible lattice.

5D. Unbounded subsets of $\Gamma \backslash G$

Geometrically, it is clear, by looking at the fundamental domain constructed in Eg. 1.22, that the sequence $\{ni\}$ tends to ∞ in $\mathrm{SL}(2, \mathbb{Z}) \backslash \mathfrak{H}^2$. In this section, we give an algebraic criterion that determines whether or not a sequence tends to ∞ in $\Gamma \backslash G$, without any need for a fundamental domain.

Recall that the *injectivity radius* of a Riemannian manifold X is the maximal $r \geq 0$, such that, for every $x \in X$, the exponential map is a diffeomorphism on the open ball of radius r around x . If X is compact, then the injectivity radius is nonzero. The following proposition shows that the converse holds in the special case where $X = \Gamma \backslash G/K$ is locally symmetric of finite volume.

(5.28) **Proposition.** *For $g \in G$, define $\phi_g: G \rightarrow \Gamma \backslash G$ by $\phi_g(x) = \Gamma gx$. The homogeneous space $\Gamma \backslash G$ is compact if and only if there is a nonempty, open subset U of G , such that, for every $g \in G$, the restriction $\phi_g|_U$ of ϕ_g to U is injective.*

Proof. ($\Rightarrow$) Define $\phi: G \rightarrow \Gamma \backslash G$ by $\phi(x) = \Gamma x$. Then ϕ is a covering map, so, for each $p \in \Gamma \backslash G$, there is a connected neighborhood V_p of p , such that the restriction of ϕ to each component of $\phi^{-1}(V_p)$ is a diffeomorphism onto V_p . Since $\{V_p \mid p \in \Gamma \backslash G\}$ is an open cover of $\Gamma \backslash G$, and $\Gamma \backslash G$ is compact, there is a connected neighborhood U of e in G , such that, for each $p \in \Gamma \backslash G$, there is some $p' \in \Gamma \backslash G$, with $pU \subset V_{p'}$ (see Exer. 5:17). Then $\phi_g|_U$ is injective, for each $g \in G$.

($\Leftarrow$) We prove the contrapositive. Let U be any nonempty, precompact, open subset of G . (We wish to show, for some $g \in G$, that $\phi_g|_U$ is not injective.) If C is any compact subset of $\Gamma \backslash G$, then, because $\Gamma \backslash G$ is not compact, we have

$$(\Gamma \backslash G) \setminus (CU^{-1}) \neq \emptyset.$$

Thus, by induction on n , we may choose a sequence $\{g_n\}$ of elements of G , such that the open sets $\phi_{g_1}(U), \phi_{g_2}(U), \dots$ are pairwise disjoint. Since $\Gamma \backslash G$ has finite volume, these sets cannot all have the same volume, so, for some n , the restriction $\phi_{g_n}|_U$ is not injective (see 5.6). $\square$

Let us restate this geometric result in algebraic terms.

(5.29) **Notation.** For elements a and b of a group H , and subsets A and B of H , let

$$a^b = b^{-1}ab, \quad a^B = \{a^b \mid b \in B\}, \quad A^b = \{a^b \mid a \in A\}, \quad \text{and} \quad A^B = \{a^b \mid a \in A, b \in B\}.$$

(5.30) **Corollary.** $\Gamma \backslash G$ is compact if and only if the identity element e is **not** an accumulation point of Γ^G .

Proof. We have

$$\phi_g|_U \text{ is injective} \quad \Leftrightarrow \quad \nexists u_1, u_2 \in U, \Gamma gu_1 = \Gamma gu_2 \quad \Leftrightarrow \quad (g^{-1}\Gamma g) \cap (UU^{-1}) = \{e\}.$$

□

This has the following interesting consequence.

(5.31) **Corollary.** If Γ has a nontrivial, unipotent element, then $\Gamma \backslash G$ is not compact.

Proof. Suppose u is a nontrivial, unipotent element of Γ . The Jacobson-Morosov Lemma (4.16) implies that there is a continuous homomorphism $\phi: \mathrm{SL}(2, \mathbb{R}) \rightarrow G$ with

$$\phi \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = u.$$

Let

$$a = \phi \begin{bmatrix} 2 & 0 \\ 0 & 1/2 \end{bmatrix} \in G.$$

Then

$$a^{-n}ua^n = \phi \left(\begin{bmatrix} 2^{-n} & 0 \\ 0 & 2^n \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2^n & 0 \\ 0 & 2^{-n} \end{bmatrix} \right) = \phi \begin{bmatrix} 1 & 2^{-2n} \\ 0 & 1 \end{bmatrix} \rightarrow \phi \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e.$$

Thus, e is an accumulation point of u^G , so Cor. 5.31 implies that $\Gamma \backslash G$ is not compact. □

If G has no compact factors, then the converse of Cor. 5.31 is true (see §16D). However, this is not easy to prove, except in the special case where Γ is “arithmetic” (see §6E).

The proofs of Prop. 5.28 and Cor. 5.30 establish the following more general version of those results.

(5.32) **Definition.** A subset C of a topological space X is *precompact* (or *relatively compact*) if the closure of C is compact.

(5.33) **Proposition.** Let Λ be a lattice in a Lie group H , and let C be a subset of H . The image of C in $\Lambda \backslash H$ is precompact if and only if the identity element e is **not** an accumulation point of Λ^C .

The following is a similar elementary result that applies to the important special case where $G = \mathrm{SL}(\ell, \mathbb{R})$ and $\Gamma = \mathrm{SL}(\ell, \mathbb{Z})$, without relying on the fact that $\mathrm{SL}(\ell, \mathbb{Z})$ is a lattice. For convenience, the result discusses G/Γ , rather than $\Gamma \backslash G$ (because we write gv , not vg , for $g \in G$ and $v \in \mathbb{R}^\ell$). Since $\Gamma \backslash G$ is diffeomorphic to G/Γ (via the map $\Gamma g \mapsto g^{-1}\Gamma$), this change of notation is of no real significance.

(5.34) **Proposition** (Mahler Compactness Criterion). Suppose $C \subset \mathrm{SL}(\ell, \mathbb{R})$. The image of C in $\mathrm{SL}(\ell, \mathbb{R})/\mathrm{SL}(\ell, \mathbb{Z})$ is precompact if and only if 0 is **not** an accumulation point of

$$C\mathbb{Z}^\ell = \{cv \mid c \in C, v \in \mathbb{Z}^\ell\}.$$

Proof. ($\Rightarrow$) Since the image of C in $\mathrm{SL}(\ell, \mathbb{R})/\mathrm{SL}(\ell, \mathbb{Z})$ is precompact, there is a compact subset C_0 of G , such that $C \subset C_0 \mathrm{SL}(\ell, \mathbb{Z})$ (see Exer. 5:8). By enlarging C , we may assume that $C = C_0 \mathrm{SL}(\ell, \mathbb{Z})$. Then $C(\mathbb{Z}^\ell \setminus \{0\}) = C_0(\mathbb{Z}^\ell \setminus \{0\})$ is closed (since $\mathbb{Z}^\ell \setminus \{0\}$, being discrete, is closed and C_0 is compact), so $C(\mathbb{Z}^\ell \setminus \{0\})$ contains all of its accumulation points. In addition, since 0 is fixed by every element of C , we know that $0 \notin C(\mathbb{Z}^\ell \setminus \{0\})$. Therefore, 0 is not an accumulation point of $C(\mathbb{Z}^\ell \setminus \{0\})$.

($\Leftarrow$) To simplify the notation (while retaining the main ideas), let us assume $\ell = 2$ (see Exer. 5:23). Suppose $\{g_n\}$ is a sequence of elements of $\mathrm{SL}(2, \mathbb{R})$, such that 0 is **not** an accumulation point of $\cup_{n=1}^\infty g_n \mathbb{Z}^2$. It suffices to show that there is a sequence $\{\gamma_n\}$ of elements of $\mathrm{SL}(2, \mathbb{Z})$, such that $\{g_n \gamma_n\}$ has a convergent subsequence.

For each n , let

- $v_n \in \mathbb{Z}^2 \setminus \{0\}$, such that $\|g_n v_n\|$ is minimal,
- $\pi_n: \mathbb{R}^2 \rightarrow \mathbb{R} g_n v_n$ and $\pi_n^\perp: \mathbb{R}^2 \rightarrow (\mathbb{R} g_n v_n)^\perp$ be the orthogonal projections, and
- $w_n \in \mathbb{Z}^2 \setminus \mathbb{R} v_n$, such that $\|\pi_n^\perp(g_n w_n)\|$ is minimal.

By replacing w_n with $w_n + k v_n$, for some $k \in \mathbb{Z}$, we may assume $\|\pi_n(g_n w_n)\| \leq \|g_n v_n\|/2$. Note that the minimality of $\|g_n v_n\|$ implies

$$\|g_n v_n\| \leq \|g_n w_n\| \leq \|\pi_n^\perp(g_n w_n)\| + \|\pi_n(g_n w_n)\| \leq \|\pi_n^\perp(g_n w_n)\| + \frac{\|g_n v_n\|}{2},$$

so

$$(5.35) \quad \|\pi_n^\perp(g_n w_n)\| \geq \frac{\|g_n v_n\|}{2}.$$

Let C be the convex hull of $\{0, v_n, w_n\}$ and (thinking of v_n and w_n as column vectors) let $\gamma_n = (v_n, w_n) \in \mathrm{Mat}_{2 \times 2}(\mathbb{Z})$. From the minimality of $\|g_n v_n\|$ and $\|\pi_n^\perp(g_n w_n)\|$, we see that $C \cap \mathbb{Z}^2 = \{0, v_n, w_n\}$ (see Exer. 5:24), so $\det \gamma_n = \pm 1$. Thus, perhaps after replacing w_n with $-w_n$, we have $\gamma_n \in \mathrm{SL}(2, \mathbb{Z})$. Since $\gamma_n(1, 0) = v_n$ and $\gamma_n(0, 1) = w_n$, we may assume, by replacing g_n with $g_n \gamma_n$, that

$$v_n = (1, 0) \quad \text{and} \quad w_n = (0, 1).$$

Note that

$$(5.36) \quad \|\pi_n^\perp(g_n w_n)\| \|g_n v_n\| = \det g_n = 1.$$

By combining this with (5.35), we see that $\{g_n v_n\}$ is a bounded sequence, so, by passing to a subsequence, we may assume $g_n v_n$ converges to some vector v . By assumption, we have $v \neq 0$.

Now, from (5.36), and the fact that $\|g_n v_n\| \rightarrow \|v\|$ is bounded away from 0, we see that $\|\pi_n^\perp(g_n w_n)\|$ is bounded. Because $\|\pi_n(g_n w_n)\|$ is also bounded, we conclude that $\|g_n w_n\|$ is bounded. Hence, by passing to a subsequence, we may assume $g_n w_n$ converges to some vector w . From (5.35), we know that $\|\pi_n^\perp(g_n w_n)\| \not\rightarrow 0$, so $w \notin \mathbb{R} v$.

Since $v \neq 0$ and $w \notin \mathbb{R} v$, there is some $g \in \mathrm{GL}(\ell, \mathbb{R})$ with $g(1, 0) = v$ and $g(0, 1) = w$. We have

$$g_n(1, 0) = g_n v_n \rightarrow v = g(1, 0)$$

and, similarly, $g_n(0, 1) \rightarrow g(0, 1)$, so $g_n x \rightarrow g x$ for all $x \in \mathbb{R}^2$. Thus, $g_n \rightarrow g$, as desired. $\square$

5E. Intersection of Γ with other subgroups of G

(5.37) **Proposition.** *Let Λ and H be closed subgroups of G , such that $\Lambda \subset H$. Then Λ is a lattice in G if and only if*

- 1) Λ is a lattice in H ; and
- 2) G/H has a finite G -invariant volume.

Proof. Because $\Lambda \backslash G$ is a bundle over $H \backslash G$, with fiber $\Lambda \backslash H$, the conclusion is essentially a consequence of Fubini's Theorem. $\square$

(5.38) **Corollary.** *Let H be a closed, normal subgroup of G . If $\Gamma \cap H$ is a lattice in H , then $H\Gamma$ is closed in G .*

The converse holds if H is normal in G .

Proof. ($\Rightarrow$) Proposition 5.33 implies that the natural inclusion map $(\Gamma \cap H) \backslash H \hookrightarrow \Gamma \backslash G$ is proper (see Exer. 5:18); hence, its image is closed.

($\Leftarrow$) From 5.37(1), with $H\Gamma$ in the role of H , we know that Γ is a lattice in $H\Gamma$. Then the desired conclusion follows from the observation that $\Gamma \backslash H\Gamma$ is H -equivariantly diffeomorphic to $(\Gamma \cap H) \backslash H$. $\square$

5F. Borel Density Theorem and some consequences

In these results, we assume that Γ projects densely into the maximal compact factor of G . This hypothesis is satisfied (vacuously) if G has no compact factors.

(5.39) **Theorem** (Borel). *Assume*

- Γ projects densely into the maximal compact factor of G ;
- V is a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$; and
- $\rho: G \rightarrow \mathrm{GL}(V)$ is a continuous homomorphism.

Then:

- 1) *Let v be any element of V . If v is $\rho(\Gamma)$ -invariant, then v is $\rho(G)$ -invariant.*
- 2) *Let W be any subspace of V . If W is $\rho(\Gamma)$ -invariant, then W is $\rho(G)$ -invariant.*

Proof. For illustration, let us prove (1) in the special case where G/Γ is compact. Assume also that G has no compact factors (see Exer. 5:25); then G is generated by its unipotent elements (see 8.21), so it suffices to show that v is invariant under $\rho(u)$, for every nontrivial unipotent element u of G . Because $\rho(u)$ is unipotent (see 4.15(3)), we see that $\rho(u^n)v$ is a polynomial function of n . (Write $\rho(u) = \mathrm{Id} + T$, where $T^{r+1} = 0$ for some r . Then $\rho(u^n)v = (\mathrm{Id} + T)^n v = \sum_{k=0}^r \binom{n}{k} T^k v$.) Because G/Γ is compact and $\rho(\Gamma)v = v$, we know that $\rho(G)v$ is compact, so $\{\rho(u^n)v \mid n \in \mathbb{N}\}$ is bounded. A bounded polynomial must be constant, so we conclude that $\rho(u^n)v = v$ for all n ; in particular, $\rho(u)v = \rho(u^1)v = v$, as desired.

In the general case, (1) reduces to (2): $\mathbb{R}v$ (or $\mathbb{C}v$) must be $\rho(G)$ -invariant, but G admits no nontrivial homomorphism to the abelian group $\mathbb{R}^\times$ (or $\mathbb{C}^\times$), so we conclude that v is $\rho(G)$ -invariant.

(2) is a special case of Cor. 5.48 below (let $H = \Gamma$). $\square$

(5.40) **Corollary.** *Assume Γ projects densely into the maximal compact factor of G . If H is a connected, closed subgroup of G that is normalized by Γ , then H is normal in G .*

Proof. The Lie algebra $\mathfrak{h}$ of H is a subspace of the Lie algebra $\mathfrak{g}$ of G . Because $\Gamma \subset H$, we know that Γ normalizes H , so $\mathfrak{h}$ is invariant under $\mathrm{Ad}_G \Gamma$. From 5.39(2), we conclude that $\mathfrak{h}$ is invariant under $\mathrm{Ad} G$; thus, H is a normal subgroup of G . $\square$

(5.41) **Corollary.** *If Γ projects densely into the maximal compact factor of G , then $C_G(\Gamma) = Z(G)$.*

Proof. For simplicity, let us assume that G is linear; more precisely, assume $G \subset \mathrm{SL}(\ell, \mathbb{R})$, for some ℓ . Let $V = \mathrm{Mat}_{\ell \times \ell}(\mathbb{R})$ be the vector space of all real $\ell \times \ell$ matrices, so $G \subset V$. For $g \in G$ and $v \in V$, define $\rho(g)v = gv g^{-1}$, so $\rho: G \rightarrow \mathrm{GL}(V)$ is a continuous representation. If $c \in C_G(\Gamma)$, then $\rho(\gamma)c = \gamma c \gamma^{-1} = c$ for every $\gamma \in \Gamma$, so Thm. 5.39(1) implies that $\rho(G)c = c$. Therefore $c \in Z(G)$. $\square$

(5.42) **Corollary.** *Assume Γ projects densely into the maximal compact factor of G . If N is a finite, normal subgroup of Γ , then $N \subset Z(G)$.*

Proof. The quotient $\Gamma/C_\Gamma(N)$ is finite, because it embeds in the finite group $\mathrm{Aut}(N)$, so $C_\Gamma(N)$ is a lattice in G (see 5.12(2)). Then, because $N \subset C_G(C_\Gamma(N))$, Cor. 5.41 implies $N \subset Z(G)$. $\square$

(5.43) **Corollary.** *If Γ projects densely into the maximal compact factor of G , then Γ has finite index in $N_G(\Gamma)$.*

Proof. Because Γ is discrete, the identity component $N_G(\Gamma)^\circ$ of $N_G(\Gamma)$ must centralize Γ . So $N_G(\Gamma)^\circ \subset C_G(\Gamma) = Z(G)$ is finite. On the other hand, $N_G(\Gamma)^\circ$ is connected. Therefore, $N_G(\Gamma)^\circ$ is trivial, so $N_G(\Gamma)$ is discrete. Hence Γ has finite index in $N_G(\Gamma)$ (see Exer. 5:7). $\square$

(5.44) **Corollary** (Borel Density Theorem). *Assume $G \subset \mathrm{SL}(\ell, \mathbb{R})$. If Γ projects densely into the maximal compact factor of G , then Γ is Zariski dense in G . That is, if $Q \in \mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$ is a polynomial function on $\mathrm{Mat}_{\ell \times \ell}(\mathbb{R})$, such that $Q(\Gamma) = 0$, then $Q(G) = 0$.*

Proof. Let

$$\mathcal{Q} = \{ Q \in \mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}] \mid Q(\Gamma) = 0 \}.$$

By definition, we have $\Gamma \subset \mathrm{Var}(\mathcal{Q})$ (see Defn. 4.1). Since $\mathrm{Var}(\mathcal{Q})$ has only finitely many connected components (see 4.5), this implies that $\mathrm{Var}(\mathcal{Q})^\circ$ is a connected subgroup of G that contains a finite-index subgroup of Γ . Hence Cor. 5.40 implies that $\mathrm{Var}(\mathcal{Q})^\circ = G$ (see Exer. 5:31), so $G \subset \mathrm{Var}(\mathcal{Q})$, as desired. $\square$

5G. Proof of the Borel Density Theorem

(5.45) **Lemma** (Poincaré Recurrence Theorem). *Let*

- (Ω, d) be a metric space;
- $T: \Omega \rightarrow \Omega$ be a homeomorphism; and
- μ be a T -invariant probability measure on A .

Then, for almost every $a \in \Omega$, there is a sequence $n_k \rightarrow \infty$, such that $T^{n_k}a \rightarrow a$.

Proof. Let

$$A_\epsilon = \{ a \in \Omega \mid \forall m > 0, d(T^m a, a) > \epsilon \}.$$

It suffices to show $\mu(A_\epsilon) = 0$ for every ϵ .

Suppose $\mu(A_\epsilon) > 0$. Then we may choose a subset B of A_ϵ , such that $\mu(B) > 0$ and $\mathrm{diam}(B) < \epsilon$. Because the sets $B, T^{-1}B, T^{-2}B, \dots$ all have the same measure, and $\mu(\Omega) < \infty$, the sets cannot all be disjoint: there exists $m < n$, such that $T^{-m}B \cap T^{-n}B \neq \emptyset$. By applying T^n , we may assume $n = 0$. For $a \in T^{-m}B \cap B$, we have $T^m a \in B$ and $a \in B$, so

$$d(T^m a, a) \leq \mathrm{diam}(B) < \epsilon.$$

This contradicts the definition of A_ϵ . $\square$

(5.46) **Proposition.** *Assume*

- G has no compact factors;
- V is a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$;
- $\rho: G \rightarrow \mathrm{GL}(V)$ is a continuous homomorphism; and
- μ is a $\rho(G)$ -invariant probability measure on the projective space $\mathbb{P}(V)$.

Then μ is supported on the set of fixed points of $\rho(G)$.

Proof. Because G is generated by its unipotent elements (see 8.21), it suffices to show that μ is supported on the set of fixed points of $\rho(u)$, for every unipotent element u of G .

Let u be a unipotent element of G , and let $v \in V \setminus \{0\}$. Let $T = \rho(u) - \mathrm{Id}$. Then T is nilpotent (because $\rho(u)$ is unipotent (see 4.15(3))), so there is some integer $r \geq 0$, such that $T^r v \neq 0$, but $T^{r+1} v = 0$. We have

$$\rho(u)T^r v = (\mathrm{Id} + T)(T^r v) = T^r v + T^{r+1} v = T^r v + 0 = T^r v,$$

so $[T^r v] \in \mathbb{P}(V)$ is a fixed point for $\rho(u)$. Also, for each $n \in \mathbb{N}$, we have

$$\rho(u^n)[v] = \left[\sum_{k=0}^r \binom{n}{k} T^k v \right] = \left[\binom{n}{r}^{-1} \sum_{k=0}^r \binom{n}{k} T^k v \right] \rightarrow [T^r v]$$

(because, for $k < r$, we have $\binom{n}{k}/\binom{n}{r} \rightarrow 0$ as $n \rightarrow \infty$). Thus, $\rho(u^n)[v]$ converges to a fixed point of $\rho(u)$, as $n \rightarrow \infty$.

The Poincaré Recurrence Theorem (5.45) implies, for μ -almost every $[v] \in \mathbb{P}(V)$, that there is a sequence $n_k \rightarrow \infty$, such that $\rho(u^{n_k})[v] \rightarrow [v]$. On the other hand, we know, from the preceding paragraph, that $\rho(u^{n_k})[v]$ converges to a fixed point of $\rho(u)$. Thus, μ -almost every element of $\mathbb{P}(V)$ is a fixed point of $\rho(u)$. In other words, μ is supported on the set of fixed points of $\rho(u)$, as desired. $\square$

The assumption that G has no compact factors cannot be omitted from Prop. 5.46. For example, the usual Lebesgue measure is an $\mathrm{SO}(n)$ -invariant probability measure on S^{n-1} , but $\mathrm{SO}(n)$ has no fixed points on S^{n-1} . We can, however, make the following weaker statement.

(5.47) **Corollary.** *Assume*

- V is a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$;
- $\rho: G \rightarrow \mathrm{GL}(V)$ is a continuous homomorphism; and
- μ is a $\rho(G)$ -invariant probability measure on the projective space $\mathbb{P}(V)$.

Then there is a cocompact, closed, normal subgroup G' of G , such that μ is supported on the set of fixed points of $\rho(G')$.

Proof. Let K be the maximal connected, compact, normal subgroup of G , and write $G \approx G' \times K$, for some closed, normal subgroup G' of G . Then G' has no compact factors, so we may apply Prop. 5.46 to the restriction $\rho|_{G'}$. $\square$

(5.48) **Corollary** (Borel). *Assume*

- V is a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$;
- $\rho: G \rightarrow \mathrm{GL}(V)$ is a continuous homomorphism;
- H is a closed subgroup of G , such that G/H has finite volume, and H projects densely into the maximal compact factor of G ; and
- W is a $\rho(H)$ -invariant subspace of V .

Then W is $\rho(G)$ -invariant.

Proof. Let $d = \dim W$, and let μ be a G -invariant probability measure on G/H . Note that ρ induces a continuous homomorphism $\hat{\rho}: G \rightarrow \mathrm{GL}(\bigwedge^d V)$. Because $\hat{\rho}(H)$ fixes $\bigwedge^d W$, $\hat{\rho}$ induces a G -equivariant map $\hat{\rho}': G/H \rightarrow \mathbb{P}(\bigwedge^d V)$ with $\rho(eH) = [\bigwedge^d W]$. Then $\hat{\rho}'_*\mu$ is a $\rho(G)$ -invariant probability measure on $\mathbb{P}(\bigwedge^d V)$.

Let us assume, for simplicity, that G has no compact factors (see Exer. 5:36). In this case, Prop. 5.46 implies that $\hat{\rho}'(G/H)$ is contained in the set of fixed points of $\hat{\rho}(G)$. In particular, $[\bigwedge^d W]$ is fixed by $\hat{\rho}(G)$, so W is invariant under $\rho(G)$. $\square$

(5.49) **Corollary.** *Let H be a closed subgroup of G that projects densely into the maximal compact factor of G . If there is a G -invariant probability measure μ on G/H , then the identity component H° is normal in G .*

Proof. Because $\mathfrak{h}$ is invariant under $\mathrm{Ad}_G(H)$, we conclude from Cor. 5.48 that it is invariant under Ad_G . Therefore H° is normal in G . $\square$

The preceding corollary implies that there is no finite G -invariant measure on G/H , unless H is discrete. We remark that if H is not unimodular, then there is not even a σ -finite G -invariant measure on G/H (see Exer. 5:6), but we do not need this more general fact.

5H. Γ is finitely presented

In this section, we describe the proof that Γ is finitely presented. For the case where $\Gamma \backslash G$ is compact, this follows from the fact that the fundamental group of any compact manifold is finitely presented.

(5.50) **Definition.** Suppose Γ acts properly discontinuously on a topological space Y . A subset $\mathcal{F}$ of Y is a *weak fundamental domain* for Γ if

- 1) $\Gamma\mathcal{F} = Y$; and
- 2) $\{\gamma \in \Gamma \mid \gamma\mathcal{F} \cap \mathcal{F} \neq \emptyset\}$ is finite.

(5.51) **Proposition.** *Suppose a discrete group Λ acts properly discontinuously on a topological space Y . If Y is connected, and Λ has a weak fundamental domain $\mathcal{F}$ that is an open subset of Y , then Λ is finitely generated.*

Proof. Let $S = \{\lambda \in \Lambda \mid \lambda\mathcal{F} \cap \mathcal{F} \neq \emptyset\}$. We know that S is finite (see 5.50(2)), so it suffices to show that S generates Λ . Here is the idea: think of $\{\lambda\mathcal{F} \mid \lambda \in \Lambda\}$ as a tiling of Y . The elements of S can move $\mathcal{F}$ to any adjacent tile, and Y is connected, so a composition of elements of S can move $\mathcal{F}$ to any tile. Thus $\langle S \rangle$ is transitive on the set of tiles. Since S also contains the entire stabilizer of the tile $\mathcal{F}$, we conclude that $\langle S \rangle = \Lambda$.

Here is a more formal version of the proof. Suppose $\langle S \rangle \neq \Lambda$. (This will lead to a contradiction.) Now $U_\lambda = \langle S \rangle \lambda \mathcal{F}$ is open, for each $\lambda \in \Lambda$, and $\cup_{\lambda \in \Lambda} U_\lambda = \Lambda \mathcal{F} = Y$. Since Y is connected, this implies that there exists $\lambda \in \Lambda$, such that $U_\lambda \cap U_e \neq \emptyset$ (and $U_\lambda \neq U_e$). From the definition of U_λ , we must have $s_1 \lambda \mathcal{F} \cap s_2 \mathcal{F} \neq \emptyset$, for some $s_1, s_2 \in \langle S \rangle$. Then $s_2^{-1} s_1 \lambda \mathcal{F} \cap \mathcal{F} \neq \emptyset$, so, by definition of S , we have $s_2^{-1} s_1 \lambda \in S$. Hence $\lambda \in s_1^{-1} s_2 S \subset \langle S \rangle$. So

$$U_\lambda = \langle S \rangle \lambda \mathcal{F} = \langle S \rangle \mathcal{F} = U_e.$$

This is a contradiction. $\square$

(5.52) **Corollary.** *If $\Gamma \backslash G$ is compact, then Γ is finitely generated.*

Proof. Because $\Gamma \backslash G$ is compact, there is a compact subset C of G , such that $\Gamma C = G$ (see Exer. 5:8). Let $\mathcal{F}$ be a precompact, open subset of G , such that $C \subset \mathcal{F}$. Because $C \subset \mathcal{F}$, we have $\Gamma \mathcal{F} = G$. Because $\mathcal{F}$ is precompact, and Γ acts properly discontinuously on G , we know that 5.50(2) holds. Thus, $\mathcal{F}$ is a weak fundamental domain for Γ . $\square$

See Exer. 5:38 for an alternate proof of Cor. 5.52 that does not use the fact that G is connected.

(5.53) **Example.** Let $\mathcal{F}$ be the closed unit square in $\mathbb{R}^2$, so $\mathcal{F}$ is a weak fundamental domain for the usual action of $\mathbb{Z}^2$ on $\mathbb{R}^2$ by translations. Define S as in the proof of Prop. 5.51, so

$$S = \{ (m, n) \in \mathbb{Z}^2 \mid m, n \in \{-1, 0, 1\} \} = \{0, \pm a_1, \pm a_2, \pm a_3\},$$

where $a_1 = (1, 0)$, $a_2 = (0, 1)$, and $a_3 = (1, 1)$. Then S generates $\mathbb{Z}^2$; in fact, the subset $\{a_1, a_2\}$ generates.

Proposition 5.51 does not apply to this situation, because $\mathcal{F}$ is not open. We could enlarge $\mathcal{F}$ slightly, without changing S . Alternatively, the proposition can be proved under the weaker hypothesis that $\mathcal{F}$ is in the interior of $\cup_{s \in S} \mathcal{F}$ (see Exer. 5:47).

Note that $\mathbb{Z}^2$ has the presentation

$$\mathbb{Z}^2 = \langle x_1, x_2, x_3 \mid x_1 x_2 = x_3, x_2 x_1 = x_3 \rangle.$$

(More precisely, if F_3 is the free group on 3 generators x_1, x_2, x_3 , then there is a surjective homomorphism $\phi: F_3 \rightarrow \mathbb{Z}^2$, defined by

$$\phi(x_1) = a_1, \quad \phi(x_2) = a_2, \quad \phi(x_3) = a_3,$$

and the kernel of ϕ is the smallest normal subgroup of F_3 that contains both $x_1 x_2 x_3^{-1}$ and $x_2 x_1 x_3^{-1}$.) The relations in this presentation simply state that the product of two elements of S is equal to another element of S . The proof of the following proposition shows that relations of this type suffice to define Λ in a very general situation.

(5.54) **Proposition.** *Suppose Λ acts properly discontinuously on a topological space Y . If Y is 1-connected, and Λ has a weak fundamental domain $\mathcal{F}$ that is a connected, open subset of Y , then Λ is finitely presented.*

Proof. This is similar to Prop. 5.51, but somewhat more involved. As before, let $S = \{ \lambda \in \Lambda \mid \lambda \mathcal{F} \cap \mathcal{F} \neq \emptyset \}$. For each $s \in S$, define a formal symbol x_s , and let F be the free group on $\{x_s\}$. Finally, let $R = \{ x_s x_t x_{st}^{-1} \mid s, t, st \in S \}$, so R is a finite subset of F .

We have a homomorphism $\phi: F \rightarrow \Lambda$ determined by $\phi(x_s) = s$. From Prop. 5.51, we know that ϕ is surjective, and it is clear that $R \subset \ker(\phi)$. The main part of the proof is to show that $\ker \phi$ is the smallest normal subgroup of F that contains R . (Since R is finite, and $F/\ker \phi \cong \Lambda$, this implies that Λ is finitely presented, as desired.)

Let N be the smallest normal subgroup of F that contains R . (It is clear that $N \subset \ker(\phi)$; we wish to show $\ker(\phi) \subset N$.)

- Define an equivalence relation $\sim$ on $(F/N) \times \mathcal{F}$ by stipulating that $(fN, y) \sim (f'N, y')$ if and only if there exists $s \in S$, such that $x_s fN = f'N$ and $sy = y'$ (see Exer. 5:48).
- Let $\tilde{Y}$ be the quotient space $((F/N) \times \mathcal{F}) / \sim$.
- Define a map $\psi: (F/N) \times \mathcal{F} \rightarrow Y$ by $\psi(fN, y) = \phi(f^{-1})y$. (Note that, because $N \subset \ker(\phi)$, the map ψ is well defined.)

Because

$$\psi(x_s fN, sy) = (\phi(f^{-1})s^{-1})(sy) = \psi(fN, y),$$

we see that ψ factors through to a well-defined map $\tilde{\psi}: \tilde{Y} \rightarrow Y$.

Let $\tilde{\mathcal{F}}$ be the image of $(\ker(\phi)/N) \times \mathcal{F}$ in $\tilde{Y}$. Then it is obvious, from the definition of ψ , that $\tilde{\psi}(\tilde{\mathcal{F}}) = \mathcal{F}$. In fact, it is not difficult to see that $\tilde{\psi}^{-1}(\mathcal{F}) = \tilde{\mathcal{F}}$ (see Exer. 5:49).

For each $f \in F$, the image $\mathcal{F}_f$ of $(fN) \times \mathcal{F}$ in $\tilde{Y}$ is open (see Exer. 5:50), and, for $f_1, f_2 \in \ker(\phi)$, one can show that $\mathcal{F}_{f_1} \cap \mathcal{F}_{f_2} = \emptyset$ if $f_1 \not\equiv f_2 \pmod{N}$ (cf. Exer. 5:51). Thus, from the preceding paragraph, we see that $\tilde{\psi}$ is a covering map over $\mathcal{F}$. Since Y is covered by translates of $\mathcal{F}$, it follows that $\tilde{\psi}$ is a covering map. Furthermore, the degree of this covering map is $|\ker(\phi)/N|$.

Because $\mathcal{F}$ is connected, it is not difficult to see that $\tilde{Y}$ is connected (see Exer. 5:52). Since Y is simply connected, and $\tilde{\psi}$ is a covering map, this implies that $\tilde{\psi}$ is a homeomorphism. Hence, the degree of the cover is 1, so $|\ker(\phi)/N| = 1$. This means $\ker(\phi) = N$, as desired. $\square$

(5.55) **Remark.** The assumption that $\mathcal{F}$ is connected can be replaced with the assumption that Y is locally connected. However, the proof is somewhat more complicated in this setting.

(5.56) **Corollary.** *If $\Gamma \backslash G$ is compact, then Γ is finitely presented.*

Proof. Let K be a maximal compact subgroup of G , so G/K is a 1-connected symmetric space, on which Γ acts properly discontinuously. Arguing as in the proof of Cor. 5.52, we see that Γ has a fundamental domain $\mathcal{F}$ that is an open subset of G/K , so Prop. 5.54 implies that Γ is finitely presented. $\square$

If $\Gamma \backslash G$ is not compact, then it is more difficult to prove that Γ is finitely presented (or even finitely generated).

(5.57) **Theorem.** *Γ is finitely presented.*

Idea of proof. It suffices to find a weak fundamental domain for Γ that is a connected, open subset of G/K . Assume, without loss of generality, that Γ is irreducible.

In each of the following two cases, a weak fundamental domain $\mathcal{F}$ can be constructed as the union of finitely many translates of “Siegel Domains.” (This will be discussed in Chap. 14.)

- 1) Γ is “arithmetic,” as defined in (6.16); or
- 2) G has a simple factor of real rank one (or, more generally, $\mathbb{Q}$ -rank(Γ) ≤ 1).

The (amazing!) Margulis Arithmeticity Theorem (6.21) implies that these two cases are exhaustive, which completes the proof. $\square$

(5.58) **Remark.** It is not necessary to appeal to the Margulis Arithmeticity Theorem if one wishes only to prove that Γ is finitely generated (not finitely presented). Namely, if (2) does not apply, then the real rank of every simple factor of G is at least two, so Kazhdan’s Property (T) (which will be discussed in Vol. 2) implies that Γ is finitely generated (see 20.19(2)).

5I. Γ has a torsion-free subgroup of finite index

(5.59) **Definition.** Γ is *torsion free* if Γ has no nontrivial finite subgroups. Equivalently, the identity element e is the only element of Γ of finite order.

(5.60) **Theorem** (Selberg’s Lemma). *If G is linear, then Γ has a torsion-free subgroup of finite index.*

Proof. Because G is linear, we may assume $\Gamma \subset \mathrm{SL}(\ell, \mathbb{R})$, for some ℓ . Let us start with an illustrative special case.

Case 1. Assume $\Gamma = \mathrm{SL}(\ell, \mathbb{Z})$. For any positive integer n , the natural ring homomorphism $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ induces a group homomorphism $\Gamma \rightarrow \mathrm{SL}(n, \mathbb{Z}/n\mathbb{Z})$ (see Exer. 5:39); let Γ_n be the kernel of this homomorphism. (This is called the *principal congruence subgroup* of $\mathrm{SL}(\ell, \mathbb{Z})$ of level n .) It is a finite-index, normal subgroup of Γ (see Exers. 5:40c and 5:41). It suffices to show that Γ_n is torsion free, for some n .

We show that Γ_n is torsion free whenever $n \geq 3$. It is easy to see that n is divisible either by 2^2 or by some prime $p \geq 3$. Thus, because $\Gamma_n \subset \Gamma_m$ whenever m is a divisor of n , there is no harm in assuming that n is a prime power: say $n = p^a$. Furthermore, either p is odd, or $a \geq 2$.

Given $\gamma \in \Gamma_n \setminus \{\mathrm{Id}\}$ and $k \in \mathbb{N} \setminus \{0\}$, we wish to show that $\gamma^k \neq \mathrm{Id}$. We may write

$$\gamma = \mathrm{Id} + p^d T,$$

where

- $d \geq a$,
- $T \in \mathrm{Mat}_{n \times n}(\mathbb{Z})$, and
- $p \nmid T$ (that is, not every matrix entry of T is divisible by p).

Also, we may assume k is prime (see Exer. 5:42). Thus, either $p \nmid k$ or $p = k$.

Subcase 1.1. Assume $p \nmid k$. Noting that

$$(p^d T)^2 = p^{2d} T^2 \equiv 0 \pmod{p^{d+1}},$$

and using the Binomial Theorem, we see that

$$\gamma^k = (\mathrm{Id} + p^d T)^k \equiv \mathrm{Id} + k(p^d T) \not\equiv \mathrm{Id} \pmod{p^{d+1}},$$

as desired.

Subcase 1.2. Assume $p = k$. Using the Binomial Theorem, we have

$$\gamma^k = (\mathrm{Id} + p^d T)^k \equiv \mathrm{Id} + k(p^d T) = \mathrm{Id} + p^{d+1} T \not\equiv \mathrm{Id} \pmod{p^{d+2}}.$$

(Note that if $p = 2$, then the congruence requires $d \geq 2$ (see Exer. 5:43).)

Case 2. Assume $\Gamma \subset \mathrm{SL}(\ell, \mathbb{Z})$. From Case 1, we know there is a torsion-free, finite-index subgroup Λ of $\mathrm{SL}(\ell, \mathbb{Z})$. Then $\Gamma \cap \Lambda$ is a torsion-free subgroup of finite index in Γ .

Case 3. The general case. The proof is very similar to Case 1, with the addition of some commutative algebra (or algebraic number theory) to account for the more general setting.

Because Γ is finitely generated (see 5.57), there exist $a_1, \dots, a_r \in \mathbb{C}$, such that every matrix entry of every element of Γ is contained in the ring $Z = \mathbb{Z}[a_1, \dots, a_r]$ generated by $\{a_1, \dots, a_r\}$ (see Exer. 5:44). Thus, letting $\Lambda = \mathrm{SL}(\ell, Z)$, we have $\Gamma \subset \Lambda$.

Now let $\mathfrak{p}$ be a maximal ideal in Z . Then $Z/\mathfrak{p}$ is a field, so, because $Z/\mathfrak{p}$ is also known to be a finitely generated ring, it must be a finite field. Thus, the kernel of the natural homomorphism $\Lambda \rightarrow \mathrm{SL}(\ell, Z/\mathfrak{p})$ has finite index in Λ . Basic facts of Algebraic Number Theory allow us to work with the prime ideal $\mathfrak{p}$ in very much the same way as we used the prime number p in Case 1. $\square$

Let us now present an alternate approach to the general case of Thm. 5.60. It requires only the Nullstellensatz, not Algebraic Number Theory.

Another proof of Thm. 5.60. Let

- Z be the subring of $\mathbb{C}$ generated by the matrix entries of the elements of Γ , and
- F be the quotient field of Z .

Because Γ is a finitely generated group (see 5.57), we know that Z is a finitely generated ring (see Exer. 5:44), so F is a finitely generated extension of $\mathbb{Q}$.

Step 1. We may assume that $F = \mathbb{Q}(x_1, \dots, x_r)$ is a purely transcendental extension of $\mathbb{Q}$. Choose a subfield $L = \mathbb{Q}(x_1, \dots, x_r)$ of F , such that

- L is a purely transcendental extension of $\mathbb{Q}$, and
- F is an algebraic extension of L .

Let d be the degree of F over L . Because F is finitely generated (and algebraic over L), we know that $d < \infty$. Thus, we may identify F^ℓ with $L^{d\ell}$, so there is an embedding

$$\Gamma \subset \mathrm{SL}(\ell, F) \hookrightarrow \mathrm{SL}(d\ell, L).$$

Thus, by replacing F with L (and replacing ℓ with $d\ell$), we may assume that F is purely transcendental.

Step 2. If γ is any element of finite order in $\mathrm{SL}(\ell, F)$, then $\mathrm{trace}(\gamma) \in \mathbb{Z}$, and $|\mathrm{trace}(\gamma)| \leq \ell$. There is a positive integer k with $\gamma^k = \mathrm{Id}$, so every eigenvalue of γ is a k^{th} root of unity. The trace of γ is the sum of these eigenvalues, and any root of unity is an algebraic integer, so we conclude that the trace of γ is an algebraic integer.

Since $\mathrm{trace}(\gamma)$ is the sum of the diagonal entries of γ , we know $\mathrm{trace}(\gamma) \in F$. Since $\mathrm{trace}(\gamma)$ is algebraic, but F is a purely transcendental extension of $\mathbb{Q}$, this implies $\mathrm{trace}(\gamma) \in \mathbb{Q}$. Since $\mathrm{trace}(\gamma)$ is an algebraic integer, this implies $\mathrm{trace}(\gamma) \in \mathbb{Z}$.

Since $\mathrm{trace}(\gamma)$ is the sum of ℓ roots of unity, and every root of unity is on the unit circle, we see, from the triangle inequality, that $|\mathrm{trace}(\gamma)| \leq \ell$.

Step 3. There is a prime number $p > 2\ell$, such that $1/p \notin Z$. From the Nullstellensatz (I.55), we know that there is a nontrivial homomorphism $\phi: Z \rightarrow \overline{\mathbb{Q}}$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Replacing Z with $\phi(Z)$, let us assume that $Z \subset \overline{\mathbb{Q}}$. Thus, for each $z \in Z$, there is some nonzero integer n , such that nz is an algebraic integer. More precisely, because Z is finitely generated, there is an integer n , such that, for each $z \in Z$, there is some positive integer k , such that $n^k z$ is an algebraic integer. It suffices to choose p so that it is not a divisor of n .

Step 4. There is a finite field E of characteristic p , and a nontrivial homomorphism $\phi_p: Z \rightarrow E$. Because $1/p \notin Z$, there is a maximal ideal $\mathfrak{p}$ of Z , such that $p \in \mathfrak{p}$. Then $E = Z/\mathfrak{p}$ is a field of characteristic p . Because it is a finitely generated ring, E must be a finite extension of the prime field $\mathbb{Z}_p$ (see I.52), so E is finite.

Step 5. Let Λ be the kernel of the induced homomorphism $\hat{\phi}_p: \mathrm{SL}(\ell, Z) \rightarrow \mathrm{SL}(\ell, E)$. Then Λ is torsion free. Let γ be an element of finite order in Λ . Then

$$\mathrm{trace}(\phi_p(\gamma)) = \mathrm{trace}(\mathrm{Id}) = \ell \pmod{p},$$

so $p \mid (\ell - \mathrm{trace}(\gamma))$. Thus, from Step 2 and the fact that $p > 2\ell$, we see that $\mathrm{trace}(\gamma) = \ell$. Since the ℓ eigenvalues of γ are roots of unity, and $\mathrm{trace}(\gamma)$ is the sum of these eigenvalues, we conclude that 1 is the only eigenvalue of γ . Since $\gamma^k = \mathrm{Id}$, we know that γ is elliptic (hence, diagonalizable over $\mathbb{C}$), so this implies $\gamma = \mathrm{Id}$, as desired. $\square$

If $\gamma^k = \text{Id}$, then every eigenvalue of γ must be a k^{th} root of unity. If, in addition, $\gamma \neq \text{Id}$, then at least one of these roots of unity must be nontrivial. Thus, the following is a strengthening of Thm. 5.60.

(5.61) **Theorem.** *There is a finite-index subgroup Γ' of Γ , such that no eigenvalue of any element of Γ' is a nontrivial root of unity.*

Proof. Assume $\Gamma = \text{SL}(\ell, \mathbb{Z})$. Let

- n be some (large) natural number,
- Γ_n be the principal congruence subgroup of Γ of level n ,
- ω be a nontrivial k^{th} root of unity, for some k ,
- γ be an element of Γ_n , such that ω is an eigenvalue of γ ,
- $T = \gamma - \text{Id}$,
- $Q(x)$ be the characteristic polynomial of T , and
- $\lambda = \omega - 1$, so λ is a nonzero eigenvalue of T .

Since $\gamma \in \Gamma_n$, we know that $n|T$, so $Q(x) = x^\ell + nR(x)$, for some integral polynomial $R(x)$. Since $Q(\lambda) = 0$, we conclude that $\lambda^\ell = n\zeta$, for some $\zeta \in \mathbb{Z}[\lambda]$. Thus, λ^ℓ is divisible by n , in the ring of algebraic integers.

The proof can be completed by noting that any particular nonzero algebraic integer is divisible by only finitely many natural numbers, and there are only finitely many roots of unity that satisfy a monic integral polynomial of degree ℓ . See Exer. 5:53 for a slightly different argument. $\square$

- (5.62) **Remark.** 1) Arguing more carefully, one can obtain a finite-index subgroup Γ' with the stronger property that, for every $\gamma \in \Gamma'$, the multiplicative group generated by the (complex) eigenvalues of γ does not contain any nontrivial roots of unity. Such a subgroup is sometimes called *net* (after the french for “nice,” apparently).
- 2) The results of this section remain valid if Γ is replaced with any finitely generated, linear group Λ . The general statement is that if F is any field of characteristic zero, then any finitely generated subgroup of $\text{SL}(\ell, F)$ has a subgroup of finite index that is torsion-free (or, more precisely, net).

The proof of Thm. 5.60 shows that Γ has nontrivial, proper, normal subgroups, so Γ is not simple. One may note that the normal subgroups constructed there all have finite index; in fact, as we will see in Vol. 2, it is often the case that every normal subgroup of Γ has finite index (see 23A). Moreover, as will also be discussed in Vol. 2, it is often the case that all of the normal subgroups of finite index are essentially of the type constructed in the course of the proof (this is the “Congruence Subgroup Property”) (see 23D).

(5.63) **Warning.** The hypothesis that G is linear cannot be omitted from Thm. 5.60 (see §23E).

5J. Γ has a nonabelian free subgroup

In this section, we describe the main ideas in the proof of the following important result.

(5.64) **Theorem** (Tits Alternative). *If Λ is a subgroup of $\text{SL}(\ell, \mathbb{R})$, then either*

- 1) Λ contains a nonabelian free subgroup; or
- 2) Λ has a solvable subgroup of finite index.

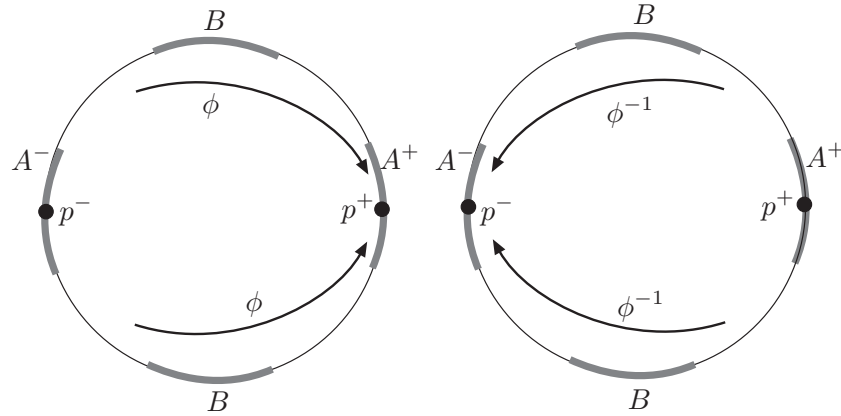


Figure 5.1. A typical (A^-, B, A^+) -contracting homeomorphism on the circle.

Since Γ is not solvable (see Exer. 5:27), the following is an immediate corollary.

(5.65) **Corollary.** *If G is not compact, then Γ contains a nonabelian free subgroup.*

(5.66) **Definition.** Let us say that a homeomorphism ϕ of a topological space M is (A^-, B, A^+) -contracting if A^-, B and A^+ are nonempty, disjoint, open subsets of M , such that $\phi(B \cup A^+) \subset A^+$ and $\phi^{-1}(B \cup A^-) \subset A^-$.

In a typical example, A^- and A^+ are small neighborhoods of points p^- and p^+ , such that ϕ collapses a large open subset of M into A^+ , and ϕ^{-1} collapses a large open subset of M into A^- (see Fig. 5.1).

(5.67) **Example.** Let

- M be the real projective line $\mathbb{P}(\mathbb{R}^2)$,
- $\gamma = \begin{bmatrix} 2 & 0 \\ 0 & 1/2 \end{bmatrix} \in \text{SL}(2, \mathbb{R})$,
- A^- be any (small) neighborhood of $p^- = [0 : 1]$ in $\mathbb{P}(\mathbb{R}^2)$,
- A^+ be any (small) neighborhood of $p^+ = [1 : 0]$ in $\mathbb{P}(\mathbb{R}^2)$, and
- B be any precompact, open subset of $\mathbb{P}(\mathbb{R}^2) \setminus \{p^-, p^+\}$.

For any $(x, y) \in \mathbb{R}^2$ with $x \neq 0$, we have

$$\gamma^n[x : y] = [2^n x : 2^{-n} y] = [1 : 2^{-2n} y/x] \rightarrow [1 : 0] = p^+$$

as $n \rightarrow \infty$, and the convergence is uniform on compact subsets. Similarly, $\gamma^{-n}[x : y] \rightarrow p^-$ as $n \rightarrow \infty$. Thus, for sufficiently large n , the homeomorphism γ^n is (A^-, B, A^+) -contracting on $\mathbb{P}(\mathbb{R}^2)$.

More generally, if γ is any nontrivial, hyperbolic element of $\text{SL}(2, \mathbb{R})$, then γ^n is (A^-, B, A^+) -contracting on $\mathbb{P}(\mathbb{R}^2)$, for some appropriate choice of A^-, B , and A^+ (see Exer. 5:54).

The following is easy to prove by induction on n .

(5.68) **Lemma.** *If ϕ is (A^-, B, A^+) -contracting, then*

- 1) $\phi^n(B) \subset A^+$ for all $n > 0$,
- 2) $\phi^n(B) \subset A^-$ for all $n < 0$,
- 3) $\phi^n(B) \subset A^- \cup A^+$ for all $n \neq 0$.

The following lemma is the key to the proof of Thm. 5.64.

(5.69) **Lemma** (Ping-Pong Lemma). *Suppose*

- ϕ and ψ are homeomorphisms of a topological space M ;
- $A^-, A^+, B^-,$ and B^+ are nonempty, pairwise-disjoint, open subsets of M ,
- ϕ is (A^-, B, A^+) -contracting, where $B = B^- \cup B^+$; and
- ψ is (B^-, A, B^+) -contracting, where $A = A^- \cup A^+$.

Then ϕ and ψ have no nontrivial relations; thus $\langle \phi, \psi \rangle$ is free.

Proof. Consider a word of the form $w = \phi^{m_1} \psi^{n_1} \dots \phi^{m_k} \psi^{n_k}$, with each m_j and n_j nonzero. We wish to show $w \neq e$.

From Lem. 5.68(3), we have

$$\phi^{m_j}(B) \subset A \quad \text{and} \quad \psi^{n_j}(A) \subset B, \quad \text{for } j = 1, 2, \dots, k.$$

Therefore

$$\begin{aligned} \psi^{n_k}(A) &\subset B, \\ \phi^{m_k} \psi^{n_k}(A) &\subset A, \\ \psi^{n_{k-1}} \phi^{m_k} \psi^{n_k}(A) &\subset B, \\ \phi^{m_{k-1}} \psi^{n_{k-1}} \phi^{m_k} \psi^{n_k}(A) &\subset A, \end{aligned}$$

and so on: points bounce back and forth between A and B . (Thus, the colloquial name of the lemma.) In the end, we see that $w(A) \subset A$.

Assume, for definiteness, that $m_1 > 0$. Then, by applying 5.68(1) in the last step, instead of 5.68(3), we obtain the more precise conclusion that $w(A) \subset A^+$. Since $A \not\subset A^+$ (recall that A^- is disjoint from A^+), we conclude that $w \neq e$, as desired. $\square$

(5.70) **Corollary.** *If γ_1 and γ_2 are two nontrivial hyperbolic elements of $\mathrm{SL}(2, \mathbb{R})$ that have no common eigenvector, then, for sufficiently large $n \in \mathbb{Z}^+$, the group $\langle (\gamma_1)^n, (\gamma_2)^n \rangle$ is free.*

Proof. Let

- v_j and w_j be linearly independent eigenvectors of γ_j , with eigenvalues λ_j and $1/\lambda_j$, such that $\lambda_j > 1$,
- A^+ and A^- be small neighborhoods of $[v_1]$ and $[w_1]$ in $\mathbb{P}(\mathbb{R}^2)$, and
- B^+ and B^- be small neighborhoods of $[v_2]$ and $[w_2]$ in $\mathbb{P}(\mathbb{R}^2)$.

By the same argument as in Eg. 5.67, we see that if n is sufficiently large, then

- $(\gamma_1)^n$ is $(A^-, B^- \cup B^+, A^+)$ -contracting, and
- $(\gamma_2)^n$ is $(B^-, A^- \cup A^+, B^+)$ -contracting

(see Exer. 5:54). Thus, the Ping-Pong Lemma (5.69) implies that $\langle (\gamma_1)^n, (\gamma_2)^n \rangle$ is free. $\square$

We can now give a direct proof of Cor. 5.65, in the special case where $G = \mathrm{SL}(2, \mathbb{R})$.

(5.71) **Corollary.** *If $G = \mathrm{SL}(2, \mathbb{R})$, then Γ contains a nonabelian, free subgroup.*

Proof. By passing to a subgroup of finite index, we may assume that Γ is torsion free (see 5.60). Hence, Γ has no elliptic elements. Not every element of Γ is unipotent (see Exer. 5:30), so we conclude that some nontrivial element γ_1 of Γ is hyperbolic.

Let v and w be linearly independent eigenvectors of γ_1 . The Borel Density Theorem (5.44) implies that there is some $\gamma \in \Gamma$, such that $\{\gamma v, \gamma w\} \cap (\mathbb{R}v \cup \mathbb{R}w) = \emptyset$ (see Exer. 5:55). Let $\gamma_2 = \gamma\gamma_1\gamma^{-1}$, so that γ_2 is a hyperbolic element of Γ with eigenvectors γv and γw .

From Cor. 5.70, we conclude that $\langle (\gamma_1)^n, (\gamma_2)^n \rangle$ is a nonabelian, free subgroup of Γ , for some $n \in \mathbb{Z}^+$. $\square$

The same ideas work in general:

Idea of direct proof of Cor. 5.65. Assume $G \subset \mathrm{SL}(\ell, \mathbb{R})$. Choose some nontrivial, hyperbolic element γ_1 of Γ , with eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell$. We may assume, without loss of generality, that $\lambda_1 > \lambda_2$. (If the eigenvalue λ_1 has multiplicity d , then we may pass to the d^{th} exterior power $\wedge^d(\mathbb{R}^\ell)$, to obtain a representation in which the largest eigenvalue of γ_1 is simple.)

Let us assume that the smallest eigenvalue λ_ℓ is also simple; that is, $\lambda_\ell < \lambda_{\ell-1}$. (One can show that this is a generic condition in G , so it can be achieved by replacing γ_1 with some other element of Γ .)

Let v be an eigenvector corresponding to the eigenvalue λ_1 of γ_1 , and let w be an eigenvector for the eigenvalue λ_ℓ . Assume, to simplify the notation, that all of the eigenspaces of γ_1 are orthogonal to each other. Then, for any $x \in \mathbb{R}^\ell \setminus v^\perp$, we have $(\gamma_1)^n[x] \rightarrow [v]$ in $\mathbb{P}(\mathbb{R}^\ell)$, as $n \rightarrow \infty$ (see Exer. 5:56). Similarly, if $x \notin w^\perp$, then $(\gamma_1)^{-n}[x] \rightarrow [w]$.

We may assume, by replacing $\mathbb{R}^\ell$ with a minimal G -invariant subspace, that G is irreducible in $\mathrm{SL}(\ell, \mathbb{R})$. Then the Borel Density Theorem implies that there exists $\gamma \in \Gamma$, such that $\{\gamma v, \gamma w\} \cap (\mathbb{R}v \cup \mathbb{R}w) = \emptyset$.

Then, for any small neighborhoods $A^-, A^+, B^-,$ and B^+ of $[v]$, $[w]$, $[\gamma v]$, and $[\gamma w]$, and any sufficiently large n , the Ping-Pong Lemma implies that $\langle (\gamma_1)^n, (\gamma\gamma_1\gamma^{-1})^n \rangle$ is free. $\square$

(5.72) **Remark.** The proof of Thm. 5.64 is similar, but involves additional complications.

- 1) In order to replace $\mathbb{R}^\ell$ with an irreducible subspace W , it is necessary that $\dim W > 1$ (otherwise, there do not exist two linearly independent eigenvectors v and w). Unfortunately, the minimal Λ -invariant subspaces may be 1-dimensional. After modding these out, the minimal subspaces in the quotient may also be 1-dimensional, and so on. In this case, the group Λ consists entirely of upper-triangular matrices (after a change of basis), so Λ is solvable.
- 2) The subgroup Λ may not have any hyperbolic elements. Even worse, it may be the case that 1 is the absolute value of every eigenvalue of every element of Λ . (For example, Λ may be a subgroup of the compact group $\mathrm{SO}(n)$, so that every element of Λ is elliptic.) In this case, one replaces the usual absolute value with an appropriate p -adic norm. Not all eigenvalues are roots of unity (cf. 5.61), so Algebraic Number Theory tells us that some element of Λ has an eigenvalue whose p -adic norm is greater than 1. One then uses this eigenvalue, and the corresponding eigenvector, just as we used λ_1 and the corresponding eigenvector v .

5K. Notes

Raghunathan's book [Rag1] is the standard reference for the basic properties of lattices. It contains almost all of the material in this chapter, except the Tits Alternative (§5J).

The Borel Density Theorem (5.39) was proved by Borel [Bor1]. It is discussed in [Mar5], [Rag1], and [Zim]. Several authors have published generalizations or alternative proofs (for example, [Dan, Fur, Wig]).

Our presentation of Props. 5.51 and 5.54 is based on [P-R, pp. 195–199]. A proof of Rem. 5.55 can also be found there.

A proof of Thm. 5.57 for the case where Γ is arithmetic can be found in [Bor3] or [P-R, Thm. 4.2, p. 195]. For the case where $\mathbb{Q}$ -rank $\Gamma = 1$, see [G-R] or [Rag1, Cor. 13.20, p. 210].

Theorem 5.60 and Rem. 5.62 are proved in [Rag1] and [Bor3]. Our alternate proof of Thm. 5.60 is excerpted from the elementary proof in [Al2].

The Tits Alternative (5.64) was proved by Tits [Tit]. A nice introduction (and a proof of some special cases) can be found in [Har].

5L. References

- [Al2] R. C. Alperin: An elementary account of Selberg’s Lemma, *L’Enseign. Math.* 33 (1987) 269–273.
- [Bor1] A. Borel: Density properties for certain subgroups of semi-simple groups without compact components, *Ann. Math.* 72 (1960) 179–188.
- [Bor3] A. Borel: *Introduction aux Groupes Arithmétiques*, Act. Sci. Ind. #1341, Hermann, Paris, 1969.
- [Dan] S. G. Dani: On ergodic quasi-invariant measures of group automorphism, *Israel J. Math.* 43 (1982) 62–74.
- [Fur] H. Furstenberg: A note on Borel’s Density Theorem, *Proc. Amer. Math. Soc.* 55 (1976) 209–212.
- [G-R] H. Garland and M. S. Raghunathan: Fundamental domains for lattices in $(\mathbb{R})$ -rank 1 semisimple Lie groups, *Ann. Math.* 92 (1970) 279–326.
- [Har] P. de la Harpe: Free groups in linear groups, *L’Enseign. Math.* 29 (1983) 129–144.
- [Mar5] G. A. Margulis: *Discrete Subgroups of Semisimple Lie Groups*. Springer, Berlin Heidelberg New York, 1991.
- [P-R] V. Platonov and A. Rapinchuk: *Algebraic Groups and Number Theory*. Academic Press, Boston, 1994.
- [Rag1] M. S. Raghunathan: *Discrete Subgroups of Lie Groups*. Springer, Berlin Heidelberg New York, 1972.
- [Tit] J. Tits: Free subgroups in linear groups, *J. Algebra* 20 (1972) 250–270.
- [Wig] D. Wigner: Un théorème de densité analytique pour les groupes semisimples, *Comment. Math. Helvetici* 62 (1987) 390–416.
- [Zim] R. J. Zimmer: *Ergodic Theory and Semisimple Groups*. Birkhäuser, Boston, 1984.

Exercises

- 5:1) Show that Γ is finite if and only if G is compact.
- 5:2) Complete the proof of Lem. 5.1; that is, show that $\mathcal{F}$ is a Borel fundamental domain.
- 5:3) Let $\mathcal{F}$ and $\mathcal{F}'$ be Borel fundamental domains for a discrete subgroup Λ in G , and let μ be Haar measure on G .
 - (a) Show, for each $g \in G$, that there is a unique element λ of Λ , such that $\lambda g \in \mathcal{F}$.
 - (b) For each Borel subset A of G , and each $\lambda \in \Lambda$, define

$$A_\lambda = \{a \in A \mid \lambda a \in \mathcal{F}\}.$$

Show that each A_λ is a Borel set, and that A is the disjoint union of the sets $\{A_\lambda \mid \lambda \in \Lambda\}$.

(c) Show $\mu(\mathcal{F}) = \mu(\mathcal{F}')$.

(d) Show that if A is a Borel subset of G , such that $\Lambda A = A$, then $\mu(A \cap \mathcal{F}) = \mu(A \cap \mathcal{F}')$.

5:4) Show, for any Haar measure μ on G , that the Borel measure ν defined in 5.2(1) is G -invariant. [Hint: For any $g \in G$, the set $\mathcal{F}g$ is a Borel fundamental domain. From Exer. 5:3d, we know that ν is independent of the choice of the fundamental domain $\mathcal{F}$.]

5:5) Show that if Λ is any discrete subgroup of G , and ν is any σ -finite, G -invariant Borel measure on $\Lambda \backslash G$, then the Borel measure μ defined in 5.2(2) is G -invariant.

5:6) Let H be a closed subgroup of G . Show that there is a σ -finite, G -invariant Borel measure ν on $H \backslash G$ if and only if H is unimodular. [Hint: $(\Rightarrow)$ Let ρ be a right Haar measure on H , and define a right Haar measure μ on G by

$$\mu(A) = \int_{H \backslash G} \rho(Ax^{-1} \cap H) d\nu(Hx).$$

Then $\mu(hA) = \Delta_H(h) \mu(A)$ for $h \in H$, where Δ_H is the unimodular function of H . Since G is unimodular, we must have $\Delta_H \equiv 1$.]

5:7) Show that if Λ is a discrete subgroup of G that contains Γ , then Λ is a lattice in G , and Γ has finite index in Λ .

5:8) Let Λ be a discrete subgroup of G . Show that a subset A of $\Lambda \backslash G$ is precompact if and only if there is a compact subset C of G , such that $A \subset \Lambda \backslash \Lambda C$. [Hint: $(\Leftarrow)$ The continuous image of a compact set is compact. $(\Rightarrow)$ Let $\mathcal{U}$ be a cover of G by precompact, open sets.]

5:9) Prove Cor. 5.12(1). [Hint: Use Exer. 5:8 and Prop. 5.9(3).]

5:10) Prove Cor. 5.12(2). [Hint: Use Prop. 5.9. A finite union of sets of finite measure has finite measure.]

5:11) Let

- H be a Lie group,
- Λ be a discrete subgroup of H ,
- μ be the left Haar measure on H , and
- $\mathcal{F}$ be a Borel fundamental domain for Λ in H , such that $\mu(\mathcal{F}) < \infty$.

Define a σ -finite Borel measure ν on $\Lambda \backslash H$ by

$$\nu(\Lambda \backslash A) = \mu(A \cap \mathcal{F}),$$

for every Borel set A in H , such that $\Lambda A = A$. Show that $\nu(\Lambda \backslash Ah^{-1}) = \Delta(h) \nu(\Lambda \backslash A)$, where Δ is the modular function of H . [Hint: Cf. Exer. 5:4.]

5:12) Verify that commensurability is an equivalence relation.

5:13) Show that $\mathrm{SL}(n, \mathbb{Q})$ commensurates $\mathrm{SL}(n, \mathbb{Z})$. [Hint: For each $g \in \mathrm{SL}(n, \mathbb{Q})$, there is a principal congruence subgroup Γ_m of $\mathrm{SL}(n, \mathbb{Z})$, such that $g^{-1} \Gamma_m g \subset \mathrm{SL}(n, \mathbb{Z})$.]

5:14) Show that if Γ_1 is commensurable with Γ_2 , then $\mathrm{Comm}_G(\Gamma_1) = \mathrm{Comm}_G(\Gamma_2)$.

5:15) Suppose Γ_1 and Γ_2 are lattices in G , such that $\Gamma_1 \subset \Gamma_2$. Show that Γ_1 has finite index in Γ_2 .

5:16) Show that if Γ is irreducible, and G is not compact, then Γ projects densely into the maximal compact factor of G .

5:17) Suppose a Lie group H acts continuously on a compact topological space M , and $\mathcal{V}$ is an open cover of M . Show that there is a neighborhood U of e in G , such that, for each

- $m \in M$, there is some $V \in \mathcal{V}$ with $Um \subset V$. [Hint: This is analogous to the fact that every open cover of a compact metric space has a “Lebesgue number.”]
- 5:18) Use Prop. 5.33 to show that if H is a closed subgroup of G , such that $\Gamma \cap H$ is a lattice in H , then the natural inclusion map $(\Gamma \cap H) \backslash H \hookrightarrow \Gamma \backslash G$ is proper. [Hint: It suffices to show that if C is a subset of H , such that the image of C in $\Gamma \backslash G$ is precompact, then the image of C in $(\Gamma \cap H) \backslash H$ is also precompact.]
- 5:19) Let $G = \mathrm{SL}(2, \mathbb{R})$, $\Gamma = \mathrm{SL}(2, \mathbb{Z})$, and A be the subgroup consisting of all the diagonal matrices in G . Show that the natural inclusion map $(\Gamma \cap A) \backslash A \hookrightarrow \Gamma \backslash G$ is proper, but $\Gamma \cap A$ is *not* a lattice in A . (Thus, the converse of Exer. 5:18 does not hold.)
- 5:20) Let $H = \mathrm{SL}(3, \mathbb{R})$, $\Lambda = \mathrm{SL}(3, \mathbb{Z})$, and $a = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1/2 \end{bmatrix} \in H$. Show that $\Lambda a^n \rightarrow \infty$ in $\Lambda \backslash H$ as $n \rightarrow \infty$. That is, show, for each compact subset C of $\Lambda \backslash H$, that, for all sufficiently large n , we have $\Lambda a^n \notin C$. (For the purposes of this exercise, do *not* assume that Λ is a lattice in H .)
- 5:21) Show that if Γ contains a nontrivial unipotent element, then $\Gamma \backslash G$ is not compact.
- 5:22) Prove $(\Rightarrow)$ of Prop. 5.34.
- 5:23) Remove the assumption $\ell = 2$ from the proof of $(\Leftarrow)$ of Prop. 5.34. [Hint: Extend the construction of v_n and w_n to an inductive construction of $u_{1,n}, \dots, u_{\ell,n} \in \mathbb{Z}^\ell$.]
- 5:24) Suppose v and w are linearly independent vectors in $\mathbb{R}^\ell$, and $x = av + bw$, with $a, b \in \mathbb{R}^+$ and $a + b \leq 1$. Show that either
- $x \in \{v, w\}$, or
 - $\|x\| < \|v\|$, or
 - $d(x, \mathbb{R}v) < d(w, \mathbb{R}v)$.
- [Hint: Consider two cases: $b = 0$, $b > 0$.]
- 5:25) Prove 5.39(1), replacing the assumption that G has no compact factors with the weaker assumption that Γ projects densely into the maximal compact factor of G .
- 5:26) Show that if G is not compact, then Γ is not abelian.
- 5:27) Generalizing Exer. 5:26, show that if G is not compact, then Γ is not solvable.
- 5:28) Strengthening Exer. 5:26, show that if G is not compact, then the commutator subgroup $[\Gamma, \Gamma]$ is infinite.
- 5:29) Assume the hypotheses of Theorem 5.39. For definiteness, assume that V is a real vector space. For any subgroup H of G , let $V[H]$ be the $\mathbb{R}$ -span of $\{\rho(h) \mid h \in H\}$ in $\mathrm{End}(V)$. Show that $V[\Gamma] = V[G]$.
- 5:30) Show that if G is not compact, then Γ has an element that is not unipotent. [Hint: Any unipotent element γ of $\mathrm{SL}(\ell, \mathbb{R})$ satisfies the polynomial $(x - 1)^\ell = 0$.]
- 5:31) Assume G has no compact factors. Show that if H is a connected subgroup of G that contains a finite-index subgroup of Γ , then $H = G$.
- 5:32) Assume G is linear and has no compact factors. Show that Γ is irreducible if and only if there is a finite-index subgroup Γ' of Γ such that Γ' is isomorphic to $A \times B$, for some infinite groups A and B .
- 5:33) Show that if Γ is irreducible, then $N \cap \Gamma$ is finite, for every connected, closed, noncompact, normal subgroup N of G , such that G/N is not compact. [Hint: See proof of Prop. 5.24.]

- 5:34) Show that there is an irreducible lattice Γ in $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SO}(3)$, such that $\Gamma \cap \mathrm{SL}(2, \mathbb{R})$ is infinite. [Hint: There is a free group F and a homomorphism $\phi: F \rightarrow \mathrm{SO}(3)$, such that $\phi(F)$ is dense in $\mathrm{SO}(3)$.]
- 5:35) Let ρ_1 and ρ_2 be finite-dimensional, real representations of G , and assume G has no compact factors. Show that if the restrictions $\rho_1|_\Gamma$ and $\rho_2|_\Gamma$ are isomorphic, then ρ_1 and ρ_2 are isomorphic.
- 5:36) Complete the proof of Cor. 5.48, by removing the assumption that G has no compact factors. [Hint: Use Cor. 5.47 in place of Prop. 5.46; $G'H$ is dense in G .]
- 5:37) Suppose M is a locally symmetric space, such that no irreducible factor of the universal cover of M is either flat or compact. Show that $\mathrm{Isom}(M)$ is finite.
- 5:38) Suppose Λ is a discrete subgroup of a locally compact group H . Show that if $\Lambda \backslash H$ is compact, and H is *compactly generated* (that is, there is a compact subset C of H , such that $\langle C \rangle = H$), then Λ is finitely generated. [Hint: For any compact subset $\mathcal{F}$ of H , such that $\mathcal{F}\Lambda = H$ (and $e \in \mathcal{F}$), let $S = \Lambda \cap (\mathcal{F}^{-1}C\mathcal{F})$.]
- 5:39) Show that $\mathrm{SL}(\ell, \cdot)$ is a (covariant) functor from the category of rings with identity to the category of groups. That is, show:
- (a) if A is any ring with identity, then $\mathrm{SL}(\ell, A)$ is a group;
 - (b) for every ring homomorphism $\phi: A \rightarrow B$ (with $\phi(1) = 1$), there is a corresponding group homomorphism $\phi_*: \mathrm{SL}(\ell, A) \rightarrow \mathrm{SL}(\ell, B)$; and
 - (c) if $\phi: A \rightarrow B$ and $\psi: B \rightarrow C$ are ring homomorphisms (with $\phi(1) = 1$ and $\psi(1) = 1$), then $(\psi \circ \phi)_* = \psi_* \circ \phi_*$.
- 5:40) Suppose A and B are rings with identity, $\phi: A \rightarrow B$ is a ring homomorphism (with $\phi(1) = 1$), and I is an ideal of B . Show, in the notation of Exer. 5:39, that
- (a) $1 + I$ is a subring of B ;
 - (b) $\mathrm{SL}(\ell, 1 + I)$ is a normal subgroup of $\mathrm{SL}(\ell, B)$; and
 - (c) $(\phi_*)^{-1}(\mathrm{SL}(\ell, 1 + I))$ is a normal subgroup of $\mathrm{SL}(\ell, A)$.
- 5:41) Show that if B is a finite ring with identity, then $\mathrm{SL}(\ell, B)$ is finite. Use this fact to show, for every positive integer n , that if Γ_n denotes the principal congruence subgroup of $\mathrm{SL}(\ell, \mathbb{Z})$ of level n (cf. Case 1 of pf. of Thm. 5.60), then Γ_n has finite index in $\mathrm{SL}(\ell, \mathbb{Z})$.
- 5:42) Show that if Γ has a nontrivial element of finite order, then Γ has an element of prime order.
- 5:43) In the notation of Case 1 of the proof of Thm. 5.60, show that Γ_2 is not torsion free. Where does the proof of Thm. 5.60 fail?
- 5:44) Show that if Λ is a finitely generated subgroup of $\mathrm{SL}(\ell, \mathbb{C})$, then there is a finitely generated subring B of $\mathbb{C}$, such that $\Lambda \subset \mathrm{SL}(\ell, B)$. [Hint: Let B be the subring of $\mathbb{C}$ generated by the matrix entries of the generators of Λ .]
- 5:45) Show that Γ is residually finite. That is, for every $\gamma \in \Gamma \setminus \{e\}$, show that there is a finite-index, normal subgroup Γ' of Γ , such that $\gamma \notin \Gamma'$. (In particular, Γ is *not* a simple group.)
- 5:46) Show that there is a sequence $N_1, N_2, \dots$ of subgroups of Γ , such that
- (a) $N_1 \supset N_2 \supset \dots$,
 - (b) each N_k is a finite-index, normal subgroup of Γ , and
 - (c) $N_1 \cap N_2 \cap \dots = \{e\}$.
- [Hint: Use Exer. 5:45.]

- 5:47) Prove Prop. 5.51, replacing the assumption that $\mathcal{F}$ is open with the weaker assumption that $\mathcal{F}$ is in the interior of $\cup_{s \in S} s\mathcal{F}$ (where S is as defined in the proof of Prop. 5.51).
- 5:48) Show that the relation $\sim$ defined in the proof of Prop. 5.54 is an equivalence relation.
- 5:49) In the notation of the proof of Prop. 5.54, show that if $\psi(fN, y) \in \mathcal{F}$, then $(fN, y) \sim (f'N, y')$, for some $f' \in \ker(\phi)$ and some $y' \in \mathcal{F}$. [Hint: We have $\psi(f) \in S$, because $\phi(f^{-1}y) \in \mathcal{F}$.]
- 5:50) In the notation of the proof of Prop. 5.54, show that the inverse image of $\mathcal{F}_f$ in $(F/N) \times \mathcal{F}$ is

$$\cup_{s \in S} ((x_s f N / N) \times (\mathcal{F} \cap s\mathcal{F})),$$

which is open.

- 5:51) In the notation of the proof of Prop. 5.54, show that if $\mathcal{F}_f \cap \mathcal{F}_e \neq \emptyset$, and $f \in \ker(\phi)$, then $f \in N$. [Hint: If $(fN, y_1) \sim (N, y_2)$, then there is some $s \in S$ with $x_s N = fN$. Since $f \in \ker(\phi)$, we have $s = \phi(x_s) = \phi(f) = e$.]
- 5:52) Show that the set $\tilde{Y}$ defined in the proof of Prop. 5.54 is connected. [Hint: For $s_1, \dots, s_r \in S$, define $\mathcal{F}_j = \{x_{s_j} \cdots x_{s_1} N\} \times \mathcal{F}$. Show there exist $a \in \mathcal{F}_j$ and $b \in \mathcal{F}_{j+1}$, such that $a \sim b$.]
- 5:53) Suppose ω is a nontrivial root of unity, $n, \ell \in \mathbb{Z}^+$, and $\zeta \in \mathbb{Z} + \mathbb{Z}\omega + \cdots + \mathbb{Z}\omega^{\ell-1}$, such that $(\omega - 1)^\ell = n\zeta$. Show that $n < 2^{(\ell+1)!}$. [Hint: Let F be the Galois closure of the field extension $\mathbb{Q}(\omega)$ of $\mathbb{Q}$ generated by ω , and define $N: F \rightarrow \mathbb{Q}$ by $N(x) = \prod_{\sigma \in \text{Gal}(F/\mathbb{Q})} \sigma(x)$. Then $N(\omega - 1)^\ell = n^d N(\zeta)$, and $|N(\omega - 1)| \leq 2^d \leq 2^{\ell!}$, where d is the degree of F over $\mathbb{Q}$.]
- 5:54) In the notation of the proof of Cor. 5.70, show that if $A^-, A^+, B^-,$ and B^+ are disjoint, then, for all large n , the homeomorphism $(\gamma_1)^n$ is $(A^-, B^- \cup B^+, A^+)$ -contracting on $\mathbb{P}(\mathbb{R}^2)$.
- 5:55) Assume that G is irreducible in $\text{SL}(\ell, \mathbb{R})$ (see Defn. 3.12), and that Γ projects densely into the maximal compact factor of G . If F is a finite subset of $\mathbb{R}^\ell \setminus \{0\}$, and $\mathcal{W}$ is a finite set of proper subspaces of $\mathbb{R}^\ell$, show that there exists $\gamma \in \Gamma$, such that

$$\gamma F \cap \bigcup_{W \in \mathcal{W}} W = \emptyset.$$

[Hint: For $v \in F$ and $W \in \mathcal{W}$, the set

$$A_{v,W} = \{g \in G \mid gv \in W\}$$

is Zariski closed, so $\bigcup_{v,W} A_{v,W}$ is Zariski closed. Apply the Borel Density Theorem and Exer. 4:7.]

- 5:56) Let

- γ be a hyperbolic element of $\text{SL}(\ell, \mathbb{R})$, with eigenvalues $\lambda_1 > \lambda_2 \geq \cdots \geq \lambda_\ell$,
- v be an eigenvector of γ corresponding to the eigenvalue λ_1 , and
- W be the sum of the other eigenspaces.

Show that if $x \in \mathbb{P}(\mathbb{R}^\ell) \setminus [W]$, then $\gamma^n x \rightarrow [v]$ as $n \rightarrow \infty$. Furthermore, the convergence is uniform on compact subsets.

What is an Arithmetic Lattice?

6A. Definition of arithmetic lattices

If G is a subgroup of $\mathrm{SL}(\ell, \mathbb{R})$, then the basic example of an arithmetic lattice is obtained by setting $\Gamma = G \cap \mathrm{SL}(\ell, \mathbb{Z})$; that is, by taking the integer points of G . However, in order for the integer points to form a lattice, G needs to be well-placed with respect to $\mathrm{SL}(\ell, \mathbb{Z})$. (If we replace G by a conjugate under some terrible irrational matrix, perhaps $G \cap \mathrm{SL}(\ell, \mathbb{Z})$ would become trivial (see Exer. 6:1).) The following example is an elementary illustration of this idea.

(6.1) **Proposition.** *Let W be a subspace of $\mathbb{R}^\ell$. The following are equivalent:*

- 1) W can be defined by a set of linear equations with rational coefficients;
- 2) W is spanned by $W \cap \mathbb{Z}^\ell$;
- 3) $W \cap \mathbb{Q}^\ell$ is dense in W ;
- 4) $W \cap \mathbb{Z}^\ell$ is a cocompact lattice in W .

Proof. (1 $\Rightarrow$ 2) By assumption, W is the solution space of a system of linear equations whose coefficients belong to $\mathbb{Q}$. By elementary linear algebra (row reductions), we may find a basis for W that consists entirely of vectors in $\mathbb{Q}^\ell$. Multiplying by a scalar to clear the denominators, we may assume that the basis consists entirely of vectors in $\mathbb{Z}^\ell$.

(2 $\Rightarrow$ 3) Let $\{\varepsilon_1, \dots, \varepsilon_k\}$ be the standard basis of $\mathbb{R}^k$. Because $W \cap \mathbb{Q}^\ell \supset W \cap \mathbb{Z}^\ell$ contains a basis of W , there is a linear isomorphism $T: \mathbb{R}^k \rightarrow W$, such that $T(\varepsilon_j) \in W \cap \mathbb{Q}^\ell$ for $j = 1, \dots, k$; then $T(\mathbb{Q}^k) \subset W \cap \mathbb{Q}^\ell$. Because $\mathbb{Q}^k$ is dense in $\mathbb{R}^k$, and T is continuous, we know that $T(\mathbb{Q}^k)$ is dense in W .

(3 $\Rightarrow$ 1) Because $W \cap \mathbb{Q}^\ell$ is dense in W , we see that $W^\perp$ is defined by a system of linear equations with rational coefficients. (Namely, for each vector w_j in some basis of $W \cap \mathbb{Q}^\ell$, we write the equation $x \cdot w_j = 0$.) Thus, from (1 $\Rightarrow$ 2), we conclude that there is a basis $v_1, \dots, v_m$ of $W^\perp$, such that each $v_j \in \mathbb{Q}^\ell$. Then $W = (W^\perp)^\perp$ is defined by the system of equations $v_1 \cdot x = 0, \dots, v_m \cdot x = 0$.

(2 $\Rightarrow$ 4) There is a linear isomorphism $T: \mathbb{R}^k \rightarrow W$, such that $T(\mathbb{Z}^k) = W \cap \mathbb{Z}^\ell$. Since $\mathbb{R}^k/\mathbb{Z}^k$ is compact, we conclude that $W/(W \cap \mathbb{Z}^\ell)$ is compact.

(4 $\Rightarrow$ 2) Let V be the $\mathbb{R}$ -span of $W \cap \mathbb{Z}^\ell$. Then W/V , being a vector space over $\mathbb{R}$, is homeomorphic to $\mathbb{R}^d$, for some d . On the other hand, we know that $W \cap \mathbb{Z}^\ell \subset V$, and that $W/(W \cap \mathbb{Z}^\ell)$ is compact, so W/V is compact. Hence $d = 0$, so $V = W$. $\square$

With the preceding example in mind, we make the following definition.

(6.2) **Definition** (cf. 4.1 and 4.6). Let H be a closed subgroup of $\mathrm{SL}(\ell, \mathbb{R})$. We say H is *defined over $\mathbb{Q}$* (or that H is a $\mathbb{Q}$ -subgroup) if there is a subset $\mathcal{Q}$ of $\mathbb{Q}[x_{1,1}, \dots, x_{\ell,\ell}]$, such that

- $\mathrm{Var}(\mathcal{Q}) = \{g \in \mathrm{SL}(\ell, \mathbb{R}) \mid Q(g) = 0, \forall Q \in \mathcal{Q}\}$ is a subgroup of $\mathrm{SL}(\ell, \mathbb{R})$;
- $H^\circ = \mathrm{Var}(\mathcal{Q})^\circ$; and
- H has only finitely many components.

(In other words, H is commensurable with $\mathrm{Var}(\mathcal{Q})$, for some set $\mathcal{Q}$ of $\mathbb{Q}$ -polynomials.

(6.3) **Example.**

- $\mathrm{SL}(\ell, \mathbb{R})$ is defined over $\mathbb{Q}$. Let $\mathcal{Q} = \emptyset$.
- If $n < \ell$, we may embed $\mathrm{SL}(n, \mathbb{R})$ in the top left corner of $\mathrm{SL}(\ell, \mathbb{R})$. Let

$$\mathcal{Q} = \{x_{i,j} - \delta_i^j \mid \max\{i, j\} > n\}.$$

- For any $A \in \mathrm{SL}(\ell, \mathbb{Q})$,

$$\{g \in \mathrm{SL}(\ell, \mathbb{R}) \mid gAg^T = A\}$$

is defined over $\mathbb{Q}$; let

$$\mathcal{Q} = \left\{ \sum_{1 \leq p, q \leq m+n} x_{i,p} A_{p,q} x_{j,q} - A_{i,j} \mid 1 \leq i, j \leq m+n \right\}.$$

In particular, $\mathrm{SO}(m, n)$, under its usual embedding in $\mathrm{SL}(m+n, \mathbb{R})$, is defined over $\mathbb{Q}$.

- $\mathrm{SL}(n, \mathbb{C})$, under its natural embedding in $\mathrm{SL}(2n, \mathbb{R})$ is defined over $\mathbb{Q}$ (cf. 4.2(4)).

(6.4) **Remark.**

- There is always a subset $\mathcal{Q}$ of $\mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$, such that G is commensurable with $\mathrm{Var}(\mathcal{Q})$ (see 4.8); that is, G is *defined over $\mathbb{R}$* . However, it may not be possible to find a set $\mathcal{Q}$ that consists entirely of polynomials whose coefficients are rational, so G may not be defined over $\mathbb{Q}$.
- If G is defined over $\mathbb{Q}$, then the set $\mathcal{Q}$ of Defn. 6.2 can be chosen to be finite (because the ring $\mathbb{Q}[x_{1,1}, \dots, x_{\ell,\ell}]$ is Noetherian).

(6.5) **Proposition.** G is isogenous to a group that is defined over $\mathbb{Q}$.

Proof. It is easy to handle direct products, so the crucial case is when G is simple. This is easy if G is classical. Indeed, the groups in Egs. 3.22 and 3.23 are defined over $\mathbb{Q}$ (after identifying $\mathrm{SL}(\ell, \mathbb{C})$ and $\mathrm{SL}(\ell, \mathbb{H})$ with appropriate subgroups of $\mathrm{SL}(2\ell, \mathbb{R})$ and $\mathrm{SL}(4\ell, \mathbb{R})$, in a natural way).

For the general case, one notes that $\mathrm{Ad} G$ is a finite-index subgroup of $\mathrm{Aut}(\mathfrak{g})$ (see I.30), so it suffices to find a basis of $\mathfrak{g}$, for which the structure constants of the Lie algebra are rational. This (and somewhat more) will be done in Chap. 13. $\square$

(6.6) **Notation.** Assume $G \subset \mathrm{SL}(\ell, \mathbb{C})$. For any subring A of $\mathbb{C}$ (containing 1), let $G_A = G \cap \mathrm{SL}(\ell, A)$. That is, G_A is the subgroup consisting of the elements of G whose matrix entries all belong to A .

(6.7) **Remark.** Let $\phi: \mathrm{SL}(n, \mathbb{C}) \rightarrow \mathrm{SL}(2n, \mathbb{R})$ be the natural embedding. Then

$$\phi(\mathrm{SL}(n, \mathbb{C}))_{\mathbb{Q}} = \phi(\mathrm{SL}(n, \mathbb{Q}[i])).$$

Thus, if we think of $\mathrm{SL}(n, \mathbb{C})$ as a Lie group over $\mathbb{R}$, then $\mathrm{SL}(n, \mathbb{Q}[i])$ represents the “ $\mathbb{Q}$ -points” of $\mathrm{SL}(n, \mathbb{C})$.

The following result provides an alternate point of view on being defined over $\mathbb{Q}$.

(6.8) **Proposition.** *Let H be a connected subgroup of $\mathrm{SL}(\ell, \mathbb{R})$ that is almost Zariski closed. The group H is defined over $\mathbb{Q}$ if and only if $H_{\mathbb{Q}}$ is dense in H .*

(6.9) **Warning.** Proposition 6.8 requires the assumption that H is connected; there are subgroups H of $\mathrm{SL}(\ell, \mathbb{R})$, such that H is defined over $\mathbb{Q}$, but $H_{\mathbb{Q}}$ is not dense in H . For example, let

$$H = \{ h \in \mathrm{SO}(2) \mid h^8 = \mathrm{Id} \}.$$

The following fundamental theorem will be proved in Chap. 15. For now, we will accept this as one of the axioms of the theory of arithmetic groups.

(6.10) **Theorem.** *If G is defined over $\mathbb{Q}$, then $G_{\mathbb{Z}}$ is a lattice in G .*

(6.11) **Example.** Let us mention some standard cases of Thm. 6.10.

- 1) $\mathrm{SL}(2, \mathbb{Z})$ is a lattice in $\mathrm{SL}(2, \mathbb{R})$. (We proved this in Eg. 1.22.)
- 2) $\mathrm{SL}(n, \mathbb{Z})$ is a lattice in $\mathrm{SL}(n, \mathbb{R})$.
- 3) $\mathrm{SO}(m, n)_{\mathbb{Z}}$ is a lattice in $\mathrm{SO}(m, n)$.
- 4) $\mathrm{SL}(n, \mathbb{Z}[i])$ is a lattice in $\mathrm{SL}(n, \mathbb{C})$ (cf. 6.7).

(6.12) **Example.** As an additional example, let $G = \mathrm{SO}(7x_1^2 - x_2^2 - x_3^2)^{\circ} \approx \mathrm{SO}(1, 2)$. Then Thm. 6.10 implies that $G_{\mathbb{Z}}$ is a lattice in G . This illustrates that the theorem is a highly nontrivial result. For example, in this case, it may not even be obvious to the reader that $G_{\mathbb{Z}}$ is infinite.

(6.13) **Warning.** Theorem 6.10 requires our standing assumption that G is semisimple; there are subgroups H of $\mathrm{SL}(\ell, \mathbb{R})$, such that H is defined over $\mathbb{Q}$, but $H_{\mathbb{Z}}$ is not a lattice in H . For example, if H is the group of diagonal matrices in $\mathrm{SL}(2, \mathbb{R})$, then $H_{\mathbb{Z}}$ is finite, not a lattice.

(6.14) **Remark.** The converse of Thm. 6.10 holds when G has no compact factors (see Exer. 6:4).

Combining Prop. 6.5 with Thm. 6.10 yields the following important conclusion:

(6.15) **Corollary.** *G has a lattice.*

In fact, if G is not compact, then G has both cocompact and noncocompact lattices (see 9.19).

A lattice of the form $G_{\mathbb{Z}}$ is said to be *arithmetic*. However, for the following reasons, a somewhat more general class of lattices is also said to be arithmetic. The idea is that there are some obvious modifications of $G_{\mathbb{Z}}$ that are also lattices, and any subgroup that is obviously a lattice will be called an arithmetic lattice.

- If $\phi: G_1 \rightarrow G_2$ is an isomorphism, and Γ_1 is an arithmetic lattice in G_1 , then we wish to be able to say that $\phi(\Gamma_1)$ is an arithmetic lattice in G_2 .
- When G is noncompact, we wish to ignore compact groups; that is, modding out a compact subgroup should not affect arithmeticity. So we wish to be able to say that if K is a compact normal subgroup of G , and Γ is a lattice in G , then Γ is arithmetic if and only if $\Gamma K/K$ is an arithmetic lattice in G/K .

- Arithmeticity should be independent of commensurability.

The following formal definition implements these considerations.

(6.16) **Definition.** Γ is an *arithmetic* lattice in G if and only if there exist

- a closed, connected, semisimple subgroup G' of some $\mathrm{SL}(\ell, \mathbb{R})$, such that G' is defined over $\mathbb{Q}$,
- compact normal subgroups K and K' of G and G' , respectively, and
- an isomorphism $\phi: G/K \rightarrow G'/K'$,

such that $\phi(\bar{\Gamma})$ is commensurable with $\overline{G'_{\mathbb{Z}}}$, where $\bar{\Gamma}$ and $\overline{G'_{\mathbb{Z}}}$ are the images of Γ and $G'_{\mathbb{Z}}$ in G/K and G'/K' , respectively.

(6.17) **Remark.**

- 1) If G has no compact factors, then the subgroup K in Defn. 6.16 must be finite.
- 2) If Γ is irreducible and $\Gamma \backslash G$ is *not* compact, then the subgroup K' may be taken to be trivial. (This is a consequence of Cor. 6.53.)

The remark shows that, in many cases, the annoying compact subgroups can be eliminated from Defn. 6.16:

(6.18) **Proposition.** *If*

- G is linear and has no compact factors,
- Γ is arithmetic and irreducible, and
- $\Gamma \backslash G$ is not compact,

then there exist

- 1) a closed, connected, semisimple subgroup G' of some $\mathrm{SL}(\ell, \mathbb{R})$, such that G' is defined over $\mathbb{Q}$, and
- 2) an isogeny $\phi: G \rightarrow G'$,

such that $\phi(G'_{\mathbb{Z}})$ is commensurable with Γ .

However, if Γ is cocompact, then a nontrivial (connected) compact group K' may be required (even if G has no compact factors). We will see many examples of this phenomenon, starting with Prop. 6.45.

(6.19) **Remark.** Up to conjugacy, there are only countably many arithmetic lattices in G , because there are only countably many finite subsets of $\mathbb{Q}[x_{1,1}, \dots, x_{\ell,\ell}]$.

(6.20) **Other terminology.** Our definition of *arithmetic* is from a Lie theorist's viewpoint, where Γ is assumed to be embedded in some Lie group G . Algebraic group theorists have a more strict definition, which requires Γ to be commensurable with $G_{\mathbb{Z}}$: arbitrary isomorphisms are not allowed, and compact subgroups cannot be ignored. At the other extreme, abstract group theorists use a much looser definition, which completely ignores G : if an abstract group Λ is virtually isomorphic to a group that is arithmetic in our sense, then they will say that Λ is arithmetic.

6B. Margulis Arithmeticity Theorem

The following astonishing theorem shows that taking integer points is usually the only way to make a lattice.

(6.21) **Theorem** (Margulis Arithmeticity Theorem). *If*

- G is not isogenous to $\mathrm{SO}(1, n) \times K$ or $\mathrm{SU}(1, n) \times K$, for any compact group K , and
- Γ is irreducible,

then Γ is arithmetic.

(6.22) **Warning.** Unfortunately,

- $\mathrm{SL}(2, \mathbb{R})$ is isogenous to $\mathrm{SO}(1, 2)$, and
- $\mathrm{SL}(2, \mathbb{C})$ is isogenous to $\mathrm{SO}(1, 3)$,

so the arithmeticity theorem does not apply to these two important groups.

(6.23) **Remark.** The conclusion of Thm. 6.21 can be strengthened: the subgroup K of Defn. 6.16 can be taken to be finite. More precisely, if G and Γ are as in Thm. 6.21, and G is noncompact and has trivial center, then there exist

- a closed, connected, semisimple subgroup G' of some $\mathrm{SL}(\ell, \mathbb{R})$, such that G' is defined over $\mathbb{Q}$; and
- a surjective (continuous) homomorphism $\phi: G' \rightarrow G$;

such that

- 1) $\phi(G'_{\mathbb{Z}})$ is commensurable with Γ ; and
- 2) the kernel of ϕ is compact.

For any G , it is possible to give a reasonably complete description of the arithmetic lattices in G (up to conjugacy and commensurability): Fig. 10.2 (on p. 153) essentially provides a list of all the irreducible arithmetic lattices in almost all of the classical groups. (Some examples are worked out in fair detail in Chap. 7.) Thus, for most groups, the arithmeticity theorem essentially provides a list of all the lattices in G .

Furthermore, knowing that Γ is arithmetic provides a foothold to use algebraic and number-theoretic techniques to explore the detailed structure of Γ . For example, the proof of Thm. 5.60 is easy if Γ is arithmetic. A more important example is that (apparently) the only known proof that every lattice is finitely presented (see 5.57) relies on the fact that if Γ is irreducible and $\mathbb{R}$ -rank $G > 1$, then Γ is arithmetic (see 6.21).

(6.24) **Remark.** It is known that there are nonarithmetic lattices in $\mathrm{SO}(1, n)$ for every n (see 7.35), but we do not have any theory to describe all the possible nonarithmetic lattices in $\mathrm{SO}(1, n)$ when $n \geq 3$. Also, nonarithmetic lattices have been constructed in $\mathrm{SU}(1, n)$ for $n \in \{1, 2, 3\}$, but (apparently) it is still not known whether they exist when $n \geq 4$.

(6.25) **Definition.** G is *isotypic* if all of its simple factors are of the same type (A_n , B_n , C_n , D_n , E_n , F_4 , or G_2 , see Fig. 3.1 and Prop. 3.32).

For example, $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(3, \mathbb{R})$ is not isotypic, because $\mathrm{SL}(2, \mathbb{R})$ is of type A_1 , but $\mathrm{SL}(3, \mathbb{R})$ is of type A_2 . Similarly, $\mathrm{SL}(5, \mathbb{R}) \times \mathrm{SO}(2, 3)$ is not isotypic, because $\mathrm{SL}(5, \mathbb{R})$ is of type A_4 , but $\mathrm{SO}(2, 3)$ is of type B_2 . Thus, the following consequence of the arithmeticity theorem implies that neither $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(3, \mathbb{R})$ nor $\mathrm{SL}(5, \mathbb{R}) \times \mathrm{SO}(2, 3)$ has an irreducible lattice.

(6.26) **Theorem.** *Assume that G has no compact factors. The group G has an irreducible lattice if and only if G is isotypic.*

Proof. ($\Leftarrow$) If G is classical and isotypic, then Sect. 10D will show how to construct a fairly explicit irreducible lattice in G , by applying Prop. 6.49. In the general case, Chap. 12 will explain how the desired conclusion is an immediate consequence of a result in Galois cohomology.

($\Rightarrow$) Suppose Γ is an irreducible lattice in G . We may assume that G is not simple (otherwise, the desired conclusion is trivially true), so G is neither $\mathrm{SO}(1, n)$ nor $\mathrm{SU}(1, n)$. Thus, from the Margulis Arithmeticity Theorem (6.21), we know that Γ is arithmetic. Then, since Γ is irreducible, the conclusion follows from the theory of arithmetic groups (see 6.55). Briefly, the only way to construct an irreducible arithmetic lattice is by applying Prop. 6.49. Thus, there is a simple subgroup G' of some $\mathrm{SL}(\ell, \mathbb{R})$, such that (modulo some finite groups)

- G' is defined over some number field F ,
- Γ is isomorphic to $G'_{\mathcal{O}}$, where $\mathcal{O}$ is the ring of integers of F , and
- G is isomorphic to $\prod_{\sigma \in S^\infty} (G')^\sigma$.

Since any Galois conjugate $(G')^\sigma$ of G' is of the same type as G' (see 6.57), the conclusion follows. $\square$

(6.27) **Remark.** By using Rem. 6.23, one can show that Thm. 6.26 remains valid under the weaker hypothesis that G is not isogenous to $\mathrm{SO}(1, n) \times K$ or $\mathrm{SU}(1, n) \times K$, for any nontrivial, connected compact group K (see Exer. 6:8).

The following provides examples of nonisotypic groups that have irreducible lattices. Thus, some restriction on G is necessary in Thm. 6.26.

(6.28) **Example.** $\mathrm{SO}(1, 2) \times K$ has an irreducible lattice, for any connected, compact Lie group K (cf. Exer. 5:34).

6C. Commensurability criterion for arithmeticity

Assume G is defined over $\mathbb{Q}$. It is easy to see that $G_{\mathbb{Q}}$ commensurates $G_{\mathbb{Z}}$ (cf. Exer. 5:13). (In fact, if G has no compact factors, and the complexification $G \otimes \mathbb{C}$ (see Notn. 10.2) has trivial center, then $\mathrm{Comm}_G(G_{\mathbb{Z}}) = G_{\mathbb{Q}}$, although this is not obvious.) Therefore, if Γ is arithmetic, and G has no compact factors, then $\mathrm{Comm}_G(G_{\mathbb{Z}})$ is dense in G . Margulis proved the converse.

(6.29) **Theorem** (Commensurability Criterion for Arithmeticity). *Assume that G has no compact factors. Then $\mathrm{Comm}_G(\Gamma)$ is dense in G if and only if Γ is arithmetic.*

6D. Why superrigidity implies arithmeticity

Let us describe the main ideas in the proof of the Margulis Arithmeticity Theorem (6.21). More precisely, we indicate how to derive it as a corollary of the Margulis Superrigidity Theorem, which will be discussed in more detail in Sect. 17F.

For simplicity, let us assume

- $G = \mathrm{SL}(n, \mathbb{R})$ with $n \geq 3$, and
- $\Gamma \backslash G$ is not compact.

We wish to show that Γ is arithmetic. It suffices to show $\Gamma \subset \mathrm{SL}(n, \mathbb{Z})$, that is, that every matrix entry of every element of Γ is an integer, for then Γ is commensurable with $\mathrm{SL}(n, \mathbb{Z})$ (see Exer. 5:7).

The Margulis Superrigidity Theorem (17.14) implies that (ignoring a finite group) every complex representation of Γ extends to a representation of G :

(6.30) **Theorem.** *If $\rho: \Gamma \rightarrow \mathrm{SL}(\ell, \mathbb{C})$ is any homomorphism, then there is a continuous homomorphism $\hat{\rho}: G \rightarrow \mathrm{SL}(\ell, \mathbb{C})$, such that $\rho = \hat{\rho}$ on a finite-index subgroup of Γ .*

(6.31) **Warning.** The statement of Thm. 6.30 relies on our current assumption that G/Γ is not compact. In general, it may be necessary to mod out a compact group, in which case, the statement is slightly more complicated.

That is the archimedean superrigidity theorem. Margulis also proved a nonarchimedean version, which applies to representations over a p -adic field, rather than $\mathbb{C}$. The philosophy of superrigidity is that every p -adic representation of Γ should extend to a p -adic representation of G . However, G is connected, but p -adic fields are totally disconnected, so G has no nontrivial p -adic representations. Thus, the philosophy suggests that every p -adic representation of Γ should be trivial. This is true, modulo a compact group:

(6.32) **Theorem.** *If $\rho: \Gamma \rightarrow \mathrm{SL}(\ell, \mathbb{Q}_p)$ is any homomorphism, then $\rho(\Gamma)$ is precompact.*

This result can be rephrased in more elementary terms, without any mention of the field $\mathbb{Q}_p$ of p -adic numbers. Namely, the denominators of the matrix entries of elements of γ are bounded:

(6.33) **Corollary.** *If $\rho: \Gamma \rightarrow \mathrm{SL}(\ell, \mathbb{Q})$ is any homomorphism, then there is some nonzero $k \in \mathbb{N}$, such that $\rho(\Gamma) \subset \frac{1}{k} \mathrm{Mat}_{\ell \times \ell}(\mathbb{Z})$.*

Proof. Let $D \subset \mathbb{N}$ be the set consisting of the denominators of the matrix entries of the elements of $\rho(\Gamma)$. We wish to show that D is bounded (or, equivalently, that D is finite).

Since Γ is finitely generated (see 5.57), some finite set of primes $\{p_1, \dots, p_r\}$ contains all the prime factors of every element of D . (If p is in the denominator of some matrix entry of $\rho(\gamma_1 \gamma_2) = \rho(\gamma_1) \rho(\gamma_2)$, then it must appear in a denominator somewhere in either $\rho(\gamma_1)$ or $\rho(\gamma_2)$.) Thus, every element of D is of the form $p_1^{m_1} \cdots p_r^{m_r}$, for some $m_1, \dots, m_r \in \mathbb{N}$. Hence, it suffices to show, for each prime p , that there is some natural number M , such that no element of D is divisible by p^M , for then D is bounded by $p_1^{M_1} \cdots p_r^{M_r}$. Thus, by definition of the p -adic topology, we wish to show that $\{1/d \mid d \in D\}$ is precompact in $\mathbb{Q}_p$. That is precisely the assertion of Thm. 6.32. $\square$

Let us use these two superrigidity theorems to prove (more or less) that $\Gamma \subset \mathrm{SL}(n, \mathbb{Z})$.

Step 1. Every matrix entry of every element of Γ is an algebraic number. This will be proved by more elementary means (as a consequence of a cohomology-vanishing theorem or a rigidity theorem), but let us show how to deduce it from superrigidity (Thm. 6.30). Suppose some $\gamma_{i,j}$ is transcendental. Then, for any transcendental number α , there is a field automorphism ϕ of $\mathbb{C}$ with $\phi(\gamma_{i,j}) = \alpha$. Applying ϕ to all the entries of a matrix induces an automorphism $\tilde{\phi}$ of $\mathrm{SL}(n, \mathbb{C})$. From Thm. 6.30, there is a continuous homomorphism $\hat{\rho}: G \rightarrow \mathrm{SL}(n, \mathbb{C})$, such that $\hat{\rho} = \tilde{\phi}$ on a finite-index subgroup of Γ .

Since there are uncountably many transcendental numbers α , there are uncountably many different choices of ϕ , so there must be uncountably many different n -dimensional representations $\tilde{\phi}$ of G . However, the theory of weights implies that there are only finitely many non-isomorphic representations of G of any given dimension, so this is a contradiction.

(*Technical note:* Actually, this is not quite a contradiction, because it is possible that two different choices of ϕ yield the same representation of Γ , up to isomorphism; that is, after a change of basis. The trace of a matrix is independent of the basis, so the preceding argument really shows that the trace of $\tilde{\phi}(\gamma)$ must be algebraic, for every $\gamma \in \Gamma$. Then one can use some algebraic methods

to show that there is some other representation ρ of Γ , such that the matrix entries of $\rho(\gamma)$ are algebraic, for every $\gamma \in \Gamma$.)

Step 2. We have $\Gamma \subset \mathrm{SL}(n, \mathbb{Q})$. Let F be the subfield of $\mathbb{C}$ generated by the matrix entries of the elements of Γ , so $\Gamma \subset \mathrm{SL}(n, F)$. From Step 1, we know that this is an algebraic extension of $\mathbb{Q}$. Furthermore, because Γ is finitely generated (see 5.57), this field extension is finitely generated. Thus, F is finite-degree field extension of $\mathbb{Q}$ (in other words, F is an algebraic number field). This means that F is almost the same as $\mathbb{Q}$, so it is only a slight exaggeration to say that we have proved $\Gamma \subset \mathrm{SL}(n, \mathbb{Q})$.

Indeed, the method of Restriction of Scalars (see §6G) provides a way to change F into $\mathbb{Q}$: there is a representation $\rho: G \rightarrow \mathrm{SL}(\ell, \mathbb{C})$, such that $\rho(G \cap \mathrm{SL}(n, F)) \subset \mathrm{SL}(\ell, \mathbb{Q})$. Thus, after changing to this new representation of G , we have the desired conclusion (without any exaggeration).

Step 3. A finite-index subgroup of Γ is contained in $\mathrm{SL}(n, \mathbb{Z})$. From p -adic superrigidity, we know that there is some $k \in \mathbb{N}$, such that $\Gamma \subset \frac{1}{k} \mathrm{Mat}_{n \times n}(\mathbb{Z})$. Note that if $k = 1$, then $\Gamma \subset \mathrm{SL}(n, \mathbb{Z})$. More generally, for any value of k , some finite-index subgroup of Γ is contained in $\mathrm{SL}(n, \mathbb{Z})$ (see Exer. 6:12).

6E. Unipotent elements of $G_{\mathbb{Z}}$: the Godement Compactness Criterion

(6.34) **Proposition** (Godement Compactness Criterion). *Assume G is defined over $\mathbb{Q}$. The homogeneous space $G_{\mathbb{Z}} \backslash G$ is compact if and only if $G_{\mathbb{Z}}$ has no nontrivial unipotent elements.*

Proof. ($\Rightarrow$) This is the easy direction (see 5.31).

($\Leftarrow$) We prove the contrapositive: suppose $G_{\mathbb{Z}} \backslash G$ is not compact. (We wish to show that $G_{\mathbb{Z}}$ has a nontrivial unipotent element.) From Prop. 5.33 (and the fact that $G_{\mathbb{Z}}$ is a lattice in G (see 6.10)), we know that there exist nontrivial $\gamma \in G_{\mathbb{Z}}$ and $g \in G$, such that $\gamma^g \approx \mathrm{Id}$. Because the characteristic polynomial of a matrix is a continuous function of the matrix entries of the matrix, we conclude that the characteristic polynomial of γ^g is approximately $(x - 1)^\ell$ (the characteristic polynomial of Id). On the other hand, similar matrices have the same characteristic polynomial, so this means that the characteristic polynomial of γ is approximately $(x - 1)^\ell$. Now all the coefficients of the characteristic polynomial of γ are integers (because γ is an integer matrix), so the only way this polynomial can be close to $(x - 1)^\ell$ is by being exactly equal to $(x - 1)^\ell$. Thus, the characteristic polynomial of γ is $(x - 1)^\ell$, so γ is unipotent. $\square$

The following corollary is a slight restatement of the result. The assumption that Γ is arithmetic will be removed in §16D. On the other hand, the assumption that G has no compact factors cannot be eliminated (see Exer. 6:13).

(6.35) **Corollary.** *Assume that Γ is arithmetic, and that G has no compact factors. The homogeneous space $\Gamma \backslash G$ is compact if and only if Γ has no nontrivial unipotent elements.*

The above proof of Prop. 6.34 relies on the fact that $G_{\mathbb{Z}}$ is a lattice in G . Unfortunately, this basic fact will not be proved until Chap. 15. Thus, the reader may be interested in the following example, which illustrates that the cocompactness of Γ can sometimes be proved quite easily from the Mahler Compactness Criterion (5.34).

(6.36) **Proposition.** *If $B(x, y)$ is an anisotropic, symmetric, bilinear form on $\mathbb{Q}^\ell$, then $\mathrm{SO}(B)_{\mathbb{Z}}$ is cocompact in $\mathrm{SO}(B)_{\mathbb{R}}$.*

Proof. Let $\Gamma = \mathrm{SO}(B)_{\mathbb{Z}}$ and $G = \mathrm{SO}(B)_{\mathbb{R}}$. (Our proof will not use the fact that Γ is a lattice in G .)

Step 1. The image of G in $\mathrm{SL}(\ell, \mathbb{R})/\mathrm{SL}(\ell, \mathbb{Z})$ is precompact. Let

- $\{g_n\}$ be a sequence of elements of G and
- $\{v_n\}$ be a sequence of elements of $\mathbb{Z}^\ell \setminus \{0\}$.

Suppose that $g_nv_n \rightarrow 0$. (This will lead to a contradiction, so the desired conclusion follows from the Mahler Compactness Criterion (5.34).)

Replacing B by an integer multiple to clear the denominators, we may assume $B(\mathbb{Z}^\ell, \mathbb{Z}^\ell) \subset \mathbb{Z}$. Then, since $B(v, v) \neq 0$ for all nonzero $v \in \mathbb{Z}^\ell$, we have $|B(v_n, v_n)| \geq 1$ for all n . Therefore

$$1 \leq |B(v_n, v_n)| = |B(g_nv_n, g_nv_n)| \rightarrow |B(0, 0)| = 0.$$

This is a contradiction.

Step 2. The image of G in $\mathrm{SL}(\ell, \mathbb{R})/\mathrm{SL}(\ell, \mathbb{Z})$ is closed. Suppose $g_n\gamma_n \rightarrow h \in \mathrm{SL}(\ell, \mathbb{R})$, with $g_n \in G$ and $\gamma_n \in \mathrm{SL}(\ell, \mathbb{Z})$. (We wish to show $h \in G \mathrm{SL}(\ell, \mathbb{Z})$.)

Let $\{v_1, \dots, v_\ell\}$ be the standard basis of $\mathbb{R}^\ell$ (so each $v_j \in \mathbb{Z}^\ell$). Replacing B by an integer multiple to clear the denominators, we may assume $B(\mathbb{Z}^\ell, \mathbb{Z}^\ell) \subset \mathbb{Z}$. Then

$$B(\gamma_nv_j, \gamma_nv_k) \subset B(\mathbb{Z}^\ell, \mathbb{Z}^\ell) \subset \mathbb{Z}.$$

We also have

$$B(\gamma_nv_j, \gamma_nv_k) = B(g_n\gamma_nv_j, g_n\gamma_nv_k) \rightarrow B(hv_j, hv_k),$$

so we conclude that $B(\gamma_nv_j, \gamma_nv_k) = B(hv_j, hv_k)$ for any sufficiently large n . Therefore $h\gamma_n^{-1} \in \mathrm{SO}(B) = G$, so $h \in G\gamma_n \subset G \mathrm{SL}(\ell, \mathbb{Z})$.

Step 3. Completion of the proof. Define $\phi: G/\Gamma \rightarrow \mathrm{SL}(\ell, \mathbb{R})/\mathrm{SL}(\ell, \mathbb{Z})$ by $\phi(g\Gamma) = g \mathrm{SL}(\ell, \mathbb{Z})$. By combining Steps 1 and 2, we see that the image of ϕ is compact. Thus, it suffices to show that ϕ is a homeomorphism onto its image.

Given a sequence $\{g_n\}$ in G , such that $\{\phi(g_n\Gamma)\}$ converges, we wish to show that $\{g_n\Gamma\}$ converges. There is a sequence $\{\gamma_n\}$ in $\mathrm{SL}(\ell, \mathbb{Z})$, and some $h \in G$, such that $g_n\gamma_n \rightarrow h$. The proof of Step 2 shows, for all large n , that $h \in G\gamma_n$. Then $\gamma_n \in Gh = G$, so $\gamma_n \in G_{\mathbb{Z}} = \Gamma$. Therefore, $\{g_n\Gamma\}$ converges (to $h\Gamma$), as desired. $\square$

6F. How to make an arithmetic lattice

The definition that (modulo commensurability, isogenies, and compact factors) an arithmetic lattice must be the $\mathbb{Z}$ -points of G has the virtue of being concrete. However, this concreteness imposes a certain lack of flexibility. (Essentially, we have limited ourselves to the standard basis of the vector space $\mathbb{R}^n$, ignoring the possibility that some other basis might be more convenient in some situations.) Let us now describe a more abstract viewpoint that makes the construction of general arithmetic lattices more transparent. (In particular, this approach will be used in §6G.) For any real vector space V , we describe analogues of the subgroups $\mathbb{Z}^\ell$ and $\mathbb{Q}^\ell$ of $\mathbb{R}^\ell$ (see 6.39(1)).

(6.37) **Definition.** Let V be a real vector space.

- A $\mathbb{Q}$ -subspace $V_{\mathbb{Q}}$ of V is a $\mathbb{Q}$ -form of V if the $\mathbb{R}$ -linear map $V_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R} \rightarrow V$ defined by $t \otimes v \mapsto tv$ is an isomorphism (see Exer. 6:15).
- A polynomial f on V is *defined over $\mathbb{Q}$* (with respect to the $\mathbb{Q}$ -form $V_{\mathbb{Q}}$) if $f(V_{\mathbb{Q}}) \subset \mathbb{Q}$ (see Exer. 6:16).

- A finitely generated subgroup $\mathcal{L}$ of the additive group of $V_{\mathbb{Q}}$ is a *vector-space lattice* in $V_{\mathbb{Q}}$ if the $\mathbb{Q}$ -linear map $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{L} \rightarrow V_{\mathbb{Q}}$ defined by $t \otimes v \mapsto tv$ is an isomorphism (see Exer. 6:17).
- The $\mathbb{Q}$ -form $V_{\mathbb{Q}}$ on V determines a corresponding $\mathbb{Q}$ -form on the real vector space $\text{End}(V)$ by

$$\text{End}(V)_{\mathbb{Q}} = \{ A \in \text{End}(V) \mid A(V_{\mathbb{Q}}) \subset V_{\mathbb{Q}} \}$$

(see Exer. 6:19).

- A function Q on a real vector space W is a *polynomial* if for some (hence, every) $\mathbb{R}$ -linear isomorphism $\phi: \mathbb{R}^{\ell} \cong W$, the composition $f \circ \phi$ is a polynomial function on $\mathbb{R}^{\ell}$.
- A virtually connected subgroup H of $\text{SL}(V)$ is *defined over $\mathbb{Q}$* (with respect to the $\mathbb{Q}$ -form $V_{\mathbb{Q}}$) if there exists a set $\mathcal{Q}$ of polynomials on $\text{End}(V)$, such that
 - every $Q \in \mathcal{Q}$ is defined over $\mathbb{Q}$ (with respect to the $\mathbb{Q}$ -form $V_{\mathbb{Q}}$),
 - $\text{Var}(\mathcal{Q}) = \{ g \in \text{SL}(V) \mid Q(g) = 0 \text{ for all } Q \in \mathcal{Q} \}$ is a subgroup of $\text{SL}(V)$; and
 - $H^{\circ} = \text{Var}(\mathcal{Q})^{\circ}$.

(6.38) **Remark.**

- Suppose $G \subset \text{SL}(\ell, \mathbb{R})$. For the standard $\mathbb{Q}$ -form $\mathbb{Q}^{\ell}$ on $\mathbb{R}^{\ell}$, we see that G is defined over $\mathbb{Q}$ in terms of Defn. 6.37 if and only if it is defined over $\mathbb{Q}$ in terms of Defn. 6.2.
- The term *vector-space lattice* is not standard. Authors usually simply call $\mathcal{L}$ a *lattice in $V_{\mathbb{Q}}$* , but this could cause confusion, because $\mathcal{L}$ is *not* a lattice in $V_{\mathbb{Q}}$, in the sense of Defn. 5.8 (although it *is* a lattice in V).

Let us first note that a $\mathbb{Q}$ -form $V_{\mathbb{Q}}$ and vector-space lattice $\mathcal{L}$ simply represent $\mathbb{Q}^{\ell}$ and $\mathbb{Z}^{\ell}$, under some identification of V with $\mathbb{R}^{\ell}$.

(6.39) **Lemma.** *Let V be an ℓ -dimensional real vector space.*

- 1) *If $V_{\mathbb{Q}}$ is a $\mathbb{Q}$ -form of V , then there is a $\mathbb{R}$ -linear isomorphism $\phi: V \rightarrow \mathbb{R}^{\ell}$, such that $\phi(V_{\mathbb{Q}}) = \mathbb{Q}^{\ell}$. Furthermore, if $\mathcal{L}$ is any vector-space lattice in $V_{\mathbb{Q}}$, then ϕ may be chosen so that $\phi(\mathcal{L}) = \mathbb{Z}^{\ell}$.*
- 2) *A polynomial f on $\mathbb{R}^{\ell}$ is defined over $\mathbb{Q}$ (with respect to the $\mathbb{Q}$ -form $\mathbb{Q}^{\ell}$) if and only if every coefficient of f is rational (see Exer. 6:16).*

Second, let us note that any two vector-space lattices in $V_{\mathbb{Q}}$ are commensurable (see Exer. 6:20):

(6.40) **Lemma.** *If $\mathcal{L}_1$ and $\mathcal{L}_2$ are two vector-space lattices in $V_{\mathbb{Q}}$, then there is some nonzero $p \in \mathbb{Z}$, such that $p\mathcal{L}_1 \subset \mathcal{L}_2$ and $p\mathcal{L}_2 \subset \mathcal{L}_1$.*

It is now easy to prove the following more abstract characterization of arithmetic lattices (see Exers. 6:21 and 6:22).

(6.41) **Proposition.** *Suppose $G \subset \text{GL}(V)$, and G is defined over $\mathbb{Q}$, with respect to the $\mathbb{Q}$ -form $V_{\mathbb{Q}}$.*

- 1) *If $\mathcal{L}$ is any vector-space lattice in $V_{\mathbb{Q}}$, then*

$$G_{\mathcal{L}} = \{ g \in G \mid g\mathcal{L} = \mathcal{L} \}$$

is an arithmetic subgroup of G .

- 2) *If $\mathcal{L}_1$ and $\mathcal{L}_2$ are any two vector-space lattices in $V_{\mathbb{Q}}$, then $G_{\mathcal{L}_1}$ and $G_{\mathcal{L}_2}$ are commensurable.*

From Prop. 6.41(2), we see that the arithmetic subgroup $G_{\mathcal{L}}$ is essentially determined by the $\mathbb{Q}$ -form $V_{\mathbb{Q}}$, and does not really depend on the particular choice of the vector-space lattice $\mathcal{L}$.

6G. Restriction of scalars

We know that $\mathrm{SL}(2, \mathbb{Z})$ is an arithmetic lattice in $\mathrm{SL}(2, \mathbb{R})$. In this section, we explain that $\mathrm{SL}(2, \mathbb{Z}[\sqrt{2}])$ is an arithmetic lattice in $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$ (see Prop. 6.44). More generally, if $\mathcal{O}$ is the ring of algebraic integers in some algebraic number field F , and G is defined over F , then $G_{\mathcal{O}}$ is an arithmetic lattice in a certain group G' related to G .

(6.42) **Remark.** In practice, we do not require $\mathcal{O}$ to be the entire ring of algebraic integers in F : it suffices for $\mathcal{O}$ to have finite index in the ring of integers (as an additive group); equivalently, the $\mathbb{Q}$ -span of $\mathcal{O}$ should be all of F , or, in other words, the ring $\mathcal{O}$ should be a vector-space lattice in F . (A vector-space lattice in F that is also a subring is called an *order* in F .)

Any complex vector space can be thought of as a real vector space (of twice the dimension). Similarly, any complex Lie group can be thought of as a real group (of twice the dimension). Restriction of scalars is the generalization of this idea to any field extension F/k , not just $\mathbb{C}/\mathbb{R}$. This yields a general method to construct arithmetic lattices.

(6.43) **Example.** Let

- $F = \mathbb{Q}(\sqrt{2})$,
- $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$, and
- σ be the nontrivial Galois automorphism of F ,

and define a ring homomorphism $\Delta: F \rightarrow \mathbb{R}^2$ by

$$\Delta(x) = (x, \sigma(x)).$$

It is easy to show that $\Delta(\mathcal{O})$ is discrete in $\mathbb{R}^2$. Namely, for $x \in \mathcal{O}$, the product of the coordinates of $\Delta(x)$ is the product $x \cdot \sigma(x)$ of all the Galois conjugates of x . This is the *norm* of the algebraic number x . Because x is an algebraic integer, its norm is an ordinary integer; hence, its norm is bounded away from 0. So it is impossible for both coordinates of $\Delta(x)$ to be small simultaneously.

More generally, if $\mathcal{O}$ is the ring of integers of any number field F , this same argument shows that if we let $\{\sigma_1, \dots, \sigma_r\}$ be the set of all embeddings of $\mathcal{O}$ in $\mathbb{C}$, and define $\Delta: \mathcal{O} \rightarrow \mathbb{C}^r$ by

$$\Delta(x) = (\sigma_1(x), \dots, \sigma_r(x)),$$

then $\Delta(\mathcal{O})$ is a *discrete* subring of $\mathbb{C}^r$. So $\Delta(\Gamma)$ is a discrete subgroup of $\mathrm{SL}(\ell, \mathbb{C})^r$, for any subgroup Γ of $\mathrm{SL}(\ell, \mathcal{O})$.

The main goal of this section is to show, in the special case that $\Gamma = G_{\mathcal{O}}$, and G is defined over F , that the discrete group $\Delta(\Gamma)$ is actually an arithmetic lattice in a certain subgroup of $\mathrm{SL}(\ell, \mathbb{C})^r$.

To illustrate, let us show that $\mathrm{SL}(2, \mathbb{Z}[\sqrt{2}])$ is isomorphic to an irreducible, arithmetic lattice in $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$.

(6.44) **Proposition.** *Let*

- $\Gamma = \mathrm{SL}(2, \mathbb{Z}[\sqrt{2}])$,
- $G = \mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$, and
- σ be the conjugation on $\mathbb{Q}[\sqrt{2}]$ (so $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$, for $a, b \in \mathbb{Q}$),

and define $\Delta: \Gamma \rightarrow G$ by $\Delta(\gamma) = (\gamma, \sigma(\gamma))$.

Then $\Delta(\Gamma)$ is an irreducible, arithmetic lattice in G .

Proof. Let $F = \mathbb{Q}(\sqrt{2})$ and $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$. Then F is a 2-dimensional vector space over $\mathbb{Q}$, and $\mathcal{O}$ is a vector-space lattice in F .

Since $\{(1, 1), (\sqrt{2}, -\sqrt{2})\}$ is both a $\mathbb{Q}$ -basis of $\Delta(F)$ and an $\mathbb{R}$ -basis of $\mathbb{R}^2$, we see that $\Delta(F)$ is a $\mathbb{Q}$ -form of $\mathbb{R}^2$. Therefore,

$$\Delta(F^2) = \{ (u, \sigma(u)) \in F^4 \mid u \in F^2 \}$$

is a $\mathbb{Q}$ -form of $\mathbb{R}^4$, and $\Delta(\mathcal{O}^2)$ is a vector-space lattice in $\Delta(F^2)$.

Now G is defined over $\mathbb{Q}$ (see Exer. 6:24), so $G_{\Delta(\mathcal{O}^2)}$ is an arithmetic lattice in G . It is not difficult to see that $G_{\Delta(\mathcal{O}^2)} = \Delta(\Gamma)$ (see Exer. 6:25). Furthermore, because $\Delta(\Gamma) \cap (\mathrm{SL}(2, \mathbb{R}) \times e)$ is trivial, we see that the lattice $\Delta(\Gamma)$ must be irreducible in G (see 5.24). $\square$

More generally, the proof of Prop. 6.44 shows that if G is defined over $\mathbb{Q}$, then $G_{\mathbb{Z}[\sqrt{2}]}$ is isomorphic to an irreducible lattice in $G \times G$.

Here is another sample application of the method.

(6.45) **Proposition.** *Let $G = \mathrm{SO}(x^2 + y^2 - \sqrt{2}z^2)^\circ \cong \mathrm{SO}(1, 2)^\circ$. Then $G_{\mathbb{Z}[\sqrt{2}]}$ is a cocompact, arithmetic lattice in G .*

Proof. As above, let σ be the conjugation on $\mathbb{Q}(\sqrt{2})$. Let $\Gamma = G_{\mathbb{Z}[\sqrt{2}]}$.

Let $K' = \mathrm{SO}(x^2 + y^2 + \sqrt{2}z^2) \cong \mathrm{SO}(3)$, so $\sigma(\Gamma) \subset K'$; thus, we may define $\Delta: \Gamma \rightarrow G \times K'$ by $\Delta(\gamma) = (\gamma, \sigma(\gamma))$. (Note that $\sigma(\Gamma) \not\subset G$.) Then the above proof shows that $\Delta(\Gamma)$ is an arithmetic lattice in $G \times K'$. (See Exer. 6:26 for the technical point of verifying that $G \times K'$ is defined over $\mathbb{Q}$.) Since K' is compact, we see, by modding out K' , that Γ is an arithmetic lattice in G . (This type of example is the reason for including the compact normal subgroup K' in Defn. 6.16.)

Let γ be any nontrivial element of Γ . Since $\sigma(\gamma) \in K'$, and compact groups have no nontrivial unipotent elements (see 8.20), we know that $\sigma(\gamma)$ is not unipotent. Thus, $\sigma(\gamma)$ has some eigenvalue $\lambda \neq 1$. Hence, γ has the eigenvalue $\sigma^{-1}(\lambda) \neq 1$, so γ is not unipotent. Therefore, Godement's Criterion (6.34) implies that Γ is cocompact. Alternatively, this conclusion can easily be obtained directly from the Mahler Compactness Criterion (5.34) (see Exer. 6:28). $\square$

Let us consider one final example before stating the general result.

(6.46) **Proposition.** *Let*

- $F = \mathbb{Q}(\sqrt[4]{2})$,
- $\mathcal{O} = \mathbb{Z}[\sqrt[4]{2}]$,
- $\Gamma = \mathrm{SL}(2, \mathcal{O})$, and
- $G = \mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{C})$.

Then Γ is isomorphic to an irreducible, arithmetic lattice in G .

Proof. For convenience, let $\alpha = \sqrt[4]{2}$. There are exactly 4 distinct embeddings $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ of F in $\mathbb{C}$ (corresponding to the 4 roots of $x^4 - 2 = 0$); they are determined by:

- $\sigma_0(\alpha) = \alpha$ (so $\sigma_0 = \mathrm{Id}$);
- $\sigma_1(\alpha) = -\alpha$;
- $\sigma_2(\alpha) = i\alpha$;
- $\sigma_3(\alpha) = -i\alpha$.

Define $\Delta: F \rightarrow \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{C}$ by $\Delta(x) = (x, \sigma_1(x), \sigma_2(x))$. Then, arguing much as before, we see that $\Delta(F^2)$ is a $\mathbb{Q}$ -form of $\mathbb{R}^2 \oplus \mathbb{R}^2 \oplus \mathbb{C}^2$, G is defined over $\mathbb{Q}$, and $G_{\Delta(\mathcal{O}^2)} = \Delta(\Gamma)$. $\square$

These examples illustrate all the ingredients of the following general result.

(6.47) **Definition.** Let F be a finite extension of $\mathbb{Q}$ (that is, an *algebraic number field*).

- Two distinct embeddings $\sigma_1, \sigma_2: F \rightarrow \mathbb{C}$ are *equivalent* if $\sigma_1(x) = \overline{\sigma_2(x)}$, for all $x \in F$ (where $\bar{z}$ denotes the usual complex conjugate of the complex number z).
- A *place* of F is an equivalence class of embeddings (see 6.48). Thus, each place consists of either one or two embeddings of F : a *real place* consists of only one embedding (with $\sigma(F) \subset \mathbb{R}$); a *complex place* consists of two embeddings (with $\sigma(F) \not\subset \mathbb{R}$).
- We let $S^\infty = \{\text{places of } F\}$, or, abusing notation, we assume that S^∞ is a set of embeddings, consisting of exactly one embedding from each place.
- For $\sigma \in S^\infty$, we let

$$F_\sigma = \begin{cases} \mathbb{R} & \text{if } \sigma \text{ is real,} \\ \mathbb{C} & \text{if } \sigma \text{ is complex.} \end{cases}$$

Note that $\sigma(F)$ is dense in F_σ , so F_σ is often called the *completion* of F at the place σ .

- For $\mathcal{Q} \subset F_\sigma[x_{1,1}, \dots, x_{\ell,\ell}]$, let

$$\text{Var}_{F_\sigma}(\mathcal{Q}) = \{g \in \text{SL}(\ell, F_\sigma) \mid \mathcal{Q}(g) = 0, \forall \mathcal{Q} \in \mathcal{Q}\}.$$

Thus, for $F_\sigma = \mathbb{R}$, we have $\text{Var}_{\mathbb{R}}(\mathcal{Q}) = \text{Var}(\mathcal{Q})$, and $\text{Var}_{\mathbb{C}}(\mathcal{Q})$ is analogous, using the field $\mathbb{C}$ in place of $\mathbb{R}$.

- Suppose $G \subset \text{SL}(\ell, \mathbb{R})$, and G is defined over F , so there is some subset $\mathcal{Q}$ of $F[x_{1,1}, \dots, x_{\ell,\ell}]$, such that $G = \text{Var}(\mathcal{Q})^\circ$. For any place σ of F , let

$$G^\sigma = \text{Var}_{F_\sigma}(\sigma(\mathcal{Q}))^\circ.$$

Then G^σ , the *Galois conjugate* of G by σ , is defined over $\sigma(F)$.

(6.48) **Remark.** We consider only the *infinite* (or *archimedean*) places; that is the reason for the superscript ∞ on S^∞ . We are ignoring the *finite* (or *nonarchimedean*, or *p-adic*) places, although they are of fundamental importance in number theory, and, therefore, in deeper aspects of the theory of arithmetic groups. For example, superrigidity at the finite places plays a crucial role in the proof of the Margulis Arithmeticity Theorem (see §6D).

(6.49) **Proposition.** If $G \subset \text{SL}(\ell, \mathbb{R})$ is defined over an algebraic number field $F \subset \mathbb{R}$, and $\mathcal{O}$ is the ring of integers of F , then $G_{\mathcal{O}}$ embeds as an arithmetic lattice in

$$\prod_{\sigma \in S^\infty} G^\sigma,$$

via the natural embedding $\Delta: \gamma \mapsto (\sigma(\gamma))_{\sigma \in S^\infty}$.

Furthermore, if G is simple, then the lattice is irreducible.

The argument in the last paragraph of the proof of Prop. 6.45 shows the following:

(6.50) **Corollary.** If G^σ is compact, for some $\sigma \in S^\infty$, then $\Delta(G_{\mathcal{O}})$ is cocompact.

(6.51) **Remark.** Proposition 6.49 is stated only for real groups, but the same conclusions hold if

- $G \subset \text{SL}(\ell, \mathbb{C})$,
- F is an algebraic number field, such that $F \not\subset \mathbb{R}$, and

- G is defined over F , as an algebraic group over $\mathbb{C}$ (see Defn. 10.2); that is, there is a subset $\mathcal{Q}$ of $F[x_{1,1}, \dots, x_{\ell,\ell}]$, such that $G = \text{Var}_{\mathbb{C}}(\mathcal{Q})^\circ$.

For example,

- 1) $\text{SO}(n, \mathbb{Z}[i, \sqrt{2}])$ embeds as an irreducible arithmetic lattice in $\text{SO}(n, \mathbb{C}) \times \text{SO}(n, \mathbb{C})$, and
- 2) $\text{SO}\left(n, \mathbb{Z}\left[\sqrt{1-\sqrt{2}}\right]\right)$ embeds as an irreducible arithmetic lattice in $\text{SO}(n, \mathbb{C}) \times \text{SO}(n, \mathbb{R}) \times \text{SO}(n, \mathbb{R})$.

The following converse shows that restriction of scalars is the only way to construct an irreducible, arithmetic lattice.

(6.52) **Proposition.** *If $\Gamma = G_{\mathbb{Z}}$ is an irreducible lattice in G , and G is not compact, then there exist*

- 1) *an algebraic number field F , with completion F_∞ ($= \mathbb{R}$ or $\mathbb{C}$),*
- 2) *a connected, simple subgroup H of $\text{SL}(\ell, F_\infty)$, for some ℓ , such that H is defined over F (as an algebraic group over F_∞), and*
- 3) *an isogeny*

$$\phi: \prod_{\sigma \in S^\infty} H^\sigma \rightarrow G,$$

such that $\phi(\Delta(H_O))$ is commensurable with Γ .

Proof. It is easier to work with the algebraically closed field $\mathbb{C}$, instead of $\mathbb{R}$, so, to avoid minor complications, let us assume that $G \subset \text{SL}(\ell, \mathbb{C})$ is defined over $\mathbb{Q}[i]$ (as an algebraic group over $\mathbb{C}$), and that $\Gamma = G_{\mathbb{Z}[i]}$. This assumption results in a loss of generality, but similar ideas apply in general.

Write $G = G_1 \times \dots \times G_r$, where each G_i is simple. Let $H = G_1$. We remark that if $r = 1$, then the desired conclusion is obvious: let $F = \mathbb{Q}[i]$, and let ϕ be the identity map.

Let Σ be the Galois group of $\mathbb{C}$ over $\mathbb{Q}[i]$. Because G is defined over $\mathbb{Q}[i]$, we have $\sigma(G) = G$ for every $\sigma \in \Sigma$. Hence, σ must permute the simple factors $\{G_1, \dots, G_r\}$.

We claim that Σ acts transitively on $\{G_1, \dots, G_r\}$. To see this, suppose, for example, that $r = 5$, and that $\{G_1, G_2\}$ is invariant under Σ . Then $A = G_1 \times G_2$ is invariant under Σ , so A is defined over $\mathbb{Q}[i]$. Similarly, $A' = G_3 \times G_4 \times G_5$ is also defined over $\mathbb{Q}[i]$. Then $A_{\mathbb{Z}[i]}$ and $A'_{\mathbb{Z}[i]}$ are lattices in A and A' , respectively, so $\Gamma = G_{\mathbb{Z}[i]} \approx A_{\mathbb{Z}[i]} \times A'_{\mathbb{Z}[i]}$ is reducible. This is a contradiction.

Let

$$\Sigma_1 = \{ \sigma \in \Sigma \mid \sigma(G_1) = G_1 \}$$

be the stabilizer of G_1 , and let

$$F = \{ z \in \mathbb{C} \mid \sigma(z) = z, \forall \sigma \in \Sigma_1 \}$$

be the fixed field of Σ_1 . Because Σ is transitive on a set of r elements, we know that Σ_1 is a subgroup of index r in Σ , so Galois Theory tells us that F is an extension of $\mathbb{Q}[i]$ of degree r .

Since Σ_1 is the Galois group of $\mathbb{C}$ over F , and $\sigma(G_1) = G_1$ for all $\sigma \in \Sigma_1$, we see that G_1 is defined over F .

Let $\sigma_1, \dots, \sigma_r$ be coset representatives of Σ_1 in Σ . Then $\sigma_1|_F, \dots, \sigma_r|_F$ are the r places of F and, after renumbering, we have $G_j = \sigma_j(G_1)$. So (with $H = G_1$), we have

$$\prod_{\sigma \in S^\infty} H^\sigma = H^{\sigma_1|_F} \times \dots \times H^{\sigma_r|_F} = \sigma_1(G_1) \times \dots \times \sigma_r(G_1) = G_1 \times \dots \times G_r = G.$$

Let ϕ be the identity map.

For $h \in H_F$, let $\Delta'(h) = \prod_{j=1}^r \sigma_j(h)$. Then $\sigma(\Delta'(h)) = \Delta'(h)$ for all $\sigma \in \Sigma$, so $\Delta'(h) \in G_{\mathbb{Q}[i]}$. In fact, it is not difficult to see that $\Delta'(H_F) = G_{\mathbb{Q}[i]}$, and then one can verify that $\Delta'(H_{\mathcal{O}}) \approx G_{\mathbb{Z}[i]} = \Gamma$, so $\phi(\Delta(H_{\mathcal{O}}))$ is commensurable with Γ . $\square$

Combining Prop. 6.52 with Cor. 6.50 yields the following result.

(6.53) **Corollary.** *If $G_{\mathbb{Z}}$ is an irreducible lattice in G , and $G/G_{\mathbb{Z}}$ is not cocompact, then G has no compact factors.*

By applying the definition of an arithmetic lattice, we obtain the following conclusion from Prop. 6.52.

(6.54) **Corollary.** *If*

- Γ is an irreducible, arithmetic lattice in G , and
- G is linear and has no compact factors,

then there exist

- 1) an algebraic number field F , with completion F_{∞} ($= \mathbb{R}$ or $\mathbb{C}$),
- 2) a connected, simple subgroup H of $\mathrm{SL}(\ell, F_{\infty})$, for some ℓ , such that H is defined over F (as an algebraic group over F_{∞}), and
- 3) a continuous surjection

$$\phi: \prod_{\sigma \in S^{\infty}} H^{\sigma} \rightarrow G,$$

with compact kernel,

such that $\phi(\Delta(H_{\mathcal{O}}))$ is commensurable with Γ .

(6.55) **Corollary.** *If $G_{\mathbb{Z}}$ is an irreducible lattice in G , and G is not compact, then G is isotypic.*

Proof. From Thm. 6.52, we see that G is isomorphic to the product of Galois conjugates of a simple group H . Since all of these Galois conjugates are of the same type (see 6.56 and 3.35), the desired conclusion follows. $\square$

(6.56) **Lemma.** *If*

- G is defined over an algebraic number field $F \subset \mathbb{R}$, and
- σ is an embedding of F in $\mathbb{R}$,

then $G \otimes \mathbb{C}$ is isogenous to $G^{\sigma} \otimes \mathbb{C}$.

Proof. Extend σ to an automorphism $\hat{\sigma}$ of $\mathbb{C}$. Then $\hat{\sigma}(G \otimes \mathbb{C}) = G^{\sigma} \otimes \mathbb{C}$, so it is clear that $G \otimes \mathbb{C}$ is isomorphic to $G^{\sigma} \otimes \mathbb{C}$. Unfortunately, however, the automorphism σ is not continuous (not even measurable) unless it happens to be the usual complex conjugation, so we have only an isomorphism of abstract groups, not an isomorphism of Lie groups. Thus, although this observation is suggestive, it is not a proof.

It is easier to give a rigorous proof at the Lie algebra level: we will show that $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to $\mathfrak{g}^{\sigma} \otimes_{\mathbb{R}} \mathbb{C}$. Let $\{v_1, \dots, v_n\}$ be a basis of $\mathfrak{g}_F$, and let $\{c_{j,k}^{\ell}\}_{j,k,\ell=1}^n$ be the structure constants with respect to this basis, that is,

$$[v_j, v_k] = \sum_{\ell=1}^n c_{j,k}^{\ell} v_{\ell}.$$

Because G is isogenous to a group that is defined over $\mathbb{Q}$ (see 6.5), there is a basis $\{u_1, \dots, u_n\}$ of $\mathfrak{g}$ with rational structure constants. Write

$$v_k = \sum_{\ell=1}^n \alpha_k^\ell u_\ell$$

with each $\alpha_k^\ell \in \mathbb{C}$, and define

$$v_k^\sigma = \sum_{\ell=1}^n \hat{\sigma}(\alpha_k^\ell) u_\ell.$$

Then $v_1^\sigma, \dots, v_n^\sigma$ is a basis of $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ whose structure constants are $\{\sigma(c_{j,k}^\ell)\}_{j,k,\ell=1}^n$. These are obviously the structure constants of $\mathfrak{g}^\sigma$, so $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to $\mathfrak{g}^\sigma \otimes_{\mathbb{R}} \mathbb{C}$, as desired. $\square$

The same proof yields the following generalization that does not require F or $\sigma(F)$ to be contained in $\mathbb{R}$.

(6.57) **Lemma.** *If*

- G is defined over an algebraic number field F (as an algebraic group over F_∞), and
- σ is an embedding of F in $\mathbb{C}$,

then G and G^σ have the same type.

More precisely, $G \otimes_{F_\infty} \mathbb{C}$ is isogenous to $G^\sigma \otimes_{F_\sigma} \mathbb{C}$ (see Defn. 10.2).

- (6.58) **Remark.** 1) See Exer. 6:31 for an example of a Lie group H , defined over an algebraic number field $F \subset \mathbb{R}$, and an embedding σ of F in $\mathbb{R}$, such that $H \otimes \mathbb{C}$ is not isogenous to $H^\sigma \otimes \mathbb{C}$.
- 2) The proof of (6.56) (or 6.57) used our standing assumption that G is semisimple only to show that G is isogenous to a group that is defined over $\mathbb{Q}$.

6H. Notes

The Margulis Arithmeticity Theorem (6.21) was proved by Margulis [Mar1, Mar3] under the assumption that $\mathbb{R}\text{-rank } G \geq 2$. (Proofs also appear in [Mar5, Thm. A, p. 298] and [Zim].) Much later, the superrigidity theorems of Corlette [Cor] and Gromov-Schoen [G-S] extended this to all groups except $\mathrm{SO}(1, n)$ and $\mathrm{SU}(1, n)$. We remark that these proofs rely on the fact that Γ is finitely generated; Venkataramana [Ven1] showed how to avoid using this assumption.

It was known quite classically that there are nonarithmetic lattices in $\mathrm{SO}(1, 2)$ (or, in other words, in $\mathrm{SL}(2, \mathbb{R})$). This was extended to $\mathrm{SO}(1, n)$, for $n \leq 5$, by Makarov [Mak] and Vinberg [Vin]. More recently, nonarithmetic lattices were constructed by Gromov and Piatetski-Shapiro [G-PS] for every n (see 7.35). Nonarithmetic lattices in $\mathrm{SU}(1, n)$ were constructed by Mostow [Mos2] for $n = 2$, and by Deligne and Mostow [D-M] for $n = 3$. These results on $\mathrm{SO}(1, n)$ and $\mathrm{SU}(1, n)$ are presented briefly in [Mar5, App. C, pp. 353–368].

The Commensurability Criterion (6.29) was proved by Margulis [Mar2]. It appears in [AC-B], [Mar5], and [Zim].

6I. References

- [AC-B] N. A'Campo and M. Burger: Réseaux arithmétiques et commensurateur d'après G. A. Margulis, *Invent. Math.* 116 (1994) 1–25.

- [Cor] K. Corlette: Archimedean superrigidity and hyperbolic geometry, *Ann. Math.* 135, no. 1 (1992) 165–182.
- [D-M] P. Deligne and G. D. Mostow: Monodromy of hypergeometric functions and non-lattice integral monodromy, *Publ. Math. IHES* 63 (1986) 5–89.
- [G-PS] M. Gromov and I. Piatetski-Shapiro: Nonarithmetic groups in Lobachevsky spaces, *Publ. Math. Inst. Hautes Études Sci.* 66 (1988) 93–103. MR **89j**:22019
- [G-S] M. Gromov and R. Schoen: Harmonic maps into singular spaces and p -adic superrigidity for lattices in groups of rank one, *Publ. Math. IHES* 76 (1992) 165–246.
- [Mak] V. S. Makarov: On a certain class of discrete groups of Lobachevsky space having an infinite fundamental region of finite measure, *Soviet Math. Dokl.* 7 (1966) 328–331.
- [Mar1] G. A. Margulis: Arithmetic properties of discrete subgroups, *Russian Math. Surveys* 29:1 (1974) 107–156. Translated from *Uspekhi Mat. Nauk* 29:1 (1974) 49–98.
- [Mar2] G. A. Margulis: Discrete groups of motions of manifolds of non-positive curvature, *Amer. Math. Soc. Translations* 109 (1977) 33–45.
- [Mar3] G. A. Margulis: Arithmeticity of the irreducible lattices in the semi-simple groups of rank greater than 1 (Russian). Appendix to Russian translation of [Rag], 1977. English translation in: *Invent. Math.* 76 (1984) 93–120.
- [Mar5] G. A. Margulis: *Discrete Subgroups of Semisimple Lie Groups*. Springer, Berlin Heidelberg New York, 1991.
- [Mos2] G. D. Mostow: Existence of a non-arithmetic lattice in $SU(2, 1)$, *Proc. Nat. Acad. Sci. USA* 75 (1978) 3029–3033.
- [Rag] M. S. Raghunathan: *Discrete Subgroups of Lie Groups*. Springer, Berlin Heidelberg New York, 1972.
- [Ven1] T. N. Venkataramana: On the arithmeticity of certain rigid subgroups, *C. R. Acad. Sci. Paris* 316, Sér. I (1993) 321–326.
- [Vin] E. B. Vinberg: Discrete groups generated by reflections in Lobachevsky spaces, *Math. USSR Sbornik* 1 (1967) 429–444.
- [Zim] R. J. Zimmer: *Ergodic Theory and Semisimple Groups*. Birkhäuser, Boston, 1984.

Exercises

6:1) Show that if

- G is connected,
- $G \subset \mathrm{SL}(\ell, \mathbb{R})$, and $-\mathrm{Id} \notin G$,

then there exists $h \in \mathrm{SL}(\ell, \mathbb{R})$, such that $(h^{-1}Gh) \cap \mathrm{SL}(\ell, \mathbb{Z})$ is trivial. [Hint: For each nontrivial $\gamma \in \mathrm{SL}(\ell, \mathbb{Z})$, let

$$X_\gamma = \{ h \in \mathrm{SL}(\ell, \mathbb{R}) \mid h\gamma h^{-1} \in G \}.$$

Then each X_γ is nowhere dense in $\mathrm{SL}(\ell, \mathbb{R})$ (see Exer. 4:2b).]

6:2) Prove ($\Leftarrow$) of Theorem 6.8.

6:3) For H as in Warning 6.9, show that $H_{\mathbb{Q}}$ is not dense in H .

6:4) Show that if $G \subset \mathrm{SL}(\ell, \mathbb{R})$, G has no compact factors, and $G_{\mathbb{Z}}$ is a lattice in G , then G is defined over $\mathbb{Q}$. [Hint: Let

$$I = \{ Q \in \mathbb{C}[x_{1,1}, \dots, x_{\ell,\ell}] \mid Q(G_{\mathbb{Z}}) = 0 \}.$$

Then I is an ideal in $\mathbb{C}[x_{1,1}, \dots, x_{\ell,\ell}]$, and we have $\sigma(I) = I$, for every field automorphism σ of $\mathbb{C}$. Thus, I is generated (as an ideal) by $\mathcal{Q} = I \cap \mathbb{Q}[x_{1,1}, \dots, x_{\ell,\ell}]$. Then $\text{Var}(\mathcal{Q}) = \text{Var}(I)$. From the Borel Density Theorem (5.44), we see that $G \subset \text{Var}(I)$. Theorem 4.8 implies that G has finite index in $\text{Var}(I)$.]

6:5) Show that if

- $G \subset \text{SL}(\ell, \mathbb{R})$, and
- $G_{\mathbb{Z}}$ is Zariski dense in G ,

then $G_{\mathbb{Z}}$ is a lattice in G . [*Hint:* It suffices to show that G is defined over $\mathbb{Q}$.]

6:6) Show that if

- G has no compact factors;
- Γ_1 and Γ_2 are arithmetic lattices in G ; and
- $\Gamma_1 \cap \Gamma_2$ is Zariski dense in G ,

then Γ_1 is commensurable to Γ_2 . [*Hint:* If $\phi_j: G \rightarrow H_j$ is an isomorphism, such that $\phi_j(\Gamma_j) = (H_j)_{\mathbb{Z}}$, define $\phi: G \rightarrow H_1 \times H_2$ by $\phi(g) = (\phi_1(g), \phi_2(g))$. Then $\phi(G)_{\mathbb{Z}} = \phi(\Gamma_1 \cap \Gamma_2)$ is Zariski dense in $\phi(G)$, so $\Gamma_1 \cap \Gamma_2$ is a lattice in G (see Exer. 6:5).]

6:7) Show, for $m, n \geq 2$, that $\text{SL}(m, \mathbb{R}) \times \text{SL}(n, \mathbb{R})$ has an irreducible lattice if and only if $m = n$.

6:8) Suppose G is not isogenous to $\text{SO}(1, n) \times K$ or $\text{SU}(1, n) \times K$, for any nontrivial, connected compact group K . Show that if G has an irreducible lattice, then G is isotypic. [*Hint:* Use Rem. 6.23 in the proof of Thm. 6.26.]

6:9) Show, for all $p \in \mathbb{Z}^+$, that $\begin{bmatrix} \sqrt{p} & 0 \\ 0 & 1/\sqrt{p} \end{bmatrix}$ commensurates $\text{SL}(2, \mathbb{Z})$. Conclude, for $G = \text{SL}(2, \mathbb{R})$, that $\text{Comm}_G(G_{\mathbb{Z}})$ is *not* commensurable with $G_{\mathbb{Q}}$.

6:10) Show, for $G = \text{SL}(3, \mathbb{R})$, that $\text{Comm}_G(G_{\mathbb{Z}})$ is *not* commensurable with $G_{\mathbb{Q}}$. [*Hint:* See Exer. 6:9.]

6:11) Show that if G is simple and Γ is not arithmetic, then Γ , $N_G(\Gamma)$, and $\text{Comm}_G(\Gamma)$ are commensurable with each other.

6:12) Suppose Λ is a subgroup of $\text{SL}(n, \mathbb{Q})$, and k is a positive integer, such that $k\lambda \in \text{Mat}_{n \times n}(\mathbb{Z})$ for every $\lambda \in \Lambda$. Show that $\Lambda \cap \text{SL}(n, \mathbb{Z})$ has finite index in Λ . [*Hint:* If $k\gamma \equiv k\lambda \pmod{k}$, then $\gamma\lambda^{-1} \in \text{Mat}_{n \times n}(\mathbb{Z})$.]

6:13) Show that there is a noncompact lattice Γ in $\text{SL}(2, \mathbb{R}) \times \text{SO}(3)$, such that no nontrivial element of Γ is unipotent.

6:14) Suppose $G \subset \text{SL}(\ell, \mathbb{R})$ is defined over $\mathbb{Q}$.

- (a) Show that if N is a closed, normal subgroup of G , and N is defined over $\mathbb{Q}$, then $G_{\mathbb{Z}}N$ is closed in G .
- (b) Show that $G_{\mathbb{Z}}$ is irreducible if and only if no proper, closed, connected, normal subgroup of G is defined over $\mathbb{Q}$. (That is, if and only if G is $\mathbb{Q}$ -simple.)
- (c) Let H be the Zariski closure of the subgroup generated by the unipotent elements of $G_{\mathbb{Z}}$. Show that H is defined over $\mathbb{Q}$.
- (d) Prove Cor. 6.53, without using Prop. 6.52, or any other results on Restriction of Scalars.

6:15) Show that a $\mathbb{Q}$ -subspace $V_{\mathbb{Q}}$ of V is a $\mathbb{Q}$ -form if and only if there is a subset $\mathcal{B}$ of $V_{\mathbb{Q}}$, such that $\mathcal{B}$ is both a $\mathbb{Q}$ -basis of $V_{\mathbb{Q}}$ and an $\mathbb{R}$ -basis of V .

6:16) For the standard $\mathbb{Q}$ -form $\mathbb{Q}^{\ell}$ of $\mathbb{R}^{\ell}$, show that a polynomial is defined over $\mathbb{Q}$ if and only if all of its coefficients are rational.

6:17) Show that a subgroup $\mathcal{L}$ of $V_{\mathbb{Q}}$ is a vector-space lattice in $V_{\mathbb{Q}}$ if and only if there is a $\mathbb{Q}$ -basis $\mathcal{B}$ of $V_{\mathbb{Q}}$, such that $\mathcal{L}$ is the additive abelian subgroup of $V_{\mathbb{Q}}$ generated by $\mathcal{B}$.

6:18) Let V be a real vector space of dimension ℓ , and let $\mathcal{L}$ be a discrete subgroup of the additive group of V .

(a) Show that $\mathcal{L}$ is a finitely generated, abelian group of rank $\leq \ell$, with equality if and only if the $\mathbb{R}$ -span of $\mathcal{L}$ is V .

(b) Show that if the rank of $\mathcal{L}$ is ℓ , then the $\mathbb{Q}$ -span of $\mathcal{L}$ is a $\mathbb{Q}$ -form of V , and $\mathcal{L}$ is a vector-space lattice in $V_{\mathbb{Q}}$.

[Hint: Induction on ℓ . For $\lambda \in \mathcal{L}$, show that the image of $\mathcal{L}$ in $V/(\mathbb{R}\mathcal{L})$ is discrete.]

6:19) Verify that if $V_{\mathbb{Q}}$ is a $\mathbb{Q}$ -form of V , then $\text{End}(V)_{\mathbb{Q}}$ is a $\mathbb{Q}$ -form of $\text{End}(V)$.

6:20) Prove Lemma 6.40, and conclude that Λ_1 and Λ_2 are commensurable.

6:21) Prove Prop. 6.41(1). [Hint: Use Lemma 6.39.]

6:22) Prove Prop. 6.41(2). [Hint: Use Lemma 6.40.]

6:23) In the notation of the proof of Prop. 6.44, show, for the $\mathbb{Q}$ -form $\Delta(F^2)$ of $\mathbb{R}^4$, that

$$\text{End}(\mathbb{R}^4)_{\mathbb{Q}} = \left\{ \begin{bmatrix} A & B \\ \sigma(B) & \sigma(A) \end{bmatrix} \mid A, B \in \text{Mat}_{2 \times 2}(F) \right\}.$$

[Hint: Since the F -span of $\Delta(F^2)$ is F^4 , we have $\text{End}(\mathbb{R}^4)_{\mathbb{Q}} \subset \text{Mat}_{4 \times 4}(F)$. Thus, for any $T \in \text{End}(\mathbb{R}^4)_{\mathbb{Q}}$, we may write $T = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, with $A, B, C, D \in \text{Mat}_{2 \times 2}(F)$. Now use the fact that, for all $u \in F^2$, we have $T(u) = (v, \sigma(v))$, for some $v \in F^2$.]

6:24) In the notation of the proof of Prop. 6.44, let

$$\mathcal{Q} = \{ x_{i,j+2} + x_{i+2,j}, x_{i,j+2}x_{i+2,j} \mid 1 \leq i, j \leq 2 \}.$$

(a) Use the conclusion of Exer. 6:23 to show that each $Q \in \mathcal{Q}$ is defined over $\mathbb{Q}$.

(b) Show that $\text{Var}(\mathcal{Q})^{\circ} = \text{SL}(2, \mathbb{R}) \times \text{SL}(2, \mathbb{R})$.

6:25) In the notation of the proof of Prop. 6.44, use Exer. 6:23 to show that $G_{\Delta(\mathcal{Q}^2)} = \Delta(\Gamma)$.

6:26) Let F , $\mathcal{O}$, σ , and Δ be as in the proof of Prop. 6.44.

If $G \subset \text{SL}(\ell, \mathbb{R})$, and G is defined over F , show that $G \times G$ is defined over $\mathbb{Q}$ (with respect to the $\mathbb{Q}$ -form on $\text{End}(\mathbb{R}^{2\ell})$ induced by the $\mathbb{Q}$ -form $\Delta(F^{\ell})$ on $\mathbb{R}^{2\ell}$).

[Hint: For each $Q \in \mathbb{Q}[x_{1,1}, \dots, x_{\ell,\ell}]$, let us define a corresponding polynomial $Q^+ \in \mathbb{Q}[x_{\ell+1,\ell+1}, \dots, x_{2\ell,2\ell}]$ by replacing every occurrence of each variable $x_{i,j}$ with $x_{\ell+i,\ell+j}$. For example, if $\ell = 2$, then

$$(x_{1,1}^2 + x_{1,2}x_{2,1} - 3x_{1,1}x_{2,2})^+ = x_{3,3}^2 + x_{3,4}x_{4,3} - 3x_{3,3}x_{4,4}.$$

Then, for some set $\mathcal{Q}_0 \subset \mathbb{Q}[x_{1,1}, \dots, x_{\ell,\ell}]$ that defines G as a subgroup of $\text{SL}(\ell, \mathbb{R})$, let

$$\mathcal{Q}_1 = \{ Q + \sigma(Q^+), Q\sigma(Q^+) \mid Q \in \mathcal{Q}_0 \}.$$

A natural generalization of Exer. 6:24 shows that $\text{SL}(\ell, \mathbb{R}) \times \text{SL}(\ell, \mathbb{R})$ is defined over $\mathbb{Q}$: let $\mathcal{Q}_2$ be the corresponding set of $\mathbb{Q}$ -polynomials. Now define $\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2$.]

6:27) Suppose $\mathcal{O}$ is the ring of integers of an algebraic number field F .

(a) Show $\Delta(\mathcal{O})$ is discrete in $\bigoplus_{\sigma \in S^{\infty}} F_{\sigma}$.

(b) Show $\Delta(F)$ is a $\mathbb{Q}$ -form of $\bigoplus_{\sigma \in S^{\infty}} F_{\sigma}$.

(c) Show $\Delta(\mathcal{O})$ is a vector-space lattice in $\Delta(F)$.

6:28) Let

- $B(v, w) = v_1w_1 + v_2w_2 - \sqrt{2}v_3w_3$, for $v, w \in \mathbb{R}^3$,
- $G = \text{SO}(B)^{\circ}$,
- $G^* = G \times G^{\sigma}$,
- $\Gamma = G_{\mathbb{Z}[\sqrt{2}]}$, and

- $\Gamma^* = \Delta(\Gamma)$.

Show:

- (a) The image of G^* in $\mathrm{SL}(6, \mathbb{R})/\mathrm{SL}(6, \mathbb{R})_{\Delta(\mathcal{O}^3)}$ is precompact (by using the Mahler Compactness Criterion).
- (b) The image of G^* in $\mathrm{SL}(6, \mathbb{R})/\mathrm{SL}(6, \mathbb{R})_{\Delta(\mathcal{O}^3)}$ is closed.
- (c) G^*/Γ^* is compact.
- (d) G/Γ is compact (without using the fact that Γ is a lattice in G).

[Hint: This is similar to Prop. 6.36.]

6:29) Suppose F is a real algebraic number field. Show that $\prod_{\sigma \in S^\infty} \mathrm{SL}(\ell, F_\sigma)$ is defined over $\mathbb{Q}$, with respect to the $\mathbb{Q}$ -form on $\mathrm{End}_{\mathbb{R}}(\bigoplus_{\sigma \in S^\infty} (F_\sigma)^\ell)$ induced by the $\mathbb{Q}$ -form $\Delta(F^\ell)$ on $\bigoplus_{\sigma \in S^\infty} (F_\sigma)^\ell$. [Hint: This is a generalization of Exer. 6:24. The proof there is based on the elementary symmetric functions of two variables: $P_1(a_1, a_2) = a_1 + a_2$ and $P_2(a_1, a_2) = a_1 a_2$. For the general case, use symmetric functions of d variables, where d is the degree of F over $\mathbb{Q}$.]

6:30) Suppose $G \subset \mathrm{SL}(\ell, \mathbb{R})$, and G is defined over a real algebraic number field F . Show that $\prod_{\sigma \in S^\infty} G^\sigma$ is defined over $\mathbb{Q}$, with respect to the $\mathbb{Q}$ -form on $\mathrm{End}_{\mathbb{R}}(\bigoplus_{\sigma \in S^\infty} (F_\sigma)^\ell)$ induced by the $\mathbb{Q}$ -form $\Delta(F^\ell)$ on $\bigoplus_{\sigma \in S^\infty} (F_\sigma)^\ell$. [Hint: This is a generalization of Exer. 6:26. See the hint to Exer. 6:29.]

6:31) For $\alpha \in \mathbb{C} \setminus \{0, -1\}$, let $\mathfrak{h}_\alpha$ be the 7-dimensional, nilpotent Lie algebra over $\mathbb{C}$, generated by $\{x_1, x_2, x_3\}$, such that

- $[\mathfrak{h}_\alpha, x_1, x_1] = [\mathfrak{h}_\alpha, x_2, x_2] = [\mathfrak{h}_\alpha, x_3, x_3] = 0$; and
- $[x_2, x_3, x_1] = \alpha[x_1, x_2, x_3]$.

- (a) Show that $[x_3, x_1, x_2] = -(1 + \alpha)[x_1, x_2, x_3]$.
- (b) For $h \in \mathfrak{h}_\alpha$, show that $[\mathfrak{h}_\alpha, h, h] = 0$ if and only if there exists $x \in \{x_1, x_2, x_3\}$ and $t \in \mathbb{C}$, such that $h \in tx + [\mathfrak{h}_\alpha, \mathfrak{h}_\alpha]$.
- (c) Show that $\mathfrak{h}_\alpha \cong \mathfrak{h}_\beta$ if and only if

$$\beta \in \left\{ \alpha, \frac{1}{\alpha}, -(1 + \alpha), -\frac{1}{1 + \alpha}, -\frac{\alpha}{1 + \alpha}, -\frac{1 + \alpha}{\alpha} \right\}.$$

- (d) Show that if the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is at least 7, then there is an embedding σ of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$, such that $\mathfrak{h}_\alpha$ is not isomorphic to $(\mathfrak{h}_\alpha)^\sigma$.

6:32) In the notation of Exer. 6:31, show that if the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is at least 7, then $\mathfrak{h}_\alpha$ is not isomorphic to any Lie algebra that is defined over $\mathbb{Q}$.

6:33) In the notation of Exer. 6:31, show, for $\alpha = \sqrt{2} - (1/2)$, that $\mathfrak{h}_\alpha$ is isomorphic to a Lie algebra that is defined over $\mathbb{Q}$. [Hint: Let $y_1 = x_1 + x_2$ and $y_2 = (x_1 - x_2)/\sqrt{2}$. Show that the $\mathbb{Q}$ -subalgebra of $\mathfrak{h}_\alpha$ generated by $\{y_1, y_2, x_3\}$ is a $\mathbb{Q}$ -form of $\mathfrak{h}_\alpha$.]

6:34) Show, for all natural numbers p and q , that there exist

- a lattice Γ in $\mathrm{SO}(p + q)$ and
- a homomorphism $\rho: \Gamma \rightarrow \mathrm{SO}(p + q)$,

such that $\rho(\Gamma)$ is dense in $\mathrm{SO}(p + q)$.

Examples of Lattices

7A. Arithmetic lattices in $\mathrm{SL}(2, \mathbb{R})$

$\mathrm{SL}(2, \mathbb{Z})$ is the obvious example of an arithmetic lattice in $\mathrm{SL}(2, \mathbb{R})$. Later in this section (see 7.8), we will show that (up to commensurability and conjugates) it is the only one that is not cocompact. In contrast, there are infinitely many cocompact, arithmetic lattices. They can be constructed by either of two methods. Perhaps the easiest way is to note that $\mathrm{SL}(2, \mathbb{R})$ is isogenous to $\mathrm{SO}(2, 1)$.

(7.1) Example.

- 1) Fix positive integers a and b , and let

$$G = \mathrm{SO}(ax^2 + by^2 - z^2; \mathbb{R})^\circ \cong \mathrm{SO}(2, 1)^\circ.$$

If $(0, 0, 0)$ is the only integer solution of the Diophantine equation $ax^2 + by^2 = z^2$, then $G_{\mathbb{Z}}$ is a cocompact, arithmetic lattice in G (see 6.36). See Exer. 7:1 for some examples of a and b satisfying the hypotheses.

- 2) Restriction of Scalars (see §6G) allows us to use algebraic number fields other than $\mathbb{Q}$. Let
 - $F \neq \mathbb{Q}$ be a *totally real* algebraic number field (that is, an algebraic number field with no complex places);
 - $a, b \in F^+$, such that $\sigma(a)$ and $\sigma(b)$ are negative, for every place $\sigma \neq \mathrm{Id}$;
 - $\mathcal{O}$ be the ring of integers of F ; and
 - $G = \mathrm{SO}(ax^2 + by^2 - z^2; \mathbb{R})^\circ \cong \mathrm{SO}(2, 1)^\circ$.

Then $G_{\mathcal{O}}$ is a cocompact, arithmetic lattice in G (cf. 6.45, or see 6.49 and 6.50). See Exer. 7:2 for an example of F , a , and b satisfying the hypotheses.

- 3) In both (1) and (2), the group G is conjugate to $\mathrm{SO}(2, 1)^\circ$, via the diagonal matrix

$$g = \mathrm{diag}(\sqrt{a}, \sqrt{b}, 1).$$

Thus, $g^{-1}(G_{\mathbb{Z}})g$ or $g^{-1}(G_{\mathcal{O}})g$ is a cocompact, arithmetic lattice in $\mathrm{SO}(2, 1)$.

(7.2) **Remark.** For a and b as in 7.1(2), $(0, 0, 0)$ is the only solution in $\mathcal{O}^3$ of the equation $ax^2 + by^2 = z^2$ (see Exer. 7:6). Therefore, 7.1(1) and 7.1(2) can easily be combined into a single construction (cf. 7.9). We separated them for pedagogical reasons.

A proof of the following proposition can be found later in the section (see 7.7).

(7.3) **Proposition.** *The lattices constructed in Eg. 7.1 are the only cocompact, arithmetic lattices in $\mathrm{SO}(2,1)$ (up to commensurability and conjugates).*

More precisely, any cocompact, arithmetic lattice in $\mathrm{SO}(2,1)$ is conjugate to a lattice that is commensurable with a lattice constructed in Eg. 7.1.

The other standard approach is based on quaternion algebras (see Defn. 7.55).

(7.4) **Proposition.** *Fix positive integers a and b , and let*

$$G = \mathrm{SL}(1, D_{a,b}(\mathbb{R})) = \{ g \in D_{a,b}(\mathbb{R}) \mid N_{\mathrm{red}}(g) = 1 \}.$$

Then:

- 1) $G \cong \mathrm{SL}(2, \mathbb{R})$;
- 2) $G_{\mathbb{Z}} = \mathrm{SL}(1, D_{a,b}(\mathbb{Z}))$ *is an arithmetic lattice in G ; and*
- 3) *the following are equivalent:*
 - (a) $G_{\mathbb{Z}}$ *is cocompact in G ;*
 - (b) $(0,0,0,0)$ *is the only integer solution of the Diophantine equation $w^2 - ax^2 - by^2 + abz^2 = 0$;*
 - (c) $D_{a,b}(\mathbb{Q})$ *is a division algebra.*

Proof. (1) Define an $\mathbb{R}$ -linear bijection $\phi: D_{a,b}(\mathbb{R}) \rightarrow \mathrm{Mat}_{2 \times 2}(\mathbb{R})$ by

$$\phi(1) = \mathrm{Id}, \quad \phi(i) = \begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix}, \quad \phi(j) = \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}, \quad \phi(k) = \begin{bmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{bmatrix}.$$

It is straightforward to check that ϕ preserves multiplication, so ϕ is a ring isomorphism.

For $g = w + xi + yj + zk \in D_{a,b}(\mathbb{R})$, we have

$$\det(\phi(g)) = (w + x\sqrt{a})(w - x\sqrt{a}) - (y + z\sqrt{a})(by - bz\sqrt{a}) = w^2 - ax^2 - by^2 + abz^2 = N_{\mathrm{red}}(g).$$

Therefore, $\phi(G) = \mathrm{SL}(2, \mathbb{R})$.

(2) For $g \in G$, define $T_g: D_{a,b}(\mathbb{R}) \rightarrow D_{a,b}(\mathbb{R})$ by $T_g(v) = gv$. Then T_g is $\mathbb{R}$ -linear.

For $\gamma \in D_{a,b}(\mathbb{R})$, we have $T_{\gamma}(D_{a,b}(\mathbb{Z})) \subset D_{a,b}(\mathbb{Z})$ if and only if $\gamma \in D_{a,b}(\mathbb{Z})$. So $G_{\mathbb{Z}} = G \cap D_{a,b}(\mathbb{Z})$ is an arithmetic lattice in G .

(3c $\Rightarrow$ 3a) We prove the contrapositive. Suppose $G_{\mathbb{Z}}$ is not cocompact. Then it has a nontrivial unipotent element γ (see 6.34). So 1 is an eigenvalue of T_{γ} ; that is, there is some nonzero $v \in D_{a,b}(\mathbb{Z})$, such that $T_{\gamma}(v) = v$. By definition of T_{γ} , this means $\gamma v = v$. Hence $(\gamma - 1)v = 0$. Since $\gamma \neq 1$ and $v \neq 0$, this implies $D_{a,b}(\mathbb{Q})$ has zero divisors, so it is not a division algebra.

(3b $\Leftrightarrow$ 3c) This is a concrete restatement of the fact that $D_{a,b}(\mathbb{Q})$ is a division algebra if and only if $N_{\mathrm{red}}(g) \neq 0$, for all nonzero $g \in D_{a,b}(\mathbb{Q})$ (see 10:21).

(3a $\Rightarrow$ 3c) We prove the contrapositive. Suppose $D_{a,b}(\mathbb{Q})$ is not a division algebra. Then $D_{a,b}(\mathbb{Q}) \cong \mathrm{Mat}_{2 \times 2}(\mathbb{Q})$ (see Exer. 11:6). So $\mathrm{SL}(1, D_{a,b}(\mathbb{Z})) \approx \mathrm{SL}(2, \mathbb{Z})$ is not cocompact. (It has nontrivial unipotent elements.) $\square$

The following can be proved similarly (see Exer. 7:3).

(7.5) **Proposition.** *Let*

- $F \neq \mathbb{Q}$ *be a totally real algebraic number field;*
- $\mathcal{O}$ *be the ring of integers of F ;*
- $a, b \in \mathcal{O}$, *such that a and b are positive, but $\sigma(a)$ and $\sigma(b)$ are negative, for every place $\sigma \neq \mathrm{Id}$; and*

- $G = \mathrm{SL}(1, D_{a,b}(\mathbb{R}))$.

Then:

- 1) $G \cong \mathrm{SL}(2, \mathbb{R})$; and
- 2) $G_{\mathcal{O}} = \mathrm{SL}(1, D_{a,b}(\mathcal{O}))$ is a cocompact, arithmetic lattice in G .

(7.6) **Proposition.** *The lattices constructed in Props. 7.4 and 7.5 are the only cocompact, arithmetic lattices in $\mathrm{SL}(2, \mathbb{R})$ (up to commensurability and conjugates).*

Proof. This can be proved directly, but let us derive it as a corollary of Prop. 7.3. For each lattice Γ in $\mathrm{SO}(2, 1)$, constructed in Eg. 7.1, we wish to show, for some arithmetic lattice Γ' in $\mathrm{SL}(2, \mathbb{R})$, constructed in Prop. 7.4 or 7.5, that there is an isogeny $\phi: \mathrm{SL}(2, \mathbb{R}) \rightarrow \mathrm{SO}(2, 1)$, such that $\phi(\Gamma')$ is commensurable with Γ .

(1) First, let us show that every lattice of type 7.1(1) appears in (7.4). Given positive integers a and b , such that $(0, 0, 0)$ is the only rational solution of the equation $ax^2 + by^2 = z^2$, let

$$G = \mathrm{SL}(1, D_{a,b}(\mathbb{R})) \cong \mathrm{SL}(2, \mathbb{R}).$$

One can show that $(0, 0, 0, 0)$ is the only rational solution of the equation $w^2 - ax^2 - by^2 + abz^2 = 0$ (see Exer. 7:4), so $G_{\mathbb{Z}}$ is a cocompact, arithmetic lattice in G (see 7.4).

As a subspace of $D_{a,b}(\mathbb{R})$, the Lie algebra $\mathfrak{g}$ of G is

$$\mathfrak{g} = \{ v \in D_{a,b}(\mathbb{R}) \mid \mathrm{Re} v = 0 \}$$

(see Exer. 7:5). For $g \in G$ and $v \in \mathfrak{g}$, we have $(\mathrm{Ad}_G g)(v) = gvg^{-1}$, so $N_{\mathrm{red}}|_{\mathfrak{g}}$ is a quadratic form on $\mathfrak{g}$ that is invariant under $\mathrm{Ad} G_F$. For $v = xi + yj + zk \in \mathfrak{g}$, we have

$$N_{\mathrm{red}}(v) = -ax^2 - by^2 + abz^2.$$

After the change of variables $x \mapsto by$ and $y \mapsto ax$, this becomes $-ab(ax^2 + by^2 - z^2)$, which is a scalar multiple of the quadratic form in 7.1(1). Thus, after identifying $\mathfrak{g}$ with $\mathbb{R}^3$ by an appropriate choice of basis, the lattice constructed in 7.1(1) (for the given values of a and b) is commensurable with $\mathrm{Ad}_G G_{\mathbb{Z}}$.

(2) Similarly, every lattice of type 7.1(1) appears in (7.5) (see Exer. 7:7). □

(7.7) **Proof of Prop. 7.3.** Let Γ be a cocompact, arithmetic lattice in $\mathrm{SO}(2, 1)$. Ignoring the technical problem that not all automorphisms are inner (cf. 4.52), it suffices to show that there is an automorphism α of $\mathrm{SO}(2, 1)$, such that $\alpha(\Gamma)$ is commensurable with one of the lattices constructed in Eg. 7.1.

Step 1. There are

- an algebraic number field $F \subset \mathbb{R}$, with ring of integers $\mathcal{O}$,
- a symmetric, bilinear form $B(x, y)$ on F^3 , and
- an isogeny $\phi: \mathrm{SO}(B; \mathbb{R}) \rightarrow \mathrm{SO}(2, 1)^{\circ}$,

such that $\phi(\mathrm{SO}(B; \mathcal{O}))$ is commensurable with Γ . We give two proofs.

First, let us note that this is immediate from Fig. 10.2 (on p. 153). There are two possibilities listed for $\mathrm{SO}(p, q)$, but $p + q = 1 + 2 = 3$ is odd in our case, so only one of the listings is relevant: Γ must be $\mathrm{SO}(B; \mathcal{O})$, for some algebraic number field $F \subset \mathbb{R}$.

Second, let us give a direct proof that does not rely on the results of Chap. 10. Because all (irreducible) arithmetic lattices are obtained by Restriction of Scalars (see 6.54), we know that there are

- an algebraic number field $F \subset \mathbb{R}$, with ring of integers $\mathcal{O}$,
- a simple Lie group $H \subset \mathrm{SL}(\ell, \mathbb{R})$ that is defined over F , and
- an isogeny $\phi: H \rightarrow \mathrm{SO}(2, 1)^\circ$,

such that $\phi(H_{\mathcal{O}})$ is commensurable with Γ . All that remains is to show that we may identify H_F with $\mathrm{SO}(B; F)$, for some symmetric bilinear form B on F^3 .

The Killing form

$$\kappa(u, v) = \mathrm{trace}((\mathrm{ad}_{\mathfrak{h}} u)(\mathrm{ad}_{\mathfrak{h}} v))$$

is a symmetric, bilinear form on the Lie algebra $\mathfrak{h}$. It is invariant under $\mathrm{Ad} H$, so Ad_H is an isogeny from H to $\mathrm{SO}(\kappa; \mathbb{R})$. Pretending that Ad_H is an isomorphism, not just an isogeny, we may identify H with $\mathrm{SO}(\kappa; \mathbb{R})$. Note that $\kappa(\mathfrak{h}_F, \mathfrak{h}_F) \subset F$, so, by identifying $\mathfrak{h}_F$ with F^3 , we may think of κ as a bilinear form on F^3 .

Step 2. We may assume that $B(x, x) = ax_1^2 + bx_2^2 - x_3^2$ for some $a, b \in F^+$ (cf. 10.64(1) and 10.72). By choosing an orthogonal basis, we may assume $B(x, x) = ax_1^2 + bx_2^2 + cx_3^2$. Since $\mathrm{SO}(B; \mathbb{R}) \approx \mathrm{SO}(2, 1)$, we know that $\pm B(x, x)$ is a signature $(2, 1)$. So we may assume $a, b, -c \in F^+$. Dividing by c (which does not change the orthogonal group) yields the desired form.

Step 3. F is totally real, and both $\sigma(a)$ and $\sigma(b)$ are negative, for all places $\sigma \neq \mathrm{Id}$. Since $\Delta(G_{\mathcal{O}})$ is an irreducible lattice in $\prod_{\sigma \in S^\infty} G^\sigma$ (see 6.49), but the projection to the first factor, namely G , is Γ , which is discrete, we know that G^σ is compact, for all $\sigma \neq \mathrm{Id}$. Thus, $G^\sigma \cong \mathrm{SO}(3)$, so $F_\sigma = \mathbb{R}$, and the three real numbers $\sigma(a)$, $\sigma(b)$, and $\sigma(-1)$ all have the same sign.

Step 4. B is anisotropic over F . Let us assume $F = \mathbb{Q}$. (This is the only case we need.) Since $G_{\mathbb{Z}}$ is cocompact, we know that it has no nontrivial unipotent elements (see 5.31 or 6.34). Therefore $B(x, x) \neq 0$, for every nonzero $x \in \mathbb{Q}^3$ (see Exer. 11:3). $\square$

(7.8) **Proposition.** $\mathrm{SL}(2, \mathbb{Z})$ is the only noncocompact, arithmetic lattice in $\mathrm{SL}(2, \mathbb{R})$ (up to commensurability and conjugates).

Proof. Let us consider the isogenous group $\mathrm{SO}(2, 1)$, instead of $\mathrm{SL}(2, \mathbb{R})$.

Step 1. There are

- a symmetric, bilinear form $B(x, y)$ on $\mathbb{Q}^3$, and
- an isogeny $\phi: \mathrm{SO}(B; \mathbb{R}) \rightarrow \mathrm{SO}(2, 1)^\circ$,

such that $\phi(\mathrm{SO}(B; \mathbb{Z}))$ is commensurable with Γ . From Steps 1 and 3 of the proof of Prop. 7.3, we have a totally real number field F , such that H^σ is compact for all $\sigma \neq \mathrm{Id}$. On the other hand, since Γ is not cocompact, we know that each H^σ is noncompact (see 6.50). Thus, Id is the only place of F , so $F = \mathbb{Q}$.

Step 2. We may assume $B(x, x) = x_1^2 + x_2^2 - x_3^2$. Because Γ is not cocompact, we know that B is isotropic over F (see 6.36). Therefore, the desired conclusion is obtained by a change of basis, and replacing B with a scalar multiple (see 10.72(3)). $\square$

7B. Teichmüller space and moduli space of lattices in $\mathrm{SL}(2, \mathbb{R})$

This section isn't written yet!!!

7C. Arithmetic lattices in $\mathrm{SO}(1, n)$

(7.9) **Proposition.** *Let*

- F be an algebraic number field that is totally real;
- $\mathcal{O}$ be the ring of integers of F ;
- $a_1, \dots, a_n \in \mathcal{O}$, such that
 - each a_j is positive, and
 - each $\sigma(a_j)$ is negative, for every place $\sigma \neq \mathrm{Id}$; and
- $G = \mathrm{SO}(a_1x_1^2 + \dots + a_nx_n^2 - x_{n+1}^2; \mathbb{R})^\circ \cong \mathrm{SO}(n, 1)^\circ$.

Then

- 1) $G_{\mathcal{O}}$ is an arithmetic lattice in G ; and
- 2) $G_{\mathcal{O}}$ is cocompact if and only if $(0, \dots, 0)$ is the only solution in $\mathcal{O}^{n+1}$ of the equation $a_1x_1^2 + \dots + a_nx_n^2 = x_{n+1}^2$.

(7.10) **Remark.** If F and $a_1, \dots, a_n$ are as in Prop. 7.9, and $G_{\mathcal{O}}$ is *not* cocompact, then $F = \mathbb{Q}$ (cf. Exer. 7:6).

These are the only arithmetic lattices when n is even (see Fig. 10.2 on p. 153):

(7.11) **Proposition.** *If n is even, then the lattices constructed in Prop. 7.9 are the only arithmetic lattices in $\mathrm{SO}(n, 1)$ (up to commensurability and conjugates).*

For any $n \neq 7$, they include all of the arithmetic lattices that are not cocompact:

(7.12) **Proposition.** *If $n \neq 7$, then any noncocompact, arithmetic lattice in $\mathrm{SO}(n, 1)$ is (up to commensurability and conjugates) one of the lattices constructed in Prop. 7.9 with $F = \mathbb{Q}$.*

(7.13) **Remark.** The case $n = 7$ is exceptional: there exist noncocompact arithmetic lattices in $\mathrm{SO}(7, 1)$ that are not obtained from Prop. 7.9 (cf. 10.51).

Theoretically, it is easy to tell whether two choices of $a_1, \dots, a_n$ give essentially the same lattice:

(7.14) **Proposition.** *Let*

- F , $\mathcal{O}$, and $a_1, \dots, a_n$ be as in Prop. 7.9,
- $\Gamma = h^{-1} \mathrm{SO}(a_1x_1^2 + \dots + a_nx_n^2 - x_{n+1}^2; \mathcal{O}) h$, where $h = \mathrm{diag}(\sqrt{a_1}, \dots, \sqrt{a_n}, 1)$,
- $a'_1, \dots, a'_n \in \mathcal{O}$, such that
 - each a_j is positive, and
 - each $\sigma(a_j)$ is negative, for every place $\sigma \neq \mathrm{Id}$;
 and
- $\Gamma' = (h')^{-1} \mathrm{SO}(a'_1x_1^2 + \dots + a'_nx_n^2 - x_{n+1}^2; \mathcal{O}) h'$, where $h' = \mathrm{diag}(\sqrt{a'_1}, \dots, \sqrt{a'_n}, 1)$.

There exists $g \in \mathrm{O}(n, 1)$, such that $g^{-1}\Gamma g$ is commensurable to Γ' if and only if the quadratic forms

$$B(x) = a_1x_1^2 + \dots + a_nx_n^2 - x_{n+1}^2 \quad \text{and} \quad B'(x) = a'_1x_1^2 + \dots + a'_nx_n^2 - x_{n+1}^2$$

are equivalent, up to a scalar multiple from $F^\times$ and a change of basis of F^{n+1} .

More precisely, if and only if there exists $\lambda \in F^\times$ and $g' \in \mathrm{GL}(n+1, F)$, such that

$$(g')^T \mathrm{diag}(a_1, \dots, a_n, -1) g' = \lambda \mathrm{diag}(a'_1, \dots, a'_n, -1).$$

Proof. ($\Leftarrow$) See Exer. 7:10.

($\Rightarrow$) Let $g' = h'gh^{-1}$. Then

$$\begin{aligned} (g')^{-1} \mathrm{SO}(B; \mathcal{O}) g' &= h' g (h^{-1} \mathrm{SO}(B; \mathcal{O}) h) g^{-1} (h')^{-1} \\ &= h' (g \Gamma g^{-1}) (h')^{-1} \\ &\approx h' \Gamma' (h')^{-1} \\ &\subset h' \mathrm{SO}(n, 1) (h')^{-1} \\ &= \mathrm{SO}(B'; \mathbb{R}). \end{aligned}$$

From the Borel Density Theorem (5.44), we know that $\mathrm{SO}(B; \mathcal{O})$ is Zariski dense in $\mathrm{SO}(B; \mathbb{R})$, so we conclude that $(g')^{-1} \mathrm{SO}(B; \mathbb{R}) g' \subset \mathrm{SO}(B'; \mathbb{R})$.

Also, we have $(g')^{-1} \mathrm{SO}(B; \mathbb{R}) g' \subset \mathrm{SO}(B \circ g'; \mathbb{R})$. Since $\mathrm{SO}(B; \mathbb{R}) \otimes \mathbb{C} \cong \mathrm{SO}(n+1; \mathbb{C})$ is irreducible on $\mathbb{C}^{n+1}$, we know that the quadratic form on $\mathbb{R}^{n+1}$ that is invariant under $(g')^{-1} \mathrm{SO}(B; \mathbb{R}) g'$ is unique up to a scalar multiple (see Exer. 10:30). Hence, there is some $\lambda \in \mathbb{R}^\times$ with $B \circ g' = \lambda B'$. Since both B and B' are defined over F , we must have $\lambda \in F^\times$. $\square$

In practice, the condition given by Prop. 7.14 is sometimes rather subtle, as the following example indicates.

(7.15) **Example.** Define quadratic forms $B_1(x)$ and $B_2(x)$ on $\mathbb{Q}^{n+1}$ by

$$B_1(x) = x_1^2 + \cdots + x_n^2 - x_{n+1}^2$$

and

$$B_2(x) = x_1^2 + \cdots + x_n^2 - 2x_{n+1}^2,$$

and let

- $\Gamma_1 = \mathrm{SO}(B_1; \mathbb{Z})$ and
- $\Gamma_2 = h^{-1} \mathrm{SO}(B_2; \mathbb{Z}) h$, where $h = \mathrm{diag}(1, \dots, 1, \sqrt{2}) \in \mathrm{GL}(n+1, \mathbb{R})$.

There exists $g \in \mathrm{O}(1, n)$, such that $g\Gamma_1 g^{-1}$ is commensurable to Γ_2 if and only if n is even.

Proof. ($\Leftarrow$) For

$$g' = \begin{bmatrix} 1 & 1 & & & & \\ 1 & -1 & & & & \\ & & 1 & 1 & & \\ & & 1 & -1 & & \\ & & & & \ddots & \\ & & & & & 1 & 1 \\ & & & & & 1 & -1 \\ & & & & & & & 2 \end{bmatrix},$$

we have

$$(g')^T \mathrm{diag}(1, \dots, 1, -1) g' = \mathrm{diag}(2, 2, \dots, 2, -4) = 2 \mathrm{diag}(1, 1, \dots, -2)$$

so the desired conclusion follows from Prop. 7.14.

($\Rightarrow$) This follows from Cor. 7.16 below, because 2 is not a square in $\mathbb{Q}$. $\square$

(7.16) **Corollary.** Let F , $\mathcal{O}$, $a_1, \dots, a_n$, $a'_1, \dots, a'_n$, Γ , and Γ' be as in Prop. 7.14.

If n is odd, and there exists $g \in \mathrm{O}(1, n)$, such that $g\Gamma g^{-1}$ is commensurable to Γ' then

$$\frac{a_1 \cdots a_n}{a'_1 \cdots a'_n} \in (F^\times)^2.$$

Proof. The *discriminant* of a quadratic form $B(x)$ on F^{n+1} is defined to be $\det[B]_{\mathcal{B}}$, for any basis $\mathcal{B}$ of F^{n+1} . This is not uniquely determined by B , but it is well-defined up to multiplication by a nonzero square in $F^\times$, because

$$\det[B]_{g\mathcal{B}} = \det(g^T[B]_{\mathcal{B}}g) = (\det g)^2 \det[B]_{\mathcal{B}},$$

for any $g \in \mathrm{GL}(n+1, F)$.

Note that $\det[\lambda B]_{\mathcal{B}} = \lambda^{n+1} \det[B]_{\mathcal{B}}$. Thus, if n is odd, then λB has the same discriminant as B (up to multiplication by a square). $\square$

When n is odd, additional cocompact lattices can be constructed by using quaternion algebras:

(7.17) **Notation** (cf. Exers. 7:8 and 7:9). Suppose

- β and γ are nonzero elements of $\mathbb{R}$, such that either β or γ is positive; and
- x is an invertible element of $D_{\beta, \gamma}(\mathbb{R})$, such that $\tau_r(x) = x$.

We may write $x = a + bi + dk$, for some $a, b, d \in \mathbb{R}$ (such that $a^2 - \beta(b^2 + \gamma d^2) \neq 0$); define

$$\varepsilon_{\beta, \gamma}(x) = \begin{cases} 1 & \text{if } \gamma(a^2 - \beta(b^2 - \gamma d^2)) > 0; \\ 0 & \text{if } \gamma < 0, \beta(b^2 - \gamma d^2) < a^2, \text{ and } a < 0; \\ 2 & \text{if } \gamma < 0, \beta(b^2 - \gamma d^2) < a^2, \text{ and } a > 0; \\ 0 & \text{if } \gamma > 0, \beta(b^2 - \gamma d^2) > a^2, \text{ and } (\beta + 1)b + (\beta - 1)d\sqrt{\gamma} > 0; \\ 2 & \text{if } \gamma > 0, \beta(b^2 - \gamma d^2) > a^2, \text{ and } (\beta + 1)b + (\beta - 1)d\sqrt{\gamma} < 0. \end{cases}$$

(7.18) **Proposition.** *Let*

- F be a totally real algebraic number field;
- β and γ be nonzero elements of F , such that, for each place σ of F , either $\sigma(\beta)$ or $\sigma(\gamma)$ is positive;
- $a_1, \dots, a_m \in D_{\beta, \gamma}(F)$, such that
 - $\tau_r(a_j) = a_j$ for each j ,
 - $\sigma(a_j)$ is invertible, for each j , and each place σ ,
 - $\sum_{j=1}^m \varepsilon_{\beta, \gamma}(a_j) = 1$, and
 - $\sum_{j=1}^m \varepsilon_{\sigma(\beta), \sigma(\gamma)}(\sigma(a_j)) \in \{0, 2m\}$ for each place $\sigma \neq \mathrm{Id}$;
- $\mathcal{O}$ be a vector-space lattice in $D_{\beta, \gamma}(F)$, such that $\mathcal{O}$ is also a subring; and
- $G = \mathrm{SU}(\mathrm{diag}(a_1, \dots, a_m); D_{\beta, \gamma}(\mathbb{R}), \tau_r)^\circ$.

Then:

- 1) $G \cong \mathrm{SO}(1, 2m - 1)^\circ$; and
- 2) $G_{\mathcal{O}}$ is a cocompact, arithmetic lattice in G .

(7.19) **Proposition.** *If $n \neq 7$, then the lattices constructed in Props. 7.9 and 7.18 are the only arithmetic lattices in $\mathrm{SO}(n, 1)$ (up to commensurability and conjugates).*

See Rem. 10.51 for a brief explanation of the need to assume $n \neq 7$.

7D. Some nonarithmetic lattices in $\mathrm{SO}(1, n)$

Section 7C describes algebraic methods to construct all of the arithmetic lattices in $\mathrm{SO}(1, n)$ (when $n \neq 7$). We now present a geometric method that sometimes allows us to produce a new lattice by combining two known lattices. The result is often nonarithmetic.

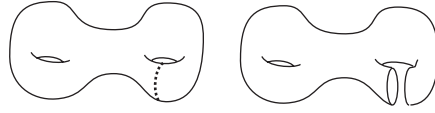


Figure 7.1. Cutting open a manifold by slicing along a closed hypersurface (dashed) results in a manifold with boundary.

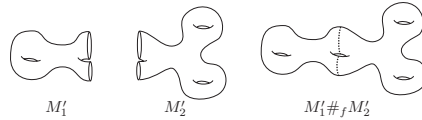


Figure 7.2. Gluing M'_1 to M'_2 along their boundaries results in a manifold without boundary.

7Da. Hyperbolic manifolds. For geometric purposes, it is more convenient to consider the locally symmetric space $\Gamma \backslash \mathfrak{H}^n$, instead of the lattice Γ .

(7.20) **Definition.** A connected, Riemannian n -manifold M is *hyperbolic* if

- 1) M is locally isometric to $\mathfrak{H}^n$ (that is, each point of M has a neighborhood that is isometric to an open set in $\mathfrak{H}^n$);
- 2) M is complete; and
- 3) M is orientable.

(7.21) **Other terminology.** Many authors do not require M to be complete or orientable. Our requirement (1) is equivalent to the assertion that M has constant sectional curvature -1 ; some authors relax this to require the sectional curvature to be a negative constant, but do not require it to be normalized to -1 .

(7.22) **Notation.** Let $\mathrm{PO}(1, n) = \mathrm{O}(1, n) / \{\pm \mathrm{Id}\}$.

Note that:

- $\mathrm{PO}(1, n)$ is isogenous to $\mathrm{SO}(1, n)$;
- $\mathrm{PO}(1, n) \cong \mathrm{Isom}(\mathfrak{H}^n)$; and
- $\mathrm{PO}(1, n)$ has two connected components (one component represents orientation-preserving isometries of $\mathfrak{H}^n$, and the other represents orientation-reversing isometries).

The following observation is easy to prove (see Exer. 7:11).

(7.23) **Proposition.** A connected Riemannian manifold M of finite volume is hyperbolic if and only if there is a torsion-free lattice Γ in $\mathrm{PO}(1, n)^\circ$, such that M is isometric to $\Gamma \backslash \mathfrak{H}^n$.

7Db. Hybrid manifolds and totally geodesic hypersurfaces. We wish to combine two (arithmetic) hyperbolic manifolds M_1 and M_2 into a single hyperbolic manifold. The idea is that we will choose closed hypersurfaces C_1 and C_2 of M_1 and M_2 , respectively, such that C_1 is isometric to C_2 . Let M'_j be the manifold with boundary that results from cutting M_j open, by slicing along C_j (see Fig. 7.1 and Exer. 7:13). The boundary of M'_1 (namely, two copies of C_1) is isometric to the boundary of M'_2 (namely, two copies of C_2) (see Exer. 7:13). So we may glue M'_1 and M'_2 together, by identifying $\partial M'_1$ with $\partial M'_2$ (see Fig. 7.2), as described in the following well-known proposition.

(7.24) **Proposition.** Suppose

- M'_1 and M'_2 are connected n -manifolds with boundary; and
- $f': \partial M'_1 \rightarrow \partial M'_2$ is any homeomorphism.

Define a topological space $M'_1 \cup_{f'} M'_2$, by gluing M'_1 to M'_2 along their boundaries:

- let $M'_1 \sqcup M'_2$ be the disjoint union of M'_1 and M'_2 ;
- define an equivalence relation on $M'_1 \sqcup M'_2$ by specifying that $m \sim f'(m)$, for every $m \in \partial M'_1$; and
- let $M'_1 \cup_{f'} M'_2 = (M'_1 \sqcup M'_2) / \sim$ be the quotient of $M'_1 \sqcup M'_2$ by this equivalence relation.

Then $M'_1 \cup_{f'} M'_2$ is an n -manifold (without boundary).

(7.25) **Corollary.** Suppose

- M_1 and M_2 are connected, orientable n -manifolds;
- C_j is a closed $(n-1)$ -submanifold of M_j ; and
- $f: C_1 \rightarrow C_2$ is any homeomorphism.

Define $M_1 \#_f M_2 = M'_1 \cup_{f'} M'_2$, where

- M'_j is the manifold with boundary obtained by slicing M_j open along C_j ; and
- $f': \partial M'_1 \rightarrow \partial M'_2$ is defined by $f'(c, k) = (f(c), k)$, under a natural identification of $\partial M'_j$ with $C_j \times \{1, 2\}$.

Then $M_1 \#_f M_2$ is a (connected) n -manifold (without boundary).

Furthermore,

- 1) $M_1 \#_f M_2$ is compact if and only if both M_1 and M_2 are compact; and
- 2) $M_1 \#_f M_2$ is connected if and only if either $M_1 \setminus C_1$ or $M_2 \setminus C_2$ is connected.

(7.26) **Other terminology.** Gromov and Piatetski-Shapiro [G-PS] call the manifold $M_1 \#_f M_2$ a *hybrid* of M_1 and M_2 , and they call this construction *interbreeding*.

Unfortunately, gluing two Riemannian manifolds together does not always result in a Riemannian manifold (in any natural way), even if the gluing map f is an isometry from $\partial M'_1$ to $\partial M'_2$.

(7.27) **Example.** Let $M'_1 = M'_2$ be the closed unit disk in $\mathbb{R}^2$, and let $f: \partial M'_1 \rightarrow \partial M'_2$ be the identity map. Then $M'_1 \cup_f M'_2$ is homeomorphic to the 2-sphere S^2 . The Riemannian metrics on M'_1 and M'_2 are flat, so the resulting Riemannian metric on S^2 would also be flat. However, there is no flat Riemannian metric on S^2 . (This follows, for example, from the Gauss-Bonnet Theorem.)

We can eliminate this problem by putting a restriction on the hypersurface C_j .

(7.28) **Definition.** A *totally geodesic hypersurface* in a hyperbolic n -manifold M is a (closed, nonempty) connected submanifold C of M , such that, for each point c of C , there are

- a neighborhood U of c in M ;
- a point x in $\mathfrak{H}^{n-1} = \{v \in \mathfrak{H}^n \mid v_1 = 0\}$;
- a neighborhood V of x in $\mathfrak{H}^n$; and
- a Riemannian isometry $g: U \rightarrow V$, such that $g(U \cap C) = V \cap \mathfrak{H}^{n-1}$.

(7.29) **Remark.** If C is a totally geodesic hypersurface in a hyperbolic n -manifold of finite volume, then there are

- a lattice Γ in $\mathrm{PO}(1, n)$, and
- an isometry $f: M \rightarrow \Gamma \backslash \mathfrak{H}^n$,

such that $f(C)$ is the image of $\mathfrak{H}^{n-1}$ in $\Gamma \backslash \mathfrak{H}^n$.

(7.30) **Proposition.** *If*

- M_1 and M_2 are hyperbolic n -manifolds;
- C_j is a totally geodesic hypersurface in M_j ; and
- $f: C_1 \rightarrow C_2$ is a Riemannian isometry; and
- M_1 and M_2 have finite volume,

then $M_1 \#_f M_2$ is a hyperbolic n -manifold of finite volume.

Proof. The main issue is to show that each point of $\partial M'_1$ has a neighborhood U in $M'_1 \cup_{f'} M'_2$, such that U is isometric to an open subset of $\mathfrak{H}^n$. This is not difficult (see Exer. 7:14).

We have $\mathrm{vol}(M_1 \#_f M_2) = \mathrm{vol}(M_1) + \mathrm{vol}(M_2) < \infty$.

If $M_1 \#_f M_2$ is compact, then it is obviously complete. More generally, since M'_1 and M'_2 are complete, and their union is all of $M'_1 \cup_f M'_2$, it seems rather obvious that every Cauchy sequence in $M'_1 \cup_f M'_2$ has a convergent subsequence. Hence, it seems to be more-or-less obvious that $M'_1 \cup_f M'_2$ is complete.

Unfortunately, if $M_1 \#_f M_2$ is not compact, then there is a technical difficulty arising from the possibility that, theoretically, the Riemannian isometry f may not be an isometry with respect to the topological metrics that C_1 and C_2 inherit as submanifolds of M_1 and M_2 , respectively. See Exer. 14:2 for an indication of how to deal with this problem. $\square$

The following lemma describes how we will construct the totally geodesic hypersurface C_j .

(7.31) **Lemma.** *Suppose*

- Γ is a torsion-free lattice in $\mathrm{PO}(1, n)^\circ$;
- C is the image of $\mathfrak{H}^{n-1}$ in $\Gamma \backslash \mathfrak{H}^n$;
- $\Gamma \cap \mathrm{PO}(1, n-1)$ is a lattice in $\mathrm{PO}(1, n-1)$;
- $\tau: \mathfrak{H}^n \rightarrow \mathfrak{H}^n$ is the reflection across $\mathfrak{H}^{n-1}$ (that is, $\tau(v_1, v_2, \dots, v_{n+1}) = (-v_1, v_2, \dots, v_{n+1})$); and
- Γ is contained in a torsion-free lattice Γ' of $\mathrm{PO}(1, n)^\circ$, such that Γ' is normalized by τ .

Then C is a totally geodesic hypersurface in $\Gamma \backslash \mathfrak{H}^n$, and C has finite volume (as an $(n-1)$ -manifold).

Proof. It is clear, from the definition of C , that we need only show C is a (closed, embedded) submanifold of $\Gamma \backslash \mathfrak{H}^n$.

Let $\Gamma_0 = \{\gamma \in \Gamma \mid \gamma(\mathfrak{H}^{n-1}) = \mathfrak{H}^{n-1}\}$. (Then $\Gamma \cap \mathrm{PO}(1, n-1)$ is a subgroup of index at most two in Γ_0 .) The natural map

$$\phi: \Gamma_0 \backslash \mathfrak{H}^{n-1} \rightarrow \Gamma \backslash \mathfrak{H}^n$$

is proper (cf. Exer. 5:18), so C , being the image of ϕ , is closed.

Because ϕ is obviously an immersion (and is a proper map), all that remains is to show that ϕ is injective. This follows from the assumption on Γ' (see Exer. 7:15). $\square$

7Dc. Construction of nonarithmetic lattices. The following theorem is the key to the construction of nonarithmetic lattices. We postpone the proof until later in the section (see 7Dd and Exer. 7:21).

(7.32) **Definition.** A hyperbolic n -manifold of finite volume is *arithmetic* if the corresponding lattice Γ in $\mathrm{PO}(1, n)$ (see 7.23) is arithmetic. (Note that Γ is well-defined, up to conjugacy (see Exer. 7:12), so this definition is independent of the choice of Γ .)

(7.33) **Theorem.** *Suppose*

- M_1 and M_2 are hyperbolic n -manifolds;
- C_j is a totally geodesic hypersurface in M_j ;
- $f: C_1 \rightarrow C_2$ is a Riemannian isometry;
- M_1 and M_2 have finite volume (as n -manifolds);
- C_1 and C_2 have finite volume (as $(n-1)$ -manifolds); and
- each of $M_1 \setminus C_1$ and $M_2 \setminus C_2$ is connected.

If the hyperbolic manifold $M_1 \#_f M_2$ is arithmetic, then $M_1 \#_f M_2$ is commensurable to M_1 ; that is, there are

- 1) a finite cover $\widetilde{M}$ of $M_1 \cup_f M_2$, and
- 2) a finite cover $\widetilde{M}_1$ of M_1 ,

such that $\widetilde{M}$ is isometric to $\widetilde{M}_1$.

(7.34) **Corollary.** *In the situation of Thm. 7.33, if the hyperbolic manifold $M_1 \#_f M_2$ is arithmetic, then M_1 is commensurable to M_2 .*

Proof. From Thm. 7.33, we know that $M_1 \#_f M_2$ is commensurable to M_1 . By interchanging M_1 and M_2 , we see that $M_1 \#_f M_2$ is also commensurable to M_2 . By transitivity, M_1 is commensurable to M_2 . $\square$

(7.35) **Corollary.** *There are nonarithmetic lattices Γ_{cpct} and Γ_{non} in $\mathrm{SO}(1, n)$, such that Γ_{cpct} is cocompact, and Γ_{non} is not cocompact.*

Proof. We construct only Γ_{non} . (See Exer. 7:16 for the construction of Γ_{cpct} , which is similar.)

Define quadratic forms $B_1(x)$ and $B_2(x)$ on $\mathbb{Q}^{n+1}$ by

$$B_1(x) = x_1^2 - x_2^2 - x_3^2 - \cdots - x_n^2 - x_{n+1}^2$$

and

$$B_2(x) = x_1^2 - x_2^2 - x_3^2 - \cdots - x_n^2 - 2x_{n+1}^2.$$

Let

- $\Gamma_1 \approx \mathrm{SO}(B_1; \mathbb{Z})$;
- $\Gamma_2 \approx h^{-1} \mathrm{SO}(B_2; \mathbb{Z})h$, where $h = \mathrm{diag}(1, 1, \dots, 1, \sqrt{2}) \in \mathrm{GL}(n+1, \mathbb{R})$;
- $M_j = \Gamma_j \backslash \mathfrak{H}^n$;
- C_j be the image of $\mathfrak{H}^{n-1}$ in M_j ; and
- $\hat{\Gamma}_j = \Gamma_j \cap \mathrm{SO}(1, n-1)$.

Then Γ_1 and Γ_2 are noncompact (arithmetic) lattices in $\mathrm{SO}(1, n)$ (see 7.9). By passing to finite-index subgroups, we may assume Γ_1 and Γ_2 are torsion free (see 5.60). Thus, M_1 and M_2 are hyperbolic n -manifolds of finite volume (see 7.23).

Because $\hat{\Gamma}_j \approx \mathrm{SO}(1, n-1; \mathbb{Z})$ is a lattice in $\mathrm{SO}(1, n-1)$, and $\mathrm{SO}(B_j; \mathbb{Z})$ is normalized by the involution τ of Lem. 7.31, we know that C_j is a totally geodesic hypersurface in M_j that has finite volume (see 7.31).

Let us assume that $M_1 \setminus C_1$ and $M_2 \setminus C_2$ are connected. (See Exer. 7:18 for a way around this issue, or note that this hypothesis can be achieved by passing to finite covers of M_1 and M_2 .)

We know that $\hat{\Gamma}_1 \approx \hat{\Gamma}_2$ (because both subgroups are commensurable to $\mathrm{SO}(1, n-1; \mathbb{Z})$). By taking a little bit of care in the choice of Γ_1 and Γ_2 , we may arrange that $\hat{\Gamma}_1 = \hat{\Gamma}_2$ (see Exer. 7:19). Then

$$C_1 \cong \hat{\Gamma}_1 \backslash \mathfrak{H}^{n-1} = \hat{\Gamma}_2 \backslash \mathfrak{H}^{n-1} \cong C_2,$$

so there is an isometry $f: C_1 \rightarrow C_2$.

If n is odd, then M_1 is not commensurable to M_2 (see 7.16), so Cor. 7.34 implies that $M_1 \#_f M_2$ is not arithmetic; thus, the corresponding lattice Γ_{non} is not arithmetic (see Defn. 7.32). When n is even, an additional argument is needed; see Exer. 7:20. $\square$

7Dd. Proof of Theorem 7.33. Let us recall the following lemma, which was proved in Exer. 6:6.

(7.36) **Lemma.** *If*

- G has no compact factors;
- Γ_1 and Γ_2 are arithmetic lattices in G ; and
- $\Gamma_1 \cap \Gamma_2$ is Zariski dense in G ,

then Γ_1 is commensurable to Γ_2 .

(7.37) **Definition.** Let M' be a Riemmanian n -manifold with boundary. We say that M' is a *hyperbolic manifold with totally geodesic boundary* if

- 1) M' is complete;
- 2) each point of $M' \setminus \partial M'$ has a neighborhood that is isometric to an open set in $\mathfrak{H}^n$; and
- 3) for each point p of $\partial M'$, there are
 - a neighborhood U of p in M' ;
 - a point x in $\mathfrak{H}^{n-1} = \{v \in \mathfrak{H}^n \mid v_1 = 0\}$;
 - a neighborhood V of x in $\mathfrak{H}^n$; and
 - an isometry $g: U \rightarrow V^+$, where

$$V^+ = \{v \in V \mid v_1 \geq 0\}.$$

(Note that $g(U \cap \partial M') = V \cap \mathfrak{H}^{n-1}$.)

The following is a generalization of Thm. 7.33 (see Exer. 7:21).

(7.38) **Theorem.** *Suppose*

- M_1 and M_2 are hyperbolic n -manifolds;
- M'_j is a connected, n -dimensional submanifold of M_j with totally geodesic boundary;
- $f': \partial M'_1 \rightarrow \partial M'_2$ is an isometry;
- M_1 and M_2 have finite volume (as n -manifolds);
- $\partial M'_j$ has only finitely many components; and

- $\partial M'_1$ and $\partial M'_2$ have finite volume (as $(n-1)$ -manifolds).

If the hyperbolic manifold $M'_1 \cup_{f'} M'_2$ is arithmetic, then $M'_1 \cup_{f'} M'_2$ is commensurable to M_1 .

Proof.

- Let $M = M'_1 \cup_{f'} M'_2$.
- Write $M = \Gamma \backslash \mathfrak{H}^n$, for some torsion-free lattice Γ in $\mathrm{PO}(1, n)$.
- Let $\phi: \mathfrak{H}^n \rightarrow M$ be the resulting covering map.
- Let $B = \phi^{-1}(\partial M'_1)$. Because M'_1 has totally geodesic boundary, we know that B is a union of disjoint hyperplanes. (That is, each component of B is of the form $g(\mathfrak{H}^{n-1})$, for some $g \in \mathrm{O}(1, n)$.)
- Let V be the closure of some connected component of $\mathfrak{H}^n \setminus B$ that contains a point of $\phi^{-1}(M'_1)$.
- Let

$$\Gamma' = \{ \gamma \in \Gamma \mid \gamma V = V \} = \{ \gamma \in \Gamma \mid \gamma V \cap V \text{ has nonempty interior} \}$$

(see Exer. 7:22), so $M'_1 = \phi(V) \cong \Gamma' \backslash V$.

By definition, V is an intersection of half-spaces, so it is (hyperbolically) convex; hence, it is simply connected. Therefore, V is the universal cover of M'_1 , and Γ' can be identified with the fundamental group of M'_1 .

Since $M'_1 \subset M_1$, we may define $\Gamma_1, \phi_1, B_1, V_1, \Gamma'_1$ as above, but with M_1 in the place of M . From the uniqueness of the universal cover of M'_1 , we know that there is an isometry $\psi: V \rightarrow V_1$, and an isomorphism $\psi_*: \Gamma' \rightarrow \Gamma'_1$, such that $\psi(\gamma v) = \psi_*(\gamma) \psi(v)$, for all $\gamma \in \Gamma'$ and $v \in V$. Since ψ extends to an isometry of $\mathfrak{H}^n$, we may assume (after replacing Γ_1 with $\psi^{-1}\Gamma_1\psi$) that $V = V_1$ and $\psi_* = \mathrm{Id}$. Hence $\Gamma' = \Gamma'_1 \subset \Gamma \cap \Gamma_1$. It suffices to show (after replacing Γ by a conjugate subgroup) that the Zariski closure of Γ' contains $\mathrm{PO}(1, n)^\circ$, for then Lem. 7.36 implies Γ is commensurable with Γ_1 .

Claim. We may assume that the Zariski closure of Γ' contains $\mathrm{PO}(1, n)^\circ$. We may assume $\mathfrak{H}^{n-1}$ is one of the connected components of ∂V . Since $\partial M'_1$ has finite volume, this means that

$$(7.39) \quad \Gamma' \cap \mathrm{SO}(1, n-1) \text{ is a lattice in } \mathrm{PO}(1, n-1).$$

Let $\overline{\Gamma'}$ be the Zariski closure of Γ' . From (7.39) and the Borel Density Theorem (5.44), we know that $\overline{\Gamma'}$ contains $\mathrm{PO}(1, n-1)^\circ$. Then, since $\mathrm{PO}(1, n-1)^\circ$ is a maximal connected subgroup of $\mathrm{PO}(1, n)$ (see Exer. 7:23), we may assume that $\overline{\Gamma'}^\circ = \mathrm{PO}(1, n-1)^\circ$. (Otherwise, the claim holds.) Because $\overline{\Gamma'}^\circ$ has finite index in $\overline{\Gamma'}$ (see 4.5), this implies that $\mathrm{PO}(1, n-1)^\circ$ contains a finite-index subgroup of Γ' . In fact,

$$(7.40) \quad \{ \gamma \in \Gamma' \mid \gamma H = H \} \text{ has finite index in } \Gamma', \text{ for every connected component } H \text{ of } \partial V.$$

This will lead to a contradiction.

Case 1. Assume ∂V is connected. We may assume $\partial V = \mathfrak{H}^{n-1}$. Then, by passing to a finite-index subgroup, we may assume that $\Gamma' \subset \mathrm{PO}(1, n-1)$ (see 7.40). Define $g \in \mathrm{Isom}(\mathfrak{H}^n)$ by

$$g(v_1, v_2, \dots, v_n) = (-v_1, v_2, \dots, v_n).$$

Then

- g centralizes Γ' ; and
- $\mathfrak{H}^n = V \cup g(V)$.

Since $\Gamma' \backslash V \cong M'_1$ has finite volume, we know that $\Gamma' \backslash g(V)$ also has finite volume. Therefore

$$\Gamma' \backslash \mathfrak{H}^n = (\Gamma' \backslash V) \cup (\Gamma' \backslash g(V))$$

has finite volume, so Γ' is a lattice in $\mathrm{PO}(1, n)$. But this contradicts the Borel Density Theorem (5.44) (since $\Gamma' \subset \mathrm{PO}(1, n-1)$).

Case 2. Assume ∂V is not connected. Let H_1 and H_2 be two distinct connected components of ∂V . Replacing Γ' by a finite-index subgroup, let us assume that each of H_1 and H_2 is invariant under Γ' (see 7.40).

To simplify the argument, let us assume that $\partial M'_1$ is compact, rather than merely that it has finite volume. (See Exer. 7:24 for the general case.) Thus, $\Gamma' \backslash H_1$ is compact, so there is a compact subset C of H_1 , such that $\Gamma' C = H_1$. Let

$$\delta = \min\{\mathrm{dist}(c, H_2) \mid c \in C\} > 0.$$

Because Γ' acts by isometries, we have $\delta = \mathrm{dist}(H_1, H_2)$. Because $\mathfrak{H}^n$ is negatively curved, there is a unique point p in H_1 , such that $\mathrm{dist}(p, H_2) = \delta$. The uniqueness implies that p is fixed by every element of Γ' . Since Γ acts freely on $\mathfrak{H}^n$ (recall that it is a group of deck transformations), we conclude that Γ' is trivial. This contradicts the fact that $\Gamma' \backslash H_1$ is compact. (Note that $H_1 \cong \mathfrak{H}^{n-1}$ is not compact.) $\square$

7E. Noncocompact lattices in $\mathrm{SL}(3, \mathbb{R})$

We saw in Prop. 7.8 that $\mathrm{SL}(2, \mathbb{Z})$ is essentially the only noncocompact, arithmetic lattice in $\mathrm{SL}(2, \mathbb{R})$. So it may be surprising that $\mathrm{SL}(3, \mathbb{Z})$ is *not* the only one in $\mathrm{SL}(3, \mathbb{R})$.

(7.41) **Proposition.** *Let*

- L be a real quadratic extension of $\mathbb{Q}$, so $L = \mathbb{Q}(\sqrt{r})$, for some square-free positive integer $r \geq 2$;
- σ be the Galois automorphism of L ;
- $\tilde{\sigma}$ be the automorphism of $\mathrm{Mat}_{3 \times 3}(L)$ induced by applying σ to each entry of a matrix;
- $J_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$; and
- $\Gamma = \mathrm{SU}(J_3; \mathbb{Z}[\sqrt{r}], \sigma) = \{g \in \mathrm{SL}(3, \mathbb{Z}[\sqrt{r}]) \mid \tilde{\sigma}(g^T) J_3 g = J_3\}$.

Then:

- 1) Γ is an arithmetic lattice in $\mathrm{SL}(3, \mathbb{R})$;
- 2) Γ is not cocompact; and
- 3) $\mathbb{Q}\text{-rank}(\Gamma) = 1$.

Proof. (1) This is a special case of Prop. 10.55(6), but we provide a concrete, explicit proof (using the methods of §6F and §6G).

Define

- $\Delta: L^3 \rightarrow \mathbb{R}^6$ by $\Delta(v) = (v, J_3 \sigma(v))$,
- $V_{\mathbb{Q}} = \Delta(L^3)$,
- $\mathcal{L} = \Delta(\mathbb{Z}[\sqrt{r}]^3)$; and
- $\rho: \mathrm{SL}(3, \mathbb{R}) \rightarrow \mathrm{SL}(6, \mathbb{R})$ by $\rho(A)(v, w) = (Av, (A^T)^{-1}w)$ for $v, w \in \mathbb{R}^3$.

Then

- $V_{\mathbb{Q}}$ is a $\mathbb{Q}$ -form of $\mathbb{R}^6$ (cf. Exer. 6:27b),
- $\mathcal{L}$ is a vector-space lattice in $V_{\mathbb{Q}}$ (cf. Exer. 6:27c),
- ρ is a homomorphism,
- $\rho(\mathrm{SL}(3, \mathbb{R}))$ is defined over $\mathbb{Q}$ (with respect to the $\mathbb{Q}$ -form $V_{\mathbb{Q}}$) (see 7.42 below), and
- $\Gamma = \{g \in \mathrm{SL}(3, \mathbb{R}) \mid \rho(g)\mathcal{L} = \mathcal{L}\}$ (cf. Exer. 6:23).

Thus, Prop. 6.41(1) (together with Thm. 6.10) implies that Γ is an arithmetic lattice in $\mathrm{SL}(3, \mathbb{R})$.

Now let us show that

$$(7.42) \quad \rho(\mathrm{SL}(3, \mathbb{R})) \text{ is defined over } \mathbb{Q}.$$

This can be verified directly, by finding an appropriate collection of $\mathbb{Q}$ -polynomials, but let us, instead, show that $\rho(\mathrm{SL}(3, \mathbb{R}))_{\mathbb{Q}}$ is dense in $\rho(\mathrm{SL}(3, \mathbb{R}))$.

Define U_1 as in (7.43), but allowing a, b, c to range over all of $\mathbb{Q}$, instead of only $2\mathbb{Z}$. Then $\rho(U_1)V_{\mathbb{Q}} \subset V_{\mathbb{Q}}$ (see Exer. 7:25), so $\rho(U_1) \subset \rho(\mathrm{SL}(3, \mathbb{R}))_{\mathbb{Q}}$. Furthermore, U_1 is dense in

$$U = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}.$$

Similarly, there is a dense subgroup U_2 of U^T , such that $\rho(U_2) \subset \rho(\mathrm{SL}(3, \mathbb{R}))_{\mathbb{Q}}$ (see Exer. 7:26). Since $\langle U, U^T \rangle = \mathrm{SL}(3, \mathbb{R})$, we know that $\langle U_1, U_2 \rangle$ is dense in $\mathrm{SL}(3, \mathbb{R})$, so $\rho(\mathrm{SL}(3, \mathbb{R}))_{\mathbb{Q}}$ is dense in $\rho(\mathrm{SL}(3, \mathbb{R}))$. Therefore $\rho(\mathrm{SL}(3, \mathbb{R}))$ is defined over $\mathbb{Q}$ (see 6.8).

(2) By calculation, one may verify, directly from the definition of Γ , that the subgroup

$$(7.43) \quad U_{\Gamma} = \left\{ \begin{bmatrix} 1 & a + b\sqrt{r} & -(a^2 - rb^2)/2 + c\sqrt{r} \\ 0 & 1 & -a + b\sqrt{r} \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in 2\mathbb{Z} \right\}$$

is contained in Γ . Then, since every element of U_{Γ} is unipotent, it is obvious that Γ has nontrivial unipotent elements. So the Godement Criterion (6.34) implies that $\Gamma \backslash G$ is not compact.

(3) Define a nondegenerate σ -Hermitian form $B(x, y)$ on L^3 by $B(x, y) = \sigma(x^T) J_3 y$. Then $(1, 0, 0)$ is an isotropic vector for B . On the other hand, because B is nondegenerate, and L^3 is 3-dimensional, there are no 2-dimensional totally isotropic subspaces (see Exer. 11:7). Thus, the maximal totally isotropic subspaces are one-dimensional, so $\mathbb{Q}\text{-rank}(\Gamma) = 1$ (cf. 9.6(2)). $\square$

(7.44) **Remark.**

- 1) Recall that $\mathbb{Q}\text{-rank}(\mathrm{SL}(3, \mathbb{Z})) = 2$ (see 2.13 and 9.6(1)). Thus, 7.41(3) implies that none of the lattices in Prop. 7.41 are conjugate to a lattice that is commensurable with $\mathrm{SL}(3, \mathbb{Z})$.

Indeed, let $X = \mathrm{SL}(3, \mathbb{R})/\mathrm{SO}(3)$ be the symmetric space associated to $\mathrm{SL}(3, \mathbb{R})$. Theorem 2.17 implies that if Γ is one of the lattices constructed in Prop. 7.41, then the geometry of the locally symmetric space $\Gamma \backslash X$ is very different from that of $\mathrm{SL}(3, \mathbb{Z}) \backslash X$. Namely, $\Gamma \backslash X$ is only mildly noncompact: it has finitely many cusps; its tangent cone at ∞ is a union of finitely many rays. In contrast, the tangent cone at ∞ of $\mathrm{SL}(3, \mathbb{Z}) \backslash X$ is a 2-complex, not just a union of rays. Even from a distance, $\Gamma \backslash X$ and $\mathrm{SL}(3, \mathbb{Z}) \backslash X$ look completely different.

- 2) Different values of r always give essentially different lattices (see Exer. 7:28), but this is not so obvious.

The classification results stated in Chap. 10 imply that these are the only lattices in $\mathrm{SL}(3, \mathbb{R})$ that are not cocompact.

(7.45) **Proposition.** *$\mathrm{SL}(3, \mathbb{Z})$ and the lattices constructed in Prop. 7.41 are the only noncocompact lattices in $\mathrm{SL}(3, \mathbb{R})$ (up to commensurability and conjugates).*

Proof (from Fig. 10.2 on p. 153). Let Γ be a lattice in $\mathrm{SL}(3, \mathbb{R})$, such that $\Gamma \backslash \mathrm{SL}(3, \mathbb{R})$ is *not* compact. We know, from the Margulis Arithmeticity Theorem (6.21), that Γ is arithmetic. Since $\Gamma \backslash \mathrm{SL}(3, \mathbb{R})$ is not compact, this implies there are

- a group $G \subset \mathrm{SL}(\ell, \mathbb{R})$, defined over $\mathbb{Q}$, and
- an isogeny $\phi: G \rightarrow \mathrm{SL}(3, \mathbb{R})$,

such that $\phi(G_{\mathbb{Z}})$ is commensurable with Γ (see 6.17).

From Fig. 10.2, we see that there are only two possibilities for $G_{\mathbb{Q}}$. Furthermore, because $\Gamma \backslash \mathrm{SL}(3, \mathbb{R})$ is not compact, we must have $F = \mathbb{Q}$ (see 10.60).

Case 1. Assume $G_{\mathbb{Q}} = \mathrm{SL}(n, D)$, for some central division algebra D of degree d over $\mathbb{Q}$, with $dn = 3$. Because 3 is prime, there are only two possibilities for n and d .

Subcase 1.1. Assume $n = 3$ and $d = 1$. Because $d = 1$, we have $\dim_{\mathbb{Q}} D = 1$, so $D = \mathbb{Q}$. Thus, $G_{\mathbb{Q}} = \mathrm{SL}(3, \mathbb{Q})$. Therefore $\Gamma \approx \mathrm{SL}(3, \mathbb{Z})$.

Subcase 1.2. Assume $n = 1$ and $d = 3$. We have $G_{\mathbb{Q}} = \mathrm{SL}(1, D)$. Then $\Gamma \approx \mathrm{SL}(1, \mathcal{O}_D)$ is cocompact (see 7.51(2)). This is a contradiction.

Case 2. Assume $G_{\mathbb{Q}} = \mathrm{SU}(B; D, \tau)$, for B, D, σ as in 10.48(6), with $F = \mathbb{Q}$, $L \subset \mathbb{R}$, and $dn = 3$. If $n = 1$, then $G_{\mathbb{Q}} = \mathrm{SL}(1, D)$, so Subcase 1.2 applies. Thus, we may assume that $n = 3$ and $d = 1$.

Since $d = 1$, we have $D = L$, so $G_{\mathbb{Q}} = \mathrm{SU}(B; L, \sigma)$, where σ is the (unique) Galois automorphism of L over $\mathbb{Q}$, and B is a σ -Hermitian form on L^3 .

Since Γ is not cocompact, we know that B is isotropic (cf. 9.6(2)), so there is a basis of L with $[B] = J_3$ (see 10.72(3)). Therefore Γ is as in Prop. 7.41. $\square$

7F. Cocompact lattices in $\mathrm{SL}(3, \mathbb{R})$

Combining the ideas of Eg. 7.1 and Prop. 7.41 results in the following construction of cocompact lattices in $\mathrm{SL}(3, \mathbb{R})$.

(7.46) **Proposition.** *Let*

- F be a totally real algebraic number field;
- L be a totally real quadratic extension of F ,
- τ be the Galois automorphism of L over F ;
- $a, b \in F^+$, such that
 - $\sigma(a)$ and $\sigma(b)$ are negative, for every place $\sigma \neq \mathrm{Id}$; and
 - $(0, 0, 0)$ is the only solution in L of the equation $ax\tau(x) + by\tau(y) = z\tau(z)$;
- $\mathcal{O}$ be the ring of integers of L ; and
- $\Gamma = \mathrm{SU}(\mathrm{diag}(a, b, -1); \mathcal{O}, \tau)$.

Then Γ is a cocompact, arithmetic lattice in $\mathrm{SL}(3, \mathbb{R})$.

Here is a construction of additional examples. See Eg. 7.49 for explicit examples of L and p that satisfy the hypotheses.

(7.47) **Proposition.** *Let*

- L be a cubic, Galois extension of $\mathbb{Q}$ (that is, a Galois extension of $\mathbb{Q}$, such that $[L : \mathbb{Q}] = 3$);
- σ be a generator of $\text{Gal}(L/\mathbb{Q})$ (note that $\text{Gal}(L/\mathbb{Q})$, being of order 3, is cyclic);
- $\mathcal{O}$ be the ring of integers of L ;
- $p \in \mathbb{Z}^+$;
- $\phi: L^3 \rightarrow \text{Mat}_{3 \times 3}(L)$ be given by

$$(7.48) \quad \phi(x, y, z) = \begin{bmatrix} x & y & z \\ p\sigma(z) & \sigma(x) & \sigma(y) \\ p\sigma^2(y) & p\sigma^2(z) & \sigma^2(x) \end{bmatrix};$$

and

- $\Gamma = \{ \gamma \in \phi(\mathcal{O}^3) \mid \det \gamma = 1 \}.$

Then:

- 1) Γ is an arithmetic lattice in $\text{SL}(3, \mathbb{R})$.
- 2) Γ is cocompact if and only if $p \neq t\sigma(t)\sigma^2(t)$, for all $t \in L$.

Proof. (1) It is easy to see that

- $L \subset \mathbb{R}$ (see Exer. 7:29);
- $\phi(L^3)$ and $\phi(\mathcal{O}^3)$ are subrings of $\text{Mat}_{3 \times 3}(L)$ (even though ϕ is *not* a ring homomorphism);
- $\phi(L^3)$ is a $\mathbb{Q}$ -form of $\text{Mat}_{3 \times 3}(\mathbb{R})$;
- $\phi(\mathcal{O}^3)$ is a vector-space lattice in $\phi(L^3)$;
- if we define $\rho: \text{Mat}_{3 \times 3}(\mathbb{R}) \rightarrow \text{End}_{\mathbb{R}}(\text{Mat}_{3 \times 3}(\mathbb{R}))$ by $\rho(g)(v) = gv$, then $\rho(\text{SL}(3, \mathbb{R}))$ is defined over $\mathbb{Q}$ (with respect to the $\mathbb{Q}$ -form $\phi(L^3)$ (see Exer. 7:30)); and
- $\Gamma = \{ g \in \text{SL}(3, \mathbb{R}) \mid g\phi(\mathcal{O}^3) = \phi(\mathcal{O}^3) \}.$

So Γ is an arithmetic lattice in $\text{SL}(3, \mathbb{R})$ (see 6.41(1)).

(2 $\Leftarrow$) If G/Γ is not compact, then there is a nontrivial unipotent element u in Γ (see 6.34). Then 1 is an eigenvalue of $\rho(u)$ (indeed, it is the only eigenvalue of $\rho(u)$), so there is some nonzero $v \in \phi(L^3)$ with $uv = v$. Hence $(u - 1)v = 0$. Since $u \neq 1$ and $v \neq 0$, we conclude that $\phi(L^3)$ has a zero divisor.

Thus, it suffices to show that $D = \phi(L^3)$ is a division algebra. (That is, every nonzero element of D is invertible.) For convenience, define $N: L \rightarrow \mathbb{Q}$ by $N(t) = t\sigma(t)\sigma^2(t)$ (see Defn. 11.6). We know that $p \neq N(t)$, for all $t \in L$. It is easy to see that $N(t_1 t_2) = N(t_1)N(t_2)$.

Note that if $xyz = 0$, but $(x, y, z) \neq (0, 0, 0)$, then $\phi(x, y, z)$ is invertible. For example, if $z = 0$, then $\det \phi(x, y, z) = N(x) + pN(y)$. Since $p \neq N(-x/y) = -N(x)/N(y)$ (assuming $y \neq 0$), we have $\det \phi(x, y, z) \neq 0$, as desired. The other cases are similar.

For any $x, y, z \in L$, with $z \neq 0$, we have

$$\phi\left(1, -\frac{x}{p\sigma(z)}, 0\right) \phi(x, y, z) = \phi(0, *, *)$$

is invertible, so $\phi(x, y, z)$ is invertible.

(2 $\Rightarrow$) If $p = t\sigma(t)\sigma^2(t)$, for some $t \in L$, then one can show that $\phi(L^3) \cong \text{Mat}_{3 \times 3}(F)$ (cf. 11.10). From this, it is easy to see that $\phi(\mathcal{O}^3)$ contains unipotent elements. This implies that $\phi(\mathcal{O}^3)$ is not cocompact. $\square$

(7.49) **Example.** Let

- $\zeta = 2\cos(2\pi/7)$,
- $L = \mathbb{Q}[\zeta]$, and
- p be any prime that is congruent to either 3 or 5, modulo 7.

Then

- 1) L is a cubic, Galois extension of $\mathbb{Q}$; and
- 2) $p \neq t\sigma(t)\sigma^2(t)$, for all $t \in L$, and any generator σ of $\text{Gal}(L/\mathbb{Q})$.

To see this, let $\omega = e^{2\pi i/7}$ be a primitive 7th root of unity, so $\zeta = \omega + \omega^6$. Now it is well known that the Galois group of $\mathbb{Q}[\omega]$ is cyclic of order 6, generated by $\tau(\omega) = \omega^3$ (see I.48). So the fixed field L of τ^3 is a cyclic extension of degree $6/2 = 3$.

Now suppose $t\sigma(t)\sigma^2(t) = p$, for some $t \in L^\times$. Clearing denominators, we have $s\sigma(s)\sigma^2(s) = pm$, where

- $m \in \mathbb{Z}^+$;
- $s = a + b(\omega + \omega^6) + c(\omega + \omega^6)^2$, with $a, b, c \in \mathbb{Z}$ and $p \nmid \gcd(a, b, c)$.

Replacing ω with the variable x , we obtain integral polynomials $s_1(x), s_2(x), s_3(x)$, such that

$$s_1(x)s_2(x)s_3(x) = pm = 0 \text{ in } \frac{\mathbb{Z}_p[x]}{\langle x^6 + x^5 + \cdots + 1 \rangle}.$$

This implies that $x^6 + x^5 + \cdots + 1$ is *not* irreducible in $\mathbb{Z}_p[x]$. This contradicts the choice of p (see Exer. 7.32).

(7.50) **Remark.** The Kronecker-Weber Theorem (cf. Rem. 11.4) implies that all of the cubic, Galois extension fields L of $\mathbb{Q}$ can be constructed quite explicitly, in the manner of Eg. 7.49.

- Choose $n \in \mathbb{Z}^+$, such that $\varphi(n)$ is divisible by 3 (where

$$\varphi(n) = \#\{k \mid 1 \leq k \leq n, \gcd(k, n) = 1\}$$

is the Euler φ -function).

- Let $\omega = e^{2\pi i/n}$ be a primitive n^{th} root of unity.
- Let H be any subgroup of index 3 in the multiplicative group $(\mathbb{Z}_n)^\times$ of units modulo n .
- Let $\zeta = \sum_{k \in H} \omega^k = \sum_{k \in H} \cos(2\pi k/n)$.
- Let $L = \mathbb{Q}[\zeta]$.

In the proof of Prop. 7.47, we showed that $\phi(L^3)$ is a division algebra if $p \neq t\sigma(t)\sigma^2(t)$. Conversely, every central division algebra of degree 3 over $\mathbb{Q}$ arises from this construction (cf. 11.7), so we can restate the proposition in the following more abstract form.

(7.51) **Proposition.** *Let*

- L be a cubic, Galois extension of $\mathbb{Q}$,
- D be a central division algebra of degree 3 over $\mathbb{Q}$, such that D contains L as a subfield, and
- $\mathcal{O}$ be a vector-space lattice in D , such that $\mathcal{O}$ is also a subring of D (see 10.40).

Then there is an embedding $\phi: D \rightarrow \text{Mat}_{3 \times 3}(\mathbb{R})$, such that

- 1) $\phi(\text{SL}(1, D))$ is a $\mathbb{Q}$ -form of $\text{Mat}_{3 \times 3}(\mathbb{R})$; and
- 2) $\phi(\text{SL}(1, \mathcal{O}))$ is a cocompact, arithmetic lattice in $\text{SL}(3, \mathbb{R})$.

Furthermore, $\phi(\text{SL}(1, \mathcal{O}))$ is essentially independent of the choice of $\mathcal{O}$ or of the embedding ϕ . Namely, if $\mathcal{O}'$ and ϕ' are some other choices, then there is an automorphism α of $\text{SL}(3, \mathbb{R})$, such that $\alpha\phi'(\text{SL}(1, \mathcal{O}'))$ is commensurable with $\phi(\text{SL}(1, \mathcal{O}))$.

The classification results summarized in Fig. 10.2 (on p. 153) show that all cocompact lattices in $\text{SL}(3, \mathbb{R})$ can be obtained from these constructions. The proof is similar to Prop. 7.45.

(7.52) **Proposition.** *The lattices constructed in Props. 7.46 and 7.47 are the only cocompact lattices in $\text{SL}(3, \mathbb{R})$ (up to commensurability and conjugates).*

7G. Lattices in $\text{SL}(n, \mathbb{R})$

Let us briefly describe how the results for $\text{SL}(3, \mathbb{R})$ generalize to higher dimensions. (The group $\text{SL}(2, \mathbb{R})$ is an exceptional case that does not fit into this pattern.) The proofs are similar to those for $\text{SL}(3, \mathbb{R})$.

Proposition 7.51 generalizes in an obvious way to provide cocompact, arithmetic lattices in $\text{SL}(n, \mathbb{R})$. By replacing $\text{SL}(1, \mathcal{O})$ with the more general $\text{SL}(m, \mathcal{O})$, we also obtain lattices that are not cocompact (if n is composite).

(7.53) **Proposition.** *Let*

- D be a central division algebra of degree d over $\mathbb{Q}$, such that D splits over $\mathbb{R}$;
- $m \in \mathbb{Z}^+$; and
- $\mathcal{O}$ be vector-space lattice in D that is also a subring of D .

Then $\phi(\text{SL}(m, \mathcal{O}))$ is an arithmetic lattice in $\text{SL}(dm, \mathbb{R})$, for any embedding $\phi: D \rightarrow \text{Mat}_{d \times d}(\mathbb{R})$, such that $\phi(D)$ is a $\mathbb{Q}$ -form of $\text{Mat}_{d \times d}(\mathbb{R})$.

It is cocompact if and only if $m = 1$.

Let us state a version of Prop. 7.46 that utilizes a division algebra, rather than the totally real field F .

(7.54) **Proposition.** *Let*

- L be a real quadratic extension of $\mathbb{Q}$;
- D be a central simple division algebra of degree d over L ;
- τ be an antiinvolution of D , such that $\tau|_L$ is the Galois automorphism of L over F ;
- $b_1, \dots, b_m \in D^\times$, such that $\tau(b_j) = b_j$ for each j ;
- $\mathcal{O}$ be a vector-space lattice in D , such that $\mathcal{O}$ is a subring of D ; and
- $\Gamma = \text{SU}(\text{diag}(b_1, b_2, \dots, b_m); \mathcal{O}, \tau)$.

Then:

- 1) Γ is an arithmetic lattice in $\text{SL}(md, \mathbb{R})$.
- 2) Γ is cocompact if and only if

$$\tau(x^T) \text{diag}(b_1, b_2, \dots, b_m) x \neq 0$$

for all nonzero $x \in D^m$.

Additional examples of cocompact lattices can be obtained by generalizing Prop. 7.54 to allow L to be a totally real quadratic extension of a totally real algebraic number field F (as in Prop. 7.46). However, in this situation, one must then require $b_1, \dots, b_m$ to be chosen in such a way that $\mathrm{SU}(\mathrm{diag}(b_1, b_2, \dots, b_m); \mathcal{O}, \tau)^\sigma$ is compact, for every place σ of F , such that $\sigma \neq \mathrm{Id}$. For $n \geq 3$, every arithmetic lattice of $\mathrm{SL}(n, \mathbb{R})$ is obtained either from this unitary construction or from Prop. 7.53.

7H. Quaternion algebras over a field F

(7.55) **Definition** (cf. 3.23(2)).

- 1) For any field F , and any nonzero $\beta, \gamma \in F$, the corresponding *quaternion algebra* over F is the ring

$$D_{\beta, \gamma}(F) = \{ a + bi + cj + dk \mid a, b, c, d \in F \},$$

where

- addition is defined in the obvious way, and
- multiplication is determined by the relations

$$i^2 = \beta, \quad j^2 = \gamma, \quad ij = k = -ji,$$

together with the requirement that every element of F is in the center of D .

- 2) The *reduced norm* of $x = a + bi + cj + dk \in D_{\beta, \gamma}(F)$ is

$$N_{\mathrm{red}}(x) = a^2 - \beta b^2 - \gamma c^2 + \beta\gamma d^2.$$

(7.56) **Example.**

- 1) We have $D_{-1, -1}(\mathbb{R}) = \mathbb{H}$.
- 2) We have $D_{b^2\beta, c^2\gamma}(F) \cong D_{\beta, \gamma}(F)$ for any nonzero $b, c \in F$ (see Exer. 11:4).
- 3) We have $D_{b^2, \gamma}(F) \cong \mathrm{Mat}_{2 \times 2}(F)$, for any nonzero $b, \gamma \in F$ (see Exer. 11:5).
- 4) We have $N_{\mathrm{red}}(gh) = N_{\mathrm{red}}(g) \cdot N_{\mathrm{red}}(h)$ for $g, h \in D_{\beta, \gamma}(F)$.

(7.57) **Lemma.** We have $D_{\beta, \gamma}(\mathbb{C}) \cong \mathrm{Mat}_{2 \times 2}(\mathbb{C})$, for all $\beta, \gamma \in \mathbb{C}$, and

$$D_{\beta, -1}(\mathbb{R}) \cong \begin{cases} \mathrm{Mat}_{2 \times 2}(\mathbb{R}) & \text{if } \beta > 0, \\ \mathbb{H} & \text{if } \beta < 0. \end{cases}$$

Proof. The conclusions follow from the observations in Eg. 7.56. □

(7.58) **Definition.** Suppose $D_{\beta, \gamma}(F)$ is a quaternion algebra over a field F .

- 1) Define $\tau_r : D_{\beta, \gamma}(F) \rightarrow D_{\beta, \gamma}(F)$ by

$$\tau_r(a_0 + a_1i + a_2j + a_3k) = a_0 + a_1i - a_2j + a_3k.$$

This is the *reversion* on D .

- 2) For $B \in \mathrm{GL}(n, D)$, with $B^T = \tau_r(B)$, let

$$\mathrm{SU}(B; D, \tau_r) = \{ g \in \mathrm{SL}(n, D) \mid \tau_r(g^T)Bg = B \}.$$

7I. Notes

The construction of all arithmetic lattices in $\mathrm{SL}(2, \mathbb{R})$ is discussed (from the point of view of quaternion algebras) in [Kat, Chap. 5].

The original paper of Gromov and Piatetski-Shapiro [G-PS] on the construction of nonarithmetic lattices in $\mathrm{SO}(1, n)$ (§7D) is highly recommended. The exposition there is very understandable, especially for a reader with some knowledge of arithmetic groups and hyperbolic manifolds. A brief treatment also appears in [Mar5, App. C.2, pp. 362–364].

Should include history of nonarithmetic lattices in $\mathrm{SO}(1, n)$!!!

7J. References

- [G-PS] M. Gromov and I. Piatetski-Shapiro: Nonarithmetic groups in Lobachevsky spaces, *Publ. Math. Inst. Hautes Études Sci.* 66 (1988) 93–103. MR **89j**:22019
- [Kat] S. Katok: *Fuchsian Groups*, Univ. of Chicago, Chicago, 1992. MR **93d**:20088
- [Mar5] G. A. Margulis: *Discrete Subgroups of Semisimple Lie Groups*. Springer, Berlin Heidelberg New York, 1991.

Exercises

- 7:1) Suppose p is a prime, such that $x^2 + y^2 \equiv 0 \pmod{p}$ has only the trivial solution $x \equiv y \equiv 0 \pmod{p}$. (For example, p could be 3.) Show that $(0, 0, 0)$ is the only integer solution of the Diophantine equation $px^2 + py^2 = z^2$.
- 7:2) Let $F = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, and $a = b = \sqrt{2} + \sqrt{3} - 3$. Show
 - (a) F is a totally real extension of $\mathbb{Q}$,
 - (b) a is positive, and
 - (c) $\sigma(a)$ is negative, for every place $\sigma \neq \mathrm{Id}$.
- 7:3) For G , F , $\mathcal{O}$, a , and b as in Prop. 7.5, show:
 - (a) $G \cong \mathrm{SL}(2, \mathbb{R})$;
 - (b) $G_{\mathcal{O}}$ is an arithmetic lattice in G ;
 - (c) if $g \in D_{a,b}(F)$ with $N_{\mathrm{red}}(g) = 0$, then $g = 0$; and
 - (d) $G_{\mathcal{O}}$ is cocompact in G .
- 7:4) Let a and b be nonzero elements of a field F . Show that if there is a nonzero solution of the equation $w^2 - ax^2 - by^2 + abz^2 = 0$, then there is a nonzero solution of the equation $w^2 - ax^2 - by^2 = 0$. [*Hint*: By assumption, there is a nonzero element g of $D_{a,b}(F)$, such that $N_{\mathrm{red}}(g) = 0$. There is some nonzero $\alpha \in F + Fi$, such that the k -component of αg is zero.]
- 7:5) For $a, b \in \mathbb{R}$, the set

$$G = \{ g \in D_{a,b}(\mathbb{R}) \mid N_{\mathrm{red}}(g) = 1 \}$$
 is a submanifold of $D_{a,b}(\mathbb{R})$. Show that the tangent space $T_1 G$ is

$$\{ v \in D_{a,b}(\mathbb{R}) \mid \mathrm{Re} v = 0 \}.$$

[*Hint*: $T_1 G$ is the kernel of the derivative $d(N_{\mathrm{red}})_1$.]
- 7:6) Let σ be a real place of an algebraic number field F . Show that if a and b are elements of F , such that $\sigma(a)$ and $\sigma(b)$ are negative, then $(0, 0, 0)$ is the only solution in F^3 of the equation $ax^2 + by^2 = z^2$.
- 7:7) Carry out Part 2 of the proof of Prop. 7.6.

7:8) Suppose β and γ are real numbers, such that $\gamma < 0$ and $\beta > 0$. Show that there is an isomorphism $\phi: D_{\beta,\gamma}(\mathbb{R}) \rightarrow \text{Mat}_{2 \times 2}(\mathbb{R})$, such that:

- (a) $\phi(\tau_r(x)) = \phi(x)^T$, for all $x \in D_{\beta,\gamma}(\mathbb{R})$;
- (b) $\phi(x)$ is symmetric, for all $x \in D_{\beta,\gamma}(\mathbb{R})$, such that $\tau_r(x) = x$; and
- (c) if x is an invertible element of $D_{\beta,\gamma}(\mathbb{R})$, such that $\tau_r(x) = x$, then the number of positive eigenvalues of $\phi(x)$ is

$$\begin{cases} 1 & \text{if } a^2 > \beta(b^2 - \gamma d^2); \\ 0 & \text{if } a^2 < \beta(b^2 - \gamma d^2) \text{ and } a < 0; \\ 2 & \text{if } a^2 < \beta(b^2 - \gamma d^2) \text{ and } a > 0. \end{cases}$$

[Hint: Let $\phi(i) = \begin{bmatrix} \sqrt{\beta} & 0 \\ 0 & -\sqrt{\beta} \end{bmatrix}$ and $\phi(j) = \begin{bmatrix} 0 & \sqrt{|\gamma|} \\ -\sqrt{|\gamma|} & 0 \end{bmatrix}$.]

7:9) Suppose β and γ are nonzero real numbers, such that $\gamma > 0$, and let

$$w = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Show that there is an isomorphism $\phi: D_{\beta,\gamma}(\mathbb{R}) \rightarrow \text{Mat}_{2 \times 2}(\mathbb{R})$, such that:

- (a) $\phi(\tau_r(x)) = w\phi(x)^T w$, for all $x \in D_{\beta,\gamma}(\mathbb{R})$;
- (b) $\phi(x)w$ is symmetric, for all $x \in D_{\beta,\gamma}(\mathbb{R})$, such that $\tau_r(x) = x$; and
- (c) if x is an invertible element of $D_{\beta,\gamma}(\mathbb{R})$, such that $\tau_r(x) = x$, then the number of positive eigenvalues of $\phi(x)w$ is

$$\begin{cases} 1 & \text{if } a^2 > \beta(b^2 - \gamma d^2); \\ 0 & \text{if } a^2 < \beta(b^2 - \gamma d^2) \text{ and } (\beta + 1)b + (\beta - 1)d\sqrt{\gamma} > 0; \\ 2 & \text{if } a^2 < \beta(b^2 - \gamma d^2) > a^2 \text{ and } (\beta + 1)b + (\beta - 1)d\sqrt{\gamma} < 0. \end{cases}$$

[Hint: Let $\phi(i) = \begin{bmatrix} 0 & 1 \\ \beta & 0 \end{bmatrix}$ and $\phi(j) = \begin{bmatrix} \sqrt{\gamma} & 0 \\ 0 & -\sqrt{\gamma} \end{bmatrix}$.]

7:10) Show, for F , B , B' , Γ , and Γ' as in Prop. 7.14, that if there is some nonzero $\lambda \in F$ and some $g' \in \text{GL}(n+1, F)$, such that

$$B(g'x) = \lambda B'(x), \text{ for all } x \in F^{n+1},$$

then there exists $g \in \text{O}(n, 1)$, such that $g^{-1}\Gamma g$ is commensurable to Γ' .

7:11) Prove Prop. 7.23.

7:12) Show that if Γ_1 and Γ_2 are torsion-free lattices in $\text{PO}(1, n)$, such that $\Gamma_1 \backslash \mathfrak{H}^n$ is isometric to $\Gamma_2 \backslash \mathfrak{H}^n$, then Γ_1 is conjugate to Γ_2 . [Hint: Any isometry $\phi: \Gamma_1 \backslash \mathfrak{H}^n \rightarrow \Gamma_2 \backslash \mathfrak{H}^n$ lifts to an isometry of $\mathfrak{H}^n$.]

7:13) Let C be a closed, connected hypersurface in an orientable Riemannian manifold M , and let M' be the manifold with boundary that results from cutting M open, by slicing along C . Show:

- (a) If C is orientable, then the boundary of M is two copies of C .
- (b) If C is not orientable, then the boundary is the orientable double cover of C .
- (c) If C is isometric to a closed, connected hypersurface C_0 in an orientable Riemannian manifold M_0 , and M'_0 is the manifold with boundary that results from cutting M_0 open, by slicing along C_0 , then the boundary of M' is isometric to the boundary of M'_0 .

- 7:14) For M_1 , M_2 , and f as in Prop. 7:14, show that if $p \in \partial M'_1$, then p has a neighborhood U in $M'_1 \cup_f M'_2$, such that U is isometric to an open subset of $\mathfrak{H}^n$. [Hint: Find an open ball V around a point x in $\mathfrak{H}^{n-1}$, and isometries $g_1: U_1 \rightarrow V^+$ and $g_2: U_2 \rightarrow V^-$, where U_j is a neighborhood of p in M'_j , such that $g_1|_{\partial M'_1} = (g_2 \circ f)|_{\partial M'_1}$.]
- 7:15) Show that the map $\phi: \Gamma_0 \backslash \mathfrak{H}^{n-1} \rightarrow \Gamma \backslash \mathfrak{H}^n$, defined in the proof of Lem. 7.31, is injective. [Hint: Suppose $\gamma x = y$, for some $\gamma \in \Gamma$ and $x, y \in \mathfrak{H}^{n-1}$. Then $\gamma^{-1}\tau\gamma\tau$ is an element of Γ' that fixes x , so it is trivial. Hence, the fixed-point set of τ is γ -invariant.]
- 7:16) Assume n is odd, and construct a cocompact, nonarithmetic lattice Γ in $\mathrm{SO}(1, n)$. [Hint: Let $F = \mathbb{Q}[\sqrt{2}]$, define quadratic forms $B_1(x) = \sqrt{2}x_1^2 - x_2^2 - x_3^2 - \cdots - x_n^2 - x_{n+1}^2$ and $B_2(x) = \sqrt{2}x_1^2 - x_2^2 - x_3^2 - \cdots - x_n^2 - 3x_{n+1}^2$ on F^{n+1} , and use the proof of Cor. 7.35.]
- 7:17) In the notation of the proof of Cor. 7.35, assume that $M_1 \setminus C_1$ and $M_2 \setminus C_2$ are *not* connected; let M'_j be the closure of a component of $M_j \setminus C_j$. Show that if $f': C_1 \rightarrow C_j$ is any isometry (and n is odd), then $M'_1 \cup_{f'} M'_2$ is a *nonarithmetic* hyperbolic n -manifold of finite volume.
- 7:18) Eliminate the assumption that $M_1 \setminus C_1$ and $M_2 \setminus C_2$ are connected from the proof of Cor. 7.35. [Hint: Define $B_3(x) = x_1^2 - x_2^2 - x_3^2 - \cdots - x_n^2 - 3x_{n+1}^2$. If $M_j \setminus C_j$ has the same number of components as $M_k \setminus C_k$ (and $j \neq k$), then either Exer. 7:17 or the proof of Cor. 7.35 applies.]
- 7:19) For $B_1(x)$ and $B_2(x)$ as in the proof of Cor. 7.35, show that there are finite-index subgroups Γ_1 and Γ_2 of $\mathrm{SO}(B_1; \mathbb{Z})$ and $\mathrm{SO}(B_2; \mathbb{Z})$, respectively, such that
 (a) Γ_1 and Γ_2 are torsion free; and
 (b) $\Gamma_1 \cap \mathrm{SO}(1, n-1) = \Gamma_2 \cap \mathrm{SO}(1, n-1)$.
 [Hint: Let $\Gamma_j = \Lambda \cap \mathrm{SO}(B_j; \mathbb{Z})$, where Λ is a torsion-free subgroup of finite index in $\mathrm{SL}(n+1, \mathbb{Z})$.]
- 7:20) In the notation of the proof of Cor. 7.35, show that if n is even (and $n \geq 4$), then Γ_{non} is not arithmetic. [Hint: If Γ_{non} is arithmetic, then its intersection with $\mathrm{SO}(1, n-1)$ is arithmetic in $\mathrm{SO}(1, n-1)$, and $n-1$ is odd.]
- 7:21) Derive Thm. 7.33 as a corollary of Thm. 7.38. [Hint: Apply Thm. 7.38 to $\widetilde{M}_j = M_j \#_{f_j} M_j$, where $f_j: C_j \rightarrow C_j$ is the identity map. Note that $\widetilde{M}_j$ is a double cover of M_j , so $\widetilde{M}_j$ is commensurable to M_j .]
- 7:22) For Γ and V as in the proof of Thm. 7.38, let $\check{V}$ be the interior of V , and show, for each $\gamma \in \Gamma$, that if $\gamma\check{V} \cap \check{V} \neq \emptyset$, then $\gamma\check{V} = \check{V}$.
- 7:23) Show that if H is a connected subgroup of $\mathrm{PO}(1, n)$ that contains $\mathrm{PO}(1, n-1)^\circ$, then $H = \mathrm{PO}(1, n-1)^\circ$.
- 7:24) Eliminate the assumption that $\partial M'_1$ is compact from Case 2 of the proof of Thm. 7.38. [Hint: The original proof applies unless $\mathrm{dist}(H_1, H_2) = 0$, which would mean that H_1 and H_2 intersect at infinity. This intersection is a single point, and it is invariant under Γ' , which contradicts the Zariski density of Γ' .]
- 7:25) For U_1 , ρ , and $V_{\mathbb{Q}}$ as in the proof of 7.41(1), show that $\rho(U_1)V_{\mathbb{Q}} \subset V_{\mathbb{Q}}$.
- 7:26) In the notation of the proof of Prop. 7.41, find a dense subgroup U_2 of

$$\begin{bmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{bmatrix},$$

such that $\rho(U_2) \subset \rho(\mathrm{SL}(3, \mathbb{R}))_{\mathbb{Q}}$.

- 7:27) Assume the notation of the proof of Prop. 7.41, and let $G = \rho(\mathrm{SL}(3, \mathbb{R}))$.
- (a) Show that G is *quasisplit*. That is, show that some Borel subgroup of G is defined over $\mathbb{Q}$.
 - (b) Show that every proper parabolic $\mathbb{Q}$ -subgroup of G is a Borel subgroup of G .
[Hint: Let B be the group of upper-triangular matrices in $\mathrm{SL}(3, \mathbb{R})$. Then B is a Borel subgroup of $\mathrm{SL}(3, \mathbb{R})$, and $\rho(B)$ is defined over $\mathbb{Q}$.]
- 7:28) Suppose Γ_1 and Γ_2 are noncocompact lattices in $\mathrm{SL}(3, \mathbb{R})$ that correspond to two different values of r , say r_1 and r_2 . Show that Γ_1 is not commensurable to any conjugate of Γ_2 .
[Hint: There is a diagonal matrix in Γ_1 whose trace is not in $\mathbb{Z}[\sqrt{r_2}]$.]
- 7:29) Show that if L is a Galois extension of $\mathbb{Q}$, such that $|L : \mathbb{Q}|$ is odd, then $L \subset \mathbb{R}$.
- 7:30) Assume the notation of the proof of Prop. 7.47. For $h \in L^3$, define $T_h \in \mathrm{End}_{\mathbb{R}}(\mathrm{Mat}_{3 \times 3}(\mathbb{R}))$ by $T_h(v) = \phi(h)v$.
- (a) Show that $\phi(h) \in \mathrm{End}_{\mathbb{R}}(\mathrm{Mat}_{3 \times 3}(\mathbb{R}))_{\mathbb{Q}}$. (This is the $\mathbb{Q}$ -form on $\mathrm{End}_{\mathbb{R}}(\mathrm{Mat}_{3 \times 3}(\mathbb{R}))$ corresponding to the $\mathbb{Q}$ -form $\phi(L^3)$ on $\mathrm{Mat}_{3 \times 3}(\mathbb{R})$.)
 - (b) Show that $\rho(\mathrm{Mat}_{3 \times 3}(\mathbb{R}))$ is the centralizer of $\{T_h \mid h \in L^3\}$.
 - (c) Show that $\rho(\mathrm{SL}(3, \mathbb{R}))$ is defined over $\mathbb{Q}$.
- 7:31) In the notation of Prop. 7.47, show that if $p = t\sigma(t)\sigma^2(t)$, then $\phi(L^3)$ is not a division algebra. *[Hint: $\phi(1, 1/t, 1/(t\sigma(t)))$ is not invertible.]*
- 7:32) Let
- p and q be distinct primes, and
 - $f(x) = x^{q-1} + \cdots + x + 1$.
- Show that $f(x)$ is reducible over $\mathbb{Z}_p$ if and only if there exists $r \in \{1, 2, \dots, q-2\}$, such that $p^r \equiv 1 \pmod{q}$. *[Hint: Let $g(x)$ be an irreducible factor of $f(x)$, and let $r = \deg g(x) < q-1$. Then $f(x)$ has a root α in a finite field F of order p^r . Since α is an element of order q in $F^\times$, we must have $q \mid \#F^\times$.]*

Real Rank

(8.1) **Assumption.** Assume that G is a closed subgroup of $\mathrm{SL}(\ell, \mathbb{R})$, for some ℓ . (The definitions and results of this chapter are independent of the particular embedding chosen.)

8A. $\mathbb{R}$ -split tori

(8.2) **Definition.** A closed, connected subgroup T of G is a *torus* if T is diagonalizable over $\mathbb{C}$; that is, if there exists $g \in \mathrm{GL}(n, \mathbb{C})$, such that $g^{-1}Tg$ consists entirely of diagonal matrices.

We will usually also assume that T is almost Zariski closed (see 4.6).

Because commuting diagonalizable matrices can be simultaneously diagonalized, we have the following:

(8.3) **Proposition.** *A subgroup T of G is a torus if and only if*

- *T is closed and connected,*
- *T is abelian, and*
- *every element of T is semisimple.*

(8.4) **Example.**

- $T = \mathrm{SO}(2)$ is a torus in $\mathrm{SL}(2, \mathbb{R})$ (see Exer. 8:1). It is clear that T is closed, connected, and abelian. Since every element of T is a normal linear transformation (that is, commutes with its transpose), we know from elementary linear algebra that every element of T is diagonalizable.
- Generalizing the preceding, we see that $T = \mathrm{SO}(2)^n$ is a torus in $\mathrm{SL}(2n, \mathbb{R})$. Note that T is homeomorphic to the n -torus $\mathbb{T}^n$. (In fact, any compact torus subgroup is homeomorphic to a topological torus.) This is the motivation for the term *torus*.
- Let T be the identity component of the group of diagonal matrices in $\mathrm{SL}(n, \mathbb{R})$. Then T is obviously a torus. However, it is homeomorphic to $\mathbb{R}^{n-1}$, so it is not a torus in the usual topological sense.
- The hypothesis that T is abelian cannot be omitted from Prop. 8.3. For example, every element of $\mathrm{SO}(n)$ is semisimple, but $\mathrm{SO}(n)$ is not abelian if $n \geq 3$.

(8.5) **Definition.** A torus T in G is *$\mathbb{R}$ -split* if T is diagonalizable over $\mathbb{R}$; that is, if there exists $g \in \mathrm{GL}(n, \mathbb{R})$, such that $g^{-1}Tg$ consists entirely of diagonal matrices.

(8.6) **Warning.** An $\mathbb{R}$ -split torus is *never* homeomorphic to $\mathbb{T}^n$ (except in the trivial case $n = 0$).

Recall that an element of G is *hyperbolic* if it is diagonalizable over $\mathbb{R}$ (see 4.11). In this terminology, we have the following analogue of Prop. 8.3.

(8.7) **Proposition.** *A subgroup T of G is an $\mathbb{R}$ -split torus if and only if*

- T is closed and connected,
- T is abelian, and
- every element of T is hyperbolic.

(8.8) **Example.** Although $\mathrm{SO}(2)$ is a torus in $\mathrm{SL}(2, \mathbb{R})$, it is *not* $\mathbb{R}$ -split. Namely, the eigenvalues of

$$g = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix} \in \mathrm{SO}(2)$$

are $\cos \theta \pm i \sin \theta$, which are (usually) not real, so g is not diagonalizable over $\mathbb{R}$.

8B. Definition of real rank

(8.9) **Definition.** $\mathbb{R}\text{-rank}(G)$ is the dimension of any maximal $\mathbb{R}$ -split torus of G . (This does not depend on the choice of the maximal torus, because all maximal $\mathbb{R}$ -split tori of G are conjugate.)

(8.10) **Example.**

- 1) $\mathbb{R}\text{-rank}(\mathrm{SL}(n, \mathbb{R})) = n - 1$. (Let T be the identity component of the group of all diagonal matrices in $\mathrm{SL}(n, \mathbb{R})$.)
- 2) We have $\mathbb{R}\text{-rank}(\mathrm{SL}(n, \mathbb{C})) = \mathbb{R}\text{-rank}(\mathrm{SL}(n, \mathbb{H})) = 1$. This is because only the *real* diagonal matrices in $\mathrm{SL}(n, \mathbb{C})$ remain diagonal when $\mathrm{SL}(n, \mathbb{C})$ is embedded in $\mathrm{SL}(2n, \mathbb{C})$.
- 3) Since $\mathrm{SO}(1, 1) \subset \mathrm{SL}(2, \mathbb{R})$, we have

$$\mathbb{R}\text{-rank}(\mathrm{SO}(1, 1)) \leq \mathbb{R}\text{-rank}(\mathrm{SL}(2, \mathbb{R})) = 1.$$

Let us show that equality holds.

Recall that $\cosh t = (e^t + e^{-t})/2$ and $\sinh t = (e^t - e^{-t})/2$, and let

$$T = \left\{ \begin{bmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{bmatrix} \mid t \in \mathbb{R} \right\}.$$

An easy calculation (using the fact that $\cosh^2 t - \sinh^2 t = 1$) shows that $T \subset \mathrm{SO}(1, 1)$. Another easy calculation shows that T is a (closed, connected) subgroup of $\mathrm{SO}(1, 1)$. Thus, T is a torus.

Since every element of T is symmetric, a theorem of linear algebra implies that every element of T is diagonalizable over $\mathbb{R}$; thus, T is $\mathbb{R}$ -split (see Exer. 8:3). Hence

$$\mathbb{R}\text{-rank}(\mathrm{SO}(1, 1)) \geq \dim T = 1,$$

as desired.

- 4) Suppose T is a nontrivial $\mathbb{R}$ -split torus in $\mathrm{SO}(m, n)$. Because T is diagonalizable, there is a basis of $\mathbb{R}^{m+n}$ that consists entirely of eigenvectors. Then, since T is nontrivial, we conclude that there is some $a \in T$ and some nonzero $v \in \mathbb{R}^{m+n}$, and some $\lambda > 1$, such that $av = \lambda v$. Since a preserves the form $\langle \cdot \mid \cdot \rangle_{\mathbb{R}^{m,n}}$, we have

$$\langle v \mid v \rangle_{\mathbb{R}^{m,n}} = \langle a^{-k}v \mid a^{-k}v \rangle_{\mathbb{R}^{m,n}} = \langle \lambda^{-k}v \mid \lambda^{-k}v \rangle_{\mathbb{R}^{m,n}} = \lambda^{-2k} \langle v \mid v \rangle_{\mathbb{R}^{m,n}} \rightarrow 0$$

as $k \rightarrow \infty$. Since $\langle v | v \rangle_{\mathbb{R}^{m,n}}$ is independent of k , we conclude that

$$\langle v | v \rangle_{\mathbb{R}^{m,n}} = 0;$$

that is, v is an *isotropic* vector.

Thus, the existence of a nontrivial $\mathbb{R}$ -split torus implies the existence of a nontrivial isotropic vector. In particular, since the usual inner product on $\mathbb{R}^n$ has no isotropic vectors, we conclude that $\mathbb{R}\text{-rank}(\text{SO}(n)) = 0$.

(8.11) **Proposition.** $\mathbb{R}\text{-rank}(\text{SO}(m, n)) = \min\{m, n\}$.

Proof. *Step 1.* We have $\mathbb{R}\text{-rank}(\text{SO}(m, n)) \geq \min\{m, n\}$. We may assume $m \leq n$. Let

$$G = \text{Isom}(x_1^2 - x_2^2 + x_3^2 - x_4^2 \pm \cdots + x_{2m-1}^2 - x_{2m}^2 + x_{2m+1}^2 + x_{2m+2}^2 + \cdots + x_{m+n}^2)^\circ.$$

Then G is isomorphic to $\text{SO}(m, n)^\circ$. (Indeed, G is conjugate to $\text{SO}(m, n)^\circ$, simply by permuting the basis vectors.) Therefore, $\mathbb{R}\text{-rank}(G) = \mathbb{R}\text{-rank}(\text{SO}(m, n))$. There is an obvious embedding of $\text{SO}(1, 1)^m$ in G :

$$\left[\begin{array}{ccccccc} \text{SO}(1, 1) & & & & & & \\ & \text{SO}(1, 1) & & & & & \\ & & \ddots & & & & \\ & & & \text{SO}(1, 1) & & & \\ & & & & \text{Id}_{n-m, n-m} & & \end{array} \right]^\circ \subset G,$$

so

$$\mathbb{R}\text{-rank}(G) \geq m \cdot \mathbb{R}\text{-rank}(\text{SO}(1, 1)) = m \cdot 1 = m.$$

Step 2. We have $\mathbb{R}\text{-rank}(G) \leq \min\{m, n\}$. By making the argument of Eg. 8.10(4) more precise, one shows that the existence of a large $\mathbb{R}$ -split torus implies the existence of a large collection of isotropic vectors, indeed, an entire *totally isotropic subspace*; that is, a subspace W , such that $\langle v | w \rangle_{\mathbb{R}^{m,n}} = 0$ for all $v, w \in \mathbb{R}^{m+n}$. More precisely, there is totally isotropic subspace whose dimension is $\mathbb{R}\text{-rank}(G)$. [Probably should prove this!!!] Since $\min\{m, n\}$ is the maximum dimension of a totally isotropic subspace of $\mathbb{R}^{m+n}$, the desired conclusion follows. $\square$

(8.12) **Remark.** In geometric terms, the real rank of $\text{SO}(m, n)$ is the dimension of a maximal totally isotropic subspace of $\mathbb{R}^{m+n}$. A similar result holds for other classical groups. More concretely, we have

$$\mathbb{R}\text{-rank} \text{SO}(m, n) = \mathbb{R}\text{-rank} \text{SU}(m, n) = \mathbb{R}\text{-rank} \text{Sp}(m, n) = \min\{m, n\}.$$

(8.13) **Lemma.**

$$\mathbb{R}\text{-rank}(G_1 \times G_2 \times \cdots \times G_r) = \mathbb{R}\text{-rank}(G_1) + \mathbb{R}\text{-rank}(G_2) + \cdots + \mathbb{R}\text{-rank}(G_r).$$

8C. Relation to geometry

The following theorem describes a natural one-to-one correspondence between the maximal $\mathbb{R}$ -split tori of G and the maximal flats in X . This provides the connection between the algebraic definition of real rank and the geometric material of §2A.

(8.14) **Example.** Let G be the identity component of the group of diagonal matrices in $G = \text{SL}(2, \mathbb{R})$. As usual, G acts on $\mathfrak{H}^2$ by linear-fractional transformations. Note that the T -orbit $Ti = \mathbb{R}^+i$ is a geodesic in $\mathfrak{H}^2$. Because G is transitive on the set of geodesics, any other geodesic in $\mathfrak{H}^2$ is of the form $(gTg^{-1})(gi)$, for some $g \in G$. Note that gTg^{-1} , being conjugate to T , is a

maximal $\mathbb{R}$ -split torus of G . Thus, each geodesic in $\mathfrak{H}^2$ corresponds to an $\mathbb{R}$ -split torus in G . The following theorem generalizes this observation to all symmetric spaces of noncompact type.

(8.15) **Definition.** A group T acts *simply transitively* on a set F if, for all $f_1, f_2 \in F$, there is a unique $t \in T$, such that $tf_1 = f_2$.

(8.16) **Theorem.** Assume G has no compact factors (or, equivalently, that X is of noncompact type). For every flat F in X , there is a unique $\mathbb{R}$ -split torus T of G , such that $TF = F$. Furthermore, T acts simply transitively on F .

Conversely, for every $\mathbb{R}$ -split torus T of G , there is a flat F in X , such that $TF = F$, and T acts simply transitively on F . Furthermore, if the $\mathbb{R}$ -split torus T is maximal, then the corresponding flat H is unique.

(8.17) **Remark.** Note that $\mathbb{R}^{\ell-1}$ acts simply transitively on $\{p\} \times \mathbb{R}^{\ell-1}$, for every $p \in \mathbb{R}$. Thus, if T is an $\mathbb{R}$ -split torus of G that is *not* maximal, then T acts simply transitively on uncountably many flats of X .

8D. Parabolic subgroups

If G is a classical group, then, from the description of parabolic subgroups as stabilizers of flags (see 4.33), it is easy to see that G has only finitely many conjugacy classes of parabolic subgroups. More precisely, it is easy to verify the following result for classical groups. (The general case is obtained from the theory of real roots.)

(8.18) **Theorem.** G has only finitely many conjugacy classes of parabolic subgroups.

More precisely, the number of conjugacy classes is 2^r , where $r = \mathbb{R}\text{-rank}(G)$.

(8.19) **Corollary.** G has a proper parabolic subgroup if and only if $\mathbb{R}\text{-rank}(G) \neq 0$.

8E. Groups of real rank zero

The following observations describe several characterizations of the groups of real rank zero (see Exer. 8:5).

(8.20) **Proposition.** The following are equivalent:

- 1) $\mathbb{R}\text{-rank}(G) = 0$;
- 2) G is compact;
- 3) every element of G is elliptic;
- 4) G has no nontrivial unipotent elements;
- 5) G does not contain a subgroup isogenous to $\text{SL}(2, \mathbb{R})$.

(8.21) **Corollary.** G is generated by unipotent elements if and only if G has no compact factors.

Here is an explicit list of the compact, connected, simple Lie groups.

(8.22) **Theorem.** Every compact, connected, simple Lie group is isogenous to either

- $\text{SO}(n)$ for some $n \geq 3$, with $n \neq 4$,
- $\text{SU}(n)$ for some $n \geq 2$,
- $\text{Sp}(n)$ for some $n \geq 1$, or
- one of the five compact exceptional groups (the compact forms of E_6 , E_7 , E_8 , F_4 and G_2).

(8.23) **Remark.** There are some redundancies in the list of Thm. 8.22 (see Rem. 3.31):

- 1) $\mathrm{Sp}(1)$ and $\mathrm{SU}(2)$ are isogenous to $\mathrm{SO}(3)$;
- 2) $\mathrm{Sp}(4)$ is isogenous to $\mathrm{SO}(5)$;
- 3) $\mathrm{SU}(4)$ is isogenous to $\mathrm{SO}(6)$.

The groups $\mathrm{SO}(1)$ and $\mathrm{SU}(1)$ are trivial. Also, $\mathrm{SO}(2) \cong \mathbb{T}$ is abelian and $\mathrm{SO}(4)$ is isogenous to $\mathrm{SO}(3) \times \mathrm{SO}(3)$, so they are not simple. Thus, these groups do not appear in the list.

(8.24) **Corollary.** $\mathbb{R}\text{-rank}(G) = 0$ if and only if G is isogenous to a direct product of groups listed in Theorem 8.22.

8F. Groups of real rank one

Here is an explicit list of the simple groups of real rank one.

(8.25) **Theorem.** Every simple Lie group of real rank one is isogenous to either

- $\mathrm{SO}(1, n)$ for some $n \geq 2$,
- $\mathrm{SU}(1, n)$ for some $n \geq 2$,
- $\mathrm{Sp}(1, n)$ for some $n \geq 2$, or
- a certain exceptional group, often denoted F_4^{-20} , and also known as $F_{4,1}$ (the form of F_4 that has real rank one).

(8.26) **Remark.** The special linear groups $\mathrm{SL}(2, \mathbb{R})$, $\mathrm{SL}(2, \mathbb{C})$ and $\mathrm{SL}(2, \mathbb{H})$ have real rank one, but they do not need to be listed explicitly, because

- $\mathrm{SL}(2, \mathbb{R})$ is isogenous to $\mathrm{SO}(1, 2)$ and $\mathrm{SU}(1, 1)$;
- $\mathrm{SL}(2, \mathbb{C})$ is isogenous to $\mathrm{SO}(1, 3)$ and $\mathrm{Sp}(1, 1)$; and
- $\mathrm{SL}(2, \mathbb{H})$ is isogenous to $\mathrm{SO}(1, 4)$.

(8.27) **Corollary.** $\mathbb{R}\text{-rank}(G) = 1$ if and only if G is isogenous to a direct product $G_0 \times G_1$, where

- G_0 is compact and
- G_1 is of one of the groups listed in Theorem 8.25.

Recall that $\mathrm{PSO}(1, n)^\circ = \mathrm{Isom}(\mathfrak{H}^n)^\circ$. Similarly, up to finite index,

- $\mathrm{PSU}(1, n)$ is the isometry group of complex hyperbolic space,
- $\mathrm{PSp}(1, n)$ is the isometry group of quaternionic hyperbolic space, and
- $F_{4,1}$ is the isometry group of the hyperbolic plane over the Cayley octonions $\mathbb{O}$. (Because $\mathbb{O}$ is not associative, it is not possible to define octonionic hyperbolic spaces of higher dimension, only the hyperbolic plane.)

Thus, Cor. 8.25 can be reformulated in the following geometric terms.

(8.28) **Corollary.** Let X be a symmetric space of noncompact type, and let $G = \mathrm{Isom}(X)^\circ$. We have $\mathbb{R}\text{-rank}(G) = 1$ if and only if either

- 1) for some $n \geq 2$, X is isometric to the n -dimensional hyperbolic space over either the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the quaternions $\mathbb{H}$, or the Cayley octonions $\mathbb{O}$ (furthermore, for $\mathbb{O}$, we must have $n = 2$); or
- 2) X is isometric to the product of a compact symmetric space with one of the hyperbolic spaces listed in (1).

We know that if $\mathbb{R}\text{-rank}(G) = 0$, then G has no unipotent elements (see 8.20(4)), and no parabolic subgroups (see 8.19). We now show that if $\mathbb{R}\text{-rank}(G) = 1$, then G has very few unipotent subgroups, and essentially only one parabolic subgroup. This can be verified directly for the classical groups, and follows from Thms. 4.39 and 4.43 in the general case. [Should prove part of this, for illustration!!!]

(8.29) **Theorem.** *The following are equivalent:*

- 1) $\mathbb{R}\text{-rank}(G) \leq 1$;
- 2) *any two maximal unipotent subgroups of G either are equal or are disjoint;*
- 3) *$C_G(a)/\langle a \rangle$ is compact, for every nontrivial hyperbolic element a of G ;*
- 4) *for every maximal unipotent subgroup U , there is a compact subgroup $E \subset N_G(U)$, such that $C_G(u) \subset EU$, for every nontrivial $u \in U$;*
- 5) *all proper parabolic subgroups of G are conjugate to each other.*

We now explain how parabolic subgroups are related to the large-scale geometry of X , when X is irreducible and $\mathbb{R}\text{-rank}(G) = 1$. Namely, the set of (proper) parabolic subgroups is in natural one-to-one correspondence with the points of ∂X , the boundary at ∞ of X . (Note that, because the proper parabolic subgroups of G are all conjugate, the set of proper parabolic subgroups can naturally be identified with G/P , for any specified proper parabolic subgroup P .)

(8.30) **Definition.** The *boundary* ∂X of X (or the *sphere at ∞* of X) is the set of equivalence classes of all geodesic rays in X , where two geodesic rays $\{x_t\}_{t=0}^\infty$ and $\{y_t\}_{t=0}^\infty$ are *equivalent* if they stay within a bounded distance of each other (more precisely, if $\sup_{t \in \mathbb{R}^+} d(x_t, y_t) < \infty$). We assume here that the geodesics are parametrized by arc length.

(8.31) **Theorem.** *Assume $X = G/K$ is a noncompact, irreducible symmetric space that is not flat. If $\mathbb{R}\text{-rank}(G) = 1$, then there is a natural identification of ∂X with G/P , for any proper parabolic subgroup P of G .*

Proof. Because G acts transitively on the space of unit tangent vectors of X (see 2.7), we see that G acts transitively on the space of all geodesic rays in X . Therefore, G acts transitively on ∂X . We wish to show, for any $p \in \partial X$, that $\text{Stab}_G(p)$ is parabolic in G .

Let $\{x_t\}_{t=0}^\infty$ be a geodesic ray, and let $x = x_0$ be the initial point of this ray. From Theorem 8.16, we know that there is an $\mathbb{R}$ -split torus T of G , such that T acts simply transitively on the flat $\{x_t\}_{t=-\infty}^\infty$. Because $\mathbb{R}\text{-rank}(G) = 1$, we know that T is a one-parameter subgroup of G ; write $T = \{a^t\}_{t=-\infty}^\infty$. Then $\{x_t\}_{t=0}^\infty = \{a^t x_0\}_{t=0}^\infty$. Let

$$P = \left\{ g \in G \mid \sup_{t \in \mathbb{R}^+} \|a^{-t} g a^t\| < \infty \right\},$$

so P is a parabolic subgroup of G .

Note that, for $x, y \in G$, we have $d_X(xK, yK) = \log \|y^{-1}x\|$, for an appropriate choice of the matrix norm $\|\cdot\|$. Thus, for any $g \in G$, we have

$$d(gx_t, x_t) = d(ga^t x_0, a^t x_0) = \|(a^t x_0)^{-1} (ga^t x_0)\| = \|x_0^{-1} (a^{-t} g a^t) x_0\| \asymp \|a^{-t} g a^t\|$$

(because x_0 is constant—*independent of t*). Thus, we see that $g\{x_t\}_{t=0}^\infty$ is equivalent to $\{x_t\}_{t=0}^\infty$ if and only if $g \in P$, as desired. $\square$

8G. Groups of higher real rank

In some situations, one has a certain subset S of G , and one can prove that the centralizer of each element of S is well-behaved. One would then like to know that these centralizers generate G , to prove that every element of G is well-behaved. The following theorem shows, in many cases, that an assumption on $\mathbb{R}\text{-rank}(G)$ is exactly what is needed to make this true.

(8.32) **Theorem.** *Assume G is not compact. The following are equivalent:*

- 1) $\mathbb{R}\text{-rank}(G) \geq 2$;
- 2) *if T is any maximal $\mathbb{R}$ -split torus of G , then there exist nontrivial elements a_1 and a_2 of T , such that $G = \langle C_G(a_1), C_G(a_2) \rangle$;*
- 3) *for every pair of nontrivial unipotent subgroups U and V of G , there is a finite sequence $U_0, \dots, U_r$ of nontrivial unipotent subgroups of G , such that $U_0 = U$, $U_r = V$, and $[U_i, U_{i-1}] = e$ for $i = 1, \dots, r$;*
- 4) *there is a finite sequence $U_0, \dots, U_r$ of nontrivial unipotent subgroups of G , such that $[U_i, U_{i-1}] = e$ for $i = 1, \dots, r$, and $\langle U_0, \dots, U_r \rangle = G$;*
- 5) *there exists a nontrivial hyperbolic element a and a nontrivial unipotent element u , such that $au = ua$.*

Proof. Assume, for simplicity, that $G = \text{SL}(3, \mathbb{R})$. (See Rem. 8.34 for a general proof, using the theory of real roots.)

(2) Assume T is the group of diagonal matrices. Let

$$a_1 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1/4 \end{bmatrix} \quad \text{and} \quad a_2 = \begin{bmatrix} 1/4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Then

$$C_G(a_1) = \begin{bmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{bmatrix} \quad \text{and} \quad C_G(a_2) = \begin{bmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{bmatrix}.$$

These generate G .

(3) If $U \cap V \neq \{e\}$, then an appropriate sequence is

$$U, Z(U), U \cap V, Z(V), V.$$

Thus, we may assume $U \cap V = \{e\}$. Furthermore, we may assume that U and V are maximal unipotent subgroups. Thus, replacing the pair (U, V) with a conjugate under $\text{SL}(3, \mathbb{R})$, we may assume

$$U = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{bmatrix}.$$

We may now take the sequence

$$\begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ * & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{bmatrix}.$$

(4) This follows from (3).

(5) This follows from (2). □

(8.33) **Remark.** We assume G is not compact in Thm. 8.32 only because (3) is vacuously true for compact groups.

(8.34) **Remark.** The above proof of Thm. 8.32 in the special case where $G = \mathrm{SL}(3, \mathbb{R})$ can be generalized to any group of real rank at least two, by using the theory of real roots (see Chap. 18). For simplicity, assume $\mathbb{R}\text{-rank}(G) = 2$. Let Φ be the set of real roots of G , and let $\{\alpha_1, \alpha_2\}$ be a basis for Φ .

(2) Take $a_i \in \ker(\alpha_i)$ for $i = 1, 2$. Then $U_{\pm\alpha_i} \subset C_G(a_i)$, and we have $\langle U_{\alpha_1}, U_{-\alpha_1}, U_{\alpha_2}, U_{-\alpha_2} \rangle = G$.

(3) We may assume U and V are disjoint maximal unipotent subgroups of G . Then, replacing the pair (U, V) by a conjugate, we may assume that

$$U = \langle U_\phi \mid \phi \in \Phi^+ \rangle \quad \text{and} \quad U = \langle U_{-\phi} \mid \phi \in \Phi^+ \rangle.$$

Since $\alpha_1 - \alpha_2$ is neither positive nor negative, it is not a root, so $[U_{\alpha_1}, U_{-\alpha_2}] = e$. Thus, we may take the sequence

$$U, Z(U), U_{\alpha_1}, U_{-\alpha_2}, Z(V), V.$$

Proposition 8.20 implies that, up to isogeny, $\mathrm{SL}(2, \mathbb{R})$ is the unique minimal group of real rank one. For real rank two, there are two minimal groups, and one is not simple.

(8.35) **Theorem.**

- 1) $\mathbb{R}\text{-rank}(G) \geq 2$ if and only if G contains a subgroup isogenous to either $\mathrm{SL}(3, \mathbb{R})$ or $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$.
- 2) Assume G is simple. $\mathbb{R}\text{-rank}(G) \geq 2$ if and only if G contains a subgroup isogenous to either $\mathrm{SL}(3, \mathbb{R})$ or $\mathrm{SO}(2, 3)$.

Proof. (1) This follows from (2) (see Exer. 8:12).

(2) Assume G is simple, and $\mathbb{R}\text{-rank } G \geq 2$. It is straightforward to verify the desired conclusion if G is classical. (The general case follows from the theory of real roots (see Chap. 18).) For example,

- $\mathrm{SL}(3, \mathbb{R})$, $\mathrm{SL}(3, \mathbb{C})$, and $\mathrm{SL}(3, \mathbb{H})$ contain $\mathrm{SL}(3, \mathbb{R})$.
- $\mathrm{SO}(2, n)$, $\mathrm{SU}(2, n)$, and $\mathrm{Sp}(2, n)$ contain $\mathrm{SO}(2, 3)$ if $n \geq 3$.
- $\mathrm{SO}(2, 2)$ is not simple (see 3.31).
- $\mathrm{SU}(2, 2)$ is isogenous to $\mathrm{SO}(2, 4)$, which contains $\mathrm{SO}(2, 3)$.
- $\mathrm{Sp}(2, 2)$ contains $\mathrm{SU}(2, 2)$.
- $\mathrm{Sp}(4, \mathbb{R})$ is isogenous to $\mathrm{SO}(2, 3)$ (see 3.31).

□

(8.36) **Remark.** As was the case when $\mathbb{R}\text{-rank}(G) = 1$, parabolic subgroups are closely related to ∂X . However, the theory is somewhat more complicated, and will be not be discussed until Vol. 2.

For $G = \mathrm{SL}(2, \mathbb{R})^m$, we have

$$\mathbb{R}\text{-rank}(G) = m = \frac{1}{2} \dim(G/K).$$

From the theory of real roots, it is easy to see that this is the extreme case:

(8.37) **Proposition.** Let X be a symmetric space of noncompact type with no flat factors, and let $G = \mathrm{Isom}(X)^\circ$. Then

$$\mathbb{R}\text{-rank}(G) \leq \frac{1}{2} \dim X,$$

with equality if and only if X is isometric to $(\mathfrak{H}^2)^m$, for some m .

8H. Notes

Haven't written this yet!!!

8I. References

[1] ??

Exercises

- 8:1) For $g = \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}$, show that $g^{-1}\mathrm{SO}(2)g$ consists entirely of diagonal matrices.
- 8:2) Prove Prop. 8.7.
- 8:3) Let T be as in Eg. 8.10(3). Find an explicit element g of $\mathrm{GL}(2, \mathbb{R})$, such that $g^{-1}Tg$ consists entirely of diagonal matrices.
- 8:4) Prove, directly from Defn. 8.5, that if G_1 is conjugate to G_2 in $\mathrm{GL}(\ell, \mathbb{R})$, then $\mathbb{R}\text{-rank}(G_1) = \mathbb{R}\text{-rank}(G_2)$.
- 8:5) In Chap. 18, we will show that if G is not compact, then G contains a subgroup isogenous to $\mathrm{SL}(2, \mathbb{R})$ (see also Rem. 3.25 for the case where G is classical). Assuming this fact, prove Prop. 8.20. [*Hint*: Prove $(2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5)$ and $(3) \Rightarrow (1) \Rightarrow (5)$.]
- 8:6) Prove the following are equivalent:
- (a) $\mathbb{R}\text{-rank}(G) = 0$;
 - (b) X is compact;
 - (c) Γ is finite.
- 8:7) Prove that $\mathbb{R}\text{-rank}(G) = 0$ if and only if every element of G is semisimple.
- 8:8) Prove that $\mathbb{R}\text{-rank}(G) = 0$ if and only if G has no nontrivial hyperbolic elements.
- 8:9) Prove Cor. 8.21.
- 8:10) Assume $\mathbb{R}\text{-rank } G = 1$. Show that if U_1 and U_2 are unipotent subgroups of G , and $U_1 \cap U_2 \neq e$, then $\langle U_1, U_2 \rangle$ is unipotent.
- 8:11) Prove that if $\mathbb{R}\text{-rank } G > 1$, then there exist unipotent subgroups U_1 and U_2 of G , such that $U_1 \cap U_2 \neq e$, and $\langle U_1, U_2 \rangle$ is not unipotent. (This is the converse of Exer. 8:10.)
- 8:12) Show that 8.35(1) follows from 8.35(2). [*Hint*: $\mathrm{SO}(2, 3)$ contains $\mathrm{SO}(2, 2)$, which is isogenous to $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$ (see 3.31). If G is not simple, and has no compact factors, then G contains $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SL}(2, \mathbb{R})$.]

$\mathbb{Q}$ -Rank

9A. $\mathbb{Q}$ -split tori

(9.1) **Definition** (cf. 8.5). A torus T in $\mathrm{SL}(\ell, \mathbb{R})$ is $\mathbb{Q}$ -split if

- T is defined over $\mathbb{Q}$; and
- T is diagonalizable over $\mathbb{Q}$. (That is, there exists $g \in \mathrm{GL}(\ell, \mathbb{Q})$, such that $g^{-1}Tg$ consists entirely of diagonal matrices.)

(9.2) **Example.**

- Let

$$T_1 = \left\{ \begin{bmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{bmatrix} \mid t \in \mathbb{R} \right\}$$

(cf. 8.10(3)). Then T_1 is defined over $\mathbb{Q}$, by the equations

$$\begin{aligned} x_{1,1}^2 - x_{1,2}^2 &= 1, \\ x_{2,1} &= x_{1,2}, \\ x_{2,2} &= x_{1,1}. \end{aligned}$$

For

$$g = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

we see that $g^{-1}T_1g$ consists of diagonal matrices, so T_1 is $\mathbb{Q}$ -split.

- Let

$$T_2 = \left\{ \begin{bmatrix} \cosh t & (\sinh t)/\sqrt{2} \\ \sqrt{2}(\sinh t) & \cosh t \end{bmatrix} \mid t \in \mathbb{R} \right\} = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{bmatrix} T_1 \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{bmatrix}^{-1}.$$

Then T_2 is defined over $\mathbb{Q}$, by the equations

$$\begin{aligned} x_{1,1}^2 - 2x_{1,2}^2 &= 1, \\ x_{2,1} &= 2x_{1,2}, \\ x_{2,2} &= x_{1,1}, \end{aligned}$$

and T_2 is $\mathbb{R}$ -split (because it is conjugate to T_1).

However, T_2 is *not* $\mathbb{Q}$ -split. For example, we have

$$\begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix} \in T_{\mathbb{Q}},$$

but the eigenvalues of this matrix are irrational (namely, $3 \pm 2\sqrt{2}$), so this rational matrix is not diagonalizable over $\mathbb{Q}$.

• Let

$$T_3 = \left\{ \begin{bmatrix} \cosh t & (\sinh t)/\pi \\ \pi (\sinh t) & \cosh t \end{bmatrix} \mid t \in \mathbb{R} \right\} = \begin{bmatrix} 1 & 0 \\ 0 & \pi \end{bmatrix} T_1 \begin{bmatrix} 1 & 0 \\ 0 & \pi \end{bmatrix}^{-1}.$$

It is not difficult to see that $(T_3)_{\mathbb{Q}}$ consists of only the identity matrix. Hence, T_3 is not defined over $\mathbb{Q}$ (see 6.8), so it is **not** $\mathbb{Q}$ -split.

(9.3) **Proposition.** *Let T be a torus in $\mathrm{SL}(\ell, \mathbb{R})$, and assume that T is defined over $\mathbb{Q}$. The following are equivalent:*

- 1) T is $\mathbb{Q}$ -split;
- 2) there is a basis $v_1, \dots, v_{\ell}$ of $\mathbb{Q}^{\ell}$, such that, for every $t \in T$ and every $i \in \{1, \dots, \ell\}$, the vector v_i is an eigenvector of t ;
- 3) there is a basis $v_1, \dots, v_{\ell}$ of $\mathbb{Q}^{\ell}$, such that, for every $t \in T_{\mathbb{Q}}$ and every $i \in \{1, \dots, \ell\}$, the vector v_i is an eigenvector of t ;
- 4) every eigenvalue of every element of $T_{\mathbb{Q}}$ is rational.

Proof. (1 $\Leftrightarrow$ 2) Diagonalizing a matrix is equivalent to finding a basis consisting of eigenvectors.

(2 $\Leftrightarrow$ 3) One direction is obvious. The other follows from the fact that $T_{\mathbb{Q}}$ is dense in T (see 6.8).

(1 $\Rightarrow$ 4) We may assume T consists of diagonal matrices. Then the eigenvalues of any $t \in T$ are simply the matrix entries of t . If $t \in T_{\mathbb{Q}}$, these matrix entries are rational.

(4 $\Rightarrow$ 3) If $t \in T_{\mathbb{Q}}$, then, for each eigenvalue λ of t , the equation $tx = \lambda x$ is a linear equation with rational coefficients, so the solution space is spanned by rational vectors. Thus, each eigenspace of t is spanned by rational vectors. Therefore, t is diagonalizable over $\mathbb{Q}$. Since this is true for each $t \in T_{\mathbb{Q}}$, and any set of commuting diagonalizable linear transformations can be simultaneously diagonalized, we conclude that $T_{\mathbb{Q}}$ is diagonalizable over $\mathbb{Q}$. $\square$

9B. $\mathbb{Q}$ -rank of an arithmetic lattice

(9.4) **Definition** (for arithmetic lattices). Assume that G is a $\mathbb{Q}$ -subgroup of $\mathrm{SL}(\ell, \mathbb{R})$, and that Γ is commensurable with $G_{\mathbb{Z}}$. Then $\mathbb{Q}$ -rank(Γ) is the dimension of any maximal $\mathbb{Q}$ -split torus of G . (Because all maximal $\mathbb{Q}$ -split tori are conjugate under $G_{\mathbb{Q}}$, this definition is independent of the particular torus chosen.)

(More generally, if $\phi: G/K \cong G'/K'$, where K and K' are compact, and $\phi(\overline{\Gamma})$ is commensurable with $\overline{G'_{\mathbb{Z}}}$ (see Defn. 6.16), then $\mathbb{Q}$ -rank(Γ) is the dimension of any maximal $\mathbb{Q}$ -split torus of G' .)

(9.5) **Remark.** The definition of $\mathbb{Q}$ -rank(Γ) is somewhat indirect, because the $\mathbb{Q}$ -split tori of G are not subgroups of Γ . Thus, it would be more correct to say that we have defined $\mathbb{Q}$ -rank($G_{\mathbb{Q}}$).

As we will see in the following example, different embeddings of G in $\mathrm{SL}(\ell, \mathbb{R})$ can give different values for the $\mathbb{Q}$ -rank. However, the theory of algebraic groups shows that the $\mathbb{Q}$ -rank is the same for all of the embeddings in which Γ is commensurable with $G_{\mathbb{Z}}$ (see 9.15); thus, $\mathbb{Q}$ -rank(Γ) is well defined as a function of Γ .

(9.6) **Example.**

- 1) $\mathbb{Q}$ -rank($\mathrm{SL}(n, \mathbb{Z})$) = $n - 1$. Let T be the torus of (positive) diagonal matrices in $\mathrm{SL}(n, \mathbb{R})$.
- 2) Let $G = \mathrm{SO}(B)^\circ$, where $B(x_1, \dots, x_\ell)$ is some quadratic form on $\mathbb{R}^\ell$, such that B is defined over $\mathbb{Q}$. (That is, all of the coefficients of B are rational.) Then G is defined over $\mathbb{Q}$, and the discussion of Eg. 8.10, with $\mathbb{Q}$ in place of $\mathbb{R}$, shows that $\mathbb{Q}$ -rank($G_\mathbb{Z}$) is the maximum dimension of a totally isotropic $\mathbb{Q}$ -subspace of $\mathbb{Q}^\ell$. For example,

$$\mathbb{Q}\text{-rank}(\mathrm{SO}(m, n)_\mathbb{Z}) = \min\{m, n\}.$$

Similarly,

$$\mathbb{Q}\text{-rank}(\mathrm{SU}(m, n)_\mathbb{Z}) = \mathbb{Q}\text{-rank}(\mathrm{Sp}(m, n)_\mathbb{Z}) = \min\{m, n\}.$$

- 3) Let $G = \mathrm{SO}(7x_1^2 - x_2^2 - x_3^2 - x_4^2)^\circ$. Then, because the equation $a^2 + b^2 + c^2 \equiv 0 \pmod{7}$ has no nontrivial solutions, it is not difficult to see that the quadratic form is anisotropic; thus, $\mathbb{Q}\text{-rank}(G_\mathbb{Z}) = 0$.

Note, however, that G is isomorphic to $\mathrm{SO}(1, 3)^\circ$; indeed, G is conjugate to $\mathrm{SO}(1, 3)^\circ$, via the matrix

$$\begin{bmatrix} \sqrt{7} & 0 & 0 & \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We see from Thm. 9.21 below that $G_\mathbb{Z} \backslash G$ is compact; thus, $G_\mathbb{Z} \backslash \mathfrak{H}^3$ is a *compact* hyperbolic 3-manifold, whereas $\mathrm{SO}(1, 3)_\mathbb{Z} \backslash \mathfrak{H}^3$ is not compact. Therefore, the Mostow Rigidity Theorem (1.25) implies that $G_\mathbb{Z}$ is not isomorphic to $\mathrm{SO}(1, 3)_\mathbb{Z}$; this is an illustration of the fact that a different embedding of G in $\mathrm{SL}(\ell, \mathbb{R})$ can yield very different integer points. (Technical remark: Actually, $G_\mathbb{Z} \backslash \mathfrak{H}^3$ is an *orbifold*. To obtain a (compact) *manifold*, replace $G_\mathbb{Z}$ with a torsion-free subgroup of finite index (see 5.60).)

Similarly, if G is defined over an algebraic number field F , then one can define F -rank(G). The following result shows that this can be used to calculate the $\mathbb{Q}$ -rank of a lattice obtained by Restriction of Scalars.

(9.7) **Lemma.** *Suppose*

- F is an algebraic number field,
- $\mathcal{O}$ is the ring of integers of F ,
- G is defined over F (as an algebraic group over F_∞), and
- $\Delta: G_F \rightarrow \prod_{\sigma \in S^\infty} G^\sigma$ is defined by $\Delta(g) = (\sigma(g))_{\sigma \in S^\infty}$, as in Prop. 6.49.

Then $\mathbb{Q}\text{-rank}(\Delta(G_\mathcal{O})) = F\text{-rank}(G)$.

Proof. If T is a torus in G , and T is defined over F , then $\prod_{\sigma \in S^\infty} T^\sigma$ is a $\mathbb{Q}$ -torus in $\prod_{\sigma \in S^\infty} G^\sigma$. Conversely, it is not difficult to see that any $\mathbb{Q}$ -torus of $\prod_{\sigma \in S^\infty} G^\sigma$ is contained in a torus of the form $\prod_{\sigma \in S^\infty} T^\sigma$. Thus, the desired conclusion follows from the fact, which will be proved in §14B, that

$$\mathbb{Q}\text{-rank}\left(\prod_{\sigma \in S^\infty} T^\sigma\right) = F\text{-rank}(T)$$

(see 14.4). □

9C. Isogenies over $\mathbb{Q}$

We know examples where G is isogenous (or even isomorphic) to H , but $G_{\mathbb{Z}}$ is very different from $H_{\mathbb{Z}}$. (For example, it may be the case that $G_{\mathbb{Z}}$ is cocompact and $H_{\mathbb{Z}}$ is not. This does not happen if the isogeny is defined over $\mathbb{Q}$ (in the sense that we now define). Because of our interest in restriction of scalars, we describe the theory over any algebraic number field F . For the particularly motivated reader, we provide some proofs.

(9.8) Definition.

- A homomorphism $\phi: G \rightarrow H$ is *defined over F* if
 - 1) ϕ is differentiable,
 - 2) the derivative $d\phi_e$ is F_{∞} -linear, and
 - 3) $\phi(G_F) \subset H_F$.
- G_1 is *isogenous to G_2 over F* (denoted $G_1 \approx_F G_2$) if there is a group G that is defined over F , and isogenies $\phi_j: G \rightarrow G_j$ that are defined over F .

(9.9) **Proposition.** *If $G_1 \approx_F G_2$, then there is a group G defined over F and **polynomial** isogenies $\phi_j: G \rightarrow G_j$ that are defined over F .*

Proof. Given isogenies $\phi_j: G \rightarrow G_j$ that are defined over F , let

$$G' = \{ (\phi_1(g), \phi_2(g)) \mid g \in G \}.$$

The projection maps $\phi'_j: G' \rightarrow G_j$ defined by $\phi'_j(g_1, g_2) = g_j$ are polynomials. □

(9.10) **Warning.** There are examples where $\phi: G_1 \rightarrow G_2$ is an isomorphism over F , and ϕ is a polynomial, but ϕ^{-1} is not a polynomial. For example, the natural homomorphism $\phi: \mathrm{SL}(3, \mathbb{R}) \rightarrow \mathrm{PSL}(3, \mathbb{R})^{\circ}$ is an isomorphism (because $\mathrm{SL}(3, \mathbb{R})$ has no center). However, there is no isomorphism from $\mathrm{PSL}(3, \mathbb{C})$ to $\mathrm{SL}(3, \mathbb{C})$ (because one of these groups has a center and the other does not), so the inverse of ϕ cannot be a polynomial (because it does not extend to a well-defined map on the complex points).

The following fundamental result implies that different embeddings of G with the same $\mathbb{Q}$ -points have essentially the same $\mathbb{Z}$ -points.

(9.11) **Proposition.** *Suppose $\phi: G \rightarrow H$ is a surjective homomorphism that is defined over F , and $\mathcal{O}$ is the ring of integers of F . Then $\phi(G_{\mathcal{O}})$ is commensurable with $H_{\mathcal{O}}$.*

Proof. Let us assume $F = \mathbb{Q}$ and $\mathcal{O} = \mathbb{Z}$. (The general case follows from this by Restriction of Scalars.) From the proof of Prop. 9.9, we see that, after replacing G with an isogenous group, we may assume that ϕ is a polynomial with rational coefficients. Assume $G \subset \mathrm{SL}(\ell, \mathbb{R})$ and $H \subset \mathrm{SL}(m, \mathbb{R})$.

Define $\phi': G \rightarrow \mathrm{Mat}_{m \times m}(\mathbb{R})$ by $\phi'(x) = \phi(x - \mathrm{Id})$. Being a polynomial, the function ϕ' is defined on all of $\mathrm{Mat}_{\ell \times \ell}(\mathbb{R})$. Because the coefficients are rational, there is some nonzero $n \in \mathbb{N}$, such that $\phi'(n \mathrm{Mat}_{\ell \times \ell}(\mathbb{R})) \subset \mathrm{Mat}_{m \times m}(\mathbb{Z})$. Thus, letting Γ_n be the principal congruence subgroup of $G_{\mathbb{Z}}$ of level n , we have $\phi(\Gamma_n) \subset H_{\mathbb{Z}}$.

Because Γ_n is a lattice in G (and $\phi(\Gamma_n)$ is discrete), we know that $\phi(\Gamma_n)$ is a lattice in H . Because $\phi(\Gamma_n) \subset H_{\mathbb{Z}}$, we conclude that $\phi(\Gamma_n)$ is commensurable with $H_{\mathbb{Z}}$ (see Exer. 5:7). □

(9.12) **Corollary.** *Suppose G and H are subgroups of $\mathrm{SL}(\ell, \mathbb{R})$ that are defined over $\mathbb{Q}$. A differentiable homomorphism $\phi: G \rightarrow H$ is defined over $\mathbb{Q}$ if and only if some finite-index subgroup of $\phi(G_{\mathbb{Z}})$ is contained in $H_{\mathbb{Q}}$.*

(9.13) **Definition.** Suppose G is a subgroup of $\mathrm{SL}(\ell, \mathbb{R})$ that is defined over $\mathbb{Q}$. We define

$$\mathbb{Q}\text{-rank}(G) = \max\{\dim T \mid T \text{ is a } \mathbb{Q}\text{-split torus contained in } G\}.$$

(9.14) **Warning.** We do not speak of $\mathbb{Q}\text{-rank}(G)$ when G is an abstract Lie group: we must have a specific embedding of G in $\mathrm{SL}(\ell, \mathbb{R})$. We have already seen examples where different embeddings of the same group can yield different values of the $\mathbb{Q}\text{-rank}$. Thus, for example, when we speak of $\mathbb{Q}\text{-rank}(\mathrm{SO}(m, n))$, we are thinking of the natural embedding of $\mathrm{SO}(m, n)$ in $\mathrm{SL}(m + n, \mathbb{R})$. If we have some other embedding in mind, say, $\phi: \mathrm{SO}(m, n) \rightarrow \mathrm{SL}(\ell, \mathbb{R})$, then we must write $\mathbb{Q}\text{-rank}(\phi(\mathrm{SO}(m, n)))$.

(9.15) **Corollary.** If $G_1 \approx_F G_2$, then $\mathbb{Q}\text{-rank}(G_1) = \mathbb{Q}\text{-rank}(G_2)$.

9D. $\mathbb{Q}$ -rank of any lattice

Technically, $\mathbb{Q}\text{-rank}(\Gamma)$ is defined only when Γ is arithmetic, but combining the following remark with the Margulis Arithmeticity Theorem (6.21) allows us to extend the definition to all lattices.

(9.16) **Remark.** Assume Γ is arithmetic.

- If $\Gamma \backslash G$ is compact, then $\mathbb{Q}\text{-rank}(\Gamma) = 0$ (see 9.21).
- If $\Gamma \backslash G$ is not compact, and $\mathbb{R}\text{-rank}(G) = 1$, then $\mathbb{Q}\text{-rank}(\Gamma) \neq 0$ (see 9.21) and $\mathbb{Q}\text{-rank}(\Gamma) \leq \mathbb{R}\text{-rank}(G) = 1$ (see 9.18); so we must have $\mathbb{Q}\text{-rank}(\Gamma) = 1$.
- If $\Gamma = \Gamma_1 \times \cdots \times \Gamma_r$ is reducible, then $\mathbb{Q}\text{-rank}(\Gamma) = \mathbb{Q}\text{-rank}(\Gamma_1) + \cdots + \mathbb{Q}\text{-rank}(\Gamma_r)$.
- If C is a compact, normal subgroup of G , and $\bar{\Gamma}$ is the image of Γ in $\bar{G} = G/C$, then $\mathbb{Q}\text{-rank}(\Gamma) = \mathbb{Q}\text{-rank}(\bar{\Gamma})$.

Thus, the following definition is consistent with Defn. 9.4.

(9.17) **Definition.** Up to isogeny, and modulo the maximal compact factor of G , we may write $G = G_1 \times \cdots \times G_r$, so that $\Gamma_i = \Gamma \cap G_i$ is an irreducible lattice in G_i for $i = 1, \dots, r$ (see 5.24). We let

$$\mathbb{Q}\text{-rank}(\Gamma) = \mathbb{Q}\text{-rank}(\Gamma_1) + \cdots + \mathbb{Q}\text{-rank}(\Gamma_r),$$

where:

- 1) If $\Gamma_i \backslash G$ is compact, then $\mathbb{Q}\text{-rank}(\Gamma_i) = 0$.
- 2) If $\Gamma_i \backslash G$ is not compact, but $\mathbb{R}\text{-rank}(G) = 1$, then $\mathbb{Q}\text{-rank}(\Gamma_i) = 1$.
- 3) If $\Gamma_i \backslash G$ is not compact, and $\mathbb{R}\text{-rank}(G) \geq 2$, then the Margulis Arithmeticity Theorem (6.21) implies that Γ_i is arithmetic, so Defn. 9.4 applies.

9E. The possible $\mathbb{Q}$ -ranks

Because any $\mathbb{Q}$ -split torus is $\mathbb{R}$ -split, we obviously have

$$(9.18) \quad 0 \leq \mathbb{Q}\text{-rank}(\Gamma) \leq \mathbb{R}\text{-rank}(G).$$

Both extremes are realized (for every G):

(9.19) **Theorem.** There are arithmetic lattices Γ_c and Γ_s in G , such that $\mathbb{Q}\text{-rank}(\Gamma_c) = 0$ and $\mathbb{Q}\text{-rank}(\Gamma_s) = \mathbb{R}\text{-rank}(G)$.

In particular, if $\mathbb{R}\text{-rank}(G) \geq 2$, then G has a lattice Γ with $\mathbb{Q}\text{-rank}(\Gamma) \geq 2$.

Proof. Suppose G is classical. Then, for the natural embeddings described in Egs. 3.22 and 3.23, it is easy to see that $\mathbb{Q}\text{-rank}(G_{\mathbb{Z}}) = \mathbb{R}\text{-rank}(G)$ (cf. Eg. 9.6(1,2)); thus, it is easy to construct Γ_s . The method of Prop. 6.45 yields a cocompact lattice Γ_c in $\mathrm{SO}(m, n)$, $\mathrm{SU}(m, n)$, or $\mathrm{Sp}(m, n)$ (see Exers. 9:5 and 9:6). A similar method applies to the other classical groups, as is explained in §10C.

A complete proof of this result (including the exceptional groups) can be found in Chap. 13. $\square$

However, although the extremes are attained, the following example shows that there can be gaps between 0 and $\mathbb{R}\text{-rank}(G)$.

(9.20) **Proposition.** *Assume $G \cong \mathrm{SO}(2, n)^\circ$, with $n \geq 5$, and assume n is odd. Then $\mathbb{R}\text{-rank}(G) = 2$, but there is no lattice Γ in G , such that $\mathbb{Q}\text{-rank}(\Gamma) = 1$.*

Proof. From 8.10(4), we have $\mathbb{R}\text{-rank}(G) = \min\{2, n\} = 2$.

Suppose $\mathbb{Q}\text{-rank}(\Gamma) = 1$. The Margulis Arithmeticity Theorem (6.21) implies that Γ is arithmetic. Since $\mathbb{Q}\text{-rank}(\Gamma) \neq 0$, this implies that (up to isogeny) there is an embedding of G in some $\mathrm{SL}(\ell, \mathbb{R})$, such that Γ is commensurable with $G_{\mathbb{Z}}$ (see 9.22). (The point here is that, because $\Gamma \backslash G$ is not compact, Rem. 6.17 shows there is no need for the compact groups K and K' of Defn. 6.16.) From the description of arithmetic subgroups of $\mathrm{SO}(m, n)$ that appears in Fig. 10.2 (and the fact that $m + n$ is odd), we conclude that we may take $\ell = n + 2$, and that there is a symmetric bilinear form $B(x, y)$ on $\mathbb{R}^{n+2}$, such that B is defined over $\mathbb{Q}$, and

- 1) B has signature $(2, n)$ on $\mathbb{R}^{n+2}$ (because $\mathbb{R}\text{-rank}(G) = 2$), but
- 2) no 2-dimensional subspace of $\mathbb{Q}^{n+2}$ is totally isotropic (because $\mathbb{Q}\text{-rank}(\Gamma) < 2$).

A theorem of number theory asserts:

- *) If $B_0(x, y)$ is any nondegenerate, symmetric bilinear form on $\mathbb{R}^d$, such that
- B is defined over $\mathbb{Q}$,
 - $d \geq 5$, and
 - B_0 is isotropic over $\mathbb{R}$ (that is, $B(v, v) = 0$ for some nonzero $v \in \mathbb{R}^d$),
- then B_0 is also isotropic over $\mathbb{Q}$ (that is, $B(v, v) = 0$ for some nonzero $v \in \mathbb{Q}^d$).

(This is related to, but more difficult than, the fact that every integer is a sum of four squares.)

From (*), we know that there is a nontrivial isotropic vector $v \in \mathbb{Q}^{n+2}$. Then, because B is nondegenerate, there is a vector $w \in \mathbb{Q}^{n+2}$, such that $B(v, w) = 1$ and $B(w, w) = 0$. Let $V = \langle v, w \rangle$. Because the restriction of B to V is nondegenerate, we have $\mathbb{R}^{n+2} = V \oplus V^\perp$. This direct sum is obviously orthogonal (with respect to B), and the restriction of B to V has signature $(1, 1)$, so we conclude that the restriction of B to $V^\perp$ has signature $(1, n - 1)$. Thus, there is an isotropic vector in $V^\perp$. From (*), we conclude that there is an isotropic vector z in $(V^\perp)_{\mathbb{Q}}$. Then $\langle v, z \rangle$ is a 2-dimensional totally isotropic subspace of $\mathbb{Q}^{n+2}$. This is a contradiction. $\square$

9F. Lattices of $\mathbb{Q}$ -rank zero

It is instructive to compare Thms. 9.21 and 9.24 with Prop. 8.20, an analogous statement with G in place of Γ , $\Gamma \backslash G$, and $G_{\mathbb{Q}}$.

The following fundamental result relates three purely algebraic conditions ((1), (3), and (4)) to a purely geometric condition (2). The equivalence $(2 \Leftrightarrow 4)$ generalizes the Godement Criterion (6.34) to the case where Γ is not assumed to be arithmetic.

(9.21) **Theorem.** *If G has no compact factors, then the following are equivalent:*

- 1) $\mathbb{Q}\text{-rank}(\Gamma) = 0$;

- 2) $\Gamma \backslash G$ is compact;
- 3) every element of Γ is semisimple;
- 4) Γ has no nontrivial unipotent elements.

Proof. Let us assume that $G \subset \mathrm{SL}(\ell, \mathbb{R})$, and that $\Gamma = G_{\mathbb{Z}}$. (There is no difficulty in generalizing the proof to any arithmetic lattice, but, for a general lattice, (4 $\Rightarrow$ 2) is rather difficult; it will be proved in §16D.)

(2 $\Rightarrow$ 1) We prove the contrapositive: suppose $\mathbb{Q}\text{-rank}(\Gamma) \neq 0$. (We wish to show $G_{\mathbb{Z}} \backslash G$ is not compact.) By definition of $\mathbb{Q}\text{-rank}(\Gamma)$, we know that there is a nontrivial $\mathbb{Q}$ -split torus T in G . Then $T_{\mathbb{Q}}$ is infinite, so there is some $g \in T_{\mathbb{Q}}$, and some (rational) eigenvalue λ of g , such that $\lambda \notin \{\pm 1\}$; for definiteness, let us assume $|\lambda| < 1$. Choose some nonzero $v \in \mathbb{Q}^{\ell}$, such that $gv = \lambda v$. Multiplying by an integer to clear the denominators, we may assume $v \in \mathbb{Z}^{\ell}$. Now

$$g^n v = \lambda^n v \rightarrow 0 \quad \text{as } n \rightarrow \infty.$$

Thus, because $g^n v \in Gv$, we conclude that 0 is an accumulation point of the orbit Gv . Hence, the Mahler Compactness Criterion (5.34) asserts that the image of G in $\mathrm{SL}(\ell, \mathbb{Z}) \backslash \mathrm{SL}(\ell, \mathbb{R})$ is not compact. Since this is the image of the natural inclusion $G_{\mathbb{Z}} \backslash G \hookrightarrow \mathrm{SL}(\ell, \mathbb{Z}) \backslash \mathrm{SL}(\ell, \mathbb{R})$, we conclude that $G_{\mathbb{Z}} \backslash G$ is not compact.

(4 $\Rightarrow$ 2) Because Γ is assumed to be arithmetic, this follows from the Godement Criterion (6.34).

(1 $\Rightarrow$ 4) We prove the contrapositive: suppose u is a nontrivial unipotent element of Γ . (We wish to show that $\mathbb{Q}\text{-rank}(\Gamma) \neq 0$.) Since $\Gamma \subset G_{\mathbb{Q}}$, the Jacobson-Morosov Lemma (4.16) implies that there is a nontrivial polynomial homomorphism $\phi: \mathrm{SL}(2, \mathbb{R}) \rightarrow G$ with $\phi(\mathrm{SL}(2, \mathbb{Q})) \subset G_{\mathbb{Q}}$. Then, letting T be a nontrivial $\mathbb{Q}$ -split torus in $\mathrm{SL}(2, \mathbb{R})$, we see that $\phi(T)$ is a nontrivial $\mathbb{Q}$ -split torus in G , so $\mathbb{Q}\text{-rank}(\Gamma) \neq 0$.

(3 $\Rightarrow$ 4) Obvious.

(1 $\Rightarrow$ 3) See Thm. 9.24(2). □

The following important result shows that if $\Gamma \backslash G$ is not compact, then there is no need for the compact group K' in Defn. 6.16.

(9.22) **Corollary.** *Assume that G has no compact factors, and that Γ is arithmetic, irreducible, and **not** cocompact. Then, after replacing G by an isogenous group, there is an embedding of G in some $\mathrm{SL}(\ell, \mathbb{R})$, such that*

- 1) G is defined over $\mathbb{Q}$, and
- 2) Γ is commensurable with $G_{\mathbb{Z}}$.

Proof. From Defn. 6.16, we see that (up to isogeny and commensurability) there is a compact group K' , such that we may embed $G' = G \times K'$ in some $\mathrm{SL}(\ell, \mathbb{R})$, such that G' is defined over $\mathbb{Q}$, and $\Gamma K' = G'_{\mathbb{Z}} K'$.

Let N be the (almost-)Zariski closure of the subgroup of G' generated by all of the unipotent elements of $G'_{\mathbb{Z}}$. From the definition, it is clear that N is normalized by the Zariski closure of $G'_{\mathbb{Z}}$. Thus, the Borel Density Theorem (5.39) implies that N is normalized by G .

Because K' has no unipotent elements (see 8.20), we know that $N \subset G$. Also, because $\Gamma \backslash G$ is not compact, we know that $G'_{\mathbb{Z}}$ contains nontrivial unipotent elements (see 9.21), so N is infinite. Therefore, under the simplifying assumption that G is simple, we conclude that $N = G$.

Thus, G is the (almost-)Zariski closure of a subset of Γ' . Since $\Gamma' \subset G'_{\mathbb{Q}}$, this implies that G is defined over $\mathbb{Q}$ (cf. Exer. 6:4). Hence, $G_{\mathbb{Z}}$ is a lattice in G , so $G_{\mathbb{Z}}$ has finite index in $G'_{\mathbb{Z}}$ (see Exer. 5:7). Because $G'_{\mathbb{Z}}K' = \Gamma K'$, we conclude that $G_{\mathbb{Z}} = \Gamma$ (up to commensurability). $\square$

(9.23) **Remark.** If the assumption that G has no compact factors is removed from Thm. 9.21, then we have $(1) \Leftrightarrow (2) \Leftrightarrow (3) \Rightarrow (4)$.

The following result compares directly with Cor. 8.19 and Prop. 8.20. For the proof, see Exer. 9:3.

(9.24) **Theorem.** *If Γ is commensurable with $G_{\mathbb{Z}}$, then the following are equivalent:*

- 1) $\mathbb{Q}$ -rank(Γ) = 0;
- 2) every element of $G_{\mathbb{Q}}$ is semisimple;
- 3) $G_{\mathbb{Q}}$ has no nontrivial unipotent elements;
- 4) $G_{\mathbb{Q}}$ does not contain a subgroup isogenous to $\mathrm{SL}(2, \mathbb{Q})$;
- 5) no proper parabolic subgroup of G is defined over $\mathbb{Q}$.

(9.25) **Remark.** In analogy with Prop. 8.20(5) and Thm. 9.24(4), one might suppose that the $\mathbb{Q}$ -rank of Γ is 0 if and only if Γ does not contain a subgroup that is isomorphic to $\mathrm{SL}(2, \mathbb{Z})$ (modulo finite groups). Unfortunately, this is false. To the contrary, every lattice in G contains a subgroup that is abstractly commensurable with $\mathrm{SL}(2, \mathbb{Z})$ (unless G is compact). Namely, Γ contains a nonabelian free subgroup (see 5.65), and it is well known that $\mathrm{SL}(2, \mathbb{Z})$ has a finite-index subgroup that is free.

9G. Lattices of $\mathbb{Q}$ -rank one

The results of this section should be compared with Thm. 8.29.

(9.26) **Theorem.** *The following are equivalent:*

- 1) $\mathbb{Q}$ -rank(Γ) ≤ 1 ;
- 2) any two maximal unipotent subgroups of Γ either are equal or are disjoint.

(9.27) **Theorem.** *If Γ is commensurable with $G_{\mathbb{Z}}$, then the following are equivalent:*

- 1) $\mathbb{Q}$ -rank(Γ) ≤ 1 ;
- 2) if U_1 and U_2 are unipotent subgroups of $G_{\mathbb{Q}}$, and $U_1 \cap U_2 \neq e$, then $\langle U_1, U_2 \rangle$ is unipotent;
- 3) any two maximal unipotent subgroups of $G_{\mathbb{Q}}$ either are equal or are disjoint;
- 4) all proper parabolic $\mathbb{Q}$ -subgroups of G are conjugate to each other (in fact, they are conjugate under $G_{\mathbb{Q}}$).

9H. Lattices of higher $\mathbb{Q}$ -rank

The following two results are analogues of Thm. 8.35 (cf. Exer. 9:9).

(9.28) **Theorem.** *Assume Γ is irreducible. Then $\mathbb{Q}$ -rank(Γ) ≥ 2 if and only if Γ contains a subgroup that is isomorphic to a finite-index subgroup of either $\mathrm{SL}(3, \mathbb{Z})$ or $\mathrm{SO}(2, 3)_{\mathbb{Z}}$.*

(9.29) **Theorem.** *Assume Γ is commensurable with $G_{\mathbb{Z}}$.*

- 1) $\mathbb{Q}$ -rank(Γ) ≥ 2 if and only if $G_{\mathbb{Q}}$ contains a subgroup isogenous to either $\mathrm{SL}(2, \mathbb{Q}) \times \mathrm{SL}(2, \mathbb{Q})$ or $\mathrm{SL}(3, \mathbb{Q})$.

- 2) Assume Γ is irreducible. Then $\mathbb{Q}\text{-rank}(\Gamma) \geq 2$ if and only if $G_{\mathbb{Q}}$ contains a subgroup isogenous to either $\mathrm{SL}(3, \mathbb{Q})$ or $\mathrm{SO}(2, 3)_{\mathbb{Q}}$.

(9.30) **Remark** (cf. Rem. 3.31).

- $\mathrm{SO}(2, 3)_{\mathbb{Z}}$ is abstractly commensurable with $\mathrm{Sp}(4, \mathbb{Z})$, and
- $\mathrm{SO}(2, 3)_{\mathbb{Q}}$ is abstractly commensurable with $\mathrm{Sp}(4, \mathbb{Q})$.

The following result can be obtained from the proof of Thm. 8.32, by replacing $\mathbb{R}$ with $\mathbb{Z}$ or $\mathbb{Q}$ in appropriate places.

(9.31) **Theorem.** *The following are equivalent:*

- 1) $\mathbb{Q}\text{-rank}(\Gamma) \geq 2$;
- 2) for every pair of nontrivial unipotent subgroups U and V of Γ , there is a finite sequence $U_0, \dots, U_r$ of nontrivial unipotent subgroups of Γ , with $U_0 = U$, $U_r = V$, and $[U_i, U_{i-1}] = e$ for $i = 1, \dots, r$;
- 3) there is a finite sequence $U_0, \dots, U_r$ of nontrivial unipotent subgroups of Γ , such that $[U_i, U_{i-1}] = e$ for $i = 1, \dots, r$, and $\langle U_0, \dots, U_r \rangle$ is a finite-index subgroup of Γ .

Unipotent generators, such as those in 9.31(3), are easy to work with. Vol. 2 will provide an introduction to their use in the study of difficult algebraic problems.

(9.32) **Remark.**

- 1) Suppose $\mathbb{Q}\text{-rank}(\Gamma) \leq 1$. Theorem 9.31 shows that it is impossible to find a generating set $\{\gamma_1, \dots, \gamma_r\}$ for Γ , such that each γ_i is nontrivial and unipotent, and γ_i commutes with γ_{i+1} , for each i . However, it is possible, in some cases, to find a generating set $\{\gamma_1, \dots, \gamma_r\}$ that has all of these properties *except* the requirement that γ_i is unipotent. For example, this is easy (up to finite index) if Γ is reducible (see Exer. 9:10).
- 2) For any prime p , let us briefly explain how to use the technique of Prop. 7.51 to construct an arithmetic lattice Γ in $\mathrm{SL}(p, \mathbb{R})$ with the property that if γ_1 and γ_2 are any nontrivial elements of Γ , such that γ_1 commutes with γ_2 , then $C_{\Gamma}(\gamma_1) = C_{\Gamma}(\gamma_2)$. (Hence, it is impossible to find a sequence of generators of Γ , such that each generator commutes with the next (see Exer. 9:11).) Let D be a division ring of degree p over $\mathbb{Q}$, such that D splits over $\mathbb{R}$; thus $\mathbb{R} \otimes_{\mathbb{Q}} D \cong \mathrm{Mat}_{p \times p}(\mathbb{R})$. Let D^1 be the multiplicative group consisting of the elements of $\mathbb{R} \otimes_{\mathbb{Q}} D$ of reduced norm 1, so $D^1 \cong \mathrm{SL}(p, \mathbb{R})$. Let $\mathcal{O}$ be the subgroup of D^1 consisting of the elements of D that are algebraic integer units over $\mathbb{Q}$; then $\mathcal{O}$ is a lattice in D^1 . Now let Γ be a torsion-free subgroup of finite index in $\mathcal{O}$. For any $\gamma_1 \in \Gamma$, we know that $C_D(\gamma_1)$ is a division ring that contains the field $\mathbb{Q}[\gamma_1]$ in its center. Because the degree p is prime, we conclude that $C_D(\gamma_1) = \mathbb{Q}[\gamma_1]$. Now, if γ_2 commutes with γ_1 , then $C_D(\gamma_2) \supset \mathbb{Q}[\gamma_1] = C_D(\gamma_1)$. By symmetry, we conclude that $C_D(\gamma_2) = C_D(\gamma_1)$.

9I. Parabolic $\mathbb{Q}$ -subgroups

Need to add some explanation to this section!!!

The structure theory of §4G has an analogue for parabolic subgroups of G that are defined over $\mathbb{Q}$ (or any other subfield of $\mathbb{C}$).

We know that if G is classical, then parabolic subgroups are stabilizers of flags. The following result states that parabolic $\mathbb{Q}$ -subgroups are stabilizers of flags that are defined over $\mathbb{Q}$.

(9.33) **Theorem.** 1) P is a parabolic $\mathbb{Q}$ -subgroup of $\mathrm{SL}(n, \mathbb{R})$ if and only if there is a chain $V_0 \subset V_1 \subset \cdots \subset V_k$ of $\mathbb{Q}$ -subspaces of $\mathbb{Q}^n$, such that

$$P = \{ g \in \mathrm{SL}(n, \mathbb{R}) \mid \forall i, g(\langle V_i \rangle_{\mathbb{R}}) = \langle V_i \rangle_{\mathbb{R}} \},$$

where $\langle V \rangle_{\mathbb{R}}$ denotes the $\mathbb{R}$ -span of the $\mathbb{Q}$ -subspace V . Similarly for $\mathrm{SL}(n, \mathbb{C})$ and $\mathrm{SL}(n, \mathbb{H})$, taking chains of $\mathbb{Q}$ -subspaces in $\mathbb{Q}(i)^n$ and $\mathbb{Q}(i, j, k)^n$.

2) Let $\langle \cdot \mid \cdot \rangle$ be a symmetric, nondegenerate bilinear form on $\mathbb{R}^n$, and assume $\langle \cdot \mid \cdot \rangle$ is defined over $\mathbb{Q}$. A group P is a parabolic $\mathbb{Q}$ -subgroup of $\mathrm{SO}(\langle \cdot \mid \cdot \rangle)$ if and only if there is a chain $V_0 \subset V_1 \subset \cdots \subset V_k$ of totally isotropic subspaces of $\mathbb{Q}^n$ (with respect to the form $\langle \cdot \mid \cdot \rangle$), such that

$$P = \{ g \in \mathrm{SO}(\langle \cdot \mid \cdot \rangle) \mid \forall i, g(\langle V_i \rangle_{\mathbb{R}}) = \langle V_i \rangle_{\mathbb{R}} \}.$$

Similarly for orthogonal groups over $\mathbb{C}$ or $\mathbb{H}$, and also for unitary or symplectic groups.

(9.34) **Theorem** (Langlands Decomposition. / If P is a parabolic $\mathbb{Q}$ -subgroup of G , then we may write P in the form $P = MAN$, where

- 1) A is a $\mathbb{Q}$ -split torus,
- 2) $MA = C_G(A)$,
- 3) $M/Z(M)^\circ$ is semisimple,
- 4) $Z(M)^\circ$ is a torus that is $\mathbb{Q}$ -anisotropic, and
- 5) N is the unipotent radical of P .

Each of M , A , and N is defined over $\mathbb{Q}$. Furthermore, the subgroups A and N are nontrivial if and only if $P \neq G$.

For some $a \in A_{\mathbb{Q}}$, we have

$$P = \left\{ g \in G \mid \limsup_{n \rightarrow \infty} \|a^{-n}ga^n\| < \infty \right\}$$

and

$$N = \left\{ g \in G \mid \lim_{n \rightarrow \infty} a^{-n}ga^n = e \right\}.$$

(9.35) **Proposition.** Assume G is defined over $\mathbb{Q}$.

- 1) If P and Q are two parabolic $\mathbb{Q}$ -subgroups of G , such that P is conjugate to Q , then there is some $g \in G_{\mathbb{Q}}$, such that $P^g = Q$.
- 2) The number of conjugacy classes of parabolic $\mathbb{Q}$ -subgroups is 2^r , where $r = \mathbb{Q}\text{-rank}(G_{\mathbb{Z}})$.
- 3) The minimal parabolic $\mathbb{Q}$ -subgroups of G are conjugate to each other (via $G_{\mathbb{Q}}$).
- 4) A parabolic $\mathbb{Q}$ -subgroup P is minimal (among all parabolic $\mathbb{Q}$ -subgroups) if and only if, in the Langlands decomposition of P , the subgroup A is a maximal $\mathbb{Q}$ -split torus of G .
- 5) A parabolic $\mathbb{Q}$ -subgroup P is minimal (among all parabolic $\mathbb{Q}$ -subgroups) if and only if, in the Langlands decomposition of P , we have $\mathbb{Q}\text{-rank}(M) = 0$.
- 6) If U is any unipotent $\mathbb{Q}$ -subgroup of G , then there is a parabolic $\mathbb{Q}$ -subgroup P of G , such that
 - (a) U is contained in the unipotent radical of P , and
 - (b) $N_G(U) \subset P$.

(9.36) **Corollary.** Assume G is defined over $\mathbb{Q}$.

- 1) The maximal unipotent $\mathbb{Q}$ -subgroups of G are precisely the unipotent radicals of the minimal parabolic $\mathbb{Q}$ -subgroups of G .

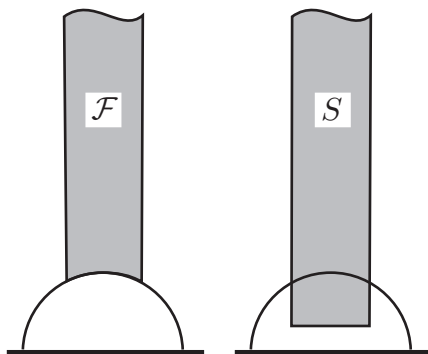


Figure 9.1. The fundamental domain $\mathcal{F}$ and the Siegel set $S_{1/2,t}$ in $\mathfrak{H}^2$.

2) All of the maximal unipotent subgroups of $G_{\mathbb{Q}}$ are conjugate (via $G_{\mathbb{Q}}$).

(9.37) **Theorem.** Assume G is defined over $\mathbb{Q}$.

- 1) For any parabolic $\mathbb{Q}$ -subgroup P of G , the double-coset space $G_{\mathbb{Z}} \backslash G_{\mathbb{Q}} / P_{\mathbb{Q}}$ is finite.
- 2) Equivalently, there is a finite collection $\{P_1, \dots, P_r\}$ of parabolic $\mathbb{Q}$ -subgroups of G , such that every parabolic $\mathbb{Q}$ -subgroup of G is a conjugate P_i^{γ} , for some i , and some $\gamma \in G_{\mathbb{Z}}$.

(9.38) **Corollary.** Γ has only finitely many conjugacy classes of maximal unipotent subgroups.

Proof. Assume $\Gamma = G_{\mathbb{Z}}$ is arithmetic.

It suffices to show that the maximal unipotent subgroups of Γ are precisely the subgroups of Γ of the form $N_{\mathbb{Z}}$, where N is the unipotent radical of a minimal parabolic $\mathbb{Q}$ -subgroup of G . (For then the desired conclusion follows from 9.37(2).)

Suppose U is a maximal unipotent subgroup of $G_{\mathbb{Z}}$. Then the Zariski closure $\overline{U}$ of U is a unipotent $\mathbb{Q}$ -subgroup of G . Hence, there is a parabolic $\mathbb{Q}$ -subgroup $P = MAN$, such that $U \subset N$. Then $U \subset \overline{U}_{\mathbb{Z}} \subset N_{\mathbb{Z}}$, so the maximality of U implies that $U = N_{\mathbb{Z}}$.

The converse is similar (and uses Lem. 9.39). □

(9.39) **Lemma.** If U is a unipotent $\mathbb{Q}$ -subgroup of $\mathrm{SL}(\ell, \mathbb{R})$, then $U_{\mathbb{Z}}$ is a cocompact lattice in U .

9J. The large-scale geometry of $\Gamma \backslash X$

Let us give a heuristic proof of Thm. 2.17. A more complete discussion appears in Sect. 14D.

(9.40) **Example.** Suppose $G = \mathrm{SL}(2, \mathbb{R})$ and $\Gamma = \mathrm{SL}(2, \mathbb{Z})$. It is well known that a fundamental domain for Γ on $\mathfrak{H}^2$ is given by

$$\mathcal{F} = \{z \in \mathfrak{H}^2 \mid -1/2 \leq \mathrm{Re} z \leq 1/2, |z| \geq 1\}.$$

To study the large-scale geometry of $\Gamma \backslash \mathfrak{H}^2$, we do not need to be so careful as to take *exactly* a fundamental domain. Let us enlarge $\mathcal{F}$ somewhat, to a set that is easier to work with:

$$S_{1/2,t} = \{z \in \mathfrak{H}^2 \mid -1/2 \leq \mathrm{Re} z \leq 1/2, \mathrm{Im} z \geq e^{-2t}\},$$

for some appropriate $t > 0$.

Recall the Iwasawa decomposition $G = KAN$ (see 4.18), where $K = \mathrm{SO}(2)$, A is the group of positive diagonal matrices, and N is the group of upper-triangular unipotent matrices. For our

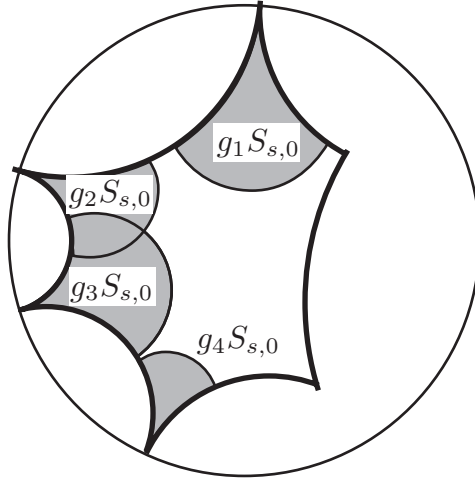


Figure 9.2. For $t = 0$ and s sufficiently large, a finite union (shaded) of translates of the Siegel set $S_{s,0}$ covers the cusps. Increasing t results in a union that contains a fundamental domain (dark outline).

purposes here, it is more convenient to reverse the order of the factors: $G = NAK$. For $s > 0$ and t as above, let

$$N_s = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mid -s \leq x \leq s \right\} \text{ and } A_t = \left\{ \begin{bmatrix} e^y & 0 \\ 0 & e^{-y} \end{bmatrix} \mid y > -t \right\}.$$

Then, as noted in Exer. 9:12, it is not difficult to verify that

$$(9.41) \quad N_{1/2} A_t K = \{ g \in G \mid g(i) \in S_{1/2,t} \}.$$

Thus, if we define the *Siegel set*

$$\mathfrak{S}_{s,t} = N_s A_t K,$$

then $\Gamma \mathfrak{S}_{1/2,t} = G$.

Note that there is some s' , such that $N_s A_t \subset A_t N_{s'}$ (see Exer. 9:13). Thus, $\Gamma \backslash G = \Gamma A_t N_{s'} K$. Since $N_{s'} K$ is compact, and A_t acts by isometries on $\mathfrak{H}^2$, this implies that every point of $\Gamma \backslash \mathfrak{H}^2$ is within a bounded distance of the geodesic ray $A_t i$. From a large distance, this bounded distance becomes negligible, so we perceive only the ray $A_0 i$; thus, the asymptotic cone at ∞ of $\Gamma \backslash \mathfrak{H}^2$ is a single ray.

(9.42) **Example.** Now suppose $G = \mathrm{SL}(2, \mathbb{R})$, but that $\Gamma \backslash \mathfrak{H}^2$ has several cusps, not only one. Then a weak fundamental domain for $\Gamma \backslash \mathfrak{H}^2$ can be obtained by taking a union of (translates of) Siegel sets, one for each cusp:

$$\mathcal{F} = g_1 S_{s,t} \cup \cdots \cup g_r S_{s,t}.$$

From a distance, each of the Siegel sets looks like a ray, so we perceive a finite union of rays. The asymptotic cone at ∞ of $\Gamma \backslash \mathfrak{H}^2$ is a union of r rays.

Proof of Thm. 2.17. The ideas of the preceding two examples generalize to other groups G . Let P be a minimal parabolic $\mathbb{Q}$ -subgroup of G . We may write $P = MAN = NMA$ (see 9.34, and note that A centralizes M). Since P is minimal, we know that $\mathbb{Q}\text{-rank}(M) = 0$ (see 9.35(5)), so there is a compact subset C_M of M , such that $M_{\mathbb{Z}} C_M = M$ (see 9.21). Similarly, there is a compact subset C_N of N , such that $N_{\mathbb{Z}} C_N = N$ (see 9.39); let $C = C_M C_N$.

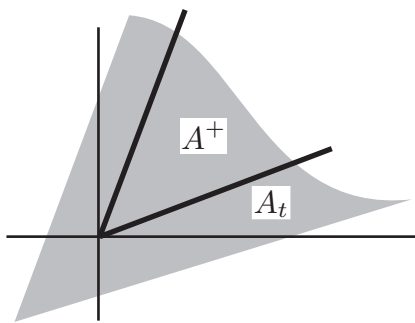


Figure 9.3. The Weyl chamber A^+ and a cone A_t (shaded) when $\dim A = 2$.

If $\mathbb{Q}\text{-rank}(\Gamma) = 1$, the subgroup A is isomorphic to $\mathbb{R}$, and we define A_t to be a ray in A , as in Eg. 9.40 above. In general, the group A is isomorphic to some $\mathbb{R}^d$, where $d = \mathbb{Q}\text{-rank}(\Gamma)$. Then

$$A^+ = \{ a \in A \mid \forall x \in N, \|a^{-1}xa\| \leq \|x\| \}$$

is a polyhedral cone in A (with nonempty interior). (It is called the *positive Weyl chamber*.) We define A_t to be the points of A that are within distance t of this Weyl chamber (see Fig. 9.3).

Define the *Siegel set* $S_{C,t} = CA_tK$. Then, for an appropriate choice of t , one can show that some finite union

$$\mathcal{F} = \cup_{i=1}^r g_i \mathfrak{S}_{C,t}$$

of translates of $\mathfrak{S}_{C,t}$ is a weak fundamental domain for $\Gamma \backslash G$. (Theorem 9.37 implies that only finitely many translates are needed.) Because A centralizes M , the definition of A_t implies that there is a compact subset C' of MN , such that $CA_t \subset A_t C'$ (see Exer. 9:14). Thus, from a large distance, $\mathfrak{S}_{C,t}$ simply looks like A^+ . Therefore, from a large distance $\Gamma \backslash X$ looks like a finite union of translates of A^+ . So the asymptotic cone at ∞ is a d -simplex. $\square$

Since A^+ is a polyhedral cone, the preceding argument shows that the asymptotic cone at ∞ of $\Gamma \backslash X$ is a cone on a certain simplicial complex at ∞ . If $\mathbb{Q}\text{-rank}(\Gamma) = 1$, this simplicial complex consists of finitely many points. We will see in Sect. 14D that if $\mathbb{Q}\text{-rank}(\Gamma) \geq 2$, then this simplicial complex is connected. This leads to the following conclusion.

(9.43) **Theorem.** *The following are equivalent:*

- 1) $\mathbb{Q}\text{-rank}(\Gamma) \geq 2$;
- 2) $\partial(\Gamma \backslash X)$ is infinite;
- 3) $\Gamma \backslash X$ has only one end and $\partial(\Gamma \backslash X)$ has more than one point.

9K. Notes

This hasn't been written yet!!!

The number-theoretic fact (*) mentioned in the proof of Prop. 9.20 can be found in [B–S, Thm. 1 of §1.7 and Thm. 5 of §1.6, pp. 61 and 51] or [S, Cor. 2 of §4.3.2, p. 43].

9L. References

- [B–S] Z. I. Borevich and I. R. Shafarevich: *Number Theory*, Academic Press, New York, 1966.
[S] J.–P. Serre: *A Course in Arithmetic*, Springer, New York 1973.

Exercises

- 9:1) Show that if T is a $\mathbb{Q}$ -split torus, then $T_{\mathbb{Z}}$ is finite.
- 9:2) Give an example of a $\mathbb{Q}$ -torus T , such that $T_{\mathbb{Z}}$ is infinite.
- 9:3) Prove Thm. 9.24. [*Hint:* (1 $\Rightarrow$ 4) Obvious. (4 $\Rightarrow$ 3) Jacobson-Morosov Lemma. (3 $\Rightarrow$ 1) Thm. 9.21(4 $\Rightarrow$ 1). (2 $\Rightarrow$ 3) Obvious. (3 $\Rightarrow$ 2) Jordan decomposition. (3 $\Rightarrow$ 5) Thm. 9.34. (5 $\Rightarrow$ 3) Thm. 9.35(6).]
- 9:4) Suppose B is a quadratic form on $\mathbb{R}^{\ell}$ that is defined over $\mathbb{Q}$. Let $G = \mathrm{SO}(B)$ and $\Gamma = G_{\mathbb{Z}}$. Prove directly (without the Jacobson-Morosov Lemma) that if Γ has a nontrivial unipotent element, then B is isotropic over $\mathbb{Q}$. [*Hint:* If $\gamma v \neq v$, then $\gamma^n v / (\|\gamma^n v\|)$ converges to an isotropic vector.]
- 9:5) Use Restriction of Scalars (see §6G) to construct cocompact arithmetic lattices in $\mathrm{SO}(m, n)$ for all m and n .
- 9:6) Use restriction of scalars (see §6G) to construct cocompact arithmetic lattices in $\mathrm{SU}(m, n)$ and $\mathrm{Sp}(m, n)$ for all m and n .
- 9:7) Show that if $\mathbb{Q}\text{-rank}(\Gamma) = 1$, and U_1 and U_2 are unipotent subgroups of Γ , such that $U_1 \cap U_2 \neq e$, then $\langle U_1, U_2 \rangle$ is unipotent.
- 9:8) Show that if U_1 and U_2 are maximal unipotent subgroups of Γ , and Γ is commensurable with $G_{\mathbb{Z}}$, then there exists $g \in G_{\mathbb{Q}}$, such that $g^{-1}U_1g$ is commensurable with U_2 .
- 9:9) (a) Show that if $\mathbb{Q}\text{-rank}(\Gamma) \geq 2$, then Γ contains a subgroup that is isomorphic to a finite-index subgroup of either $\mathrm{SL}(3, \mathbb{Z})$ or $\mathrm{SL}(2, \mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z})$.
 (b) Show that there is a lattice Γ , in some semisimple group G , such that $\mathbb{Q}\text{-rank}(\Gamma) < 2$, but Γ contains a subgroup that is isomorphic to a finite-index subgroup of $\mathrm{SL}(2, \mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z})$.
- 9:10) Show that if Γ is reducible, and G has no compact factors, then there is a finite subset $\{\gamma_1, \dots, \gamma_r\}$ of Γ , such that
 (a) $\{\gamma_1, \dots, \gamma_r\}$ generates a finite-index subgroup of Γ ,
 (b) each γ_i is nontrivial, and
 (c) γ_i commutes with γ_{i+1} , for each i .
- 9:11) Suppose Γ is infinite and has the property that if γ_1 and γ_2 are any nontrivial elements of Γ , such that γ_1 commutes with γ_2 , then $C_{\Gamma}(\gamma_1) = C_{\Gamma}(\gamma_2)$. Show that it is impossible to find a generating set $\{\gamma_1, \dots, \gamma_r\}$ for Γ , such that each γ_i is nontrivial, and γ_i commutes with γ_{i+1} , for each i .
- 9:12) Verify (9.41). [*Hint:* K fixes i ; elements of A_t move i vertically; and elements of $N_{1/2}$ move points horizontally.]
- 9:13) For N_s and A_t as in Eg. 9.40, show that $N_s A_t \subset A_t N_{e^{2t}s}$.
- 9:14) Define A_t and N as in the pf. of Thm. 2.17. Show that if C is any compact subset of N , then there is a compact subset C' of N , such that $CA_t \subset A_t C'$.

Arithmetic Lattices in Classical Groups

10A. Complexification of G

Intuitively, the *complexification* of G is the complex Lie group that is obtained from G by replacing real numbers with complex numbers. That is, G is (isogenous to) the set of real solutions of a certain set of equations, and we let $G \otimes \mathbb{C}$ be the set of complex solutions of the same set of equations. For example, the complexification of $\mathrm{SL}(n, \mathbb{R})$ is $\mathrm{SL}(n, \mathbb{C})$.

(10.1) **Warning.** The notation may be misleading: the complexification $G \otimes \mathbb{C}$ is **not** a tensor product, because the group G is a nonlinear object. However, this construction does correspond to the usual tensor product at the level of Lie algebras (see Exer. 10:1).

(10.2) **Notation.** Assume $G \subset \mathrm{SL}(\ell, \mathbb{R})$, for some ℓ . There is a subset $\mathcal{Q}$ of $\mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}]$, such that $G = \mathrm{Var}(\mathcal{Q})^\circ$ (see 4.8). Let

$$G \otimes \mathbb{C} = \mathrm{Var}_{\mathbb{C}}(\mathcal{Q}) = \{g \in \mathrm{SL}(\ell, \mathbb{C}) \mid Q(g) = 0, \text{ for all } Q \in \mathcal{Q}\}.$$

Then $G \otimes \mathbb{C}$ is a (complex, semisimple) Lie group.

(10.3) **Example.**

- 1) $\mathrm{SL}(n, \mathbb{R}) \otimes \mathbb{C} = \mathrm{SL}(n, \mathbb{C})$.
- 2) $\mathrm{SO}(n) \otimes \mathbb{C} = \mathrm{SO}(n, \mathbb{C})$.
- 3) $\mathrm{SO}(p, q) \otimes \mathbb{C} \cong \mathrm{SO}(p + q, \mathbb{C})$ (see Exer. 10:2).

(10.4) **Definition.** If $G \otimes \mathbb{C}$ is isomorphic to H , then we say that

- H is the *complexification* of G , and that
- G is a *real form* of H .

From Eg. 10.3(3), we see that a single complex group may have many different real forms.

There is an explicit list of all the complex simple Lie groups (see Fig. 3.2):

(10.5) **Proposition.** *Each simple factor of $G \otimes \mathbb{C}$ is isogenous to either*

- 1) $\mathrm{SL}(n, \mathbb{C})$, for some $n \geq 2$, or

- 2) $\mathrm{SO}(n, \mathbb{C})$, for some $n \geq 5$, with $n \neq 6$, or
- 3) $\mathrm{Sp}(2n, \mathbb{C})$, for some $n \geq 3$, or
- 4) one of the five exceptional complex Lie groups: $E_6(\mathbb{C})$, $E_7(\mathbb{C})$, $E_8(\mathbb{C})$, $F_4(\mathbb{C})$, $G_2(\mathbb{C})$.

Thus, for a classical simple Lie group G , determining the complexification of G is a matter of deciding whether it is special linear, orthogonal, or symplectic, and choosing a value of n . (This determines the type A_ℓ , B_ℓ , C_ℓ , or D_ℓ of G (see Fig. 3.1).) It is not difficult to memorize the correspondence. For example, it is obvious from the notation that the complexification of $\mathrm{Sp}(p, q)$ is symplectic. Indeed, the only case that really requires memorization is the complexification of $\mathrm{SU}(p, q)$ (see 10.6(4)).

(10.6) **Proposition.** *We have*

- 1) $\mathrm{SL}(n, \mathbb{R}) \otimes \mathbb{C} = \mathrm{SL}(n, \mathbb{C})$;
- 2) $\mathrm{SL}(n, \mathbb{C}) \otimes \mathbb{C} = \mathrm{SL}(n, \mathbb{C}) \times \mathrm{SL}(n, \mathbb{C})$;
- 3) $\mathrm{SL}(n, \mathbb{H}) \otimes \mathbb{C} = \mathrm{SL}(2n, \mathbb{C})$;
- 4) $\mathrm{SU}(p, q) \otimes \mathbb{C} = \mathrm{SL}(p + q, \mathbb{C})$;
- 5) $\mathrm{SO}(n, \mathbb{C}) \otimes \mathbb{C} = \mathrm{SO}(n, \mathbb{C}) \times \mathrm{SO}(n, \mathbb{C})$;
- 6) $\mathrm{SO}(n, \mathbb{H}) \otimes \mathbb{C} = \mathrm{SO}(2n, \mathbb{C})$;
- 7) $\mathrm{SO}(p, q) \otimes \mathbb{C} = \mathrm{SO}(p + q, \mathbb{C})$;
- 8) $\mathrm{Sp}(n, \mathbb{R}) \otimes \mathbb{C} = \mathrm{Sp}(n, \mathbb{C})$;
- 9) $\mathrm{Sp}(n, \mathbb{C}) \otimes \mathbb{C} = \mathrm{Sp}(n, \mathbb{C}) \times \mathrm{Sp}(n, \mathbb{C})$; and
- 10) $\mathrm{Sp}(p, q) \otimes \mathbb{C} = \mathrm{Sp}(2(p + q), \mathbb{C})$.

Some parts of this proposition are obvious (see 10.3). A few other examples appear in §10B below, and the methods used there can be applied to all of the cases. In fact, all of the calculations are straightforward adaptations of the examples, except perhaps the calculations for $\mathrm{SO}(n, \mathbb{H}) \otimes \mathbb{C}$ (see Exer. 10:6).

(10.7) **Remark.**

- 1) The Lie algebra of $G \otimes \mathbb{C}$ is the tensor product $\mathfrak{g} \otimes \mathbb{C}$ (see Exer. 10:1). This is independent of the embedding of G in $\mathrm{SL}(\ell, \mathbb{C})$, so, up to isogeny, $G \otimes \mathbb{C}$ is independent of the embedding of G in $\mathrm{SL}(\ell, \mathbb{C})$. Thus, we will often speak of the complexification of G , even if G is not a group of matrices, with the understanding that the complexification is not entirely well defined (see 10.8).
- 2) There is a technical problem in Ntn. 10.2: there may be many different choices of $\mathcal{Q}$ (having the same set of real solutions), and it may be the case that different choices yield different sets of complex solutions. (In fact, a bad choice of $\mathcal{Q}$ can yield a set of complex solutions that is not a group.) To eliminate this problem, we should insist that $\mathcal{Q}$ be maximal; that is,

$$\mathcal{Q} = \{ Q \in \mathbb{R}[x_{1,1}, \dots, x_{\ell,\ell}] \mid Q(g) = 0, \text{ for all } g \in G \}.$$

Then $G \otimes \mathbb{C}$ is the Zariski closure of G (over the field $\mathbb{C}$), from which it follows that $G \otimes \mathbb{C}$, like G , is a semisimple Lie group.

(10.8) **Example.** Because the center of $\mathrm{SL}(3, \mathbb{R})$ is trivial, we see that $\mathrm{SL}(3, \mathbb{R})$ is isomorphic to $\mathrm{PSL}(3, \mathbb{R})^\circ$. On the other hand, we have

$$\mathrm{SL}(3, \mathbb{R}) \otimes \mathbb{C} = \mathrm{SL}(3, \mathbb{C}) \not\cong \mathrm{PSL}(3, \mathbb{C}) = \mathrm{PSL}(3, \mathbb{R})^\circ \otimes \mathbb{C}.$$

This is a concrete illustration of the fact that different embeddings of G can yield different complexifications. Note, however, that $\mathrm{SL}(3, \mathbb{C})$ is isogenous to $\mathrm{PSL}(3, \mathbb{C})$, so the difference between the complexifications is negligible (cf. 10.7(1)).

10B. Calculating the complexification of G

Obviously, $\mathrm{SL}(n, \mathbb{C})$ is a complex Lie group. However, we can think of it as a real Lie group of twice the dimension. As such, it has a complexification, which we now calculate.

(10.9) **Proposition.** $\mathrm{SL}(n, \mathbb{C}) \otimes \mathbb{C} \cong \mathrm{SL}(n, \mathbb{C}) \times \mathrm{SL}(n, \mathbb{C})$.

Proof. We should embed $\mathrm{SL}(n, \mathbb{C})$ as a subgroup of $\mathrm{SL}(2n, \mathbb{R})$, find the corresponding set $\mathcal{Q}$ of defining polynomials, and determine the complex solutions. However, it is more convenient to sidestep some of these calculations by using restriction of scalars, the method described in §6G.

Define $\Delta: \mathbb{C} \rightarrow \mathbb{C} \oplus \mathbb{C}$ by $\Delta(z) = (z, \bar{z})$. Then $\Delta(1) = (1, 1)$ and $\Delta(i) = (i, -i)$ are linearly independent (over $\mathbb{C}$), so they form a basis of $\mathbb{C} \oplus \mathbb{C}$. Thus, $\Delta(\mathbb{C})$ is the $\mathbb{R}$ -span of a basis, so it is a $\mathbb{R}$ -form of $\mathbb{C} \oplus \mathbb{C}$. Therefore, letting $V = \mathbb{C}^{2n}$, we see that

$$V_{\mathbb{R}} = \Delta(\mathbb{C}^n) = \{ (v, \bar{v}) \mid v \in \mathbb{C}^n \}$$

is a real form of V . Let

$$(\mathrm{SL}(n, \mathbb{C}) \times \mathrm{SL}(n, \mathbb{C}))_{\mathbb{R}} = \{ g \in \mathrm{SL}(n, \mathbb{C}) \times \mathrm{SL}(n, \mathbb{C}) \mid g(V_{\mathbb{R}}) = V_{\mathbb{R}} \}.$$

Then we have an isomorphism

$$\tilde{\Delta}: \mathrm{SL}(n, \mathbb{C}) \xrightarrow{\cong} (\mathrm{SL}(n, \mathbb{C}) \times \mathrm{SL}(n, \mathbb{C}))_{\mathbb{R}},$$

defined by $\tilde{\Delta}(g) = (g, \bar{g})$, so

$$\mathrm{SL}(n, \mathbb{C}) \otimes \mathbb{C} \cong (\mathrm{SL}(n, \mathbb{C}) \times \mathrm{SL}(n, \mathbb{C}))_{\mathbb{R}} \otimes \mathbb{C} = \mathrm{SL}(n, \mathbb{C}) \times \mathrm{SL}(n, \mathbb{C}).$$

□

(10.10) **Remark.**

- 1) Generalizing Prop. 10.9, one can show that if G is isogenous to a complex Lie group, then $G \otimes \mathbb{C}$ is isogenous to $G \times G$. For example,

$$\mathrm{SO}(1, 3) \otimes \mathbb{C} \cong \mathrm{SO}(4, \mathbb{C}) \sim \mathrm{SL}(2, \mathbb{C}) \times \mathrm{SL}(2, \mathbb{C}) \sim \mathrm{SO}(1, 3) \times \mathrm{SO}(1, 3)$$

(see (3d) and (3b) of Rem. 3.31).

- 2) From Prop. 10.9, we see that $G \otimes \mathbb{C}$ need not be simple, even if G is simple. However, this only happens when G is complex: if G is simple, and G is not isogenous to a complex Lie group, then $G \otimes \mathbb{C}$ is simple.

Although not stated explicitly there, the proof of Prop. 10.9 is based on the fact that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$. Namely, the map

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \rightarrow \mathbb{C} \oplus \mathbb{C} \text{ defined by } (v, \lambda) \mapsto \Delta(v) \lambda$$

is an isomorphism of $\mathbb{C}$ -algebras. Analogously, the understanding of groups defined from $\mathbb{H}$ will be based on a calculation of $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$.

(10.11) **Lemma.** *The tensor product $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to $\mathrm{Mat}_{2 \times 2}(\mathbb{C})$.*

Proof. Define an $\mathbb{R}$ -linear map $\phi: \mathbb{H} \rightarrow \text{Mat}_{2 \times 2}(\mathbb{C})$ by

$$\phi(1) = \text{Id}, \quad \phi(i) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \phi(j) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \phi(k) = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

It is straightforward to verify that ϕ is an injective ring homomorphism. Furthermore, $\phi(\{1, i, j, k\})$ is a $\mathbb{C}$ -basis of $\text{Mat}_{2 \times 2}(\mathbb{C})$. Therefore, the map $\hat{\phi}: \mathbb{H} \otimes \mathbb{C} \rightarrow \text{Mat}_{2 \times 2}(\mathbb{C})$ defined by $\hat{\phi}(v, \lambda) = \phi(v) \lambda$ is a ring isomorphism (see Exer. 10:3). $\square$

(10.12) **Proposition.** $\text{SL}(n, \mathbb{H}) \otimes \mathbb{C} \cong \text{SL}(2n, \mathbb{C})$.

Proof. From Lem. 10.11, we have

$$\text{SL}(n, \mathbb{H}) \otimes \mathbb{C} \cong \text{SL}(n, \text{Mat}_{2 \times 2}(\mathbb{C})) \cong \text{SL}(2n, \mathbb{C})$$

(see Exers. 10:4 and 10:5). $\square$

As additional examples, let us calculate the complexifications of the classical compact simple Lie groups, namely, $\text{SO}(n)$, $\text{SU}(n)$, and $\text{Sp}(n)$ (see 8.22). As observed in 10.3(2), we have $\text{SO}(n) \otimes \mathbb{C} = \text{SO}(n, \mathbb{C})$. The other cases are not as obvious.

(10.13) **Proposition.** $\text{SU}(n) \otimes \mathbb{C} = \text{SL}(n, \mathbb{C})$.

Proof. Let

- $\sigma: \mathbb{C} \rightarrow \mathbb{C}$,
- $\overrightarrow{\sigma}: \mathbb{C}^n \rightarrow \mathbb{C}^n$, and
- $\tilde{\sigma}: \text{SL}(n, \mathbb{C}) \rightarrow \text{SL}(n, \mathbb{C})$

be the usual complex conjugations $\sigma(z) = \bar{z}$, $\overrightarrow{\sigma}(v) = \bar{v}$, and $\tilde{\sigma}(g) = \bar{g}$. We have

$$\begin{aligned} \text{SU}(n) &= \{ g \in \text{SL}(n, \mathbb{C}) \mid g^* g = \text{Id} \} \\ &= \{ g \in \text{SL}(n, \mathbb{C}) \mid \sigma(g^T) g = \text{Id} \}, \end{aligned}$$

so, in order to calculate $\text{SU}(n) \otimes \mathbb{C}$, we should determine the map $\tilde{\eta}$ on $\text{SL}(n, \mathbb{C}) \times \text{SL}(n, \mathbb{C})$ that corresponds to $\tilde{\sigma}$ when we identify $\mathbb{C}^n$ with $(\mathbb{C}^n \otimes \mathbb{C}^n)_{\mathbb{R}}$ under the map $\overrightarrow{\Delta}$.

First, let us determine $\overrightarrow{\eta}$. That is, we wish to identify $\mathbb{C}^n$ with $\mathbb{R}^{2n}$, and extend $\overrightarrow{\sigma}$ to a $\mathbb{C}$ -linear map on $\mathbb{C}^{2n}$. However, as usual, we use the $\mathbb{R}$ -form $\overrightarrow{\Delta}(\mathbb{C}^n)$, in place of $\mathbb{R}^{2n}$. It is obvious that if we define $\overrightarrow{\eta}: \mathbb{C}^n \oplus \mathbb{C}^n \rightarrow \mathbb{C}^n \oplus \mathbb{C}^n$ by $\overrightarrow{\eta}(x, y) = (y, x)$, then $\overrightarrow{\eta}$ is $\mathbb{C}$ -linear, and the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C}^n & \xrightarrow{\overrightarrow{\Delta}} & \mathbb{C}^n \oplus \mathbb{C}^n \\ \downarrow \overrightarrow{\sigma} & & \downarrow \overrightarrow{\eta} \\ \mathbb{C}^n & \xrightarrow{\overrightarrow{\Delta}} & \mathbb{C}^n \oplus \mathbb{C}^n. \end{array}$$

Thus, it is fairly clear that $\tilde{\eta}(g, h) = (h, g)$. Hence

$$\begin{aligned} \text{SU}(n) \otimes \mathbb{C} &= \{ (g, h) \in \text{SL}(n, \mathbb{C}) \times \text{SL}(n, \mathbb{C}) \mid \tilde{\eta}(g^T, h^T)(g, h) = (\text{Id}, \text{Id}) \} \\ &= \{ (g, h) \in \text{SL}(n, \mathbb{C}) \times \text{SL}(n, \mathbb{C}) \mid (h^T, g^T)(g, h) = (\text{Id}, \text{Id}) \} \\ &= \{ (g, (g^T)^{-1}) \mid g \in \text{SL}(n, \mathbb{C}) \} \\ &\cong \text{SL}(n, \mathbb{C}), \end{aligned}$$

as desired. $\square$

(10.14) **Proposition.** $\mathrm{Sp}(n) \otimes \mathbb{C} = \mathrm{Sp}(2n, \mathbb{C})$.

Proof. Let

- $\phi: \mathbb{H} \hookrightarrow \mathrm{Mat}_{2 \times 2}(\mathbb{C})$ be the embedding described in the proof of Lem. 10.11;
- τ be the usual conjugation on $\mathbb{H}$,
- $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, and
- $\eta: \mathrm{Mat}_{2 \times 2}(\mathbb{C}) \rightarrow \mathrm{Mat}_{2 \times 2}(\mathbb{C})$ be defined by $\eta(x) = J^{-1}x^T J$.

Then η is $\mathbb{C}$ -linear, and the following diagram commutes:

$$\begin{array}{ccc} \mathbb{H} & \xrightarrow{\phi} & \mathrm{Mat}_{2 \times 2}(\mathbb{C}) \\ \downarrow \tau & & \downarrow \eta \\ \mathbb{H} & \xrightarrow{\phi} & \mathrm{Mat}_{2 \times 2}(\mathbb{C}). \end{array}$$

Thus, because

$$\begin{aligned} \mathrm{Sp}(2) &= \{ g \in \mathrm{SL}(2, \mathbb{H}) \mid g^* g = \mathrm{Id} \} \\ &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathbb{H}) \mid \begin{bmatrix} \tau(a) & \tau(c) \\ \tau(b) & \tau(d) \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \mathrm{Id} \right\}, \end{aligned}$$

we see that

$$\begin{aligned} \mathrm{Sp}(2) \otimes \mathbb{C} &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathrm{Mat}_{2 \times 2}(\mathbb{C})) \mid \begin{bmatrix} \eta(a) & \eta(c) \\ \eta(b) & \eta(d) \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \mathrm{Id} \right\} \\ &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathrm{Mat}_{2 \times 2}(\mathbb{C})) \mid J^{-1} \begin{bmatrix} a^T & c^T \\ b^T & d^T \end{bmatrix} J \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \mathrm{Id} \right\} \\ &= \{ g \in \mathrm{SL}(4, \mathbb{C}) \mid J^{-1} g^T J g = \mathrm{Id} \} \\ &= \{ g \in \mathrm{SL}(4, \mathbb{C}) \mid g^T J g = J \} \\ &= \mathrm{Sp}(4, \mathbb{C}). \end{aligned}$$

Similarly, letting

$$\hat{J}_n = \begin{bmatrix} J & & & \\ & J & & \\ & & \ddots & \\ & & & J \end{bmatrix} \in \mathrm{SL}(2n, \mathbb{C}),$$

the same calculations show that

$$\mathrm{Sp}(n) \otimes \mathbb{C} = \{ g \in \mathrm{SL}(2n, \mathbb{C}) \mid g^T \hat{J}_n g = \hat{J}_n \} \cong \mathrm{Sp}(2n, \mathbb{C}).$$

□

10C. Cocompact lattices in some classical groups

In this section, we construct cocompact lattices in some classical simple groups. This introduces some of the ideas that will be used in the following section, where we will show that every classical group has a cocompact lattice. (In Chap. 13, we will give proofs that also apply to exceptional groups.)

Let us begin by briefly recalling the prototypical case (cf. 6.45).

(10.15) **Proposition.** $\mathrm{SO}(p, q)$ has a cocompact, arithmetic lattice.

Proof. Let

- $F = \mathbb{Q}(\sqrt{2})$,
- σ be the Galois automorphism of F over $\mathbb{Q}$,
- $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$,
- $B(x, y) = \sum_{j=1}^p x_j y_j - \sqrt{2} \sum_{j=1}^q x_{p+j} y_{p+j}$, for $x, y \in F^{p+q}$,
- $G = \mathrm{SO}(B)^\circ$,
- $\Gamma = G_{\mathcal{O}}$, and
- $\Delta: G_F \rightarrow G \times G^\sigma$ defined by $\Delta(g) = (g, \sigma(g))$.

We know (from Restriction of Scalars) that $\Delta(\Gamma)$ is an irreducible, arithmetic lattice in $G \times G^\sigma$ (see 6.49). Since $G^\sigma \cong \mathrm{SO}(p+q)$ is compact, we may mod it out, to conclude that Γ is an arithmetic lattice in $G \cong \mathrm{SO}(p, q)^\circ$. Also, since G^σ is compact, we know that Γ is cocompact (see 6.50). $\square$

(10.16) **Proposition.** $\mathrm{SU}(p, q)$ has a cocompact, arithmetic lattice.

Proof. Let

- $F = \mathbb{Q}(\sqrt{2})$,
- $L = F[i] = \mathbb{Q}(\sqrt{2}, i)$,
- τ be the usual complex conjugation (that is, the Galois automorphism of L over F),
- σ be the Galois automorphism of F over $\mathbb{Q}$, so $S_\infty = \{\mathrm{Id}, \sigma\}$,
- $\mathcal{O} = \mathbb{Z}[\sqrt{2}, i]$,
- $B(x, y) = \sum_{j=1}^p x_j \tau(y_j) - \sqrt{2} \sum_{j=1}^q x_{p+j} \tau(y_{p+j})$, for $x, y \in L^{p+q}$,
- $G = \{g \in \mathrm{SL}(p+q, \mathbb{C}) \mid B(gx, gy) = B(x, y), \text{ for all } x, y \in \mathbb{C}^{p+q}\} \cong \mathrm{SU}(p, q)$, and
- $\Gamma = G_{\mathcal{O}}$.

Since $G^\sigma \cong \mathrm{SU}(p+q)$ is compact, we see that Γ is a cocompact, arithmetic lattice in G . $\square$

The same argument can easily be applied to $\mathrm{Sp}(p, q)$ (see Exer. 10:25). Let us see that it also applies to $\mathrm{SL}(n, \mathbb{R})$. First, we introduce some useful notation.

(10.17) **Remark.** In order to specify a group G that is defined over F , it suffices to specify G_F . Because G_F is dense in G (cf. 6.8), this does determine G uniquely.

Recall that the complexification $G \otimes \mathbb{C}$ is obtained by replacing real numbers with complex numbers. Analogously, if G is defined over F , then, for any field L containing F , we may replace elements of F with elements of L ; the resulting group is denoted $G_F \otimes_F L$.

(10.18) **Definition** (cf. 10.2 and 10.7(2)). • For any subfield L of $\mathbb{C}$ and any subset $\mathcal{Q}$ of $L[x_{1,1}, \dots, x_{\ell,\ell}]$, let

$$\mathrm{Var}_L(\mathcal{Q}) = \{g \in \mathrm{SL}(\ell, L) \mid Q(g) = 0, \forall Q \in \mathcal{Q}\}.$$

- We say that G is *defined over F* (as an algebraic group over F_∞) if there is a subset $\mathcal{Q}$ of $F[x_{1,1}, \dots, x_{\ell,\ell}]$, such that $G = \mathrm{Var}_{F_\infty}(\mathcal{Q})^\circ$.
- If G is *defined over F* (as an algebraic group over F_∞), and L is any subfield of $\mathbb{C}$ that contains F , then we define

$$G_F \otimes_F L = \mathrm{Var}_L(\mathcal{Q}),$$

where

$$\mathcal{Q} = \{Q \in F[x_{1,1}, \dots, x_{\ell,\ell}] \mid Q(G_F) = 0\}.$$

(10.19) **Proposition.** $\mathrm{SL}(n, \mathbb{R})$ has a cocompact, arithmetic lattice.

Proof. Let

- $F = \mathbb{Q}(\sqrt{2})$,
- $L = F[\sqrt[4]{2}] = \mathbb{Q}[\sqrt[4]{2}]$,
- τ be the Galois automorphism of L over F ,
- $\mathcal{O} = \mathbb{Z}[\sqrt[4]{2}]$,
- $B(x, y) = \sum_{j=1}^n x_j \tau(y_j)$, for $x, y \in L^n$,
- $G_F = \mathrm{SU}(B; L, \tau)$, and
- $\Gamma = G_{\mathcal{O}}$.

Let σ be the Galois automorphism of F over $\mathbb{Q}$, and extend σ to an embedding of L in $\mathbb{C}$. Note that $\sigma(L)$ is an **imaginary** extension of F (because the square root of $\sigma(\sqrt{2}) = -\sqrt{2}$ is imaginary), but $\sigma(F) = F$ is real. This implies that the Galois automorphism of $\sigma(L)$ over $\sigma(F)$ is the usual complex conjugation, so $B^{\sigma}(x, y) = \sum_{j=1}^n x_j \overline{y_j}$ for $x, y \in \mathbb{C}^n$. Therefore $G^{\sigma} \cong \mathrm{SU}(n)$ is compact, so Γ is a cocompact, arithmetic lattice in G .

Since $F_{\infty} = \mathbb{R}$, we have $G_F \otimes_F \mathbb{R} \approx G$ (see Exer. 10:8). On the other hand, because $L \subset \mathbb{R}$, the proof of Prop. 10.13 shows that $G_F \otimes_F \mathbb{R} \cong \mathrm{SL}(n, \mathbb{R})$ (see Exer. 10:9). Hence $G \approx \mathrm{SL}(n, \mathbb{R})$, so Γ is a cocompact lattice in $\mathrm{SL}(n, \mathbb{R})$. $\square$

In general, to prove that a simple group G has a cocompact, arithmetic lattice, let K be the compact form of G (that is, the compact group of the same type (A_n , B_n , C_n or D_n) as G), and show that $G \times K$ has an irreducible, arithmetic lattice. Since the choice of K implies that $G \times K$ is isotypic, this is a special case of the results in the following section (if G is classical).

10D. Isotypic classical groups have irreducible lattices

(10.20) **Proposition.** *Every isotypic classical group has an irreducible, arithmetic lattice.*

In Chap. 12, we will remove the restriction to classical groups.

Before proving the proposition, let us note that irreducible lattices are often cocompact. (The restriction to arithmetic lattices cannot be omitted (see Exer. 10:7).)

(10.21) **Proposition.** *Suppose $G \subset \mathrm{SL}(\ell, \mathbb{R})$, and G is defined over $\mathbb{Q}$. If at least one of the simple factors of G is compact, and $G_{\mathbb{Z}}$ is a irreducible lattice in G , then $G_{\mathbb{Z}}$ is cocompact.*

Proof. Every irreducible, arithmetic lattice can be constructed by restriction of scalars (see 6.54), so this is the assertion of Cor. 6.50. Alternatively, the proof of Cor. 9.22 provides an argument that does not rely on restriction of scalars. $\square$

(10.22) **Corollary.** *If G is isotypic, then G has a cocompact, irreducible, arithmetic lattice.*

Proof. Choose a compact simple Lie group K , such that $G \times K$ is isotypic. Proposition 10.20 (or the generalization in Chap. 12 if G is not classical) implies that $G \times K$ has an irreducible, arithmetic lattice Γ' . The compact factor K implies that Γ' is cocompact (see 10.21). By modding out K , we obtain a cocompact, irreducible, arithmetic lattice in G . $\square$

(10.23) **Corollary.** *G has a cocompact, arithmetic lattice.*

Proof. We may assume G is simple. (If Γ_1 and Γ_2 are cocompact, arithmetic lattices in G_1 and G_2 , then $\Gamma_1 \times \Gamma_2$ is a cocompact, arithmetic lattice in $G_1 \times G_2$.) Then G is isotypic, so Cor. 10.22 applies. $\square$

Let us begin the proof of Prop. 10.20 with a simple example.

(10.24) **Proposition.** $H = \mathrm{SO}(2, 3) \times \mathrm{SO}(1, 4) \times \mathrm{SO}(1, 4) \times \mathrm{SO}(5)$ has an irreducible, arithmetic lattice.

Proof. Let

- $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$,
- $\mathcal{O} = \mathbb{Z}(\sqrt{2}, \sqrt{3})$,
- $\alpha = \sqrt{2} + \sqrt{3}$,
- $S_\infty = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, with

$$\sigma_1(\alpha) = \sqrt{2} + \sqrt{3} \approx 3.1$$

$$\sigma_2(\alpha) = -\sqrt{2} + \sqrt{3} \approx 0.3$$

$$\sigma_3(\alpha) = \sqrt{2} - \sqrt{3} \approx -0.3$$

$$\sigma_4(\alpha) = -\sqrt{2} - \sqrt{3} \approx -3.1,$$

- $G = \mathrm{SO}((\alpha + 2)x_1^2 + (\alpha - 2)x_2^2 + (\alpha - 4)x_3^2 + (\alpha - 4)x_4^2 + (\alpha - 4)x_5^2)^\circ$, and
- $\Gamma = G_\mathcal{O}$.

Then Restriction of Scalars implies that Γ is an irreducible, arithmetic lattice in $\prod_{\sigma \in S_\infty} G^\sigma$ (see 6.49). Since

$$\sigma_1(\alpha + 2, \alpha - 2, \alpha - 4, \alpha - 4, \alpha - 4) \approx (5.1, 1.1, -0.9, -0.9, -0.9) \sim (+, +, -, -, -)$$

$$\sigma_2(\alpha + 2, \alpha - 2, \alpha - 4, \alpha - 4, \alpha - 4) \approx (2.3, -1.7, -3.7, -3.7, -3.7) \sim (+, -, -, -, -)$$

$$\sigma_3(\alpha + 2, \alpha - 2, \alpha - 4, \alpha - 4, \alpha - 4) \approx (1.7, -2.3, -4.3, -4.3, -4.3) \sim (+, -, -, -, -)$$

$$\sigma_4(\alpha + 2, \alpha - 2, \alpha - 4, \alpha - 4, \alpha - 4) \approx (-1.1, -5.1, -7.1, -7.1, -7.1) \sim (-, -, -, -, -),$$

we have $\prod_{\sigma \in S_\infty} G^\sigma \approx H$. $\square$

The same elementary method applies to any product of various groups of the form $\mathrm{SO}(p, q)$.

(10.25) **Proposition.** If $p_1, \dots, p_r$ are natural numbers with $0 \leq p_j \leq n$, then

$$\prod_{j=1}^r \mathrm{SO}(p_j, n - p_j)$$

has an irreducible, arithmetic lattice.

Proof. There is no harm in adding several copies of the compact factor $\mathrm{SO}(n)$, so we may assume that $r = 2^t$ is a power of 2. Also, we may assume that

$$p_1 \geq p_2 \geq \dots \geq p_r.$$

Let

- $m_1, \dots, m_t \geq 2$ be square-free positive integers that are pairwise relatively prime;
- $F = \mathbb{Q}(\sqrt{m_1}, \dots, \sqrt{m_t})$,
- $\mathcal{O} = \mathbb{Z}(\sqrt{m_1}, \dots, \sqrt{m_t})$,

- $\alpha = \sqrt{m_1} + \cdots + \sqrt{m_t}$,
- $S_\infty = \{\sigma_1, \dots, \sigma_r\}$, with $\sigma_1(\alpha) > \sigma_2(\alpha) > \cdots > \sigma_r(\alpha)$,
- $a_\ell \in \mathbb{Q}$ with $\max\{\sigma_j(\alpha) \mid \ell > p_j\} < a_\ell < \min\{\sigma_j(\alpha) \mid \ell \leq p_j\}$, for $\ell = 1, \dots, n$,
- $G = \mathrm{SO}(\sum_{\ell=1}^n (\alpha - a_\ell)x_\ell^2)$, and
- $\Gamma = G_{\mathcal{O}}$.

From the choice of a_ℓ , we have $\sigma_j(\alpha - a_\ell) > 0$ if and only if $\ell \leq p_j$. Hence, $G^{\sigma_j} \cong \mathrm{SO}(p_j, n - p_j)$. $\square$

Let us also give a more abstract version of the proof that generalizes more easily. It relies on two basic facts of Algebraic Number Theory.

The first is a special case of the Weak Approximation Theorem.

(10.26) **Lemma.** *If F is any algebraic number field, then $\Delta(F)$ is dense in $\bigoplus_{\sigma \in S_\infty} F_\sigma$.*

Proof. This follows from Exer. 6:27, which states that $\Delta(F)$ is a $\mathbb{Q}$ -form of $\bigoplus_{\sigma \in S_\infty} F_\sigma$. $\square$

(10.27) **Lemma.** *For any natural numbers r and s , not both 0, there is an algebraic number field F with exactly r real places and exactly s imaginary places.*

Proof. Let $n = r + 2s$. It suffices to find an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree n , such that $f(x)$ has exactly r real roots. (Then we may let $F = \mathbb{Q}(\alpha)$, where α is any root of $f(x)$.)

Choose a monic polynomial $g(x) \in \mathbb{Z}[x]$, such that

- $g(x)$ has degree n ,
- $g(x)$ has exactly r real roots, and
- all of the real roots of $g(x)$ are simple.

(For example, choose distinct integers $a_1, \dots, a_r$, and let $g(x) = (x - a_1) \cdots (x - a_r)(x^{2s} + 1)$.)

Fix a prime p . Replacing $g(x)$ with $k^n g(x/k)$, for an appropriate integer k , we may assume

- 1) $g(x) \equiv x^n \pmod{p^2}$, and
- 2) $\min\{g(t) \mid g'(t) = 0\} > p$

(see Exer. 10:31).

Let $f(x) = g(x) - p$. From (1), we know that $f(x) \equiv x^n - p \pmod{p^2}$, so the Eisenstein Criterion (I.57) implies that f is irreducible. From (2), we see that $f(x)$, like $g(x)$, has exactly r real roots (see Fig. 10.1). $\square$

Conceptual proof of Prop. 10.25.

- Let F be a totally real algebraic number field of degree r over $\mathbb{Q}$; that is, F has exactly r real places and no imaginary places (see 10.27).
- For $j = 1, \dots, r$ and $\ell = 1, \dots, n$, define $\varepsilon_\ell^j = \begin{cases} + & \text{if } \ell \leq p_j \\ - & \text{if } \ell > p_j. \end{cases}$
- Because $\Delta(F)$ is dense in $\bigoplus_{\sigma \in S_\infty} F_\sigma$ (see 10.26), we may choose, for each $\ell = 1, \dots, n$, some $a_\ell \in F$, such that the sign (positive or negative) of $\sigma_j(a_\ell)$ is ε_ℓ^j for $j = 1, \dots, r$.
- Then the signature of $\sigma_j(\sum_{\ell=1}^n a_\ell x_\ell^2)$ is $(p_j, n - p_j)$, for $j = 1, \dots, r$.

$\square$

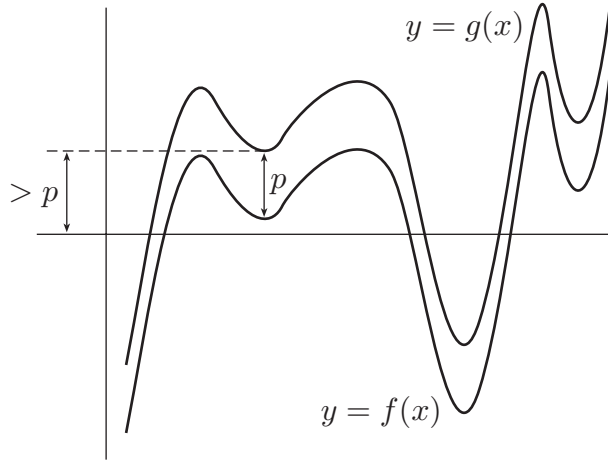


Figure 10.1. The polynomials $f(x)$ and $g(x)$ have the same number of real roots.

By requiring F to have precisely s imaginary places, along with r real places, the above conceptual proof can easily be extended to show, for any natural number s , that there is an irreducible, arithmetic lattice in

$$(10.28) \quad \mathrm{SO}(n, \mathbb{C})^s \times \prod_{j=1}^r \mathrm{SO}(p_j, n - p_j)$$

(see Exer. 10:10). Hence, every isotypic group of type B_ℓ has an irreducible, arithmetic lattice.

Now let us show that every isotypic group of type D_n has an irreducible lattice. Many such groups are of the form (10.28). All that remains is the case where the group has at least one simple factor that is isogenous to $\mathrm{SO}(n, \mathbb{H})$. This requires some understanding of unitary groups over quaternion algebras $D_{\beta, \gamma}(F)$ (see Defn. 7.55).

(10.29) **Lemma.** *If*

- β is any nonzero element of an algebraic number field F ,
- $D = D_{\beta, -1}(F)$, and
- B is a nondegenerate τ_r -Hermitian form on D^n ,

then

$$\mathrm{SU}(B; D, \tau_r) \otimes_F F_\infty \cong \begin{cases} \mathrm{SO}(2n, \mathbb{C}) & \text{if } F_\infty = \mathbb{C}, \\ \mathrm{SO}(p, 2n - p) \text{ (for some } p) & \text{if } F_\infty = \mathbb{R} \text{ and } \beta > 0, \\ \mathrm{SO}(n, \mathbb{H}) & \text{if } F_\infty = \mathbb{R} \text{ and } \beta < 0. \end{cases}$$

Proof. One case is fairly obvious: if $F_\infty = \mathbb{R}$ and $\beta < 0$, then

$$\mathrm{SU}(B; D, \tau_r) \otimes_F F_\infty \cong \mathrm{SU}(B; D \otimes_F \mathbb{R}, \tau_r) \cong \mathrm{SU}(B; \mathbb{H}, \tau_r) \cong \mathrm{SU}(\mathrm{Id}_{n \times n}; \mathbb{H}, \tau_r) = \mathrm{SO}(n, \mathbb{H}).$$

The other cases are completely analogous to the calculation that $\mathrm{SO}(n, \mathbb{H}) \otimes \mathbb{C} \cong \mathrm{SO}(2n, \mathbb{C})$ (see Exer. 10:6). The key point is to verify that $X \mapsto X^T$ is the F_∞ -linear map on $\mathrm{Mat}_{2 \times 2}(F_\infty)$ that corresponds to the antiinvolution τ_r . $\square$

It is now easy to prove that isotypic groups of type D_n have irreducible lattices.

(10.30) **Proposition.** *If $p_1, \dots, p_r$ are natural numbers with $0 \leq p_j \leq 2n$, and s and t are any natural numbers, then*

$$\mathrm{SO}(n, \mathbb{H})^t \times \mathrm{SO}(2n, \mathbb{C})^s \times \prod_{j=1}^r \mathrm{SO}(p_j, 2n - p_j)$$

has an irreducible, arithmetic lattice.

Proof.

- Let F be an algebraic number field with exactly $r + t$ real places $\sigma_1, \dots, \sigma_{r+t}$ and exactly s imaginary places (see 10.27).
 - Because $\Delta(F)$ is dense in $\bigoplus_{\sigma \in S_\infty} F_\sigma$ (see 10.26), there is some nonzero $\beta \in F$, such that
 - $\sigma(\beta) \notin \mathbb{R}$, for each imaginary place σ , and
 - $\sigma_j(\beta) < 0$ if and only if $r + 1 \leq j \leq r + t$.
 - Let
 - $D = D_{\beta, -1}(F)$,
 - $D^\dagger = \{x \in D \mid \tau_r(x) = x\}$,
 - $\mathrm{diag}_n(D^\dagger)$ be the set of $n \times n$ diagonal matrices with entries in $D^\dagger$,
 - $\mathrm{Mat}_{2 \times 2}(\mathbb{R})^\dagger = \{X \in \mathrm{Mat}_{2 \times 2}(\mathbb{R}) \mid X^T = X\}$, and
 - $\mathrm{diag}_n(\mathrm{Mat}_{2 \times 2}(\mathbb{R})^\dagger)$ be the set of $n \times n$ diagonal matrices with entries in $\mathrm{Mat}_{2 \times 2}(\mathbb{R})^\dagger$.
- For $j = 1, \dots, r$, we have $\sigma_j(\beta) > 0$ and $F_{\sigma_j} = \mathbb{R}$, so

$$D_{\sigma_j(\beta), -1}(\sigma_j(F)) \otimes_{\sigma(F_j)} F_{\sigma_j} \cong \mathrm{Mat}_{2 \times 2}(\mathbb{R});$$

hence, σ_j induces an embedding

$$\sigma'_j: D \hookrightarrow \mathrm{Mat}_{2 \times 2}(\mathbb{R}),$$

with $\sigma'_j(D^\dagger) \subset \mathrm{Mat}_{2 \times 2}(\mathbb{R})^\dagger$. Because $\Delta(F)$ is dense in $\bigoplus_{\sigma \in S_\infty} F_\sigma$, we see that

$$\{(\sigma'_j(B))_{j=1}^r \mid B \in \mathrm{diag}_n(D^\dagger)\} \text{ is dense in } \prod_{j=1}^r \mathrm{diag}_n(\mathrm{Mat}_{2 \times 2}(\mathbb{R})^\dagger),$$

so we may choose $B \in \mathrm{diag}_n(D^\dagger)$, such that the signature of $\sigma'_j(B)$, thought of as a $2n \times 2n$ real symmetric matrix, is $(p_j, 2n - p_j)$, for each $j = 1, \dots, r$.

- From Lem. 10.29, we see that $\prod_{\sigma \in S_\infty} \mathrm{SU}(B; D, \tau_r) \cong H$.

□

Fairly similar considerations apply to the other classical groups (that is, of type A_n or C_n), but we omit the details.

The following example shows that the converse of Prop. 10.21 is false, even under the assumption that G is isotypic. The proof relies on material from later in the chapter.

(10.31) **Proposition.** *Every irreducible lattice in $\mathrm{SO}(1, 5) \times \mathrm{SO}(3, \mathbb{H})$ is cocompact.*

Proof. Suppose Γ is an irreducible lattice in $G = \mathrm{SO}(1, 5) \times \mathrm{SO}(3, \mathbb{H})$, such that $\Gamma \backslash G$ is **not** compact. This will lead to a contradiction.

The Margulis Arithmeticity Theorem (6.21) implies that Γ is arithmetic, so Prop. 6.54 implies that Γ can be obtained by restriction of scalars: there exist

- an algebraic number field $F \subset \mathbb{R}$,
- a connected, simple subgroup H of $\mathrm{SL}(\ell, F_\infty)$, for some ℓ , such that
 - H is isogenous to $\mathrm{SO}(3, \mathbb{H})$, and

- H is defined over F , and
- a continuous surjection

$$\phi: \prod_{\sigma \in S^\infty} H^\sigma \rightarrow G,$$

with compact kernel,

such that $\phi(\Delta(H_\mathcal{O}))$ is commensurable with Γ .

From the classification of arithmetic lattices (see Fig. 10.2 on p. 153), we see that (after replacing H by an isogenous group) the group H must be described in 10.48(5): there is a quaternion algebra D over F (such that D is a central simple division algebra), and a Hermitian form B on D^3 , such that $H_F = \mathrm{SU}(B; D, \tau_r)$.

Now, because G/Γ is not compact, we have $\mathbb{Q}\text{-rank}(\Gamma) \geq 1$ (see 9.21), so there must be a nontrivial isotropic vector v in D^3 (see Fig. 10.2 on p. 153). We know, from Prop. 10.70(2), that there is a basis of D^3 , for which the matrix of B is

$$[B] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & p \end{bmatrix},$$

for some $p \in D$ (see Exer. 10:13). Thus, we may assume

$$H_F = \mathrm{SU}([B]; D, \tau_r).$$

There is some $\sigma \in S^\infty$, such that H^σ is isogenous to $\mathrm{SO}(1, 5)$. Then $D^\sigma \otimes_{\sigma(F)} \mathbb{R}$ is isomorphic to $\mathrm{Mat}_{2 \times 2}(\mathbb{R})$ (see 10.55(5)). Since $\mathrm{Id}_{2 \times 2}$ is the image of $1 \in D$ under the isomorphism $D \otimes_F \mathbb{R} \rightarrow \mathrm{Mat}_{2 \times 2}(\mathbb{R})$, we see that

$$H^\sigma = \mathrm{SU}(\sigma([B]); D^\sigma \otimes_{\sigma(F)} \mathbb{R}) \cong \mathrm{SO} \left(\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * & * \end{bmatrix} \right).$$

Thus, H^σ is isomorphic to either $\mathrm{SO}(2, 4)$ or $\mathrm{SO}(3, 3)$; it is not isogenous to $\mathrm{SO}(1, 5)$. This is a contradiction. $\square$

10E. What is a central division algebra over F ?

The list of classical simple Lie groups includes groups, such as $\mathrm{SL}(n, \mathbb{H})$, that are based on the quaternions. Analogously, the list of simple groups over an algebraic number field F includes groups, such as $\mathrm{SL}(n, D)$, that are based on central division algebras over F . In this section, we provide some basic information on central division algebras and the associated unitary groups. For most of our purposes, it suffices to have some familiarity with the special case of quaternion algebras (see 7.55 and 10.35(3)). The interested reader can find a more substantial introduction to the theory of central division algebras (including how to construct them) in Chap. 11.

(10.32) **Definition.** An associative ring D is a *central division algebra* over a field F if

- 1) D contains F as a subring,
- 2) the element $1 \in F$ is the identity element of D ,

3) F is the center of D ; that is,

$$F = \{ z \in D \mid \forall x \in D, \, xz = zx \},$$

4) $\dim_F D < \infty$, and

5) every nonzero element of D has a multiplicative inverse.

(10.33) **Remark.**

- D is an *algebra* over F if (1) and (2) hold, and F is contained in the center of D .
- The word *central* requires the center of D to be exactly F , not some larger field.
- Although not all authors agree with this terminology, we also use *central* to include (4). We have no need for infinite-dimensional algebras.
- The word *division* requires (5).
- We consider only associative algebras here, but the algebra of octonions, which is nonassociative, also arises in the theory of arithmetic groups (cf. 8.28).

(10.34) **Other terminology.** Division algebras are sometimes called *skew fields* or *division rings*.

(10.35) **Example.**

- 1) Any field F is a central division algebra over itself.
- 2) $\mathbb{H} = D_{-1,-1}(\mathbb{R})$ is a central division algebra over $\mathbb{R}$.
- 3) A quaternion algebra $D_{\beta,\gamma}(F)$ is a central division algebra over F if and only if $N_{\text{red}}(x) \neq 0$, for every nonzero $x \in D_{\beta,\gamma}(F)$ (see Exer. 10:21). Note that this is consistent with (2).

(10.36) **Definition.** Let D be a central division algebra. A map $\tau: D \rightarrow D$ is an *antiinvolution* if $\tau^2 = \text{Id}$ and τ is an **anti**-automorphism; that is, $\tau(x + y) = \tau(x) + \tau(y)$ and $\tau(xy) = \tau(y)\tau(x)$. (Note that τ reverses the order of the factors in a product.)

(10.37) **Other terminology.** Some authors call τ an involution, rather than an antiinvolution, but, to avoid confusion, we wish to emphasize the fact that τ is *not* an automorphism (unless D is commutative).

(10.38) **Example.** Let D be a quaternion division algebra. Then

- 1) The map $\tau_c: D \rightarrow D$ defined by

$$\tau_c(a + bi + cj + dk) = a - bi - cj - dk$$

is an antiinvolution. It is called the *standard antiinvolution* of D , or the *conjugation* on D .

- 2) The map $\tau_r: D \rightarrow D$ defined by

$$\tau_r(a + bi + cj + dk) = a + bi - cj + dk$$

is an antiinvolution. It is called the *reversion* on D .

(10.39) **Definition.**

- 1) Let τ be an antiinvolution of a central division algebra D over F . A *Hermitian form* (or, more precisely, a τ -*Hermitian form*) on D^n is a map $B: D^n \times D^n \rightarrow D$, such that
 - $B(x_1 + x_2, y) = B(x_1, y) + B(x_2, y)$ and $B(x, y_1 + y_2) = B(x, y_1) + B(x, y_2)$, for all $x, x_1, x_2, y, y_1, y_2 \in D^n$,
 - $B(ax, y) = aB(x, y)$ and $B(x, ay) = B(x, y)\tau(a)$ for all $a \in D$ and $x, y \in D^n$, and
 - $B(y, x) = \tau(B(x, y))$ for all $x, y \in D^n$.

- 2) The Hermitian form B is *nondegenerate* if, for each nonzero $x \in D^n$, there exists $y \in D^n$, such that $B(x, y) \neq 0$.

The following lemma provides an analogue, for a central division algebra D , of the ring of integers in an algebraic number field F .

(10.40) **Lemma.** *If D is a central division algebra over an algebraic number field F , then there is a subring $\mathcal{O}_D$ of D , such that $\mathcal{O}_D$ is a vector-space lattice in D .*

Proof. Let $\{v_0, v_1, \dots, v_r\}$ be a basis of D over $\mathbb{Q}$, with $v_0 = 1$. Let $\{c_{j,k}^\ell\}_{j,k,\ell=0}^r$ be the structure constants of D with respect to this basis. That is, for $j, k \in \{0, \dots, r\}$, we have

$$v_j v_k = \sum_{\ell=0}^r c_{j,k}^\ell v_\ell.$$

There is some nonzero $m \in \mathbb{Z}$, such that $mc_{j,k}^\ell \in \mathbb{Z}$, for all j, k, ℓ . Let $\mathcal{O}_D$ be the $\mathbb{Z}$ -span of $\{1, mv_1, \dots, mv_r\}$. $\square$

(10.41) **Definition.** Suppose D is a central division algebra over a field F , and L is some extension field of F . We say that D *splits* over L if $D \otimes_F L \cong \text{Mat}_{d \times d}(L)$, for some natural number d . In this case, we call d the *degree* of D , and we have $\dim_F D = d^2$ (because $\dim_L(D \otimes_F L) = d^2$).

Every central division algebra splits over some extension of F :

(10.42) **Proposition.** *If D is a central division algebra over a subfield F of $\mathbb{C}$, then D splits over $\mathbb{C}$.*

In fact, D splits over a much smaller field than $\mathbb{C}$ (unless F itself is almost all of $\mathbb{C}$).

(10.43) **Proposition.** *If D is a central division algebra over a field F , and L is any maximal subfield of D , then D splits over L .*

Proof. Define a ring homomorphism $f: D \otimes_F D \rightarrow \text{End}_F(D)$ by $f(x, y)(v) = xvy$. Because D is a division algebra, it is obvious that D is an irreducible module for $f(1 \otimes D)$, so D is irreducible for $f(L \otimes_F D)$. Thus, the Jacobson Density Theorem (11.23) implies that $f(L \otimes_F D)$ is isomorphic to $\text{Mat}_{d \times d}(E)$, where

$$E = \text{End}_{f(L \otimes_F D)}(D) = f(L \otimes 1) \cong L$$

(see Exer. 11:18). Since $L \otimes_F D$ is simple (see Exer. 11:19), we know that f is faithful, so $L \otimes_F D \cong f(L \otimes_F D)$. $\square$

10F. What is an absolutely simple group?

(10.44) **Definition.**

- G is *absolutely simple* (as a real Lie group) if $G \otimes \mathbb{C}$ is simple.
- Suppose G is defined over an algebraic number field F (as an algebraic group over F_∞) (see Defn. 10.18). We say that G_F is *absolutely simple* over F if and only if $G_F \otimes_F \mathbb{C}$ is simple. (See Exer. 10:15 for an alternate characterization that avoids mention of $\otimes_F$.)

From Rem. 10.10, we see that if G is simple, but not absolutely simple (as a real Lie group), then (up to isogeny), G is a Lie group over $\mathbb{C}$. This generalizes to other fields: if G_F is simple, but not absolutely simple over F , then, after replacing G by an isogenous group (over F) there is an extension field L of F , and a group H that is absolutely simple over L , such that G_F is isomorphic to H_L .

(10.45) **Example.** If $L \supsetneq F$, then $\mathrm{SL}(n, L)$ is absolutely simple over L , but it is not absolutely simple over F (see Exer. 10:17).

(10.46) **Definition.** Suppose G_1 and G_2 are defined over F (as algebraic groups over F_∞).

- A map $\phi: G_1 \rightarrow G_2$ is an *isogeny over F* (or an *F -isogeny*) if
 - ϕ is a surjective homomorphism with finite kernel, and
 - each matrix entry of $\phi(g)$ is a polynomial function of the matrix entries of g , and all of the coefficients of these polynomials belong to F .
- G_1 and G_2 are *isogenous over F* if there is a group G that is defined over F (as an algebraic group over F_∞), such that there exist F -isogenies $\phi_1: G \rightarrow G_1$ and $\phi_2: G \rightarrow G_2$. This is an equivalence relation.

(10.47) **Remark.**

- 1) Note that if $\phi: G \rightarrow H$ is an isogeny over F , then $\phi(G_F) \subset H_F$. However, $\phi(G_F)$ may have infinite index in H_F (cf. Exer. 6:9).
- 2) If $\mathcal{O}$ is the ring of integers of F , then there is a finite-index subgroup Λ of $G_{\mathcal{O}}$, such that $\phi(\Lambda) \subset H_{\mathcal{O}}$ (see Exer. 10:18). Then, by using the fact that arithmetic subgroups are lattices, one can show that $\phi(G_{\mathcal{O}})$ is commensurable with $H_{\mathcal{O}}$ (see Exer. 10:19). Thus, when studying an arithmetic group $G_{\mathcal{O}}$, there is no real harm in replacing G with a group that is isogenous over F .

10G. Absolutely simple classical groups

From Prop. 6.54, we know that every irreducible, arithmetic lattice can be obtained by restriction of scalars. Thus, to construct an irreducible lattice, we choose

- an algebraic number field F , and
- a simple Lie group $G \subset \mathrm{SL}(\ell, F_\infty)$, for some ℓ , such that G is defined over F .

(Then $G_{\mathcal{O}}$ embeds as an irreducible lattice in $\prod_{\sigma \in S^\infty} G^\sigma$, where $\mathcal{O}$ is the ring of integers of F .)

Therefore, to understand all of the different arithmetic lattices, we wish to understand all of the possible choices of G (up to isogeny). That is, for each algebraic number field F , we wish to describe all of the simple Lie groups G that are defined over F .

As mentioned in Rem. 10.17, it is usually most convenient to specify G_F (rather than G itself); recall that G_F is dense in G , so G_F does determine G uniquely.

We assume that G_F is *absolutely simple* over F (see §10F). This avoids the redundancy that would result from listing each complex group twice (once as a complex group, and again as a real group of twice the dimension).

Recall that any classical simple Lie group is either a special linear group, a symplectic group, an orthogonal group, or a unitary group (see 3.22 and 3.23). Theorem 10.48 shows that the same is true for simple groups over any number field (except in the special case where $G \otimes \mathbb{C}$ is isogenous to $\mathrm{SO}(8, \mathbb{C})$ or $\mathrm{SO}(8, \mathbb{C}) \times \mathrm{SO}(8, \mathbb{C})$ (see 10.51)).

(10.48) **Theorem.** *Let F be an algebraic number field. If G is a classical group that is absolutely simple over F , and G is not of type D_4 , then G is isogenous (over F) to a simple group H , such that H_F is one of the following:*

- 1) $\mathrm{SL}(n, D)$, for some $n \geq 1$, and some central division algebra D over F ; or
- 2) $\mathrm{Sp}(2n, F)$ for some $n \geq 2$; or

- 3) $\mathrm{SO}(B; F)$, for some nondegenerate, symmetric, bilinear form B on F^n , for some $n \geq 3$; or
- 4) $\mathrm{SU}(B; D, \tau_c)$, for some quaternion algebra D over F , with the standard antiinvolution τ_c , and some nondegenerate Hermitian form B on D^n ; or
- 5) $\mathrm{SU}(B; D, \tau_r)$, for some quaternion algebra D over F , with the reversion τ_r , and some nondegenerate Hermitian form B on D^n ; or
- 6) $\mathrm{SU}(B; D, \tau)$, for some central division algebra D over a quadratic extension L of F , with an antiinvolution τ whose restriction to L is the Galois automorphism of L over F , and some nondegenerate Hermitian form B on D^n .

(10.49) **Remark.** Theorem 10.48 is directly analogous to the classification of the classical simple Lie groups (see 3.22 and 3.23). Specifically:

- 1) $\mathrm{SL}(n, D)$ is the analogue of $\mathrm{SL}(n, \mathbb{R})$, $\mathrm{SL}(n, \mathbb{C})$, and $\mathrm{SL}(n, \mathbb{H})$;
- 2) $\mathrm{Sp}(2n, F)$ is the analogue of $\mathrm{Sp}(n, \mathbb{R})$ and $\mathrm{Sp}(n, \mathbb{C})$;
- 3) $\mathrm{SO}(B; F)$ is the analogue of $\mathrm{SO}(p, q)$ and $\mathrm{SO}(n, \mathbb{C})$;
- 4) $\mathrm{SU}(B; D, \tau_c)$ is the analogue of $\mathrm{Sp}(p, q)$;
- 5) $\mathrm{SU}(B; D, \tau_r)$ is the analogue of $\mathrm{SO}(n, \mathbb{H})$; and
- 6) $\mathrm{SU}(B; D, \tau)$ (with τ nontrivial on the center) is the analogue of $\mathrm{SU}(p, q)$.

(10.50) **Warning.**

- 1) In 10.48(6), the division algebra D is **not** central over F . (Its center is L , not F .) In all other cases, D is central over F .
- 2) Theorem 10.48 asserts that G is isogenous to H . However, this does not imply that G_F is essentially equal to H_F . For example, the image of $\mathrm{SL}(2, \mathbb{Q})$ in $\mathrm{PSL}(2, \mathbb{Q})$ has infinite index (cf. Exer. 6:9).

(10.51) **Remark.** The assumption that G is not of type D_4 cannot be omitted from Thm. 10.48. Let us see why.

- The map $g \mapsto (g^{-1})^T$ is a holomorphic outer automorphism of $\mathrm{SL}(n, \mathbb{C})$, and this automorphism has order 2. Any quadratic extension L of F has a Galois automorphism σ of order 2. By combining the automorphism of $\mathrm{SL}(n, \mathbb{C})$ with the Galois automorphism of L , unitary groups are constructed. Namely, for any $B \in \mathrm{GL}(n, L)$, such that

$$(10.52) \quad \sigma(B) = (B^{-1})^T,$$

we have

$$\mathrm{SU}(B; L, \sigma) = \{ g \in \mathrm{SL}(n, L) \mid (g^{-1})^T B = B\sigma(g) \}.$$

The group $\mathrm{SU}(B; L, \sigma)$ is said to be an *outer form* of $\mathrm{SL}(n, \mathbb{C})$, because it is constructed using an outer automorphism in an essential way (see §12C for a more precise definition). To specify that the outer automorphism is of order 2, one may say that $\mathrm{SU}(B; L, \sigma)$ is of type ${}^2A_{n-1}$, rather than simply that it is of type A_{n-1} (if $p + q = n$).

- It turns out that $\mathrm{PSO}(8, \mathbb{C})$ has a holomorphic outer automorphism ϕ of order 3. Any cubic extension L of F has a Galois automorphism σ of order 3. Because the automorphisms have the same order, they can be combined (much as in unitary groups) to construct outer forms that do not appear in Thm. 10.48 (and are neither orthogonal, symplectic, nor unitary); for $J \in \mathrm{PSO}(8, L)$, satisfying a certain technical condition analogous to (10.52), let

$$G_F = \{ g \in \mathrm{PSO}(8, L) \mid \phi(g) J = J\sigma(g) \}.$$

This is an outer form of type 3D_4 . There are also outer forms of type 6D_4 , constructed by using the entire outer automorphism group (which has order 6), instead of only a cyclic subgroup of order 3. See Chap. 12 for some discussion of the construction of outer forms.

- For any connected, classical, complex, simple Lie group that is not isogenous to $\mathrm{SO}(8, \mathbb{C})$, the outer automorphism group has order ≤ 2 . (Equivalently, D_4 is the only irreducible Dynkin diagram with more than two automorphisms (see Fig. 18.1 on p. 191).) So $\mathrm{SO}(8, \mathbb{C})$ is a special case.

10H. The Lie group corresponding to each F -group

We now describe H , given H_F . Recall that $H \approx H_F \otimes_F F_\infty$ (see Exer. 10:8). Thus, the desired information is provided by either Prop. 10.54 (when $F \not\subset \mathbb{R}$) or Prop. 10.55 (when $F \subset \mathbb{R}$).

We begin by finding the complexification of each of the groups in Thm. 10.48 (see 10.54). This is similar to the calculations that appear in §10B, so we omit the details.

(10.53) **Definition.** If D is a central division algebra over a field F , then the tensor product $D \otimes_F \mathbb{C}$ is isomorphic to $\mathrm{Mat}_{d \times d}(\mathbb{C})$, for some natural number d (see 10.42). This number d is called the *degree* of D . We remark that $\dim_F D = d^2$.

(10.54) **Proposition.** *The notation of each part of this proposition is taken from the corresponding part of Thm. 10.48. We use d to denote the degree of the central division algebra D .*

- 1) $\mathrm{SL}(n, D) \otimes_F \mathbb{C} \cong \mathrm{SL}(dn, \mathbb{C})$.
- 2) $\mathrm{Sp}(2n, F) \otimes_F \mathbb{C} \cong \mathrm{Sp}(2n, \mathbb{C})$.
- 3) $\mathrm{SO}(B; F) \otimes_F \mathbb{C} \cong \mathrm{SO}(n, \mathbb{C})$.
- 4) $\mathrm{SU}(B; D, \tau_c) \otimes_F \mathbb{C} \cong \mathrm{Sp}(2n, \mathbb{C})$.
- 5) $\mathrm{SU}(B; D, \tau_r) \otimes_F \mathbb{C} \cong \mathrm{SO}(2n, \mathbb{C})$.
- 6) $\mathrm{SU}(B; D, \tau) \otimes_F \mathbb{C} \cong \mathrm{SL}(dn, \mathbb{C})$.

(10.55) **Proposition.** *Assume F is an algebraic number field, and $F \subset \mathbb{R}$. The notation of each part of this proposition is taken from the corresponding part of Thm. 10.48. We use d to denote the degree of the central division algebra D .*

- 1) $\mathrm{SL}(n, D) \otimes_F \mathbb{R} \cong \begin{cases} \mathrm{SL}(dn, \mathbb{R}) & \text{if } D \text{ splits over } \mathbb{R}, \\ \mathrm{SL}(dn/2, \mathbb{H}) & \text{if } D \text{ does not split over } \mathbb{R}. \end{cases}$
- 2) $\mathrm{Sp}(2n, F) \otimes_F \mathbb{R} \cong \mathrm{Sp}(2n, \mathbb{R})$.
- 3) $\mathrm{SO}(B; F) \otimes_F \mathbb{R} \cong \mathrm{SO}(B, \mathbb{R}) \cong \mathrm{SO}(p, q)$.
- 4) $\mathrm{SU}(B; D, \tau_c) \otimes_F \mathbb{R} \cong \begin{cases} \mathrm{Sp}(2n, \mathbb{R}) & \text{if } D \text{ splits over } \mathbb{R}, \\ \mathrm{SU}(B; \mathbb{H}, \tau_c) \cong \mathrm{Sp}(p, q) & \text{if } D \text{ does not split over } \mathbb{R}. \end{cases}$
- 5) $\mathrm{SU}(B; D, \tau_r) \otimes_F \mathbb{R} \cong \begin{cases} \mathrm{SO}(p, q) & \text{if } D \text{ splits over } \mathbb{R}, \\ \mathrm{SO}(n, \mathbb{H}) & \text{if } D \text{ does not split over } \mathbb{R}. \end{cases}$
- 6) $\mathrm{SU}(B; D, \tau) \otimes_F \mathbb{R} \cong \begin{cases} \mathrm{SU}(p, q) & \text{if } L \not\subset \mathbb{R} \\ \mathrm{SL}(dn, \mathbb{R}) & \text{if } L \subset \mathbb{R} \text{ and } D \text{ splits over } \mathbb{R}, \\ \mathrm{SL}(nd/2, \mathbb{H}) & \text{if } L \subset \mathbb{R} \text{ and } D \text{ does not split over } \mathbb{R}. \end{cases}$

(10.56) **Remark.** Proposition 10.55 does not specify the values of p and q , where they appear. However, they can be calculated for any particular form B .

For example, to calculate them in (6), note that, because $L \not\subset \mathbb{R}$, we have $D \otimes_F \mathbb{R} \cong \text{Mat}_{d \times d}(\mathbb{C})$, so we may think of $[B] \in \text{Mat}_{n \times n}(D)$ as a $(dn) \times (dn)$ Hermitian matrix. Then p is the number of positive eigenvalues of this Hermitian matrix, and q is the number of negative eigenvalues.

In each of the other cases, it is not difficult to give a fairly uniform calculation of p and q (cf. Exers. 10:26 and 10:27, and Props. 7.18, 10.64(1), and 10.70(1)).

10I. The arithmetic lattices in classical groups

Theorem 10.48 provides a classification of all the irreducible, arithmetic lattices in semisimple Lie groups. Namely, if Γ is an irreducible, arithmetic lattice in G , then there is a group H_F listed in Thm. 10.48, such that (modulo compact factors and commensurability) G is isomorphic to $\prod_{\sigma \in S_\infty} H^\sigma$, via an isomorphism that takes Γ to $H_\mathcal{O}$ (see 6.52). (Restriction of Scalars (6.49 and 6.51) tells us that $H_\mathcal{O}$ is (isomorphic to) an irreducible, arithmetic lattice in $\prod_{\sigma \in S_\infty} H^\sigma$.)

Figure 10.2 lists the groups of Thm. 10.48 in a format that is intended to make it easier to find the irreducible lattices in a given group.

The following two propositions illustrate this. We use $\text{Sp}(p, q)$ for our example, because it is one of the easiest cases: Fig. 10.2 lists only one possibility for this group, and the division algebra involved is known to be a quaternion algebra. Other groups can be treated similarly, but there are more possibilities to consider.

Our first result describes what we learn from Fig. 10.2, just by knowing one of the factors of G .

(10.57) **Proposition.** *Suppose*

- Γ is an irreducible, arithmetic lattice in G ,
- some simple factor of G is isomorphic to $\text{Sp}(p, q)$ for some $p, q \geq 1$, and
- G has no compact factors.

Then (after replacing G with an isogenous group) there are

- 1) a quaternion algebra $D = D_{\beta, \gamma}(F)$ over an algebraic number field $F \subset \mathbb{R}$,
- 2) a τ_c -Hermitian form B on D^{p+q} ,
- 3) a subset S of S^∞ (containing Id), such that H^σ is compact, for all $\sigma \in S^\infty \setminus S$, where $H_F = \text{SU}(B; D, \tau_c)$, and
- 4) an isomorphism $\phi: \prod_{\sigma \in S} H^\sigma \rightarrow G$,

such that

$$\phi(\text{SU}(B; D(\mathcal{O}), \tau_c)) \text{ is commensurable with } \Gamma,$$

for any subring $\mathcal{O}$ of D that is a vector-space lattice in D .

Proof. Figure 10.2 lists only one possibility for $\text{Sp}(p, q)$. The reference is to 10.48(4), with $F \subset \mathbb{R}$ and $p + q = n$. $\square$

Propositions 10.54 and 10.55 can be used to calculate H^σ , for each $\sigma \in S^\infty$. Thus, we get more precise information about Γ if a particular group G is given. To illustrate, let us take the simplest case, where G has only one simple factor.

(10.58) **Corollary.** *Let Γ be an arithmetic lattice in $G = \text{Sp}(p, q)$, for some $p, q \geq 1$. Then there are*

simple factor of G	irreducible lattice Γ	reference	m or $p + q$	$\mathbb{Q}$ -rank(Γ)
$\mathrm{SL}(m, \mathbb{R})$	$\mathrm{SL}(n, \mathcal{O}_D)$	(1), $F \subset \mathbb{R}$, D split/ $\mathbb{R}$	$m = dn$	$n - 1$
	$\mathrm{SU}(B; \mathcal{O}_D, \tau)$	(6), $F \subset L \subset \mathbb{R}$, D split/ $\mathbb{R}$	$m = dn$	D -subspace
$\mathrm{SL}(m, \mathbb{C})$	$\mathrm{SL}(n, \mathcal{O}_D)$	(1), $F \not\subset \mathbb{R}$	$m = dn$	$n - 1$
	$\mathrm{SU}(B; \mathcal{O}_D, \tau)$	(6), $F \not\subset \mathbb{R}$ (so $L \not\subset \mathbb{R}$)	$m = dn$	D -subspace
$\mathrm{SL}(m, \mathbb{H})$	$\mathrm{SL}(n, \mathcal{O}_D)$	(1), $F \subset \mathbb{R}$, D not split/ $\mathbb{R}$	$m = dn/2$, d even	$n - 1$
	$\mathrm{SU}(B; \mathcal{O}_D, \tau)$	(6), $F \subset L \subset \mathbb{R}$, D not split/ $\mathbb{R}$	$m = dn/2$, d even	D -subspace
$\mathrm{SU}(p, q)$	$\mathrm{SU}(B; \mathcal{O}_D, \tau)$	(6), $F \subset \mathbb{R}$, $L \not\subset \mathbb{R}$	$p + q = dn$	D -subspace
$\mathrm{SO}(p, q)$	$\mathrm{SO}(B; \mathcal{O}_F)$	(3), $F \subset \mathbb{R}$	$p + q = n$	F -subspace
	$\mathrm{SU}(B; \mathcal{O}_D, \tau_r)$	(5), $F \subset \mathbb{R}$, D split/ $\mathbb{R}$	$p + q = 2n$, $d = 2$	D -subspace
	?	Rem. 10.51	$p + q = 8$	?
$\mathrm{SO}(m, \mathbb{C})$	$\mathrm{SO}(B; \mathcal{O}_F)$	(3), $F \not\subset \mathbb{R}$	$m = n$	F -subspace
	$\mathrm{SU}(B; \mathcal{O}_D, \tau_r)$	(5), $F \not\subset \mathbb{R}$	$m = 2n$, $d = 2$	D -subspace
	?	Rem. 10.51	$m = 8$	?
$\mathrm{SO}(m, \mathbb{H})$	$\mathrm{SU}(B; \mathcal{O}_D, \tau_r)$	(5), $F \subset \mathbb{R}$, D not split/ $\mathbb{R}$	$m = n$, $d = 2$	D -subspace
	?	Rem. 10.51	$m = 4$	?
$\mathrm{Sp}(2m, \mathbb{R})$	$\mathrm{Sp}(2n, \mathcal{O}_F)$	(2), $F \subset \mathbb{R}$	$m = n$	n
	$\mathrm{SU}(B; \mathcal{O}_D, \tau_c)$	(4), $F \subset \mathbb{R}$, D split/ $\mathbb{R}$	$m = n$, $d = 2$	D -subspace
$\mathrm{Sp}(2m, \mathbb{C})$	$\mathrm{Sp}(2n, \mathcal{O}_F)$	(2), $F \not\subset \mathbb{R}$	$m = n$	n
	$\mathrm{SU}(B; \mathcal{O}_D, \tau_c)$	(4), $F \not\subset \mathbb{R}$	$m = n$, $d = 2$	D -subspace
$\mathrm{Sp}(p, q)$	$\mathrm{SU}(B; \mathcal{O}_D, \tau_c)$	(4), $F \subset \mathbb{R}$, D not split/ $\mathbb{R}$	$p + q = n$, $d = 2$	D -subspace

Figure 10.2. The irreducible arithmetic lattices in G , except that (as indicated by “?”) the list is not complete for groups of type D_4 . The reference is to 10.48 and to 10.54 (for $F_\sigma = \mathbb{C}$) and 10.55 (for $F_\sigma = \mathbb{R}$).

- a totally real algebraic number field F ,
- $\beta, \gamma \in F$, such that $\sigma(\beta)$ and $\sigma(\gamma)$ are negative, for every place σ of F ;
- $b_1, \dots, b_{p+q} \in F$, such that
 - $b_1, \dots, b_p$ are positive,
 - $b_{p+1}, \dots, b_{p+q}$ are negative, and
 - for each place $\sigma \neq \text{Id}$, the real numbers $\sigma(b_1), \dots, \sigma(b_{p+q})$ are either all positive or all negative;
 and
- an isomorphism $\phi: \text{SU}(B; D_{\beta, \gamma}(F), \tau_c) \otimes_F \mathbb{R} \rightarrow \text{Sp}(p, q)$, where B is the τ_c -hermitian form on D^{p+q} defined by

$$(10.59) \quad B(x, y) = \sum_{j=1}^{p+q} b_j x_j \tau_c(y_j),$$

such that

$$\phi(\text{SU}(B; D_{\beta, \gamma}(\mathcal{O}), \tau_c)) \text{ is commensurable with } \Gamma,$$

for any subring $\mathcal{O}$ of $D_{\beta, \gamma}(F)$ that is a vector-space lattice in $D_{\beta, \gamma}(F)$.

Proof. Because G has only one simple factor, we have $S = \{\text{Id}\}$.

Because $H = H_F \otimes_F \mathbb{R} \cong \text{Sp}(p, q)$, we see, from 10.55(4), that $D_{\beta, \gamma}(F)$ does not split over $\mathbb{R}$; thus, β and γ are negative (see 7.56(3)).

For each $\sigma \neq \text{Id}$, we know that H^σ is compact, so we see, from 10.54(4) and 10.55(4), that $F_\sigma = \mathbb{R}$ and both $\sigma(\beta)$ and $\sigma(\gamma)$ are negative.

By a change of basis, we may assume B is diagonal (see 10.70(1)); thus, there exist $b_1, \dots, b_{p+q} \in D_{\beta, \gamma}(F)$, such that B is of the form (10.59). Since B is Hermitian, we must have $\tau_c(b_j) = b_j$, so $b_j \in F$.

Since $H \cong \text{Sp}(p, q)$, we know that p of the b_j 's are of one sign, and the other q of the b_j 's are of the opposite sign. Thus, by permuting, and perhaps replacing B with $-B$, we may assume that $b_1, \dots, b_p$ are positive, and $b_{p+1}, \dots, b_{p+q}$ are negative.

Since H^σ is compact, for $\sigma \neq \text{Id}$, we see that $\sigma(b_1), \dots, \sigma(b_{p+q})$ are all of the same sign. $\square$

(10.60) **Proposition.** *If G is simple, Γ is arithmetic, and $\Gamma \backslash G$ is not compact, then, in the notation of Fig. 10.2, we have*

$$F = \begin{cases} \mathbb{Q} & \text{if } F \subset \mathbb{R}, \\ \text{a quadratic extension of } \mathbb{Q} & \text{if } F \not\subset \mathbb{R}. \end{cases}$$

10J. What are the possible Hermitian forms?

Some cases of Thm. 10.48 assert the existence of a bilinear or Hermitian form. In this section, we provide a description of the possible forms.

10Ja. Symplectic forms.

(10.61) **Notation.** Let $\mathcal{B} = \{v_1, \dots, v_\ell\}$ be an ordered basis of a vector space V over a field F .

- If $x \in V$, then $[x] = [x]_{\mathcal{B}}$ is the column vector with entries $x_1, \dots, x_\ell$, where $x = \sum_{j=1}^{\ell} x_j v_j$.
- If $B(x, y)$ be a nondegenerate bilinear form on V , then $[B] = [B]_{\mathcal{B}}$ is the $\ell \times \ell$ matrix whose (i, j) -entry is $B(v_i, v_j)$.

(10.62) **Lemma.**

- 1) For $x, y \in V$, we have $B(x, y) = [x]^T [B] [y]$.
- 2) If B is symmetric, then $[B]^T = [B]$.
- 3) If B is symplectic, then $[B]^T = -[B]$.

It is well known that, up to a change of basis, there is only one symplectic form on any given vector space. The following proposition describes the usual descriptions of this form.

(10.63) **Proposition.** Let $B(x, y)$ be a symplectic form on a vector space V over a field F , and let $n = \dim_F V$.

- 1) n is even.
- 2) There is a basis $\mathcal{B}$ of V , such that

$$[B]_{\mathcal{B}} = J_n^- = \begin{bmatrix} 0 & J_{n/2} \\ -J_{n/2} & 0 \end{bmatrix} = \begin{bmatrix} & & & & & 1 \\ & & & & \ddots & \\ & & & 1 & & \\ & & \ddots & & -1 & \\ & -1 & & & & \\ & & & & & \end{bmatrix}.$$

- 3) There is a basis $\mathcal{B}$ of V , such that

$$[B]_{\mathcal{B}} = \begin{bmatrix} 0 & \text{Id}_{n/2} \\ -\text{Id}_{n/2} & 0 \end{bmatrix}.$$

- 4) There is a basis $\mathcal{B}$ of V , such that

$$[B]_{\mathcal{B}} = \begin{bmatrix} J_2^- & & & \\ & J_2^- & & \\ & & \ddots & \\ & & & J_2^- \end{bmatrix}.$$

Proof. (2) Let $u \in V \setminus \{0\}$. Because symplectic forms are, by definition, nondegenerate, there is some $v \in V$, such that $B(u, v) \neq 0$.

By induction on $\dim V$, there is a good basis $\mathcal{B}_1$ of $W^\perp$. Let $\mathcal{B} = \{u\} \cup \mathcal{B}_1 \cup \{v\}$.

- (3) If $\{x_1, \dots, x_{n/2}, y_1, \dots, y_{n/2}\}$ is a basis as in (2), let

$$\mathcal{B} = \{x_1, \dots, x_{n/2}, y_{n/2}, \dots, y_2, y_1\}.$$

(4) The desired basis is a permutation of the basis for (4). Alternatively, use the same proof as (2), but with $\mathcal{B} = \{u, v\} \cup \mathcal{B}_1$.

- (1) This follows from (2). □

10Jb. Symmetric, bilinear forms. There is usually more than one symmetric, bilinear form on a vector space V , but the following proposition shows that they can all be diagonalized, and that the isotropic part of the form can be understood completely.

(10.64) **Proposition.** Let $B(x, y)$ be a nondegenerate, symmetric, bilinear form on a vector space V over a field F (of characteristic 0).

- 1) There is a basis $\mathcal{B}$ of V , such that $[B]_{\mathcal{B}}$ is diagonal.

2) More precisely, there is a basis $\mathcal{B}$ of V , such that

$$(10.65) \quad [B]_{\mathcal{B}} = \begin{bmatrix} \text{Id}_{m,m} & 0 \\ 0 & B' \end{bmatrix},$$

where

- m is the maximal dimension of a totally isotropic subspace of V , and
- B' is the matrix of an anisotropic form (and B' is diagonal).

3) Alternatively, the $2m \times 2m$ submatrix $\text{Id}_{m,m}$ in (10.65) can be replaced with any of:

$$(a) \quad \begin{bmatrix} \text{Id}_{1,1} & & & \\ & \text{Id}_{1,1} & & \\ & & \ddots & \\ & & & \text{Id}_{1,1} \end{bmatrix},$$

$$(b) \quad J_{2m} = \begin{bmatrix} & & & 1 \\ & & & \\ & & \ddots & \\ & & & 1 \\ & 1 & & \\ & & \ddots & \\ 1 & & & \end{bmatrix}, \text{ or}$$

$$(c) \quad \begin{bmatrix} J_2 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_2 \end{bmatrix}.$$

4) There is a basis $\mathcal{B}$ of V , such that

$$(10.66) \quad [B]_{\mathcal{B}} = \begin{bmatrix} & & & & & & 1 \\ & & & & & & \\ & & & & & 1 & \\ & & & & \ddots & & \\ & & & 1 & & & \\ & & & & B' & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & 1 & & & & & \\ 1 & & & & & & \end{bmatrix},$$

with B' as in (2).

Proof. (1) To diagonalize B , choose $\mathcal{B}$ to be an orthogonal basis.

(3a) We prove the more precise result by induction on $\dim V$. We may assume B is isotropic (otherwise, there is nothing to prove), so there is some nonzero $u \in V$ with $B(u, u) = 0$. Because B is nondegenerate, there is some $v \in V$, such that $B(u, v) \neq 0$.

Note that the expression

$$B(v + tu, v + tu) = B(v, v) + 2tB(u, v) + t^2B(u, u) = B(v, v) + 2tB(u, v)$$

is linear in t , so it has a zero. Thus, by replacing v with $v + tu$, for some $t \in F$, we may assume that $B(v, v) = 0$.

Let $W = \langle u, v \rangle$. Then $[B|_W]_{\{u, v\}} = \text{Id}_{1,1}$, and, by induction on $\dim V$, there is a good basis $\mathcal{B}_1$ of $W^\perp$. Let $\mathcal{B} = \{u, v\} \cup \mathcal{B}_1$.

(2) The diagonal entries in (2) are a permutation of the diagonal entries in (3a). Thus, the desired basis is a permutation of the basis for (3a).

(3c) If $[B]_{\{u,v\}} = \text{Id}_{1,1}$, and $\mathcal{B} = \{u + \frac{1}{2}v, u - \frac{1}{2}v\}$, then $[B]_{\mathcal{B}} = J_2$.

(3b) The desired basis is a permutation of the basis for (3c).

(4) The desired basis is a permutation of the basis for (3b). □

The following observation is obvious.

(10.67) **Corollary.** Assume $F \subset \mathbb{R}$. For B and B' as in (10.65), we have

$$\text{SO}(B; \mathbb{R}) \otimes_F \mathbb{R} \cong \text{SO}(m+p, m+q),$$

where

- p is the number of positive entries in the diagonal matrix B' , and
- q is the number of negative entries in the diagonal matrix B' .

10Jc. Hermitian forms. Let us now see that Prop. 10.64 generalizes to Hermitian forms, even over division algebras.

(10.68) **Notation.** Let

- D be a division algebra (over a field of characteristic 0), with an antiinvolution τ , and
- $\mathcal{B} = \{v_1, \dots, v_\ell\}$ be an ordered basis of a vector space V over D .

For $x \in V$, and any Hermitian form $B(x, y)$ on V , we define $[x]_{\mathcal{B}}$ and $[B]_{\mathcal{B}}$ as in Ntn. 10.61.

(10.69) **Lemma.** 1) For $x, y \in V$, we have $B(x, y) = [x]^T [B] \tau([y])$.

2) We have $\tau([B]^T) = [B]$.

(10.70) **Proposition.** Let

- D be a division algebra (over a field of characteristic 0), with an antiinvolution τ , and
- $B(x, y)$ be a nondegenerate, Hermitian form on a vector space V over D .

Then Conclusions (1), (2), (3), and (4) of Prop. 10.64 hold.

(10.71) **Remark.** If

- D is a field (that is, if D is commutative),
- B is a nondegenerate τ -Hermitian form on D^n , and
- λ is a nonzero element of D , such that $\tau(\lambda) = \lambda$,

then

- 1) λB is a nondegenerate, Hermitian form, and
- 2) $\text{SO}(B; D) = \text{SO}(\lambda B; D)$.

Thus, if we are interested in the isometry group of B , not B itself, then additional simplification of $[B]$ is possible.

(10.72) **Corollary.** Let D , τ , and B be as in Prop. 10.70.

- 1) If $\dim_D V = 2$, and B is isotropic, then there is a basis of V , such that $[B] = \text{Id}_{1,1}$. (There is also a basis with $[B] = J_2$.)
- 2) If $\dim_D V = 2$, and D is a field, then there are
 - some nonzero λ and b in D , with $\tau(\lambda) = \lambda$ and $\tau(b) = b$, and
 - a basis of V ,

such that

$$[\lambda B] = \begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix}.$$

3) If

- $\dim_D V = 3$,
- D is a field, and
- B is isotropic,

then there are

- some nonzero $\lambda \in D$, with $\tau(\lambda) = \lambda$, and
- a basis of V ,

such that $[\lambda B] = \text{Id}_{2,1}$. (There is also a basis with $[\lambda B] = J_3$.)

Proof. (1) and (2) are immediate from Prop. (10.64).

(3) Choose $w \in V$, such that $w^\perp$ contains an isotropic vector u , and let $\lambda = 1/B(w, w)$. Then $\lambda B(w, w) = 1$, so the desired conclusion follows from the proof of 10.64(3a). $\square$

(10.73) **Warning.** Do not try to use (2) or (3) unless D is commutative. If D is noncommutative, then

- 1) λB may not be τ -Hermitian, even if $\tau(\lambda) = \lambda$, and
- 2) $\text{SU}(\lambda B; D, \tau)$ may not be isogenous to $\text{SU}(B; D, \tau)$, even if λB is τ -Hermitian.

Should probably give an example!!!

Let us mention one additional well-known way to simplify $[B]$.

(10.74) **Lemma.** Suppose

- $\mathcal{B} = \{v_1, \dots, v_n\}$, and
- $[B]_{\mathcal{B}}$ is the diagonal matrix $\text{diag}(b_1, \dots, b_n)$.

Replacing $\mathcal{B}$ with $\{\lambda_1 v_1, \dots, \lambda_n v_n\}$ results in

$$[B] = \begin{cases} \text{diag}(\lambda_1^2 b_1, \dots, \lambda_n^2 b_n) & \text{if } B \text{ is bilinear,} \\ \text{diag}(\lambda_1 b_1 \tau(\lambda_1), \dots, \lambda_n b_n \tau(\lambda_n)) & \text{if } B \text{ is } \tau\text{-Hermitian.} \end{cases}$$

10Jd. Witt's Theorem.

(10.75) **Theorem** (Witt's Theorem). Let $B(v, w)$ be a nondegenerate, symmetric bilinear form on a finite-dimensional vector space V over a field F of characteristic 0. Suppose W_1 and W_2 are subspaces of V , and $\phi: W_1 \rightarrow W_2$ is a bijective linear transformation, such that $B(\phi(v), \phi(w)) = B(v, w)$, for every $v, w \in W_1$. Then ϕ extends to an isometry of V .

We begin by proving a special case, from which the general result follows easily.

(10.76) **Lemma.** Let $B(v, w)$ be a nondegenerate, symmetric bilinear form on a finite-dimensional vector space V over a field F of characteristic 0. Suppose W_1 and W_2 are subspaces of V , and $\phi: W_1 \rightarrow W_2$ is a bijective linear transformation, such that

- $B(\phi(v), \phi(w)) = B(v, w)$, for every $v, w \in W_1$, and
- there is a codimension-one subspace U of W_1 , such that $\phi(u) = u$, for every $u \in U$.

Then ϕ extends to an isometry of V .

Proof. We proceed by induction on the codimension of W_1 in V . We may assume $U \neq W_1$ (for otherwise Id is an extension of ϕ); let $w_1 \in W_1 \setminus U$.

Case 1. Suppose $(\phi(w_1) - w_1)^\perp \not\subset W_1 \cup W_2$. Choose $u_0 \in (\phi(w_1) - w_1)^\perp \setminus (W_1 \cup W_2)$, and define $\hat{\phi}: W_1 \oplus Fu_0 \rightarrow W_2 \oplus Fu_0$ by $\hat{\phi}(w + \lambda u_0) = \phi(w) + \lambda u_0$, for $w \in W_1$ and $\lambda \in F$. Then $\hat{\phi}$ is a linear bijection, $B(\phi(v), \phi(w)) = B(v, w)$, for every $v, w \in W_1 + Fu_0$, and $\phi(u) = u$, for every $u \in U + Fu_0$. Since $\text{codim}(W_1 + Fu_0) < \text{codim}(W_1)$, we know, from the induction hypothesis, that $\hat{\phi}$ extends to an isometry of V . This isometry also extends ϕ .

Case 2. Suppose $(\phi(w_1) - w_1)^\perp \subset W_1 \cup W_2$. We must have either $(\phi(w_1) - w_1)^\perp \subset W_1$ or $(\phi(w_1) - w_1)^\perp \subset W_2$. By interchanging W_1 with W_2 (and replacing ϕ with ϕ^{-1}) if necessary, we may assume $(\phi(w_1) - w_1)^\perp \subset W_1$. Since $\text{codim}(\phi(w_1) - w_1)^\perp = 1$, and we may assume $W_1 \neq V$ (for otherwise there is nothing to prove), we have

$$(10.77) \quad W_1 = (\phi(w_1) - w_1)^\perp.$$

Therefore

$$\begin{aligned} 0 &= B(w_1, \phi(w_1) - w_1) = B(w_1, \phi(w_1)) - B(w_1, w_1) \\ &= B(w_1, \phi(w_1)) - B(\phi(w_1), \phi(w_1)) = B(w_1 - \phi(w_1), \phi(w_1)), \end{aligned}$$

so $\phi(w_1) \in (\phi(w_1) - w_1)^\perp = W_1$. Hence $W_2 = \phi(W_1) = \langle \phi(w_1), U \rangle \subset W_1$. By comparing dimensions, we conclude that

$$W_2 = W_1.$$

This implies that

$$\phi(w_1) - w_1 \in W_2 - W_1 = W_1 = (\phi(w_1) - w_1)^\perp,$$

so

$$B^2(\phi(w_1) - w_1) = 0,$$

where, for convenience, we define

$$B^2(v) = B(v, v).$$

Now fix some $v \in V \setminus W_1$. There exists $\delta \in U^\perp$, such that

$$B(\delta, \phi(w_1)) = -B(v, \phi(w_1) - w_1),$$

so

$$B(v + \delta, \phi(w_1)) = B(v, w_1).$$

For any scalar t , we have

$$B^2(v + \delta + t(\phi(w_1) - w_1)) = B^2(v + \delta) + tB(v + \delta, \phi(w_1) - w_1),$$

so, for an appropriate choice of t , we have

$$B^2(v + \delta + t(\phi(w_1) - w_1)) = B^2(v).$$

We may extend ϕ to V by defining

$$\hat{\phi}(v) = v + \delta + t(\phi(w_1) - w_1).$$

□

Proof of Thm. 10.75. Let U be a codimension-one subspace of W_1 . By induction on $\dim W_1$, we may assume that the restriction $\phi|_U$ extends to an isometry ψ of V . Then, by composing ϕ with the inverse of ψ , we may assume that $\phi(u) = u$, for every $u \in U$. Hence, Lem. 10.76 applies. □

10K. Notes

Theorem 10.48 is due to Weil [Wei]. A proof (together with Props. 10.6 and 10.54) appears in [P-R, §2.3, pp. 78–92]. We copied (10.6), (10.48), and (10.54) from the summary on [P-R, p. 92], except that [P-R] uses a different description of the groups in 10.48(5) (see Exer. 10:24).

As will be explained in Chap. 12, a theorem of A. Borel and G. Harder [B-H] on Galois cohomology immediately implies that if G is isotypic, then G has a cocompact, irreducible, arithmetic lattice. The concrete approach described in §10D was carried out in detail by F. E. A. Johnson [Joh] for all classical groups.

G. Prasad (personal communication) pointed out the example in Prop. 10.31. This disproves the statement in [Joh] that the converse of Prop. 10.21 holds for isotypic groups.

Remark 10.10 is in Bourbaki's *Lie Groups and Lie Algebras* (at the Lie algebra level). Need to relocate the specific reference!!!

See [P-R, Thm. 4.1, p. 204] or [Bor, Thm. 8.9] for a proof of Rem. 10.47(2).

Theorem 10.75 was proved by E. Witt [Wit, p. 34]. Our proof is based on [Che, Thm. I.4.1, pp. 80–81] and [Die, §11, pp. 21–22].

10L. References

- [Bor] A. Borel: *Introduction aux Groupes Arithmétiques*, Act. Sci. Ind. #1341, Hermann, Paris, 1969.
- [B-H] A. Borel and G. Harder: Existence of discrete cocompact subgroups of reductive groups over local fields, *J. Reine Angew. Math.* 298 (1978) 53–64.
- [Che] C. Chevalley: *The Algebraic Theory of Spinors and Clifford Algebras*, Collected Works, Vol. 2, Springer, Berlin, 1997.
- [Die] J. Dieudonné: *La Géométrie des Groupes Classiques*, 2nd ed., Springer, Berlin, 1963.
- [Joh] F. E. A. Johnson: On the existence of irreducible discrete subgroups in isotypic Lie groups of classical type, *Proc. London Math. Soc.* (3) 56 (1988) 51–77.
- [P-R] V. Platonov and A. Rapinchuk: *Algebraic Groups and Number Theory*. Academic Press, Boston, 1994.
- [Wei] A. Weil: Algebras with involution and the classical groups, *J. Indian Math. Soc.* 24 (1960) 589–623.
- [Wit] E. Witt: Theorie der quadratischen Formen in beliebigen Körpern, *J. reine angew. Math.* 176 (1937) 31–44.

Exercises

- 10:1) Show that the Lie algebra of $G \otimes \mathbb{C}$ is $\mathfrak{g} \otimes \mathbb{C}$.
- 10:2) Show that $\mathrm{SO}(p, q) \otimes \mathbb{C} \cong \mathrm{SO}(p + q, \mathbb{C})$. [*Hint*: $\mathrm{SO}(p, q) \otimes \mathbb{C}$ is conjugate to $\mathrm{SO}(p + q, \mathbb{C})$ in $\mathrm{SL}(p + q, \mathbb{C})$, because -1 is a square in $\mathbb{C}$.]
- 10:3) In the proof of Lem. 10.11, verify:
 - (a) ϕ is an injective ring homomorphism;
 - (b) $\phi(\{1, i, j, k\})$ is a $\mathbb{C}$ -basis of $\mathrm{Mat}_{2 \times 2}(\mathbb{C})$; and
 - (c) $\hat{\phi}$ is an isomorphism of $\mathbb{C}$ -algebras.
- 10:4) Show $\mathrm{SL}(n, \mathbb{H}) \otimes \mathbb{C} \cong \mathrm{SL}(n, \mathrm{Mat}_{2 \times 2}(\mathbb{C}))$. [*Hint*: Define ϕ as in the proof of Lem. 10.11. Use the proof of Prop. 10.9, with ϕ in the place of Δ .]

- 10:5) Show $\mathrm{SL}(n, \mathrm{Mat}_{d \times d}(\mathbb{C})) \cong \mathrm{SL}(dn, \mathbb{C})$.
- 10:6) Show that $\mathrm{SO}(n, \mathbb{H}) \otimes \mathbb{C} \cong \mathrm{SO}(2n, \mathbb{C})$. [Hint: Similar to (10.14). To calculate $\tau_r \otimes \mathbb{C}$, note that $\tau_r(x) = j^{-1} \tau(x) j$, for $x \in \mathbb{H}$.]
- 10:7) Show that there is an irreducible lattice in $\mathrm{SL}(2, \mathbb{R}) \times \mathrm{SO}(3)$ that is not cocompact. [Hint: The free group F_2 is a noncocompact lattice in $\mathrm{SL}(2, \mathbb{R})$. Let Γ be the graph of a homomorphism $F_2 \rightarrow \mathrm{SO}(3)$ that has dense image.]
- 10:8) Suppose $G \subset \mathrm{SL}(\ell, F_\infty)$, and G is defined over F (as an algebraic group over F_∞). Show that G is isogenous to $G_F \otimes_F F_\infty$.
- 10:9) Let
- L be a quadratic extension of a real algebraic number field F ,
 - τ be the Galois automorphism of L over F , and
 - B be a nondegenerate Hermitian form on L^n .
- Show that if $L \subset \mathbb{R}$, then $\mathrm{SU}(B; L, \tau) \otimes_F \mathbb{R} \cong \mathrm{SL}(n, \mathbb{R})$. [Hint: See the proof of Prop. 10.13. For $\Delta(x) = (x, \sigma(x))$ and $\eta(x, y) = (y, x)$, the diagram

$$\begin{array}{ccc} L & \xrightarrow{\Delta} & \mathbb{R} \oplus \mathbb{R} \\ \downarrow \tau & & \downarrow \eta \\ L & \xrightarrow{\Delta} & \mathbb{R} \oplus \mathbb{R}. \end{array}$$

commutes.]

- 10:10) Use (10.27) and (10.26) to show that there is an irreducible, arithmetic lattice in $\mathrm{SO}(n, \mathbb{C})^s \times \prod_{j=1}^r \mathrm{SO}(p_j, n - p_j)$. Is your proof still valid when $r = 0$ or $s = 0$?
- 10:11) Show that if
- G is isotypic of type B_n , and
 - G has no compact factors,
- then G has an irreducible lattice that is **not** cocompact.
- 10:12) Show that if
- G is isotypic of type D_n , with $n \geq 5$, and
 - $\mathbb{R}\text{-rank}(G_j) \geq 2$, for every simple factor G_j of G ,
- then G has an irreducible lattice that is **not** cocompact.
- 10:13) Let B be a central simple division algebra over an algebraic number field F , and let B be a nondegenerate Hermitian form on D^3 , with respect to some antiinvolution τ of D . Show (without using Prop. 10.70) that if there is a nonzero vector v in D^3 , such that $B(v, v) = 0$, then there is a B -orthogonal D -basis $\{x, y, z\}$ of D^3 , such that $B(x, x) = 1$ and $B(y, y) = -1$.
- 10:14) Let $G = \mathrm{SO}(1, 2n - 1) \times \mathrm{SO}(n, \mathbb{H})$, with $n \geq 3$. Show that if Γ is an irreducible lattice in either G or $G \times \mathrm{SO}(2n, \mathbb{C})$, then Γ is cocompact. [Hint: Proof of Prop. 10.31.]
- 10:15) Show that G_F is absolutely simple over F if and only if either
- (a) $F_\infty = \mathbb{R}$, and $G \otimes \mathbb{C}$ is simple, or
 - (b) $F_\infty = \mathbb{C}$, and G is simple.
- [Hint: Use the fact that $G_F \otimes_F F_\infty$ is isogenous to G (see Exer. 10:8).]
- 10:16) Show that if G is absolutely simple, then G is simple.
- 10:17) Suppose F and L are algebraic number fields with $F \subset L$, and let S be the set of places σ of L , such that $\sigma|_F = \mathrm{Id}$.
- (a) Show that $\mathrm{SL}(n, L) \otimes_F F_\infty \cong \prod_{\sigma \in S} \mathrm{SL}(n, L_\sigma)$.

- (b) Show that $\mathrm{SL}(n, L) \otimes_F \mathbb{C} \cong \mathrm{SL}(n, \mathbb{C})^d$, where d is the degree of L over F .
- (c) Show that if $F \subsetneq L$, then $\mathrm{SL}(n, L)$ is not absolutely simple over F .
- 10:18) Assume $G \subset \mathrm{SL}(\ell, \mathbb{R})$ is defined over $\mathbb{Q}$, and let $\Gamma = G_{\mathbb{Z}}$. Show that if $\phi: G \rightarrow H$ is a $\mathbb{Q}$ -isogeny, then there is a finite-index subgroup Γ of $G_{\mathbb{Z}}$, such that $\phi(\Gamma) \subset H_{\mathbb{Z}}$. [Hint: Show that if $f \in \mathbb{Q}[x_{1,1}, \dots, x_{\ell,\ell}]$, and $f(\mathrm{Id}) \in \mathbb{Z}$, then there is a principal congruence subgroup Γ_n of Γ (see pf. of 5.60), such that $f(\Gamma_n) \subset \mathbb{Z}$.]
- 10:19) Suppose
- $\phi: G_1 \rightarrow G_2$ is a (continuous) surjective homomorphism,
 - Γ_1 and Γ_2 are lattices in G_1 and G_2 , respectively, and
 - $\phi(\Gamma_1) \subset \Gamma_2$.
- Show $\phi(\Gamma_1)$ is a finite-index subgroup of Γ_2 . [Hint: Show the invariant measure on G_1/Γ_1 pushes to a G_2 -invariant probability measure on $G_2/\phi(\Gamma_1)$, so $\phi(\Gamma_1)$ is a lattice in G_2 .]
- 10:20) Show $N_{\mathrm{red}}(xy) = N_{\mathrm{red}}(x) N_{\mathrm{red}}(y)$ for all elements x and y of a quaternion algebra $D_{\beta,\gamma}(F)$.
- 10:21) Show that the quaternion algebra $D_{\beta,\gamma}(F)$ is a central division algebra over F if and only if $N_{\mathrm{red}}(x) \neq 0$, for every nonzero $x \in D_{\beta,\gamma}(F)$. [Hint: If $N_{\mathrm{red}}(x) \neq 0$, then multiply the conjugate of x by an element of F to obtain a multiplicative inverse of x . If $N_{\mathrm{red}}(x) = 0$, then x is a zero divisor.]
- 10:22) Let $D = D_{\beta,\gamma}(F)$ be a quaternion algebra over some field F , and let $L = F + Fi \subset D$.
- (a) Show that if β is not a square in F , then L is a subfield of D .
 - (b) Show that D is a two-dimensional (left) vector space over L .
 - (c) For each $x \in D$, define $R_x: D \rightarrow D$ by $R_x(v) = vx$, and show that R_x is an L -linear transformation.
 - (d) For each $x \in D$, show $\det(R_x) = N_{\mathrm{red}}(x)$.
- 10:23) Let τ be an antiinvolution on a division algebra D .
- (a) For any $J \in \mathrm{Mat}_{n \times n}(D)$, define $B_J: D^n \times D^n \rightarrow D$ by
- $$B_J(x, y) = \tau(x^T)Jy$$
- for all $x, y \in D^n = \mathrm{Mat}_{n \times 1}(D)$. Show that B_J is a Hermitian form if and only if $\tau(J^T) = J$.
- (b) Conversely, show that if B is a Hermitian form on D^n , then $B = B_J$, for some $J \in \mathrm{Mat}_{n \times n}(D)$.
- 10:24) Show that if $G = \mathrm{SU}(B; D, \tau_r)$, as in 10.48(5), then there is a skew-Hermitian form B' on D^n , with respect to the standard antiinvolution τ_c , such that $G = \mathrm{SU}(B'; D, \tau_c)$. [Hint: Use the fact that $\tau_r(x) = j^{-1}\tau_c(x)j$.]
- 10:25) Show that $\mathrm{Sp}(p, q)$ has a cocompact lattice. [Hint: Use the proof of Prop. 10.16, with the quaternion algebra $D_{-1,-1}(F)$ in place of L .]
- 10:26) Suppose $F \subset \mathbb{R}$, and $B(x, y)$ is a nondegenerate, symmetric, bilinear form on F^n , such that $[B]$ is diagonal (with respect to some basis). Show that if exactly p of the diagonal entries of $[B]$ are positive, then $\mathrm{SU}(B; \mathbb{R}) \cong \mathrm{SO}(p, n - p)$.
- 10:27) Suppose $F \subset \mathbb{R}$, $D = D_{\beta,\gamma}$ a quaternion division algebra over F , and $B(x, y)$ is a nondegenerate τ_c -Hermitian form on D^n such that $[B]$ is diagonal (with respect to some basis). Show:
- (a) every entry of the matrix $[B]$ belongs to F (and, hence, to $\mathbb{R}$); and
 - (b) if exactly p of the diagonal entries of $[B]$ are positive, then $\mathrm{SU}(B; D, \tau_c) \otimes \mathbb{R} \cong \mathrm{Sp}(p, n - p)$.

- 10:28) Show that $\text{cont}(g_1(x)g_2(x)) = \text{cont}(g_1(x)) \cdot \text{cont}(g_2(x))$, for $g_1(x), g_2(x) \in \mathbb{Z}[x]$. [Hint: Assume $\text{cont}(g_j(x)) = 1$. If $p \mid \text{cont}(g_1(x)g_2(x))$, then $\overline{g_1(x)} \overline{g_2(x)} = 0$ in $\mathbb{Z}_p[x]$.]
- 10:29) Let D be a (finite-dimensional) central algebra over a field F . Show that D is a central division algebra over F if and only if D has no proper, nonzero left ideals. (We remark that, by definition, D is *simple* if and only if it has no proper, nonzero two-sided ideals.)
- 10:30) Suppose G is an irreducible subgroup of $\text{GL}(\ell, \mathbb{C})$, and that B_1 and B_2 are (nonzero) G -invariant quadratic forms on $\mathbb{C}^\ell$. Show that there exists $\lambda \in \mathbb{C}$, such that $B_1 = \lambda B_2$.
- 10:31) (a) Suppose $g(x)$ is a monic polynomial of degree n , and k is a nonzero integer, such that $k g(x) \in \mathbb{Z}[x]$. Show that $k^n g(x/k) \in \mathbb{Z}[x]$.
- (b) Suppose $g(x)$ is a monic, integral polynomial of degree n , and p is a prime. Show that $p^{2n} g(x/p^2) \equiv x^n \pmod{p^2}$.
- (c) Suppose $g(x)$ and $h(x)$ are monic polynomials, and k and n are nonzero integers, such that $h(x) = k^n g(x/k)$. Show that

$$\min\{|h(t)| \mid h'(t) = 0\} = k^n \min\{|g(t)| \mid g'(t) = 0\}.$$

Central division algebras over number fields

Many of the arithmetic groups in Chap. 10 were constructed by using division algebras. Thus, an understanding of division algebras deepens one's understanding of arithmetic groups. For the interested reader, we present some of the basic structure theory, even though it is not needed in later chapters.

11A. How to construct central division algebras over number fields

(11.1) **Example.** Let σ be a Galois automorphism of some quadratic extension $L = F[\sqrt{\beta}]$ of a field F ; for clarity, we may write ${}^\sigma z$, instead of $\sigma(z)$.

- 1) Define a noncommutative F -algebra

$$L[\sigma] = \{a + b\sigma \mid a, b \in L\}$$

with multiplication given by

- (a) $\sigma^2 = 1$ and
- (b) $\sigma z = {}^\sigma z \sigma$ for $z \in L$.

Then $L[\sigma] \cong \text{Mat}_{2 \times 2}(F)$, via the F -linear map defined by

$$1 \mapsto \text{Id}, \quad \sqrt{\beta} \mapsto \begin{bmatrix} 0 & \beta \\ 1 & 0 \end{bmatrix}, \quad \sigma \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sqrt{\beta} \sigma \mapsto \begin{bmatrix} 0 & -\beta \\ 1 & 0 \end{bmatrix}$$

(see Exer. 11:1).

- 2) The quaternion algebra $D_{\beta, \gamma}(F)$ can be obtained by a very slight modification of the preceding construction: define an algebra $L^\gamma[\sigma]$ by replacing (1a) with

$$(1a') \quad \sigma^2 = \gamma.$$

Then $L[\sigma] \cong \text{Mat}_{2 \times 2}(F)$, via the F -linear map defined by

$$1 \mapsto 1, \quad \sqrt{\beta} \mapsto i, \quad \sigma \mapsto j, \quad \sqrt{\beta} \sigma \mapsto k$$

(see Exer. 11:2).

Additional examples of central division algebras can be obtained by generalizing the construction of Eg. 11.1 to field extensions L of degree > 2 . We consider only the case where L is cyclic.

(11.2) **Definition.** Let

- L be a *cyclic extension* of a field F (that is, L is a Galois extension of F , and the Galois group $\text{Gal}(L/F)$ is cyclic);
- σ be a generator of the Galois group $\text{Gal}(L/F)$; and
- $d = |L : F|$ be the degree of L over F .

1) Define an F -algebra

$$L[\sigma] = \left\{ \sum_{j=0}^{d-1} a_j \sigma^j \mid a_j \in L \right\}$$

with multiplication given by

(a) $\sigma z = {}^\sigma z \sigma$ for $z \in L$, and

$$(b) \sigma^j \sigma^k = \begin{cases} \sigma^{j+k} & \text{if } j+k < d, \\ \sigma^{j+k-d} & \text{if } j+k \geq d. \end{cases}$$

Then $L[\sigma] \cong \text{Mat}_{d \times d}(F)$ (see Exer. 11:8).

2) For $\alpha \in F^\times$, let $L^\alpha[\sigma]$ be defined as in (1), but replacing (1b) with

$$(1b') \sigma^j \sigma^k = \begin{cases} \sigma^{j+k} & \text{if } j+k < d, \\ \alpha \sigma^{j+k-d} & \text{if } j+k \geq d. \end{cases}$$

(Thus, $\sigma^d = \alpha$ in $L^\alpha[\sigma]$.) Then $L^\alpha[\sigma]$ is a central simple algebra (see Exers. 11:13 and 11:14).

(11.3) **Example.** For $L = F[\sqrt{\beta}]$, we have $L^\alpha[\sigma] \cong D_{\beta, \alpha}(F)$.

(11.4) **Remark.** If ω is any root of unity, then $F[\omega]$ is a abelian extension of F ; it has many cyclic subextensions. Conversely, a classical theorem of Kronecker and Weber states that if L is a cyclic (or, more generally, abelian) extension of $\mathbb{Q}$, then $L \subset \mathbb{Q}[\omega]$, for some root of unity ω . Unfortunately, there does not seem to be such a simple characterization of the cyclic extensions of other algebraic number fields F . However, because abelian groups are solvable, any abelian extension is contained in an extension obtained by taking a sequence of n^{th} roots, for various n .

The following theorem shows that the above construction yields all of the division algebras of interest to us. Some ideas of the proof appear later in this chapter.

(11.5) **Theorem.** If D is a central division algebra over an algebraic number field F , then there is a cyclic extension L of F , and some $\alpha \in F^\times$, such that $D \cong L^\alpha[\sigma]$.

With the help of Thm. 11.9 below, this can be restated in the following more concrete form:

(11.6) **Definition.** Let L be a cyclic extension of a field F . Define a multiplicative homomorphism $N_{L/F}: L^\times \rightarrow F^\times$ by

$$N_{L/F}(x) = x \cdot \sigma(x) \cdot \sigma^2(x) \cdots \sigma^{d-1}(x),$$

where σ is any generator of $\text{Gal}(L/F)$, and $d = |L : F|$. (Note that $N_{L/F}(x)$ is independent of the choice of σ (see Exer. 11:9).) Then $N_{L/F}(x)$ is called the *norm* of x .

(11.7) **Corollary.** Let

- F be an algebraic number field;
- L be a cyclic extension of F ;
- σ be a generator of $\text{Gal}(L/F)$;
- $d = |L : F|$;

- $p \in F$, such that $p^k \notin N_{L/F}(L)$, for all $k \in \{1, 2, \dots, d-1\}$; and
- $\phi: L^d \rightarrow \text{Mat}_{d \times d}(L)$ be given by

$$\phi(x_1, x_2, \dots, x_d) = \begin{bmatrix} x_1 & x_2 & x_3 & \dots & x_{d-1} & x_d \\ p\sigma(x_d) & \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_{d-2}) & \sigma(x_{d-1}) \\ p\sigma^2(x_{d-1}) & p\sigma^2(x_d) & \sigma^2(x_1) & \dots & \sigma^2(x_{d-3}) & \sigma^2(x_{d-2}) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ p\sigma^{d-2}(x_3) & p\sigma^{d-2}(x_4) & p\sigma^{d-2}(x_5) & \dots & \sigma^{d-2}(x_1) & \sigma^{d-2}(x_2) \\ p\sigma^{d-1}(x_2) & p\sigma^{d-1}(x_3) & p\sigma^{d-1}(x_4) & \dots & p\sigma^{d-1}(x_d) & \sigma^{d-1}(x_1) \end{bmatrix}.$$

Then $\phi(L^d)$ is a central division algebra over F .

Conversely, every central division algebra over F can be constructed in this way.

(11.8) **Remark.** I do not know whether Thm. 11.5 remains valid when F is allowed to be any field (say of characteristic 0), rather than only an algebraic number field.

If $\alpha = 1$ (and $L \neq F$), then $L^\alpha[\sigma]$ is not a division algebra (see Exer. 11:8). The following proposition shows, in general, how to tell whether $L^\alpha[\sigma]$ is a division algebra or not. (It is always a central simple algebra (see 11.2(2)).)

(11.9) **Theorem.** Let σ be a generator of $\text{Gal}(L/F)$, for some cyclic extension L of an algebraic number field F , and let $\alpha \in F^\times$. The ring $L^\alpha[\sigma]$ is a central division algebra over F if and only if $\alpha^k \notin N_{L/F}(L^\times)$, for $k = 1, 2, \dots, d-1$, where $d = |L : F|$.

Proof. The general case is a rather difficult theorem of Algebraic Number Theory, so let us assume that d is prime. This suffices to construct many interesting examples, and we will see that it follows easily from Lem. 11.10 below.

($\Rightarrow$) Suppose $\alpha^k \in N_{L/F}(L^\times)$, with $1 \leq k < d$. Because $\alpha^d = N_{L/F}(\alpha) \in N_{L/F}(L^\times)$ (see Exer. 11:9), we may assume $k|d$ (by replacing k with $\gcd(k, d)$). From our simplifying assumption that d is prime, we conclude that $k = 1$; thus, $\alpha \in N_{L/F}(L^\times)$. So $L^\alpha[\sigma] \cong \text{Mat}_{d \times d}(F)$. Therefore, $L^\alpha[\sigma]$ is not a division algebra.

Alternatively, one can easily give a very elementary proof. We have $1/\alpha = N_{L/F}(x)$, for some $x \in L^\times$. Then

$$(x\sigma)^d = (x \cdot \sigma x \cdot \sigma^2 x \cdots \sigma^{d-1} x)(\sigma^d) = (N_{L/F}(x))(\alpha) = 1,$$

so

$$((x\sigma) - 1)((x\sigma)^{d-1} + (x\sigma)^{d-2} + \cdots + 1) = (x\sigma)^d - 1 = 0,$$

so $x\sigma$ is a zero divisor. Therefore, $L^\alpha[\sigma]$ is not a division algebra.

($\Leftarrow$) Because $L^\alpha[\sigma]$ is central simple (see Exers. 11:13 and 11:14), Wedderburn's Theorem (11.25) implies that $L^\alpha[\sigma] \cong \text{Mat}_{r \times r}(D)$, for some central division algebra D , and some r . Because $r|d$, and d is prime, there are only two possibilities to consider.

If $r = 1$, then $L^\alpha[\sigma] = D$ is a division algebra, as desired.

If $r = d$, then $\deg D = 1$, so $L^\alpha[\sigma] \cong \text{Mat}_{d \times d}(F)$. From Lem. 11.10, we conclude that $\alpha \in N_{L/F}(L^\times)$. $\square$

(11.10) **Lemma.** $L^\alpha[\sigma] \cong \text{Mat}_{d \times d}(F)$ if and only if $\alpha \in N_{L/F}(L^\times)$.

Proof. ($\Leftarrow$) Note that $L^\alpha[\sigma] \cong L^1[\sigma]$ (via the map $\sigma \mapsto x\sigma$). Then the desired conclusion follows from the observation that $L^1[\sigma] \cong \text{Mat}_{d \times d}(F)$ (see Exer. 11:8).

($\Rightarrow$) We have $L^\alpha[\sigma] \cong \text{Mat}_{r \times r}(F) \cong L^1[\sigma]$, so there is some subfield L' of $L^\alpha[\sigma]$, and some $\tau \in L^\alpha[\sigma]$, such that

- L' is isomorphic to L ;
- the map $L' \rightarrow L'$ given by $x \mapsto \tau x \tau^{-1}$ generates $\text{Gal}(L'/F)$; and
- $\tau^d = 1$.

The Noether-Skolem Theorem (11.20) implies that we may assume $L' = L$ (after conjugating by an automorphism of $L^\alpha[\sigma]$). Then, replacing τ by a power, we may assume that $\tau x \tau^{-1} = \sigma x \sigma^{-1}$ for all $x \in L$. So $\tau^{-1} \sigma$ centralizes L . Since L is a maximal subfield (see Exer. 11:13), we conclude that $\sigma = a\tau$, for some $a \in L^\times$. Then

$$\alpha = \sigma^d = (a\tau)^d = (a \cdot \tau a \cdot \tau^2 a \cdots \tau^{d-1} a)(\tau^d) = (N_{L/F}(a))(1),$$

so $\alpha = N_{L/F}(a)$. □

(11.11) **Corollary.** *Let D be a central division algebra of degree d over an algebraic number field F . Then D is an element of order (exactly) d in the Brauer group $\mathcal{B}(F)$ (see Defn. 11.13). That is, $dD = 0$ in $\mathcal{B}(F)$, but $kD \neq 0$ for $1 \leq k < d$.*

Proof. From Thm. 11.5, we know that $D \cong L^\alpha[\sigma]$, for some cyclic extension L of F , and some $\alpha \in F^\times$. From the cohomological approach to division algebras (see §11E), it is not difficult to see that $kD = L^{\alpha^k}[\sigma]$ in $\mathcal{B}(F)$. Therefore, Lem. 11.10 implies that $kD = 0$ if and only if $\alpha^k \in N_{L/F}(L^\times)$. So the desired conclusion follows from Thm. 11.9. □

This has the following important consequence.

(11.12) **Corollary.** *If D is a central division algebra over an algebraic number field F (with $D \neq F$), then the following are equivalent:*

- 1) D is a quaternion algebra (that is, D has degree 2);
- 2) D has an antiinvolution;
- 3) $D \cong D^{\text{op}}$, the opposite algebra, with the same addition and scalar multiplication as D , but with multiplication reversed;
- 4) $2D = 0$ in $\mathcal{B}(F)$.

Proof. (1 $\Rightarrow$ 2) We have the antiinvolutions τ_c and τ_r .

(2 $\Rightarrow$ 3) Any antiinvolution is (by definition) an isomorphism from D to D^{op} .

(3 $\Rightarrow$ 4) Since $D \circ D^{\text{op}} = 0$ in $\mathcal{B}(F)$ (see Exer. 11:15), and $D \cong D^{\text{op}}$, we have $2D = 0$ in $\mathcal{B}(F)$.

(4 $\Rightarrow$ 1) From Cor. 11.11, we see that D has degree 2. □

11B. The Brauer group

(11.13) **Definition** (Brauer group). Let $\mathcal{B}(F)$ be the set of central division algebras over F .

We define a binary, associative operation $\circ$ on $\mathcal{B}(F)$ in the following way: Suppose $D_1, D_2 \in \mathcal{B}(F)$. Then $D_1 \otimes_F D_2$ is a central simple algebra over F (see Defn. 11.19), so Wedderburn's Theorem (11.25) implies that

$$D_1 \otimes_F D_2 \cong \text{Mat}_{n \times n}(D),$$

for some central division algebra D over F (and some n). We define

$$D_1 \circ D_2 = D.$$

This makes $\mathcal{B}(D)$ into an abelian group. (For the existence of inverses, see Exer. 11:15.) It is called the *Brauer group* of F .

Now, the following deep theorem provides a classification of the central division algebras over any algebraic number field.

(11.14) **Theorem** (Brauer-Hasse-Noether Theorem). *If F is an algebraic number field, then*

$$(11.15) \quad \mathcal{B}(F) \cong (\mathbb{Z}_2)^r \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \cdots,$$

where r is the number of real places of F .

Outline of proof. Let us assume $F = \mathbb{Q}$. If D is any central division algebra over $\mathbb{Q}$, then $D \otimes_{\mathbb{Q}} \mathbb{R}$ is a simple algebra, so, by Wedderburn's Theorem (11.25), there is a corresponding central division algebra $D_{\mathbb{R}}$ over $\mathbb{R}$. Thus, we have a natural homomorphism $\mathcal{B}(F) \rightarrow \mathcal{B}(\mathbb{R})$. It is well-known that there are only two central division algebras over $\mathbb{R}$, namely $\mathbb{R}$ and $\mathbb{H}$, so $\mathcal{B}(\mathbb{R}) \cong \mathbb{Z}_2$.

For each prime p , we have a p -adic field $\mathbb{Q}_p$. Since $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a central simple algebra over $\mathbb{Q}_p$, there is a natural homomorphism $\mathcal{B}(F) \rightarrow \mathcal{B}(\mathbb{Q}_p)$. Classifying the central division algebras over $\mathbb{Q}_p$ yields the conclusion that $\mathcal{B}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$.

By combining the preceding paragraphs, we see that there is a natural homomorphism

$$\mathcal{B}(F) \rightarrow \mathcal{B}(\mathbb{R}) \oplus \bigoplus_{p \text{ prime}} \mathcal{B}(\mathbb{Q}_p) \cong \mathbb{Z}_2 \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \cdots.$$

To complete the proof, one shows that the map is injective, and that its image is

$$\{ (a_0, a_1, \dots) \mid a_0 + a_1 + \cdots = 0 \},$$

where we realize $\mathbb{Z}_2$ as the subgroup $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ of $\mathbb{Q}/\mathbb{Z}$. These last steps are the hard part. □

(11.16) **Corollary.** *For every algebraic number field F , and any $d \geq 2$, there are infinitely many central division algebras of degree d over F .*

Proof. From Thm. 11.14, it is clear that there are infinitely many elements of order d in $\mathcal{B}(F)$. Each of these elements corresponds to a central division algebra of degree d over F (see 11.11). □

(11.17) **Corollary.** *Let $d \geq 2$, and consider the central division algebras of degree d over $\mathbb{Q}$.*

- 1) *If d is odd, then all of these division algebras split over $\mathbb{R}$.*
- 2) *If d is even, then infinitely many of these division algebras split over $\mathbb{R}$, and infinitely many do not split.*

Proof. From the pf. of Thm. 11.14, we see that the central division algebras that split over $\mathbb{R}$ correspond to the elements of the RHS of (11.15), such that $a_0 = 0$. Any element with $a_0 \neq 0$ has even order, so all central division algebras of odd degree split over $\mathbb{R}$. (This conclusion can also be proved easily by elementary means.)

On the other hand, if d is even, then it is easy to construct infinitely many elements of order d with $a_0 = 0$, and infinitely many elements of order d with $a_0 \neq 0$. So infinitely many central division algebras split over $\mathbb{R}$, and infinitely many do not split. □

Corollary 11.17 can be generalized to other number fields (see Exer. 11:16).

11C. Division algebras are cyclic

For the special case where F is an algebraic number field, the following theorem shows that the maximal subfield L can be chosen to be a cyclic extension of F .

(11.18) **Theorem.** *If D is a central division algebra over an algebraic number field F , then some maximal subfield L of D is a cyclic, Galois extension of F .*

(11.19) **Definition.** An algebra A over a field F is *central simple* over F if

- 1) A is simple (that is, A has no nontrivial, proper, two-sided ideals),
- 2) the center of A is F , and
- 3) $\dim_F A < \infty$.

(11.20) **Theorem** (Noether-Skolem Theorem). *Let A and B be simple F -subalgebras of a central simple algebra R over a field F . If $\phi: A \rightarrow B$ is any ring isomorphism, such that $\phi|_F = \text{Id}$, then there is an invertible element r of R , such that $\phi(a) = r^{-1}ar$, for all $a \in A$.*

Theorem 11.5 is obtained by combining the following corollary with Thm. 11.18.

(11.21) **Corollary.** *If L is a maximal subfield of a central division algebra D over a field F , and L is cyclic over F , then $D \cong L^\alpha[\sigma]$, for some $\alpha \in F^\times$. (Hence $\dim_F D = d^2$, where $d = |L : F|$.)*

Proof. There is some $r \in D$, such that $\sigma(x) = r^{-1}xr$, for all $x \in L$ (see 11.20). Let $\alpha = r^d$. We have

$$\alpha^{-1}x\alpha = r^{-d}xr^d = \sigma^d(x) = x$$

for all $x \in L$, so $\alpha \in C_D(L) = L$. Furthermore,

$$\sigma(\alpha) = r^{-1}(\alpha)r = r^{-1}(r^d)r = r^d = \alpha,$$

so $\alpha \in F$.

Let

$$R = L[r] = \left\{ \sum_{j=0}^{d-1} a_j r^j \mid a_j \in L \right\} \subset D,$$

so R is a subring of D . Because $C_D(R) = F$, we see, by arguing as in the proof of Prop. 10.43, that $R \otimes_F D \cong \text{Mat}_{n \times n}(F)$, where $n = \dim_F D$. Then

$$(\dim_F R)n \geq \dim_F(R \otimes_F D) = \dim_F \text{Mat}_{n \times n}(F) = n^2,$$

so $\dim_F R \geq n = \dim_F D$. Therefore $R = D$. Hence, $\{1, r, \dots, r^{d-1}\}$ spans D over L .

The set $\{1, \sigma, \dots, \sigma^{d-1}\} = \text{Gal}(L/F)$ is linearly independent over L (as a subset of $\text{End}_F(L)$). (For example, this follows from Prop. 10.26.) Therefore, $\{1, r, \dots, r^{d-1}\}$ is linearly independent over L .

Now, it is clear that $D = R \cong L^\alpha[\sigma]$. □

(11.22) **Remark.** If L is any maximal subfield of a central division algebra D over F , then $|L : F|$ is equal to the degree of D (even if L is not a cyclic extension of F).

11D. Simple algebras are matrix algebras

We now describe two standard results in ring theory that were used above.

(11.23) **Theorem** (Jacobson Density Theorem). *Suppose*

- R is an algebra over some field F ,
- M is a faithful, irreducible R -module that is finite-dimensional over F , and
- $E = \text{End}_R(M)$.

Then

- 1) E is a division algebra,
- 2) R is isomorphic to $\text{Mat}_{d \times d}(E)$, where d is the dimension of M as a vector space over E , and
- 3) after identifying R with $\text{Mat}_{d \times d}(E)$, the module M is isomorphic to E^d .

Proof. (1) This is known as *Schur's Lemma*. Let $c \in E$. It is straightforward to verify that $\ker c$ is an R -submodule of M (because $c \in \text{End}_R(M)$). Hence, $\ker c$ is either $\{0\}$ or all of M (because M is irreducible). Thus, c is either invertible or 0. Because c is an arbitrary element of E , this means that E is a division algebra.

(2, 3) Given an E -basis $\{m_1, \dots, m_d\}$ of M , and any $v_1, \dots, v_d \in M$, we wish to show that there exists $r \in R$ with $rm_j = v_j$ for $j = 1, \dots, d$. That is, we wish to show that the R -submodule $R(m_1, \dots, m_d)$ of M^d generated by $(m_1, \dots, m_d)$ is all of M^d . Let us consider only M^2 , rather than M^d . The proof can be completed by induction (see Exer. 11:21).

Given $m_1, m_2 \in M$, such that

$$m_1 \text{ and } m_2 \text{ are linearly independent over } E,$$

we wish to show that

$$R(m_1, m_2) = M^2.$$

Note that $R(m_1, m_2)$ is (obviously) an R -submodule of M^2 .

The projection of $R(m_1, m_2)$ to $M \times \{0\}$ is an R -submodule of $M \times \{0\}$. It is nontrivial (because it contains $(m_1, 0)$), so the irreducibility of M implies

$$(11.24) \quad \text{the projection of } R(m_1, m_2) \text{ to } M \times \{0\} \text{ is all of } M \times \{0\}.$$

Also, the intersection $R(m_1, m_2) \cap (\{0\} \times M)$ is an R -submodule of $\{0\} \times M$. Because M is irreducible, there are only two possibilities to consider.

Case 1. Assume $R(m_1, m_2) \cap (\{0\} \times M) = \{0\} \times M$. This means that $\{0\} \times M \subset R(m_1, m_2)$, so

$$(\{0\} \times M) + R(m_1, m_2) = R(m_1, m_2).$$

On the other hand, (11.24) can be restated as $(\{0\} \times M) + R(m_1, m_2) = M^2$. Therefore $R(m_1, m_2) = M^2$, as desired.

Case 2. Assume $R(m_1, m_2) \cap (\{0\} \times M) = \{(0, 0)\}$. For each $x \in M$, we know, from (11.24), that there exists $y \in M$ with $(m, y) \in R(m_1, m_2)$. Furthermore, the assumption of this case implies that y is unique. Thus, $R(m_1, m_2)$ is the graph of a well-defined function $f: M \rightarrow M$.

Because the graph of f is an R -submodule of M^2 , it is straightforward to verify that $f \in \text{End}_R(M)$. Furthermore, we have $f(m_1) = m_2$ (because $(m_1, m_2) \in R(m_1, m_2)$). Therefore $m_2 \in Em_1$. This contradicts the fact that m_1 and m_2 are linearly independent over E . $\square$

Should explain why it's called a "density" theorem!!!

The following is an easy, but important, special case of Wedderburn's Theorem on the structure of semisimple artinian rings.

(11.25) **Corollary** (Wedderburn's Theorem). *If A is a central simple algebra over a field F , then A is isomorphic to $\text{Mat}_{n \times n}(D)$, for some n , and some central simple division algebra D over F .*

Proof. Let $\mathfrak{m}$ be a maximal left ideal of A . (Since A is finite dimensional, it is obvious that maximal ideals exist. However, if A is a division algebra, then $\mathfrak{m} = 0$.) Then $A/\mathfrak{m}$ is an irreducible left A -module.

The identity element 1 acts nontrivially on $A/\mathfrak{m}$, so the annihilator of this module is a proper ideal of A . Since A is simple, we conclude that the annihilator is trivial, so the module is faithful. Thus, the Jacobson Density Theorem (11.23) implies that $A \cong \text{Mat}_{n \times n}(D)$. $\square$

11E. Cohomological approach to division algebras

For the interested reader, let us also describe the cohomological approach to division algebras.

(11.26) **Definition.** Let L be a Galois extension of a field F , and let $\Delta = \text{Gal}(L/F)$. To avoid confusion, let us use $*$ to denote the group operation in Δ .

- A function $\alpha: \Delta \times \Delta \rightarrow L^\times$ is a 2-cocycle if it satisfies the *cocycle identity*

$$(11.27) \quad \alpha(\sigma_1, \sigma_2) \alpha(\sigma_1 * \sigma_2, \sigma_3) = \alpha(\sigma_1, \sigma_2 * \sigma_3) \sigma_1(\alpha(\sigma_2, \sigma_3)).$$

- For any $\beta: \Delta \rightarrow L^\times$, define $\delta\beta: \Delta \times \Delta \rightarrow L^\times$ by

$$\delta\beta(\sigma_1, \sigma_2) = \frac{\beta(\sigma_1)^{\sigma_1}(\beta(\sigma_2))}{\beta(\sigma_1 * \sigma_2)}.$$

Then $\delta\beta$ is a 2-cocycle. It is called the *coboundary* of β .

- Define

$$\mathcal{H}^2(L/F, L^\times) = \frac{Z^2(L/F, L^\times)}{B^2(L/F, L^\times)},$$

where $Z^2(L/F, L^\times)$ is the set of 2-cocycles, and $B^2(L/F, L^\times)$ is the set of coboundaries. (Note that the set $Z^2(L/F, L^\times)$ is an abelian group under pointwise multiplication, and $B^2(L/F, L^\times)$ is a subgroup.) This is the (second) *Galois cohomology group* of L over F .

- If L is any extension of F , let

$$\mathcal{B}_L(F) = \{ D \in \mathcal{B}(F) \mid D \text{ splits over } L \}.$$

This is a subgroup of $\mathcal{B}(F)$.

(11.28) **Proposition.** *If L is any Galois extension of F , then $\mathcal{H}^2(L/F, L^\times) \cong \mathcal{B}_L(F)$.*

Proof. Given $\alpha \in Z^2(L/F, L^\times)$, define an F -algebra

$$L_\alpha[\Delta] = \left\{ \sum_{\sigma \in \Delta} a_\sigma \sigma \mid a_\sigma \in L \right\}$$

with multiplication given by

- $\sigma z = {}^\sigma z \sigma$ for $\sigma \in \Delta$ and $z \in L$, and
- $\sigma_1 \sigma_2 = \alpha(\sigma_1, \sigma_2) (\sigma_1 * \sigma_2)$.

(The cocycle identity (11.27) implies that $L_\alpha[\Delta]$ is associative (see Exer. 11:20).)

Now $L_\alpha[\Delta]$ may not be a division algebra, but it turns out that it is always a central simple algebra over F . So the Wedderburn Theorem (11.25) tells us that it is isomorphic to $\text{Mat}_{n \times n}(D_\alpha)$, for some n , and some central division algebra D_α . Define $f(\alpha) = D_\alpha$.

It is easy to see that $f(\alpha_1) = f(\alpha_2)$ if α_1 and α_2 are in the same coset of $B^2(L/F, L^\times)$ (see Exer. 11:17), so f is well defined as a map $\mathcal{H}^2(L/F, L^\times) \rightarrow \mathcal{B}(F)$.

A reasonable effort shows that f is injective.

The proof of Prop. 10.43 shows that $L \otimes_F L_\alpha[\Delta] \cong \text{Mat}_{d \times d}(L)$, so $f(\alpha)$ splits over L . This means that the image of f is contained in $\mathcal{B}_L(F)$.

An argument similar to the proof of Cor. 11.21 shows that every element of $\mathcal{B}_L(F)$ is in the image of f . $\square$

(11.29) **Remark.** Let $\overline{F}$ be the algebraic closure of an algebraic number field F . By definition, $\mathcal{H}^2(\overline{F}/F, \overline{F}^\times)$ is the direct limit of the groups $\mathcal{H}^2(L/F, L^\times)$, where L ranges over all Galois extensions of F . Then $\mathcal{H}^2(\overline{F}/F, \overline{F}^\times) \cong \mathcal{B}(F)$, so the Brauer-Hasse-Noether Theorem (11.14) can be restated as the calculation of a Galois cohomology group.

11F. Notes

This hasn't been written yet!!!

Need references for the theorems quoted without proof!!!

The Kronecker-Weber Theorem (11.4) can be found in [Jan, Thm. 5.9, p. 165].

11G. References

- [Jan] G. J. Janusz: *Algebraic Number Fields*, Academic, New York, 1973. (New version available from the American Mathematical Society.)

Exercises

- 11:1) Show that the F -linear map of Eg. 11.1(1) is an algebra isomorphism.
- 11:2) Show that the F -linear map of Eg. 11.1(2) is an algebra isomorphism.
- 11:3) Suppose $B(x, x)$ is a symmetric, bilinear form on a vector space V over a field F . Show that if B is isotropic, and $\dim_F V \geq 3$, then $\text{SO}(B; F)$ has a nontrivial unipotent element. [Hint: $\text{SO}(1, 2)_F$ has a unipotent element, because it is isogenous to $\text{SL}(2, F)$.]
- 11:4) Show $D_{b^2\beta, c^2\gamma}(F) \cong D_{\beta, \gamma}(F)$, for any nonzero $b, c \in F$. [Hint: An isomorphism is given by $1 \mapsto 1, i \mapsto bi, j \mapsto cj, k \mapsto bck$.]
- 11:5) Show $D_{a^2, \gamma}(F) \cong \text{Mat}_{2 \times 2}(F)$, for any field F , and any $a, \gamma \in F$. [Hint: See the proof of 7.4(1).]
- 11:6) Show that if the ring $D_{a,b}(\mathbb{Q})$ is not a division algebra, then it is isomorphic to $\text{Mat}_{2 \times 2}(\mathbb{Q})$. [Hint: This follows from Wedderburn's Theorem (11.25) or its proof.]
- 11:7) Suppose σ is an involution of a field L , and $B(x, y)$ is a nondegenerate σ -Hermitian form on a vector space V over L . Show that if W is any totally isotropic subspace of V , then $\dim W \leq (\dim V)/2$.
- 11:8) Define $L[\sigma]$ as in Eg. 11.2(1). Show $L[\sigma] \cong \text{Mat}_{d \times d}(F)$. [Hint: Identifying L with F^d yields a natural homomorphism $L[\sigma] \rightarrow \text{Mat}_{d \times d}(F)$.]

- 11:9) Let L be a cyclic extension of F . Show, for $x \in L^\times$, that $N_{L/F}(x)$ is independent of the choice of the generator σ of $\text{Gal}(L/F)$. [Hint: $N_{L/F}(x) = \prod_{\tau \in \text{Gal}(L/F)} \tau(x)$.]
- 11:10) Let L be a cyclic extension of F , with $|L : F| = d$. Show that if $x \in F^\times$, then $N_{L/F}(x) = x^d$.
- 11:11) Let L be a cyclic extension of F , and let F' be a subfield of L that contains F . Show that $N_{L/F}(L^\times) \subset N_{L/F'}(L^\times)$.
- 11:12) Let σ be a generator of $\text{Gal}(L/F)$, for some cyclic extension L of a field F . Show that if $\alpha_1 \in \alpha_2 N_{L/F}(L^\times)$, then $L^{\alpha_1}[\sigma] \cong L^{\alpha_2}[\sigma]$. [Hint: Define $f: L^{\alpha_1}[\sigma] \rightarrow L^{\alpha_2}[\sigma]$ by $f(\sigma^j) = (\beta\sigma)^j$.]
- 11:13) Let L be a cyclic extension of F , and let σ be a generator of $\text{Gal}(L/F)$. Show, for every $\alpha \in F^\times$, that
- (a) the centralizer of L in $L^\alpha[\sigma]$ is L ; and
 - (b) the center of $L^\alpha[\sigma]$ is F .
- 11:14) Let L be a cyclic extension of F , σ be a generator of $\text{Gal}(L/F)$, and $\alpha \in F^\times$. Show that $L^\alpha[\sigma]$ has no nontrivial, proper, two-sided ideals. [Hint: For any $x = \sum_{j=0}^{d-1} a_j \sigma^j \in I$, with $a_0 \neq 0$, and any $b \in L^\times$, the difference $x - bxb^{-1}$ has fewer nonzero terms than x does.]
- 11:15) Show that if D^{op} is the opposite algebra of a central division algebra D over a field F , then D^{op} is the inverse of D in $\mathcal{B}(F)$. [Hint: Recall that the multiplication $*$ in D^{op} is defined by $a * b = ba$. It suffices to show that $D \otimes_F D^{\text{op}} \cong \text{Mat}_{d^2 \times d^2}(F)$, where d is the degree of D . Define a homomorphism $\phi: D \otimes_F D^{\text{op}} \rightarrow \text{End}_F(D)$ by $\phi(a, b)(x) = axb$, and apply the Jacobson Density Theorem (11.23).]
- 11:16) Let F be an algebraic number field, let $d \geq 2$, and consider the central division algebras of degree d over F .
- (a) Show that all of these division algebras split at every imaginary place of F . (That is, if σ is an imaginary place of F , then $D \otimes_F F_\sigma \cong \text{Mat}_{d \times d}(F_\sigma)$.)
 - (b) Show that if d is odd, then all of these division algebras split at every place of F .
 - (c) Show that if d is even, and S is any set of real places of F , then there are infinitely many of these division algebras that split at all of the places in S , but do not split at any real place that is not in S .
- 11:17) Let L be a Galois extension of a field F . Show that if $\alpha_1 \in \alpha_2 Z^2(L/F, L^\times)$, then $L_{\alpha_1}[\text{Gal}(L/F)] \cong L_{\alpha_2}[\text{Gal}(L/F)]$. [Hint: Define $f: L_{\alpha_1}[\text{Gal}(L/F)] \rightarrow L_{\alpha_2}[\text{Gal}(L/F)]$ by $f(\sigma) = \beta(\sigma)\sigma$.]
- 11:18) Let F , D , and f be as in the proof of Prop. 10.43.
- (a) Show that $\text{End}_{f(1 \otimes D)}(D) = f(D \otimes 1)$.
 - (b) Show that if L is any maximal subfield of D , then $\text{End}_{f(L \otimes_F D)}(D) = f(L \otimes 1)$.
- 11:19) Suppose A and B are simple algebras over a field F . Show that if either A or B is central simple over F , then $A \otimes_F B$ is simple.
- 11:20) Let $\alpha: \Delta \times \Delta \rightarrow L^\times$. Show that $L_\alpha[\Delta]$ is associative if and only if α satisfies the cocycle identity (11.27).
- 11:21) Prove 11.23(2) and 11.23(2). [Hint: Given linearly independent $m_1, \dots, m_k \in M$, show that $R(m_1, \dots, m_k) = M^k$. Assume, by induction on k , that $R(m_1, \dots, m_k)$ projects onto all of M^{k-1} . Then $R(m_1, \dots, m_k)$ is either M^k or the graph of an R -equivariant map $f: M^{k-1} \rightarrow M$. The restriction of f to each factor of M_{k-1} defines an element f_i of E . We have $f_1(m_1) + \dots + f_{k-1}(m_{k-1}) = f(m_1, \dots, m_{k-1}) = m_k$.]

Actions on the Circle

(25.1) **Assumption.** In this chapter, we assume

- 1) $\mathbb{R}$ -rank $G \geq 2$,
- 2) no simple factor of G is isogenous to $\mathrm{SL}(2, \mathbb{R})$, and
- 3) Γ is irreducible.

(25.2) **Notation.**

- $S^1 = \mathbb{R}/\mathbb{Z}$ is the circle,
- $\mathrm{Homeo}(S^1)$ is the group of homeomorphisms of S^1 ,
- $\mathrm{Homeo}_+(S^1)$ is the group of orientation-preserving homeomorphisms of S^1 (it is a subgroup of index two in $\mathrm{Homeo}(S^1)$),
- $\mathrm{Diff}^r(S^1)$ is the group of C^r diffeomorphisms of S^1 ,
- $\mathrm{Diff}_+^r(S^1)$ is the group of orientation-preserving C^r diffeomorphisms of S^1 (it is a subgroup of index two in $\mathrm{Diff}^r(S^1)$, and
- we use the notation of group actions: if $\phi: \Gamma \rightarrow \mathrm{Homeo}(S^1)$ is a homomorphism, then, for $\gamma \in \Gamma$ and $x \in S^1$, we often write γx or $\gamma(x)$ for the image of x under the homeomorphism $\phi(\gamma)$.

25A. Overview

It is believed (under the conditions of Assump. 25.1) that Γ has no faithful actions on the circle:

(25.3) **Conjecture.** *If $\phi: \Gamma \rightarrow \mathrm{Homeo}(S^1)$ is any homomorphism, then the kernel of ϕ is nontrivial.*

By passing to a finite-index subgroup, we may assume that Γ is torsion free (see 5.60), in which case, the Margulis Normal Subgroup Theorem (23.1) implies that every nontrivial normal subgroup has finite index. Thus, the conjecture can be restated in the following form (see Exer. 25:1).

(25.3') **Conjecture.** *If $\phi: \Gamma \rightarrow \mathrm{Homeo}(S^1)$ is any homomorphism, then $\phi(\Gamma)$ is finite.*

In other words, some finite-index subgroup of Γ acts trivially on S^1 .

There are four main pieces of evidence for this conjecture (see 25.4, 25.6, 25.7, and 25.10), each of which will be proved later in this chapter.

We wish to show that some finite-index subgroup Γ' of Γ fixes every point of S^1 . A major step in this direction is to show, not that every point is fixed, but that, at least, there exists a point that is fixed:

(25.4) **Theorem.** *If $\phi: \Gamma \rightarrow \text{Homeo}(S^1)$ is any homomorphism, then $\phi(\Gamma)$ has a finite orbit.*

In other words, there is a finite-index subgroup Γ' of Γ , such that Γ' fixes some point of S^1 .

What remains is to show that the rest of the points of S^1 are also fixed. This is a consequence of the following result, if we assume that the action of Γ is differentiable, rather than only continuous. Thus, the conjecture is true if we restrict our attention to diffeomorphisms, rather than allowing homeomorphisms that are not differentiable.

(25.5) **Proposition** (Reeb-Thurston Stability Theorem). *Suppose*

- Λ is a finitely generated subgroup of $\text{Diff}_+(S^1)$,
- Λ has a fixed point, and
- the abelianization $\Lambda/[\Lambda, \Lambda]$ is finite.

Then $\Lambda = \{e\}$ is trivial.

(25.6) **Corollary.** *If $\phi: \Gamma \rightarrow \text{Diff}^1(S^1)$ is any homomorphism, then $\phi(\Gamma)$ is finite.*

The following result shows that if we strengthen the differentiability hypothesis slightly, then the conjecture is true for all Kazhdan groups (see Defn. 20.12). This is a very broad class of groups (including many groups that are not even linear), so one would expect a much stronger result to hold for the special case of arithmetic groups. Thus, this seems to be quite strong evidence for Conjecture 25.3'.

(25.7) **Theorem.** *If*

- Λ is any discrete group with Kazhdan's property T , and
- $\phi: \Lambda \rightarrow \text{Diff}^2(S^1)$ is any homomorphism,

then $\phi(\Lambda)$ is finite.

(25.8) **Remark.** Because lattices in $\text{Sp}(1, n)$ and $F_{4,1}$ are Kazhdan (see 20.19), we conclude that if

- Λ is a lattice in either
 - $\text{Sp}(1, n)$, with $n \geq 2$, or
 - $F_{4,1}$, the form of F_4 with real rank 1,
 and
- $\phi: \Lambda \rightarrow \text{Diff}^2(S^1)$ is any homomorphism,

then $\phi(\Lambda)$ is finite.

(25.9) **Problem.** Does there exist a (discrete) Kazhdan group Λ , and a homomorphism $\phi: \Lambda \rightarrow \text{Homeo}(S^1)$, such that $\phi(\Lambda)$ is infinite?

Our final piece of evidence is that the conjecture is true (without assuming any differentiability) for some choices of Γ .

(25.10) **Theorem.** *Suppose $\phi: \Gamma \rightarrow \text{Homeo}(S^1)$ is any homomorphism.*

- 1) *If $\Gamma = \text{SL}(3, \mathbb{Z})$ (or a finite-index subgroup), then $\phi(\Gamma)$ is finite.*
- 2) *If $\Gamma = \text{SO}(2, 3)_{\mathbb{Z}}$ (or a finite-index subgroup), then $\phi(\Gamma)$ is finite.*

3) If $\mathbb{Q}\text{-rank}(\Gamma) \geq 2$, then $\phi(\Gamma)$ is finite.

The proofs of Thms. 25.7 and 25.10 (and Prop. 25.5) are fairly elementary, but Thm. 25.4 is a deeper result.

25B. Algebraic reformulation of the conjecture

In this section, we show that Conj. 25.3' can be reformulated in a purely algebraic form (see 25.3''). The proof (25.16) has two main parts: having an action on S^1 is almost the same as having an action on $\mathbb{R}$, and having an action on $\mathbb{R}$ is essentially the same as being left orderable.

(25.11) **Definition.** Γ is *left orderable* if there is a left-invariant total order on Γ . More precisely, there is an order relation $<$ on Γ , such that

- 1) $<$ is a total order (that is, for all $\gamma, \lambda \in \Gamma$, either $\gamma < \lambda$ or $\gamma > \lambda$, or $\gamma = \lambda$); and
- 2) $<$ is left-invariant (that is, for all $\gamma, \lambda, \mu \in \Gamma$, if $\gamma < \lambda$, then $\mu\gamma < \mu\lambda$).

(25.12) **Other terminology.** The group Γ is *right orderable* if there is a *right*-invariant total order on Γ . The choice between “left orderable” and “right orderable” is entirely a matter of personal preference: Γ is left orderable if and only if it is right orderable (see Exer. 25:2).

(25.13) **Remark** (see Exer. 25:4). Γ is left orderable if and only if there exists a subset P of Γ , such that

- 1) $\Gamma = P \sqcup \{e\} \sqcup P^{-1}$ (disjoint union), where $P^{-1} = \{\gamma^{-1} \mid \gamma \in P\}$; and
- 2) P is closed under multiplication (that is, $\gamma\lambda \in P$, for all $\gamma, \lambda \in P$).

Thus, we see that being left orderable is a property of the internal algebraic structure of Γ .

(25.3'') **Conjecture.** Γ is not left orderable.

(25.14) **Warning.** We do not (quite) show that the two conjectures are equivalent for each individual group Γ . Rather, if one of the conjectures is valid for all Γ (satisfying (25.1)), then the other conjecture is also valid for all Γ . More precisely, if one of the conjectures is valid for every finite-index subgroup of Γ , then the other conjecture is also valid for Γ .

Let us begin by giving a geometric interpretation of being left orderable.

(25.15) **Lemma.** Γ is left orderable if and only if there is a faithful homomorphism $\phi: \Gamma \rightarrow \text{Homeo}_+(\mathbb{R})$.

Proof. ($\Leftarrow$) For $\gamma, \lambda \in \Gamma$, define

$$\gamma < \lambda \text{ if } \gamma(0) < \lambda(0).$$

It is easy to see that $<$ is transitive and antisymmetric, so it defines a partial order on Γ .

For any $\mu \in \Gamma$, the function $x \mapsto \mu(x)$ is an increasing function on $\mathbb{R}$ (because $\phi(\mu)$ is orientation preserving), so it is easy to verify that $<$ is left-invariant (as required in 25.11(2)).

However, the relation $<$ may not be a total order, because it could happen that $\gamma(0) = \lambda(0)$, even though $\gamma \neq \lambda$. But it is not difficult to modify the definition to deal with this technical point (see Exer. 25:6).

($\Rightarrow$) This implication is not difficult to prove (see Exer. 25:7), but it is not required for our main results. $\square$

(25.16) **Proposition.** There is a counterexample to Conj. 25.3 if and only if there is a counterexample to Conj. 25.3'.

Proof. ($\Leftarrow$) Suppose Γ is left orderable. Then Γ has a faithful action on $\mathbb{R}$ (see 25.15). This implies that Γ acts faithfully on the one-point compactification of $\mathbb{R}$, which is homeomorphic to S^1 .

($\Rightarrow$) Suppose Γ has a faithful action on S^1 . By passing to a subgroup of finite index, we may assume that Γ has a fixed point p (see 25.4). Then Γ acts faithfully on the complement $S^1 \setminus \{p\}$, which is homeomorphic to $\mathbb{R}$. Let Γ' be the subgroup of Γ consisting of the elements that act by orientation-preserving homeomorphisms (so either $\Gamma' = \Gamma$ or $|\Gamma/\Gamma'| = 2$). Then Γ' is left orderable (see 25.15). $\square$

(25.17) **Remark.** In order to prove that Conj. 25.3'' implies Conj. 25.3, we appealed to Thm. 25.4, which is quite deep. A stronger algebraic conjecture (that no central extension of Γ is left orderable) can easily be shown to imply Conj. 25.3 (see Exer. 25:12).

25C. Continuous actions on the circle

In this section, we prove Thm. 25.10(1). This also illustrates the main ideas involved in establishing the other parts of the theorem.

Theorem 25.10(1) can be restated in the following algebraic form (cf. 25.16).

(25.18) **Theorem.** *If Γ is a finite-index subgroup of $\mathrm{SL}(3, \mathbb{Z})$, then Γ is not left orderable.*

Our proof of this theorem is based on Lem. 25.22, which can be viewed as a complete description of the left orderings of a certain nilpotent group, the *discrete Heisenberg group*. Analogously, a proof of Thm. 25.10(2) can be based on a similar description of the left orderings of a slightly different nilpotent group.

(25.19) **Definition.** Suppose $<$ is a left-invariant order relation on Γ . For elements γ and λ of Γ , we say γ is *infinitely smaller* than λ (denoted $\gamma \ll \lambda$) if either $\gamma^i < \lambda$ for all $i \in \mathbb{Z}$ or $\gamma^i < \lambda^{-1}$ for all $i \in \mathbb{Z}$. Notice that the relation $\ll$ is transitive.

(25.20) **Notation.** The commutator $\gamma^{-1}\lambda^{-1}\gamma\lambda$ of elements γ and λ of a group Γ is denoted $[\gamma, \lambda]$. It is straightforward to check that γ commutes with λ if and only if $[\gamma, \lambda] = e$ (the identity element of Γ).

(25.21) **Lemma** (see Exer. 25:13). *Let γ and λ be elements of Γ . If $[\gamma, \lambda]$ commutes with both γ and λ , then $[\lambda^n, \gamma^m] = [\gamma, \lambda]^{-mn}$ for all $m, n \in \mathbb{Z}$.*

(25.22) **Lemma.** *Let γ, λ, ζ be non-identity elements of a right-ordered group H , with $[\gamma, \lambda] = \zeta^k$ for some nonzero $k \in \mathbb{Z}$, and $[\gamma, \zeta] = [\lambda, \zeta] = e$. Then either $\zeta \ll \gamma$ or $\zeta \ll \lambda$.*

Proof. Assume, for simplicity, that $\gamma, \lambda, \zeta^k \geq e$ (see Exer. 25:9) and that $k = 1$ (see Exer. 25:10). We may assume $\zeta \not\ll \gamma$, so $\gamma < \zeta^p$ for some $p \in \mathbb{Z}^+$. Similarly, we may assume $\lambda < \zeta^q$ for some $q \in \mathbb{Z}^+$. Then (using the left-invariance of $<$) we have

$$e < \gamma^{-1}\zeta^p, \quad e < \lambda^{-1}\zeta^q, \quad e < \gamma, \quad e < \lambda, \quad e < \zeta.$$

Hence, for all $n \in \mathbb{Z}^+$, we have

$$\begin{aligned}
 e &< (\gamma^{-1}\zeta^p)^n(\lambda^{-1}\zeta^q)^n\gamma^n\lambda^n && \text{(see Exer. 25:3)} \\
 &= \gamma^{-n}\lambda^{-n}(\gamma^n\lambda^n)\zeta^{(p+q)n} && (\zeta \text{ commutes with } \gamma \text{ and } \lambda) \\
 &= \gamma^{-n}\lambda^{-n}(\lambda^n\gamma^n)\zeta^{-n^2}\zeta^{(p+q)n} && \text{(see 25.21)} \\
 &= \zeta^{-n^2+(p+q)n} \\
 &= \zeta^{\text{negative}} && \text{(if } n \text{ is sufficiently large)} \\
 &< e && \text{(see Exer. 25:3).}
 \end{aligned}$$

This is a contradiction. $\square$

Proof of Thm. 25.18. Suppose Γ is left orderable. (This will lead to a contradiction.) Because Γ has finite index in $\text{SL}(3, \mathbb{Z})$, there is some $k \in \mathbb{Z}^+$ such that the six matrices

$$\begin{aligned}
 \gamma_1 &= \begin{bmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, & \gamma_2 &= \begin{bmatrix} 1 & 0 & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, & \gamma_3 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & k \\ 0 & 0 & 1 \end{bmatrix}, \\
 \gamma_4 &= \begin{bmatrix} 1 & 0 & 0 \\ k & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, & \gamma_5 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ k & 0 & 1 \end{bmatrix}, & \gamma_6 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & k & 1 \end{bmatrix}
 \end{aligned}$$

all belong to Γ . A straightforward check shows that $[\gamma_i, \gamma_{i+1}] = e$ and $[\gamma_{i-1}, \gamma_{i+1}] = (\gamma_i)^{\pm k}$ for $i = 1, \dots, 6$, with subscripts read modulo 6 (see Exer. 25:11). Thus, Lem. 25.22 asserts either $\gamma_i \ll \gamma_{i-1}$ or $\gamma_i \ll \gamma_{i+1}$. In particular, we must have either $\gamma_1 \ll \gamma_6$ or $\gamma_1 \ll \gamma_2$. Assume for definiteness that $\gamma_1 \ll \gamma_2$. (The other case is very similar.) For each i , Lemma 25.22 implies that if $\gamma_{i-1} \ll \gamma_i$, then $\gamma_i \ll \gamma_{i+1}$. Since $\gamma_1 \ll \gamma_2$, we conclude by induction that

$$\gamma_1 \ll \gamma_2 \ll \gamma_3 \ll \gamma_4 \ll \gamma_5 \ll \gamma_6 \ll \gamma_1.$$

Thus $\gamma_1 \ll \gamma_1$, a contradiction. $\square$

For the reader acquainted with root systems (see Chap. 18), let us give a more conceptual presentation of the proof of Thm. 25.18. This version generalizes quite easily to $\text{SO}(2, 3)_{\mathbb{Z}}$.

Alternate version of the proof. The root system of $\text{SL}(3, \mathbb{Z})$ is of type A_2 , pictured in Fig. 25C. For $i = 1, \dots, 6$, let U_i be the root space of Γ corresponding to the root α_i . (Note that $U_i \cong \mathbb{Z}$ is cyclic. In the notation of the above proof, the element γ_i belongs to U_i .) Define

$$\alpha_i \ll \alpha_j \text{ if there exists } u \in U_j, \text{ such that } U_i < u$$

(that is, $v < u$, for all $v \in U_i$).

It is obvious, from Fig. 25C, that $\alpha_{i-1} + \alpha_{i+1} = \alpha_i$, and that $\alpha_i + \alpha_{i+1}$ is not a root, so

$$e \neq [U_{i-1}, U_{i+1}] \subset U_i \quad \text{and} \quad [U_i, U_{i+1}] = e.$$

Hence, Lem. 25.22 implies that either $\alpha_i \ll \alpha_{i-1}$ or $\alpha_i \ll \alpha_{i+1}$. Arguing as in the above proof, we conclude that

$$\alpha_1 \ll \alpha_2 \ll \alpha_3 \ll \alpha_4 \ll \alpha_5 \ll \alpha_6 \ll \alpha_1.$$

Thus $\alpha_1 \ll \alpha_1$, a contradiction. $\square$

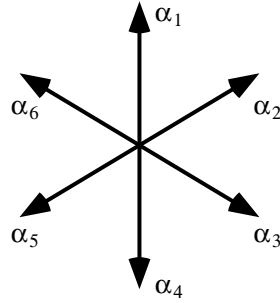


Figure 25.1. The root system of $\mathrm{SL}(3, \mathbb{Z})$ (type A_2).

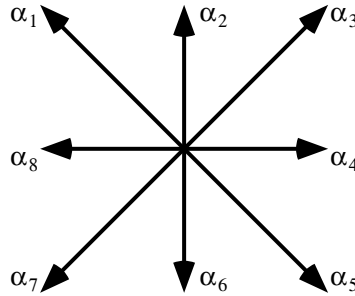


Figure 25.2. The root system of $\mathrm{SO}(2, 3)_{\mathbb{Z}}$ (type B_2).

Proof of Thm. 25.10(2). We adapt the above alternate proof to this situation. Suppose Γ is a finite-index subgroup of $\mathrm{SO}(2, 3)_{\mathbb{Z}}$, such that Γ is left orderable (cf. 25.16). The root system of $\mathrm{SO}(2, 3)_{\mathbb{Z}}$ is of type B_2 , pictured in Fig. 25C.

Let us show that

$$(25.23) \quad \text{either} \quad \alpha_1 \ll \alpha_2 \ll \alpha_3 \quad \text{or} \quad \alpha_1 \ll \alpha_8 \ll \alpha_7.$$

Lem. 25.22 implies that either $\alpha_1 \ll \alpha_2$ or $\alpha_1 \ll \alpha_8$. Let us assume that

$$\alpha_1 \ll \alpha_2.$$

Now $\alpha_3 + \alpha_8 = \alpha_2$, so a generalized version of Lem. 25.22 (see Exers. 25:15 and 25:16) implies that either

$$\alpha_2 \ll \alpha_3 \text{ or } \alpha_2 \ll \alpha_8.$$

We may assume $\alpha_2 \ll \alpha_8$ (otherwise, $\alpha_2 \ll \alpha_3$, so (25.23) holds). Because $\alpha_3 + \alpha_8 = \alpha_2$ we see (from the generalized version of (25.22)) that either $\alpha_2 \ll \alpha_8$ or $\alpha_2 \ll \alpha_3$. If $\alpha_2 \ll \alpha_3$, then we are done, so assume $\alpha_2 \ll \alpha_8$. Then $\alpha_8 \not\ll \alpha_2$, so we conclude (from the generalized version of (25.22)) that $\alpha_8 \ll \alpha_7$. Because $\alpha_1 \ll \alpha_2 \ll \alpha_8$, this implies $\alpha_1 \ll \alpha_8 \ll \alpha_7$, as desired.

Now, from (25.23), we may assume without loss of generality that $\alpha_1 \ll \alpha_2 \ll \alpha_3$. From (25.23) (and symmetry) we know that either $\alpha_3 \ll \alpha_2 \ll \alpha_1$ or $\alpha_3 \ll \alpha_4 \ll \alpha_5$. Clearly, we must have $\alpha_3 \ll \alpha_4 \ll \alpha_5$. Then, by a similar argument, it follows from (25.23) (and symmetry) that $\alpha_5 \ll \alpha_6 \ll \alpha_7$. Therefore, it follows from (25.23) (and symmetry) that $\alpha_7 \ll \alpha_8 \ll \alpha_1$. By transitivity, we have $\alpha_1 \ll \alpha_1$, a contradiction. $\square$

Proof of Thm. 25.10(3). Because $\mathbb{Q}$ -rank $\Gamma \geq 2$, we know Γ contains a subgroup Γ' that is isomorphic to a finite-index subgroup of either $\mathrm{SL}(3, \mathbb{Z})$ or $\mathrm{SO}(2, 3)_{\mathbb{Z}}$ (see 9.28). From 25.10(1) or 25.10(2) (whichever is appropriate) and (25.16), we know that the restriction of ϕ to Γ' is not faithful. So ϕ is not faithful. $\square$

Theorem 25.10(3) establishes Conj. 25.3 for many lattices, but, unfortunately, none of these lattices are cocompact (see 9.21). Apparently, the conjecture remains completely open for cocompact lattices:

(25.24) **Problem.** Find a cocompact lattice Γ , such that no finite-index subgroup of Γ is left orderable.

25D. Smooth actions of Kazhdan groups on the circle

In this section, we prove Thm. 25.7.

Proof of Thm. 25.7. To simplify notation,

- we identify g with $\phi(g)$, for $g \in \Gamma$, and
- we may think of S^1 as $[-\pi/2, \pi/2]$.

In particular, for $g \in \Gamma$ and $r \in S^1$, the derivative $g'(r)$ is a well-defined real number.

We make the following definitions:

- Let $(S^1 \times S^1)$ be the vector space of measurable functions on $S^1 \times S^1$ (with two functions being identified if they are equal almost everywhere).
- Define an action of $\mathrm{Diff}^2(S^1)$ on $(S^1 \times S^1)$ by

$$F^g(r, s) = F(g(r), g(s)) |g'(r)|^{1/2} |g'(s)|^{1/2}$$

for $F \in (S^1 \times S^1)$ and $g \in \mathrm{Diff}^2(S^1)$.

- Let $\|F\|_2 = \left(\int_{S^1} \int_{S^1} F(r, s)^2 dr ds \right)^{1/2}$ be the L^2 -norm of F ; note that $\|F\|_2 = \infty$ if $F \notin L^2(S^1 \times S^1)$.

Note that

$$(25.25) \quad F^{gh} = (F^g)^h \quad \text{and} \quad \|F^g\|_2 = \|F\|_2 \quad \text{for } F \in (S^1 \times S^1) \text{ and } g, h \in \mathrm{Diff}^2(S^1)$$

(see Exer. 25:17).

Choose a function f on S^1 , such that

- f has a $1/x$ pole at the point 0 of S^1 , and
- f is C^∞ everywhere else;

that is, identifying S^1 with $[-\pi/2, \pi/2]$, we have

$$(25.26) \quad f(x) - \frac{1}{x} \in C^\infty(S^1).$$

For example, one may take $f(x) = \cot(x)$.

Now define

$$\Phi(r, s) = f(r - s) \text{ on } S^1 \times S^1.$$

Because of the $1/x$ singularity of f , it is easy to see that $\Phi \notin L^2(S^1 \times S^1)$ (see Exer. 25:18).

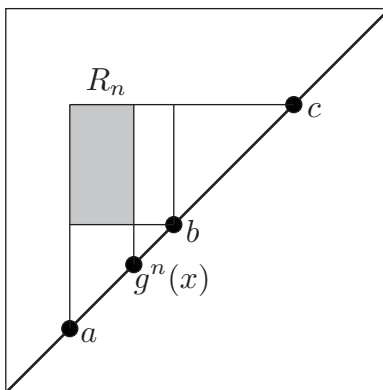


Figure 25.3. A rectangle R_n (shaded) in $S^1 \times S^1$.

For any $g \in \text{Diff}^2(S^1)$, Lem. 25.29 below shows that $\Phi^g - \Phi$ is bounded (this is because the singularity of Φ^g cancels the singularity of Φ). Therefore

$$(25.27) \quad (\Phi + L^2(S^1 \times S^1))^g = \Phi + L^2(S^1 \times S^1) \text{ for all } g \in \text{Diff}^2(S^1).$$

Thus, Γ acts (by isometries) on the affine Hilbert space $\Phi + L^2(S^1 \times S^1)$. One of the several equivalent definitions of Kazhdan's Property T is that there is a fixed point for any action of Γ by isometries on any affine Hilbert space (see 20.26), so we conclude that Γ has a fixed point F in $\Phi + L^2(S^1 \times S^1)$:

$$F^g = F \text{ for all } g \in \Gamma.$$

Because $\Phi \notin L^2(S^1 \times S^1)$, and $F - \Phi \in L^2(S^1 \times S^1)$, it is obvious that $F \notin L^2(S^1 \times S^1)$.

Now, define a measure μ on $S^1 \times S^1$ by $\mu = F^2 dr ds$. Then

- 1) μ is a Γ -invariant measure on $S^1 \times S^1$ (because F is Γ -invariant) (see Exer. 25:19); and
- 2) if $R = (a_1, b_1) \times (a_2, b_2)$ is a rectangle in $S^1 \times S^1$, then

$$\mu(R) = \begin{cases} \infty & \text{if } R \text{ intersects the diagonal;} \\ \text{finite} & \text{if } R \text{ is away from the diagonal.} \end{cases}$$

For example, in Fig. 25.3, the rectangle $(a, b) \times (b, c)$ has infinite measure (see Exer. 25:20), because it touches the diagonal at (b, b) , but the shaded rectangle R_n has finite measure (see Exer. 25:21), because it does not touch the diagonal.

Because Γ is not abelian, we may choose $g \in \Gamma$, such that g has a fixed point (see Exer. 25:22). Then, by passing to a triple cover of S^1 , we obtain an action of (a finite extension of) Γ in which g has at least 3 fixed points:

$$g(a) = a, \quad g(b) = b, \quad g(c) = c.$$

By perhaps replacing a and b with different fixed points, we may assume, for $x \in (a, b)$, that

$$\lim g^n(x) = \begin{cases} b & \text{as } n \rightarrow \infty \\ a & \text{as } n \rightarrow -\infty. \end{cases}$$

For each $n \in \mathbb{Z}$, define

$$R_n = (a, g^n(x)) \times (b, c)$$

(see Fig. 25.3). Then

$$g(R_n) = R_{n+1},$$

so

$$\mu(R_n) = \mu(R_{n+1}).$$

Therefore

$$\begin{aligned} 0 &= \sum_{n=-\infty}^{\infty} (\mu(R_{n+1}) - \mu(R_n)) \\ &= \mu(\cup_{n=-\infty}^{\infty} (R_{n+1} \setminus R_n)) \\ &= \mu((a, b) \times (b, c)). \end{aligned}$$

However, the rectangle $(a, b) \times (b, c)$ touches the diagonal at the point (b, b) , so it has infinite measure (see 25:20). This is a contradiction. $\square$

(25.28) **Remark.** In the proof of Thm. 25.7, the assumption that the elements of Γ are C^2 was used only to establish (25.27). For this, it is not necessary to show that $\Phi^g - \Phi$ is bounded (as in (25.29)), but only that $\Phi^g - \Phi \in L^2(S^1 \times S^1)$. This holds under the weaker hypothesis that $g \in C^{1+\delta}$, for some $\delta > 1/2$ (see Exer. 25:23). Thus, for any $\delta > 1/2$, the group $\text{Diff}^2(S^1)$ can be replaced with $\text{Diff}^{1+\delta}(S^1)$ in the statement of Thm. 25.7.

(25.29) **Lemma.** *In the notation of the proof of Thm. 25.7, the difference $\Phi^g - \Phi$ is a bounded function on $S^1 \times S^1$, for any $g \in \text{Diff}^2(S^1)$.*

Proof. From (25.26), we see that there is no harm in working with the function $\Phi_0(r, s) = 1/(r-s)$, instead of Φ .

$$\begin{aligned} |\Phi^g(r, s) - \Phi(r, s)| &\approx |\Phi_0^g(r, s) - \Phi_0(r, s)| \\ &= \left| \frac{g'(r)^{1/2}g'(s)^{1/2}}{\Phi_0(g(r), g(s))} - \Phi_0(r, s) \right| \\ &= \left| \frac{g'(r)^{1/2}g'(s)^{1/2}}{g(r) - g(s)} - \frac{1}{r - s} \right| \\ &= \left| \frac{g'(r)^{1/2}g'(s)^{1/2}}{g'(t)(r - s)} - \frac{1}{r - s} \right| && (\exists t \in (r, s), \text{ by Mean Value Thm.}) \\ &= \frac{|g'(r)^{1/2}g'(s)^{1/2} - g'(t)|}{g'(t)|r - s|} \\ &= \frac{|g'(r)g'(s) - g'(t)^2|}{(g'(r)^{1/2}g'(s)^{1/2} + g'(t))g'(t)|r - s|} && (\text{multiply by conjugate of numerator}) \\ &= O\left(\frac{|g'(r)g'(s) - g'(t)^2|}{|r - s|}\right) && (g \text{ diffeomorphism} \Rightarrow g' \text{ is never } 0). \end{aligned}$$

Now, we wish to show that the numerator is bounded by a constant multiple of the denominator.

$$\begin{aligned}
|g'(r)g'(s) - g'(t)^2| &\leq g'(r)|g'(s) - g'(t)| && \text{(Triangle inequality)} \\
&\quad + g'(t)|g'(r) - g'(t)| \\
&= g'(r)|g''(u)||s - t| && \text{(Mean Value Thm., applied to } g') \\
&\quad + g'(t)|g''(v)||r - t| \\
&\leq g'(r)|g''(u)||r - s| && (t \in (r, s) \Rightarrow |r - s| > \max\{|s - t|, |r - t|\}) \\
&\quad + g'(t)|g''(v)||r - s| \\
&= O(|r - s|) && (g' \text{ and } g'', \text{ being continuous, are bounded}).
\end{aligned}$$

□

25E. The Reeb-Thurston Stability Theorem

A differentiable action on S^1 that has a fixed point can be transformed into a differentiable action on the unit interval $[0, 1]$ (cf. pf. of 25.16($\Rightarrow$)). Thus, Prop. 25.5 can be reformulated as follows.

(25.5') **Proposition.** *Suppose*

- $I = [0, 1]$ is the unit interval,
- Λ is a finitely generated subgroup of $\text{Diff}_+^1(I)$, and
- the abelianization $\Lambda/[\Lambda, \Lambda]$ is finite.

Then $\Lambda = \{e\}$ is trivial.

Proof. Define $\sigma: \Lambda \rightarrow \mathbb{R}^+$ by $\sigma(\lambda) = \lambda'(0)$. From the Chain Rule, we see that σ is a (multiplicative) homomorphism. Because $\Lambda/[\Lambda, \Lambda]$ is finite and $\mathbb{R}^+$ is abelian, this implies that $\sigma(\Lambda)$ is finite. However, $\mathbb{R}^+$ has no nontrivial, finite subgroups, so this implies that $\sigma(\Lambda)$ is trivial; therefore

$$\lambda'(0) = 1, \text{ for all } \lambda \in \Lambda.$$

For simplicity, let us assume, henceforth, that each element of Λ is real-analytic, rather than merely differentiable. (We remark that there is no need to assume Λ is finitely generated in the real analytic case. The proof in the general case is similar, but requires just a bit of extra effort (see Exer. 25:24).) Thus, each element λ of Λ can be expressed as a power series in a neighborhood of 0:

$$\lambda(x) = x + a_{\lambda,2}x^2 + a_{\lambda,3}x^3 + \cdots.$$

(There is no constant term, because $\lambda(0) = 0$; the coefficient of x is 1, because $\lambda'(0) = 1$.) Then, for $\lambda, \gamma \in \Lambda$, we have

$$\begin{aligned}
x + a_{\lambda\gamma,2}x^2 + O(x^3) &= (\lambda\gamma)(x) \\
&= \lambda(\gamma(x)) \\
&= \gamma(x) + a_{\lambda,2}(\gamma(x))^2 + O(x^3) \\
&= (x + a_{\gamma,2}x^2 + O(x^3)) + a_{\lambda,2}(x + a_{\gamma,2}x^2 + O(x^3))^2 + O(x^3) \\
&= x + (a_{\gamma,2} + a_{\lambda,2})x^2 + O(x^3).
\end{aligned}$$

Thus, the map $\tau: \Lambda \rightarrow \mathbb{R}$, defined by $\tau(\lambda) = a_{\lambda,2}$, is an additive homomorphism. Because $\Lambda/[\Lambda, \Lambda]$ is finite, but $\mathbb{R}$ has no nontrivial, finite subgroups, this implies that $\tau(\Lambda)$ is trivial; therefore $a_{\lambda,2} = 0$ for every $\lambda \in \Lambda$.

By combining this argument with induction on n , one can show that $a_{\lambda,n} = 0$ for each $n \geq 2$ (see Exer. 25:25); thus, $\lambda(x) = x$ for all x in some neighborhood of 0. Because λ is real analytic, we conclude that $\lambda(x) = x$ for all x in I ; thus, λ is trivial. Since λ is an arbitrary element of Λ , we conclude that Λ is trivial, as desired. $\square$

25F. Existence of a finite orbit

In this section, we prove Ghys's Theorem (25.4). To get started, let us show that it suffices to find an invariant measure.

(25.30) **Lemma.** *If*

- $\phi: \Gamma \rightarrow \text{Homeo}(S^1)$ *is any homomorphism, and*
- *there is a $\phi(\Gamma)$ -invariant probability measure μ on S^1 ,*

then $\phi(\Gamma)$ has a finite orbit.

We preface the proof with a definition.

(25.31) **Definition.** Let μ be a measure on a topological space Ω .

- An *atom* of μ is a point $p \in \Omega$, such that $\mu(p) \neq 0$.
- We say that μ is *atomless* if μ has no atoms.

Proof. We consider two cases.

Case 1. Assume μ has at least one atom p . Let

$$\Gamma p = \{ \gamma p \mid \gamma \in \Gamma \}$$

be the orbit of p . Because μ is Γ -invariant, we have $\mu(\gamma p) = \mu(p)$, for every $\gamma \in \Gamma$. Therefore

$$\mu(\Gamma p) = \sum_{\gamma \in \Gamma} \mu(\gamma p) = \sum_{\gamma \in \Gamma} \mu(p) = \#(\Gamma p) \mu(p).$$

Since μ is a probability measure, we know that $\mu(\Gamma p) < \infty$, so we conclude that Γp is a finite set. That is, the orbit of p is finite.

Case 2. Assume μ is atomless. To simplify the proof, let us assume that the support of μ is all of S^1 (see Exer. 25:33). (In other words, every nonempty open subset of S^1 has positive measure.) For $x, y \in S^1$, define

$$(25.32) \quad d(x, y) = \mu([x, y]),$$

where $[x, y]$ is a path from x to y , and, for a given x and y , we choose the path $[x, y]$ to minimize $\mu([x, y])$. It is easy to see that d is a metric on S^1 (see Exer. 25:34).

Because μ is $\phi(\Gamma)$ -invariant, we know that d is $\phi(\Gamma)$ -invariant (see Exer. 25:35). Hence, $\phi(\Gamma)$ consists of orientation-preserving isometries of the metric space (S^1, d) . Up to isometry, there is a unique metric on S^1 (see Exer. 25:36), so we may assume that d is the standard metric. Then every orientation-preserving isometry of S^1 is a rotation (see Exer. 25:37), so we conclude that $\phi(\Gamma)$ is isomorphic to a subgroup of $\text{SO}(2) \cong \mathbb{T}$. Hence, $\phi(\Gamma)$ is abelian. But every abelian homomorphic image of Γ is finite (see 23.3), so we conclude that $\phi(\Gamma)$ is finite. Hence, every orbit is finite. $\square$

Proof of Thm. 25.4. For simplicity, let us assume

$$G = \mathrm{SL}(3, \mathbb{R})$$

(see 25.36). Let

$$P = \begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{bmatrix} \subset G,$$

so P is a minimal parabolic subgroup of G . Because P is amenable (see 20.10), we know that there is a Γ -equivariant, Borel measurable map

$$\psi: G/P \rightarrow \mathrm{Prob}(S^1)$$

(see 20.11). It will suffice to show that ψ is essentially constant, for then:

- the essential range of ψ consists of a single point $\mu \in \mathrm{Prob}(S^1)$, and
- the essential range of ψ is Γ -invariant, because ψ is Γ -equivariant.

So μ is Γ -invariant.

There are two basic cases to consider: either the measure $\psi(x)$ consists entirely of atoms, or $\psi(x)$ has no atoms. It is also possible that $\psi(x)$ consists partly of atoms, and partly of nonatomic, but it is not difficult to reduce to the two extreme cases (see Exer. 25:28).

Case 1. Assume $\psi(x)$ has no atoms, for a.e. $x \in G/P$.

- Let $\mathrm{Prob}_0(S^1) = \{ \mu \in \mathrm{Prob}(S^1) \mid \mu \text{ has no atoms} \}$.
- By assumption, we know $\psi: G/P \rightarrow \mathrm{Prob}_0(S^1)$, so we may define

$$\psi^2: (G/P)^2 \rightarrow (\mathrm{Prob}_0(S^1))^2$$

by $\psi^2(x, y) = (\psi(x), \psi(y))$. Then ψ^2 , like ψ , is measurable and Γ -equivariant.

- Define $d: (\mathrm{Prob}_0(S^1))^2 \rightarrow \mathbb{R}$ by

$$d(\mu_1, \mu_2) = \sup_J |\mu_1(J) - \mu_2(J)|,$$

where J ranges over all intervals (that is, over all connected subsets of S^1).

It is important to note that

$$(25.33) \quad d \text{ is continuous,}$$

with respect to the usual weak* topology that $\mathrm{Prob}_0(S^1)$ inherits from being a subset of $\mathrm{Prob}(S^1)$ (see Exer. 25:29). Because ψ^2 is measurable, this implies that the composition $d \circ \psi^2$ is measurable.

On the other hand, because ψ^2 is Γ -equivariant, and d is Γ -invariant (see Exer. 25:31), we also know that $d \circ \psi^2$ is Γ -invariant. (*Note:* we are saying *invariant*, not just *equivariant*.) From the Moore Ergodicity Theorem, we know that Γ is ergodic on $(G/P)^2$ (see 21.11), so we conclude that $d \circ \psi^2$ is essentially constant; say $d(\psi^2(x, y)) = c$, for a.e. $x, y \in G/P$.

We wish to show that $c = 0$, for then it is clear that $\psi(x) = \psi(y)$ for a.e. $x, y \in G/P$, so ψ is essentially constant.

It is obvious that $d(\psi^2(x, x)) = 0$ for every $x \in G/P$. If ψ were actually constant, rather than merely *essentially* constant, then it would follow immediately that $c = 0$. Unfortunately, the

diagonal $\{(x, x)\}$ is a set of measure 0 in $(G/P)^2$, so a little bit of additional argument is required (see Exer. 25:32). This is where we use the fact that d is continuous, not just measurable.

Case 2. Assume $\psi(x)$ consists entirely of atoms, for a.e. $x \in G/P$. To simplify the notation, without losing the main ideas, let us assume that $\psi(x)$ consists of a single atom, for every $x \in G/P$ (see Exer. 25:39). Thus, we may think of ψ as a Γ -equivariant, measurable map

$$\psi: G/P \rightarrow S^1.$$

Surprisingly, even with the simplifying assumption, the argument here seems to be harder (more subtle) than in Case 1. The idea is to obtain a contradiction from the Γ -equivariance of ψ , by contrasting two fundamental observations:

- $\text{Homeo}_+(S^1)$ is *not* triply transitive on S^1 : if x, y , and z are distinct, then no orientation-preserving homeomorphism of S^1 can map the triple (x, y, z) to (y, x, z) — they have opposite orientations under the circular order on S^1 .
- The action of $\text{GL}(2, \mathbb{R})$ on the projective line $\mathbb{R}P^1 = \mathbb{R} \cup \{\infty\}$ by linear-fractional transformations

$$g(x) = \frac{ax + b}{cx + d} \quad \text{if } g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is triply transitive: if (x_1, y_1, z_1) and (x_2, y_2, z_2) are two ordered triples of distinct elements of $\mathbb{R} \cup \{\infty\}$, then there is some $g \in \text{GL}(2, \mathbb{R})$ with $g(x_1) = x_2$, $g(y_1) = y_2$, and $g(z_1) = z_2$ (see Exer. 25:40).

To illustrate, let us give an easy proof that is not quite correct; the actual proof is a modified version of this. Define

$$\psi^3: (G/P)^3 \rightarrow (S^1)^3 \quad \text{by } \psi^3(x, y, z) = (\psi(x), \psi(y), \psi(z)).$$

Then ψ^3 is Γ -equivariant, so

$$X^+ = \{ (x, y, z) \in (G/P)^3 \mid (\psi(x), \psi(y), \psi(z)) \text{ is positively oriented} \}$$

is a Γ -invariant, measurable subset of $(G/P)^3$. Let us assume that Γ is ergodic on $(G/P)^3$. (This assumption is false (see Exer. 21:1), so it is where the proof breaks down.) Then X^+ must be (essentially) all of $(G/P)^3$; thus, $(\psi(x), \psi(y), \psi(z))$ is positively oriented, for (almost) every $x, y, z \in G/P$. But this is nonsense: either $(\psi(x), \psi(y), \psi(z))$ or $(\psi(y), \psi(x), \psi(z))$ is negatively oriented, so there are many negatively oriented triples.

To salvage the above faulty proof, we replace $(G/P)^3$ with a subset X , on which Γ does act ergodically. Let

- $Q = \begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{bmatrix} \subset G$, and
- $X = \left\{ (x_1, x_2, x_3) \in (G/P)^3 \mid \begin{array}{l} x_1 Q = x_2 Q = x_3 Q, \\ x_1, x_2, x_3 \text{ distinct} \end{array} \right\}.$

Note that X is a submanifold of $(G/P)^3$. (If this is not obvious, it follows from the fact, proven below, that X is a single G -orbit in $(G/P)^3$.)

Assume, for the moment, that Γ is ergodic on X (with respect to any (hence, every) Lebesgue measure on the manifold X). Then the above proof, with X in the place of $(G/P)^3$, implies that

$$X^+ = \{ (x, y, z) \in X \mid (\psi(x), \psi(y), \psi(z)) \text{ is positively oriented} \}$$

is a null set. Then it is not difficult to see that ψ is essentially constant on X . Hence ψ is essentially right Q -invariant: for each $q \in Q$, we have $\psi(xqP) = \psi(xP)$ for a.e. $x \in G/P$.

By a similar argument, we see that ψ is essentially right Q' -invariant, where

$$Q' = \begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix} \subset G.$$

Because Q and Q' , taken together, generate all of G (see Exer. 25:41), it then follows that ψ is essentially right G -invariant (see Exer. 25:42). Hence, ψ is essentially constant (see Exer. 25:44).

All that remains is to show that Γ is ergodic on X . By the Moore Ergodicity Theorem (21.8), we need only show that

- 1) G is transitive on X , and
- 2) the stabilizer of some element of X is not compact.

These are perhaps easiest to see from a geometric perspective.

Recall that a *flag* in $\mathbb{R}^3$ consists of a pair (ℓ, π) , where

- ℓ is a 1-dimensional vector subspace of $\mathbb{R}^3$ (a line), and
- π is a 2-dimensional vector subspace of $\mathbb{R}^3$ (a plane) that contains ℓ .

The group $G = \mathrm{SL}(3, \mathbb{R})$ acts transitively on the set of flags, and P is the stabilizer of the standard flag

$$F_0 = (\ell_0, \pi_0), \text{ where } \ell_0 = \begin{bmatrix} * \\ 0 \\ 0 \end{bmatrix} \text{ and } \pi_0 = \begin{bmatrix} * \\ * \\ 0 \end{bmatrix},$$

so G/P can be identified with the space $\mathcal{F}$ of all flags, by identifying xP with the flag xF_0 .

The (parabolic) subgroup Q is the stabilizer of the plane π_0 . Hence, QF_0 is the set of all flags whose plane is π_0 . Therefore, under the identification of G/P with $\mathcal{F}$, we see that

$$(25.34) \quad X = \left\{ ((\ell_1, \pi_1), (\ell_2, \pi_2), (\ell_3, \pi_3)) \in \mathcal{F}^3 \mid \begin{array}{l} \pi_1 = \pi_2 = \pi_3, \\ \ell_1, \ell_2, \ell_3 \text{ distinct} \end{array} \right\}$$

(see Exer. 25:45).

- (1) Let us show that G is transitive on X . Given

$$((\ell_1, \pi), (\ell_2, \pi), (\ell_3, \pi)), ((\ell'_1, \pi'), (\ell'_2, \pi'), (\ell_3, \pi')) \in X,$$

it suffices to show that there exists $g \in G$, such that

$$(25.35) \quad g((\ell_1, \pi), (\ell_2, \pi), (\ell_3, \pi)) = ((\ell'_1, \pi'), (\ell'_2, \pi'), (\ell_3, \pi')).$$

Because G is transitive on the set of 2-dimensional subspaces, we may assume

$$\pi = \pi' = \pi_0 = \mathbb{R}^2.$$

Then, because $\mathrm{GL}(2, \mathbb{R})$ is triply transitive on $\mathbb{R}P^1$, there exists $T \in \mathrm{GL}(2, \mathbb{R})$, such that

$$T(\ell_1, \ell_2, \ell_3) = (\ell'_1, \ell'_2, \ell'_3).$$

Letting

$$g = \begin{bmatrix} T & 0 \\ 0 & 1/(\det T) \end{bmatrix}$$

yields (25.35).

(2) Let us show that the stabilizer of some element of X is not compact. Let

$$A = \left\{ \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1/a^2 \end{bmatrix} \mid a \in \mathbb{R}^\times \right\}.$$

Then A is a closed, noncompact subgroup of G . Furthermore, every element of A acts as a scalar on π_0 , so every element of A fixes every 1-dimensional vector subspace of π_0 . Thus, if

$$((\ell_1, \pi), (\ell_2, \pi), (\ell_3, \pi)) \in X,$$

with $\pi = \pi_0$, then A is contained in the stabilizer of this element of X , so the stabilizer is not compact. $\square$

(25.36) **Remark.** To generalize the proof of Thm. 25.4 to groups G other than $\mathrm{SL}(3, \mathbb{R})$, it is helpful to use a somewhat different manifold for X , replacing the parabolics P and Q with much smaller subgroups. Let

- $\mathrm{SL}^\pm(2, \mathbb{R}) = \{ T \in \mathrm{GL}(2, \mathbb{R}) \mid \det T = \pm 1 \},$
- $L = \left\{ \begin{bmatrix} T & 0 \\ 0 & 1/(\det T) \end{bmatrix} \mid T \in \mathrm{SL}^\pm(2, \mathbb{R}) \right\} \subset \mathrm{SL}(3, \mathbb{R}) = G;$
- $B = L \cap P = \left\{ \begin{bmatrix} a & b & 0 \\ 0 & d & 0 \\ 0 & 0 & 1/(ad) \end{bmatrix} \right\};$
- $X = \left\{ (x_1 B, x_2 B, x_3 B) \in (G/B)^3 \mid \begin{array}{l} x_1 L = x_2 L = x_3 L, \\ x_1 B, x_2 B, x_3 B \text{ distinct} \end{array} \right\}.$

Then G is transitive on X , with noncompact stabilizer (see Exer. 25:46), so Γ is ergodic on X .

Lift ψ to a $(\Gamma$ -equivariant) map $\tilde{\psi}: G \rightarrow S^1$. Because $B \subset P$, the map ψ induces a well-defined $(\Gamma$ -equivariant) map $\tilde{\psi}: G/B \rightarrow S^1$. Then the above proof shows that $\tilde{\psi}$ is (essentially) right L -invariant, so ψ is (essentially) right L -invariant. By a similar argument, ψ is (essentially) right L' -invariant, where

$$L' = \left\{ \begin{bmatrix} 1/(\det T) & 0 \\ 0 & T \end{bmatrix} \mid T \in \mathrm{SL}^\pm(2, \mathbb{R}) \right\} \subset \mathrm{SL}(3, \mathbb{R}) = G.$$

By definition, ψ is right P -invariant. Taken together, P , L , and L' generate G , so we conclude that ψ is right G -invariant. Therefore, ψ is essentially constant.

It is not difficult to generalize this version of the proof to other semisimple groups G . Numerous proofs in Lie theory rely on the fact that G contains many copies of $\mathrm{SL}(2, \mathbb{R})$ – enough to generate G . By a similar argument, it is not difficult to find enough copies of $\mathrm{SL}^\pm(2, \mathbb{R})$ so that, taken together with P , they generate all of G (under our assumption that no simple factor of G is isogenous to $\mathrm{SL}(2, \mathbb{R})$).

(25.37) **Remark.** It is a fairly elementary (though not obvious!) observation that if the second bounded cohomology group $\mathcal{H}_b^2(\Gamma; \mathbb{R})$ vanishes, then every action of Γ on S^1 has a finite orbit (cf. Exer. 25:47). Thus, another approach to the proof of Thm. 25.4 could be to establish that $\mathcal{H}_b^2(\Gamma; \mathbb{R}) = 0$. It has been shown, under the assumption of (25.1), that the natural comparison map $\mathcal{H}_b^2(\Gamma; \mathbb{R}) \rightarrow \mathcal{H}^2(\Gamma; \mathbb{R})$ is injective. This yields a completely different proof of Thm. 25.4 under the additional hypothesis that $\mathcal{H}^2(\Gamma; \mathbb{R}) = 0$, an assumption that is true for many interesting arithmetic groups Γ .

25G. Complements

25Ga. Some arithmetic groups that do act on the circle. In this section, we discuss the need for Assump. 25.1. To reduce the possibility of confusion, we use G_0 and Γ_0 to denote the groups considered in this section, because they are not required to satisfy (25.1). Thus,

$$\Gamma_0 \text{ is a lattice in } G_0.$$

The following two conjectures suggest that Conj. 25.3' fails for lattices in $\mathrm{SO}(1, n)$. Thus, Assump. 25.1(1) cannot be omitted, although it may be possible to weaken it.

(25.38) **Conjecture.** *If $G_0 = \mathrm{SO}(1, n)$, then there are*

- *a finite-index subgroup Γ' of Γ_0 , and*
- *a surjective homomorphism $\phi: \Gamma' \rightarrow \mathbb{Z}$.*

Because $\mathbb{Z}$ obviously has a C^∞ action on the circle (by rotations) that is faithful and has no finite orbits, this implies the following conjecture:

(25.39) **Conjecture.** *If $G_0 = \mathrm{SO}(1, n)$, then there are*

- *a finite-index subgroup Γ' of Γ_0 , and*
- *a homomorphism $\phi: \Gamma' \rightarrow \mathrm{Diff}^\infty(S^1)$, such that*
 - 1) *$\phi(\Gamma')$ is infinite, and*
 - 2) *$\phi(\Gamma')$ has no finite orbits.*

These conjectures have been proved almost completely, under the assumption that Γ_0 is arithmetic.

(25.40) **Theorem.** *If*

- $G_0 = \mathrm{SO}(1, n)$,
- Γ_0 *is arithmetic, and*
- $n \notin \{3, 7\}$,

then the conclusions of Conjs. 25.38 and 25.39 hold.

(25.41) **Remark.**

- 1) There exist lattices in $\mathrm{SO}(1, 3)$ that act *faithfully* on S^1 . (Thus, Conj. 25.3 fails for these lattices.) It would be very interesting to know whether or not there exist such lattices in $\mathrm{SO}(1, n)$ for $n \geq 4$, or in other groups of real rank one.
- 2) The conclusions of Conj. 25.38 and 25.39 hold for the non-arithmetic “hybrid” lattices constructed in §7D. Thus, a counterexample to these conjectures would have to be constructed by some other method.

The following elementary observation shows that Assump. 25.1(2) is necessary in Conjs. 25.3 and 25.3'.

(25.42) **Proposition.** *If G_0 has a simple factor that is isogenous to $\mathrm{SL}(2, \mathbb{R})$, then there is a homomorphism $\phi: \Gamma_0 \rightarrow \mathrm{Diff}^\infty(S^1)$, such that*

- 1) *$\ker \phi$ is finite, and*
- 2) *$\phi(\Gamma_0)$ has no finite orbits.*

Proof. By assumption, there is a surjective homomorphism $\phi_0: G_0 \rightarrow \mathrm{PSL}(2, \mathbb{R})$. Let

$$\psi: \mathrm{PSL}(2, \mathbb{R}) \rightarrow \mathrm{Diff}^\infty(S^1)$$

represent the usual action by linear-fractional transformations. Then the composition $\phi = (\psi \circ \phi_0)|_{\Gamma_0}$ satisfies (1) and (2) (see Exer. 25:48). $\square$

(25.43) **Remark.** If (1) and (3) of 25.1 hold, then any action of Γ_0 on S^1 has a quotient that is constructed from an $\mathrm{SL}(2, \mathbb{R})$ -factor of G_0 as in the proof of Prop. 25.42.

(25.44) **Remark.**

- 1) Assumption 25.1(3) cannot be omitted from Conj. 25.3 (cf. Exer. 25:49).
- 2) Assumption 25.1(3) cannot be omitted from Conj. 25.3', but, up to commensurability, the question of whether or not Γ_0 has an interesting action on S^1 reduces to the same question about its irreducible factors (see Exer. 25:50), so, in relation to this conjecture, the assumption is merely a convenience.

25Gb. Actions on manifolds of higher dimension. Up to this point, the topic of this chapter has been the conjecture that Γ has no interesting actions on a compact 1-manifold (see 25.3'). With more restrictive assumptions on G , it is conjectured that there are no interesting actions on manifolds of other small dimensions. This is easiest to state for the case $G = \mathrm{SL}(n, \mathbb{R})$.

(25.45) **Conjecture.** *If*

- Γ is a lattice in $\mathrm{SL}(n, \mathbb{R})$ (with $n \geq 3$),
- M is a compact manifold,
- $1 + \dim M < n$, and
- $\phi: \Gamma \rightarrow \mathrm{Diff}^\infty(M)$,

then $\phi(\Gamma)$ is finite.

(25.46) **Remark.** This conjecture generalizes to irreducible lattices Γ in more general G , by requiring that

- $1 + \dim M$ is smaller than the dimension of every nontrivial $\mathfrak{g}$ -module, and
- $(1 + \dim M)(2 + \dim M)/2$ is smaller than the dimension of every simple factor of G .

See Exers. 25:51 and 25:52 for some standard examples that motivate these requirements.

There has been very little progress on this conjecture (except when $\dim M = 1$), but there has been a lot of activity on the special case of volume-preserving actions.

(25.47) **Conjecture.** *If*

- Γ is a lattice in $\mathrm{SL}(n, \mathbb{R})$ (with $n \geq 3$),
- M is a compact manifold,
- $\dim M < n$,
- $\phi: \Gamma \rightarrow \mathrm{Diff}^\infty(M)$, and
- there is a $\phi(\Gamma)$ -invariant volume form on M ,

then $\phi(\Gamma)$ is finite.

(25.48) **Remark.** This conjecture generalizes to irreducible lattices Γ in more general G , allowing the dimension of M to be one greater than it would have to be to satisfy the conditions of Rem. 25.46.

The conjecture has been verified when $\dim M = 2$:

(25.49) **Theorem.** *If*

- Γ is a finite-index subgroup of $\mathrm{SL}(n, \mathbb{Z})$ (with $n \geq 3$),
- M is a compact manifold,
- $\dim M = 2$,
- $\phi: \Gamma \rightarrow \mathrm{Diff}^\infty(M)$, and
- there is a $\phi(\Gamma)$ -invariant volume form on M ,

then $\phi(\Gamma)$ is finite.

There are also results, such as the following, for manifolds of higher dimension, under the assumption that the action is real analytic.

(25.50) **Theorem.** *If*

- Γ is a finite-index subgroup of $\mathrm{SL}(n, \mathbb{Z})$, with $n \geq 8$,
- M is a compact manifold,
- $\dim M = 4$,
- the Euler characteristic of M is nonzero,
- $\phi: \Gamma \rightarrow \mathrm{Diff}^\omega(M)$, and
- there is a $\phi(\Gamma)$ -invariant volume form on M ,

then $\phi(\Gamma)$ is finite.

25Gc. Isometric actions on trees. The real line and the circle are the only connected 1-manifolds, but graphs are another important class of 1-dimensional structures. They can be thought of as 1-dimensional simplicial complexes, but we use a less sophisticated (more algebraic) definition.

(25.51) **Definition.**

- A *graph* X is a pair (V, E) , where
 - V is a nonempty set, and
 - E is a collection of 2-element subsets of V .
 The elements of $V = V(X)$ are the *vertices* of X , and the elements of $E = E(X)$ are the *edges* of X .
- For any nonempty set V ,
 - the *empty graph* on V is the pair $(V, \emptyset)$ (a graph with no edges), and
 - the *complete graph* on V is the pair $K_V = (V, V^{(2)})$, where $V^{(2)}$ is the collection of *all* 2-element subsets of V .
- An *automorphism* of a graph $X = (V, E)$ is a bijection $\phi: V \rightarrow V$, such that $\phi(\{x, y\}) \in E$ if and only if $\{x, y\} \in E$, for all $x, y \in V$.
- We use $\mathrm{Aut}(X)$ to denote the automorphism group of a graph X .

(25.52) **Remark.** The automorphism group of the empty graph is the entire group of all permutations on V (and the same is true of the complete graph), so it is easy to construct a graph X , and a homomorphism $\phi: \Gamma \rightarrow \mathrm{Aut}(X)$, such that

- $\phi(\Gamma)$ is transitive on $V(X)$, and
- no nontrivial element of $\phi(\Gamma)$ has a fixed point on $V(X)$.

Cayley graphs (see Exer. 25:53) provide examples that are more interesting. In particular, X can be constructed to be both connected and of finite valence (see Defns. 25.53 and 25.53).

Remark 25.52 implies that there is no restriction on the groups that act on an arbitrary graph. Focusing our attention on the groups that act on trees (see Defn. 25.54) leads to an interesting theory (the *Bass-Serre theory of group actions on trees*). We discuss only the special case where Γ is an arithmetic group satisfying Assump. 25.1.

(25.53) **Definition.** Suppose $X = (V, E)$ is a graph.

- A *walk* in X is a finite sequence $v_0, v_1, \dots, v_n$ of vertices of X , such that $\{v_i, v_{i+1}\} \in E$, for $i = 0, \dots, n-1$. We say that the walk is from v_0 to v_n .
- A *path* in X is a walk $v_0, v_1, \dots, v_n$, such that $v_0, v_1, \dots, v_n$ are distinct.
- We say that X is *connected* if, for all vertices u and v of X , there is a walk from u to v .

(25.54) **Definition.** A connected graph is a tree if and only if, for every pair of vertices u and v , there is a unique path from u to v . (See Exer. 25:55 for a slightly different, but equivalent, definition.)

(25.55) **Notation.** For vertices u and v of a tree T , the unique path from u to v is often denoted $[u, v]$.

It is easy to construct a faithful action of Γ on a tree (see Exer. 25:56), even if we assume that every vertex has finite valence (see Exer. 25:57). However, the following theorem states that every such action has a finite orbit. This can be thought of as an analogue of Thm. 25.4 for actions on trees.

(25.56) **Theorem.** *If*

- Assump. 25.1 holds,
- T is a tree, and
- $\phi: \Gamma \rightarrow \text{Aut}(T)$,

then $\phi(\Gamma)$ has a finite orbit on $V(T)$.

(25.57) **Remark.** In fact, the finite orbit can be taken to be either a single vertex or a single edge of T (see Exer. 25:60).

(25.58) **Other terminology.** A group Λ is said to have *property (FA)* if every action of Λ on a tree has a finite orbit; thus, Thm. 25.56 is precisely the statement that Γ has property (FA). The “A” in “(FA)” is for “arbre,” the French word for “tree,” because this is a property about actions on trees. The “F” is for “fixed point,” because placing a slight restriction on the action of Γ guarantees that there will be a fixed point, not just a finite orbit (see 25.63).

(25.59) **Remark.** A fundamental conclusion of the Bass-Serre theory is that a countable group Λ has property (FA) if and only if

- 1) Λ is finitely generated,
- 2) $\Lambda/[\Lambda, \Lambda]$ is finite, and
- 3) Λ cannot be written in any nontrivial way as a free product with amalgamation $A *_C B$.

We know that Γ is finitely generated (see 5.57) and that $\Gamma/[\Gamma, \Gamma]$ is finite (see 23.3). Thus, in algebraic terms, Thm. 25.56 is the assertion that Γ is not a free product with amalgamation.

We will prove only two special cases of the theorem (see 25.60 and 25.71).

(25.60) **Theorem.** *If*

- $\Gamma = \mathrm{SL}(3, \mathbb{Z})$
- T is a tree, and
- $\phi: \Gamma \rightarrow \mathrm{Aut}(T)$,

then $\phi(\Gamma)$ has a finite orbit on $V(T)$.

Before proving Thm. 25.60, let us establish some definitions and lemmas. Like the proof of Thm. 25.10(1), the argument is based on an understanding of the *discrete Heisenberg group* (see 25.65). The theorem generalizes to $\mathrm{SL}(n, \mathbb{Z})$, but we assume $n = 3$ to simplify the notation in the proof.

(25.61) **Definition.** Suppose $X = (V, E)$ is a graph.

- The *length* of the walk $v_0, v_1, \dots, v_n$ is n (the number of edges in the walk).
- The *distance* $d(u, v)$ from u to v is the length of the shortest path from u to v . (By convention, this is ∞ if there does not exist such a path. However, if X is connected, then $d(u, v)$ is finite for all $u, v \in V$ (see Exer. 25:54).)
- A subset B of V is *bounded* if $\sup_{x, y \in B} d(x, y) < \infty$.
- The *valence* (or *degree*) of a vertex x is the number of edges that contain x . The *valence* of X is the supremum of the valences of its vertices.

(25.62) **Definition.** Suppose T is a tree.

- An automorphism σ of T is *without inversion* if there does *not* exist an edge $\{x, y\}$ of T , such that $\sigma(x) = y$ and $\sigma(y) = x$.
- A homomorphism $\phi: \Lambda \rightarrow \mathrm{Aut}(T)$ is *without inversion* if $\phi(\lambda)$ is without inversion, for each $\lambda \in \Lambda$.
- An *axis* of an automorphism σ of T is a σ -invariant, bi-infinite path $\dots, v_{-1}, v_0, v_1, v_2, \dots$.
- A *subtree* of T is a subset T' of $V(T)$, such that T' contains the path from v to w , for every $v, w \in T'$.

From the barycentric subdivision, one sees that there is no loss of generality in assuming that an action is without inversion (see Exer. 25:58). But the following lemma shows that this assumption often allows us to ignore the difference between a finite orbit and a fixed point.

(25.63) **Lemma** (cf. Exer. 25:60). *If $\phi: \Gamma \rightarrow \mathrm{Aut}(T)$ is without inversion, and $\phi(\Gamma)$ has a finite orbit on $V(T)$ (or, more generally, a bounded orbit on $V(T)$), then $\phi(\Gamma)$ fixes some vertex of T .*

(25.64) **Lemma** (see Exer. 25:62). *Suppose σ is an automorphism of a tree T , such that*

- σ is without inversion, and
- σ has no fixed point on $V(T)$.

Then:

- 1) σ has a unique axis $\dots, v_{-1}, v_0, v_1, v_2, \dots$, and
- 2) there is some $p \in \mathbb{Z}$, such that $\sigma(v_k) = v_{k+p}$, for all $k \in \mathbb{Z}$.

(25.65) **Proposition.** *If*

- $H = \langle \gamma, \lambda, \zeta \mid [\gamma, \lambda] = \zeta, \gamma\zeta = \zeta\gamma, \lambda\zeta = \zeta\lambda \rangle$ is the discrete Heisenberg group,
- T is a tree, and

- $\phi: H \rightarrow \text{Aut}(T)$, without inversion,

then $\phi([H, H])$ fixes some vertex of T .

Proof. Because $\langle \zeta \rangle = [H, H]$, we may assume that ζ has no fixed point (otherwise, the desired conclusion holds). Therefore, ζ has a unique axis $\{v_k\}_{k=-\infty}^{\infty}$, and there is some p , such that $\zeta(v_k) = v_{k+p}$ for all k (see 25.64). Because γ and λ commute with ζ , the uniqueness implies that

- the axis is invariant under both γ and λ , and
- there exist m and n , such that $\gamma(v_k) = v_{k+m}$ and $\lambda(v_k) = v_{k+n}$, for all k (see Exer. 25:63).

Then

$$\zeta(v_k) = (\gamma^{-1}\lambda^{-1}\gamma\lambda)(v_k) = v_{k+n+m-n-m} = v_k,$$

so each v_k is fixed by ζ . □

(25.66) **Corollary.** *If*

- $H = \langle \gamma, \lambda, \zeta \mid [\gamma, \lambda] = \zeta, \gamma\zeta = \zeta\gamma, \lambda\zeta = \zeta\lambda \rangle$ is the discrete Heisenberg group,
- T is a tree,
- $\phi: H \rightarrow \text{Aut}(T)$, without inversion, and
- the automorphisms $\phi(\gamma)$ and $\phi(\lambda)$ each fix some vertex of T ,

then $\phi(H)$ fixes some vertex of T .

Proof. Let F_γ , F_λ , and F_ζ be the set of all vertices fixed by $\phi(\gamma)$, $\phi(\lambda)$, and $\phi(\zeta)$, respectively. By assumption, and Prop. 25.65, each of these sets is nonempty. So each is a subtree of T (see Exer. 25:64).

Let us now show that $F_\gamma \cap F_\zeta \neq \emptyset$. If this were not the case, then there would be a unique path $[u, v]$ of minimal length from F_γ to F_ζ (see Exer. 25:61). It is obvious that F_γ is invariant under $\phi(\gamma)$. Because $\phi(\gamma)$ commutes with $\phi(\zeta)$, we also know that F_ζ is invariant under $\phi(\gamma)$. Hence, the uniqueness implies that $[u, v]$ is invariant under $\phi(\gamma)$. So v is invariant under $\phi(\gamma)$, which means $v \in F_\gamma$. From the choice of the path $[u, v]$, we know that v also belongs to F_ζ . So $v \in F_\gamma \cap F_\zeta$.

Because λ normalizes $\langle \gamma, \zeta \rangle$, we know that $F_\gamma \cap F_\zeta = F_{\langle \gamma, \zeta \rangle}$ is $\phi(\lambda)$ -invariant. Hence, the argument of the preceding paragraph shows that $F_H = F_\lambda \cap (F_\gamma \cap F_\zeta) \neq \emptyset$. □

The following proposition will allow us to combine the fixed points of Heisenberg subgroups of $\text{SL}(3, \mathbb{Z})$ into fixed points of the entire group. We precede it with a lemma.

(25.67) **Lemma.** *If*

- σ is an automorphism of a tree T , and
- σ fixes some vertex of T ,

then, for any vertex v of T ,

- 1) $d(v, \sigma(v))$ is even, and
- 2) the midpoint of the path $[v, \sigma(v)]$ is fixed by σ .

Proof. Let F be the set of all vertices that are fixed by σ . We may assume $v \notin F$ (otherwise, we have $d(v, \sigma(v)) = 0$, so the desired conclusions are obvious). Then there is a unique path $[v, w]$ of minimal length from v to F (see Exers. 25:64 and 25:61). (Note that $\sigma([v, w]) = [\sigma(v), w]$.) It is not difficult to see (from the uniqueness of paths) that each vertex of $[v, w] \cap \sigma([v, w])$ is fixed by σ (see Exer. 25:65), so, from the minimality of $[v, w]$, we know that $[v, w] \cap \sigma([v, w]) = \{w\}$. Then

$[v, w] \cup [w, \sigma(v)]$ is a path from v to $\sigma(v)$. Its length, $2d(v, w)$, is even, and its midpoint, w , is fixed by σ . $\square$

(25.68) **Proposition.** *Suppose*

- $T = (V, E)$ is a tree,
- $\phi: \Lambda \rightarrow \text{Aut}(T)$, without inversion,
- $a_1, \dots, a_n$ and g are elements of Λ ,
- the subgroup $\langle a_1, \dots, a_n \rangle$ generated by $\{a_1, \dots, a_n\}$ fixes some vertex of T , and
- the elements $ga_1, \dots, ga_n$ and g each fix some vertex of T .

Then $\langle a_1, \dots, a_n, g \rangle$ fixes some vertex of T .

Proof. Let v be a vertex that is fixed by $\langle a_1, \dots, a_n \rangle$, and let w be the midpoint of the path $[v, g(v)]$. From Lem. 25.67, we know that

w is fixed by g .

From the choice of v , we have $ga_k(v) = g(v)$, for each k , so the midpoint of $[v, ga_k(v)] = [v, g(v)]$ is w ; thus, Lem. 25.67 implies that

w is fixed by ga_k , for each k .

Therefore, w is fixed by

$$\langle g, a_1g, a_2g, \dots, a_ng \rangle = \langle a_1, a_2, \dots, a_n, g \rangle,$$

as desired. $\square$

Proof of Thm. 25.60. There is no harm in assuming that ϕ is without inversion (see Exer. 25:58).

Much as in the proof of Thm. 25.18, let

$$\begin{aligned} \gamma_1 &= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, & \gamma_2 &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, & \gamma_3 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \\ \gamma_4 &= \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, & \gamma_5 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, & \gamma_6 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}. \end{aligned}$$

A straightforward check shows that $[\gamma_i, \gamma_{i+1}] = e$ and $[\gamma_{i-1}, \gamma_{i+1}] = (\gamma_i)^{\pm 1}$ for $i = 1, \dots, 6$, with subscripts read modulo 6 (see Exer. 25:11). Thus, Prop. 25.65 implies:

(25.69) for each i , γ_i fixes some vertex of T .

From (25.69), we know that γ_{i-1} and γ_{i+1} each fix some vertex of T . So Cor. 25.66 implies that $\langle \gamma_{i-1}, \gamma_i, \gamma_{i+1} \rangle$ fixes some vertex of T .

Now let $a_1 = \gamma_1$, $a_2 = \gamma_3$, and $g = \gamma_5$. From the conclusion of the preceding paragraph, we know:

- $\langle a_1, a_2 \rangle$ fixes some vertex of T (by letting $i = 2$);
- $\langle g, a_1 \rangle$ fixes some vertex of T (by letting $i = 6$), so a_1g fixes some vertex of T ;
- $\langle a_2, g \rangle$ fixes some vertex of T (by letting $i = 4$), so a_2g fixes some vertex of T .

In addition, we know, from (25.69), that g fixes some vertex of T . Hence, Prop. 25.68 implies that $\langle a_1, a_2, g \rangle$ fixes some vertex v of T . But

$$\langle a_1, a_2, g \rangle = \langle \gamma_1, \gamma_3, \gamma_5 \rangle = \mathrm{SL}(3, \mathbb{Z})$$

(see Exer. 25:66), so this is what we wanted. $\square$

(25.70) **Remark.** The proof of Thm. 25.60 can easily be generalized to finite-index subgroups of $\mathrm{SL}(3, \mathbb{Z})$, if one replaces Exer. 25:66 with the fact that $\langle (\gamma_1)^k, (\gamma_3)^k, (\gamma_5)^k \rangle$ is a finite-index subgroup of $\mathrm{SL}(3, \mathbb{Z})$, for every nonzero $k \in \mathbb{Z}$ (see 23.12). More generally, a similar proof can be applied whenever $\mathbb{Q}$ -rank $\Gamma \geq 2$ (and Γ is irreducible).

The following generalization of Thm. 25.60 establishes Thm. 25.56 under the additional assumption that G has no simple factors that are isogenous to $\mathrm{SO}(1, n)$ or $\mathrm{SU}(1, n)$ (see 20.19(1)).

(25.71) **Theorem.** *If*

- Λ is Kazhdan group (see Defn. 20.12),
- T is a tree, and
- $\phi: \Lambda \rightarrow \mathrm{Aut}(T)$,

then $\phi(\Lambda)$ has a finite orbit on $V(T)$.

Proof. Let

$$\mathcal{H} = L^2(E(T))$$

be the Hilbert space with orthonormal basis $E(T)$. Fix some vertex $v_0 \in V(T)$, and define $f: V(T) \rightarrow \mathcal{H}$ by

$$f(v) = e_1 + e_2 + \cdots + e_n,$$

where $e_1, \dots, e_n$ are the edges of the unique path from v_0 to v . (By convention, $f(v_0) = 0$.) Then

- A) $\|f(v) - f(w)\|^2 = d(v, w)$ for all $v, w \in V$ (see Exer. 25:67), and
- B) for every automorphism σ of T , there is a (unique) corresponding affine isometry $\hat{\sigma}$ of $\mathcal{H}$, such that $\hat{\sigma}(f(v)) = f(\sigma(v))$, for every $v \in V(T)$ (see Exer. 25:68).

Because Λ is Kazhdan, we know that the orbit $\widehat{\phi(\Lambda)} f(v_0)$ is a bounded subset of $\mathcal{H}$ (see 20.22(2)), so (A) implies that $\phi(\Lambda)v_0$ is a bounded subset of $V(T)$. Then, under the harmless assumption that ϕ is without inversion (see Exer. 25:58), Lem. 25.63 implies that $\phi(\Lambda)$ fixes some vertex of T . $\square$

25H. Notes

The survey of É. Ghys [Gh3] is an excellent introduction to the study of group actions on the circle.

Versions of Conj. 25.3 were discussed in conversation as early as 1990, but the first published appearance may be in [Gh2, p. 200].

Theorem 25.4 was proved by É. Ghys [Gh2, Thm. 1.1]. (An exposition of the case $G = \mathrm{SL}(n, \mathbb{R})$ can be found in [Gh3, §7.3].) Ghys's original proof has a geometric flavor; it is based on viewing G/P as a space of flags. The slightly modified (more algebraic) version outlined in Rem. 25.36 is due to D. Witte and R.J. Zimmer [W-Z]. In particular, the existence of sufficiently many copies of $\mathrm{SL}^\pm(2, \mathbb{R})$ is [W-Z, Lem. 3.1].

The fact that $\mathcal{H}_b^2(\Gamma; \mathbb{R})$ injects into $\mathcal{H}^2(\Gamma; \mathbb{R})$ (see Rem. 25.37) was proved by M. Burger and N. Monod [B-M1, B-M2]. Exercise 25:47 is a result of É. Ghys [Gh1].

Proposition 25.5 was proved by W. Thurston [Thu] in a more general form that also applies to actions on manifolds of higher dimension. (It was inspired by the Reeb Stability Theorem [Ree].) Elegant proofs can be found in [R–S] and [Sch]. The proof outlined in Exer. 25:26 is due to R. J. Zimmer [W–Z, §5, pp. 108–109].

Theorem 25.7 (in the stronger form of Rem. 25.28) was proved by A. Navas [Nav]. The idea to use Lem. 25.29 (and Exer. 25:23) came from earlier work of A. Pressley and G. Segal [P–S] and A. Reznikov [Rez, Chap. 2].

Theorem 25.10 was proved by D. Witte [Wit]. Lemma 25.22 and Exer. 25:15 are special cases of a general result proved (independently) by J. C. Ault [Aul] and A. H. Rhemtulla [Rhe]: if Λ is any left-ordered, nilpotent group, then there is some $\lambda \in \Lambda$ with $[\Lambda, \Lambda] < \lambda$.

Lemma 25.15 is proved in [Gh3] and [Wit], but seems to have been known some decades earlier.

Conjecture 25.38 is attributed to W. Thurston (see [Bor, p. 88]). Theorem 25.40 combines work of J. Millson, J. S. Li, M. S. Raghunathan, and T. N. Venkataramana [Mil, Li, L–M, R–V]. (See [Rag2] for a survey.) Remark 25.41(1) is explained in [Gh3, §7.4]. Remark 25.41(2) is due to A. Lubotzky [Lub].

Remark 25.43 was proved by É. Ghys [Gh2, Thm. 1.2].

The first published appearance of Conj. 25.45 and its generalization may be in [FS1]. These were motivated by Conj. 25.47 and its generalization, which are due to R. J. Zimmer [Zim, Conj. 2, p. 1250]. (Zimmer has many results in this direction; some are discussed in [Zim].) Theorem 25.49 was proved by L. Polterovich [Pol] for surfaces of genus at least two. The remaining cases were settled by J. Franks and M. Handel [F–H] (the 2-sphere) and B. Farb and P. Shalen [FS3] (the 2-torus). Theorem 25.50 is due to B. Farb and P. Shalen [FS2], and they have results on real-analytic actions on manifolds of other dimensions [FS1].

J.–P. Serre’s wonderful book [Se2] is the standard introduction to the Bass-Serre theory of actions on trees. (It contains proofs of Rem. 25.59 [Se2, Thm. 15, p. 58] and Thm. 25.60 [Se2, Thm. 16, p. 67].) Theorem. 25.56 is due to G. A. Margulis [Mar4, Thm. 2]. Theorem 25.60 had been proved earlier by J.–P. Serre [Se1].

Theorem 25.71 is due to R. Alperin [Al1] and Y. Watatani [Wat], independently. Proofs can also be found in [H–V, Prop. 6.4, p. 71] and [Mar5, Thm. 3.3.9 and ¶3.3.10]. (Our proof, taken from [Mar5], is due to J.–P. Serre.) The theorem can be generalized to actions by isometries on $\mathbb{R}$ -trees, that is, on metric spaces in which each pair of distinct points is joined by a unique injective path (see, for example, [H–V, Prop. 6.11, p. 74]).

25I. References

- [Al1] R. C. Alperin: Locally compact groups acting on trees and property T , *Mh. Math.* 93 (1982) 261–265.
- [Aul] J. C. Ault: Right-ordered locally nilpotent groups, *J. London Math. Soc.* (2) 4 (1972) 662–666.
- [Bor] A. Borel: Cohomologie de sous-groupes discrets et représentations de groupes semi-simples, *Astérisque* 32–33 (1976) 73–112.
- [B–M1] M. Burger and N. Monod: Bounded cohomology of lattices in higher rank Lie groups, *J. Eur. Math. Soc.* 1 (1999) 199–235.
- [B–M2] M. Burger and N. Monod: Continuous bounded cohomology and applications to rigidity theory *Geom. Funct. Anal.* (to appear).

- [FS1] B. Farb and P. B. Shalen: Real-analytic actions of lattices, *Invent. Math.* 135 (1999) 273–296.
- [FS2] B. Farb and P. B. Shalen: Real-analytic, volume-preserving actions of lattices on 4-manifolds, *C. R. Acad. Sci. Paris* 334 (2002), no. 11, 1011–1014.
- [FS3] B. Farb and P. B. Shalen: Some remarks on symplectic actions of discrete groups (in preparation, 2002).
- [F–H] J. Franks and M. Handel: Area preserving group actions on S^2 (preprint, 2002). [arXiv:math.DS/0203159](#)
- [Gh1] É. Ghys: Groupes d’homéomorphismes du cercle et cohomologie bornée, in: *The Lefschetz Centennial Conference, Part III (Mexico City, 1984)*. *Contemp. Math.*, vol. 58, Part III. Amer. Math. Soc., Providence, 1987, pp. 81–106.
- [Gh2] É. Ghys: Actions de réseaux sur le cercle, *Invent. Math.* 137 (1999) 199–231.
- [Gh3] É. Ghys: Groups acting on the circle, *L’Enseign. Math.* 47 (2001) 329–407.
- [Gor] D. Gorenstein: *Finite Groups*. Chelsea (New York) 1980.
- [H–V] P. de la Harpe and A. Valette: *La propriété (T) de Kazhdan pour les groupes localement compacts*, *Astérisque* #175, Soc. Math. France, 1989. (A second edition, in English, is expected soon from the American Mathematical Society.)
- [Li] J. S. Li: Non-vanishing theorems for the cohomology of certain arithmetic quotients, *J. reine angew. Math.* 428 (1992) 177–217.
- [L–M] J. S. Li and J. Millson: On the first Betti number of a hyperbolic manifold with an arithmetic fundamental group, *Duke Math. J.* 71 (1993) 365–401.
- [Lub] A. Lubotzky: Free quotients and the first Betti number of some hyperbolic manifolds, *Transformation Groups* 1 (1996) 71–82.
- [Mar4] G. A. Margulis: On the decomposition of discrete subgroups into amalgams, *Selecta Math. Sovietica* 1 (1981) 197–213.
- [Mar5] G. A. Margulis: *Discrete Subgroups of Semisimple Lie Groups*. Springer, Berlin Heidelberg New York, 1991.
- [Mil] J. Millson: On the first Betti number of a constant negatively curved manifold, *Ann. Math.* 104 (1976) 235–247.
- [Nav] A. Navas: Actions de groupes de Kazhdan sur le cercle, (preprint, 2001).
- [Pol] L. Polterovich: Growth of maps, distortion in groups and symplectic geometry, *Invent. Math.* 150 (2002), no. 3, 655–686.
- [P–S] A. Pressley and G. Segal: *Loop Groups*. Oxford U. Press, Oxford, 1986.
- [Rag1] M. S. Raghunathan: *Discrete Subgroups of Lie Groups*. Springer, Berlin Heidelberg New York, 1972.
- [Rag2] M. S. Raghunathan: The first Betti number of compact locally symmetric spaces, in: S. D. Adhikari, ed., *Current Trends in Mathematics and Physics—A Tribute to Harish-Chandra*, Narosa Publishing House, New Delhi, 1995, pp. 116–137.
- [R–V] M. S. Raghunathan and T. N. Venkataramana: The first Betti number of arithmetic groups and the congruence subgroup problem, *Contemp. Math.* 153 (1993) 95–107.
- [Ree] G. Reeb: Sur certaines propriétés topologiques des variétés feuilletées (French), *Publ. Inst. Math. Univ. Strasbourg* 11, pp. 5–89, 155–156. *Actualités Sci. Ind.* #1183. Hermann, Paris, 1952. MR 14,1113a

- [R–S] G. Reeb and P. Schweitzer: Un théorème de Thurston établi au moyen de l'analyse non standard, in: P. A. Schweitzer, ed., *Differential Topology, Foliations and Gelfand-Fuks Cohomology* (Proc. Sympos., Pontificia Univ. Católica, Rio de Janeiro, January 1976), Lecture Notes in Math., vol. 652, Springer, New York, 1978, p. 138.
- [Rez] A. Reznikov: Analytic topology of groups, actions, strings, and varieties, (preprint).
- [Rhe] A. H. Rhemtulla: Right-ordered groups. *Canad. J. Math.* 24 (1972) 891–895.
- [Sch] W. Schachermayer: Une modification standard de la démonstration non standard de Reeb et Schweitzer, in: P. A. Schweitzer, ed., *Differential Topology, Foliations and Gelfand-Fuks Cohomology* (Proc. Sympos., Pontificia Univ. Católica, Rio de Janeiro, January 1976), Lecture Notes in Math., vol. 652, Springer, New York, 1978, pp. 139–140.
- [Se1] J.–P. Serre: Amalgames et points fixes, in: *Proceedings of the Second International Conference on the Theory of Groups (Australian Nat. Univ., Canberra, 1973)*. *Lecture Notes in Math.* #372. Springer, Berlin, 1974, pp. 633–640. MR 51 #13057
- [Se2] J.–P. Serre: *Trees*, Springer, New York, 1980.
- [Thu] W. Thurston: A generalization of the Reeb stability theorem, *Topology* 13 (1974) 347–352.
- [Wat] Y. Watatani, Property (T) of Kazhdan implies property (FA) of Serre, *Math. Japon.* 27 (1981) 97–103.
- [Wit] D. Witte: Arithmetic groups of higher $\mathbb{Q}$ -rank cannot act on 1-manifolds, *Proc. Amer. Math. Soc.* 122 (1994) 333–340.
- [W–Z] D. Witte and R. J. Zimmer: Actions of semisimple Lie groups on circle bundles, *Geometriae Dedicata* 87 (2001) 91–121.
- [Zim] R. J. Zimmer: Actions of semisimple groups and discrete subgroups, in: A. M. Gleason, ed., *Proc. Internat. Congress Math. (Berkeley, California, August 3–11, 1986)*, Vol. 2. Amer. Math. Soc., Providence, 1987.

Exercises

- 25:1) Prove that Conjectures (25.3) and (25.3') are equivalent.
- 25:2) Show that Γ is left orderable if and only if Γ is right orderable. [Hint: Define $x \prec y$ if $x^{-1} < y^{-1}$. Alternatively, the conclusion can be derived from Rem. 25.13 and its analogue for right orderable groups.]
- 25:3) Show that if
 - $<$ is a left-invariant total order on Γ , and
 - $\gamma_1, \dots, \gamma_n > e$, where e is the identity element of Γ ,
 then
 - (a) $\gamma_1 \gamma_2 \cdots \gamma_n > e$, and
 - (b) $\gamma_1^{-1} \gamma_2^{-1} \cdots \gamma_n^{-1} < e$.
- 25:4) Establish the assertion of Rem. 25.13. [Hint: Given P , define $\gamma < \lambda$ if $\gamma^{-1} \lambda \in P$. Given $<$, define $P = \{\gamma \in \Gamma \mid \gamma < e\}$.]
- 25:5) Show that every subgroup of a left-orderable group is left orderable.
- 25:6) Complete the proof of Lem. 25.15($\Leftarrow$), by defining a left-invariant total order on Γ . [Hint: Make a list $q_1, q_2, \dots$ of the rational numbers, and define $\gamma < \lambda$ if $\gamma(q_n) < \lambda(q_n)$, where n is minimal with $\gamma(q_n) \neq \lambda(q_n)$.]
- 25:7) Prove Lem. 25.15($\Rightarrow$). [Hint: If the order relation $(\Gamma, <)$ is dense (that is, if $\gamma < \lambda \Rightarrow \exists \mu \in \Gamma, \gamma < \mu < \lambda$), then it is order-isomorphic to $\mathbb{Q}$. The action of Γ on $(\Gamma, <)$ by left

multiplication extends to a continuous action of Γ on the Dedekind completion, which is homeomorphic to $\mathbb{R}$.]

- 25:8) Show that if Γ is left orderable, then Γ is torsion free. [*Hint*: This follows easily from Rem. 25.13.]
- 25:9) Show that there is no loss of generality in assuming that $\gamma, \lambda, \zeta^k > e$ in the proof of Lem. 25.22. [*Hint*: Consider replacing any or all of these elements by their inverse, and/or interchanging γ with λ .]
- 25:10) Remove the assumption that $k = 1$ from the proof of Lem. 25.22. [*Hint*: Insert appropriate factors of k in the calculations.]
- 25:11) In the notation of the proof of Thm. 25.18, show, for each i , that
- (a) $[\gamma_i, \gamma_{i+1}] = e$, and
 - (b) $[\gamma_{i-1}, \gamma_{i+1}] = \gamma_i^{\pm k}$.
- 25:12) A *central extension* of Γ is a group Λ , such that $\Lambda/Z \cong \Gamma$, for some subgroup Z of the center of Λ .

Show that if there is a faithful homomorphism $\phi: \Gamma \rightarrow \text{Homeo}_+(\mathbb{R})$, then some central extension of Γ is left orderable. [*Hint*: Because $\mathbb{R}$ is the universal cover of S^1 , every homeomorphism of S^1 lifts to a homeomorphism of $\mathbb{R}$, and the lift is unique modulo an element of the fundamental group $\mathbb{Z}$. Let Λ be the subgroup of $\text{Homeo}_+(\mathbb{R})$ consisting of all of the possible lifts of all of the elements of Γ , and show that Λ is a central extension that is left orderable.]

- 25:13) [Gor, Lems 2.2.2(i) and 2.2.4(iii), pp. 19 and 20] Prove Lem. 25.21.
- 25:14) Complete the proof of Lem. 25.22, by removing the assumptions that $k = 1$, and that $\gamma, \lambda, \zeta > e$. [*Hint*: Show that these assumptions can be fulfilled by replacing ζ with ζ^k , by replacing some of γ, λ, ζ by their inverses if necessary, and perhaps interchanging γ and λ .]
- 25:15) Suppose
- $\Lambda = \langle \lambda, \gamma_1, \gamma_2, \gamma_3 \rangle$ is a group,
 - $<$ is a left-invariant total order on Λ ,
 - $\langle \gamma_1, \gamma_2, \gamma_3 \rangle \cong \mathbb{Z}^3$ is abelian,
 - $[\lambda, \gamma_1] = \gamma_2$, $[\lambda, \gamma_2] = \gamma_3$, and $[\lambda, \gamma_3] = e$.
- Show there is some $h \in \Lambda$, such that $\langle \gamma_1, \gamma_2 \rangle < h$. [*Hint*: Choose $g \in H$, such that $\langle \gamma_3 \rangle < g$ (see 25.22). Show $[\lambda^n, \gamma_1^m] \in \gamma_2^{-mn} \langle \gamma_3 \rangle$, and follow the proof of Lem. 25.22, with an extra factor of g to compensate for powers of γ_3 .]

- 25:16) Suppose
- Λ is a group,
 - $<$ is a left-invariant total order on a group Λ ,
 - S is a generating set for Λ , and
 - there exists $h \in \Lambda$, such that $[\Lambda, \Lambda] < h$.

Show there is some $s \in S$, such that $[\Lambda, \Lambda] < s$.

- 25:17) Establish (25.25).

- 25:18) Show $\int_{-\pi/2}^{\pi/2} \int_{-\pi/2}^{\pi/2} 1/(r-s)^2 dr ds = \infty$.

- 25:19) Suppose
- $\phi: \Gamma \rightarrow \text{Diff}^1(S^1)$, and
 - $F_0 \in (S^1 \times S^1)$,

such that

$$F_0(g(r), g(s)) |g'(r)| |g'(s)| = F_0(r, s),$$

for all $r, s \in S^1$ and $g \in \Gamma$. Show

$$\int_{S^1} \int_{S^1} \Psi(g(r), g(s)) F_0(r, s) dr ds = \int_{S^1} \int_{S^1} \Psi(r, s) F_0(r, s) dr ds,$$

for all $\Psi \in (S^1 \times S^1)$ and $g \in \Gamma$.

25:20) Show that if $a < b < c$, then $\int_b^c \int_a^b 1/(r-s)^2 dr ds = \infty$.

25:21) Show that if $-\pi/2 \leq a < d < b < c \leq \pi/2$, and F is any C^∞ function on

$$\{(r, s) \in S^1 \times S^1 \mid r \neq s\},$$

then $\int_b^c \int_a^d F dr ds < \infty$. [*Hint*: A continuous function is bounded on compact sets.]

25:22) Show that if Λ is a nonabelian subgroup of $\text{Homeo}_+(S^1)$, then some nonidentity element of Λ has a fixed point. [*Hint*: Proof by contradiction. By passing to the universal cover, replace S^1 with $\mathbb{R}$. Fix $\gamma \in \Lambda \setminus \{e\}$, such that $\gamma(0) > 0$. For each $\lambda \in \Lambda$, and $n \in \mathbb{Z}$, define

$$f_0(\lambda, n) = \min\{m \in \mathbb{Z} \mid \gamma^m(0) > \lambda^n(0)\},$$

and let $f(\lambda) = \lim_{n \rightarrow \infty} f_0(n)/n$. Show that f is an injective homomorphism from Λ to $\mathbb{R}$.]

25:23) Recall that a real-valued function f on a subset I of $\mathbb{R}$ is δ -Hölder if there exists $k \in \mathbb{R}^+$, such that $f(r) - f(s) \leq k(r-s)^\delta$, for all $r, s \in I$. Show that if $g \in \text{Diff}^1(S^1)$, and the derivative g' is δ -Hölder, for some $\delta > 1/2$, then, in the notation of the proof of Thm. 25.7, $\Phi^g - \Phi \in L^2(S^1 \times S^1)$.

25:24) Prove Thm. 25.5, without assuming that the elements of Λ are real analytic. [*Hint*: Let S be a finite set that generates Λ , let $\lambda_0 \in S$, and suppose there is a sequence $x_n \rightarrow 0$ in I , such that $\lambda_0(x_n) \neq x_n$, for every n . For $\lambda \in \Lambda$, define

$$\tau_n(\lambda) = \frac{\lambda(x_n) - x_n}{\lambda_0(x_n) - x_n}.$$

By passing to a subsequence, and perhaps replacing λ_0 with some other element of S , assume, for all $\lambda \in \Lambda$, that $\tau(\lambda) = \lim_{n \rightarrow \infty} \tau_n(\lambda)$ exists (and is finite). Show that $\tau: \Lambda \rightarrow \mathbb{R}$ is a homomorphism, which contradicts the fact that $\tau(\lambda_0) = 1$.]

25:25) Complete the proof of Prop. 25.5', under the assumption that each element of Λ is real analytic, by showing that $a_n^\lambda = 0$ for each $n \geq 2$.

25:26) Fill in the details of the following outline of a proof of Prop. 25.5', under the additional assumption that Λ has Kazhdan's Property T .

- (a) It suffices to show that the fixed points of Γ form a dense subset of I ; thus, we may assume that 0 and 1 are the only points that are fixed by Γ .
- (b) We have $\gamma'(0) = 1$ for all $\gamma \in \Gamma$.
- (c) Define a unitary representation of Γ on $L^2(I)$ by

$$f^\gamma(t) = f(\gamma t) |\gamma'(t)|^{1/2}.$$

- (d) For any $\gamma \in \Gamma$ and any $\delta > 0$, if f is the characteristic function of a sufficiently small neighborhood of 0, then $\|f^\gamma - f\| < \delta \|f\|$.
- (e) There is $f \in L^2(I) \setminus \{0\}$, such that $f^\gamma = f$ for all $\gamma \in \Gamma$.
- (f) Every point in the essential support of f is a fixed point of Γ .
- (g) This is a contradiction.

25:27) Show that if

- ψ is a measure-preserving automorphism of a measure space (Ω, μ) , and
- $\omega \in \Omega$,

then

$$\{x \in \Omega \mid \mu(x) = \mu(\omega)\}$$

is ψ -invariant.

25:28) In the notation of the proof of Thm. 25.4, show that if $\psi: G/P \rightarrow \text{Prob}(S^1)$ is a Γ -equivariant, Borel measurable map, then there is a Γ -equivariant, Borel measurable map $\psi_0: G/P \rightarrow \text{Prob}(S^1)$, such that either

- for a.e. $x \in G/P$, the measure $\psi_0(x)$ has no atoms, or
- for a.e. $x \in G/P$, the measure $\psi_0(x)$ consists entirely of atoms.

[Hint: For each $x \in G/P$, write $\psi(x) = \psi_{\text{noatom}}(x) + \psi_{\text{atom}}(x)$, where $\psi_{\text{noatom}}(x)$ has no atoms, and $\psi_{\text{atom}}(x)$ consists entirely of atoms. Use the ergodicity of Γ on G/P to show that either ψ_{noatom} or ψ_{atom} can be normalized to define a function into $\text{Prob}(S^1)$.]

25:29) Prove (25.33).

25:30) Define $d: (\text{Prob}(S^1))^2 \rightarrow \mathbb{R}$ by

$$d(\mu_1, \mu_2) = \sup_J |\mu_1(J) - \mu_2(J)|,$$

where J ranges over all intervals (that is, over all connected subsets of S^1). Show that d is *not* continuous, with respect to the usual weak* topology on $\text{Prob}(S^1)$.

25:31) In the notation of Case 1 of the proof of Thm. 25.4, show that d is Γ -invariant. That is, $d(\gamma x, \gamma y) = d(x, y)$, for all $\gamma \in \Gamma$ and $x, y \in S^1$.

25:32) In the notation of Case 1 of the proof of Thm. 25.4, show that $c = 0$. [Hint: There is a subset U of G/P , such that $\mu(U) \neq 0$, and ψ is continuous on G/P (Lusin's Theorem).]

25:33) Complete Case 2 of the proof of Lem. 25.30, by eliminating the assumption that the support of μ is all of S^1 . [Hint: Show that every point in the support of μ is a fixed point.]

25:34) Show that the function d defined in (25.32) is a metric on S^1 (under the assumption that the support of μ is all of S^1). That is, show $d(x, x) = 0$, $d(x, y) = d(y, x)$, and $d(x, y) \leq d(x, z) + d(z, y)$.

25:35) Show, for the metric d defined in (25.32), that $d(\gamma x, \gamma y) = d(x, y)$, for all $\gamma \in \Gamma$ and $x, y \in S^1$.

25:36) Show that, up to isometry, and a normalizing scalar multiple, there is a unique metric on S^1 . [Hint: Given metrics d_1 and d_2 on the unit interval I , such that $d_1(0, 1) = d_2(0, 1)$, define $f: I \rightarrow I$ by $d_1(0, t) = d_2(0, f(t))$, and show that f is an isometry from (I, d_1) to (I, d_2) .]

25:37) Show that if ψ is an orientation-preserving isometry of $S^1 = \mathbb{R}/\mathbb{Z}$, then there is some $k \in \mathbb{R}$, such that $\psi(x + \mathbb{Z}) = x + k + \mathbb{Z}$, for every $x \in \mathbb{R}$.

25:38) For any natural number k , let S_k^1 be the collection of all k -element subsets of S^1 . There is a natural surjection from $(S^1)^k$ onto S_k^1 , and we define a subset of S_k^1 to be Borel measurable if and only if its inverse image is a Borel subset of $(S^1)^k$.

- (a) Show that $\text{Homeo}_+(S^1)$ acts transitively on S_k^1 and $(S_k^1)^2$.
- (b) Show that $\text{Homeo}_+(S^1)$ has only finitely many orbits on $(S_k^1)^3$, and that each of these orbits is a Borel subset of $(S_k^1)^3$.
- (c) Show that if $(A_1, A_2, A_3) \in (S_k^1)^3$, such that (A_2, A_1, A_3) is in the $\text{Homeo}_+(S^1)$ -orbit of (A_1, A_2, A_3) , then $A_1 = A_2$.

25:39) Assume, in the notation of the proof of Thm. 25.4, that $\psi(x)$ consists entirely of atoms, for a.e. $x \in G/P$.

- (a) Show, for some natural number k , that there is a Γ -equivariant, Borel measurable map $\psi_0: G/P \rightarrow S_k^1$, where S_k^1 denotes the collection of all k -element subsets of S^1 .
- (b) Define $\psi_0^3: (G/P)^3 \rightarrow (S_k^1)^3$ in the obvious way. The argument given in Case 2 of the proof of Thm. 25.4 (using the ergodicity of Γ on X) shows that $\psi_0^3((G/P)^3)$ is essentially contained in a single $\text{Homeo}_+(S^1)$ -orbit on $(S_k^1)^3$. Assuming this, show that ψ_0 is essentially constant.
- (c) Show that if ψ_0 is constant, then Γ has a finite orbit on S^1 .
- [Hint: (25:39a) For some $t > 0$, let $\psi_0(x) = \{p \in S^1 \mid \mu(p) = t\}$. (25:39b) Use Exer. 25:38.]

25:40) Show that the action of $\text{GL}(2, \mathbb{R})$ on $\mathbb{R} \cup \{\infty\}$ by linear-fractional transformations is triply transitive.

25:41) Let

$$Q = \begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{bmatrix} \subset \text{SL}(3, \mathbb{R}), \quad \text{and} \quad Q' = \begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix} \subset \text{SL}(3, \mathbb{R}).$$

Show that $\langle Q, Q' \rangle = \text{SL}(3, \mathbb{R})$.

25:42) Show that if P is a closed subgroup of G , and ψ is a measurable function on G/P , then

$$(25.72) \quad \{g \in G \mid \psi(xgP) = \psi(xP) \text{ for a.e. } x \in G\}$$

is a subgroup of G .

25:43) Show that the subgroup (25.72) is closed.

25:44) Show that if the subgroup (25.72) is all of G , then ψ is essentially constant. Also prove the converse.

25:45) Establish (25.34).

25:46) In the notation of Rem. 25.36, show that

- (a) G is transitive on X , and
 (b) there is some point in X whose stabilizer is not compact.

25:47) Suppose $\phi: \Gamma \rightarrow \text{Homeo}_+(S^1)$, and that $\phi(\Gamma)$ has no fixed point. Construct a bounded function

$$\alpha: \Gamma \times \Gamma \rightarrow \mathbb{Z},$$

such that

- (a) $\alpha(g_1, g_2) - \alpha(g_1, g_2 g_3) + \alpha(g_1 g_2, g_3) - \alpha(g_2, g_3) = 0$ for all $g_1, g_2, g_3 \in \Gamma$, and
 (b) there does not exist a bounded function $\beta: \Gamma \rightarrow \mathbb{Z}$, such that $\alpha(g, h) = \beta(g) + \beta(h) - \beta(gh)$.

[Hint: Define

$$\alpha(g_1, g_2) = \begin{cases} 0 & \text{if } \tilde{g}_1 \tilde{g}_2(0) < 1 \\ 1 & \text{if } \tilde{g}_1 \tilde{g}_2(0) \geq 1, \end{cases}$$

where $\tilde{g}$ is the lift of g to a homeomorphism of $\mathbb{R}$, with $\tilde{g}(0) \in [0, 1)$.]

25:48) Complete the proof of Prop. 25.42, by showing that ϕ satisfies 25.42(1) and 25.42(2).

25:49) Show that if there are faithful homomorphisms $\phi_1: \Gamma_1 \rightarrow \text{Homeo}(S^1)$ and $\phi_2: \Gamma_2 \rightarrow \text{Homeo}(S^1)$, such that $\phi_1(\Gamma_1)$ and $\phi_2(\Gamma_2)$ each have a fixed point, then there is a faithful homomorphism $\phi: \Gamma_1 \times \Gamma_2 \rightarrow \text{Homeo}(S^1)$.

25:50) Show that there is a homomorphism $\phi: \Gamma_1 \times \Gamma_2 \rightarrow \text{Homeo}(S^1)$, such that $\phi(\Gamma_1 \times \Gamma_2)$ is infinite, if and only if either

- there is a homomorphism $\phi_1: \Gamma_1 \rightarrow \text{Homeo}(S^1)$, such that $\phi_1(\Gamma_1)$ is infinite, or

- there is a homomorphism $\phi_2: \Gamma_2 \rightarrow \text{Homeo}(S^1)$, such that $\phi_2(\Gamma_2)$ is infinite.

25:51) Suppose

- V is a nontrivial, real G -module,
- $M = \mathbb{P}V$ is the projective space on V , and
- G is connected, with no compact factors.

Show that there is a homomorphism $\phi: \Gamma \rightarrow \text{Diff}^\infty(M)$, such that $\phi(\Gamma)$ is infinite.

25:52) Suppose

- Γ is a lattice in $\text{SO}(p, q)$,
- there is a homomorphism $\rho: \Gamma \rightarrow \text{SO}(p+q)$, such that $\rho(\Gamma)$ is dense in $\text{SO}(p+q)$, and
- M is the $(p+q)$ -dimensional sphere S^{p+q}

(see Exer. 6:34). Show that there is a homomorphism $\phi: \Gamma \rightarrow \text{Diff}^\infty(M)$, such that $\phi(\Gamma)$ is infinite.

25:53) Suppose S is a symmetric subset of a group Λ , such that $e \notin S$. (By *symmetric*, we mean that $S = S^{-1}$, where $S^{-1} = \{s^{-1} \mid s \in S\}$.) Define the *Cayley graph* of the generators S on the group Λ to be the graph $\text{Cay}(S; \Lambda) = (V, E)$, where

- $V = \Lambda$, and
- $E = \{ \{x, xs\} \mid x \in \Lambda, s \in S \}$.

Show:

- $\text{Cay}(S; \Lambda)$ is a graph.
- For each $g \in \Lambda$, the permutation $x \mapsto gx$ is an automorphism of Λ .
- There is a homomorphism $\phi: \Lambda \rightarrow \text{Aut}(\text{Cay}(S; \Lambda))$, such that
 - $\phi(\Lambda)$ is transitive on V , and
 - no nontrivial element of $\phi(\Lambda)$ has a fixed point on V .
- $\text{Cay}(S; \Lambda)$ is connected if and only if S generates Λ .
- $\text{Cay}(S; \Lambda)$ has finite valence if and only if S is finite.

25:54) Show that if u and v are vertices of a graph X , and there is a walk from u to v , then there is a path from u to v . More precisely, any walk from u to v of minimal length is a path.

25:55) A *cycle* in a graph X is a walk $v_0, v_1, \dots, v_n$, such that

- $v_0 = v_n$,
- $v_0, \dots, v_{n-1}$ are distinct, and
- $n \geq 3$.

Show that a connected graph X is a tree if and only if X has no cycles.

25:56) For any group Λ , construct a tree T , and a faithful homomorphism $\phi: \Lambda \rightarrow \text{Aut}(T)$. [*Hint:* Let $V = A \cup \{x_0\}$ and $E = \{ \{a, x_0\} \mid a \in A \}$, for some set A on which Λ acts faithfully.]

25:57) Construct a tree T , such that each vertex of T has finite valence, and a faithful homomorphism $\phi: \Gamma \rightarrow \text{Aut}(T)$. [*Hint:* Define V to be the disjoint union of all Γ/N_k , and let

$$E = \left\{ \{ \gamma N_k, \gamma N_{k+1} \} \mid \begin{array}{l} \gamma \in \Gamma, \\ k = 0, 1, \dots \end{array} \right\},$$

for some chain $\Gamma = N_0 \supset N_1 \supset \dots$ of finite-index, normal subgroups of Γ , such that $\cap_k N_k = \{e\}$ (see Exer. 5:46).]

25:58) Suppose T is a tree, and $\phi: \Gamma \rightarrow \text{Aut}(T)$, such that $\phi(\Gamma)$ has no finite orbit on $V(T)$. Show that there is a tree T' , and a homomorphism $\phi': \Gamma \rightarrow \text{Aut}(T')$, such that $\phi'(\Gamma)$ has no finite orbit on $V(T')$. [*Hint:* Let $V' = V \cup E$ and $E' = \{ \{v, e\} \mid v \in e \}$.]

25:59) Suppose B is a nonempty, bounded set of vertices of a tree T , and let

$$\text{diam}(B) = \max_{x,y \in B} d(x,y).$$

(a) If $\text{diam}(B)$ is even, show that there is a unique vertex $v \in V(T)$, such that $d(v,b) \leq \text{diam}(B)/2$, for all $b \in B$.

(b) If $\text{diam}(B)$ is odd, show that there is a unique edge $\{v_1, v_2\}$ of T , such that $d(v_k, b) \leq \lceil \text{diam}(B)/2 \rceil$, for $k = 1, 2$ and all $b \in B$.

[Hint: (25:59a) If $x, y \in B$ with $d(x, y) = \text{diam}(B)$, then there is a unique vertex v of T , such that $d(v, x) = d(v, y) = \text{diam}(B)/2$. Show that v is independent of the choice of x and y .]

25:60) Show, for any bounded set B of vertices of any tree T , that there is a finite set F of vertices of T , such that

(a) $\sigma(F) = F$, for every $\sigma \in \text{Aut}(T)$, such that $\sigma(B) = B$, and

(b) F is either a single vertex or a single edge of T (so $\#F \in \{1, 2\}$).

[Hint: Use Exer. 25:59.]

25:61) Show that if T_1 and T_2 are disjoint subtrees of T , then there is a unique path of minimal length from T_1 to T_2 . [Hint: If $[x_1, y_1]$ and $[x_2, y_2]$ are two paths of minimal length, and $x_1 \neq x_2$, then there is a cycle in T .]

25:62) Prove Lem. 25.64. [Hint: For existence and (2), choose $v \in V(T)$ to minimize $d(v, \sigma(v))$. Let P be the path from v to $\sigma(v)$, and show that $\cup_{k \in \mathbb{Z}} \sigma^k(P)$ is an axis of σ . For uniqueness, use Exer. 25:61.]

25:63) Show that if

- γ is an automorphism of a bi-infinite path $\dots, v_{-1}, v_0, v_1, v_2, \dots$, and
- γ commutes with the automorphism $v_k \mapsto v_{k+p}$, for some nonzero $p \in \mathbb{Z}$,

then there is some $m \in \mathbb{Z}$, such that $\gamma(v_k) = v_{k+m}$ for all k .

25:64) Suppose

- $\phi: \Lambda \rightarrow \text{Aut}(T)$, for some tree T ,
- T' is the set of all vertices that are fixed by $\phi(\Lambda)$, and
- $T' \neq \emptyset$.

Show that T' is a subtree of T .

25:65) In the notation of the proof of Lem. 25.67, show that each vertex of $[v, w] \cap \sigma([v, w])$ is fixed by σ . [Hint: If $x, y \in [v, w]$, and $d(x, w) = d(y, w)$, then $x = y$.]

25:66) In the notation of the proof of Thm. 25.60, show that $\langle \gamma_1, \gamma_3, \gamma_5 \rangle = \text{SL}(3, \mathbb{Z})$.

25:67) Prove assertion (A) of the proof of Thm. 25.71.

25:68) Prove assertion (B) of the proof of Thm. 25.71.

Assumed Background

This appendix is very preliminary!!! There are no explanations yet, and more topics will be added.

I.A. Riemannian manifolds

(I.1) **Definition.** Let M be a topological space. An (n -dimensional) *coordinate system* on an open set U of M is a diffeomorphism ϕ from U onto an open subset of $\mathbb{R}^n$. An (n -dimensional) *atlas* on M is a collection $\{(\phi_\alpha, U_\alpha)\}_{\alpha \in A}$ of n -dimensional coordinate systems on M , for some n , such that

- the coordinate patches cover M , that is, $\bigcup_{\alpha \in A} U_\alpha = M$; and
- the overlap maps are diffeomorphisms; that is, for all $\alpha, \beta \in A$, the composition $\phi_\alpha \circ \phi_\beta^{-1}$ is a diffeomorphism from $\phi_\beta(U_\alpha \cap U_\beta)$ onto $\phi_\alpha(U_\alpha \cap U_\beta)$.

A (smooth) *manifold* is a Hausdorff topological space M , together with an atlas.

(I.2) **Definition.**

- An *inner product* on a real vector space V is a symmetric, positive-definite, bilinear form $\langle \cdot | \cdot \rangle$ on V .
- A *Riemannian manifold* is a smooth manifold M , together with the choice of an inner product $\langle \cdot | \cdot \rangle_x$ on the tangent space $T_x M$, for each $x \in M$, such that $\langle \cdot | \cdot \rangle_x$ varies smoothly as x varies.
- The *norm* $\|v\|_x$ of a vector $v \in T_x M$ is $\sqrt{\langle v | v \rangle_x}$.

(I.3) **Definition.** If M_1 and M_2 are Riemannian manifolds, then the *cartesian product* $M_1 \times M_2$ is also a Riemannian manifold, with inner product given by

$$\langle (u_1, u_2) | (v_1, v_2) \rangle_{(p_1, p_2)} = \langle u_1 | v_1 \rangle_{p_1} + \langle u_2 | v_2 \rangle_{p_2}$$

for $p_i \in M_i$ and $u_i, v_i \in T_{p_i} M_i$.

I.B. Geodesics

(I.4) **Definition.**

- For any smooth curve $c: [a, b] \rightarrow M$ in a Riemannian manifold M , we define the *length* of c to be

$$\int_a^b \|c'(t)\|_{c(t)} dt.$$

- Then a topological metric d is defined on M by

$$d(x, y) = \inf\{\text{length}(c) \mid c \text{ is a smooth curve from } x \text{ to } y\}.$$

- A smooth curve $\gamma: [a, b] \rightarrow M$ is a *length-minimizing geodesic* if $\|\gamma'(t)\|_{\gamma(t)}$ is constant (independent of t) and $\text{length}(\gamma) = d(\gamma(a), \gamma(b))$.
- A smooth curve $\gamma: I \rightarrow M$ is a *geodesic* if I can be written as a (locally finite) union of closed intervals I_m , such that the restriction $\gamma|_{I_m}$ is a length-minimizing geodesic, for each m .
- A diffeomorphism $f: M_1 \rightarrow M_2$ between two Riemannian manifolds is an *Riemannian isometry* if $|Df(p)v|_{f(v)} = |v|_p$, for every $(p, v) \in TM_1$. (Note that f must also be an isometry with respect to the associated topological metrics on M_1 and M_2 .)

(I.5) **Warning.** If C is a submanifold of a Riemannian manifold M , then C is a Riemannian manifold, so there is an associated topological metric d_C on C . There is also a metric $d|_C$, obtained by restricting the topological metric on M . These two metrics can be very different, because two points of C that are near to each other in M may not be joined by a short curve that lies entirely in C .

(I.6) **Proposition** (Existence and Uniqueness of Geodesics). *Let M be a Riemannian manifold. For any $(p, v) \in TM$, there is a geodesic $\gamma: (-\epsilon, \epsilon) \rightarrow M$, for some $\epsilon > 0$, such that $\gamma(0) = p$ and $\gamma'(0) = v$.*

Furthermore, if $\bar{\gamma}: I \rightarrow M$, is any geodesic, such that $\bar{\gamma}(0) = p$ and $\bar{\gamma}'(0) = v$, then $\bar{\gamma}(t) = \gamma(t)$ for all $t \in I \cap (-\epsilon, \epsilon)$.

(I.7) **Definition.** A neighborhood V of 0 in a real vector space is:

- *star-shaped* if $tV \subset V$ for all $t \in [0, 1]$;
- *symmetric* if $-V = V$.

(I.8) **Corollary.** *For each $p \in M$, there is a star-shaped, symmetric neighborhood V of 0 in $T_p(M)$, such that we may define a smooth map $\exp_p: V \rightarrow M$ by letting $\exp_p(v) = \gamma(1)$, where γ is a geodesic such that $\gamma(0) = p$ and $\gamma'(0) = v$. Furthermore, if V is sufficiently small, then $\exp_p$ is a diffeomorphism onto its image.*

(I.9) **Definition.** Note that, by identifying $T_p M$ with $\mathbb{R}^n$, the inverse of $\exp_p$ defines a coordinate system on a neighborhood of p . These are called *exponential coordinates* at p .

There are two different definitions of completeness for a Riemannian manifold. Fortunately, they are equivalent.

(I.10) **Definition.** Let M be a Riemannian manifold.

- M is *geodesically complete* if, for every geodesic segment $\gamma: (-\epsilon, \epsilon) \rightarrow M$, there is a geodesic $\bar{\gamma}: \mathbb{R} \rightarrow M$, such that $\bar{\gamma}(t) = \gamma(t)$, for all $t \in (-\epsilon, \epsilon)$.
- M is *complete* if all Cauchy sequences converge.

(I.11) **Proposition.** *A Riemannian manifold is geodesically complete if and only if it is complete.*

I.C. Lie groups

(I.12) **Definition.** A *Lie group* G is a smooth manifold, equipped with a group structure, such that the group operations are smooth. That is, the maps $G \times G \rightarrow G: (g, h) \mapsto gh$ and $G \rightarrow G: g \mapsto g^{-1}$ are smooth.

(I.13) **Proposition.** If H is a closed subgroup of a Lie group G , then H is a smooth submanifold of G , so H is itself a Lie group. Also, the quotient space G/H is a smooth manifold.

(I.14) **Definition.** Let G be a topological group, and X be a topological space.

- An *action* of G on X is a homomorphism $\phi: G \rightarrow \text{Perm}(X)$, where $\text{Perm}(X)$ is the group of all permutations of X . Equivalently, an *action* is a function $\alpha: G \times X \rightarrow X$, such that
 - $\alpha(1, x) = x$ for all $x \in X$, and
 - $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ for $g, h \in G$ and $x \in X$.

The equivalence is obtained by taking $\alpha(g, x) = (\phi(g))(x)$.

- An action is *continuous* if the map α is continuous.
- An action is *proper* if the map α is proper; that is, if the inverse image of every compact set is compact.

(I.15) **Definition.** Let a group Γ act continuously on a topological space M .

- The action is *free* if no nonidentity element of Γ has a fixed point.
- The action is *properly discontinuous* if, for every compact subset C of M , the set

$$\{\gamma \in \Gamma \mid C \cap (\gamma C) \neq \emptyset\}$$

is finite.

- For any $p \in M$, we define $\text{Stab}_\Gamma(p) = \{\gamma \in \Gamma \mid \gamma p = p\}$. This is a closed subgroup of Γ .

(I.16) **Proposition.** If Γ acts freely and properly discontinuously on a topological space M , then the natural map $M \rightarrow \Gamma \backslash M$ is a covering map.

(I.17) **Proposition.** If M is any locally compact metric space, then $\text{Isom}(M)$ is a locally compact topological group, under the compact-open topology (that is, under the topology of uniform convergence on compact sets). The action of $\text{Isom}(M)$ on M is proper; that is, for every compact subset C of M , the set

$$\{\phi \in \text{Isom}(M) \mid \phi(C) \cap C \neq \emptyset\}$$

is compact.

If M is a smooth manifold, then the topological group $\text{Isom}(M)$ can be given the structure of a Lie group, so that the action of $\text{Isom}(M)$ on M is smooth.

(I.18) **Notation.** For any topological group G , we use G° to denote the identity component of G .

(I.19) **Proposition** (Existence and Uniqueness of Haar Measure). If G is any locally compact topological group, then there is a unique (up to a scalar multiple) σ -finite Borel measure μ on G , such that

- 1) $\mu(C)$ is finite, for every compact subset C of G , and
- 2) $\mu(gA) = \mu(A)$, for every Borel subset A of G , and every $g \in G$.

(I.20) **Definition.**

- The measure μ of Prop. I.19 is called the *left Haar measure* on G . Analogously, there is a unique *right Haar measure* with $\mu(Ag) = \mu(A)$.

- G is *unimodular* if there is a σ -finite Borel measure μ on G , such that

- 1) $\mu(C)$ is finite, for every compact subset C of G , and
- 2) $\mu(gA) = \mu(Ag) = \mu(A)$, for every Borel subset A of G , and every $g \in G$.

In other words, a group is unimodular if its two Haar measures (left and right) are the same.

(I.21) **Proposition.** *There is a continuous homomorphism $\Delta: G \rightarrow \mathbb{R}^+$, such that $\mu(gAg^{-1}) = \Delta(g)\mu(A)$, for any (left or right) Haar measure μ on G , and any Borel set $A \subset G$.*

Proof. Define $\phi_g: G \rightarrow G$ by $\phi_g(x) = gxg^{-1}$. Then ϕ_g is an automorphism of G , so $(\phi_g)_*\mu$ is a (left or right) Haar measure on G . By uniqueness, we conclude that there exists $\Delta(g) \in \mathbb{R}^+$, such that $(\phi_g)_*\mu = \Delta(g)\mu$. It is easy to see that Δ is a continuous homomorphism. $\square$

(I.22) **Definition.** The function Δ defined in Prop. I.21 is called the *modular function* of G .

(I.23) **Other terminology.** Some authors call $1/\Delta$ the modular function, because they use the conjugation $g^{-1}Ag$, instead of gAg^{-1} .

(I.24) **Corollary.** *Let Δ be the modular function of G .*

- 1) *If μ is any right Haar measure on G , then $\mu(gA) = \Delta(g)\mu(A)$ for any Borel set $A \subset G$.*
- 2) *If μ is any left Haar measure on G , then $\mu(Ag) = \Delta(g^{-1})\mu(A)$ for any Borel set $A \subset G$.*
- 3) *G is unimodular if and only if $\Delta(g) = 1$, for all $g \in G$.*
- 4) *If G is a Lie group, then $\Delta(g) = |\det(\text{Ad}_G g)|$ for all $g \in G$.*

(I.25) **Proposition.** *Let μ be the left Haar measure on a locally compact topological group G . Then $\mu(G) < \infty$ if and only if G is compact.*

Proof. ($\Leftarrow$) Haar measure is finite on compact sets (see I.19(1)).

($\Rightarrow$) We prove the contrapositive. Let C be a compact subset of nonzero measure. Because $G \times G \rightarrow G: (g, h) \mapsto gh^{-1}$ is continuous, and the continuous image of a compact set is compact, we know CC^{-1} is compact. Since G is not compact, then there exists $g_1 \notin CC^{-1}$; thus g_1C is disjoint from C . Continuing, we construct, by induction on n , a sequence $\{g_n\}$ of elements of G , such that $\{g_nC\}$ is a collection of pairwise disjoint sets. They all have the same measure (since μ is G -invariant), so we conclude that

$$\mu(G) \geq \mu\left(\bigcup_{n=1}^{\infty} g_nC\right) = \infty.$$

$\square$

(I.26) **Example.** Important examples of Lie groups are:

- $\text{SL}(n, \mathbb{R})$, the group consisting of all $n \times n$ real matrices of determinant 1;
- $\text{SO}(n) = \{g \in \text{SL}(n, \mathbb{R}) \mid gg^T = \text{Id}\}$, where g^T denotes the transpose of the matrix g ; and
- $\text{SO}(m, n) = \{g \in \text{SL}(m+n, \mathbb{R}) \mid gI_{m,n}g^T = I_{m,n}\}$, where $I_{m,n}$ is the $(m+n) \times (m+n)$ diagonal matrix whose diagonal entries are $1, 1, \dots, 1, -1, -1, \dots, -1$, where there are m 1's, followed by n -1's.

(I.27) **Definition.** The *Lie algebra* $\mathfrak{g}$ of G is the tangent space $T_e(G)$. It can also be identified with the space of all left-invariant vector fields on G , so the usual bracket of vector fields provides it with the structure of a Lie algebra.

(I.28) **Definition.** The *adjoint representation* of G is the differential of the action of G on itself by conjugation. That is, for each $g \in G$, define

$$\mathrm{Ad}_G g: \mathfrak{g} \rightarrow \mathfrak{g}$$

by $\mathrm{Ad}_G g = df_e$, where $f: G \rightarrow G$ is defined by $f(x) = gxg^{-1}$.

Then $\mathrm{Ad}_G: G \rightarrow \mathrm{GL}(\mathfrak{g})$ is a homomorphism.

(I.29) **Example.**

- 1) For $G = \mathrm{GL}(\ell, \mathbb{R})$, we have $\mathfrak{g} = \mathrm{Mat}_{\ell \times \ell}(\mathbb{R})$, and $(\mathrm{Ad}_G g)(x) = gxg^{-1}$.
- 2) If $H \subset G$, then $\mathfrak{h} \subset \mathfrak{g}$, and we have $\mathrm{Ad}_H h = (\mathrm{Ad}_G h)|_{\mathfrak{h}}$, for $h \in H$.

(I.30) **Theorem.** If G is semisimple, then

- 1) $\mathrm{Ad} G$ is a normal subgroup of $\mathrm{Aut}(\mathfrak{g})$ and
- 2) the quotient group $(\mathrm{Aut}(\mathfrak{g})) / (\mathrm{Ad} G)$ is finite.

(I.31) **Theorem.** If

- H and L are Lie groups, and
- $\rho: H \rightarrow L$ is a Borel-measurable homomorphism,

then ρ is continuous. In fact, ρ is C^∞ .

Proof. *Step 1.* ρ is continuous. It suffices to show that ρ is continuous at e (see Exer. I:1). Thus, given a neighborhood V of e in L , we wish to find a neighborhood U of e in H , such that $\rho(U) \subset V$.

Choose a neighborhood V_1 of e in L , such that

- V_1 is symmetric (that is, $(V_1)^{-1} = V_1$), and
- $(V_1)^4 = V_1 \cdot V_1 \cdot V_1 \cdot V_1 \subset V$.

Let $U_1 = \rho^{-1}(V_1)$, and $U = (U_1)^4$.

Because $(V_1)^4 \subset V$, it is clear that $\rho(U) \subset V$, so we need only show that U contains a neighborhood of e in H . To this end, note that L is the union of countably many translates gV_1 of V_1 , so H is the union of countably many translates of U_1 ; therefore, U_1 is not a null set. Hence $(U_1)^2$ contains an open subset of H (see Exer. I:2). So

$$U = (U_1)^4 = (U_1)^2 \cdot (U_1)^{-2}$$

contains a neighborhood of e .

Step 2. ρ is C^∞ .

Case 1. Assume $H = \mathbb{R}$. For simplicity, let us assume $L = \mathrm{SL}(\ell, \mathbb{R})$. There are neighborhoods U of 0 in $\mathrm{Mat}_{\ell \times \ell}(\mathbb{R})$ and V of Id in $\mathrm{GL}(\ell, \mathbb{R})$, such that the exponential map,

$$\exp X = \mathrm{Id} + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \cdots,$$

is a diffeomorphism from U onto V . Furthermore, by shrinking U , we may assume that U is star-shaped; that is, if $X \in U$ and $t \in [0, 1]$, then $tX \in U$.

Choose a neighborhood U_1 of 0 in U , such that

- $tU_1 \subset U_1$, for all $t \in [0, 1]$, and
- $2U_1 \subset U$,

and let

$$V_1 = \exp(U_1) \subset V.$$

From Step 1, we know there is some $\epsilon > 0$, such that

$$\rho(t) \in V_1 \text{ for all } t \text{ with } |t| \leq \epsilon.$$

By rescaling, we may assume, without loss of generality, that

$$\epsilon = 1.$$

Let ξ be the unique element of U_1 with $\exp \xi = \rho(1)$, and define $\rho': \mathbb{R} \rightarrow \mathrm{SL}(\ell, \mathbb{R})$ by

$$\rho'(t) = \exp(t\xi).$$

Then

- 1) ρ' is a C^∞ homomorphism, and
- 2) $\rho'(1) = \exp \xi = \rho(1)$.

Let ζ be the unique element of U_1 with $\exp \zeta = \rho(1/2)$. Then

$$\exp(2\zeta) = \rho(1/2)^2 = \rho(1) = \exp \xi.$$

Since 2ζ and ξ each belong to U , we conclude that $2\zeta = \xi$, so $\zeta = (1/2)\xi$. Therefore

$$\rho(1/2) = \exp(\zeta) = \exp((1/2)\xi) = \rho'(1/2).$$

Proceeding by induction on n , we see that

$$\rho(1/2^n) = \rho'(1/2^n) \text{ for each } n \in \mathbb{N}.$$

Because ρ and ρ' are homomorphisms, this implies that $\rho(k/2^n) = \rho'(k/2^n)$ for all $k \in \mathbb{Z}$ and all $n \in \mathbb{N}$. Since $\{k/2^n\}$ is dense in $\mathbb{R}$ and ρ is continuous (see Step 1), we conclude that $\rho = \rho'$ is C^∞ , as desired.

Case 2. The general case. For simplicity, let us assume that H is a closed subgroup of $\mathrm{SL}(\ell, \mathbb{R})$. Let $\xi_1, \dots, \xi_n$ be a basis of the Lie algebra $\mathfrak{h}$ of H , and, for each i , define a homomorphism $\rho_i: \mathbb{R} \rightarrow L$ by

$$\rho_i(t) = \rho(\exp(t\xi_i)).$$

- From Case 1, we know that each ρ_i is C^∞ . Hence, the map $\rho': \mathbb{R}^n \rightarrow L$, defined by

$$\rho'(t_1, \dots, t_n) = \rho_1(t_1) \rho_2(t_2) \rho_3(t_3) \cdots \rho_n(t_n),$$

is C^∞ .

- The Inverse Function Theorem implies that the map $\phi: \mathbb{R}^n \rightarrow H$, defined by

$$\phi(t_1, \dots, t_n) = \exp(t_1\xi_1) \exp(t_2\xi_2) \exp(t_3\xi_3) \cdots \exp(t_n\xi_n),$$

is a local diffeomorphism at 0; there is a neighborhood U of 0 in $\mathbb{R}^n$ and a neighborhood V of e in H , such that $\phi|_U$ is a diffeomorphism from U onto V .

By construction, we have $\rho \circ \phi = \rho'$, so we conclude that ρ is C^∞ on V . Hence, ρ is C^∞ on all of H (see Exer. I:1). $\square$

(I.32) **Remark.** It can be shown that every (measurable) homomorphism of Lie groups is real analytic, but we do not need this stronger fact.

I.D. Galois theory and field extensions

(I.33) **Theorem** (Fundamental Theorem of Algebra). *The field $\mathbb{C}$ of complex numbers is algebraically closed; that is, every nonconstant polynomial $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.*

Proof. This can be proved algebraically, by combining Galois Theory with the elementary fact that every real polynomial of odd degree has a real zero (see Exer. I:3), but we use a bit of complex analysis.

Suppose $f(x)$ has no root. Then $1/f$ is holomorphic on $\mathbb{C}$. Furthermore, because $f(z) \rightarrow \infty$ as $z \rightarrow \infty$, it is easy to see that $1/f$ is bounded on $\mathbb{C}$. Hence, Liouville's Theorem asserts that $1/f$ is constant. This contradicts the fact that f is not constant. $\square$

(I.34) **Proposition.** *Suppose F is a field, and α is a root of some irreducible polynomial $f(x) \in F[x]$. Then the extension field $F[\alpha]$ is isomorphic to $F[x]/I$, where $I = f(x)F[x]$ is the principal ideal of $F[x]$ generated by $f(x)$.*

Proof. The map $\phi: F[x] \rightarrow F[\alpha]$ defined by $\phi(g(x)) = g(\alpha)$ is a surjective ring homomorphism whose kernel is I . $\square$

(I.35) **Corollary.** *Suppose F is a field. If α and β are two roots of an irreducible polynomial $f(x) \in F[x]$, then there is an isomorphism $\sigma: F[\alpha] \rightarrow F[\beta]$ with $\sigma(\alpha) = \beta$.*

(I.36) **Corollary.** *Let F be a subfield of $\mathbb{C}$, and let $\sigma: F \rightarrow \mathbb{C}$ be any embedding. Then σ extends to an automorphism $\hat{\sigma}$ of $\mathbb{C}$.*

(I.37) **Notation.** If F is a subfield of a field L , then $|L : F|$ denotes $\dim_F L$. This is called the *degree* of L over F .

(I.38) **Corollary.** *If F and L are subfields of $\mathbb{C}$, such that $F \subset L$, then $|L : F|$ is equal to the number of embeddings σ of L in $\mathbb{C}$, such that $\sigma|_F = \text{Id}$.*

(I.39) **Definition.** An extension L of a field F is *Galois* if, for every irreducible polynomial $f(x) \in F[x]$, such that $f(x)$ has a root in L , there exist $\alpha_1, \dots, \alpha_n \in L$, such that

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

That is, if an irreducible polynomial in $F[x]$ has a root in L , then all of its roots are in L .

(I.40) **Definition.** Let L be a Galois extension of a field F . Then

$$\text{Gal}(L/F) = \{ \sigma \in \text{Aut}(L) \mid \sigma|_F = \text{Id} \}.$$

This is the *Galois group* of L over F .

(I.41) **Proposition.** *If L is a Galois extension of a field F of characteristic 0, then $\# \text{Gal}(L/F) = |L : F|$.*

(I.42) **Corollary.** *If L is a Galois extension of a field F of characteristic 0, then there is a one-to-one correspondence between*

- the subfields K of L , such that $F \subset K$, and
- the subgroups H of $\text{Gal}(L/F)$.

Proof. Given K , with $F \subset K \subset L$, let $H_K = \text{Gal}(L/K)$. Conversely, given a subgroup H of $\text{Gal}(L/F)$, let

$$K_H = \{ x \in L \mid \sigma(x) = x, \forall \sigma \in H \}$$

be the fixed field of H . $\square$

I.E. Algebraic numbers and transcendental numbers

(I.43) Definition.

- A complex number z is *algebraic* if there is a nonzero polynomial $f(x) \in \mathbb{Z}[x]$, such that $f(z) = 0$.
- A complex number that is not algebraic is said to be *transcendental*.
- A (nonzero) polynomial is *monic* if its leading coefficient is 1; that is, we may write $f(x) = \sum_{k=0}^n a_k x^k$ with $a_n = 1$.
- A complex number z is an *algebraic integer* if there is a *monic* polynomial $f(x) \in \mathbb{Z}[x]$, such that $f(z) = 0$.

(I.44) **Proposition** ($\mathbb{Z}$ is integrally closed). *A rational number t is an algebraic integer if and only if $t \in \mathbb{Z}$.*

Proof. ($\Leftarrow$) t is a root of the monic polynomial $x - t$.

($\Rightarrow$) Suppose $f(t) = 0$, where $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$ with each $a_k \in \mathbb{Z}$. Writing $t = p/q$ (in lowest terms) with $p, q \in \mathbb{Z}$, we have

$$0 = q^n \cdot 0 = q^n f(t) = q^n \left(\frac{p^n}{q^n} + \sum_{k=0}^{n-1} a_k \frac{p^k}{q^k} \right) = p^n + \sum_{k=0}^{n-1} a_k p^k q^{n-k} \equiv p^n \pmod{q}.$$

Since p^n is relatively prime to q (recall that $t = p/q$ is in lowest terms), we conclude that $q = 1$, so $t = p/1 \in \mathbb{Z}$. $\square$

(I.45) **Proposition.** *If α is an algebraic number, then there is some nonzero $m \in \mathbb{Z}$, such that $m\alpha$ is an algebraic integer.*

Proof. Suppose $g(\alpha) = 0$, where $g(x) = \sum_{k=0}^n b_k x^k$, with each $b_k \in \mathbb{Z}$, and $b_n \neq 0$. Let

- $m = a_n$,
- $a_k = m^{n-k-1} b_k$, and
- $f(x) = \sum_{k=0}^n a_k x^k$.

Then $f(x)$ is a monic, integral polynomial, and

$$f(m\alpha) = \sum_{k=0}^n (m^{n-k-1} b_k) (m\alpha)^k = m^{n-1} \sum_{k=0}^n b_k \alpha^k = m^{n-1} g(\alpha) = m^{n-1} \cdot 0 = 0.$$

$\square$

(I.46) **Lemma.** *For $t \in \mathbb{C}$, the following are equivalent:*

- 1) t is an algebraic integer;
- 2) $\mathbb{Z}[t]$ is a finitely-generated $\mathbb{Z}$ -module;
- 3) $\mathbb{Z}[t]$ is a Noetherian $\mathbb{Z}$ -module.

(I.47) **Proposition.** *The set of algebraic integers is a subring of $\mathbb{C}$.*

(I.48) **Proposition.** *Let*

- ω be a primitive n^{th} root of unity, and
- $\mathbb{Z}_n^\times$ denotes the multiplicative group of units modulo n ,

for some n . Then there is an isomorphism

$$f: \mathbb{Z}_n^\times \rightarrow \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}),$$

such that $f(k)(\omega) = \omega^k$, for all $k \in \mathbb{Z}_n^\times$.

I.F. Polynomial rings and the Nullstellensatz

(I.49) **Definition.** A commutative ring R is *Noetherian* if the following equivalent conditions hold:

- 1) Every ideal of R is finitely generated.
- 2) Every nonempty collection of ideals of R has a maximal element.
- 3) If $I_1 \subset I_2 \subset \cdots$ is any increasing chain of ideals of R , then $I_m = I_{m+1} = \cdots$ for some m .

(I.50) **Theorem.** If R is Noetherian, then the polynomial ring $R[x]$ is Noetherian.

Proof. Suppose J is an ideal of $R[x]$. (We wish to show that J is finitely generated.) For $d \in \mathbb{N}$, let

$$J_d = \{0\} \cup \{\text{lead}(f) \mid f \in J, \deg f = d\}.$$

Then J_d is an ideal of R , and we have $J_1 \subset J_2 \subset \cdots$, so there is some d_0 , such that $J_d = J_{d_0}$, for all $d \geq d_0$.

For each d , let F_d be a finite set of polynomials of degree d , such that $\{\text{lead}(f) \mid f \in F_d\}$ generates J_d .

Then $F_0 \cup F_1 \cup \cdots \cup F_{d_0}$ generates J . (For any $f \in J$, there exists $f' \in \langle F_0 \cup F_1 \cup \cdots \cup F_{d_0} \rangle$, such that $\deg f' = \deg f$, and $\text{lead}(f') = \text{lead}(f)$. Then $\deg(f - f') < \deg f$, so we may assume, by induction, that $f - f' \in \langle F_0 \cup F_1 \cup \cdots \cup F_{d_0} \rangle$. $\square$)

(I.51) **Corollary.** For any field F , the polynomial ring $F[x_1, \dots, x_s]$ (in any number of variables) is Noetherian.

Proof. Note that F has only one proper ideal, namely $\{0\}$, so it is obviously Noetherian. Now use Thm. I.50 to induct on s . $\square$

There are many equivalent formulations of the following important theorem.

(I.52) **Theorem.** Let F be a subfield of a field L . If L is finitely generated as an F -algebra (that is, if there exist $c_1, \dots, c_r \in L$, such that $L = F[c_1, \dots, c_r]$), then L is algebraic over F .

Proof. Suppose L is transcendental over F . (This will lead to a contradiction.) Let $\{x_1, \dots, x_n\}$ be a transcendence basis for L over F . (That is, L is algebraic over $F[x_1, \dots, x_n]$, and x_k is transcendental over $F[x_1, \dots, x_{k-1}]$, for each k .) By replacing F with $F[x_1, \dots, x_{n-1}]$, we may assume $n = 1$. Therefore, $L = F[x, a_1, \dots, a_m]$, where each a_j is algebraic over $F[x]$.

From the proof of Prop. I.44, we see that there exists $g \in F[x]$, such that $ga_1, \dots, ga_m$ are integral over $F[x]$. Choose some irreducible $f \in F[x]$, such that

$$f \nmid g.$$

We have

$$1/f \in L = F[x, a_1, \dots, a_m] = F[x, ga_1, \dots, ga_m, 1/g],$$

so $g^k/f \in F[x, ga_1, \dots, ga_m]$, for some $k \geq 0$. Therefore, g^k/f is integral over $F[x]$.

From the proof of Prop. I.44, we conclude that $g^k/f \in F[x]$. (The ring $F[x]$ is integrally closed.) This contradicts the choice of f . $\square$

(I.53) **Corollary.** *Let*

- F be an algebraically closed field,
- $F[x_1, \dots, x_r]$ be a polynomial ring over F , and
- $\mathfrak{m}$ be any maximal ideal of $F[x_1, \dots, x_r]$.

Then

- 1) the natural inclusion $F \hookrightarrow F[x_1, \dots, x_r]/\mathfrak{m}$ is an isomorphism, and
- 2) there exist $a_1, \dots, a_r \in F$, such that $\mathfrak{m} = \langle (x_1 - a_1), \dots, (x_r - a_r) \rangle$.

Proof. (1) Let $L = F[x_1, \dots, x_r]/\mathfrak{m}$. Then L is a field (because $\mathfrak{m}$ is maximal), so Thm. I.52 implies L is algebraic over F . Since F is algebraically closed, we conclude that $L = F$, as desired.

(2) From (1), we know there exists $a_j \in F$, such that $a_j \equiv x_j \pmod{\mathfrak{m}}$; let

$$I = \langle (x_1 - a_1), \dots, (x_r - a_r) \rangle.$$

From the choice of $a_1, \dots, a_r$, we have $I \subset \mathfrak{m}$. On the other hand, it is easy to see that

$$F[x_1, \dots, x_r]/I \cong F$$

is a field, so I must be a maximal ideal. Hence, it is equal to $\mathfrak{m}$. □

(I.54) **Corollary** (Nullstellensatz). *Let*

- F be an algebraically closed field,
- $F[x_1, \dots, x_r]$ be a polynomial ring over F , and
- I be any proper ideal of $F[x_1, \dots, x_r]$.

Then there exist $a_1, \dots, a_r \in F$, such that $f(a_1, \dots, a_r) = 0$ for all $f(x_1, \dots, x_r) \in I$.

Proof. Let $\mathfrak{m}$ be a maximal ideal that contains I , and choose $a_1, \dots, a_r \in F$ as in I.53(2). Then $f(a_1, \dots, a_r) = 0$ for all $f(x_1, \dots, x_r) \in \mathfrak{m}$, so, since $I \subset \mathfrak{m}$, the desired conclusion follows. □

(I.55) **Corollary.** *If B is any finitely generated subring of $\mathbb{C}$, then there is a nontrivial homomorphism $\phi: B \rightarrow \overline{\mathbb{Q}}$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.*

Proof. We have $B = \mathbb{Z}[b_1, \dots, b_r]$, for some $b_1, \dots, b_r \in B$. There is a homomorphism

$$\phi: \mathbb{Q}[x_1, \dots, x_r] \rightarrow \mathbb{C},$$

defined by $\phi(f(x_1, \dots, x_r)) = f(b_1, \dots, b_r)$. Let I be the kernel of ϕ , and choose a maximal ideal $\mathfrak{m}$ that contains I . Then $I \subset \mathfrak{m}$, so there is a natural homomorphism

$$B = \phi(\mathbb{Z}[x_1, \dots, x_r]) \subset \phi(\overline{\mathbb{Q}}[x_1, \dots, x_r]) \cong \frac{\overline{\mathbb{Q}}[x_1, \dots, x_r]}{I} \rightarrow \frac{\overline{\mathbb{Q}}[x_1, \dots, x_r]}{\mathfrak{m}} \cong \overline{\mathbb{Q}}$$

(see I.53(1)). □

I.G. Eisenstein Criterion

(I.56) **Lemma.** *If $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$.*

Proof. We prove the contrapositive: suppose $f(x)$ is reducible over $\mathbb{Q}$. Clearing denominators, we may write $nf(x) = g_1(x)g_2(x)$, for some nonzero $n \in \mathbb{Z}$, with $g_j(x) \in \mathbb{Z}[x]$ and $\deg g_j(x) \geq 1$.

Dividing $f(x)$ by an integer constant, we may assume $\text{cont}(f(x)) = 1$, where $\text{cont}(f(x))$ denotes the *content* of $f(x)$, that is, the greatest common divisor of the coefficients of $f(x)$. Then, letting $d_j = \text{cont}(g_j(x))$, we have

$$n = \text{cont}(nf(x)) = \text{cont}(g_1(x)g_2(x)) = d_1d_2$$

(see Exer. 10:28). Thus, letting $\hat{g}_j(x) = \frac{1}{d_j}g_j(x) \in \mathbb{Z}[x]$, we have

$$f(x) = \frac{g_1(x)g_2(x)}{d_1d_2} = \hat{g}_1(x)\hat{g}_2(x),$$

so $f(x)$ is reducible over $\mathbb{Z}$, as desired. $\square$

(I.57) **Lemma** (Eisenstein Criterion). *Let $f(x) \in \mathbb{Z}[x]$. If there is a prime number p , and some $a \in \mathbb{Z}_p \setminus \{0\}$, such that*

- $f(x) \equiv ax^n \pmod{p}$, where $n = \deg f(x)$, and
- $f(0) \not\equiv 0 \pmod{p^2}$,

then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. Suppose $f(x)$ is reducible over $\mathbb{Q}$. (This will lead to a contradiction.) Then $f(x)$ is also reducible over $\mathbb{Z}$ (see I.56), so we may write $f(x) = g_1(x)g_2(x)$, with $g_j(x) \in \mathbb{Z}[x]$ and $\deg g_j(x) \geq 1$. Then

$$g_1(x)g_2(x) = f(x) \equiv ax^n \pmod{p}.$$

From the unique factorization of polynomials in $\mathbb{Z}_p[x]$ (recall that $\mathbb{Z}_p[x]$ is a Euclidean domain, because $\mathbb{Z}_p$ is a field), we conclude that there exist $b_1, b_2 \in \mathbb{Z}_p \setminus \{0\}$ and $m_1, m_2 \in \mathbb{N}$, such that $g_j(x) \equiv b_j x^{m_j} \pmod{p}$. Since

$$m_1 + m_2 = n = \deg f(x) = \deg(g_1(x)g_2(x)) = \deg g_1(x) + \deg g_2(x),$$

and $m_j \leq \deg g_j(x)$, we conclude that $m_j = \deg g_j(x) > 1$. Therefore $g_j(0) \equiv 0 \pmod{p}$, so $f(0) = g_1(0)g_2(0) \equiv 0 \pmod{p^2}$. This is a contradiction. $\square$

I.H. Notes

Need to track down references for this stuff!!!

The fact that measurable homomorphisms are continuous (see I.31) was proved by G. Mackey. A proof can be found in [Zm, Thm. B.3, p. 198]. A proof that continuous homomorphisms are real analytic (hence C^∞) can be found in [Ch, Prop. 1 of §4.8, pp. 128–129].

I.I. References

- [Ch] C. Chevalley: *Theory of Lie Groups*, Princeton Univ. Press, Princeton, 1946.
- [Zm] R. J. Zimmer: *Ergodic Theory and Semisimple Groups*, Birkhäuser, Boston, 1984.

Exercises

- I:1) Suppose $\rho: H \rightarrow L$ is a homomorphism of Lie groups. Show:
- (a) If ρ is continuous on some open subset of H , then ρ is continuous.
 - (b) If ρ is C^∞ on some open subset of H , then ρ is C^∞ .
- I:2) Suppose A and B are measurable subsets of a Lie group H , with Haar measure μ . If $\mu(A) > 0$ and $\mu(B) > 0$, then

$$A \cdot B = \{ ab \mid a \in A, b \in B \}$$

contains an open subset of H . [*Hint:* Assume $\mu(A)$ and $\mu(B)$ are finite, and let χ_A and χ_B be the characteristic functions of the two sets. Define the convolution $\chi_A * \chi_B$ by defined by

$$(\chi_A * \chi_B)(h) = \int_H \chi_A(t) \chi_B(t^{-1}h) d\mu(t).$$

Show that $\|\chi_A * \chi_B\|_1 = \|\chi_A\|_1 \|\chi_B\|_1 \neq 0$, and that $\chi_A * \chi_B$ is continuous. (Approximate χ_A and χ_B by continuous functions, and use uniform convergence.)]

- I:3) Let F be a field of characteristic zero, such that
- (a) if $f \in F[x]$ has odd degree, then f has a root in F ;
 - (b) if $a \in F$, then either a or $-a$ has a square root in F ; and
 - (c) -1 does not have a square root in F .

Show that $F[i]$ is algebraically closed (where $i = \sqrt{-1}$). [*Hint:* Let L be a finite, Galois extension of $F[i]$. If P is a Sylow 2-subgroup of $\text{Gal}(L/F)$, then the fixed field of P has odd degree over F , so this fixed field must be trivial. Thus, $|L : F|$ is a power of 2. Hence, L can be obtained by a series of quadratic extensions. Since every element of F has a square root in $F[i]$, the half-angle formulas show that every element of $F[i]$ has a square root in $F[i]$. Therefore $L \subset F[i]$.]

- I:4) Derive Thm. I.52 as a corollary of Cor. I.53. [*Hint:* Let $\overline{F}$ be the algebraic closure of F . The proof of Cor. I.55 shows that there is a nontrivial homomorphism $\phi: L \rightarrow \overline{F}$, such that $\phi|_F = \text{Id}$. Show ϕ is injective, so L is isomorphic to a subfield of $\overline{F}$.]

Index

- (A^-, B, A^+) -contracting, 60
- 2-cocycle, 171
- absolutely simple, 148
- absolutely simple Lie group, 148
- absolutely simple over F , 149, 161
- act without inversion, 237
- action of G , 252
- adjoint representation, 254
- algebraic group over $\mathbb{R}$, 32
- algebraic integer, 257
- algebraic number, 257
- algebraic number field, 80
- almost simple Lie group, 20
- anisotropic bilinear form, 38
- antiinvolution, 147
- archimedean place, 80
- arithmetic hyperbolic manifold, 98
- arithmetic lattice, 9
- arithmetic subgroup, 71
- Arithmetic subgroups are lattices, 8
- atlas on a manifold, 250
- atom (of a measure), 228
- atomless measure, 228
- automorphism (of a graph), 235
- axis of a tree automorphism, 237
- Bass-Serre theory of group actions on trees, 236
- Borel Density Theorem, 52
- Borel subgroup, 39
- boundary of X , 117
- bounded subset of a graph, 237
- Brauer group, 167, 168
- Brauer-Hasse-Noether Theorem, 168
- Cartan Decomposition, 36
- Cartan involution, 36
- cartesian product of Riemannian manifolds, 250
- Cayley graph, 248
- central division algebra, 146, 163
- central extension, 244
- central simple algebra, 169
- classical group, 22
- coboundary, 171
- cocompact subgroup, 45
- cocycle identity, 171
- Commensurability Criterion for Arithmeticity, 73
- commensurability subgroup, 46
- commensurable, 33
- commensurable (abstractly), 47
- commensurator, 46
- compactly generated, 66
- complete graph, 235
- complete metric space, 251
- completely reducible, 22
- completion of F , 80
- complex hyperbolic space, 116
- complex place, 80
- complexification, 26, 135
- conjugation on a quaternion algebra, 147
- connected graph, 236
- content of an integral polynomial, 260
- continuous action, 252
- coordinate system, 250
- cycle (in a graph), 248
- cyclic extension of F , 165
- defined over $\mathbb{Q}$, 69, 76, 77
- defined over $\mathbb{R}$, 69
- defined over F , 124, 140
- degree (of a division algebra), 148
- degree of L over F , 256
- degree of a division algebra, 151
- degree of a vertex, 237
- discrete Heisenberg group, 221, 237
- discriminant (of quadratic form), 94
- distance (in a graph), 237
- division ring, 147
- edge (of a graph), 235
- Eisenstein Criterion, 260
- elliptic element of G , 34, 35
- empty graph, 235
- equivalent embeddings in $\mathbb{C}$, 80
- Existence and Uniqueness of Geodesics, 251
- Existence and Uniqueness of Haar Measure, 252
- exponential coordinates, 251

- F -isogeny, 149
- finite place, 80
- finite volume (homogeneous space), 45
- fixed point, 2
- flag of subspaces, 231
- flat (in X), 14
- free action, 252
- Fundamental Theorem of Algebra, 256
- Galois cohomology group, 171
- Galois conjugate of G , 80
- Galois extension, 256
- Galois group, 256
- geodesic symmetry, 3
- geodesically complete, 11, 251
- geodesics, existence and uniqueness, 251
- Godement Compactness Criterion, 75
- graph, 235
- Haar measure, 252
- Haar measure (left or right), 252
- Hermitian form, 147
- Holder function, 245
- homogeneous space, 1
- hybrid (of hyperbolic manifolds), 96
- hyperbolic element of G , 34, 35, 113
- hyperbolic manifold, 95
- hyperbolic manifold with totally geodesic boundary, 99
- infinite place, 80
- infinitely smaller, 221
- injectivity radius, 48
- inner automorphism, 40
- inner product, 250
- interbreeding hyperbolic manifolds, 96
- involution, 2
- involutive isometry, 2
- irreducible linear group, 21
- irreducible locally symmetric space, 9
- irreducible symmetric space, 5
- irreducible Zariski-closed subset, 42
- isogenous, 19
- isogenous over F , 124, 149
- isogeny over F , 149
- isolated fixed point, 2
- isotropic bilinear form, 38
- isotropic vector, 114
- isotypic semisimple Lie group, 72
- Jacobson Density Theorem, 170
- Jacobson-Morosov Lemma, 35
- Jordan Decomposition, Real, 35
- Killing form, 91
- Langlands Decomposition, 38, 130
- lattice subgroup, 7, 15, 45, 46
- Lebesgue number, 65
- left orderable, 220
- length (of a walk in a graph), 237
- length (smooth curve), 251
- Lie algebra, 253
- linear Lie group, 20
- locally isomorphic, 20
- locally symmetric, 6, 7
- Mahler Compactness Criterion, 49
- manifold, 250
- Margulis Arithmeticity Theorem, 72
- modular function, 253
- monic polynomial, 257
- Mostow Rigidity Theorem, 9
- net subgroup, 59
- Noether-Skolem Theorem, 169
- Noetherian ring, 258
- nonarchimedean place, 80
- noncompact type, 7
- nondegenerate Hermitian form, 148
- norm of a tangent vector, 250
- norm of an algebraic number, 78
- norm of an element of L , 165
- Nullstellensatz, 259
- octonions, 116, 147
- opposite algebra, 167
- order (in an algebraic number field), 78
- outer automorphism group, 40
- outer form, 150
- p -adic place, 80
- parabolic element of G , 34, 35
- parabolic subgroup, 37
- path (in a graph), 236
- Ping-Pong Lemma, 61
- place of F , 80
- Poincaré Recurrence Theorem, 52
- polynomial (on a vector space), 77
- positive definite, 5
- positive Weyl chamber, 133
- precompact, 49
- principal congruence subgroup, 57
- proper action, 252
- properly discontinuous, 252
- property (FA), 236
- $\mathbb{Q}$ -form, 76
- $\mathbb{Q}$ -rank, 125
- $\mathbb{Q}$ -rank(Γ), 122
- $\mathbb{Q}$ -simple group, 85
- $\mathbb{Q}$ -split torus, 121
- $\mathbb{Q}$ -subgroup, 69
- quasisplit $\mathbb{Q}$ -form of G , 111
- quaternion algebra, 107
- quaternionic hyperbolic space, 116
- $\mathbb{R}$ -split torus, 112
- radical of a Lie group, 20
- real algebraic group, 32
- Real Jordan Decomposition, 35
- real place, 80
- reduced norm, 23, 107
- reducible lattice, 47
- reducible linear group, 21
- Reeb-Thurston Stability Theorem, 219
- relatively compact, 49
- reversion antiinvolution, 107, 147
- Riemannian isometry, 251
- Riemannian manifold, 250
- right Haar measure, 252
- right orderable, 220

- Schur's Lemma, 170
- Selberg's Lemma (on torsion-free subgroups), 56
- semisimple element of G , 34
- semisimple Lie group, 20
- Siegel set, 132, 133
- simple (abstract group), 20
- simple algebra, 163
- simple Lie group, 20
- simply transitively, 115
- skew field, 147
- solvable Lie group, 20
- special linear group, 22, 23
- Special orthogonal group, 22, 23
- Special unitary group, 22
- sphere at ∞ , 117
- splits over a field, 148
- standard antiinvolution, 147
- star-shaped, 251
- subtree, 237
- symmetric neighborhood, 251, 254
- symmetric space, 2, 3
- symmetric subset of a group, 248
- symplectic group, 22, 23
- symplectic unitary group, 23

- tangent cone at infinity, 16
- Tits Alternative, 59
- Tits building, 17
- torsion free, 56
- torus, 112
- torus subgroup, 112
- totally geodesic hypersurface, 96
- totally isotropic subspace, 37, 114
- totally real number field, 88
- transcendental number, 257
- two-point homogeneous, 15
- type $(A_n, B_n, C_n, D_n, \dots)$, 24

- uniform subgroup, 45
- unimodular group, 253
- unipotent element of G , 34, 35
- unipotent radical, 38

- valence of a graph, 237
- valence of a vertex, 237
- variety, 32
- vector-space lattice, 77
- vertex (of a graph), 235
- virtually isomorphic, 47

- walk (in a graph), 236
- weak fundamental domain, 54
- Wedderburn's Theorem (semisimple artinian rings), 171
- weights of a representation, 21
- without inversion, 237
- Witt's Theorem, 38, 158

- $\mathbb{Z}$ is integrally closed, 257
- Zariski closed, 32
- Zariski closure, 32