Arithmetic Groups and Locally Symmetric Spaces

Preliminary version — send comments to `dwitte@math.okstate.edu`

Dave Witte

Department of Mathematics, Oklahoma State University, Stillwater, Oklahoma 74078, USA

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

List of Chapters

(Only 1–6, 8–10, and App. I are available so far)

Contents

Chapter 1

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 $\mathrm{Isom}(X)$ 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 $\mathrm{Isom}(S^n)^\circ = \mathrm{SO}(n+1)$. 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 $\mathrm{Isom}(\mathbb{R}^n)^\circ = \mathrm{SO}(n) \ltimes \mathbb{R}^n$. Any point in $\mathbb{R}^n$ can be translated to any other point, so $\mathbb{R}^n$ is homogeneous.
- The hyperbolic plane $\mathfrak{H}^2 = \{\, z \in \mathbb{C} \mid \mathrm{Im}\, z > 0 \,\}$, where the inner product on $T_z\mathfrak{H}^n$ is given by
$$\langle u \mid v \rangle_{\mathfrak{H}^2} = \frac{1}{4(\mathrm{Im}\, z)^2} \langle u \mid v \rangle_{\mathbb{R}^2}.$$
One may show that $\mathrm{Isom}(\mathfrak{H}^2)^\circ$ is isomorphic to $\mathrm{PSL}(2,\mathbb{R})^\circ = \mathrm{SL}(2,\mathbb{R})/\{\pm 1\}$, by noting that $\mathrm{SL}(2,\mathbb{R})$ 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 $\mathrm{Isom}(\mathfrak{H}^n)^\circ$ is isomorphic to $\mathrm{SO}(1,n)^\circ$ (see Exer. 1:4).
- A cartesian product of any combination of the above (see Exer. 1:6).

(1.3) **Definition.** Let $\phi\colon X \to X$.

- We may say that ϕ is *involutive* (or that ϕ is an *involution*) if $\phi^2 = \mathrm{Id}$.
- 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 $\phi_1\colon S^n \to S^n$ by
$$\phi_1(x_1,\ldots,x_{n+1}) = (-x_1,\ldots,-x_n,x_{n+1}).$$
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 $e_{n+1} = (0,0,\ldots,0,1)$. Thus, e_{n+1} is an isolated fixed point of ϕ_1.
- Define $\phi_2\colon \mathbb{R}^n \to \mathbb{R}^n$ 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 $\phi_3\colon \mathfrak{H}^2 \to \mathfrak{H}^2$ 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 $\phi^2 = \mathrm{Id}$ 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 Riemmanian manifold X, and suppose p is an isolated fixed point of ϕ. Then*

1) $d\phi_p = -\mathrm{Id}$*; and*
2) *for every geodesic γ with $\gamma(0) = p$, we have $\phi\bigl(\gamma(t)\bigr) = \gamma(-t)$, 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 $\phi^2 = \mathrm{Id}$, we know that $d(\phi^2)_p = d\,\mathrm{Id}_p = \mathrm{Id}$. We conclude that $(d\phi_p)^2 = \mathrm{Id}$; thus, the linear transformation $d\phi_p \colon T_pX \to T_pX$ satisfies the polynomial equation $x^2 - 1 = 0$.

Suppose $d\phi_p \neq -\mathrm{Id}$. (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 $d\phi_p \neq -\mathrm{Id}$, 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

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

and

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

Since a geodesic is uniquely determined by prescribing its initial position and its initial velocity, we conclude that $\phi \circ \gamma = \gamma$. Therefore, $\phi\big(\gamma(t)\big) = \gamma(t)$, 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 $\overline{\gamma}(t) = \gamma(-t)$, so $\overline{\gamma}$ is a geodesic. Because ϕ is an isometry, we know that $\phi \circ \gamma$ is also a geodesic. We have

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

and, from (1),

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

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

(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.7). The *geodesic symmetry* at p is the diffeomorphism τ of U defined by

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

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 $\tau\big(\gamma(t)\big) = \gamma(-t)$.

(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 $G = \mathrm{Isom}(X)^\circ$. Because $\mathrm{Isom}(X)$ 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

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

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 $\mathbb{R}^n = \big(\mathrm{SO}(n) \ltimes \mathbb{R}^n\big)/\mathrm{SO}(n)$. Note that the map $\sigma\colon (k, v) \mapsto (k, -v)$ 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 $(1, -1, -1, \ldots, -1)$, 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 Riemmanian 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 $K^+ = \langle \sigma \rangle \times K$, 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

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

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, $gK = eK$. □

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 $\alpha\colon G \times X \to X$ by $\alpha(g,x) = gxg^T$. Then:

a) α defines an action of G on X; that is, we have $\alpha(gh,x) = \alpha\big(g,\alpha(h,x)\big)$ 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 $\tau\colon X \to X$, defined by $\tau(A) = A^{-1}$, is an involutive isometry of X, such that $\tau\big(\alpha(g,x)\big) = \sigma(g)\,\tau(x)$ 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
- $\mathrm{SO}(p,q)^\circ/\big(\mathrm{SO}(p) \times \mathrm{SO}(q)\big)$.

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

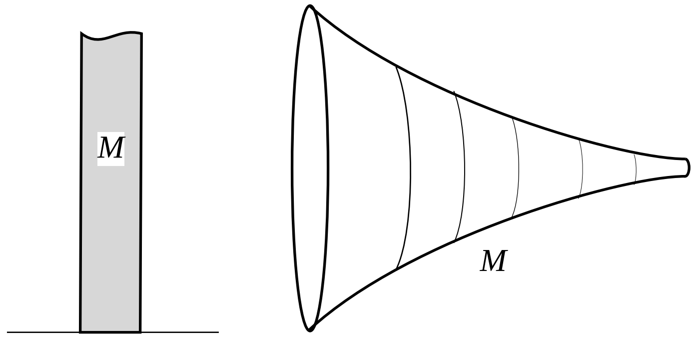

Figure 1.1. The cusp M.

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 $g\colon \mathfrak{H}^2 \to \mathfrak{H}^2$ 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.

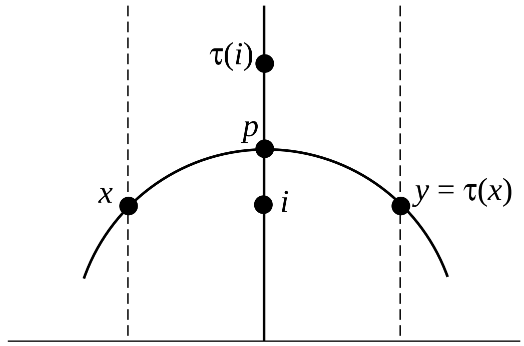

Figure 1.2. The geodesic symmetry τ at p.

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.)

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

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

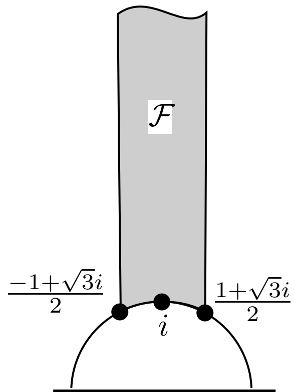

Figure 1.3. A fundamental domain $\mathcal{F}$ for $\mathrm{SL}(2,\mathbb{Z})$ in $\mathrm{SL}(2,\mathbb{R})$.

(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** (Borel-Harish-Chandra, Mostow-Tamagawa)**.** *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 6.20).) 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 $H^n(\Gamma';\mathbb{Z})$ 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 [Rag1].

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].

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

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

and let $e_n = (0, 0, \ldots, 0, 1) \in \mathbb{R}^n$. Show that the map $\phi \colon B^n \to \mathfrak{H}^n$ 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 $\psi \colon B^n \to X_{1,n}^{+}$ defined by

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

is an isometry. (Note that this implies that the restriction of $\langle \cdot \mid \cdot \rangle_{1,n}$ to $T_x X_{1,n}^{+}$ is positive definite, even though $\langle \cdot \mid \cdot \rangle_{1,n}$ 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 $X_1, X_2, \ldots, X_n$ are homogeneous spaces, then the cartesian product $X_1 \times X_2 \times \cdots \times X_n$ is also homogeneous.

1:7) Show that every homogeneous space is *geodesically complete*. That is, for every geodesic segment $\gamma \colon (-\epsilon, \epsilon) \to X$, there is a doubly-infinite geodesic $\overline{\gamma} \colon \mathbb{R} \to X$, such that $\overline{\gamma}(t) = \gamma(t)$ for all $t \in (-\epsilon, \epsilon)$.

1:8) Show that if $X_1, \ldots, X_n$ are symmetric spaces, then the cartesian product $X_1 \times X_2 \times \cdots \times X_n$ 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.16 to show that the closure of H in $\mathrm{Isom}(M)$ is compact.

1:14) Let K be a compact group, and let $\rho\colon K \to \mathrm{GL}(n,\mathbb{R})$ be a continuous homomorphism. Show that there is a K-invariant inner product $\langle \cdot \mid \cdot \rangle_K$ on $\mathbb{R}^n$; that is, such that

$$\big\langle \rho(k)u \mid \rho(k)v \big\rangle_K = \big\langle u \mid v \big\rangle_K$$

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

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

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 is 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 $\big(M, \langle \cdot \mid \cdot \rangle_x\big)$. Define a new inner product $\langle \cdot \mid \cdot \rangle'_x$ on each tangent space T_xM by

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

(a) Show that the Riemannian metric $\langle \cdot \mid \cdot \rangle'$ on M is F-invariant.
(b) Show that if G is a group of isometries of $\big(M, \langle \cdot \mid \cdot \rangle_x\big)$, and G is normalized by F, then $\langle \cdot \mid \cdot \rangle'$ 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 $G = \mathrm{Isom}(X)^\circ$ and $K = \mathrm{Stab}_G(p)$. 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 $\mathrm{Isom}(X)$ 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 $g\colon \mathfrak{H}^2 \to \mathfrak{H}^2$ 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 $G = \mathrm{Isom}(X)$.

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 $\mathrm{Isom}(M)$ 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 $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, 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 $\operatorname{Im}\gamma(p) \leq \operatorname{Im} p$ for all $\gamma \in \Gamma$, and $-1/2 \leq \operatorname{Re} p \leq 1/2$, then $p \in \mathcal{F}$.]

1:29) Let $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, 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 $\operatorname{Im} w \leq z$. 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 $w = -1/z$.]

Chapter 2

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 $-\mathrm{Id}$ 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.** $\operatorname{rank}(X)$ 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 $G = \operatorname{Isom}(X)^\circ$. 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 $\mathrm{SL}(\ell, \mathbb{R})$, 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.** $\mathbb{R}$-$\operatorname{rank}(G)$ *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 $\mathbb{R}$-$\operatorname{rank}(G) = 0$. 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:

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

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 $\mathbb{R}\text{-rank}(G) = \operatorname{rank}(X)$ 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 set of unit tangent vectors of X if and only if $\mathbb{R}\text{-rank}(G) = 1$.*

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

Proof. For $G = \mathrm{SO}(1, n)$, we have $X = \mathfrak{H}^n$. The stabilizer $\mathrm{SO}(n)$ 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. □

More generally, $\mathbb{R}\text{-rank}\big(\mathrm{SO}(m, n)\big) = \min\{m, n\}$. Also, $\mathbb{R}\text{-rank}\big(\mathrm{SL}(n, \mathbb{R})\big) = n - 1$. 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 $\mathbb{R}\text{-rank}(G) = 1$.*

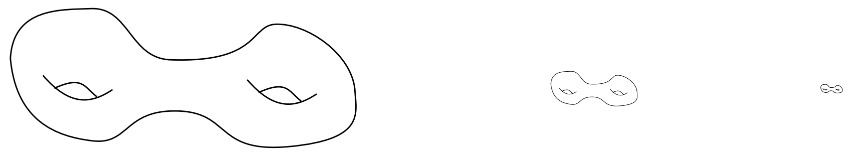

Figure 2.1. Looking at a compact manifold from farther and farther away.

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 largest natural number r, such that $\Gamma\backslash X$ contains a closed, simply connected, r-dimensional flat.*

(2.11) **Remark.** Clearly, we have $0 \le \mathbb{Q}\text{-rank}(\Gamma) \le \mathbb{R}\text{-rank}(G)$. The extreme values are always attained: there are lattices Γ_c and Γ_s in G with $\mathbb{Q}\text{-rank}(\Gamma_c) = 0$ and $\mathbb{Q}\text{-rank}(\Gamma_c) = \mathbb{R}\text{-rank}(G)$. So it is perhaps surprising that there may be gaps in between (see 9.18).

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

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

and

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

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.

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

More generally, $\mathbb{Q}$-rank(Γ) is the unique 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. This 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.

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

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

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).)

(2.15) **Example.**

- 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 $\mathbb{Q}\text{-rank}(\Gamma) = 0$.

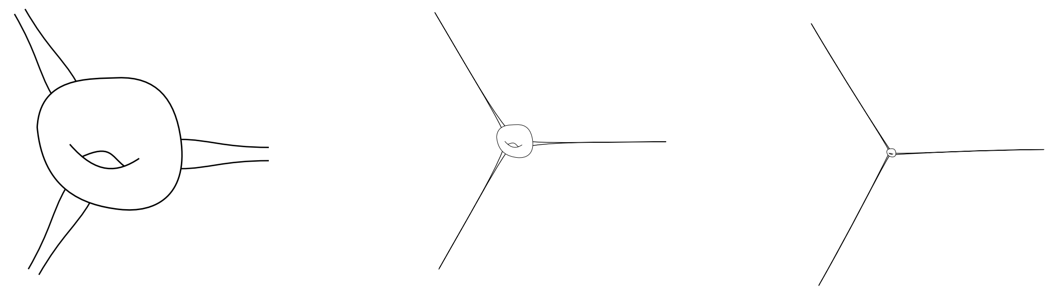

Figure 2.2. Looking at a manifold with cusps from farther and farther away.

- 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 $\mathbb{Q}\text{-rank}(\Gamma) = 1$.

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

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 $\mathbb{Q}\text{-rank}(\Gamma)$.

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

2C. Notes

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

If Γ is arithmetic, Theorem 2.13 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. 2.16 (providing a more precise description of the geometry of the simplicial complex) was proved by Hattori [Hat]. Theorem 2.17 is due to Borel and Serre [B-S].

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. 2.10, that if $\Gamma\backslash X$ is compact, then $\mathbb{Q}\text{-rank}(\Gamma) = 0$.

Chapter 3

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', Γ_1, Γ_2, Γ', 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 $\operatorname{Ad} G_1 \cong \operatorname{Ad} G_2$; 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.** $G = \mathrm{SL}(n, \mathbb{R})$ is a simple Lie group. If n is even, then $\{\pm \mathrm{Id}\}$ 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) **Remark.** Some authors would say that $\mathrm{SL}(n, \mathbb{R})$ 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 $\operatorname{Rad} H$. Our statement of Thm. 3.8 is equivalent to the more usual statement that H is semisimple if and only if $\operatorname{Rad} H$ 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 $\mathrm{SL}(\ell, \mathbb{R})$, for some ℓ.

The following result makes it easy to see that the classical groups, such as $\mathrm{SL}(n, \mathbb{R})$, $\mathrm{SO}(m, n)$, and $\mathrm{SU}(m, n)$, 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 $1 \le k \le n-1$.

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 $w\colon A \to \mathbb{C}^\times$, 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 $\big(h(w)\big)(a) = w(h^{-1}ah)$. 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. □

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. □

(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. 3.21 and 3.22 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. Note that we do not require a form to be positive-definite in order to be called "Hermitian."

(3.20) **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.

(3.21) **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.

(3.22) **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 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 involution on $\mathbb{H}$ defined by
$$\tau_r(a_0 + a_1 i + a_2 j + a_3 k) = a_0 + a_1 i - a_2 j + a_3 k.$$
   (The involution τ_r compensates for the noncommutativity of $\mathbb{H}$ (see Exer. 3:25); note that $\tau_r(ab) = \tau_r(b)\,\tau_r(a)$ (see Exer. 3:23).)

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 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 $\mathrm{Sp}(0,n)$).

(3.23) **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 3.29(1b)); and $\mathrm{Sp}(1,1)$ is isogenous to $\mathrm{SO}(1,4)$ (see 3.29(2b)), which contains $\mathrm{SO}(1,2)$.

(3.24) **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 3.29(1b)).) A complete list of these redundancies is given in §3E below.

(3.25) **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:

(3.26) **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?

(3.27) **Notation.** For reasons that will be more clear later (see Prop. 3.33 and Chap. 24), 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 $n \ge 1$. 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 4^{th} group of type F_4 is the only exceptional group that will play any role in this book (cf. 8.25).

(3.28) **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 $\mathrm{SO}(\ell)$ has an outer automorphism (cf. Exer. 3:27).

(3.29) **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 $\mathrm{SO}(5,\mathbb{C})$.
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);

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	$\mathrm{SU}(n+1)$	$2n^2+4n$
	$\mathrm{SL}\big(\frac{n+1}{2},\mathbb{H}\big)$	n odd	$(n-1)/2$	$\mathrm{Sp}\big((n+1)/2\big)$	n^2+2n
	$\mathrm{SU}(p,q)$	$p+q=n+1$	$\min\{p,q\}$	$\mathrm{S}\big(\mathrm{U}(p)\times\mathrm{U}(q)\big)$	n^2+2n
B_n	$\mathrm{SO}(p,q)$	$p+q=2n+1$	$\min\{p,q\}$	$\mathrm{S}\big(\mathrm{O}(p)\times\mathrm{O}(q)\big)$	$2n^2+n$
	$\mathrm{SO}(2n+1,\mathbb{C})$		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	$\mathrm{SO}(p,q)$	$p+q=2n$	$\min\{p,q\}$	$\mathrm{S}\big(\mathrm{O}(p)\times\mathrm{O}(q)\big)$	$2n^2-n$
	$\mathrm{SO}(2n,\mathbb{C})$		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 $n \ge 1$).

(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 $\mathrm{SU}(1,3)$.

Groups of type D_1 are abelian, not semisimple. Furthermore, we see, from Rem. 3.29, that the types B_1, C_1, C_2, D_1, D_2, and D_3 are redundant. Thus, we have the following proposition.

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

1) *A_n, with $n \ge 1$; or*
2) *B_n, with $n \ge 2$; or*
3) *C_n, with $n \ge 3$; or*
4) *D_n, with $n \ge 4$; or*
5) *E_6, E_7, E_8, F_4, or G_2.*

type	complex group	restriction on n
A_n	$\mathrm{SL}(n+1,\mathbb{C})$	$n \ge 1$
B_n	$\mathrm{SO}(2n+1,\mathbb{C})$	$n \ge 2$
C_n	$\mathrm{Sp}(2n,\mathbb{C})$	$n \ge 3$
D_n	$\mathrm{SO}(2n,\mathbb{C})$	$n \ge 4$
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.

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

(3.31) **Proposition.** *Under the restrictions on n given in Prop. 3.30, 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.

(3.32) **Notation.** As will be explained in Sect. 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
- $\mathrm{SL}(n,\mathbb{C}) \otimes \mathbb{C} = \mathrm{SL}(n,\mathbb{C}) \times \mathrm{SL}(n,\mathbb{C})$.

(3.33) **Proposition.** *Two simple Lie groups G_1 and G_2 are of the same type* (*under the restrictions on n given in Prop. 3.30*) *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. 24.1).) 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. 3.29.

(3.34) **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. 3.30*).

Proof of Prop. 3.31. Suppose G_1 and G_2 are two of the groups listed in Fig. 3.1, with the restrictions on n given in Prop. 3.30. Assume that G_1 is isogenous to G_2.

From Cor. 3.34, 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 $p \le q$ (see (4), (5), and (6) of Prop. 3.31).

Case 1. Assume G_1 and G_2 are of type A_n, for some $n \ge 1$. 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 $G_1 = \mathrm{SL}\big(\frac{n+1}{2}, \mathbb{H}\big)$ (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 $1 \le p \le q$. Now the maximal compact subgroup of G_1 is $\mathrm{Sp}(n)$, which is simple, but the maximal compact subgroup of G_2 is

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

which is not simple. This is a contradiction.

Case 2. Assume G_1 and G_2 are of type B_n, for some $n \ge 2$. 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 $n \ge 3$. 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 $n \ge 4$. 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. 3.34 implies that $n - 1 \le 3$, so $n = 4$. (Recall that, by assumption, we have $n \ge 4$.) Hence, Conclusion 3.31(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 the classical groups.

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. 3.26 and Props. 3.30 and 3.31) 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. 3.29 and Prop. 3.31 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 $\mathrm{SO}(p,q)$ are connected. For a geometric proof of 3.29(2c), see [Hel2, §10.A.2, p. 521].

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 $\phi\colon G \to A$ 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 $\{1,\ldots,r\}$, 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
$$\mathrm{SU}(B;\mathbb{H},\tau_c) = \{\, g \in \mathrm{SL}(\ell,\mathbb{H}) \mid \tau_c(g^T) B g = B \,\}.$$
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 $m \le n$, and let $\pi \colon \mathbb{R}^{m+n} \to \mathbb{R}^m$ 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 $f(g) = \det\bigl(\pi \circ g \circ (\pi|_L)^{-1}\bigr)$ 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. 3.22, 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 $g, h \in \mathrm{SL}(n,\mathbb{H})$, show that $\tau_r\big((gh)^T\big) = \tau_r(h^T)\,\tau_r(g^T)$.

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 $\phi_g \colon \mathrm{SO}(\ell) \to \mathrm{SO}(\ell)$, 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 $T_g \colon \mathbb{H} \to \mathbb{H}$ by $T_g(x) = xg^{-1}$; then, after identifying $\mathbb{H}$ with $\mathbb{C}^2$, the linear map T_g is unitary. Let

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

For $g \in \mathbb{H}^*$, define $S_g \colon V \to V$ 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 isomorphic to $\mathrm{SL}(2,\mathbb{R})$. [*Hint:* For the usual action of $\mathrm{SL}(2,\mathbb{C})$ on $\mathbb{C} \cup \{\infty\}$ by linear-fractional transformations, we have

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

and

$$\mathrm{SU}(1,1) = \{\, g \in \mathrm{SL}(2,\mathbb{C}) \mid g(\mathbb{T}) = \mathbb{T} \,\}$$

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

3:31) Show that $\mathrm{SL}(2,\mathbb{R})$ is isogenous to $\mathrm{SO}(1,2)$. [*Hint:* The Killing form $K(A,B) = \operatorname{trace}(AB)$ 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 3.29(1a) or 3.29(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 $T_{g,h} \colon \mathbb{H} \to \mathbb{H}$ by $T_{g,h}(x) = gxh^{-1}$; 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 $T_g(v) = gvg^*$. 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 $(g,h,T) \mapsto gTh^{-1}$ 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 3.29(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 $\phi \colon \mathbb{C} \to \mathbb{H}$ be the embedding defined by $\phi(i) = j$. Then $\mathrm{SO}(2,\mathbb{H})$ contains

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

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

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

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

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

Chapter 4

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 $\mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}]$ to denote the set of real polynomials in the ℓ^2 variables $\{\, x_{i,j} \mid 1 \le i,j \le \ell \,\}$.
- For any $Q \in \mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}]$, and any $g \in \operatorname{Mat}_{\ell\times\ell}(\mathbb{C})$, 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 $\mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}]$, let

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

  This is the *variety* associated to $\mathcal{Q}$.
- A subset H of $\operatorname{SL}(\ell,\mathbb{R})$ is *Zariski closed* if there is a subset $\mathcal{Q}$ of $\mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}]$, such that $H = \operatorname{Var}(\mathcal{Q})$. (In the special case where H is a sub*group* of $\operatorname{SL}(\ell,\mathbb{R})$, 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 $\operatorname{SL}(\ell,\mathbb{R})$ is the (unique) smallest Zariski closed subset of $\operatorname{SL}(\ell,\mathbb{R})$ that contains H. The Zariski closure is sometimes denoted $\overline{H}$.

(4.2) **Example.** 1) $\operatorname{SL}(\ell,\mathbb{R})$ is Zariski closed. Let $\mathcal{Q} = \emptyset$.

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

3) For any $A \in \mathrm{GL}(\ell, \mathbb{R})$, the centralizer of A is Zariski closed. Let
$$\mathcal{Q} = \left\{ \sum_{k=1}^{\ell} (x_{i,k} A_{k,j} - A_{i,k} x_{k,j}) \;\middle|\; 1 \le i, j \le \ell \right\}.$$

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. 3.21 and 3.22 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
$$H = \left\{ \begin{pmatrix} e^{2t} & 0 & 0 \\ 0 & e^{-t} & t \\ 0 & 0 & e^{-t} \end{pmatrix} \;\middle|\; t \in \mathbb{R} \right\} \subset \mathrm{SL}(3, \mathbb{R}).$$
Then H is a 1-dimensional subgroup that is not Zariski closed. Its Zariski closure is
$$\overline{H} = \left\{ \begin{pmatrix} a^2 & 0 & 0 \\ 0 & 1/a & t \\ 0 & 0 & 1/a \end{pmatrix} \;\middle|\; \begin{array}{c} a \in \mathbb{R} \smallsetminus \{0\}, \\ t \in \mathbb{R} \end{array} \right\} \subset \mathrm{SL}(3, \mathbb{R}).$$
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 $\mathbb{R}[x_{1,1}, \ldots, x_{\ell,\ell}]$ 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. 4:2).

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. 4:4). 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)). □

(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) **Warning.**
- 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 $\mathrm{Ad}\, h$ is a hyperbolic element of $\mathrm{SL}(\mathfrak{g})$, 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 $\operatorname{Ad} h$ is a unipotent element of $\operatorname{SL}(\mathfrak{g})$, 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 $\rho\colon G \to \operatorname{SL}(n,\mathbb{R})$ be any 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 $G = \operatorname{SL}(2,\mathbb{R})$ 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 $a^{-n} g a^n \to \operatorname{Id}$, so $\rho(a)^{-n}\rho(g)\rho(a)^n \to \operatorname{Id}$. 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. □

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 $\operatorname{SL}(2,\mathbb{R})$, such that $u \in H$.*

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

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 $K \times A \times N \to G$ 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.** A *Cartan involution* of G is an involution σ of G, such that

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

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

$$P = \left\{ g \in G \;\middle|\; \limsup_{n\to\infty} \|a^{-n} g a^{n}\| < \infty \right\}.$$

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

(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 $\langle \cdot \mid \cdot \rangle_{\mathbb{R}^{m,n}}$ 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 nondegenerate, symmetric, bilinear form on a finite-dimensional vector space V over any field F of characteristic 0. 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*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{4.36}$$

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

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

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 $\mathcal{B} = \{u,v\} \cup \mathcal{B}'$. □

(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*
- *$\sigma\colon W_1 \to W_2$ is any linear map, such that $B\big(\sigma(v),\sigma(w)\big) = B(v,w)$, 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

$$N = \left\{ g \in G \;\middle|\; \lim_{n\to\infty} a^{-n} g a^n = e \right\}.$$

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

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

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

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

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.)

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

(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 $\mathrm{Aut}(G)$, denoted $\mathrm{Inn}(G)$.
- The *outer automorphism group* of G is $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

(4.52) **Corollary.** 1) $\mathrm{Out}(G)$ *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 $\mathrm{SO}(p,q)$ has two components if $\min\{p,q\} \geq 1$ (see Exers. 3:20 and 4:12). Also, each of these groups is simple, except $\mathrm{SO}(4)$, $\mathrm{SO}(2,2)$, $\mathrm{SO}(4,\mathbb{C})$, and $\mathrm{SO}(2,\mathbb{H})$ (see 3.29(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)!!!

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

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

If a rational function $f \colon \mathbb{R} \smallsetminus \{0\} \to \mathbb{R}$ vanishes on $\mathbb{R}^+$, then it also vanishes on $\mathbb{R}^-$.]

4:3) Show, for any subspace V of $\mathbb{R}^\ell$, that

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

is Zariski closed.

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

4:5) A Zariski-closed subset of $\mathrm{SL}(\ell,\mathbb{R})$ is *irreducible* if it cannot be written as the union of two Zariski-closed, proper subsets. Show that every Zariski-closed subset A of $\mathrm{SL}(\ell,\mathbb{R})$ 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 $\mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}]$ 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.]

4:6) Let H be a connected subgroup of $\mathrm{SL}(\ell,\mathbb{R})$. Show that if $H \subset A_1 \cup A_2$, where A_1 and A_2 are Zariski-closed subsets of $\mathrm{SL}(\ell,\mathbb{R})$, then either $H \subset A_1$ or $H \subset A_2$. [*Hint:* The Zariski closure $\overline{H} = B_1 \cup \cdots \cup B_r$ is an irredundant union of irreducible, Zariski-closed subsets (see Exer. 4:5). For $h \in H$, we have $\overline{H} = hB_1 \cup \cdots \cup hB_r$, so uniqueness implies that h acts as a permutation of $\{B_j\}$. Because H is connected, conclude that $\overline{H} = B_1$ is irreducible.]

4:7) Show that:
  (a) Id is the only element of $\mathrm{GL}(\ell,\mathbb{R})$ that is both semisimple and unipotent; and
  (b) Id is the only element of $\mathrm{GL}(\ell,\mathbb{R})$ that is both hyperbolic and elliptic.

4:8) Show (without using Prop. 4.14) that the Jordan decomposition $g = aku$ is unique, if it exists.

4:9) Show that if $g \in \mathrm{GL}(\ell,F)$, for some subfield F of $\mathbb{C}$, and $g = aku$ is the Jordan decomposition of g, then $a,k,u \in \mathrm{GL}(\ell,F)$. [*Hint:* For any Galois automorphism of $\mathbb{C}$ over F, uniqueness of the Jordan decomposition implies that $\sigma(a) = a$, $\sigma(k) = k$, and $\sigma(u) = u$.]

4:10) 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:* $h^{-1}gh = (h^{-1}ah)(h^{-1}kh)(h^{-1}uh)$.]

4:11) This exercise constructs a simple Lie group that has finite center, but is not linear. Let $G = \mathrm{SL}(2,\mathbb{R})$.
   (a) Show that $\mathrm{SL}(2,\mathbb{C})$ 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 $\mathrm{SO}(2) \times \mathbb{R}^2$.]
   (c) Show that G has a (unique) cover G_k of any degree k.
   (d) Show that if $\rho\colon G_k \to \mathrm{SL}(n,\mathbb{R})$ is any finite-dimensional representation of G_k, then there is a homomorphism $\sigma_{\mathbb{C}}\colon \mathrm{SL}(2,\mathbb{C}) \to \mathrm{SL}(n,\mathbb{C})$, such that $\sigma_{\mathbb{C}} \circ \pi = \rho$, where $\pi\colon G_k \to G$ is the covering map. [*Hint:* By complexifying $d\rho$, we obtain a Lie algebra homomorphism $d\rho_{\mathbb{C}}\colon \mathfrak{sl}(2,\mathbb{C}) \to \mathfrak{sl}(n,\mathbb{C})$. Now use the fact that $\mathrm{SL}(2,\mathbb{C})$ is simply connected.]
   (e) Show $\ker\pi \subset \ker\rho$.
   (f) Show that if $k > 1$, then G_k is not linear.

4:12) Show that $\mathrm{SO}(m,n)$ is not connected if $m,n > 0$. [*Hint:* The maximal compact subgroup is not connected.]

4:13) Prove ($\Leftarrow$) of Prop. 4.48.

4:14) Use Prop. 4.48 to show that $\mathrm{SL}(n,\mathbb{R})$ is connected.

Chapter 5

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 $\mathcal{F} \to \Lambda\backslash G$ 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 $\cup_{n=1}^{\infty} U g_n = G$. Let

$$\mathcal{F} = \bigcup_{n=1}^{\infty} \left(U g_n \smallsetminus \bigcup_{i<n} \Lambda U g_i \right).$$

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

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

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

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

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 $\phi\colon G \to \Lambda\backslash G$ 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 $\nu\big(\phi(A)\big) = \mu(A)$.*

(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 no 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 $\nu(\Lambda \backslash A h^{-1}) = \Delta(h)\, \nu(\Lambda \backslash A)$ (see Exer. 5:11). Since $H = Hh^{-1}$, this implies that
$$\nu(\Lambda \backslash H) = \nu(\Lambda \backslash H h^{-1}) = \Delta(h)\, \nu(\Lambda \backslash H).$$
Since $\Lambda \backslash H$ has finite volume, we conclude that $\Delta(h) = 1$, as desired. □

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
$$\mathrm{Comm}_G(\Gamma) = \{\, g \in G \mid g \text{ commensurates } \Gamma \,\}.$$
This is called the *commensurater* of Γ (or the *commensurability subgroup* of Γ).

(5.20) **Remark.** The commensurater of Γ may be much larger than the normalizer of Γ. For example, let $G = \mathrm{SL}(n, \mathbb{R})$ and $\Gamma = \mathrm{SL}(n, \mathbb{Z})$. Then $N_G(\Gamma)$ is commensurable with Γ (see 5.43), but $\mathrm{SL}(n, \mathbb{Q}) \subset \mathrm{Comm}_G(\Gamma)$ (see Exer. 5:13), so $\mathrm{Comm}_G(\Gamma)$ 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 $G = \mathrm{SO}(1, n)$, then it is known that there are examples in which Γ, $N_G(\Gamma)$, and $\mathrm{Comm}_G(\Gamma)$ are commensurable with each other (see Exer. 6:7 and §7E).

(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) **Warning.** 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 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. 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. □

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 $\Gamma_1\backslash X_1, \ldots, \Gamma_r\backslash X_r$, 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. 6.43 that $\mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{R})$ has an irreducible lattice (for example, a lattice isomorphic to $\mathrm{SL}\big(2,\mathbb{Z}[\sqrt{2}]\big)$). More generally, Thm. 6.25 shows that if all the simple factors of G are of the same type (see 3.27), 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* a Riemannian manifold X is the the maximal (or, actually, supremal) $r \geq 0$, such that, for every $x \in X$, the exponential map is a diffeomorphism on the 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 $\phi_g \colon G \to \Gamma\backslash G$ by $\phi_g(x) = \Gamma g x$. 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 $\phi \colon G \to \Gamma\backslash G$ 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

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

Thus, by induction on n, we may choose a sequence $\{g_n\}$ of elements of G, such that the open sets $\phi_{g_1}(U), \phi_{g_2}(U), \ldots$ 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

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

(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

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

□

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 $\phi\colon \operatorname{SL}(2,\mathbb{R}) \to G$ with

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

Let

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

Then

$$a^{-n} u a^n = \phi\left(\begin{pmatrix} 2^{-n} & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^n & 0 \\ 0 & 2^{-n} \end{pmatrix} \right) = \phi\begin{pmatrix} 1 & 2^{-2n} \\ 0 & 1 \end{pmatrix} \to \phi\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e.$$

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 §15D). 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 $G = \operatorname{SL}(\ell,\mathbb{R})$ and $\Gamma = \operatorname{SL}(\ell,\mathbb{Z})$, without relying on the fact that $\operatorname{SL}(\ell,\mathbb{Z})$ 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)**.** *Let $C \subset \operatorname{SL}(\ell,\mathbb{R})$. The image of C in $\operatorname{SL}(\ell,\mathbb{R})/\operatorname{SL}(\ell,\mathbb{Z})$ 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 $\operatorname{SL}(\ell,\mathbb{R})/\operatorname{SL}(\ell,\mathbb{Z})$ is precompact, there is a compact subset C_0 of G, such that $C \subset C_0 \operatorname{SL}(\ell,\mathbb{Z})$ (see Exer. 5:8). By enlarging C, we may assume that $C = C_0 \operatorname{SL}(\ell,\mathbb{Z})$. Then $C\big(\mathbb{Z}^\ell \smallsetminus \{0\}\big) = C_0\big(\mathbb{Z}^\ell \smallsetminus \{0\}\big)$ is closed (since $\mathbb{Z}^\ell \smallsetminus \{0\}$, being discrete, is closed and C_0 is compact), so $C\big(\mathbb{Z}^\ell \smallsetminus \{0\}\big)$ contains all of its accumulation points. In addition, since 0 is fixed by every element of C, we know that $0 \notin C(\mathbb{Z}^\ell \smallsetminus \{0\})$. Therefore, 0 is not an accumulation point of $C(\mathbb{Z}^\ell \smallsetminus \{0\})$.

($\Leftarrow$) 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

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

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

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

so

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

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

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

Note that

$$\|\pi_n^\perp(g_n w_n)\| \, \|g_n v_n\| = \det g_n = 1. \tag{5.36}$$

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 $\|g_n v_n\| \to \|v\|$ 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 $\|\pi_n^\perp(g_n w_n)\| \not\to 0$, 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

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

and, similarly, $g_n(0,1) \to g(0,1)$, so $g_n x \to gx$ for all $x \in \mathbb{R}^2$. Thus, $g_n \to g$, 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. □

(5.38) **Corollary.** *Let N be a closed, normal subgroup of G. The intersection $\Gamma \cap N$ is a lattice in N if and only if $N\Gamma$ is closed in G.*

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

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

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*

- *G has no compact factors;*
- *V is a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$; and*
- *$\rho\colon G \to \mathrm{GL}(V)$ 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 $\mathbb{R}^\times$ (or $\mathbb{C}^\times$) , so we conclude that v is $\rho(G)$-invariant.

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

(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. □

(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 $\rho(g)v = gvg^{-1}$, so $\rho\colon G \to \mathrm{GL}(V)$ 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 $c \in Z(G)$. □

(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 $\operatorname{Aut}(N)$, so $C_\Gamma(N)$ is a lattice in G (see 5.12(2)). Then, because $N \subset C_G\bigl(C_\Gamma(N)\bigr)$, Cor. 5.41 implies $N \subset Z(G)$. □

(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). □

(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 $Q \in \mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}]$ is a polynomial function on $\operatorname{Mat}_{\ell\times\ell}(\mathbb{R})$, such that $Q(\Gamma)=0$, then $Q(G)=0$.*

Proof. Let
$$\mathcal{Q} = \{\, Q \in \mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}] \mid Q(\Gamma) = 0 \,\}.$$
By definition, we have $\Gamma \subset \operatorname{Var}(\mathcal{Q})$ (see Defn. 4.1). Since $\operatorname{Var}(\mathcal{Q})$ has only finitely many connected components (see 4.5), this implies that $\operatorname{Var}(\mathcal{Q})^\circ$ is a connected subgroup of G that contains a finite-index subgroup of Γ. Hence Cor. 5.40 implies that $\operatorname{Var}(\mathcal{Q})^\circ = G$ (see Exer. 5:30), so $G \subset \operatorname{Var}(\mathcal{Q})$, as desired. □

5G. Proof of the Borel Density Theorem

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

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

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

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 $\operatorname{diam}(B) < \epsilon$. Because the sets $B, T^{-1}B, T^{-2}B, \ldots$ 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
$$d(T^m a, a) \le \operatorname{diam}(B) < \epsilon.$$
This contradicts the definition of A_ϵ. □

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

- *G has no compact factors;*
- *V is a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$;*
- *$\rho\colon G \to \mathrm{GL}(V)$ 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 $v \in V \smallsetminus \{0\}$. 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

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

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

The Poincaré Recurrence Theorem (5.45) implies, for μ-almost every $[v] \in \mathbb{P}(V)$, that there is a sequence $n_k \to \infty$, such that $\rho(u^{n_k})[v] \to [v]$. 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. □

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 $\mathbb{C}$;*
- *$\rho\colon G \to \mathrm{GL}(V)$ 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 $\rho|_{G'}$. □

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

- *V is a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$;*
- *$\rho\colon G \to \mathrm{GL}(V)$ 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 $\hat{\rho}\colon G \to \mathrm{GL}(\bigwedge^d V)$. Because $\hat{\rho}(H)$ fixes $\bigwedge^d W$, $\hat{\rho}$ induces a G-equivariant map $\hat\rho'\colon G/H \to \mathbb{P}(\bigwedge^d V)$ 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. 5:35). 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 $\rho(G)$. □

(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 $\operatorname{Ad}_G(H)$, we conclude from Cor. 5.48 that it is invariant under $\operatorname{Ad} G$. Therefore H° is normal in G. □

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 $\langle S\rangle = \mathcal{F}$.

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 $\lambda \in s_1^{-1}s_2S \subset \langle S\rangle$. So

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

This is a contradiction. □

(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. □

(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. 5:44).

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

$$\mathbb{Z}^2 = \langle x_1, x_2, x_3 \mid x_1x_2 = x_3, x_2x_1 = x_3\rangle.$$

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

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

and the kernel of ϕ is the smallest normal subgroup of F_3 that contains both $x_1x_2x_3^{-1}$ and $x_2x_1x_3^{-1}$.) 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 $\phi\colon F \to \Lambda$ 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. 5:45).
- Let $\widetilde{Y}$ be the quotient space $\big((F/N) \times \mathcal{F}\big)/\sim$.
- Define a map $\psi\colon (F/N) \times \mathcal{F} \to Y$ by $\psi(fN, y) = \phi(f^{-1})y$. (Note that, because $N \subset \ker(\phi)$, the map ψ is well defined.)

Because

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

we see that ψ factors through to a well-defined map $\widetilde{\psi}\colon \widetilde{Y} \to Y$.

Let $\widetilde{\mathcal{F}}$ be the image of $\big(\ker(\phi)/N\big) \times \mathcal{F}$ in $\widetilde{Y}$. Then it is obvious, from the definition of ψ, that $\widetilde{\psi}(\widetilde{\mathcal{F}}) = \mathcal{F}$. In fact, it is not difficult to see that $\widetilde{\psi}^{-1}(\mathcal{F}) = \widetilde{\mathcal{F}}$ (see Exer. 5:46).

For each $f \in F$, the image $\mathcal{F}_f$ of $(fN) \times \mathcal{F}$ in $\tilde{Y}$ is open (see Exer. 5:47), 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. 5:48). Thus, from the preceding paragraph, we see that $\widetilde{\psi}$ is a covering map over $\mathcal{F}$. Since Y is covered by translates of $\mathcal{F}$, it follows that $\widetilde{\psi}$ 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 $\widetilde{Y}$ is connected (see Exer. 5:49). Since Y is simply connected, and $\widetilde{\psi}$ is a covering map, this implies that $\widetilde{\psi}$ is a homeomorphism. Hence, the degree of the cover is 1, so $|\ker(\phi)/N| = 1$. This means $\ker(\phi) = N$, as desired. □

(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. □

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. 13.)

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

The (amazing!) Margulis Arithmeticity Theorem (6.20) implies that these two cases are exhaustive, which completes the proof. □

(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) implies that Γ is finitely generated (see 17.17(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 $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ induces a group homomorphism $\Gamma \to \mathrm{SL}(n, \mathbb{Z}/n\mathbb{Z})$ (see Exer. 5:37); 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. 5:38c and 5:39). 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 $\gamma \in \Gamma_n \smallsetminus \{\mathrm{Id}\}$ and $k \in \mathbb{N} \smallsetminus \{0\}$, 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. 5:40). 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. 5:41).)

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 $a_1, \ldots, a_r \in \mathbb{C}$, such that every matrix entry of every element of Γ is contained in the ring $Z = \mathbb{Z}[a_1, \ldots, a_r]$ generated by $\{a_1, \ldots, a_r\}$ (see Exer. 5:42). 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 $\Lambda \to \mathrm{SL}(\ell, Z/\mathfrak{p})$ 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. □

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 F.

Because Γ is a finitely generated group (see 5.57), we know that Z is a finitely generated ring (see Exer. 5:42), so F is a finitely generated extension of $\mathbb{Q}$.

Step 1. We may assume that $F = \mathbb{Q}(x_1, \ldots, x_r)$ is a purely transcendental extension of $\mathbb{Q}$. Choose a subfield $L = \mathbb{Q}(x_1, \ldots, x_r)$ 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.49), we know that there is a nontrivial homomorphism $\phi\colon Z \to \overline{\mathbb{Q}}$, 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 $\phi_p\colon Z \to E$. 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.48), so E is finite.

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

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

so $p \mid \big(\ell - \mathrm{trace}(\gamma)\big)$. 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. □

If $\gamma^k = \mathrm{Id}$, then every eigenvalue of γ must be a k^{th} root of unity. If, in addition, $\gamma \neq \mathrm{Id}$, 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 $\Gamma = \mathrm{SL}(\ell, \mathbb{Z})$. 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,
- $T = \gamma - \mathrm{Id}$,
- $Q(x)$ 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. 5:50 for a slightly different argument. □

(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 $\mathrm{SL}(\ell, F)$ 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, it is often the case that every normal subgroup of Γ has finite index (see §23A). Moreover, 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 §23C).

(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 $\mathrm{SL}(\ell, \mathbb{R})$, then either*

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

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.*

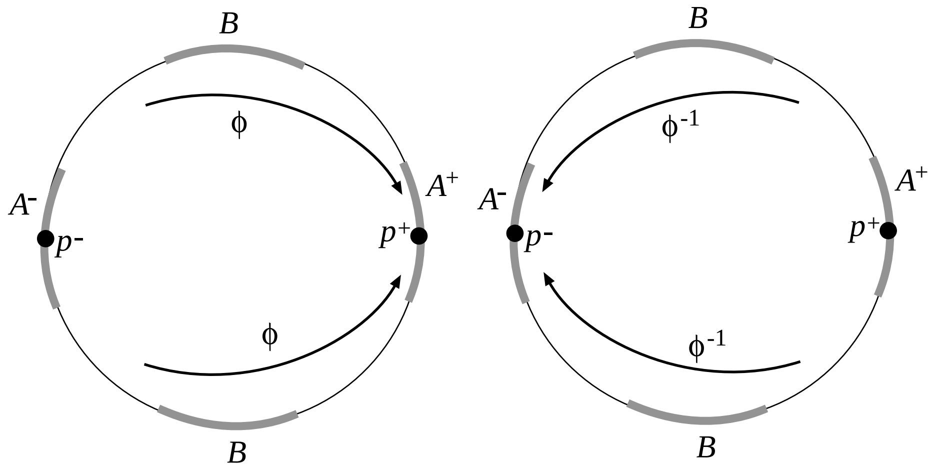

Figure 5.1. A typical (A^-, B, A^+)-contracting homeomorphism on the circle.

(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 $\mathbb{P}(\mathbb{R}^2)$,
- $\gamma = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R})$,
- 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 $\mathbb{P}(\mathbb{R}^2) \smallsetminus \{p^-, p^+\}$.

For any $(x, y) \in \mathbb{R}^2$ with $x \neq 0$, we have

$$\gamma^n[x : y] = [2^n x : 2^{-n} y] = [1 : 2^{-2n} y/x] \to [1 : 0] = p^+$$

as $n \to \infty$, and the convergence is uniform on compact subsets. Similarly, $\gamma^{-n}[x : y] \to p^-$ as $n \to \infty$. 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 $\mathrm{SL}(2, \mathbb{R})$, 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. 5:51).

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

$$\phi^{m_j}(B) \subset A \qquad \text{and} \qquad \psi^{n_j}(A) \subset B, \qquad \text{for } j = 1, 2, \dots, k.$$

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. □

(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. 5:51). Thus, the Ping-Pong Lemma (5.69) implies that $\langle (\gamma_1)^n, (\gamma_2)^n \rangle$ is free. □

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. 5:29), 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. 5:52). 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 $n \in \mathbb{Z}^+$. □

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 $x \in \mathbb{R}^\ell \smallsetminus v^\perp$, we have $(\gamma_1)^n[x] \to [v]$ in $\mathbb{P}(\mathbb{R}^\ell)$, as $n \to \infty$ (see Exer. 5:53). Similarly, if $x \notin w^\perp$, then $(\gamma_1)^{-n}[x] \to [w]$.

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. □

(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, including 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 [Mar4], [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 $\mathbb{Q}\text{-rank}\,\Gamma = 1$, 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 [Alp].

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].

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 $a = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1/2 \end{pmatrix} \in H$. Show that $\Lambda a^n \to \infty$ in $\Lambda\backslash H$ as $n \to \infty$. 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 $u_{1,n}, \ldots, u_{\ell,n} \in \mathbb{Z}^\ell$.]

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) 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 $\operatorname{End}(V)$. Show that $V[\Gamma] = V[G]$.

5:29) 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 $(x-1)^\ell = 0$.]

5:30) 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 $H = G$.

5:31) 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.

5:32) 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.]

5:33) 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 $\phi \colon F \to \mathrm{SO}(3)$, such that $\phi(F)$ is dense in $\mathrm{SO}(3)$.]

5:34) 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.

5:35) 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.]

5:36) 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 $\operatorname{Isom}(M)$ is finite.

5:37) 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 $\phi \colon A \to B$ (with $\phi(1) = 1$), there is a corresponding group homomorphism $\phi_* \colon \mathrm{SL}(\ell, A) \to \mathrm{SL}(\ell, B)$; and
   (c) if $\phi \colon A \to B$ and $\psi \colon B \to C$ are ring homomorphisms (with $\phi(1) = 1$ and $\psi(1) = 1$), then $(\psi \circ \phi)_* = \psi_* \circ \phi_*$.

5:38) Suppose A and B are rings with identity, $\phi \colon A \to B$ is a ring homomorphism (with $\phi(1) = 1$), and I is an ideal of B. Show, in the notation of Exer. 5:37, 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) $(\phi_*)^{-1}\big(\mathrm{SL}(\ell, 1+I)\big)$ is a normal subgroup of $\mathrm{SL}(\ell, A)$.

5:39) 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 $\mathrm{SL}(\ell, \mathbb{Z})$.

5:40) Show that if Γ has a nontrivial element of finite order, then Γ has an element of prime order.

5:41) 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?

5:42) 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.]

5:43) Show that Γ is residually finite. That is, for every $\gamma \in \Gamma \smallsetminus \{e\}$, 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.)

5:44) 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).

5:45) Show that the relation $\sim$ defined in the proof of Prop. 5.54 is an equivalence relation.

5:46) 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 $\phi(f^{-1}y \in \mathcal{F}$.]

5:47) 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

$$\cup_{s\in S}\big((x_s fN/N)\times(\mathcal{F}\cap s\mathcal{F})\big),$$

which is open.

5:48) 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 $s = \phi(x_s) = \phi(f) = e$.]

5:49) Show that the set $\widetilde{Y}$ defined in the proof of Prop. 5.54 is connected. [*Hint:* For $s_1,\ldots,s_r \in S$, 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 $a \sim b$.]

5:50) 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 $N\colon F\to\mathbb{Q}$ by $N(x)=\prod_{\sigma\in\mathrm{Gal}(F/\mathbb{Q})}\sigma(x)$. Then $N(\omega-1)^\ell = n^d N(\zeta)$, and $|N(\omega-1)| \le 2^d \le 2^{\ell!}$, where d is the degree of F over $\mathbb{Q}$.]

5:51) 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 $\mathbb{P}(\mathbb{R}^2)$.

5:52) Assume that G is irreducible in $\mathrm{SL}(\ell,\mathbb{R})$ (see Defn. 3.12), and that Γ projects densely into the maximal compact factor of G. If F is a finite subset of $\mathbb{R}^\ell \smallsetminus \{0\}$, 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. 4:6.]

5:53) Let

- γ be a hyperbolic element of $\mathrm{SL}(\ell,\mathbb{R})$, with eigenvalues $\lambda_1 > \lambda_2 \ge \cdots \ge \lambda_\ell$,
- v be an eigenvector of γ corresponding to the eigenvalue λ_1, and
- W be the sum of the other eigenspaces.

Show that if $x \in \mathbb{P}(\mathbb{R}^\ell)\smallsetminus[W]$, then $\gamma^n x \to [v]$ as $n\to\infty$. Furthermore, the convergence is uniform on compact subsets.

Chapter 6

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.) 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 $W \cap \mathbb{Z}^n$;*
3) *$W \cap \mathbb{Q}^\ell$ is dense in W;*
4) *$W \cap \mathbb{Z}^n$ 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 $T\colon \mathbb{R}^k \to W$, 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 is defined by the system of equations $x \cdot v_1 = 0, \dots, x \cdot v_m = 0$.

($2 \Rightarrow 4$) There is a linear isomorphism $T\colon \mathbb{R}^k \to W$, 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 $V = W$. □

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 Q* (or that H is a $\mathbb{Q}$*-subgroup*) if there is a subset $\mathcal{Q}$ of $\mathbb{Q}[x_{1,1},\ldots,x_{\ell,\ell}]$, 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
$$\mathcal{Q} = \left\{ \sum_{1\le p,q\le m+n} x_{i,p}A_{p,q}x_{j,q} - A_{i,j} \;\middle|\; 1 \le i,j \le m+n \right\}.$$
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 is 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 $\mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}]$, such that G is commensurable with $\mathrm{Var}(\mathcal{Q})$ (see 4.8); that is, G is *defined over 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 $\mathbb{Q}[x_{1,1},\ldots,x_{\ell,\ell}]$ 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. 3.21 and 3.22 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.29), 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. 12. □

(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 $\phi\colon \mathrm{SL}(n,\mathbb{C}) \to \mathrm{SL}(2n,\mathbb{R})$ be the natural embedding. Then
$$\phi\big(\mathrm{SL}(n,\mathbb{C})\big)_{\mathbb{Q}} = \phi\big(\mathrm{SL}(n,\mathbb{Q}[i])\big).$$
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. 14. 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. 6:3).

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 9.17).

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 $\phi\colon G_1 \to G_2$ 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 $\phi\colon G/K \to G'/K'$,

such that $\phi(\overline{\Gamma})$ is commensurable with $\overline{G'_{\mathbb{Z}}}$, where $\overline{\Gamma}$ and $\overline{G'_{\mathbb{Z}}}$ are the images of Γ and $G'_{\mathbb{Z}}$ in G/K and G'/K', respectively.

If G has no compact factors, then the subgroup K in Defn. 6.16 must be finite. If Γ is irreducible and *not* cocompact, then the subgroup K' may be taken to be trivial:

(6.17) **Proposition.** *If Γ is arithmetic, and $\Gamma\backslash G$ is not compact, 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 homomorphism $\phi\colon G \to G'$, with finite kernel,*

such that $\phi(\Gamma)$ is commensurable with $G'_{\mathbb{Z}}$.

However, if Γ is not cocompact, then a nontrivial (connected) compact group K' may be required (even if G has no compact factors).

(6.18) **Remark.** Up to conjugacy, there are only countably many arithmetic lattices in G, because there are only countably many finite subsets of $\mathbb{Q}[x_{1,1},\ldots,x_{\ell,\ell}]$.

(6.19) **Warning.** Our definition of *arithmetic* is from a Lie theorist's viewpoint, where Γ is assumed to be embedding 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.

(6.20) **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.

(6.21) **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.

(6.22) **Remark.** The conclusion of Thm. 6.20 can be strengthened: the subgroup K of Defn. 6.16 can be taken to be finite.

For any G, it is possible to give a reasonably complete description of the arithmetic lattices in G (up to conjugacy and commensurability): Fig. 10.1 (on p. 124) 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 (as far as I know) the only known proof that every lattice is finitely presented (see 5.57) relies on the fact that if Γ is irreducible and $\mathbb{R}\text{-rank}\, G > 1$, then Γ is arithmetic (see 6.20).

(6.23) **Remark.** It is known that there are nonarithmetic lattices in $\mathrm{SO}(1,n)$ for every n (see §7E), 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 I think it is still not known whether they exist when $n \geq 4$.

(6.24) **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. 3.30.

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.

(6.25) **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. 11 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 (6.20), we know that Γ is arithmetic. Then, since Γ is irreducible, the conclusion follows from the theory of arithmetic groups (see 6.54). 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 6.56), the conclusion follows. □

(6.26) **Remark.** By using Rem. 6.22, one can show that Thm. 6.25 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.

(6.27) **Example.** $\mathrm{SO}(1,2) \times K$ has an irreducible lattice, for any connected, compact Lie group K (cf. Exer. 5:33).

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.

(6.28) **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 (6.20). 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. 16E.

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 (16.14) implies that (ignoring a finite group) every complex representation of Γ extends to a representation of G:

(6.29) **Theorem.** *If $\rho\colon \Gamma \to \mathrm{SL}(\ell,\mathbb{C})$ is any homomorphism, then there is a continuous homomorphism $\hat\rho\colon G \to \mathrm{SL}(\ell,\mathbb{C})$, such that $\rho = \hat\rho$ on a finite-index subgroup of Γ.*

(6.30) **Warning.** The statement of Thm. 6.29 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:

(6.31) **Theorem.** *If $\rho\colon \Gamma \to \mathrm{SL}(\ell,\mathbb{Q}_p)$ 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:

(6.32) **Corollary.** *If $\rho\colon \Gamma \to \mathrm{SL}(\ell,\mathbb{Q})$ 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 $\{p_1,\ldots,p_r\}$ 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 $m_1,\ldots,m_r \in \mathbb{N}$. 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. 6.31. □

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) in Chap. 16, but let us show how to deduce it from superrigidity (Thm. 6.29). 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 $\widetilde{\phi}$ of $\mathrm{SL}(n,\mathbb{C})$. From Thm. 6.29, there is a continuous homomorphism $\hat{\rho}\colon G \to \mathrm{SL}(n,\mathbb{C})$, such that $\hat{\rho} = \widetilde{\phi}$ 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 $\widetilde{\phi}$ 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 $\widetilde{\phi}(\gamma)$ 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 $\rho\colon G \to \mathrm{SL}(\ell,\mathbb{C})$, such that $\rho\big(G \cap \mathrm{SL}(n,F)\big) \subset \mathrm{SL}(\ell,\mathbb{Q})$. 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 $\Gamma \subset \frac{1}{k}\operatorname{Mat}_{n\times n}(\mathbb{Z})$. 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. 6:8).

6E. Unipotent elements of $G_{\mathbb{Z}}$: the Godement Compactness Criterion

(6.33) **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 §15D. On the other hand, the assumption that G has no compact factors cannot be eliminated (see Exer. 6:9).

(6.34) **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. 6.33 relies on the fact that $G_{\mathbb{Z}}$ is a lattice in G. Unfortunately, this basic fact will not be proved until Chap. 14. 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).

(6.35) **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 $\mathbb{Z}^\ell \smallsetminus \{0\}$.

Suppose that $g_n v_n \to 0$. (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

$$1 \leq |B(v_n,v_n)| = |B(g_n v_n, g_n v_n)| \to |B(0,0)| = 0.$$

This is a contradiction.

Step 2. The image of G in $\mathrm{SL}(\ell,\mathbb{R})/\mathrm{SL}(\ell,\mathbb{Z})$ is closed. Suppose $g_n\gamma_n \to h \in \mathrm{SL}(\ell,\mathbb{R})$, 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 $\{v_1,\cdots,v_\ell\}$ 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

$$B(\gamma_n v_j, \gamma_n v_k) \subset B(\mathbb{Z}^\ell,\mathbb{Z}^\ell) \subset \mathbb{Z}.$$

We also have

$$B(\gamma_n v_j, \gamma_n v_k) = B(g_n\gamma_n v_j, g_n\gamma_n v_k) \to B(hv_j, hv_k),$$

so we conclude that $B(\gamma_n v_j, \gamma_n v_k) = B(hv_j, hv_k)$ 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 $\phi\colon G/\Gamma \to \mathrm{SL}(\ell,\mathbb{R})/\mathrm{SL}(\ell,\mathbb{Z})$ 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 $g_n\gamma_n \to h$. 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. □

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 6.38(1)).

(6.36) **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 $V_\mathbb{Q} \otimes_\mathbb{Q} \mathbb{R} \to V$ defined by $t \otimes v \mapsto tv$ is an isomorphism (see Exer. 6:10).
- A polynomial f on V is *defined over* Q (with respect to the $\mathbb{Q}$-form $V_\mathbb{Q}$) if $f(V_\mathbb{Q}) \subset \mathbb{Q}$ (see Exer. 6:11).
- A finitely generated subgroup Λ of the additive group of $V_\mathbb{Q}$ is a *vector-space lattice* in $V_\mathbb{Q}$ if the $\mathbb{Q}$-linear map $\mathbb{Q} \otimes_\mathbb{Z} \Lambda \to V_\mathbb{Q}$ defined by $t \otimes v \mapsto tv$ is an isomorphism (see Exer. 6:12).
- The $\mathbb{Q}$-form $V_\mathbb{Q}$ on V determines a corresponding $\mathbb{Q}$-form on the real vector space $\operatorname{End}(V)$ by
$$\operatorname{End}(V)_\mathbb{Q} = \{\, A \in \operatorname{End}(V) \mid A(V_\mathbb{Q}) \subset V_\mathbb{Q} \,\}$$
(see Exer. 6:14).
- A function Q on a real vector space W is a *polynomial* if for some (hence, every) $\mathbb{R}$-linear isomorphism $\phi\colon \mathbb{R}^\ell \cong W$, the composition $f \circ \phi$ is a polynomial function on $\mathbb{R}^\ell$.
- A virtually connected subgroup H of $\operatorname{SL}(V)$ is *defined over* Q (with respect to the $\mathbb{Q}$-form $V_\mathbb{Q}$) if there exists a set $\mathcal{Q}$ of polynomials on $\operatorname{End}(V)$, such that
  - every $Q \in \mathcal{Q}$ is defined over $\mathbb{Q}$ (with respect to the $\mathbb{Q}$-form $V_\mathbb{Q}$),
  - $\operatorname{Var}(\mathcal{Q}) = \{\, g \in \operatorname{SL}(V) \mid Q(g) = 0 \text{ for all } Q \in \mathcal{Q} \,\}$ is a subgroup of $\operatorname{SL}(V)$; and
  - $H^\circ = \operatorname{Var}(\mathcal{Q})^\circ$.

(6.37) **Remark.**
- Suppose $G \subset \operatorname{SL}(\ell, \mathbb{R})$. 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. 6.36 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 Λ a *lattice in* V_Q, but this could cause confusion, because Λ 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 Λ simply represent $\mathbb{Q}^\ell$ and $\mathbb{Z}^\ell$, under some identification of V with $\mathbb{R}^\ell$.

(6.38) **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 $\phi\colon V \to \mathbb{R}^\ell$, such that $\phi(V_\mathbb{Q}) = \mathbb{Q}^\ell$. Furthermore, if Λ is any vector-space lattice in $V_\mathbb{Q}$, then ϕ may be chosen so that $\phi(\Lambda) = \mathbb{Z}^\ell$.*
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. 6:11).*

Second, let us note that any two vector-space lattices in $V_\mathbb{Q}$ are commensurable (see Exer. 6:15):

(6.39) **Lemma.** *If Λ_1 and Λ_2 are two vector-space lattices in $V_{\mathbb{Q}}$, then there is some nonzero $p \in \mathbb{Z}$, such that $p\Lambda_1 \subset \Lambda_2$ and $p\Lambda_2 \subset \Lambda_1$.*

It is now easy to prove the following more abstract characterization of arithmetic lattices (see Exers. 6:16 and 6:17).

(6.40) **Proposition.** *Suppose $G \subset \mathrm{GL}(V)$, and G is defined over $\mathbb{Q}$, with respect to the $\mathbb{Q}$-form $V_{\mathbb{Q}}$.*

1) *If Λ is any lattice in $V_{\mathbb{Q}}$, then*
$$G_\Lambda = \{\, g \in G \mid g\Lambda = \Lambda \,\}$$
is an arithmetic subgroup of G.
2) *If Λ_1 and Λ_2 are any two lattices in $V_{\mathbb{Q}}$, then G_{Λ_1} and G_{Λ_1} are commensurable.*

From Prop. 6.40(2), we see that the arithmetic subgroup G_Λ 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 Λ.

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 $\mathrm{SL}\big(2,\mathbb{Z}[\sqrt{2}]\big)$ is an arithmetic lattice in $\mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{R})$ (see Prop. 6.43). 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.

(6.41) **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, $\mathcal{O}$ 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.

(6.42) **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 $\Delta\colon F \to \mathbb{R}^2$ by
$$\Delta(x) = \big(x, \sigma(x)\big).$$
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 $\{\sigma_1, \ldots, \sigma_r\}$ be the set of all embeddings of $\mathcal{O}$ in $\mathbb{C}$, and define $\Delta\colon \mathcal{O} \to \mathbb{C}^r$ by
$$\Delta(x) = \big(\sigma_1(x), \ldots, \sigma_r(x)\big),$$
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 $\mathrm{SL}\big(2,\mathbb{Z}[\sqrt{2}]\big)$ is isomorphic to an irreducible, arithmetic lattice in $\mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{R})$.

(6.43) **Proposition.** *Let*

- $\Gamma = \mathrm{SL}\big(2,\mathbb{Z}[\sqrt{2}]\big)$,
- $G = \mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{R})$, *and*
- σ *be the conjugation on* $\mathbb{Q}[\sqrt{2}]$ (*so* $\sigma\big(a + b\sqrt{2}\big) = a - b\sqrt{2}$, *for* $a, b \in \mathbb{Q}$),

and define $\Delta\colon \Gamma \to G$ *by* $\Delta(\gamma) = \big(\gamma, \sigma(\gamma)\big)$.

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 $\big\{(1,1), (\sqrt{2}, -\sqrt{2})\big\}$ 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,

$$\Delta(F^2) = \big\{\, \big(u, \sigma(u)\big) \in F^4 \mid u \in F^2 \,\big\}$$

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. 6:19), 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. 6:20). Furthermore, because $\Delta(\Gamma) \cap \big(\mathrm{SL}(2,\mathbb{R}) \times e\big)$ is trivial, we see that the lattice $\Delta(\Gamma)$ must be irreducible in G (see 5.24). □

More generally, the proof of Prop. 6.43 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.

(6.44) **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 lattice in* G.

Proof. As above, let σ be the conjugation on $\mathbb{Q}(\sqrt{2})$.

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 $\Delta\colon \Gamma \to G \times K'$ by $\Delta(\gamma) = \big(\gamma, \sigma(\gamma)\big)$. (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. 6:21 for the technical point of verifying that $G \times K'$ is defined over $\mathbb{Q}$.) Since K' is compact, the desired conclusion is obtained by modding out K'. (This type of example is the reason for including the compact normal subgroup K' in Defn. 6.16.) □

(6.45) **Remark.** Let γ be any nontrivial element of the lattice Γ of Prop. 6.44. 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 (6.33) implies that Γ is cocompact. Alternatively, this conclusion can easily be obtained directly from the Mahler Compactness Criterion (5.34) (see Exer. 6:23).

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 lattice in* G.

Proof. For convenience, let $\alpha = \sqrt[4]{2}$. There are exactly 4 distinct embeddings σ_0, σ_1, σ_2, σ_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 $\Delta\colon F \to \mathbb{R} \times \mathbb{R} \times \mathbb{C}$ by $\Delta(x) = \big(x, \sigma_1(x), \sigma_2(x)\big)$. Then, arguing much as before, we see that $\Delta(F^2)$ is a $\mathbb{Q}$-form of $\mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{C}^2$, G is defined over $\mathbb{Q}$, and $G_{\Delta(\mathcal{O}^2)} = \Delta(\Gamma)$. □

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 $\sigma_1, \sigma_2\colon F \to \mathbb{C}$ are *equivalent* if $\sigma_1(x) = \overline{\sigma_2(x)}$, for all $x \in F$ (where $\overline{z}$ 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 $\mathcal{Q} \subset F_\sigma[x_{1,1}, \ldots, x_{\ell,\ell}]$, let
$$\mathrm{Var}_{F_\sigma}(\mathcal{Q}) = \{\, g \in \mathrm{SL}(\ell, F_\sigma) \mid Q(g) = 0,\ \forall Q \in \mathcal{Q} \,\}.$$
Thus, for $F_\sigma = \mathbb{R}$, we have $\mathrm{Var}_{\mathbb{R}}(\mathcal{Q}) = \mathrm{Var}(\mathcal{Q})$, and $\mathrm{Var}_{\mathbb{C}}(\mathcal{Q})$ is analogous, using the field $\mathbb{C}$ in place of $\mathbb{R}$.
- Suppose $G \subset \mathrm{SL}(\ell,\mathbb{R})$, and G is defined over F, so there is some subset $\mathcal{Q}$ of $F[x_{1,1}, \ldots, x_{\ell,\ell}]$, such that $G = \mathrm{Var}(\mathcal{Q})^\circ$. For any place σ of F, let
$$G^\sigma = \mathrm{Var}_{F_\sigma}\big(\sigma(\mathcal{Q})\big)^\circ.$$
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 $G \subset \mathrm{SL}(\ell,\mathbb{R})$ 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 $\Delta\colon \gamma \mapsto \big(\sigma(\gamma)\big)_{\sigma \in S^\infty}$.

Furthermore, if G is simple, then the lattice is irreducible.

The argument in Rem. 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

- $G \subset \mathrm{SL}(\ell,\mathbb{C})$,
- 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 $F[x_{1,1},\ldots,x_{\ell,\ell}]$, such that $G = \mathrm{Var}_{\mathbb{C}}(\mathcal{Q})^\circ$.

For example,

1) $\mathrm{SO}\big(n,\mathbb{Z}\,[i,\sqrt{2}\,]\big)$ embeds as an irreducible arithmetic lattice in $\mathrm{SO}(n,\mathbb{C}) \times \mathrm{SO}(n,\mathbb{C})$, and
2) $\mathrm{SO}\left(n,\mathbb{Z}\left[\sqrt{1-\sqrt{2}}\right]\right)$ embeds as an irreducible arithmetic lattice in $\mathrm{SO}(n,\mathbb{C}) \times \mathrm{SO}(n,\mathbb{R}) \times \mathrm{SO}(n,\mathbb{R})$.

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 $\mathrm{SL}(\ell,F_\infty)$, for some ℓ, such that H is defined over F (as an algebraic group over F_∞), and*
3) *an isogeny*

$$\phi\colon \prod_{\sigma \in S^\infty} H^\sigma \to G,$$

such that $\phi\big(\Delta(H_{\mathcal{O}})\big)$ 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 $G \subset \mathrm{SL}(\ell,\mathbb{C})$ 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 $G = G_1 \times \cdots \times G_r$, 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 $\{G_1,\ldots,G_r\}$.

We claim that Σ acts transitively on $\{G_1,\ldots,G_r\}$. 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 $\sigma_1, \ldots, \sigma_r$ be coset representatives of Σ_1 in Σ. Then $\sigma_1|_F, \ldots, \sigma_r|_F$ are the r places of F and, after renumbering, we have $G_j = \sigma_j(G_1)$. So (with $H = G_1$), we have

$$\prod_{\sigma \in S^\infty} H^\sigma = H^{\sigma_1|_F} \times \cdots \times H^{\sigma_r|_F} = \sigma_1(G_1) \times \cdots \times \sigma_r(G_1) = G_1 \times \cdots \times G_r = G.$$

Let ϕ be the identity map.

For $h \in H_F$, let $\Delta'(h) = \prod_{j=1}^r \sigma_j(h)$. Then $\sigma\big(\Delta'(h)\big) = \Delta'(h)$ 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 $\phi\big(\Delta(H_{\mathcal{O}})$ is commensurable with Γ. □

By applying the definition of an arithmetic lattice, we immediately obtain the following conclusion.

(6.53) **Corollary.** *If Γ is an irreducible, arithmetic lattice in G, and G 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*
$$\phi\colon \prod_{\sigma \in S^\infty} H^\sigma \to G,$$
with compact kernel,

such that $\phi\big(\Delta(H_{\mathcal{O}})\big)$ is commensurable with Γ.

(6.54) **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 6.55 and 3.33), the desired conclusion follows. □

(6.55) **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 $\{v_1, \ldots, v_n\}$ 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 $\{u_1, \ldots, u_n\}$ 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 $v_1^\sigma, \ldots, v_n^\sigma$ 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. □

The same proof yields the following generalization that does not require F or $\sigma(F)$ to be contained in $\mathbb{R}$.

(6.56) **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).

(6.57) **Remark.**
1) See Exer. 6:26 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 (6.55) (or 6.56) 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 (6.20) was proved by Margulis [Mar1, Mar3] under the assumption that $\mathbb{R}\text{-rank}\, G \geq 2$. (Proofs also appear in [Mar4, 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 §7E). 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 [Mar4, App. C, pp. 353–368].

The Commensurability Criterion (6.28) was proved by Margulis [Mar2]. It appears in [AC-B], [Mar4], and [Zim].

Exercises

6:1) Prove ($\Leftarrow$) of Theorem 6.8.

6:2) For H as in Warning 6.9, show that $H_{\mathbb{Q}}$ is not dense in H.

6:3) 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 $\mathrm{Var}(\mathcal{Q}) = \mathrm{Var}(I)$. From the Borel Density Theorem (5.44), we see that $G \subset \mathrm{Var}(I)$. Theorem 4.8 implies that G has finite index in $\mathrm{Var}(I)$.]

6:4) Show, for $m,n \geq 2$, that $\mathrm{SL}(m,\mathbb{R}) \times \mathrm{SL}(n,\mathbb{R})$ has an irreducible lattice if and only if $m = n$.

6:5) Show, for all $p \in \mathbb{Z}^+$, that $\begin{pmatrix} \sqrt{p} & 0 \\ 0 & 1/\sqrt{p} \end{pmatrix}$ commensurates $\mathrm{SL}(2,\mathbb{Z})$. Conclude, for $G = \mathrm{SL}(2,\mathbb{R})$, that $\mathrm{Comm}_G(G_{\mathbb{Z}})$ is *not* commensurable with $G_{\mathbb{Q}}$.

6:6) Show, for $G = \mathrm{SL}(3,\mathbb{R})$, that $\mathrm{Comm}_G(G_{\mathbb{Z}})$ is *not* commensurable with $G_{\mathbb{Q}}$. [*Hint:* See Exer. 6:5.]

6:7) Show that if G is simple and Γ is not arithmetic, then Γ, $N_G(\Gamma)$, and $\mathrm{Comm}_G(\Gamma)$ are commensurable with each other.

6:8) Suppose Λ is a subgroup of $\mathrm{SL}(n,\mathbb{Q})$, and k is a positive integer, such that $k\lambda \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ for every $\lambda \in \Lambda$. Show that $\Lambda \cap \mathrm{SL}(n,\mathbb{Z})$ has finite index in Λ. [*Hint:* If $k\gamma \equiv k\lambda \pmod{k}$, then $\gamma\lambda^{-1} \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$.]

6:9) Show that there is a noncocompact lattice Γ in $\mathrm{SL}(2,\mathbb{R}) \times \mathrm{SO}(3)$, such that no nontrivial element of Γ is unipotent.

6:10) Show that a $\mathbb{Q}$-subspace $V_{\mathbb{Q}}$ of V is a $\mathbb{Q}$-form if an 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.

6:11) 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.

6:12) Show that a subgroup Λ 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 Λ is the additive abelian subgroup of $V_{\mathbb{Q}}$ generated by $\mathcal{B}$.

6:13) Let V be a real vector space of dimension ℓ, and let Λ be a discrete subgroup of the additive group of V.
   (a) Show that Λ is a finitely generated, abelian group of rank $\leq \ell$, with equality if and only if the $\mathbb{R}$-span of Λ is V.
   (b) Show that if the rank of Λ is ℓ, then the $\mathbb{Q}$-span of Λ is a $\mathbb{Q}$-form of V, and Λ is a vector-space lattice in $V_{\mathbb{Q}}$.

   [*Hint:* Induction on ℓ. For $\lambda \in \Lambda$, show that the image of Λ in $V/(\mathbb{R}\lambda)$ is discrete.]

6:14) Verify that if $V_{\mathbb{Q}}$ is a $\mathbb{Q}$-form of V, then $\mathrm{End}(V)_{\mathbb{Q}}$ is a $\mathbb{Q}$-form of $\mathrm{End}(V)$.

6:15) Prove Lemma 6.39, and conclude that Λ_1 and Λ_2 are commensurable.

6:16) Prove Prop. 6.40(1). [*Hint:* Use Lemma 6.38.]

6:17) Prove Prop. 6.40(2). [*Hint:* Use Lemma 6.39.]

6:18) In the notation of the proof of Prop. 6.43, show, for the $\mathbb{Q}$-form $\Delta(F^2)$ of $\mathbb{R}^4$, that

$$\operatorname{End}(\mathbb{R}^4)_{\mathbb{Q}} = \left\{ \begin{pmatrix} A & B \\ \sigma(B) & \sigma(A) \end{pmatrix} \;\middle|\; A, B \in \operatorname{Mat}_{2\times 2}(F) \right\}.$$

[*Hint:* Since the F-span of $\Delta(F^2)$ is F^4, we have $\operatorname{End}(\mathbb{R}^4)_{\mathbb{Q}} \subset \operatorname{Mat}_{4\times 4}(F)$. Thus, for any $T \in \operatorname{End}(\mathbb{R}^4)_{\mathbb{Q}}$, we may write $T = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, with $A, B, C, D \in \operatorname{Mat}_{2\times 2}(F)$. Now use the fact that, for all $u \in F^2$, we have $T(u) = \big(v, \sigma(v)\big)$, for some $v \in F^2$.]

6:19) In the notation of the proof of Prop. 6.43, let

$$\mathcal{Q} = \{\, x_{i,j+2} + x_{i+2,j},\ x_{i,j+2}x_{i+2,j} \mid 1 \le i, j \le 2 \,\}.$$

(a) Use the conclusion of Exer. 6:18 to show that each $Q \in \mathcal{Q}$ is defined over $\mathbb{Q}$.
(b) Show that $\operatorname{Var}(\mathcal{Q})^\circ = \operatorname{SL}(2,\mathbb{R}) \times \operatorname{SL}(2,\mathbb{R})$.

6:20) In the notation of the proof of Prop. 6.43, use Exer. 6:18 to show that $G_{\Delta(\mathcal{O}^2)} = \Delta(\Gamma)$.

6:21) Let F, $\mathcal{O}$, σ, and Δ be as in the proof of Prop. 6.43.

If $G \subset \operatorname{SL}(\ell,\mathbb{R})$, and G is defined over F, show that $G \times G$ is defined over $\mathbb{Q}$ (with respect to the $\mathbb{Q}$-form on $\operatorname{End}(\mathbb{R}^{2\ell})$ induced by the $\mathbb{Q}$-form $\Delta(F^\ell)$ on $\mathbb{R}^{2\ell}$.

[*Hint:* For each $Q \in \mathbb{Q}[x_{1,1}, \ldots, x_{\ell,\ell}]$, let us define a corresponding polynomial $Q^+ \in \mathbb{Q}[x_{\ell+1,\ell+1}, \ldots, x_{2\ell,2\ell}]$ 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 $\mathcal{Q}_0 \subset \mathbb{Q}[x_{1,1}, \ldots, x_{\ell,\ell}]$ that defines G as a subgroup of $\operatorname{SL}(\ell,\mathbb{R})$, let

$$\mathcal{Q}_1 = \{\, Q + \sigma(Q^+),\ Q\,\sigma(Q^+) \mid Q \in \mathcal{Q}_0 \,\}.$$

A natural generalization of Exer. 6:19 shows that $\operatorname{SL}(\ell,\mathbb{R}) \times \operatorname{SL}(\ell,\mathbb{R})$ is defined over $\mathbb{Q}$: let $\mathcal{Q}_2$ be the corresponding set of $\mathbb{Q}$-polynomials. Now define $\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2$.]

6:22) 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 $\Delta(F)$.

6:23) Let
- $B(v,w) = v_1w_1 + v_2w_2 - \sqrt{2}v_3w_3$, for $v, w \in \mathbb{R}^3$,
- $G = \operatorname{SO}(B)^\circ$,
- $G^* = G \times G^\sigma$,
- $\Gamma = G_{\mathbb{Z}[\sqrt{2}]}$, and
- $\Gamma^* = \Delta(\Gamma)$.

Show:
(a) The image of G^* in $\operatorname{SL}(6,\mathbb{R}) / \operatorname{SL}(6,\mathbb{R})_{\Delta(\mathcal{O}^3)}$ is precompact (by using the Mahler Compactness Criterion).
(b) The image of G^* in $\operatorname{SL}(6,\mathbb{R}) / \operatorname{SL}(6,\mathbb{R})_{\Delta(\mathcal{O}^3)}$ 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. 6.35.]

6:24) 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 $\mathrm{End}_{\mathbb{R}}\bigl(\bigoplus_{\sigma \in S^\infty} (F_\sigma)^\ell\bigr)$ 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. 6:19. 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 $\mathbb{Q}$.]

6:25) 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 $\mathrm{End}_{\mathbb{R}}\bigl(\bigoplus_{\sigma \in S^\infty} (F_\sigma)^\ell\bigr)$ 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. 6:21. See the hint to Exer. 6:24.]

6:26) For $\alpha \in \mathbb{C} \smallsetminus \{0, -1\}$, 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 $(\mathfrak{h}_\alpha)^\sigma$.

6:27) In the notation of Exer. 6:26, 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 $\mathbb{Q}$.

6:28) In the notation of Exer. 6:26, 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 $\mathfrak{h}_\alpha$.]

Chapter 8

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

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \in \mathrm{SO}(2)$$

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) $\mathbb{R}\text{-rank}\big(\mathrm{SL}(n,\mathbb{R})\big) = n-1$. (Let T be the identity component of the group of all diagonal matrices in $\mathrm{SL}(n,\mathbb{R})$.)

2) We have $\mathbb{R}\text{-rank}\big(\mathrm{SL}(n,\mathbb{C})\big) = \mathbb{R}\text{-rank}\big(\mathrm{SL}(n,\mathbb{H})\big) = 1$. 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
$$\mathbb{R}\text{-rank}\big(\mathrm{SO}(1,1)\big) \le \mathbb{R}\text{-rank}\big(\mathrm{SL}(2,\mathbb{R})\big) = 1.$$
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
$$T = \left\{ \begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix} \;\middle|\; t \in \mathbb{R} \right\}.$$
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
$$\mathbb{R}\text{-rank}\big(\mathrm{SO}(1,1)\big) \ge \dim T = 1,$$
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
$$\langle v \mid v \rangle_{\mathbb{R}^{m,n}} = \langle a^{-k} v \mid a^{-k} v \rangle_{\mathbb{R}^{m,n}} = \langle \lambda^{-k} v \mid \lambda^{-k} v \rangle_{\mathbb{R}^{m,n}} = \lambda^{-2k} \langle v \mid v \rangle_{\mathbb{R}^{m,n}} \to 0$$
as $k \to \infty$. Since $\langle v \mid v \rangle_{\mathbb{R}^{m,n}}$ is independent of k, we conclude that
$$\langle v \mid v \rangle_{\mathbb{R}^{m,n}} = 0;$$

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 $\mathbb{R}\text{-rank}\big(\mathrm{SO}(n)\big) = 0$.

(8.11) **Proposition.** $\mathbb{R}\text{-rank}\big(\mathrm{SO}(m,n)\big) = \min\{m,n\}$.

Proof. *Step 1. We have* $\mathbb{R}\text{-rank}\,\mathrm{SO}(m,n)\big) \geq \min\{m,n\}$. We may assume $m \leq n$. Let

$$G = \mathrm{Isom}(x_1^2 - x_2^2 + x_3^2 - x_4^2 \pm \cdots + x_{2m-1}^2 - x_{2m}^2 + x_{2m+1}^2 + x_{2m+2}^2 + \cdots + x_{m+n}^2)^\circ.$$

Then G is isomorphic to $\mathrm{SO}(m,n)^\circ$. (Indeed, G is conjugate to $\mathrm{SO}(m,n)^\circ$, simply by permuting the basis vectors.) Therefore, $\mathbb{R}\text{-rank}(G) = \mathbb{R}\text{-rank}\big(\mathrm{SO}(m,n)\big)$. There is an obvious embedding of $\mathrm{SO}(1,1)^m$ in G:

$$\begin{pmatrix} \mathrm{SO}(1,1) & & & & \\ & \mathrm{SO}(1,1) & & & \\ & & \ddots & & \\ & & & \mathrm{SO}(1,1) & \\ & & & & \mathrm{Id}_{n-m,n-m} \end{pmatrix}^\circ \subset G,$$

so

$$\mathbb{R}\text{-rank}(G) \geq m\,\mathbb{R}\text{-rank}\big(\mathrm{SO}(1,1)\big) = m \cdot 1 = m.$$

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 $\langle v \mid w \rangle_{\mathbb{R}^{m,n}} = 0$ 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 $\mathrm{SO}(m,n)$ 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

$$\mathbb{R}\text{-rank}\,\mathrm{SO}(m,n) = \mathbb{R}\text{-rank}\,\mathrm{SU}(m,n) = \mathbb{R}\text{-rank}\,\mathrm{Sp}(m,n) = \min\{m,n\}.$$

(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 $G = \mathrm{SL}(2,\mathbb{R})$. 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 is 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 $\mathrm{SL}(2,\mathbb{R})$.*

(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*

- $\mathrm{SO}(n)$ *for some $n \geq 5$, with $n \neq 6$,*
- $\mathrm{SU}(n)$ *for some $n \geq 2$,*
- $\mathrm{Sp}(n)$ *for some $n \geq 3$, 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 Theorem 8.22:

1) $\mathrm{SO}(3)$ is isogenous to $\mathrm{SU}(2)$;

2) SO(5) is isogenous to Sp(4);
3) SO(6) is isogenous to SU(4).

The groups SO(1), SU(1), and Sp(2) are trivial. Also, $\mathrm{SO}(2) \cong \mathbb{T}$ is abelian and 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 $\mathrm{SO}(1,n)^\circ = \mathrm{Isom}(\mathfrak{H}^n)^\circ$. Similarly, $\mathrm{SU}(1,n)$ is the isometry group of *complex hyperbolic space*, and $\mathrm{Sp}(1,n)$ is the isometry group of *quaternionic hyperbolic space*. Analogously, $F_{4,1}$ 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 other than 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) $\mathbb{R}$-rank$(G) \le 1$*;*
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 $\mathbb{R}$-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* $\mathbb{R}$-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 $\operatorname{Stab}_G(p)$ 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 $\mathbb{R}$-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

$$P = \left\{ g \in G \;\middle|\; \sup_{t\in\mathbb{R}^+} \|a^{-t} g a^t\| < \infty \right\},$$

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

$$d(gx_t, x_t) = d(ga^t x_0, a^t x_0) = \|(a^t x_0)^{-1}(g a^t x_0)\| = \|x_0^{-1}(a^{-t} g a^t) x_0\| \asymp \|a^{-t} g a^t\|$$

(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. □

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 $\mathbb{R}$-rank(G) is exactly what is needed to make this true.

(8.32) **Theorem.** *Assume G is not compact. The following are equivalent:*

1) $\mathbb{R}$-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 $U_0, \ldots, U_r$ of nontrivial unipotent subgroups of G, such that $U_0 = U$, $U_r = V$, and $[U_i, U_{i-1}] = e$ for $i = 1, \ldots, r$;*
4) *there is a finite sequence $U_0, \ldots, U_r$ of nontrivial unipotent subgroups of G, such that $[U_i, U_{i-1}] = e$ for $i = 1, \ldots, r$, and $\langle U_0, \ldots, U_r\rangle = G$;*
5) *there exists a nontrivial hyperbolic element a and a nontrivial unipotent element u, such that $au = ua$.*

Proof. Assume, for simplicity, that $G = \mathrm{SL}(3,\mathbb{R})$. (See Rem. 8.34 for a general proof, using the theory of real roots.)

(2) Assume T is the group of diagonal matrices. Let

$$a_1 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1/4 \end{pmatrix} \qquad \text{and} \qquad a_2 = \begin{pmatrix} 1/4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Then

$$C_G(a_1) = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{pmatrix} \qquad \text{and} \qquad C_G(a_2) = \begin{pmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

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 $\mathrm{SL}(3,\mathbb{R})$, we may assume

$$U = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{pmatrix}.$$

We may now take the sequence

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ * & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{pmatrix}.$$

(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. 24). For simplicity, assume $\mathbb{R}$-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

$$U = \langle U_\phi \mid \phi \in \Phi^+ \rangle \qquad \text{and} \qquad U = \langle U_{-\phi} \mid \phi \in \Phi^+ \rangle.$$

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. 24).) 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 3.29).
- $\mathrm{SU}(2,2)$ 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 3.29).

□

(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 discussed in Sect. 28D.

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!!!

Exercises

8:1) For $g = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$, show that $g^{-1}\,\mathrm{SO}(2)g$ consists entirely of diagonal matrices.

8:2) Prove Prop. 8.7.

8:3) Let T be the torus T of 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. 24, we will show that if G is not compact, then G contains a subgroup isogenous to $\mathrm{SL}(2,\mathbb{R})$ (see also Rem. 3.23 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 3.29). 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 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
$$T_1 = \left\{ \begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix} \;\middle|\; t \in \mathbb{R} \right\}$$
(cf. 8.10(3)). Then, for
$$g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$
we see that $g^{-1}T_1 g$ consists of diagonal matrices, so T_1 is $\mathbb{Q}$-split.
- Let
$$T_2 = \left\{ \begin{pmatrix} \cosh t & (\sinh t)/\sqrt{2} \\ \sqrt{2}\,(\sinh t) & \cosh t \end{pmatrix} \;\middle|\; t \in \mathbb{R} \right\} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{pmatrix} T_1 \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{pmatrix}^{-1}.$$
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
$$\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \in T_{\mathbb{Q}},$$
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
$$T_3 = \left\{ \begin{pmatrix} \cosh t & (\sinh t)/\pi \\ \pi\,(\sinh t) & \cosh t \end{pmatrix} \;\middle|\; t \in \mathbb{R} \right\} = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} T_1 \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}^{-1}.$$

Then T_3 is not defined over $\mathbb{Q}$ (indeed, $(T_3)_{\mathbb{Q}}$ consists of only the identity matrix), so T_3 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 $v_1,\ldots,v_\ell$ of $\mathbb{Q}^\ell$, such that, for every $t \in T$ and every $i \in \{1,\ldots,\ell\}$, the vector v_i is an eigenvector of t;*
3) *there is a basis $v_1,\ldots,v_\ell$ of $\mathbb{Q}^\ell$, such that, for every $t \in T_{\mathbb{Q}}$ and every $i \in \{1,\ldots,\ell\}$, 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 $\mathbb{Q}$. □

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 $\phi\colon G/K \cong G'/K'$, 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 9.13); thus, $\mathbb{Q}$-rank(Γ) is well defined as a function of Γ.

(9.6) **Example.**

1) $\mathbb{Q}\text{-rank}\big(\mathrm{SL}(n,\mathbb{Z})\big) = n-1$. Let T be the torus of (positive) diagonal matrices in $\mathrm{SL}(n,\mathbb{R})$.
2) Let $G = \mathrm{SO}(B)^\circ$, where $B(x_1,\ldots,x_\ell)$ 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,
$$\mathbb{Q}\text{-rank}\big(\mathrm{SO}(m,n)_{\mathbb{Z}}\big) = \min\{m,n\}.$$
Similarly,
$$\mathbb{Q}\text{-rank}\big(\mathrm{SU}(m,n)_{\mathbb{Z}}\big) = \mathbb{Q}\text{-rank}\big(\mathrm{Sp}(m,n)_{\mathbb{Z}}\big) = \min\{m,n\}.$$

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
$$\begin{pmatrix} \sqrt{7} & 0 & 0 & \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$
   We see from Thm. 9.19 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 (16.2) 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 $F\text{-rank}(G)$. 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*
- *$\Delta\colon G_F \to \prod_{\sigma \in S^\infty} G^\sigma$ is defined by $\Delta(g) = \big(\sigma(g)\big)_{\sigma \in S^\infty}$, as in Prop. 6.49.*

Then $\mathbb{Q}\text{-rank}\big(\Delta(G_{\mathcal{O}})\big) = F\text{-rank}(G)$.

Proof. If T is an F-split torus in G, then $\Delta(T)$ is a $\mathbb{Q}$-split torus in $\prod_{\sigma \in S^\infty} G^\sigma$. [Should give more explanation here!!!] □

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 $\phi\colon G \to H$ 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 $\phi_j\colon G \to G_j$ 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 $\phi_j\colon G \to G_j$ that are defined over F.*

Proof. Given isogenies $\phi_j \colon G \to G_j$ that are defined over F, let
$$G' = \bigl\{\, \bigl(\phi_1(g), \phi_2(g)\bigr) \bigm| g \in G \,\bigr\}.$$
The projection maps $\phi_j' \colon G' \to G_j$ defined by $\phi_j'(g_1, g_2) = g_j$ are polynomials. □

(9.10) **Warning.** There are examples where $\phi \colon G_1 \to G_2$ is an isomorphism over F, and ϕ is a polynomial, but ϕ^{-1} is not a polynomial. For example, the natural homomorphism $\phi\colon \mathrm{SL}(3,\mathbb{R}) \to \mathrm{PSL}(3,\mathbb{R})^\circ$ 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 map 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 $\phi \colon G \to H$ 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 $\phi' \colon G \to \mathrm{Mat}_{m\times m}(\mathbb{R})$ 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 $\phi'\bigl(n\,\mathrm{Mat}_{\ell\times\ell}(\mathbb{R}) \subset \mathrm{Mat}_{m\times m}(\mathbb{Z})$. 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 $\phi \colon G \to H$ 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) **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, $\mathbb{Q}$-rank(Γ) is defined only when Γ is arithmetic, but combining the following remark with the Margulis Arithmeticity Theorem (6.20) allows us to extend the definition to all lattices.

(9.14) **Remark.** Assume Γ is arithmetic.

- If $\Gamma\backslash G$ is compact, then $\mathbb{Q}\text{-rank}(\Gamma) = 0$ (see 9.19).
- If $\Gamma\backslash G$ is not compact, and $\mathbb{R}\text{-rank}(G) = 1$, then $\mathbb{Q}\text{-rank}(\Gamma) \neq 0$ (see 9.19) and $\mathbb{Q}\text{-rank}(\Gamma) \le \mathbb{R}\text{-rank}(G) = 1$ (see 9.16); so we must have $\mathbb{Q}\text{-rank}(\Gamma) = 1$.
- If $\Gamma = \Gamma_1 \times \cdots \times \Gamma_r$ is reducible, then $\mathbb{Q}\text{-rank}(\Gamma) = \mathbb{Q}\text{-rank}(\Gamma_1) + \cdots + \mathbb{Q}\text{-rank}(\Gamma_r)$.

Thus, the following definition is consistent with Defn. 9.4.

(9.15) **Definition.** Up to isogeny, 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 $i = 1, \ldots, r$ (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 $\mathbb{Q}$-rank$(\Gamma_i) = 0$.
2) If $\Gamma_i \backslash G$ is not compact, but $\mathbb{R}$-rank$(G) = 1$, then $\mathbb{Q}$-rank$(\Gamma_i) = 1$.
3) If $\Gamma_i \backslash G$ is not compact, and $\mathbb{R}$-rank$(G) \geq 2$, then the Margulis Arithmeticity Theorem (6.20) 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

(9.16) $$0 \leq \mathbb{Q}\text{-rank}(\Gamma) \leq \mathbb{R}\text{-rank}(G).$$

Both extremes are realized (for every G):

(9.17) **Theorem.** *There are arithmetic lattices Γ_c and Γ_s in G, such that $\mathbb{Q}$-rank$(\Gamma_c) = 0$ and $\mathbb{Q}$-rank$(\Gamma_s) = \mathbb{R}$-rank(G).*

In particular, if $\mathbb{R}$-rank$(G) \geq 2$, then G has a lattice Γ with $\mathbb{Q}$-rank$(\Gamma) \geq 2$.

Proof. Suppose G is classical. Then, for the natural embeddings described in Egs. 3.21 and 3.22, it is easy to see that $\mathbb{Q}$-rank$(G_{\mathbb{Z}}) = \mathbb{R}$-rank$(G)$ (cf. Eg. 9.6(1,2)); thus, it is easy to construct Γ_s. The method of Prop. 6.44 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. 12. □

However, although the extremes are attained, the following example shows that there can be gaps between 0 and $\mathbb{R}$-rank(G).

(9.18) **Proposition.** *Assume $G \cong \mathrm{SO}(2,n)^\circ$, with $n \geq 5$, and assume n is odd. Then $\mathbb{R}$-rank$(G) = 2$, but there is no lattice Γ in G, such that $\mathbb{Q}$-rank$(\Gamma) = 1$.*

Proof. From 8.10(4), we have $\mathbb{R}$-rank$(G) = \min\{2, n\} = 2$.

Suppose $\mathbb{Q}$-rank$(\Gamma) = 1$. The Margulis Arithmeticity Theorem (6.20) implies that Γ is arithmetic. Since $\mathbb{Q}$-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 9.20). (The point here is that, because $\Gamma \backslash G$ is not compact, 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 Chap. 10, 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 $\mathbb{R}$-rank$(G) = 2$), but
2) there does *not* exist a 2-dimensional totally isotropic subspace of $\mathbb{Q}^{n+2}$ (because $\mathbb{Q}$-rank$(\Gamma) < 2$).

A theorem of number theory [Get a reference for this!!!] 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. □

9F. Lattices of $\mathbb{Q}$-rank zero

It is instructive to compare Thms. 9.19 and 9.22 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 (6.33) to the case where Γ is not assumed to be arithmetic.

(9.19) **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 §15D.)

$(2 \Rightarrow 1)$ 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

$$g^n v = \lambda^n v \to 0 \qquad \text{as } n \to \infty.$$

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 (6.33).

$(1 \Rightarrow 4)$ 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 $\phi\colon \mathrm{SL}(2, \mathbb{R}) \to G$ with $\phi\big(\mathrm{SL}(2, \mathbb{Q})\big) \subset G_{\mathbb{Q}}$. 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. 9.22(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.

(9.20) **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 9.19), 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. 6:3). 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). □

(9.21) **Remark.** If the assumption that G has no compact factors is removed from Thm. 9.19, 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.

(9.22) **Theorem.** *If Γ is commensurable with $G_{\mathbb{Z}}$, then the following are equivalent:*

1) $\mathbb{Q}\text{-rank}(\Gamma) = 0$*;*
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 $\mathbb{Q}$.*

(9.23) **Remark.** In analogy with Prop. 8.20(5) and Thm. 9.22(4), one might suppose that $\mathbb{Q}\text{-rank}(\Gamma) = 0$ 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.

(9.24) **Theorem.** *The following are equivalent:*

1) $\mathbb{Q}\text{-rank}(\Gamma) \leq 1$*;*
2) *any two maximal unipotent subgroups of Γ either are equal or are disjoint.*

(9.25) **Theorem.** *If Γ is commensurable with $G_{\mathbb{Z}}$, then the following are equivalent:*

1) $\mathbb{Q}$-rank$(\Gamma) \le 1$;
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).

(9.26) **Theorem.** *Assume Γ is irreducible. Then* $\mathbb{Q}$-rank$(\Gamma) \ge 2$ *if and only if Γ contains a subgroup that is isomorphic to a finite-index subgroup of either* $\mathrm{SL}(3,\mathbb{Z})$ *or* $\mathrm{SO}(2,3)_{\mathbb{Z}}$.

(9.27) **Theorem.** *Assume Γ is commensurable with $G_{\mathbb{Z}}$.*

1) $\mathbb{Q}$-rank$(\Gamma) \ge 2$ *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* $\mathbb{Q}$-rank$(\Gamma) \ge 2$ *if and only if $G_{\mathbb{Q}}$ contains a subgroup isogenous to either* $\mathrm{SL}(3,\mathbb{Q})$ *or* $\mathrm{SO}(2,3)_{\mathbb{Q}}$.

(9.28) **Remark** (cf. Rem. 3.29)**.** $\mathrm{SO}(2,3)_{\mathbb{Z}}$ 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.

(9.29) **Theorem.** *The following are equivalent:*

1) $\mathbb{Q}$-rank$(\Gamma) \ge 2$;
2) *for every pair of nontrivial unipotent subgroups U and V of Γ, there is a finite sequence $U_0, \ldots, U_r$ of nontrivial unipotent subgroups of Γ, such that $U_0 = U$, $U_r = V$, and $[U_i, U_{i-1}] = e$ for $i = 1, \ldots, r$;*
3) *there is a finite sequence $U_0, \ldots, U_r$ of nontrivial unipotent subgroups of Γ, such that $[U_i, U_{i-1}] = e$ for $i = 1, \ldots, r$, and $\langle U_0, \ldots, U_r \rangle$ is a finite-index subgroup of Γ.*

Unipotent generators, such as those in 9.29(3), are easy to work with. See §23B and §23C for an introduction to their use in the study of difficult algebraic problems. See §26B for a much easier example.

(9.30) **Remark.** 1) Suppose $\mathbb{Q}$-rank$(\Gamma) \le 1$. Theorem 9.29 shows that it is impossible to find a generating set $\{\gamma_1, \ldots, \gamma_r\}$ 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 $\{\gamma_1, \ldots, \gamma_r\}$ 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 use the material of Chap. 10 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 $\mathbb{Q}$.

(9.31) **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*

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

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 $\mathrm{SO}\big(\langle\cdot \mid \cdot\rangle\big)$ 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*

$$P = \{\, g \in \mathrm{SO}\big(\langle\cdot \mid \cdot\rangle\big) \mid \forall i,\ g\big(\langle V_i\rangle_{\mathbb{R}}\big) = \langle V_i\rangle_{\mathbb{R}} \,\}.$$

Similarly for orthogonal groups over $\mathbb{C}$ or $\mathbb{H}$, and also for unitary or symplectic groups.

(9.32) **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

$$P = \left\{ g \in G \;\middle|\; \limsup_{n\to\infty} \|a^{-n} g a^n\| < \infty \right\}$$

and

$$N = \left\{ g \in G \;\middle|\; \lim_{n\to\infty} a^{-n} g a^n = e \right\}.$$

(9.33) **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) *$N_G(U) \subset P$.*

(9.34) **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.*
2) *All of the maximal unipotent subgroups of $G_{\mathbb{Q}}$ are conjugate (via $G_{\mathbb{Q}}$).*

(9.35) **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 $\{P_1, \ldots, P_r\}$ 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 $\gamma \in G_{\mathbb{Z}}$.*

(9.36) **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 9.35(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. 9.37). □

(9.37) **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. 2.16. A more complete discussion appears in Sect. 13D.

(9.38) **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

$$\mathcal{F} = \{\, z \in \mathfrak{H}^2 \mid -1/2 \le \operatorname{Re} z \le 1/2,\ |z| \ge 1 \,\}.$$

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:

$$S_{1/2,t} = \{\, z \in \mathfrak{H}^2 \mid -1/2 \le \operatorname{Re} z \le 1/2,\ \operatorname{Im} z \ge e^{-2t} \,\},$$

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

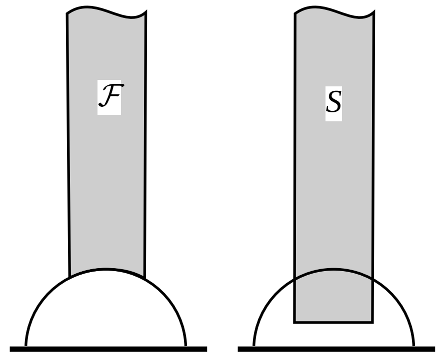

Figure 9.1. The fundamental domain $\mathcal{F}$ and the Siegel set $S_{1/2,t}$ in $\mathfrak{H}^2$.

purposes here, it is more convenient to reverse the order of the factors: $G = NAK$. For $s > 0$ and t as above, let

$$N_s = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \,\middle|\, -s \leq x \leq s \right\} \text{ and } A_t = \left\{ \begin{pmatrix} e^y & 0 \\ 0 & e^{-y} \end{pmatrix} \,\middle|\, y > -t \right\}.$$

Then, as noted in Exer. 9:12, it is not difficult to verify that

$$N_{1/2} A_t K = \{\, g \in G \mid g(i) \in S_{1/2,t} \,\}. \tag{9.39}$$

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.

(9.40) **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. 2.16. 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 9.32, and note that A centralizes M). Since P is minimal, we know that $\mathbb{Q}\text{-rank}(M) = 0$ (see 9.33(5)), so there is a compact subset C_M of M, such that $M_{\mathbb{Z}} C_M = M$ (see 9.19). Similarly, there is a compact subset C_N of N, such that $N_{\mathbb{Z}} C_N = N$ (see 9.37); let $C = C_M C_N$.

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. 9.38 above. In general, the group A is isomorphic to some $\mathbb{R}^d$, where $d = \mathbb{Q}\text{-rank}(\Gamma)$. Then

$$A^+ = \left\{\, a \in A \mid \forall x \in N,\ \|a^{-1} x a\| \leq \|x\| \,\right\}$$

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).

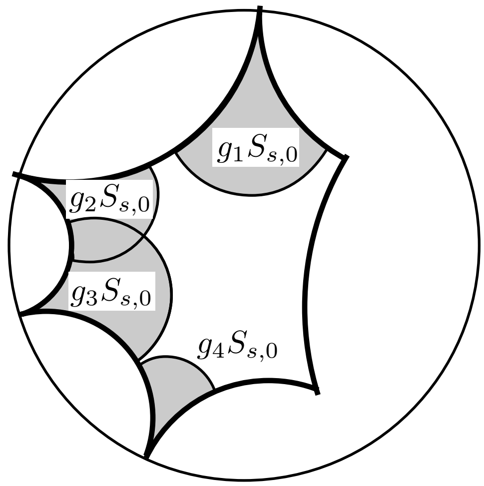

Figure 9.2. For $t = 0$ and s sufficiently large, a finite union (shaded) of translates of the Siegel set $S_{s,0}$ covers the cusps. Increasing t results in a union that contains a fundamental domain (dark outline).

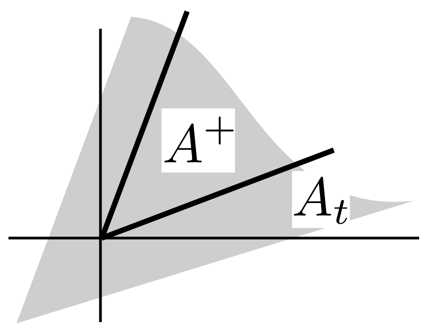

Figure 9.3. The Weyl chamber A^+ and a cone A_t (shaded) when $\dim A = 2$.

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 9.35 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 $CA_t \subset A_tC'$ (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. □

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. 13D that if $\mathbb{Q}\text{-rank}(\Gamma) \geq 2$, then this simplicial complex is connected. This leads to the following conclusion.

(9.41) **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!!!

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. 9.22. [*Hint:* ($1 \Rightarrow 4$) Obvious. ($4 \Rightarrow 3$) Jacobson-Morosov Lemma. ($3 \Rightarrow 1$) Thm. 9.19($4 \Rightarrow 1$). ($2 \Rightarrow 3$) Obvious. ($3 \Rightarrow 2$) Jordan decomposition. ($3 \Rightarrow 5$) Thm. 9.32. ($5 \Rightarrow 3$) Thm. 9.33(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 $\gamma^n v / \big(\|\gamma^n v\|\big)$ converges to an isotropic vector.]

9:5) Use restriction of scalars (see §6G) to construct a cocompact arithmetic lattice 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 $g^{-1} U_1 g$ 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 generating set $\{\gamma_1, \ldots, \gamma_r\}$ for some finite-index subgroup of Γ, such that each γ_i is nontrivial, and 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 $\{\gamma_1, \ldots, \gamma_r\}$ for Γ, such that each γ_i is nontrivial, and γ_i commutes with γ_{i+1}, for each i.

9:12) Verify (9.39). [*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. 9.38, 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. 2.16. Show that if C is any compact subset of N, then there is a compact subset C' of N, such that $C A_t \subset A_t C'$.

Chapter 10

k-Forms of 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 $\mathbb{R}[x_{1,1}, \ldots, x_{\ell,\ell}]$, 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.

(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) $\mathrm{Sp}(p,q) \otimes \mathbb{C} = \mathrm{Sp}\big(2(p+q),\mathbb{C}\big)$*.*

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).
2) There is a technical problem in Not. 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,
$$\mathcal{Q} = \{\, Q \in \mathbb{R}[x_{1,1},\ldots,x_{\ell,\ell}] \mid Q(g) = 0, \text{ for all } g \in G \,\}.$$
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. 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 $\Delta\colon\mathbb{C}\to\mathbb{C}\oplus\mathbb{C}$ by $\Delta(z)=(z,\overline{z})$. 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

$$V_{\mathbb{R}}=\Delta(\mathbb{C}^n)=\{\,(v,\overline{v})\mid v\in\mathbb{C}^n\,\}$$

is a real form of V. Let

$$\big(\mathrm{SL}(n,\mathbb{C})\times\mathrm{SL}(n,\mathbb{C})\big)_{\mathbb{R}}=\{\,g\in\mathrm{SL}(n,\mathbb{C})\times\mathrm{SL}(n,\mathbb{C})\mid g(V_{\mathbb{R}})=V_{\mathbb{R}}\,\}.$$

Then we have an isomorphism

$$\tilde{\Delta}\colon\ \mathrm{SL}(n,\mathbb{C})\xrightarrow{\cong}\big(\mathrm{SL}(n,\mathbb{C})\times\mathrm{SL}(n,\mathbb{C})\big)_{\mathbb{R}},$$

defined by $\tilde{\Delta}(g)=(g,\overline{g})$, so

$$\mathrm{SL}(n,\mathbb{C})\otimes\mathbb{C}\cong\big(\mathrm{SL}(n,\mathbb{C})\times\mathrm{SL}(n,\mathbb{C})\big)_{\mathbb{R}}\otimes\mathbb{C}=\mathrm{SL}(n,\mathbb{C})\times\mathrm{SL}(n,\mathbb{C}).$$

□

(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. 3.29).

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

$$\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}\to\mathbb{C}\oplus\mathbb{C}\text{ defined by }(v,\lambda)\mapsto\Delta(v)\,\lambda$$

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 $\mathrm{Mat}_{2\times2}(\mathbb{C})$.*

Proof. Define an $\mathbb{R}$-linear map $\phi\colon\mathbb{H}\to\mathrm{Mat}_{2\times2}(\mathbb{C})$ by

$$\phi(1)=\mathrm{Id},\qquad\phi(i)=\begin{pmatrix}i&0\\0&-i\end{pmatrix},\qquad\phi(j)=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\qquad\phi(k)=\begin{pmatrix}0&i\\i&0\end{pmatrix}.$$

It is straightforward to verify that ϕ is an injective ring homomorphism. Furthermore, $\phi\big(\{1,i,j,k\}\big)$ is a $\mathbb{C}$-basis of $\mathrm{Mat}_{2\times2}(\mathbb{C})$. Therefore, the map $\hat{\phi}\colon\mathbb{H}\otimes\mathbb{C}\to\mathrm{Mat}_{2\times2}(\mathbb{C})$ defined by $\hat{\phi}(v,\lambda)=\phi(v)\,\lambda$ is a ring isomorphism (see Exer. 10:3). □

(10.12) **Proposition.** $\mathrm{SL}(n,\mathbb{H})\otimes\mathbb{C}\cong\mathrm{SL}(2n,\mathbb{C})$.

Proof. From Lem. 10.11, we have

$$\mathrm{SL}(n,\mathbb{H})\otimes\mathbb{C}\cong\mathrm{SL}\big(n,\mathrm{Mat}_{2\times 2}(\mathbb{C})\big)\cong\mathrm{SL}(2n,\mathbb{C})$$

(see Exers. 10:4 and 10:5). □

As additional examples, let us calculate the complexifications of the classical compact simple Lie groups, namely, $\mathrm{SO}(n)$, $\mathrm{SU}(n)$, and $\mathrm{Sp}(n)$ (see 8.22). As observed in 10.3(2), we have $\mathrm{SO}(n)\otimes\mathbb{C}=\mathrm{SO}(n,\mathbb{C})$. The other cases are not as obvious.

(10.13) **Proposition.** $\mathrm{SU}(n)\otimes\mathbb{C}=\mathrm{SL}(n,\mathbb{C})$.

Proof. Let

- $\sigma\colon\mathbb{C}\to\mathbb{C}$,
- $\overrightarrow{\sigma}\colon\mathbb{C}^n\to\mathbb{C}^n$, and
- $\tilde\sigma\colon\ \mathrm{SL}(n,\mathbb{C})\to\mathrm{SL}(n,\mathbb{C})$

be the usual complex conjugations $\sigma(z)=\overline{z}$, $\overrightarrow{\sigma}(v)=\overline{v}$, and $\tilde\sigma(g)=\overline{g}$. We have

$$\begin{aligned}\mathrm{SU}(n)&=\{\,g\in\mathrm{SL}(n,\mathbb{C})\mid g^*g=\mathrm{Id}\,\}\\&=\{\,g\in\mathrm{SL}(n,\mathbb{C})\mid \sigma(g^T)g=\mathrm{Id}\,\},\end{aligned}$$

so, in order to calculate $\mathrm{SU}(n)\otimes\mathbb{C}$, we should determine the map $\tilde\eta$ on $\mathrm{SL}(n,\mathbb{C})\times\mathrm{SL}(n,\mathbb{C})$ 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 $\overrightarrow{\eta}\colon\mathbb{C}^n\oplus\mathbb{C}^n\to\mathbb{C}^n\oplus\mathbb{C}^n$ by $\overrightarrow{\eta}(x,y)=(y,x)$, then $\overrightarrow{\eta}$ is $\mathbb{C}$-linear, and the following diagram commutes:

$$\begin{array}{ccc}\mathbb{C}^n & \xrightarrow{\overrightarrow{\Delta}} & \mathbb{C}^n\oplus\mathbb{C}^n\\ \Big\downarrow{\scriptstyle\overrightarrow{\sigma}} & & \Big\downarrow{\scriptstyle\overrightarrow{\eta}}\\ \mathbb{C}^n & \xrightarrow{\overrightarrow{\Delta}} & \mathbb{C}^n\oplus\mathbb{C}^n.\end{array}$$

Thus, it is fairly clear that $\tilde\eta(g,h)=(h,g)$. Hence

$$\begin{aligned}\mathrm{SU}(n)\otimes\mathbb{C}&=\{\,(g,h)\in\mathrm{SL}(n,\mathbb{C})\times\mathrm{SL}(n,\mathbb{C})\mid\tilde\eta\big(g^T,h^T\big)(g,h)=(\mathrm{Id},\mathrm{Id})\,\}\\&=\{\,(g,h)\in\mathrm{SL}(n,\mathbb{C})\times\mathrm{SL}(n,\mathbb{C})\mid\big(h^T,g^T\big)(g,h)=(\mathrm{Id},\mathrm{Id})\,\}\\&=\{\,\big(g,(g^T)^{-1}\big)\mid g\in\mathrm{SL}(n,\mathbb{C})\,\}\\&\cong\mathrm{SL}(n,\mathbb{C}),\end{aligned}$$

as desired. □

(10.14) **Proposition.** $\mathrm{Sp}(n)\otimes\mathbb{C}=\mathrm{Sp}(2n,\mathbb{C})$.

Proof. Let

- $\phi\colon\mathbb{H}\hookrightarrow\mathrm{Mat}_{2\times 2}(\mathbb{C})$ be the embedding described in the proof of Lem. 10.11;
- τ be the usual conjugation on $\mathbb{H}$,
- $J=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, and
- $\eta\colon\ \mathrm{Mat}_{2\times 2}(\mathbb{C})\to\mathrm{Mat}_{2\times 2}(\mathbb{C})$ be defined by $\eta(x)=J^{-1}x^TJ$.

Then η is $\mathbb{C}$-linear, and the following diagram commutes:

$$\begin{array}{ccc} \mathbb{H} & \xrightarrow{\phi} & \mathrm{Mat}_{2\times 2}(\mathbb{C}) \\ \Big\downarrow \tau & & \Big\downarrow \eta \\ \mathbb{H} & \xrightarrow{\phi} & \mathrm{Mat}_{2\times 2}(\mathbb{C}). \end{array}$$

Thus, because

$$\begin{aligned} \mathrm{Sp}(2) &= \{\, g \in \mathrm{SL}(2,\mathbb{H}) \mid g^* g = \mathrm{Id} \,\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{H}) \;\middle|\; \begin{pmatrix} \tau(a) & \tau(c) \\ \tau(b) & \tau(d) \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{Id} \right\}, \end{aligned}$$

we see that

$$\begin{aligned} \mathrm{Sp}(2) \otimes \mathbb{C} &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}\big(2, \mathrm{Mat}_{2\times 2}(\mathbb{C})\big) \;\middle|\; \begin{pmatrix} \eta(a) & \eta(c) \\ \eta(b) & \eta(d) \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{Id} \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}\big(2, \mathrm{Mat}_{2\times 2}(\mathbb{C})\big) \;\middle|\; J^{-1} \begin{pmatrix} a^T & c^T \\ b^T & d^T \end{pmatrix} J \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{Id} \right\} \\ &= \{\, g \in \mathrm{SL}(4,\mathbb{C}) \mid J^{-1} g^T J g = \mathrm{Id} \,\} \\ &= \{\, g \in \mathrm{SL}(4,\mathbb{C}) \mid g^T J g = J \,\} \\ &= \mathrm{Sp}(4,\mathbb{C}). \end{aligned}$$

Similarly, letting

$$\hat{J}_n = \begin{pmatrix} J & & & \\ & J & & \\ & & \ddots & \\ & & & J \end{pmatrix} \in \mathrm{SL}(2n,\mathbb{C}),$$

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. 12, we will give proofs that also apply to exceptional groups.)

Let us begin by briefly recalling the prototypical case (cf. 6.44).

(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
- $\Delta\colon G_F \to G \times G^\sigma$ defined by $\Delta(g) = \big(g, \sigma(g)\big)$.

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). □

(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 $x, y \in L^{p+q}$,
- $G = \{\, g \in \mathrm{SL}(p+q, \mathbb{C}) \mid B(gx, gy) = B(x,y)$, 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. □

The same argument can easily be applied to $\mathrm{Sp}(p,q)$ (see Exer. 10:27). 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 $L[x_{1,1}, \ldots, x_{\ell,\ell}]$, 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 $F[x_{1,1}, \ldots, x_{\ell,\ell}]$, 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
$$\mathcal{Q} = \{\, Q \in F[x_{1,1}, \ldots, x_{\ell,\ell}] \mid Q(G_F) = 0\,\}.$$

(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 $\mathrm{SL}(n, \mathbb{R})$. □

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. 11, 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.** *If at least one of the simple factors of G is compact, then every irreducible, arithmetic lattice in G is cocompact.*

Proof. Every irreducible, arithmetic lattice can be constructed by restriction of scalars (see 6.53), so this is the assertion of Cor. 6.50. Alternatively, the proof of Cor. 9.20 provides an argument that does not rely on restriction of scalars. □

(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. 11) 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. □

(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. □

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
$$\begin{aligned} \sigma_1(\alpha) &= \sqrt{2} + \sqrt{3} && \approx 3.1 \\ \sigma_2(\alpha) &= -\sqrt{2} + \sqrt{3} && \approx 0.3 \\ \sigma_3(\alpha) &= \sqrt{2} - \sqrt{3} && \approx -0.3 \\ \sigma_4(\alpha) &= -\sqrt{2} - \sqrt{3} && \approx -3.1, \end{aligned}$$
- $G = \mathrm{SO}\big((\alpha+2)x_1^2 + (\alpha-2)x_2^2 + (\alpha-4)x_3^2 + (\alpha-4)x_4^2 + (\alpha-4)x_5^2\big)^\circ$, 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

$$\begin{aligned} \sigma_1(\alpha+2, \alpha-2, \alpha-4, \alpha-4, \alpha-4) &\approx (5.1, 1.1, -0.9, -0.9, -0.9) && \sim (+,+,-,-,-) \\ \sigma_2(\alpha+2, \alpha-2, \alpha-4, \alpha-4, \alpha-4) &\approx (2.3, -1.7, -3.7, -3.7, -3.7) && \sim (+,-,-,-,-) \\ \sigma_3(\alpha+2, \alpha-2, \alpha-4, \alpha-4, \alpha-4) &\approx (1.7, -2.3, -4.3, -4.3, -4.3) && \sim (+,-,-,-,-) \\ \sigma_4(\alpha+2, \alpha-2, \alpha-4, \alpha-4, \alpha-4) &\approx (-1.1, -5.1, -7.1, -7.1, -7.1) && \sim (-,-,-,-,-), \end{aligned}$$

we have $\prod_{\sigma \in S_\infty} G^\sigma \approx H$. □

The same elementary method applies to any product of various groups of the form $\mathrm{SO}(p,q)$.

(10.25) **Proposition.** *If $p_1, \ldots, p_r$ are natural numbers with $0 \le p_j \le n$, 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

$$p_1 \ge p_2 \ge \cdots \ge p_r.$$

Let

- $m_1, \ldots, m_t \ge 2$ be square-free positive integers that are pairwise relatively prime;
- $F = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_t})$,
- $\mathcal{O} = \mathbb{Z}(\sqrt{m_1}, \ldots, \sqrt{m_t})$,
- $\alpha = \sqrt{m_1} + \cdots + \sqrt{m_t}$,
- $S_\infty = \{\sigma_1, \ldots, \sigma_r\}$, with $\sigma_1(\alpha) > \sigma_2(\alpha) > \cdots > \sigma_r(\alpha)$,
- $a_\ell \in \mathbb{Q}$ with $\max\{\, \sigma_j(\alpha) \mid \ell > p_j \,\} < a_\ell < \min\{\, \sigma_j(\alpha) \mid \ell \le p_j \,\}$, for $\ell = 1, \ldots, n$,
- $G = \mathrm{SO}\big(\sum_{\ell=1}^n (\alpha - a_\ell) x_\ell^2\big)$, and
- $\Gamma = G_{\mathcal{O}}$.

From the choice of a_ℓ, we have $\sigma_j(\alpha - a_\ell) > 0$ if and only if $\ell \le p_j$. Hence, $G^{\sigma_j} \cong \mathrm{SO}(p_j, n-p_j)$. □

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 (see 10.52 and 10.53).

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 10.52).

- For $j = 1, \ldots, r$ and $\ell = 1, \ldots, n$, define $\varepsilon_\ell^j = \begin{cases} + & \text{if } \ell \le p_j \\ - & \text{if } \ell > p_j. \end{cases}$
- Because $\Delta(F)$ is dense in $\prod_{\sigma \in S_\infty} F_\sigma$ (see 10.53), we may choose, for each $\ell = 1, \ldots, n$, some $a_\ell \in F$, such that the sign (positive or negative) of $\sigma_j(a_\ell)$ is ε_ℓ^j for $j = 1, \ldots, r$.
- Then the signature of $\sigma_j\bigl(\sum_{\ell=1}^n a_\ell x_\ell^2\bigr)$ is $(p_j, n - p_j)$, for $j = 1, \ldots, r$.

□

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

$$\mathrm{SO}(n, \mathbb{C})^s \times \prod_{j=1}^r \mathrm{SO}(p_j, n - p_j) \tag{10.26}$$

(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 (10.26). 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 quaternion algebras over algebraic number fields.

(10.27) **Definition** (cf. 3.22(2)). 1) For any field F, and any nonzero $\beta, \gamma \in F$, the corresponding *quaternion algebra* over F is the ring

$$D = D_{\beta,\gamma}(F) = \{\, a + bi + cj + dk \mid a, b, c, d \in F \,\},$$

where

- addition is defined in the obvious way, and
- multiplication is determined by the relations

$$i^2 = \beta,\ j^2 = \gamma,\ ij = k = -ji,$$

together with the requirement that every element of F is in the center of D.

2) Define $\tau_r \colon D \to D$ by

$$\tau_r(a_0 + a_1 i + a_2 j + a_3 k) = a_0 + a_1 i - a_2 j + a_3 k.$$

This is the *reversion* on D.

3) For $B \in \mathrm{GL}(n, D)$, with $\tau_r\bigl(B^T\bigr) = B$, let

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

(10.28) **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. 10:11).

3) The proof of Lem. 10.11 shows that $D_{b^2,\gamma}(F) \cong \mathrm{Mat}_{2\times 2}(F)$, for any nonzero $b, \gamma \in F$ (see Exer. 10:12).

(10.29) **Lemma.** *If β is any nonzero element of an algebraic number field F, then*

$$D_{\beta,-1}(F) \otimes_F F_\infty \cong \begin{cases} \mathrm{Mat}_{2\times 2}(\mathbb{C}) & \textit{if } F_\infty = \mathbb{C}, \\ \mathrm{Mat}_{2\times 2}(\mathbb{R}) & \textit{if } F_\infty = \mathbb{R} \textit{ and } \beta > 0, \\ \mathbb{H} & \textit{if } F_\infty = \mathbb{R} \textit{ and } \beta < 0. \end{cases}$$

(Here, $\otimes_F$ denotes the usual tensor product of algebras over F.)

Proof. We have $D_{\beta,-1}(F) \otimes_F F_\infty \cong D_{\beta,-1}(F_\infty)$, so the conclusions follow from the observations in Eg. 10.28. □

(10.30) **Proposition.** *If β is any nonzero element of an algebraic number field F, and $D = D_{\beta,-1}(F)$, then*

$$\mathrm{SU}(B; D, \tau_r) \otimes_F F_\infty \cong \begin{cases} \mathrm{SO}(2n, \mathbb{C}) & \textit{if } F_\infty = \mathbb{C}, \\ \mathrm{SO}(p, 2n-p) \ (\textit{for some } p) & \textit{if } F_\infty = \mathbb{R} \textit{ and } \beta > 0, \\ \mathrm{SO}(n, \mathbb{H}) & \textit{if } F_\infty = \mathbb{R} \textit{ and } \beta < 0. \end{cases}$$

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 involution τ_r. □

It is now easy to prove that isotypic groups of type D_n have irreducible lattices.

(10.31) **Proposition.** *If $p_1, \ldots, p_r$ are natural numbers with $0 \le p_j \le 2n$, 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 $\sigma_1, \ldots, \sigma_{r+t}$ and exactly s imaginary places (see 10.52).
- Because $\Delta(F)$ is dense in $\prod_{\sigma \in S_\infty} F_\sigma$ (see 10.53), 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 $r + 1 \le j \le r + t$.
- 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
  - $\mathrm{diag}_n\big(\mathrm{Mat}_{2\times 2}(\mathbb{R})^\dagger\big)$ be the set of $n \times n$ diagonal matrices with entries in $\mathrm{Mat}_{2\times 2}(\mathbb{R})^\dagger$.

  For $j = 1, \ldots, r$, we have $\sigma_j(\beta) > 0$ and $F_{\sigma_j} = \mathbb{R}$, so

  $$D_{\sigma_j(\beta),-1}\big(\sigma_j(F)\big) \otimes_{\sigma(F_j)} F_{\sigma_j} \cong \mathrm{Mat}_{2\times 2}(\mathbb{R});$$

  hence, σ_j induces an embedding

  $$\sigma_j' \colon D \hookrightarrow \mathrm{Mat}_{2\times 2}(\mathbb{R}),$$

with $\sigma_j'(D^\dagger) \subset \mathrm{Mat}_{2\times 2}(\mathbb{R})^\dagger$. Because $\Delta(F)$ is dense in $\prod_{\sigma\in S_\infty} F_\sigma$, we see that

$$\left\{ \left(\sigma_j'(B)\right)_{j=1}^r \mid B \in \mathrm{diag}_n(D^\dagger) \right\} \text{ is dense in } \prod_{j=1}^r \mathrm{diag}_n\left(\mathrm{Mat}_{2\times 2}(\mathbb{R})^\dagger\right),$$

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 $j = 1, \ldots, r$.

- From Prop. 10.30, we see that $\prod_{\sigma\in S_\infty} \mathrm{SU}(B; D, \tau_r) \cong H$.

□

Fairly similar considerations apply to groups 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.

(10.32) **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 (6.20) implies that Γ is arithmetic, so Prop. 6.53 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

$$\phi\colon \prod_{\sigma\in S^\infty} H^\sigma \to G,$$

  with compact kernel,

such that $\phi\big(\Delta(H_{\mathcal{O}})\big)$ is commensurable with Γ.

From the classification of arithmetic lattices (see Fig. 10.1), we see that (after replacing H by an isogenous group) the group H must be described in 10.43(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 $\mathbb{Q}$-rank$(\Gamma) \geq 1$ (see 9.19), so there must be a nontrivial isotropic vector v in D^3 (see Fig. 10.1). Arguing as in §7C, we see there is a basis of D^3, for which the matrix of B is

$$[B] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & p \end{pmatrix},$$

for some $p \in D$ (see Exer. 10:15). Thus, we may assume

$$H_F = \mathrm{SU}\big([B]; D, \tau_r\big).$$

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 10.49(5)). Since $\mathrm{Id}_{2\times 2}$ is the image of $1 \in D$ under the isomorphism $D \otimes_F \mathbb{R} \to$

$\mathrm{Mat}_{2\times 2}(\mathbb{R})$, we see that

$$H^\sigma = \mathrm{SU}\big(\sigma\big([B]\big); D^\sigma \otimes_{\sigma(F)} \mathbb{R}\big) \cong \mathrm{SO}\left(\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * & * \end{pmatrix}\right).$$

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 an absolutely simple group?

(10.33) **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. 10:17 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.

(10.34) **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. 10:19).

(10.35) **Definition.** Suppose G_1 and G_2 are defined over F (as algebraic groups over F_∞).

- A map $\phi\colon G_1 \to G_2$ 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 $\phi_1\colon G \to G_1$ and $\phi_2\colon G \to G_2$. This is an equivalence relation.

(10.36) **Remark.**

1) Note that if $\phi\colon G \to H$ 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. 6:5).
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. 10:20). 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. 10:21). 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.

10F. Absolutely simple classical groups

From Prop. 6.53, 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 §10E). 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 3.21 and 3.22). Theorem 10.43 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 $\mathrm{SO}(8, \mathbb{C})$ (see 10.48)).

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 F includes groups, such as $\mathrm{SL}(n, D)$, that are based on central division algebras over F (see 10.37). The interested reader can find an introduction to the theory of central division algebras (including how to construct them) in §10I. For most of our purposes, it suffices to have some familiarity with the special case of quaternion algebras (see 10.27 and 10.39(3)).

(10.37) **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.

(10.38) **Remark.**
- D is an *algebra* over F is (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).

(10.39) **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 $\mathrm{N}_{\mathrm{red}}(x) \neq 0$, for every nonzero $x \in D_{\beta,\gamma}(F)$ (see Exer. 10:23), where the *reduced norm* of $x = a + bi + cj + dk \in D_{\beta,\gamma}(F)$ is
$$\mathrm{N}_{\mathrm{red}}(x) = a^2 + b^2\beta + c^2\gamma - d^2\beta\gamma.$$
Note that this is consistent with (2).

(10.40) **Definition.** Let D be a central division algebra. A map $\tau\colon D \to D$ is an *involution* if $\tau^2 = \mathrm{Id}$ 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.)

(10.41) **Example.** Let D be a quaternion division algebra. Then

1) The map $\tau_c\colon D \to D$ defined by
$$\tau_c(a + bi + cj + dk) = a - bi - cj - dk$$
is an involution. It is called the *standard involution* of D, or the *conjugation* on D.
2) The map $\tau_r\colon D \to D$ defined by
$$\tau_r(a + bi + cj + dk) = a + bi - cj + dk$$
is an involution. It is called the *reversion* on D.

(10.42) **Definition.** Let τ be an involution of a central division algebra D over F. A *Hermitian form* on D^n is a map $B\colon D^n \times D^n \to D$, 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 $B(x, ay) = \tau(a)B(x, y)$ for all $a \in D$ and $x, y \in D^n$, and
- $B(y, x) = \tau\big(B(x, y)\big)$ for all $x, y \in D^n$.

The Hermitian form B is *nondegenerate* if, for each $x \in D^n$, there exists $y \in D^n$, such that $B(x, y) \neq 0$.

(10.43) **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 involution τ_c, and some 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 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 involution τ whose restriction to L is the Galois automorphism of L over F, and some Hermitian form B on D^n.*

(10.44) **Remark.** Theorem 10.43 is directly analogous to the classification of the classical simple Lie groups (see 3.21 and 3.22). 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 $\mathrm{SU}(p, q)$.

It is not difficult to find the complexification of each of the groups in Thm. 10.43 (see 10.46). This is similar to the calculations that appear in §10B.

(10.45) **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 10.64). This number d is called the *degree* of D. We remark that $\dim_F D = d^2$.

(10.46) **Proposition.** *The notation of each part of this proposition is taken from the corresponding part of Thm. 10.43. 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) $\mathrm{SU}(B; D, \tau) \otimes_F \mathbb{C} \cong \mathrm{SL}(dn, \mathbb{C})$.

(10.47) **Warning.** 1) In 10.43(6), the division algebra D is **not** central over F. (Its center is L.) In all other cases, D is central over F.

2) Theorem 10.43 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 $\mathrm{SL}(2, F)$ in $\mathrm{PSL}(2, F)$ has infinite index (cf. Exer. 6:5).

(10.48) **Remark.** The assumption that G is not of type D_4 cannot be omitted from Thm. 10.43. 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 of order 2. By combining the automorphism of $\mathrm{SL}(n, \mathbb{C})$ with the Galois automorphism of L, unitary groups, such as $\mathrm{SU}(p, q)$ are constructed. The group $\mathrm{SU}(p, q)$ 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. To specify that the outer automorphism is of order 2, one may say that $\mathrm{SU}(p, q)$ 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. 10.43 (and are neither orthogonal, symplectic, nor unitary); for $J \in \mathrm{PSO}(8, L)$, satisfying a certain technical condition, let
$$G_F = \{\, g \in \mathrm{PSO}(8, L) \mid J\phi(g) = \sigma(g)J \,\}.$$
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. 11 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. 24.1).) So $\mathrm{SO}(8, \mathbb{C})$ is a special case.

10G. The arithmetic lattices in classical groups

Theorem 10.43 provides a classification of all the irreducible, arithmetic lattices in semisimple Lie groups. Namely, for each group H_F listed in Thm. 10.43, we know that $H_{\mathcal{O}}$ is (isomorphic to) a lattice in $\prod_{\sigma \in S_\infty} H^\sigma$.

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 Prop. 10.46 when $F \not\subset \mathbb{R}$. We now consider the remaining case, where F is real.

(10.49) **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. 10.43. 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) $\mathrm{SU}(B; D, \tau) \otimes_F \mathbb{R} \cong \begin{cases} \mathrm{SU}(p, q) & \text{if } L \not\subset \mathbb{R} \\ \mathrm{SL}(2dn, \mathbb{R}) & \text{if } L \subset \mathbb{R} \text{ and } D \text{ splits over } \mathbb{R}, \\ \mathrm{SL}(nd, \mathbb{H}) & \text{if } L \subset \mathbb{R} \text{ and } D \text{ does not split over } \mathbb{R}. \end{cases}$

The values of p and q, where they appear, can be calculated from B.

10H. Very basic algebraic number theory

(10.50) **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 $\mathrm{cont}\big(f(x)\big) = 1$, where $\mathrm{cont}\big(f(x)\big)$ denotes the *content* of $f(x)$, that is, the greatest common divisor of the coefficients of $f(x)$. Then, letting $d_j = \mathrm{cont}\big(g_j(x)\big)$, we have

$$n = \mathrm{cont}\big(nf(x)\big) = \mathrm{cont}\big(g_1(x) g_2(x)\big) = d_1 d_2$$

(see Exer. 10:28). Thus, letting $\hat{g}_j(x) = \frac{1}{d_j} g_j(x) \in \mathbb{Z}[x]$, we have

$$f(x) = \frac{g_1(x) g_2(x)}{d_1 d_2} = \hat{g}_1(x) \hat{g}_2(x),$$

so $f(x)$ is reducible over $\mathbb{Z}$, as desired. □

(10.51) **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*

simple factor of G	irreducible lattice Γ	$\mathbb{Q}$-rank(Γ)	reference	m or $p+q$
$\mathrm{SL}(m,\mathbb{R})$	$\mathrm{SL}(n,\mathcal{O}_D)$	$n-1$	(1), $F\subset\mathbb{R}$	$m=dn$
	$\mathrm{SU}(B;\mathcal{O}_D,\tau)$	D-subspace	(6), $F\subset\mathbb{R}$	$m=dn$
$\mathrm{SO}(p,q)$	$\mathrm{SO}(B;\mathcal{O}_F)$	F-subspace	(3), $F\subset\mathbb{R}$	$p+q=n$
	$\mathrm{SU}(B;\mathcal{O}_D,\tau_r)$	D-subspace	(5), $F\subset\mathbb{R}$	$p+q=2n$, $d=2$
$\mathrm{SU}(p,q)$	$\mathrm{SU}(B;\mathcal{O}_D,\tau)$	D-subspace	(6), $F\subset\mathbb{R}$	$p+q=dn$
$\mathrm{Sp}(p,q)$	$\mathrm{SU}(B;\mathcal{O}_D,\tau_c)$	D-subspace	(4), $F\subset\mathbb{R}$	$p+q=n$, $d=2$
$\mathrm{Sp}(2m,\mathbb{R})$	$\mathrm{Sp}(2n,\mathcal{O}_F)$	n	(2), $F\subset\mathbb{R}$	$m=n$
	$\mathrm{SU}(B;\mathcal{O}_D,\tau_c)$	D-subspace	(4), $F\subset\mathbb{R}$	$m=n$, $d=2$
$\mathrm{SL}(m,\mathbb{C})$	$\mathrm{SL}(n,\mathcal{O}_D)$	$n-1$	(1), $F\not\subset\mathbb{R}$	$m=dn$
	$\mathrm{SU}(B;\mathcal{O}_D,\tau)$	D-subspace	(6), $F\not\subset\mathbb{R}$	$m=dn$
$\mathrm{SO}(m,\mathbb{C})$	$\mathrm{SO}(B;\mathcal{O}_F)$	F-subspace	(3), $F\not\subset\mathbb{R}$	$m=n$
	$\mathrm{SU}(B;\mathcal{O}_D,\tau_r)$	D-subspace	(5), $F\not\subset\mathbb{R}$	$m=2n$, $d=2$
$\mathrm{Sp}(2m,\mathbb{C})$	$\mathrm{Sp}(2n,\mathcal{O}_F)$	n	(2), $F\not\subset\mathbb{R}$	$m=n$
	$\mathrm{SU}(B;\mathcal{O}_D,\tau_c)$	D-subspace	(4), $F\not\subset\mathbb{R}$	$m=n$, $d=2$
$\mathrm{SL}(m,\mathbb{H})$	$\mathrm{SL}(n,\mathcal{O}_D)$	$n-1$	(1), $F\subset\mathbb{R}$	$m=dn/2$, d even
	$\mathrm{SU}(B;\mathcal{O}_D,\tau)$	D-subspace	(6), $F\subset\mathbb{R}$	$m=dn/2$, d even
$\mathrm{SO}(m,\mathbb{H})$	$\mathrm{SU}(B;\mathcal{O}_D,\tau_r)$	D-subspace	(5), $F\subset\mathbb{R}$	$m=n$, $d=2$

Figure 10.1. The irreducible arithmetic lattices in G. The list is not complete for groups of type D_4.

- $f(x)\equiv ax^n \pmod p$, *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 10.50), 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 $b_1,b_2\in\mathbb{Z}_p\smallsetminus\{0\}$ and $m_1,m_2\in\mathbb{N}$, such that $g_j(x)\equiv b_jx^{m_j} \pmod p$. Since

$$m_1+m_2=n=\deg f(x)=\deg\bigl(g_1(x)g_2(x)\bigr)=\deg g_1(x)+\deg g_2(x),$$

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. □

(10.52) **Proposition.** *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.*

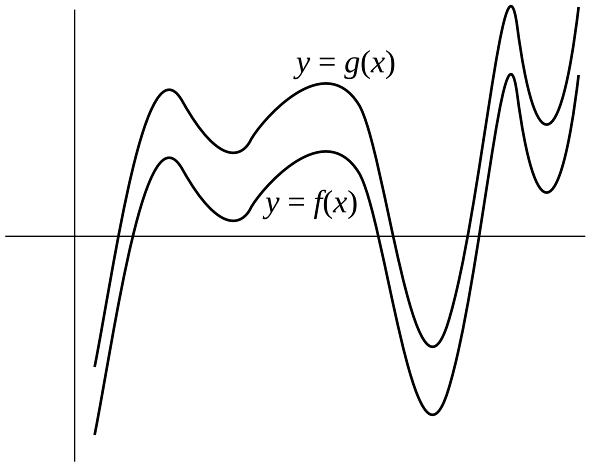

Figure 10.2. The polynomials $f(x)$ and $g(x)$ have the same number of real roots.

Proof. Let $n = r + 2s$. It suffices to find an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ 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 $g(x) \in \mathbb{Q}[x]$, 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 $a_1, \ldots, a_r$, 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) $g(x) \in \mathbb{Z}[x]$,
2) $g(x) \equiv x^n \pmod{p^2}$, and
3) $\min\{\, g(t) \mid g'(t) = 0 \,\} > p$

(see Exer. 10:29).

Let $f(x) = g(x) - p$. From (2), we know that $f(x) \equiv x^n - p \pmod{p^2}$, so the Eisenstein Criterion (10.51) implies that f is irreducible. From (3), we see that $f(x)$, like $g(x)$, has exactly r real roots (see Fig. 10.2). □

The following is a special case of the Weak Approximation Theorem.

(10.53) **Proposition.** *If F is any algebraic number field, then $\Delta(F)$ is dense in $\prod_{\sigma \in S^\infty} F_\sigma$.*

Proof. This follows from Exer. 6:22, which states that $\Delta(F)$ is a $\mathbb{Q}$-form of $\prod_{\sigma \in S^\infty} F_\sigma$. □

10I. Central division algebras over number fields

The following lemma provides an analogue, for a central division algebra D, of the ring of integers in an algebraic number field F.

(10.54) **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 $\{v_0, v_1, \ldots, v_r\}$ 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 $j,k \in \{0,\ldots,r\}$, 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 $\{1, mv_1, \ldots, mv_r\}$. □

(10.55) **Example.** Let σ be Galois automorphism of some quadratic extension $L = F[\sqrt{\beta}]$ of a field F; we may write ${}^{\sigma}z$, instead of $\sigma(z)$.

1) Define an 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 $L[\sigma] \cong \mathrm{Mat}_{2\times 2}(F)$, via the map
$$x + iy \mapsto \begin{pmatrix} x & y \\ \beta y & x \end{pmatrix} \qquad \text{and} \qquad x + iy \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

2) The quaternion algebra $D_{\beta,\gamma}(F)$ can be obtained by a very slight modification of the preceding construction: simply replace (1a) with
$$(1\mathrm{a}')\ \sigma^2 = \gamma.$$

The construction of Eg. 10.55 can be generalized to field extensions of degree > 2:

(10.56) **Example.** Let $\Delta = \mathrm{Gal}(L/F)$, for some Galois extension L of a field F. Let us use $\circ$ to denote the group operation in Δ.

1) Define an F-algebra
$$L[\Delta] = \left\{ \sum_{\sigma\in\Delta} a_\sigma \sigma \;\middle|\; a_\sigma \in L \right\}$$
with multiplication given by
(a) $\sigma_1\sigma_2 = \sigma_1 \circ \sigma_2$ for $\sigma_1, \sigma_2 \in \Delta$, and
(b) $\sigma z = {}^{\sigma}z\sigma$ for $z \in L$ and $\sigma \in \Delta$.
Then $L[\Delta] \cong \mathrm{Mat}_{d\times d}(F)$, where $d = |L : F|$ (see Exer. 10:30).

2) For $\alpha\colon \Delta \times \Delta \to L^{\times}$, let $L^{\alpha}[\Delta]$ be defined as in (1), but replacing (1a) with
$$(1\mathrm{a}')\ \sigma_1\sigma_2 = \alpha(\sigma_1,\sigma_2)\,(\sigma_1 \circ \sigma_2).$$
In order for this multiplication to be associative, we require that α satisfy the *cocycle equation*

(10.57) $$\alpha(\sigma_1,\sigma_2)\,\alpha(\sigma_1\sigma_2,\sigma_3) = \alpha(\sigma_1,\sigma_2\sigma_3)\ {}^{\sigma_1}\big(\alpha(\sigma_2,\sigma_3)\big)$$

(see Exer. 10:31).

For example, the quaternion algebra $D_{\beta,\gamma}$ is obtained by taking
$$\alpha(\sigma_1,\sigma_2) = \begin{cases} 1 & \text{if } \sigma_1 = 1 \text{ or } \sigma_2 = 1, \\ \gamma & \text{if } \sigma_1 = \sigma_2 = \sigma. \end{cases}$$

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 section.

(10.58) **Theorem.** *If D is a central division algebra over an algebraic number field F, then there is a Galois extension L of F, and a 2-cocycle $\alpha\colon \mathrm{Gal}(L/F)\times\mathrm{Gal}(L/F)\to L^\times$, such that $D\cong L^\alpha\big[\mathrm{Gal}(L/F)\big]$.*

(10.59) **Remark.** I do not know whether Thm. 10.69 remains valid when F is allowed to be any field (of characteristic 0), rather than only an algebraic number field.

(10.60) **Definition.** Let L be a Galois extension of a field F, and let $\Delta=\mathrm{Gal}(L/F)$.

- A function $\alpha\colon \Delta\times\Delta\to L^\times$ is a 2-*cocycle* if (10.57) holds.
- For any $\beta\colon\Delta\to L^\times$, define $\delta\beta\colon\Delta\times\Delta\to L^\times$ by
$$\delta\beta(\sigma_1,\sigma_2)=\frac{\beta(\sigma_1)\,{}^{\sigma_1}\!\big(\beta(\sigma_2)\big)}{\beta(\sigma_1\sigma_2)}.$$
Then $\delta\beta$ is a 2-cocycle. It is called the *coboundary* of β.
- Define
$$H^2(L/F)=\frac{Z^2(L/F)}{B^2(L/F)},$$
where $Z^2(L/F)$ is the set of 2-cocycles, and $B^2(L/F)$ is the set of coboundaries. (Note that $Z^2(L/F)$ is an abelian group under pointwise multiplication, and $B^2(Z/F)$ is a subgroup.) This is the (second) *Galois cohomology group* of L over F.

(10.61) **Proposition.** *Let $\overline{F}$ be the algebraic closure of an algebraic number field F. There is a one-to-one correspondence between $H^2(\overline{F}/F)$ and the isomorphism classes of central division algebras over F.*

Proof. Suppose $\alpha\in H^2(L/F)$, for some (finite) Galois extension L of F. Then $L^\alpha\big[\mathrm{Gal}(L/F)\big]$ may not be a division algebra, but it turns out that it is always a central simple algebra over F. So the Wedderburn Theorem (10.72) tells us that it is isomorphic to $\mathrm{Mat}_{n\times n}(D_\alpha)$, 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 $B^2(L/F)$ (see Exer. 10:32), so f is well defined.

Theorem 10.58 shows that f is surjective.

A reasonable effort shows that f is injective. □

Now, the following deep theorem shows that there are infinitely many central division algebras over any algebraic number field.

(10.62) **Theorem** (Brauer-Hasse-Noether Theorem)**.** *If $\overline{F}$ is the algebraic closure of an algebraic number field F, then*
$$H^2(\overline{F}/F)\cong(\mathbb{Z}_2)^r\oplus\frac{\mathbb{Q}}{\mathbb{Z}}\oplus\frac{\mathbb{Q}}{\mathbb{Z}}\oplus\frac{\mathbb{Q}}{\mathbb{Z}}\oplus\frac{\mathbb{Q}}{\mathbb{Z}}\oplus\cdots,$$
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 (10.72), there is a corresponding central division algebra $D_{\mathbb{R}}$ over $\mathbb{R}$. Thus, we have a natural homomorphism
$$H^2(\overline{F}/F)\to H^2(\mathbb{C}/\mathbb{R}).$$
It is well-known that there are only two central division algebras over $\mathbb{R}$, namely $\mathbb{R}$ and $\mathbb{H}$, so $H^2(\mathbb{C}/\mathbb{R})\cong\mathbb{Z}_2$.

For each prime p, we have a p-adic field $\mathbb{Q}_p$. For the same reason as above, there is a natural homomorphism
$$H^2(\overline{F}/F) \to H^2(\overline{\mathbb{Q}_p}/\mathbb{Q}_p).$$
Classifying the central division algebras over $\mathbb{Q}_p$ yields the conclusion that $H^2(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$.

By combining the preceding paragraphs, we see that there is a natural homomorphism
$$H^2(\overline{F}/F) \to \mathbb{Z}_2 \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \frac{\mathbb{Q}}{\mathbb{Z}} \oplus \cdots .$$
To complete the proof, one shows that the map is injective, and that its image is
$$\{\, (a_0, a_1, \ldots) \mid a_0 + a_1 + \cdots = 0 \,\},$$
where we realize $\mathbb{Z}_2$ as the subgroup $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ of $\mathbb{Q}/\mathbb{Z}$. □

(10.63) **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 $D \otimes_F L \cong \operatorname{Mat}_{d\times d}(L)$, 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:

(10.64) **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 $\mathbb{C}$:

(10.65) **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 $f\colon D \otimes_F D \to \operatorname{End}_F(D)$ 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 (10.70) implies that $f(L \otimes_F D)$ is isomorphic to $\operatorname{Mat}_{d\times d}(E)$, where
$$E = \operatorname{End}_{f(L\otimes_F D)}(D) = f(L \otimes 1) \cong L$$
(see Exer. 10:33). Since $L \otimes_F D$ is simple (see Exer. 10:34), we know that f is faithful, so $L \otimes_F D \cong f(L \otimes_F D)$. □

(10.66) **Theorem** (Noether-Skolem Theorem)**.** *Let A and B be simple F-subalgebras of a central simple algebra R over a field F. If $\phi\colon A \to B$ is any ring isomorphism, such that $\phi|_F = \mathrm{Id}$, then there is an invertible element r of R, such that $\phi(a) = r^{-1}ar$, for all $a \in A$.*

(10.67) **Corollary.** *Let L be a maximal subfield of a central division algebra D over a field F, and assume that L is a Galois extension of F.*

1) *For each $\sigma \in \operatorname{Gal}(L/F)$, there is an invertible element $r_\sigma \in R$, such that $r_\sigma^{-1} x r_\sigma = \sigma(x)$, for all $x \in L$. The element r_σ is uniquely determined up to scalar multiplication by a nonzero element of L.*
2) *The set $\{\, r_\sigma \mid \sigma \in \operatorname{Gal}(L/F) \,\}$ is a basis of D over L.*
3) *We have $|L : F| = d$, where d is the degree of D over F.*

Proof. (1) The existence of r_σ is obtained by taking $A = B = L$ in Thm. 10.66. Uniqueness follows from the observation that the maximality of L implies $C_D(L) = L$.

(2) Let
$$R = L[r_\sigma]_{\sigma\in\operatorname{Gal}(L/F)} = \left\{ \sum_{\sigma\in\operatorname{Gal}(L/F)} a_\sigma r_\sigma \;\middle|\; a_\sigma \in L \right\} \subset D,$$

so R is a subring of D. Because $C_D(R) = F$, we see, by arguing as in the proof of Prop. 10.65, that $R \otimes_F D \cong \mathrm{Mat}_{n\times n}(F)$, where $n = \dim_F D$. Then

$$(\dim_F R)n \geq \dim_F(R \otimes_F D) = \dim_F \mathrm{Mat}_{n\times n}(F) = n^2,$$

so $\dim_F R \geq n = \dim_F D$. Therefore $R = D$. Hence, $\{ r_\sigma \}$ spans D over L.

The set $\mathrm{Gal}(L/F)$ is linearly independent over L (as a subset of $\mathrm{End}_F(L)$). (For example, this follows from Prop. 10.53.) Therefore, $\{ r_\sigma \}$ is linearly independent over L.

(3) From (2), we have

$$\dim_L D = |\,\mathrm{Gal}(L/F)| = |L : F|,$$

so

$$d^2 = \dim_F D = (\dim_L D)(\dim_F L) = |L : F|^2.$$

□

(10.68) **Remark.** The degree of D over F is equal to $|L : F|$ for every maximal subfield L of D (even if L is not Galois).

(10.69) **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.*

Proof of Thm. 10.58. Let

- L be a maximal subfield of D, such that L is a cyclic, Galois extension of F (see 10.69),
- $\{ r_\sigma \mid \sigma \in \mathrm{Gal}(L/F)$ as in (10.67).

For $\sigma, \tau \in \mathrm{Gal}(L/K)$, the uniqueness of $r_{\sigma\tau}$ implies that $r_\sigma r_\tau = \alpha(\sigma,\tau) r_{\sigma\tau}$, for some $\alpha(\sigma,\tau) \in L^\times$. Then $D \cong D_{L,\alpha}$. □

We conclude the section with two standard results in ring theory that were used above.

(10.70) **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*
- *$E = \mathrm{End}_R(M)$.*

Then

1) *E is a division algebra,*
2) *R is isomorphic to $\mathrm{Mat}_{d\times d}(E)$, where d is the dimension of M as a vector space over E, and*
3) *after identifying R with $\mathrm{Mat}_{d\times d}(E)$, 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 $c \in \mathrm{End}_R(M)$). 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 $\{m_1, \ldots, m_d\}$ of M, and any $v_1, \ldots, v_d \in M$, we wish to show that there exists $r \in R$ with $rm_j = v_j$ for $j = 1, \ldots, d$. That is, we wish to show $R(m_1, \ldots, m_d) = M^d$. Let us consider only M^2, rather than M^d. The proof can be completed by induction (see Exer. 10:35).

Given $m_1, m_2 \in M$, such that m_1 and m_2 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

(10.71) the projection of $R(m_1, m_2)$ to $M \times \{0\}$ is all of $M \times \{0\}$.

Similarly, the intersection $R(m_1, m_2) \cap \big(\{0\} \times M\big)$ is an R-submodule of $\{0\} \times M$. Because M is irreducible, there are only two possibilities to consider.

Case 1. Assume $R(m_1, m_2) \cap \big(\{0\} \times M\big) = \{0\} \times M$. This means that $\{0\} \times M \subset R(m_1, m_2)$. On the other hand, (10.71) can be restated as $\big(\{0\} \times M\big) + R(m_1, m_2) = M^2$. Therefore

$$R(m_1, m_2) = \big(\{0\} \times M\big) + R(m_1, m_2) = M^2.$$

Case 2. Assume $R(m_1, m_2) \cap \big(\{0\} \times M\big) = \{(0,0)\}$. For each $x \in M$, we know, from (10.71), 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 $f \colon M \to M$.

Because the graph of f is an R-submodule of M^2, it is straightforward to verify that $f \in \operatorname{End}_R(M)$. 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. □

The following is an easy special case of Wedderburn's Theorem on the structure of semisimple artinian rings.

(10.72) **Corollary** (Wedderburn). *If A is a central simple algebra over a field F, then A is isomorphic to* $\operatorname{Mat}_{n \times n}(D)$, *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.

To shorten the argument, let us assume that A has an identity element, so the module $A/\mathfrak{m}$ is obviously nontrivial. Thus, 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 (10.70) implies that $A \cong \operatorname{Mat}_{n \times n}(D)$. □

10J. Notes

Theorem 10.43 is due to Weil [Wei]. A proof (together with Props. 10.6 and 10.46) appears in [P-R, §2.3, pp. 78–92]. We copied (10.6), (10.43), and (10.46) from the summary on [P-R, p. 92], except that [P-R] uses a different description of the groups in 10.43(5) (see Exer. 10:26).

As will be explained in Chap. 11, 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. 10.32. 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 [Bor3, Thm. 8.9] for a proof of Rem. 10.36(2).

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) $\phi\big(\{1,i,j,k\}\big)$ 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 $\mathrm{SL}(n,\mathbb{H}) \otimes \mathbb{C} \cong \mathrm{SL}\big(n, \mathrm{Mat}_{2\times 2}(\mathbb{C})\big)$. [*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 $\mathrm{SL}\big(n, \mathrm{Mat}_{d\times d}(\mathbb{C})\big) \cong \mathrm{SL}(dn,\mathbb{C})$.

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 $F_2 \to SO(3)$ 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 $\Delta(x) = \big(x, \sigma(x)\big)$ and $\eta(x,y) = (y,x)$, the diagram

$$\begin{array}{ccc} L & \xrightarrow{\Delta} & \mathbb{R} \oplus \mathbb{R} \\ \Big\downarrow \tau & & \Big\downarrow \eta \\ L & \xrightarrow{\Delta} & \mathbb{R} \oplus \mathbb{R}. \end{array}$$

commutes.]

10:10) Use (10.52) and (10.53) 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 $D_{b^2\beta, c^2\gamma}(F) \cong D_{\beta,\gamma}(F)$, for any nonzero $b, c \in F$. [*Hint:* An isomorphism is given by $1 \mapsto 1$, $i \mapsto bi$, $j \mapsto cj$, $k \mapsto bck$.]

10:12) Show $D_{1,\gamma}(F) \cong \mathrm{Mat}_{2\times 2}(F)$, for any field F, and any $\gamma \in F$.

10:13) 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.

10:14) 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.

10:15) 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 involution τ of D. Show 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 $B(y,y) = -1$.

10:16) 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. 10.32.]

10:17) 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).]

10:18) Show that if G is absolutely simple, then G is simple.

10:19) 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.

10:20) Assume $G \subset \mathrm{SL}(\ell, \mathbb{R})$ is defined over $\mathbb{Q}$, and let $\Gamma = G_{\mathbb{Z}}$. Show that if $\phi\colon G \to H$ 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 $f \in \mathbb{Q}[x_{1,1}, \ldots, x_{\ell,\ell}]$, 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 $f(\Gamma_n) \subset \mathbb{Z}$.]

10:21) Suppose
  - $\phi\colon G_1 \to G_2$ 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.]

10:22) Show $\mathrm{N}_{\mathrm{red}}(xy) = \mathrm{N}_{\mathrm{red}}(x)\, \mathrm{N}_{\mathrm{red}}(y)$ for all elements x and y of a quaternion algebra $D_{\beta,\gamma}(F)$.

10:23) Show that the quaternion algebra $D_{\beta,\gamma}(F)$ is a central division algebra over F if and only if $\mathrm{N}_{\mathrm{red}}(x) \neq 0$, for every nonzero $x \in D_{\beta,\gamma}(F)$. [*Hint:* If $\mathrm{N}_{\mathrm{red}}(x) \neq 0$, then the conjugate of x is a multiplicative inverse of x. If $\mathrm{N}_{\mathrm{red}}(x) = 0$, then x is a zero divisor.]

10:24) 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 $R_x\colon D \to D$ by $R_x(v) = vx$, and show that R_x is an L-linear transformation.
  (d) For each $x \in D$, show $\det(R_x) = \mathrm{N}_{\mathrm{red}}(x)$.

10:25) Let τ be an involution on a division algebra D.
  (a) For any $J \in \mathrm{Mat}_{n\times n}(D)$, define $B_J\colon D^n \times D^n \to D$ by

$$B_J(x,y) = \tau(x^T) J y$$

  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 there exists $J \in \mathrm{Mat}_{n\times n}(D)$, such that $B = B_J$.

10:26) Show that if $G = \mathrm{SU}(B; D, \tau_r)$, as in 10.43(5), then there is a skew-Hermitian form B' on D^n, with respect to the standard involution τ_c, such that $G = \mathrm{SU}(B'; D, \tau_c)$. [*Hint:* Use the fact that $\tau_r(x) = j^{-1}\tau_c(x)j$.]

10:27) 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.]

10:28) Show that $\mathrm{cont}\big(g_1(x)g_2(x)\big) = \mathrm{cont}\big(g_1(x)\big) \cdot \mathrm{cont}\big(g_2(x)\big)$, for $g_1(x), g_2(x) \in \mathbb{Z}[x]$. [*Hint:* Assume $\mathrm{cont}\big(g_j(x)\big) = 1$. If $p | \mathrm{cont}\big(g_1(x)g_2(x)\big)$, then $\overline{g_1(x)}\,\overline{g_2(x)} = 0$ in $\mathbb{Z}_p[x]$.]

10:29) (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

$$\min\{\, |h(t)| \mid h'(t) = 0 \,\} = k^n \min\{\, |g(t)| \mid g'(t) = 0 \,\}.$$

10:30) Define $L[\Delta]$ as in Eg. 10.56(1). Show $L[\Delta] \cong \mathrm{Mat}_{d\times d}(F)$, where $d = |L : F|$. [*Hint:* Identifying L with F^d yields a natural homomorphism $L[\Delta] \to \mathrm{Mat}_{d\times d}(F)$.]

10:31) Show that $L^\alpha[\Delta]$ is associative if and only if (10.57) holds for all $\sigma_1, \sigma_2, \sigma_3 \in \Delta$.

10:32) Let L be a Galois extension of a field F. Show that if $\alpha_1 \in \alpha_2 Z^2(L/F)$, then $L^{\alpha_1}\big[\mathrm{Gal}(L/F)\big] \cong L^{\alpha_2}\big[\mathrm{Gal}(L/F)\big]$. [*Hint:* Define $f\colon L^{\alpha_1}\big[\mathrm{Gal}(L/F)\big] \to L^{\alpha_2}\big[\mathrm{Gal}(L/F)\big]$ by $f(\sigma) = \beta(\sigma)\,\sigma$.]

10:33) Let F, D, and f be as in the proof of Prop. 10.65.

(a) Show that $\mathrm{End}_{f(1\otimes D)}(D) = f(D \otimes 1)$.

(b) Show that if L is any maximal subfield of D, then $\mathrm{End}_{f(L\otimes_F D)}(D) = f(L \otimes 1)$.

10:34) 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.

10:35) Prove 10.70(2) and 10.70(2). [*Hint:* Given linearly independent $m_1, \ldots, m_k \in M$, show that $R(m_1, \ldots, m_k) = M^k$. Assume, by induction on k, that $R(m_1, \ldots, m_k)$ projects onto all of M^{k-1}. Then $R(m_1, \ldots, m_k)$ is either M^k or the graph of an R-equivariant map $f\colon M^{k-1} \to M$. The restriction of f to each factor of M_{k-1} defines an element f_i of E. We have $f_1(m_1) + \cdots + f_{k-1}(m_{k-1}) = f(m_1, \ldots, m_{k-1}) = m_k$.]

Appendix I

Assumed Background

This appendix is very preliminary!!! There are no explanations yet, and more topics will be added.

I.A. Riemmanian 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 $\langle \cdot \mid \cdot \rangle$ on V.
- A *Riemannian manifold* is a smooth manifold M, together with the choice of an inner product $\langle \cdot \mid \cdot \rangle_x$ on the tangent space $T_x M$, for each $x \in M$, such that $\langle \cdot \mid \cdot \rangle_x$ varies smoothly as x varies.
- The *norm* $\|v\|_x$ of a vector $v \in T_x M$ is $\sqrt{\langle v \mid v \rangle_x}$.

(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

$$\big\langle (u_1, u_2) \mid (v_1, v_2) \big\rangle_{(p_1,p_2)} = \langle u_1 \mid v_1 \rangle_{p_1} + \langle u_2 \mid v_2 \rangle_{p_2}$$

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 $c \colon [a,b] \to M$ 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 $\gamma\colon [a,b] \to M$ is a *length-minimizing geodesic* if $\|\gamma'(t)\|_{\gamma(t)}$ is constant (independent of t) and $\text{length}(\gamma) = d\big(\gamma(a), \gamma(b)\big)$.
- A smooth curve $\gamma\colon I \to M$ 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.

(I.5) **Proposition.** *Let M be a Riemannian manifold. For any $(p,v) \in TM$, there is a geodesic $\gamma\colon (-\epsilon,\epsilon) \to M$, for some $\epsilon > 0$, such that $\gamma(0) = p$ and $\gamma'(0) = v$.*

Furthermore, if $\overline{\gamma}\colon I \to M$, is any geodesic, such that $\overline{\gamma}(0) = p$ and $\overline{\gamma}'(0) = v$, then $\overline{\gamma}(t) = \gamma(t)$ for all $t \in I \cap (-\epsilon,\epsilon)$.

(I.6) **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.7) **Corollary.** *For each 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 $\exp_p\colon V \to M$ 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.8) **Definition.** Note that, by identifying T_pM 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.9) **Definition.** Let M be a Riemannian manifold.

- M is *geodesically complete* if, for every geodesic segment $\gamma\colon (-\epsilon,\epsilon) \to M$, there is a geodesic $\overline{\gamma}\colon \mathbb{R} \to M$, such that $\overline{\gamma}(t) = \gamma(t)$, for all $t \in (-\epsilon,\epsilon)$.
- M is *complete* if all Cauchy sequences converge.

(I.10) **Proposition.** *A Riemannian manifold is geodesically complete if and only if it is complete.*

I.C. Lie groups

(I.11) **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 $G \times G \to G\colon (g,h) \mapsto gh$ and $G \to G\colon g \mapsto g^{-1}$ are smooth.

(I.12) **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.13) **Definition.** Let G be a topological group, and X be a topological space.

- An *action* of G on X is a homomorphism $\phi\colon G \to \text{Perm}(X)$, where $\text{Perm}(X)$ is the group of all permutations of X. Equivalently, an *action* is a function $\alpha\colon G \times X \to X$, such that
  - $\alpha(1,x) = x$ for all $x \in X$, and
  - $\alpha\big(g, \alpha(h,x)\big) = \alpha(gh,x)$ for $g,h \in G$ and $x \in X$.

  The equivalence is obtained by taking $\alpha(g,x) = \big(\phi(g)\big)(x)$.

- 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.14) **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 $\operatorname{Stab}_\Gamma(p) = \{\, \gamma \in \Gamma \mid \gamma p = p \,\}$. This is a closed subgroup of Γ.

(I.15) **Proposition.** *If Γ acts freely and properly discontinuously on a topological space M, then the natural map $M \to \Gamma \backslash M$ is a covering map.*

(I.16) **Proposition.** *If M is any locally compact metric space, then* $\operatorname{Isom}(M)$ *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* $\operatorname{Isom}(M)$ *on M is proper; that is, for every compact subset C of M, the set*
$$\{\, \phi \in \operatorname{Isom}(M) \mid \phi(C) \cap C \neq \emptyset \,\}$$
is compact.

If M is a smooth manifold, then the topological group $\operatorname{Isom}(M)$ *can be given the structure of a Lie group, so that the action of* $\operatorname{Isom}(M)$ *on M is smooth.*

(I.17) **Notation.** For any topological group G, we use G° to denote the identity component of G.

(I.18) **Proposition.** *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.19) **Definition.**

- The measure μ of Prop. I.18 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.20) **Proposition.** *There is a continuous homomorphism $\Delta\colon G \to \mathbb{R}^+$, 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 $\phi_g\colon G \to G$ 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. □

(I.21) **Definition.** The function Δ defined in Prop. I.20 is called the *modular function* of G.

(I.22) **Warning.** Some authors call $1/\Delta$ the modular function, because they use the conjugation $g^{-1}Ag$, instead of gAg^{-1}.

(I.23) **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 $\Delta(g) = |\det(\mathrm{Ad}_G\, g)|$ for all $g \in G$.*

(I.24) **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.18(1)).

($\Rightarrow$) We prove the contrapositive. Let C be a compact subset of nonzero measure. Because $G \times G \to G\colon (g,h) \mapsto gh^{-1}$ 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 $g_1 C$ is disjoint from C. Continuing, we construct, by induction on n, a sequence $\{g_n\}$ of elements of G, such that $\{g_n C\}$ is a collection of pairwise disjoint sets. They all have the same measure (since μ is G-invariant), so we conclude that

$$\mu(G) \geq \mu\Bigl(\bigcup_{n=1}^{\infty} g_n C\Bigr) = \infty.$$

□

(I.25) **Example.** Important examples of Lie groups are:

- $\mathrm{SL}(n,\mathbb{R})$, the group consisting of all $n \times n$ real matrices of determinant 1;
- $\mathrm{SO}(n) = \{\, g \in \mathrm{SL}(n,\mathbb{R}) \mid gg^T = \mathrm{Id}\,\}$, where g^T denotes the transpose of the matrix g; and
- $\mathrm{SO}(m,n) = \{\, g \in \mathrm{SL}(m+n,\mathbb{R}) \mid gI_{m,n}g^T = I_{m,n}\,\}$, where $I_{m,n}$ is the $(m+n) \times (m+n)$ diagonal matrix whose diagonal entries are $1, 1, \ldots, 1, -1, -1, \ldots, -1$, where there are m 1's, followed by n $-1's$.

(I.26) **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.27) **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

$$\mathrm{Ad}_G\, g\colon \mathfrak{g} \to \mathfrak{g}$$

by $\mathrm{Ad}_G\, g = df_e$, where $f\colon G \to G$ is defined by $f(x) = gxg^{-1}$.

Then $\mathrm{Ad}_G\colon G \to \mathrm{GL}(\mathfrak{g})$ is a homomorphism.

(I.28) **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.29) **Theorem.** *If G is semisimple, then*

1) $\mathrm{Ad}\, G$ *is a normal subgroup of* $\mathrm{Aut}(\mathfrak{g})$ *and*
2) *the quotient group* $\bigl(\mathrm{Aut}(\mathfrak{g})\bigr)/(\mathrm{Ad}\, G)$ *is finite.*

I.D. Galois theory and field extensions

(I.30) **Theorem.** *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 $\mathbb{C}$.*

(I.31) **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 $\phi\colon F[x] \to F[\alpha]$ defined by $\phi\big(g(x)\big) = g(\alpha)$ is a surjective ring homomorphism whose kernel is I. □

(I.32) **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 $\sigma\colon F[\alpha] \to F[\beta]$ with $\sigma(\alpha) = \beta$.*

(I.33) **Corollary.** *Let F be a subfield of $\mathbb{C}$, and let $\sigma\colon F \to \mathbb{C}$ be any embedding. Then σ extends to an automorphism $\hat{\sigma}$ of $\mathbb{C}$.*

(I.34) **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.35) **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 $\sigma|_F = \mathrm{Id}$.*

(I.36) **Definition.** Let F be a subfield of a field L. Then

$$\mathrm{Gal}(L/F) = \{\, \sigma \in \mathrm{Aut}(L) \mid \sigma|_F = \mathrm{Id} \,\}.$$

This is the *Galois group* of L over F.

(I.37) **Proposition.** *If F is any subfield of a field L of characteristic 0, then $\#\,\mathrm{Gal}(L/F) = |L : F|$.*

(I.38) **Corollary.** *If F is any subfield of a field L 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 $\mathrm{Gal}(L/F)$.*

Proof. Given K, with $F \subset K \subset L$, let $H_K = \mathrm{Gal}(L/K)$. Conversely, given a subgroup H of $\mathrm{Gal}(L/F)$, let

$$K_H = \{\, x \in L \mid \sigma(x) = x,\ \forall \sigma \in H \,\}$$

be the fixed field of H. □

(I.39) **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.40) **Proposition.** *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 $t = p/1 \in \mathbb{Z}$. □

(I.41) **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

$$f(m\alpha) = \sum_{k=0}^{n} (m^{n-k-1} b_k)(m\alpha)^k = m^{n-1} \sum_{k=0}^{n} b_k \alpha^k = m^{n-1} g(\alpha) = m^{n-1} \cdot 0 = 0.$$

□

(I.42) **Proposition.** *The set of algebraic numbers is a subring of $\mathbb{C}$.*

I.E. Polynomial rings and the Nullstellensatz

(I.43) **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.44) **Theorem.** *If R is Noetherian, then the polynomial ring $R[x]$ is Noetherian.*

(I.45) **Corollary.** *For any field F, the polynomial ring $F[x_1, \ldots, x_s]$ (in any number of variables) is Noetherian.*

There are many equivalent formulations of the following important theorem.

(I.46) **Theorem** (Nullstellensatz)**.** *Let*

- *F be an algebraically closed field,*
- *$F[x_1, \ldots, x_r]$ be a polynomial ring over F, and*
- *I be any proper ideal of $F[x_1, \ldots, x_r]$.*

Then there exist $a_1, \ldots, a_r \in F$, such that $f(a_1, \ldots, a_r) = 0$ for all $f(x_1, \ldots, x_r) \in I$.

(I.47) **Corollary.** *Let*

- *F be an algebraically closed field,*
- *$F[x_1, \ldots, x_r]$ be a polynomial ring over F, and*

- $\mathfrak{m}$ *be any maximal ideal of* $F[x_1, \ldots, x_r]$.

Then

1) *the natural inclusion* $F \hookrightarrow F[x_1, \ldots, x_r]/\mathfrak{m}$ *is an isomorphism, and*
2) *there exist* $a_1, \ldots, a_r \in F$*, such that* $\mathfrak{m} = \langle (x_1 - a_1), \ldots, (x_r - a_r) \rangle$.

(I.48) **Corollary.** *Let F be a subfield of a field L. If L is finitely generated as an F-algebra (that is, if there exist $c_1, \ldots, c_r \in L$, such that $L = F[c_1, \ldots, c_r]$), then L is algebraic over F.*

Proof. There is a surjective homomorphism $\phi\colon F[x_1, \ldots, x_r] \to L$, defined by $\phi\big(f(x_1, \ldots, x_r)\big) = f(c_1, \ldots, c_r)$. Since L is a field, the kernel $\mathfrak{m}$ of ϕ is a maximal ideal. By passing to the algebraic closure, we may assume, without loss of generality, that F is algebraically closed, we conclude that there exist $a_1, \ldots, a_r$ as in Cor. I.47. Then

$$L = \phi\big(F[x_1, \ldots, x_r]\big) \cong \frac{F[x_1, \ldots, x_r]}{\mathfrak{m}} \cong F.$$

So $L = F$ is algebraic over F. □

(I.49) **Corollary.** *If B is any finitely generated subring of $\mathbb{C}$, then there is a nontrivial homomorphism $\phi\colon B \to \overline{\mathbb{Q}}$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.*

Proof. We have $B = \mathbb{Z}[b_1, \ldots, b_r]$, for some $b_1, \ldots, b_r \in B$. There is a homomorphism

$$\phi\colon \overline{\mathbb{Q}}[x_1, \ldots, x_r] \to \mathbb{C},$$

defined by $\phi\big(f(x_1, \ldots, x_r)\big) = f(b_1, \ldots, b_r)$. 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

$$B \cong \frac{\overline{\mathbb{Q}}[x_1, \ldots, x_r]}{I} \to \frac{\overline{\mathbb{Q}}[x_1, \ldots, x_r]}{\mathfrak{m}} \cong \overline{\mathbb{Q}}$$

(see I.47(1)). □

I.F. Notes

Need to track down references for this stuff!!!

Bibliography

[AC-B] N. A'Campo and M. Burger: Réseaux arithmétiques et commensurateur d'après G.A. Margulis, *Invent. Math.* 116 (1994) 1–25. 6H

[Alp] R. C. Alperin: An elementary account of Selberg's Lemma, *L'Enseign. Math.* 33 (1987) 269–273. 5K

[Bor1] A. Borel: Density properties for certain subgroups of semi-simple groups without compact components, *Ann. Math.* 72 (1960) 179–188. 5K

[Bor2] A. Borel: Compact Clifford-Klein forms of symmetric spaces, *Topology* 2 (1963) 111–122. 12B, 12B, 12B, 12.6

[Bor3] A. Borel: *Introduction aux Groupes Arithmétiques,* Act. Sci. Ind. #1341, Hermann, Paris, 1969. 5K, 10J

[Bor4] A. Borel: *Linear Algebraic Groups*, 2nd ed., Springer, New York, 1991. 3F

[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. 10J

[B-HC] A. Borel and Harish-Chandra: Arithmetic subgroups of algebraic groups. *Ann. Math.* (2) 75 (1962) 485–535. 2C

[B-S] A. Borel and J. P. Serre: Corners and arithmetic groups, *Comment. Math. Helvetici* 48 (1973) 436–491. 2C

[Car] É. Cartan: Les groupes réels simples finis et continus, *Ann. Sci. École Norm. Sup.* 31 (1914) 263–355. 3F

[Che] C. Chevalley: Sur certains groupes simples, *Tohoku Math. J.* (2) 7 (1955) 14–66. 12B

[Cor] K. Corlette: Archimedean superrigidity and hyperbolic geometry, *Ann. Math.* 135, no. 1 (1992) 165–182. 6H

[Dan] S. G. Dani: On ergodic quasi-invariant measures of group automorphism, *Israel J. Math.* 43 (1982) 62–74. 5K

[Del] P. Deligne: Extensions centrales non résiduellement finies de groupes arithmétiques, *Comptes Rendus Acad. Sci. Paris*, Ser. A, 287 (1978) 203–208. 23E

[D-M] P. Deligne and G. D. Mostow: Monodromy of hypergeometric functions and non-lattice integral monodromy, *Publ. Math. IHES* 63 (1986) 5–89. 6H

[E-N] R. Ellis and M. Nerurkar: Enveloping semigroup in ergodic theory and a proof of Moore's ergodicity theorem, in: J. C. Alexander., ed., *Dynamical systems* (*College Park, MD, 1986–87*), 172–179, Lecture Notes in Math. #1342, Springer, Berlin-New York, 1988. MR **90g:**28024 19F

[Far] B. Farb: The quasi-isometry classification of lattices in semisimple Lie groups, *Math. Res. Letters* 4 (1997), no. 5, 705–718. 16D

[Fur] H. Furstenberg: A note on Borel's Density Theorem, *Proc. Amer. Math. Soc.* 55 (1976) 209–212. 5K

[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. 5K

[Ghy] É. Ghys: Actions de réseaux sur le cercle, *Invent. Math.* 137 (1999) 199–231.

[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 6H, 7E

[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. 6H

[Har] P. de la Harpe: Free groups in linear groups, *L'Enseign. Math.* 29 (1983) 129–144. 5K

[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 revised english edition is coming soon from the American Mathematical Society.)

[Hat] T. Hattori: Asymptotic geometry of arithmetic quotients of symmetric spaces. *Math. Z.* 222 (1996) 247–277. MR **98d:**53061 2C

[Hel1] S. Helgason: *Differential Geometry and Symmetric Spaces.* American Mathematical Society, Providence, RI, 1962. ISBN 0-8218-2735-9 1D

[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.) 1D, 2C, 3F, 4J

[Hoc1] G. Hochschild: *The Structure of Lie Groups*, Holden-Day, San Francisco, 1965. 4J

[Hoc2] G. Hochschild: *Basic Theory of Algebraic Groups and Lie Algebras*, Springer, New York, 1981. 4J

[Hum1] J. E. Humphreys: *Introduction to Lie Algebras and Representation Theory.* Springer, Berlin Heidelberg New York, 1972. 3F

[Hum2] J. E. Humphreys: *Linear Algebraic Groups.* Springer, Berlin Heidelberg New York, 1975.

[Iwa] K. Iwasawa: On some types of topological groups, *Ann. Math.* 50 (1949) 507–558. 4J

[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. 10J

[Kaz] D. A. Kazhdan: Connection of the dual space of a group with the structure of its closed subgroups, *Func. Anal. Appl.* 1 (1967) 63–65.

[Lub] A. Lubotzky: *Discrete Groups, Expanding Graphs and Invariant Measures.* Birkhäuser, Boston, 1994.

[LMR] A. Lubotzky, S. Mozes, M. S. Raghunathan: Cyclic subgroups of exponential growth and metrics on discrete groups, *Comptes Rendus Acad. Sci. Paris*, Ser. A, 317 (1993), no. 8, 735–740. MR **94m:**22009

[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. 6H

[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. 6H

[Mar2] G. A. Margulis: Discrete groups of motions of manifolds of non-positive curvature, *Amer. Math. Soc. Translations* 109 (1977) 33–45. 6H

[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 [Rag1], 1977. English translation in: *Invent. Math.* 76 (1984) 93–120. 6H

[Mar4] G. A. Margulis: *Discrete Subgroups of Semisimple Lie Groups.* Springer, Berlin Heidelberg New York, 1991. 5K, 6H, 7E, 16E, 16H, 21G, 23.1

[Mil] J. Millson: Real vector bundles with discrete structure group, *Topology* 18 (1979), no. 1, 83–89. MR **82i:**55016 23E

[Mos1] G. D. Mostow: Self adjoint groups, *Ann. Math.* 62 (1955) 44–55. 3F

[Mos2] G. D. Mostow: Existence of a non-arithmetic lattice in $\mathrm{SU}(2,1)$, *Proc. Nat. Acad. Sci. USA* 75 (1978) 3029–3033. 6H

[Mos3] G. D. Mostow: *Strong Rigidity of Locally Symmetric Spaces.* Princeton University Press, Princeton, 1973. 16H

[M-T] G. D. Mostow and T. Tamagawa: On the compactness of arithmetically defined homogeneous spaces, *Ann. Math.* 76 (1961) 446–463. 2C

[Oh] H. Oh: Discrete subgroups generated by lattices in opposite horospherical subgroups, *J. Algebra* 203 (1998) 621–676. 12

[P-R] V. Platonov and A. Rapinchuk: *Algebraic Groups and Number Theory.* Academic Press, Boston, 1994. 1D, 3F, 4J, 5K, 7C, 10J

[Pra] G. Prasad: Strong rigidity of $\mathbb{Q}$-rank 1 lattices, *Invent. Math.* 21 (1973) 255–286. 16H

[Rag1] M. S. Raghunathan: *Discrete Subgroups of Lie Groups.* Springer, Berlin Heidelberg New York, 1972. 1D, 5K, 16H, 10J

[Rag2] M. S. Raghunathan: Torsion in cocompact lattices in coverings of $\mathrm{Spin}(2, n)$ *Math. Ann.* 266 (1984) 403–419; corrigendum 303 (1995) 575–578. MR **86k:**22027, MR **96g:**22019 23E, 23.29

[Rag3] M. S. Raghunathan: A note on generators for arithmetic subgroups of algebraic groups, *Pacific J. Math.* 152 (1992) 365–373.

[Ser] J.–P. Serre: *Trees*, Springer, New York, 1980.

[Tit] J. Tits: Free subgroups in linear groups, *J. Algebra* 20 (1972) 250–270. 5K

[Var] V. S. Varadarajan: *Lie Groups, Lie Algebras, and their Representations.* Springer, Berlin Heidelberg New York, 1984.

[Ven1] T. N. Venkataramana: On the arithmeticity of certain rigid subgroups, C. R. Acad. Sci. Paris 316, Sér. I (1993) 321–326. 6H

[Ven2] T. N. Venkataramana: On systems of generators of arithmetic subgroups of higher rank groups. *Pacific J. Math.* 166 (1994) 193–212.

[Vin] E. B. Vinberg: Discrete groups generated by reflections in Lobachevsky spaces, *Math. USSR Sbornik* 1 (1967) 429–444. 6H

[Wan] S. P. Wang: The dual space of semi-simple Lie groups, *Amer. J. Math.* 91 (1969) 921–937.

[Wei] A. Weil: Algebras with involution and the classical groups, *J. Indian Math. Soc.* 24 (1960) 589–623. 3F, 10J

[Wig] D. Wigner: Un théorème de densité analytique pour les groupes semisimples, *Comment. Math. Helvetici* 62 (1987) 390–416. 5K

[Zim] R. J. Zimmer: *Ergodic Theory and Semisimple Groups.* Birkhäuser, Boston, 1984. 5K, 6H, 19F

Index