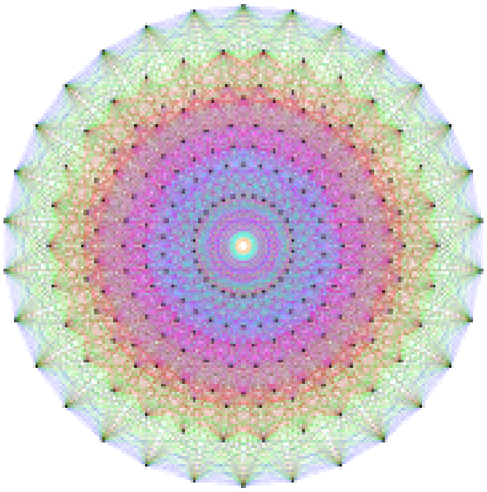
Introduction to Lie Groups

MAT 4144/5158

Winter 2015



Alistair Savage

Department of Mathematics and Statistics

University of Ottawa

Contents

Preface iii

1 Introduction and first examples 1
- 1.1 Category theoretic definitions 1
- 1.2 The circle: $\mathbb{S}^1$ 3
- 1.3 Matrix representations of complex numbers 5
- 1.4 Quaternions 6
- 1.5 Quaternions and space rotations 9
- 1.6 Isometries of $\mathbb{R}^n$ and reflections 14
- 1.7 Quaternions and rotations of $\mathbb{R}^4$ 16
- 1.8 $\mathrm{SU}(2) \times \mathrm{SU}(2)$ and $\mathrm{SO}(4)$ 17

2 Matrix Lie groups 20
- 2.1 Definitions 20
- 2.2 Finite groups 21
- 2.3 The general and special linear groups 21
- 2.4 The orthogonal and special orthogonal groups 21
- 2.5 The unitary and special unitary groups 22
- 2.6 The complex orthogonal groups 23
- 2.7 The symplectic groups 23
- 2.8 The Heisenberg group 25
- 2.9 The groups $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{S}^1$ and $\mathbb{R}^n$ 26
- 2.10 The Euclidean group 26
- 2.11 Homomorphisms of Lie groups 27

3 Topology of Lie groups 29
- 3.1 Connectedness 29
- 3.2 Polar Decompositions 33
- 3.3 Compactness 36
- 3.4 Lie groups 37

4 Maximal tori and centres 39
- 4.1 Maximal tori 39
- 4.2 Centres 44
- 4.3 Discrete subgroups and the centre 45

5 Lie algebras and the exponential map 47
5.1 The exponential map onto SO(2) 47
5.2 The exponential map onto SU(2) 48
5.3 The tangent space of SU(2) 49
5.4 The Lie algebra $\mathfrak{su}(2)$ of SU(2) 51
5.5 The exponential of square matrices 52
5.6 The tangent space 55
5.7 The tangent space as a Lie algebra 59
5.8 Complex Lie groups and complexification 61
5.9 The matrix logarithm 64
5.10 The exponential mapping 65
5.11 The logarithm into the tangent space 67
5.12 Some more properties of the exponential 71
5.13 The functor from Lie groups to Lie algebras 73
5.14 Lie algebras and normal subgroups 78
5.15 The Campbell–Baker–Hausdorff Theorem 79

6 Covering groups 85
6.1 Simple connectedness 85
6.2 Simply connected Lie groups 88
6.3 Three Lie groups with tangent space $\mathbb{R}$ 89
6.4 Three Lie groups with the cross-product Lie algebra 90
6.5 The Lie group-Lie algebra correspondence 91
6.6 Covering groups 95
6.7 Subgroups and subalgebras 97

7 Further directions of study 101
7.1 Lie groups, Lie algebras, and quantum groups 101
7.2 Superalgebras and supergroups 101
7.3 Algebraic groups and group schemes 102
7.4 Finite simple groups 102
7.5 Representation theory 103

Preface

These are notes for the course *Introduction to Lie Groups* (cross-listed as MAT 4144 and MAT 5158) at the University of Ottawa. At the title suggests, this is a first course in the theory of Lie groups. Students are expected to a have an undergraduate level background in group theory, ring theory and analysis. We focus on the so-called matrix Lie groups since this allows us to cover the most common examples of Lie groups in the most direct manner and with the minimum amount of background knowledge. We mention the more general concept of a general Lie group, but do not spend much time working in this generality.

After some motivating examples involving quaternions, rotations and reflections, we give the definition of a matrix Lie group and discuss the most well-studied examples, including the classical Lie groups. We then study the topology of Lie groups, their maximal tori, and their centres. In the second half of the course, we turn our attention to the connection between Lie algebras and Lie groups. We conclude with a discussion of simply connected Lie groups and covering groups.

Acknowledgement: The author would like to thank the students of MAT 4144/5158 for making this such an enjoyable course to teach, for asking great questions, and for pointing out typographical errors in the notes.

Alistair Savage Ottawa, 2015.

Course website: `http://alistairsavage.ca/mat4144/`

Chapter 1

Introduction and first examples

In this chapter we introduce the concept of a Lie group and then discuss some important basic examples.

1.1 Category theoretic definitions

We will motivate the definition of a Lie group in category theoretic language. Although we will not use this language in the rest of the course, it provides a nice viewpoint that makes the analogy with usual groups precise.

Definition 1.1.1 (Category)**.** A *category* $\mathcal{C}$ consists of

- a class of *objects* $\operatorname{ob}\mathcal{C}$,
- for each two objects $A, B \in \operatorname{ob}\mathcal{C}$, a class $\hom(A, B)$ of *morphisms* between them,
- for every three objects $A, B, C \in \operatorname{ob}\mathcal{C}$, a binary operation
  $$\hom(B, C) \times \hom(A, B) \to \hom(A, C)$$
  called *composition* and written $(f, g) \mapsto f \circ g$

such that the following axioms hold:

- *Associativity.* If $f \in \hom(A, B)$, $g \in \hom(B, C)$ and $h \in \hom(C, D)$, then $h \circ (g \circ f) = (h \circ g) \circ f$.
- *Identity.* For every object X, there exists a morphism $1_X \in \hom(X, X)$ such that for every morphism $f \in \hom(A, B)$ we have $1_B \circ f = f = f \circ 1_A$.

Definition 1.1.2 (Terminal object)**.** An object T of a category $\mathcal{C}$ is a *terminal object* if there exists a single morphism $X \to T$ for every $X \in \operatorname{ob}\mathcal{C}$.

Examples 1.1.3.

Objects	Morphisms	Terminal object(s)	Product
Sets	Set maps	Singletons	Cartesian product
Vector spaces	Linear maps	0	Tensor product
Topological spaces	Continuous maps	Single point	Cartesian product (product topology)
Smooth manifolds	Smooth maps	Single point	Cartesian product (induced manifold structure)
Algebraic varieties	Algebraic maps	Single point	Product variety

Recall that a *group* is a set G together with a *maps of sets* $G \times G \to G$, often called multiplication and denoted $(g, h) \mapsto g \cdot h$, satisfying the following properties:

- *Associativity.* For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- *Identity element.* $\exists\, e \in G$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$.
- *Inverse element.* $\forall\, a \in G\ \exists\, b \in G$ such that $a \cdot b = b \cdot a = e$. One can show that the element b is unique and we call it the *inverse* of a and denote it a^{-1}.

Note that G is a *set* and the multiplication is a map of *sets*. We can generalize this definition to (almost) any other category.

Definition 1.1.4 (Group object)**.** Suppose we have a category $\mathcal{C}$ with finite products and a terminal object 1. Then a *group object* of $\mathcal{C}$ is an object $G \in \operatorname{ob}\mathcal{C}$ together with morphisms

- $m\colon G \times G \to G$ (thought of as the "group multiplication"),
- $e\colon 1 \to G$ (thought of as the "inclusion of the identity element"),
- $\iota\colon G \to G$ (thought of as the "inversion operator"),

such that the following properties are satisfied:

- m is associative: $m \circ (m \times 1_G) = m \circ (1_G \times m)$ as morphisms $G \times G \times G \to G$.
- e is a two-sided unit of m:

  $$m \circ (1_G \times e) = p_1,$$
  $$m \circ (e \times 1_G) = p_2,$$

  where $p_1 : G \times 1 \to G$ and $p_2 : 1 \times G \to G$ are the canonical projections.
- ι is a two-sided inverse for m: if $d\colon G \to G \times G$ is the diagonal map, and $e_G\colon G \to G$ is the composition

  $$G \to 1 \xrightarrow{e} G,$$

  then $m \circ (1_G \times \iota) \circ d = e_G$ and $m \circ (\iota \times 1_G) \circ d = e_G$.

We can now generalize the definition of group by considering group objects in other categories.

Category	Group objects
Sets	Groups
Topological spaces	Topological groups
Smooth manifolds	Lie groups
Algebraic varieties	Algebraic groups

So a *Lie group* is just a group object in the category of smooth manifolds. It is a group which is also a finite-dimensional (real) smooth manifold, and in which the group operations of multiplication and inversion are smooth maps. Roughly, Lie groups are "continuous groups".

Examples 1.1.5. (a) Euclidean space $\mathbb{R}^n$ with vector addition as the group operation.

(b) The circle group $\mathbb{S}^1$ (complex numbers with absolute value 1) with multiplication as the group operation.

(c) General linear group $\mathrm{GL}(n, \mathbb{R})$ with matrix multiplication.

(d) Special linear group $\mathrm{SL}(n, \mathbb{R})$ with matrix multiplication.

(e) Orthogonal group $\mathrm{O}(n, \mathbb{R})$ and special orthogonal group $\mathrm{SO}(n, \mathbb{R})$.

(f) Unitary group $\mathrm{U}(n)$ and special unitary group $\mathrm{SU}(n)$.

(g) *Physics:* Lorentz group, Poincaré group, Heisenberg group, gauge group of the Standard Model.

Many of the above examples are *linear groups* or *matrix Lie groups* (subgroups of some $\mathrm{GL}(n, \mathbb{R})$). In this course, we will focuss on linear groups instead of the more abstract full setting of Lie groups.

Exercises.

1.1.1. Show that the notions of *group* and *group object in the category of sets* are equivalent.

1.2 The circle: $\mathbb{S}^1$

Consider the plane $\mathbb{R}^2$. If we use column vector notation for points of $\mathbb{R}^2$, then rotation about the origin through an angle θ is a linear transformation corresponding to (left multiplication by) the matrix

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

This rotation corresponds to the map

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto R_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}.$$

Rotating first by θ and then by φ corresponds to multiplication by R_θ and then by R_φ or, equivalently, by $R_\varphi R_\theta$. So composition of rotation corresponds to multiplication of matrices.

Definition 1.2.1 (SO(2))**.** The group $\{R_\theta \mid \theta \in \mathbb{R}\}$ is called the *special orthogonal group* SO(2). The term *special* refers to the fact that their determinant is one (check!) and the term *orthogonal* refers to the fact that they do not change distances (or that $R_\theta R_\theta^T = 1$ for any θ) – we will come back to this issue later.

Another way of viewing the plane is as the set of complex numbers $\mathbb{C}$. Then the point (x, y) corresponds to the complex number $x + iy$. Then rotation by θ corresponds to multiplication by

$$z_\theta = \cos\theta + i\sin\theta$$

since

$$\begin{aligned} z_\theta(x + iy) &= (\cos\theta + i\sin\theta)(x + iy) \\ &= x\cos\theta - y\sin\theta + i(x\sin\theta + y\cos\theta). \end{aligned}$$

Composition of rotations corresponds to multiplication of complex numbers since rotating by θ and then by φ is the same as multiplying by $z_\varphi z_\theta$.

Note that

$$\mathbb{S}^1 := \{z_\theta \mid \theta \in \mathbb{R}\}$$

is the precisely the set of complex numbers of absolute value 1. Thus $\mathbb{S}^1$ is the circle of radius 1 centred at the origin. Therefore, $\mathbb{S}^1$ has a geometric structure (as a circle) and a group structure (via multiplication of complex numbers). The multiplication and inverse maps are both smooth and so $\mathbb{S}^1$ is a Lie group.

Definition 1.2.2 (Matrix group and linear group)**.** A *matrix group* is a set of invertible matrices that is closed under multiplication and inversion. A *linear group* is a group that is isomorphic to a matrix group.

Remark 1.2.3. Some references use the term *linear group* to mean a group consisting of matrices (i.e. a matrix group as defined above).

Example 1.2.4. We see that SO(2) is a matrix group. Since $\mathbb{S}^1$ is isomorphic (as a group) to SO(2) (Exercise 1.2.2), $\mathbb{S}^1$ is a linear group.

Exercises.

1.2.1. Verify that if $u, v \in \mathbb{R}^2$ and $R \in \mathrm{SO}(2)$, then the distance between the points u and v is the same as the distance between the points Ru and Rv.

1.2.2. Prove that the map $z_\theta \mapsto R_\theta$, $\theta \in \mathbb{R}$, is a group isomorphism from $\mathbb{S}^1$ to $\mathrm{SO}(2)$.

1.3 Matrix representations of complex numbers

Define

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The set of matrices

$$\tilde{\mathbb{C}} := \{a\mathbf{1} + b\mathbf{i} \mid a, b \in \mathbb{R}\} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$$

is closed under addition and multiplication, and hence forms a subring of $M_2(\mathbb{R})$ (Exercise 1.3.1).

Theorem 1.3.1. *The map*

$$\mathbb{C} \to \tilde{\mathbb{C}}, \quad a + bi \mapsto a\mathbf{1} + b\mathbf{i},$$

is a ring isomorphism.

Proof. It is easy to see that it is a bijective map that commutes with addition and scalar multiplication. Since we have

$$\mathbf{1}^2 = \mathbf{1}, \quad \mathbf{1}\mathbf{i} = \mathbf{i}\mathbf{1} = \mathbf{i}, \quad \mathbf{i}^2 = -\mathbf{1},$$

it is also a ring homomorphism. □

Remark 1.3.2. Theorem 1.3.1 will allow us to convert from matrices with complex entries to (larger) matrices with real entries.

Note that the squared absolute value $|a + bi|^2 = a^2 + b^2$ is the determinant of the corresponding matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Let z_1, z_2 be two complex numbers with corresponding matrices A_1, A_2. Then

$$|z_1|^2 |z_2|^2 = \det A_1 \det A_2 = \det(A_1 A_2) = |z_1 z_2|^2,$$

and thus

$$|z_1||z_2| = |z_1 z_2|.$$

So multiplicativity of the absolute value corresponds to multiplicativity of determinants.

Note also that if $z \in \mathbb{C}$ corresponds to the matrix A, then

$$z^{-1} = \frac{a - bi}{a^2 + b^2}$$

corresponds to the inverse matrix

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Of course, this also follows from the ring isomorphism above.

Exercises.

1.3.1. Show that the set of matrices

$$\tilde{\mathbb{C}} := \{a\mathbf{1} + b\mathbf{i} \mid a, b \in \mathbb{R}\} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$$

is closed under addition and multiplication and hence forms a subring of $M_n(\mathbb{R})$.

1.4 Quaternions

Definition 1.4.1 (Quaternions)**.** Define a multiplication on the real vector space with basis $\{1, i, j, k\}$ by

$$\begin{gathered} 1i = i1 = i, \quad 1j = j1 = j, \quad 1k = k1 = k, \\ ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j, \\ 1^2 = 1, \quad i^2 = j^2 = k^2 = -1, \end{gathered}$$

and extending by linearity. The elements of the resulting ring (or algebra) $\mathbb{H}$ are called *quaternions*.

Strictly speaking, we need to check that the multiplication is associative and distributive over addition before we know it is a ring (but see below). Note that the quaternions are *not* commutative.

We would like to give a matrix realization of quaternions like we did for the complex numbers. Define 2×2 complex matrices

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Then define

$$\tilde{\mathbb{H}} = \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\} = \left\{ \begin{pmatrix} a + di & -b - ci \\ b - ci & a - di \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \middle| \; z, w \in \mathbb{C} \right\}.$$

The map

$$\mathbb{H} \to \tilde{\mathbb{H}}, \quad a + bi + cj + dk \mapsto a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}, \tag{1.1}$$

is an isomorphism of additive groups that commutes with the multiplication (Exercise 1.4.1).

It follows that the quaternions satisfy the following properties.

Addition:

- *Commutativity.* $q_1 + q_2 = q_2 + q_1$ for all $q_1, q_2 \in \mathbb{H}$.
- *Associativity.* $q_1 + (q_2 + q_3) = (q_1 + q_2) + q_3$ for all $q_1, q_2, q_3 \in \mathbb{H}$.
- *Inverse law.* $q + (-q) = 0$ for all $q \in \mathbb{H}$.
- *Identity law.* $q + 0 = q$ for all $q \in \mathbb{H}$.

Multiplication:

- *Associativity.* $q_1(q_2q_3) = (q_1q_2)q_3$ for all $q_1, q_2, q_3 \in \mathbb{H}$.
- *Inverse law.* $qq^{-1} = q^{-1}q = 1$ for $q \in \mathbb{H}$, $q \neq 0$. Here q^{-1} is the quaternion corresponding to the inverse of the matrix corresponding to q.
- *Identity law.* $1q = q1 = q$ for all $q \in \mathbb{H}$.
- *Left distributive law.* $q_1(q_2 + q_3) = q_1q_2 + q_1q_3$ for all $q_1, q_2, q_3 \in \mathbb{H}$.
- *Right distributive law.* $(q_2 + q_3)q_1 = q_2q_1 + q_3q_1$ for all $q_1, q_2, q_3 \in \mathbb{H}$.

In particular, $\mathbb{H}$ is a ring. We need the right and left distributive laws because $\mathbb{H}$ is not commutative.

Remark 1.4.2. Note that $\mathbb{C}$ is a subring of $\mathbb{H}$ (spanned by 1 and i).

Following the example of complex numbers, we define the *absolute value* of the quaternion $q = a + bi + cj + dk$ to be the (positive) square root of the determinant of the corresponding matrix. That is

$$|q|^2 = \det \begin{pmatrix} a + id & -b - ic \\ b - ic & a - id \end{pmatrix} = a^2 + b^2 + c^2 + d^2.$$

In other words, $|q|$ is the distance of the point (a, b, c, d) from the origin in $\mathbb{R}^4$.

As for complex numbers, multiplicativity of the determinant implies multiplicativity of absolute values of quaternions:

$$|q_1q_2| = |q_1||q_2| \quad \text{for all} \quad q \in \mathbb{H}.$$

From our identification with matrices, we get an explicit formula for the inverse. If $q = a + bi + cj + dk$, then

$$q^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk).$$

If $q = a + bi + cj + dk$, then $\bar{q} := a - bi - cj - dk$ is called the *quaternion conjugate* of q. So we have

$$\bar{q}q = q\bar{q} = a^2 + b^2 + c^2 + d^2 = |q|^2.$$

Because of the multiplicative property of the absolute value of quaternions, the *3-sphere of unit quaternions*

$$\{q \in \mathbb{H} \mid |q| = 1\} = \{a + bi + cj + dk \mid a^2 + b^2 + c^2 + d^2 = 1\}$$

is closed under multiplication. Since $\mathbb{H}$ can be identified with $\mathbb{R}^4$, this shows that $\mathbb{S}^3$ is a group under quaternion multiplication (just like $\mathbb{S}^1$ is group under complex multiplication).

If X is a matrix with complex entries, we define X^* to be the matrix obtained from the transpose X^T by taking the complex conjugate of all entries.

Definition 1.4.3 (U(n) and SU(n))**.** A matrix $X \in M_n(\mathbb{C})$ is called *unitary* if $X^*X = I_n$. The *unitary group* U(n) is the subgroup of $GL(n, \mathbb{C})$ consisting of unitary matrices. The *special unitary group* SU(n) is the subgroup of U(n) consisting of matrices of determinant 1.

Remark 1.4.4. Note that $X^*X = I$ implies that $|\det X| = 1$.

Proposition 1.4.5. *The group $\mathbb{S}^3$ of unit quaternions is isomorphic to* SU(2)*.*

Proof. Recall that under our identification of quaternions with matrices, absolute value corresponds to the determinant. Therefore, the group of unit quaternions is isomorphic to the matrix group

$$\left\{ Q = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \,\middle|\, \det Q = 1 \right\}.$$

Now, if $Q = \begin{pmatrix} z & w \\ x & y \end{pmatrix}$, $w, x, y, z \in \mathbb{C}$, and $\det Q = 1$, then $Q^{-1} = \begin{pmatrix} y & -w \\ -x & z \end{pmatrix}$. Therefore

$$Q^* = Q^{-1} \iff \begin{pmatrix} \bar{z} & \bar{x} \\ \bar{w} & \bar{y} \end{pmatrix} = \begin{pmatrix} y & -w \\ -x & z \end{pmatrix} \iff y = \bar{z},\ w = -\bar{x}$$

and the result follows. □

Exercises.

1.4.1. Show that the map (1.1) is an isomorphism of additive groups that commutes with the multiplication.

1.4.2. Show that if $q \in \mathbb{H}$ corresponds to the matrix A, then $\bar{q}$ corresponds to the matrix A^*. Show that it follows that

$$\overline{q_1 q_2} = \bar{q}_2 \bar{q}_1.$$

1.5 Quaternions and space rotations

The *pure imaginary quaternions*

$$\mathbb{R}i + \mathbb{R}j + \mathbb{R}k := \{bi + cj + dk \mid b, c, d \in \mathbb{R}\}$$

form a three-dimensional subspace of $\mathbb{H}$, which we will often simply denote by $\mathbb{R}^3$ when the context is clear. This subspace is not closed under multiplication. An easy computation shows that

$$\begin{gathered}(u_1 i + u_2 j + u_3 k)(v_1 i + v_2 j + v_3 k) \\ = -(u_1 v_1 + u_2 v_2 + u_3 v_3) + (u_2 v_3 - u_3 v_2) i - (u_1 v_3 - u_3 v_1) j + (u_1 v_2 - u_2 v_1) k.\end{gathered}$$

If we identify the space of pure imaginary quaternions with $\mathbb{R}^3$ by identifying i, j, k with the standard unit vectors, we see that

$$uv = -u \cdot v + u \times v,$$

where $u \times v$ is the vector cross product.

Recall that $u \times v = 0$ if u and v are parallel (i.e. if one is a scalar multiple of the other). Thus, if u is a pure imaginary quaterion, we have

$$u^2 = -u \cdot u = -|u|^2.$$

So if u is a unit vector in $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, then $u^2 = -1$. So every unit vector in $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ is a square root of -1.

Let

$$t = t_0 + t_1 i + t_2 j + t_3 k \in \mathbb{H}, \quad |t| = 1.$$

Let

$$t_I = t_1 i + t_2 j + t_3 k$$

be the imaginary part of t. We have

$$t = t_0 + t_I, \quad 1 = |t|^2 = t_0^2 + t_1^2 + t_2^2 + t_3^2 = t_0^2 + |t_I|^2.$$

Therefore, $(t_0, |t_I|)$ is a point on the unit circle and so there exists θ such that

$$t_0 = \cos\theta, \quad |t_I| = \sin\theta$$

and

$$t = \cos\theta + \frac{t_I}{|t_I|}|t_I| = \cos\theta + u\sin\theta$$

where

$$u = \frac{t_I}{|t_I|}$$

is a unit vector in $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ and hence $u^2 = -1$.

We want to associate to the unit quaternion t a rotation of $\mathbb{R}^3$. However, this cannot be simply by multiplication by t since this would not preserve $\mathbb{R}^3$. However, note that multiplication by t (on the left or right) preserves distances in $\mathbb{R}^4$ (we identify $\mathbb{H}$ with $\mathbb{R}^4$ here) since if $u, v \in \mathbb{H}$, then

$$\begin{aligned} |tu - tv| &= |t(u - v)| = |t||u - v| = |u - v|, \quad \text{and} \\ |ut - vt| &= |(u - v)t| = |u - v||t| = |u - v|. \end{aligned}$$

It follows that multiplication by t preserves the dot product on $\mathbb{R}^4$. Indeed, since it sends zero to zero, it preserves absolute values (since $|u| = |u - 0|$ is the distance from u to zero), and since we can write the dot product in terms of absolute values,

$$u \cdot v = \frac{1}{2}(|u + v|^2 - |u|^2 - |v|^2),$$

multiplication by t preserves the dot product. Therefore, *conjugation by t*

$$q \mapsto tqt^{-1}$$

is an isometry (e.g. preserves distances, angles, etc.). Note that this map also fixes the real numbers since for $r \in \mathbb{R}$,

$$trt^{-1} = tt^{-1}r = 1 \cdot r = r \in \mathbb{R}.$$

Therefore, it maps $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ (the orthogonal complement to $\mathbb{R}$) to itself.

Recall that if u is a (unit) vector in $\mathbb{R}$, then rotation through an angle about u is rotation about the line determined by u (i.e. the line through the origin in the direction u) in the direction given by the right hand rule.

Proposition 1.5.1. *Let $t = \cos\theta + u\sin\theta$, where $u \in \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ is a unit vector. Then conjugation by t on $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ is rotation through angle 2θ about u.*

Proof. Note that

$$t^{-1} = \frac{\bar{t}}{|t|^2} = \cos\theta - u\sin\theta$$

and so conjugation by t fixes $\mathbb{R}u$ since

$$\begin{aligned} tut^{-1} &= (\cos\theta + u\sin\theta)u(\cos\theta - u\sin\theta) \\ &= (u\cos\theta + u^2\sin\theta)(\cos\theta - u\sin\theta) \\ &= (u\cos\theta - \sin\theta)(\cos\theta - u\sin\theta) \\ &= u(\cos^2\theta + \sin^2\theta) - \sin\theta\cos\theta - u^2\sin\theta\cos\theta \\ &= u \end{aligned}$$

(and the conjugation map is linear in $\mathbb{R}$). Therefore, since conjugation by t is an isometry, it is determined by what it does to the orthogonal complement to $\mathbb{R}u$ (i.e. the plane in $\mathbb{R}^3$ through the origin orthogonal to u). It suffices to show that the action of the conjugation map on this plane is rotation through angle 2θ (in the direction given by the right hand rule).

Let $v \in \mathbb{R}^3$ be a unit vector orthogonal to u (i.e. $u \cdot v = 0$) and let $w = u \times v$. Then $\{u, v, w\}$ is an orthonormal basis of $\mathbb{R}^3$. We have

$$uv = -u \cdot v + u \times v = u \times v.$$

Similarly,

$$uv = -vu = w, \quad vw = -wv = u, \quad wu = -uw = v.$$

We compute

$$\begin{aligned} twt^{-1} &= (\cos\theta + u\sin\theta)w(\cos\theta - u\sin\theta) \\ &= (w\cos\theta + uw\sin\theta)(\cos\theta - u\sin\theta) \\ &= w\cos^2\theta + uw\sin\theta\cos\theta - wu\sin\theta\cos\theta - uwu\sin^2\theta \\ &= w\cos^2\theta - 2wu\sin\theta\cos\theta + u^2w\sin^2\theta \\ &= w(\cos^2\theta - \sin^2\theta) - 2v\sin\theta\cos\theta \\ &= w\cos 2\theta - v\sin 2\theta. \end{aligned}$$

Similarly,

$$tvt^{-1} = v\cos 2\theta + w\sin 2\theta.$$

Therefore, in the basis $\{v, w\}$, conjugation by t is given by

$$\begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$$

and is thus rotation by an angle 2θ. This is rotation measured in the direction from v to w and is thus in the direction given by the right hand rule (with respect to u). □

Remark 1.5.2. In [Sti08, §1.5], the conjugation map is given by $q \mapsto t^{-1}qt$. This gives a rotation by -2θ instead of a rotation by 2θ (since it is the inverse to the conjugation used above).

Therefore, rotation of $\mathbb{R}^3$ through an angle α about the axis u is given by conjugation by

$$t = \cos\frac{\alpha}{2} + u\sin\frac{\alpha}{2}$$

and so *all* rotations of $\mathbb{R}^3$ arise as conjugation by a unit quaternion.

Note that

$$(-t)q(-t)^{-1} = tqt^{-1}$$

and so conjugation by $-t$ is the same rotation as conjugation by t. We can also see this since

$$-t = -\cos\frac{\alpha}{2} - u\sin\frac{\alpha}{2} = \cos\left(\frac{\alpha}{2} + \pi\right) + u\sin\left(\frac{\alpha}{2} + \pi\right) = \cos\left(\frac{\alpha + 2\pi}{2}\right) + u\sin\left(\frac{\alpha + 2\pi}{2}\right)$$

which is rotation through an angle of $\alpha + 2\pi$ about u, which is the same transformation.

Are there any other quaternions that give the same rotation? We could have rotation through an angle of $-\alpha$ about $-u$:

$$\cos\left(-\frac{\alpha}{2}\right) + (-u)\sin\left(-\frac{\alpha}{2}\right) = \cos\frac{\alpha}{2} + u\sin\frac{\alpha}{2} = t.$$

Definition 1.5.3 ($\mathrm{O}(n)$ and $\mathrm{SO}(n)$)**.** The subgroup of $\mathrm{GL}(n,\mathbb{R})$ consisting of orthogonal matrices is called the *orthogonal group* and is denoted $\mathrm{O}(n)$. That is,

$$\mathrm{O}(n) = \{X \in \mathrm{GL}(n,\mathbb{R}) \mid XX^T = I_n\}.$$

The *special orthogonal group* $\mathrm{SO}(n)$ is the subgroup of $\mathrm{O}(n)$ consisting of matrices of determinant 1:

$$\mathrm{SO}(n) = \{X \in \mathrm{GL}(n,\mathbb{R}) \mid XX^T = I_n,\ \det X = 1\}.$$

Remark 1.5.4. Note that $XX^T = I_n$ implies $X^TX = I_n$ and $\det X = \pm 1$.

Proposition 1.5.5. *The rotations of* $\mathbb{R}^3$ *form a group isomorphic to* $\mathrm{SO}(3)$*.*

Proof. First note that by choosing an orthonormal basis for $\mathbb{R}^3$ (for instance, the standard basis), we can identify linear transformations of $\mathbb{R}^3$ with 3×3 matrices. The dot product in $\mathbb{R}^3$ is a bilinear form given by $(v,w) \mapsto v \cdot w = v^Tw$. Thus, an element of $M_3(\mathbb{R})$ preserves the dot product (equivalently, distances) if and only if for all $v, w \in \mathbb{R}^3$,

$$v^Tw = (Xv)^T(Xw) = v(X^TX)w.$$

This true iff $X^TX = I_3$ (take v and w to be the standard basis vectors to show that each entry in X^TX must equal the corresponding entry in I_3). Therefore $\mathrm{O}(3)$ is the group of matrices preserving the bilinear form. Since rotations preserve the bilinear form, all rotations are elements of $\mathrm{O}(3)$. In fact, since rotations preserve orientation, they are elements of $\mathrm{SO}(3)$. It remains to show that every element of $\mathrm{SO}(3)$ is a rotation (through an angle about some axis).

Recall that rotations fix an axis (the axis of rotation). Thus, any rotation has 1 as an eigenvalue (the corresponding eigenvector is any nonzero vector on the axis). So we first show that any element of $\mathrm{SO}(3)$ has 1 as an eigenvalue.

Let $X \in \mathrm{SO}(3)$. Then

$$\begin{aligned}\det(X-I) = \det(X-I)^T = \det(X^T - I) = \det(X^{-1} - I) &= \det X^{-1}(I-X) \\ = \det X^{-1}\det(I-X) = \det(I-X) &= -\det(X-I).\end{aligned}$$

Thus

$$2\det(X-I) = 0 \implies \det(X-I) = 0$$

and so 1 is an eigenvalue of X with some unit eigenvector u. Thus X fixes the line $\mathbb{R}u$ and its orthogonal complement (since it preserves the dot product). If we pick an orthonormal basis $\{v,w\}$ of this orthogonal complement, then $\{u,v,w\}$ is an orthonormal basis of $\mathbb{R}^3$ (if necessary, switch the order of v and w so that this basis is right-handed). Let $A = \begin{bmatrix} u & v & w\end{bmatrix}$. Then A is orthogonal (check!) and

$$A^{-1}XA = A^TXA = \begin{pmatrix} 1 & 0 \\ 0 & Y \end{pmatrix}$$

where $Y \in M_2(\mathbb{C})$. Then $1 = \det X = 1 \cdot \det Y = \det Y$ and

$$\begin{pmatrix}1 & 0\\ 0 & Y^T\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & Y\end{pmatrix}^T = (A^TXA)^T = A^TX^TA = A^TX^{-1}A$$
$$= (A^TXA)^{-1} = \begin{pmatrix}1 & 0\\ 0 & Y\end{pmatrix}^{-1} = \begin{pmatrix}1 & 0\\ 0 & Y^{-1}\end{pmatrix}.$$

Thus $Y^T = Y^{-1}$ and so $Y \in \mathrm{SO}(2)$. But we showed earlier that $\mathrm{SO}(2)$ consists of the 2×2 rotation matrices. Thus there exists θ such that

$$A^{-1}XA = \begin{pmatrix}1 & 0 & 0\\ 0 & \cos\theta & -\sin\theta\\ 0 & \sin\theta & \cos\theta\end{pmatrix}$$

and so X is rotation through the angle θ about the axis u. □

Corollary 1.5.6. *The rotations of $\mathbb{R}^3$ form a subgroup of the group of isometries of $\mathbb{R}^3$. In other words, the inverse of a rotation is a rotation and the product of two rotations is a rotation.*

Note that the statement involving products is obvious for rotations of $\mathbb{R}^2$ but not of $\mathbb{R}^3$.

Proposition 1.5.7. *There is a surjective group homomorphism $\mathrm{SU}(2) \to \mathrm{SO}(3)$ with kernel $\{\pm 1\}$ (i.e. $\{\pm I_2\}$).*

Proof. Recall that we can identity the group of unit quaternions with the group $\mathrm{SU}(2)$. By the above, we have a surjective map

$$\begin{aligned}\varphi : \mathrm{SU}(2) &\longrightarrow \{\text{rotations of } \mathbb{R}^3\} \cong \mathrm{SO}(3),\\ t &\mapsto (q \mapsto t^{-1}qt)\end{aligned}$$

and $\varphi(t_1) = \varphi(t_2)$ iff $t_1 = \pm t_2$. In particular, the kernel of the map is $\{\pm 1\}$. It remains to show that this map is a group homomorphism. Suppose that

$$t_i = \cos\frac{\alpha_i}{2} + u_i \sin\frac{\alpha_i}{2}.$$

and let r_i, $i = 1, 2$, be rotation through angle α_i about axis u_i. Then r_i corresponds to conjugation by t_i. That is, $\varphi(t_i) = r_i$, $i = 1, 2$. The composition of rotations r_2r_1 (r_1 followed by r_2 – we read functions from right to left as usual) corresponds to the composition of the two conjugations which is the map

$$q \mapsto t_1qt_1^{-1} \mapsto t_2t_1qt_1^{-1}t_2^{-1} = (t_2t_1)q(t_2t_1)^{-1}.$$

Therefore $\varphi(t_2t_1) = r_2r_1 = \varphi(t_2)\varphi(t_1)$ and so φ is a group homomorphism. □

Corollary 1.5.8. *We have a group isomorphism $\mathrm{SO}(3) \cong \mathrm{SU}(2)/\{\pm 1\}$.*

Proof. This follows from the fundamental isomorphism theorem for groups. □

Remark 1.5.9. Recall that the elements of $\mathrm{SU}(2)/\{\pm 1\}$ are cosets $\{\pm t\}$ and multiplication is given by $\{\pm t_1\}\{\pm t_2\} = \{\pm t_1 t_2\}$. The above corollary is often stated as "SU(2) is a double cover of SO(3)." It has some deep applications to physics. If you "rotate" an electron through an angle of 2π it is not the same as what you started with. This is related to the fact that electrons are described by representations of SU(2) and not SO(3). One can illustrate this idea with *Dirac's belt trick*.

Proposition 1.5.7 allows one to identify rotations of $\mathbb{R}^3$ with pairs $\pm t$ of antipodal unit quaternions. One can thus do things like compute the composition of rotations (and find the axis and angle of the composition) via quaternion arithmetic. This is actually done in the field of computer graphics.

Recall that a subgroup H of a group G is called *normal* if $gHg^{-1} = H$ for all $g \in G$. Normal subgroups are precisely those subgroups that arise as kernels of homomorphisms. A group G is *simple* if its only normal subgroups are the trivial subgroup and G itself.

Proposition 1.5.10 (Simplicity of SO(3)). *The group* SO(3) *is simple.*

Proof. See [Sti08, p. 33]. We will return to this issue later with a different proof (see Corollary 5.14.7). □

1.6 Isometries of $\mathbb{R}^n$ and reflections

We now want to give a description of rotations in $\mathbb{R}^4$ via quaternions. We first prove some results about isometries of $\mathbb{R}^n$ in general. Recall that an *isometry* of $\mathbb{R}^n$ is a map $f : \mathbb{R}^n \to \mathbb{R}^n$ such that

$$|f(u) - f(v)| = |u - v|, \quad \forall\, u, v \in \mathbb{R}^n.$$

Thus, isometries are maps that preserve distance. As we saw earlier, preserving dot products is the same as preserving distance and fixing the origin.

Definition 1.6.1. A *hyperplane* H through O is an $(n-1)$-dimensional subspace of $\mathbb{R}^n$, and *reflection in* H is the linear endomorphism of $\mathbb{R}^n$ that fixes the points of H and reverses vectors orthogonal to H.

We can give an explicit formula for reflection r_u in the hyperplane orthogonal to a (nonzero) vector u. It is

$$r_u(v) = v - 2\frac{v \cdot u}{|u|^2}u, \quad v \in \mathbb{R}^n. \tag{1.2}$$

Theorem 1.6.2 (Cartan–Dieudonné Theorem). *Any isometry of* $\mathbb{R}^n$ *that fixes the origin* O *is the product of at most* n *reflections in hyperplanes through* O.

Note: There is an error in the proof of this result given in [Sti08, p. 36]. It states there that $r_u f$ is the identity on $\mathbb{R}u$ when it should be $\mathbb{R}v$.

Proof. We prove the result by induction on n.

Base case ($n = 1$). The only isometries of $\mathbb{R}$ fixing O are the identity and the map $x \mapsto -x$, which is reflection in O (a hyperplane in $\mathbb{R}$).

Inductive step. Suppose the result is true for $n = k - 1$ and let f be an isometry of $\mathbb{R}^k$ fixing O. If f is the identity, we're done. Therefore, assume f is not the identity. Then there exists $v \in \mathbb{R}^k$ such that $f(v) = w \neq v$. Let r_u be the reflection in the hyperplane orthogonal to $u = v - w$. Then

$$\begin{aligned}
r_u(w) &= w - 2\frac{w \cdot u}{|u|^2}u = w - 2\frac{w \cdot (v - w)}{|v - w|^2}(v - w) \\
&= w - 2\frac{w \cdot v - w \cdot w}{v \cdot v - 2w \cdot v + w \cdot w}(v - w) \\
&= w - 2\frac{w \cdot v - w \cdot w}{2w \cdot w - 2w \cdot v}(v - w) \qquad (\text{since } v \cdot v = f(v) \cdot f(v) = w \cdot w) \\
&= w + (v - w) = v.
\end{aligned}$$

Thus $r_u f(v) = r_u(w) = v$ and so v is fixed by $r_u f$. Since isometries are linear transformations, $r_u f$ is the identity on the subspace $\mathbb{R}v$ of $\mathbb{R}^n$ and is determined by its restriction g to the $\mathbb{R}^{k-1}$ orthogonal to $\mathbb{R}v$. By induction, g is the product of $\leq k - 1$ reflections. Therefore $f = r_u g$ is the product of $\leq k$ reflections. □

Remark 1.6.3. The full Cartan–Dieudonné Theorem is actually more general, concerning isometries of n-dimensional vector spaces over a field of characteristic not equal to 2 with a non-degenerate bilinear form. What we proved above is just a special case.

Definition 1.6.4 (Orientation-preserving and orientation-reversing)**.** A linear map is called *orientation-preserving* if its determinant is positive and *orientation-reversing* otherwise.

Reflections are linear and have determinant -1. To see this, pick a basis compatible with the reflection, i.e. a basis $\{v_1, \ldots, v_n\}$ where $\{v_1, \ldots, v_{n-1}\}$ span the hyperplane of reflection and v_n is orthogonal to the hyperplane of reflection. Then in this basis, the reflection is diagonal with diagonal entries $1, \ldots, 1, -1$.

So we see that a product of reflections is orientation-preserving iff it contains an even number of terms.

Definition 1.6.5 (Rotation)**.** A *rotation of* $\mathbb{R}^n$ *about* O is an orientation-preserving isometry that fixes O.

It follows that if we choose an orthonormal basis of $\mathbb{R}^n$ (for instance, the standard basis) so that linear maps correspond to $n \times n$ matrices, the rotations of $\mathbb{R}^n$ correspond to $\mathrm{SO}(n)$.

Exercises.

1.6.1. Verify that the map r_u defined by (1.2) is indeed reflection in the hyperplane orthogonal to the nonzero vector U. (It helps to draw a picture.) Note that it suffices to show that the right hand side maps u to u and fixes any vector orthogonal to u.

1.7 Quaternions and rotations of $\mathbb{R}^4$

It follows from the Cartan–Dieudonné Theorem that any rotation of $\mathbb{R}^4$ is the product of 0, 2, or 4 reflections. Recall that we identify the group of unit quaternions with $\mathrm{SU}(2)$ and $\mathbb{H}$ with $\mathbb{R}^4$.

Proposition 1.7.1. *Let $u \in \mathrm{SU}(2)$ be a unit quaternion. The map*

$$r_u : \mathbb{H} \to \mathbb{H}, \quad r_u(q) = -u\bar{q}u$$

is reflection in the hyperplane through O orthogonal to u.

Proof. Note that $q \mapsto -\bar{q}$ is the map

$$a + bi + cj + dk \mapsto -a + bi + cj + dk, \quad a, b, c, d \in \mathbb{R}$$

and is therefore reflection in the hyperplane $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, which is an isometry. We saw before that left or right multiplication by a unit quaternion is an isometry and thus the composition

$$q \mapsto -\bar{q} \mapsto -u\bar{q} \mapsto -u\bar{q}u$$

is also an isometry. Now, for $v \in \mathbb{H}$, we have

$$r_u(vu) = -u\overline{(vu)}u = -u\bar{u}\bar{v}u = -|u|^2\bar{v}u = -\bar{v}u.$$

Therefore, we have

$$r_u(u) = -u, \quad r_u(iu) = iu, \quad r_u(ju) = ju, \quad r_u(ku) = ku.$$

So r_u reverses vectors parallel to u and fixes points in the space spanned by iu, ju and ku. Therefore, it suffices to show that iu, ju and ku span the hyperplane through O orthogonal to u. First note that if $u = a + bi + cj + dk$, then

$$u \cdot iu = (a, b, c, d) \cdot (-b, a, -d, c) = 0.$$

Similarly, one can show that u is also orthogonal to ju and ku. So it remains to show that iu, ju and ku span a 3-dimensional subspace of $\mathbb{H}$ or, equivalently, that u, iu, ju, ku span all of $\mathbb{H}$. But this is true since for any $v \in \mathbb{H}$, we have

$$v = (vu^{-1})u$$

and we can express vu^{-1} as an $\mathbb{R}$-linear combination of 1, i, j and k. □

Proposition 1.7.2. *The rotations of $\mathbb{H} = \mathbb{R}^4$ about O are precisely the maps of the form $q \mapsto vqw$, where $v, w \in \mathrm{SU}(2)$ are unit quaternions.*

Proof. We know that any rotation of $\mathbb{H}$ is a product of an even number of reflections. The composition of reflections in the hyperplanes orthogonal to $u_1, u_2, \dots, u_{2n} \in \mathrm{SU}(2)$ is the map

$$q \mapsto -u_1 \bar{q} u_1 \mapsto -u_2 \overline{(-u_1 \bar{q} u_1)} u_2 = u_2 \bar{u}_1 q \bar{u}_1 u_2 \mapsto \dots \mapsto u_{2n} \cdots \bar{u}_3 u_2 \bar{u}_1 q \bar{u}_1 u_2 \bar{u}_3 \cdots u_{2n}.$$

Thus we have that this composition is the map $q \mapsto vqw$ where

$$v = u_{2n} \cdots \bar{u}_3 u_2 \bar{u}_1, \qquad w = \bar{u}_1 u_2 \bar{u}_3 \cdots u_{2n}.$$

It follows that all rotations are of this form.

It remains to show that all maps of the form $q \mapsto vqw$ for $v, w \in \mathrm{SU}(2)$ are rotations of $\mathbb{H}$ about O. Since this map is the composition of left multiplication by v followed by right multiplication by w, it is enough to show that multiplication of $\mathbb{H}$ on either side by a unit quaternion is an orientation-preserving isometry (i.e. a rotation). We have already shown that such a multiplication is an isometry, so we only need to show it is orientation-preserving. Let

$$v = a + bi + cj + dk, \quad a^2 + b^2 + c^2 + d^2 = 1,$$

be an arbitrary unit quaternion. Then in the basis $\{1, i, j, k\}$ of $\mathbb{H} = \mathbb{R}^4$, left multiplication by v has matrix

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

and one can verify by direct computation that this matrix has determinant one. The proof that right multiplication by w is orientation-preserving is analogous. □

1.8 SU(2) × SU(2) and SO(4)

Recall that the *direct product* $G \times H$ of groups G and H is the set

$$G \times H = \{(g, h) \mid g \in G,\ h \in H\}$$

with multiplication

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

The unit of $G \times H$ is $(1_G, 1_H)$ where 1_G is the unit of G and 1_H is the unit of H and the inverse of (g, h) is (g^{-1}, h^{-1}).

If G is a group of $n \times n$ matrices and H is a group of $m \times m$ matrices, then the map

$$(g, h) \mapsto \begin{pmatrix} g & \mathbf{0} \\ \mathbf{0} & h \end{pmatrix}$$

is an isomorphism from $G \times H$ to the group

$$\left\{ \begin{pmatrix} g & \mathbf{0} \\ \mathbf{0} & h \end{pmatrix} \;\middle|\; g \in G,\ h \in H \right\}$$

of block diagonal matrices $(n+m) \times (n+m)$ matrices since

$$\begin{pmatrix} g_1 & \mathbf{0} \\ \mathbf{0} & h_1 \end{pmatrix} \begin{pmatrix} g_2 & \mathbf{0} \\ \mathbf{0} & h_2 \end{pmatrix} = \begin{pmatrix} g_1 g_2 & \mathbf{0} \\ \mathbf{0} & h_1 h_2 \end{pmatrix}.$$

For each pair of unit quaternions $(v,w) \in \mathrm{SU}(2) \times \mathrm{SU}(2)$, we know that the map

$$q \mapsto vqw^{-1}$$

is a rotation of $\mathbb{H} = \mathbb{R}^4$ (since w^{-1} is also a unit quaterion) and is hence an element of $\mathrm{SO}(4)$.

Proposition 1.8.1. *The map*

$$\varphi : \mathrm{SU}(2) \times \mathrm{SU}(2) \to \mathrm{SO}(4), \quad (v,w) \mapsto (q \mapsto vqw^{-1}),$$

is a surjective group homomorphism with kernel $\{(1,1),(-1,-1)\}$.

Proof. For $q \in \mathbb{H}$,

$$\begin{aligned} \varphi((v_1,w_1)(v_2,w_2))(q) &= \varphi(v_1v_2, w_1w_2)(q) = (v_1v_2)q(w_1w_2)^{-1} \\ &= v_1(v_2qw_2^{-1})w_1^{-1} = \varphi(v_1,w_1)\varphi(v_2,w_2)(q). \end{aligned}$$

Therefore

$$\varphi((v_1,w_1)(v_2,w_2)) = \varphi(v_1,w_1)\varphi(v_2,w_2),$$

and so φ is a group homomorphism. It is surjective since we showed earlier that *any* rotation of $\mathbb{R}^4$ is of the form $q \mapsto vqw^{-1}$ for $v,w \in \mathrm{SU}(2)$.

Now suppose that $(v,w) \in \ker \varphi$. Then $q \mapsto vqw^{-1}$ is the identity map. In particular

$$v1w^{-1} = 1$$

and thus $v = w$. Therefore $\varphi(v,w) = \varphi(v,v)$ is the map $q \mapsto vqv^{-1}$. We saw in our description of rotations of $\mathbb{R}^3$ using quaternions that this map fixes the real axis and rotates the space of pure imaginary quaternions. We also saw that it is the identity map if and only if $v = \pm 1$. □

Remark 1.8.2. Our convention here is slightly different from the one used in [Sti08]. That reference uses the map $q \mapsto v^{-1}qw$. This difference is analogous to one noted in the description of rotations of $\mathbb{R}^3$ by quaternions (see Remark 1.5.2). Essentially, in [Sti08], the composition of rotations r_1 and r_2 is thought of as being r_1r_2 instead of r_2r_1. We use the latter composition since it corresponds to the order in which you apply functions (right to left).

Corollary 1.8.3. *We have a group isomorphism* $(\mathrm{SU}(2) \times \mathrm{SU}(2))/\{\pm 1\} \cong \mathrm{SO}(4)$. *Here* $1 = (1,1)$ *is the identity element of the product group* $\mathrm{SU}(2) \times \mathrm{SU}(2)$ *and* $-1 = (-1,-1)$.

Proof. This follows from the fundamental isomorphism theorem for groups. □

Lemma 1.8.4. *The group* $\mathrm{SO}(4)$ *is not simple.*

Proof. The subgroup $\mathrm{SU}(2) \times \{1\} = \{(v, 1) \mid v \in \mathrm{SU}(2)\}$ is the kernel of the group homomorphism $(v, w) \mapsto (1, w)$, projection onto the second factor, and is thus a normal subgroup of $\mathrm{SU}(2) \times \mathrm{SU}(2)$. It follows that its image (under the map φ above) is a normal subgroup of $\mathrm{SO}(4)$. This subgroup consists of the maps $q \mapsto vq$. This subgroup is nontrivial and is not the whole of $\mathrm{SO}(4)$ because since it does not contain the map $q \mapsto qw^{-1}$ for $w \neq 1$ (recall that maps $q \mapsto v_1 q w_1^{-1}$ and $q \mapsto v_2 q w_2^{-1}$ are equal if and only if $(v_1, w_1) = (\pm v_1, \pm w_1)$ by the above corollary). □

Chapter 2

Matrix Lie groups

In this chapter, we will study what is probably the most important class of Lie groups, matrix Lie groups. In addition to containing the important subclass of *classical Lie groups*, focussing on matrix Lie groups (as opposed to abstract Lie groups) allows us to avoid much discussion of abstract manifold theory.

2.1 Definitions

Recall that we can identify $M_n(\mathbb{R})$ with $\mathbb{R}^{n^2}$ and $M_n(\mathbb{C})$ with $\mathbb{C}^{n^2}$ by interpreting the n^2 entries

$$a_{11}, a_{12}, \dots, a_{1n}, a_{21}, \dots, a_{2n}, \dots, a_{n1}, \dots, a_{nn}$$

as the coordinates of a point/matrix.

Definition 2.1.1 (Convergence of matrices)**.** Let $(A_m)_{m\in\mathbb{N}}$ be a sequence of elements of $M_n(\mathbb{C})$. We say that A_m *converges* to a matrix A if each entry of A_m converges (as $m \to \infty$) to the corresponding entry of A. That is, A_m converges to A if

$$\lim_{m\to\infty} |(A_m)_{k\ell} - A_{k\ell}| = 0, \ \forall\ 1 \le k, \ell \le n.$$

Note that convergence in the above sense is the same as convergence in $\mathbb{C}^{n^2}$.

Definition 2.1.2 (Matrix Lie group)**.** A *matrix group* is any subgroup of $\mathrm{GL}(n,\mathbb{C})$. A *matrix Lie group* is any subgroup G of $\mathrm{GL}(n,\mathbb{C})$ with the following property: If $(A_m)_{m\in\mathbb{N}}$ is a sequence of matrices in G, and A_m converges to some matrix A then either $A \in G$, or A is not invertible.

Remark 2.1.3. The convergence condition on G in Definition 2.1.2 is equivalent to the condition that G be a closed subset of $\mathrm{GL}(n,\mathbb{C})$. Note that this does not imply that G is a closed subset of $M_n(\mathbb{C})$. So matrix Lie groups are *closed subgroups* of $GL(n,\mathbb{C})$.

Definition 2.1.4 (Linear group)**.** A *linear group* is any group that is isomorphic to a matrix group. A *linear Lie group* is any group that is isomorphic to a matrix Lie group. We will sometimes abuse terminology and refer to linear Lie groups as matrix Lie groups.

Before discussing examples of matrix Lie groups, let us give a non-example. Let G be the set of all $n \times n$ invertible matrices with (real) rational entries. Then, for example,

$$\lim_{m\to\infty} \begin{pmatrix} \sum_{k=0}^{m} \frac{1}{k!} & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} = \begin{pmatrix} e & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix},$$

which is invertible but not in G. Therefore G is not a matrix Lie group.

We now discuss important examples of matrix Lie groups.

2.2 Finite groups

Suppose G is a finite subgroup of $\mathrm{GL}(n,\mathbb{C})$. Then any convergent sequence $(A_m)_{m\in\mathbb{N}}$ in G is eventually stable (i.e. there is some $A \in G$ such that $A_m = A$ for m sufficiently large). Thus G is a matrix Lie group.

Recall that S_n is isomorphic to a subgroup of $\mathrm{GL}(n,\mathbb{C})$ as follows. Consider the standard basis $X = \{e_1, \dots, e_n\}$ of $\mathbb{C}^n$. Then permutations of this set correspond to elements of $\mathrm{GL}(n,\mathbb{C})$. Thus S_n is a linear Lie group.

Any finite group G acts on itself (regarded as a set) by left multiplication. This yields an injective group homomorphism $G \to S_G$ and so G is isomorphic to a subgroup of S_G and, hence, all finite groups are linear Lie groups.

2.3 The general and special linear groups

The *complex general linear group* $\mathrm{GL}(n,\mathbb{C})$ is certainly a subgroup of itself. If $(A_m)_{m\in\mathbb{N}}$ is a sequence of matrices in $\mathrm{GL}(n,\mathbb{C})$ converging to A, then A is in $\mathrm{GL}(n,\mathbb{C})$ or A is not invertible (by the definition of $\mathrm{GL}(n,\mathbb{C})$). Therefore $\mathrm{GL}(n,\mathbb{C})$ is a matrix Lie group.

$\mathrm{GL}(n,\mathbb{R})$ is a subgroup of $\mathrm{GL}(n,\mathbb{C})$ and if A_m is a sequence of matrices in $\mathrm{GL}(n,\mathbb{R})$ converging to A, then the entries of A are real. Thus either $A \in \mathrm{GL}(n,\mathbb{R})$ or A is not invertible. Therefore the *real general linear group* $\mathrm{GL}(n,\mathbb{R})$ is a matrix Lie group.

The *real special linear group* $\mathrm{SL}(n,\mathbb{R})$ and *complex special linear group* $\mathrm{SL}(n,\mathbb{C})$ are both subgroups of $\mathrm{GL}(n,\mathbb{C})$. Suppose $(A_m)_{m\in\mathbb{N}}$ is a sequence of matrices in $\mathrm{SL}(n,\mathbb{R})$ or $\mathrm{SL}(n,\mathbb{C})$ converging to A. Since the determinant is a continuous function of the entries of a matrix, $\det A = 1$. Therefore $\mathrm{SL}(n,\mathbb{R})$ and $\mathrm{SL}(n,\mathbb{C})$ are both matrix Lie groups.

2.4 The orthogonal and special orthogonal groups

Recall that we have an inner product (dot product) on $\mathbb{R}^n$ defined as follows. If $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$, then

$$u \cdot v = u^T v = u_1 v_1 + \cdots + u_n v_n.$$

(In the above, we view u and v as column vectors.) We have that $|u|^2 = u \cdot u$ and we know that a linear transformation preserves length (or distance) if and only if it preserves the inner product. We showed that an $n \times n$ matrix X preserves the dot product if and only if

$$X \in \mathrm{O}(n) = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid A^T A = I_n\}.$$

Since we defined rotations to be orientation preserving isometries, we have that X is a rotation if and only if

$$X \in \mathrm{SO}(n) = \{A \in \mathrm{O}(n) \mid \det A = 1\}.$$

One easily checks (Exercise 2.4.1) that the *orthogonal group* $\mathrm{O}(n)$ and *special orthogonal group* $\mathrm{SO}(n)$ are closely under multiplication and inversion and contain the identity matrix. For instance, if $A, B \in \mathrm{O}(n)$, then

$$(AB)^T(AB) = B^T A^T AB = B^T IB = B^T B = I.$$

Thus $\mathrm{SO}(n)$ is a subgroup of $\mathrm{O}(n)$ and both are subgroups of $\mathrm{GL}(n, \mathbb{C})$.

Suppose $(A_m)_{m \in \mathbb{N}}$ is a sequence of matrices in $\mathrm{O}(n)$ converging to A. Since multiplication of matrices is a continuous function (Exercise 2.4.2), we have that $A^T A = I_n$ and hence $A \in \mathrm{O}(n)$. Therefore $\mathrm{O}(n)$ is a matrix Lie group. Since the determinant is a continuous function, we see that $\mathrm{SO}(n)$ is also a matrix Lie group.

Remark 2.4.1. Note that we do not write $\mathrm{O}(n, \mathbb{R})$ because, by convention, $\mathrm{O}(n)$ *always* consists of real matrices.

Exercises.

2.4.1. Verify that $\mathrm{SO}(n)$ and $\mathrm{O}(n)$ are both subgroups of $\mathrm{GL}(n, \mathbb{C})$.

2.4.2. Show that multiplication of matrices is a continuous function in the entries of the matrices.

2.5 The unitary and special unitary groups

The *unitary group*

$$\mathrm{U}(n) = \{A \in \mathrm{GL}(n, \mathbb{C}) \mid AA^* = I_n\}, \quad \text{where } (A^*)_{jk} = \overline{A_{kj}}$$

is a subgroup of $\mathrm{GL}(n, \mathbb{C})$. The same argument used for the orthogonal and special orthogonal groups shows that $\mathrm{U}(n)$ is a matrix Lie group, and so is the *special unitary group*

$$\mathrm{SU}(n) = \{A \in U(n) \mid \det A = 1\}.$$

Remark 2.5.1. A unitary matrix can have determinant $e^{i\theta}$ for any θ, whereas an orthogonal matrix can only have determinant ± 1. Thus $\mathrm{SU}(n)$ is a "smaller" subset of $\mathrm{U}(n)$ than $\mathrm{SO}(n)$ is of $\mathrm{O}(n)$.

Remark 2.5.2. For a real or complex matrix A, the condition $AA^* = I$ (which reduces to $AA^T = I$ if A is real) is equivalent to the condition $A^*A = I$. This follows from the standard result in linear algebra that if A and B are square and $AB = I$, then $B = A^{-1}$ (one doesn't need to check that $BA = I$ as well).

Exercises.

2.5.1. For an arbitrary $\theta \in \mathbb{R}$, write down an element of $\mathrm{U}(n)$ with determinant $e^{i\theta}$.

2.5.2. Show that the unitary group is precisely the group of matrices preserving the bilinear form on $\mathbb{C}^n$ given by

$$\langle x, y \rangle = x_1 \bar{y}_n + \cdots + x_n \bar{y}_n.$$

2.6 The complex orthogonal groups

The *complex orthogonal group* is the subgroup

$$\mathrm{O}(n, \mathbb{C}) = \{A \in \mathrm{GL}(n, \mathbb{C}) \mid AA^T = I_n\}$$

of $\mathrm{GL}(n, \mathbb{C})$. As above, we see that $\mathrm{O}(n, \mathbb{C})$ is a matrix Lie group and so is the *special complex orthogonal group*

$$\mathrm{SO}(n, \mathbb{C}) = \{A \in \mathrm{O}(n, \mathbb{C}) \mid \det A = 1\}.$$

Note that $\mathrm{O}(n, \mathbb{C})$ is the subgroup of $\mathrm{GL}(n, \mathbb{C})$ preserving the bilinear form on $\mathbb{C}^n$ given by

$$\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n.$$

Note that this is *not* an inner product since it is symmetric rather than conjugate-symmetric.

2.7 The symplectic groups

We have a natural inner product on $\mathbb{H}^n$ given by

$$\langle (p_1, \ldots, p_n), (q_1, \ldots, q_n) \rangle = p_1 \bar{q}_1 + \ldots p_n \bar{q}_n.$$

Note that $\mathbb{H}^n$ is *not* a vector space over $\mathbb{H}$ since quaternions do not act properly as "scalars" since their multiplication is not commutative ($\mathbb{H}$ is not a field).

Since quaternion multiplication is associative, matrix multiplication of matrices with quaternionic entries is associative. Therefore we can use them to define linear transformations of $\mathbb{H}^n$. We define the *(compact) symplectic group* $\mathrm{Sp}(n)$ to be the subset of $M_n(\mathbb{H})$ consisting of those matrices that preserve the above bilinear form. That is,

$$\mathrm{Sp}(n) = \{A \in M_n(\mathbb{H}) \mid \langle Ap, Aq \rangle = \langle p, q \rangle \ \forall\ p, q \in \mathbb{H}^n\}.$$

The proof of the following lemma is an exercise (Exercise 2.7.1). It follows from this lemma that $\mathrm{Sp}(n)$ is a matrix Lie group.

Lemma 2.7.1. *We have*

$$\mathrm{Sp}(n) = \{A \in M_n(\mathbb{H}) \mid AA^\star = I_n\}$$

where $A^\star$ denotes the quaternion conjugate transpose of A.

Remark 2.7.2. Note that, for a quaternionic matrix A, the condition $AA^\star = I$ is equivalent to the condition $A^\star A = I$. This follows from the fact that $\mathrm{Sp}(n)$ is a group, or from the realization of quaternionic matrices as complex matrices (see Section 1.4 and Remark 2.5.2).

Because $\mathbb{H}$ is not a field, it is often useful to express $\mathrm{Sp}(n)$ in terms of complex matrices. Recall that we can identify quaternions with matrices of the form

$$\begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix}, \qquad \alpha, \beta \in \mathbb{C}.$$

Replacing the quaternion entries in $A \in M_n(\mathbb{H})$ with the corresponding 2×2 complex matrices produces a matrix in $A \in M_{2n}(\mathbb{C})$ and this identification is a ring isomorphism.

Preserving the inner product means preserving length in the corresponding real space $\mathbb{R}^{4n}$. For example, $\mathrm{Sp}(1)$ consists of the 1×1 quaternion matrices, multiplication by which preserves length in $\mathbb{H} = \mathbb{R}^4$. We saw before that these are simply the unit quaternions, which we identified with $\mathrm{SU}(2)$. Therefore,

$$\mathrm{Sp}(1) = \left\{ \begin{pmatrix} a+id & -b-ic \\ b-ic & a-id \end{pmatrix} \middle| \ a^2+b^2+c^2+d^2 = 1 \right\} = \mathrm{SU}(2).$$

We would like to know, for general values of n, which matrices in $M_{2n}(\mathbb{C})$ correspond to elements of $\mathrm{Sp}(n)$.

Define a skew-symmetric bilinear form B on $\mathbb{R}^{2n}$ or $\mathbb{C}^{2n}$ by

$$B((x_1, y_1, \dots, x_n, y_n), (x_1', y_1', \dots, x_n', y_n')) = \sum_{k=1}^n x_k y_k' - y_k x_k'.$$

Then the *real symplectic group* $\mathrm{Sp}(n, \mathbb{R})$ (respectively, *complex symplectic group* $\mathrm{Sp}(n, \mathbb{C})$) is the subgroup of $\mathrm{GL}(2n, \mathbb{R})$ (respectively, $\mathrm{GL}(2n, \mathbb{C})$) consisting of matrices preserving B.

Let

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and let

$$J_{2n} = \begin{pmatrix} J & & 0 \\ & \ddots & \\ 0 & & J \end{pmatrix}.$$

Then

$$B(x,y) = x^T J_{2n} y$$

and

$$\begin{aligned} \mathrm{Sp}(n,\mathbb{R}) &= \{A \in \mathrm{GL}(2n,\mathbb{R}) \mid A^T J_{2n} A = J_{2n}\}, \\ \mathrm{Sp}(n,\mathbb{C}) &= \{A \in \mathrm{GL}(2n,\mathbb{C}) \mid A^T J_{2n} A = J_{2n}\}. \end{aligned}$$

Note that we use the transpose (not the conjugate transpose) in the definition of $\mathrm{Sp}(n,\mathbb{C})$.

For a symplectic (real or complex) matrix, we have

$$\det J_{2n} = \det(A^T J_{2n} A) = (\det A)^2 \det J_{2n} \implies \det A = \pm 1.$$

In fact one can show that $\det A = 1$ for $A \in \mathrm{Sp}(n,\mathbb{R})$ or $A \in \mathrm{Sp}(n,\mathbb{C})$. We will come back to this point later.

The proof of the following proposition is an exercise (see [Sti08, Exercises 3.4.1–3.4.3]).

Proposition 2.7.3. *We have*

$$\mathrm{Sp}(n) = \mathrm{Sp}(n,\mathbb{C}) \cap \mathrm{U}(2n).$$

Remark 2.7.4. Some references write $\mathrm{Sp}(2n,\mathbb{C})$ for what we have denoted $\mathrm{Sp}(n,\mathbb{C})$.

Example 2.7.5 (The metaplectic group). There do exist Lie groups that are not matrix Lie groups. One example is the *metaplectic group* $\mathrm{Mp}(n,\mathbb{R})$, which is the unique connected double cover (see Section 6.6) of the symplectic Lie group $\mathrm{Sp}(n,\mathbb{R})$. It is not a matrix Lie group because it has no faithful finite-dimensional representations.

Exercises.

2.7.1. Prove Lemma 2.7.1.

2.8 The Heisenberg group

The *Heisenberg group* H is the set of all 3×3 real matrices of the form

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad a,b,c \in \mathbb{R}.$$

It is easy to check that $I \in H$ and that H is closed under multiplication. Also

$$A^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

and so H is closed under inversion. It is clear that the limit of matrices in H is again in H and so H is a matrix Lie group.

The name "Heisenberg group" comes from the fact that the Lie algebra of H satisfies the Heisenberg commutation relations of quantum mechanics.

2.9 The groups $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{S}^1$ and $\mathbb{R}^n$

The groups $\mathbb{R}^*$ and $\mathbb{C}^*$ under matrix multiplication are isomorphic to $\mathrm{GL}(1,\mathbb{R})$ and $\mathrm{GL}(1,\mathbb{C})$, respectively, and so we view them as matrix Lie groups. The group $\mathbb{S}^1$ of complex numbers with absolute value one is isomorphic to $\mathrm{U}(1)$ and so we also view it as a matrix Lie group.

The group $\mathbb{R}^n$ under vector addition is isomorphic to the group of diagonal real matrices with positive diagonal entries, via the map

$$(x_1, \ldots, x_n) \mapsto \begin{pmatrix} e^{x_1} & & 0 \\ & \ddots & \\ 0 & & e^{x_n} \end{pmatrix}.$$

One easily checks that this is a matrix Lie group and thus we view $\mathbb{R}^n$ as a matrix Lie group as well.

2.10 The Euclidean group

The *Euclidean group* $\mathrm{E}(n)$ is the group of all one-to-one, onto, distance-preserving maps from $\mathbb{R}^n$ to itself:

$$E(n) = \{f : \mathbb{R}^n \to \mathbb{R}^n \mid |f(x) - f(y)| = |x-y| \ \forall\ x, y \in \mathbb{R}^n\}.$$

Note that we do not require these maps to be linear.

The orthogonal group $\mathrm{O}(n)$ is the subgroup of $\mathrm{E}(n)$ consisting of all *linear* distance-preserving maps of $\mathbb{R}^n$ to itself. For $x \in \mathbb{R}^n$, define *translation by* x, denoted T_x, by

$$T_x(y) = x + y.$$

The set of all translations is a subgroup of $E(n)$.

Proposition 2.10.1. *Every element of* $\mathrm{E}(n)$ *can be written uniquely in the form*

$$T_x R, \quad x \in \mathbb{R}^n,\ R \in \mathrm{O}(n).$$

Proof. The proof of this proposition can be found in books on Euclidean geometry. □

One can show (Exercise 2.10.2) that the Euclidean group is isomorphic to a matrix Lie group.

Exercises.

2.10.1. Show that, for $x_1, x_2 \in \mathbb{R}^n$ and $R_1, R_2 \in \mathrm{O}(n)$, we have

$$(T_{x_1} R_1)(T_{x_2} R_2) = T_{x_1 + R_1 x_2}(R_1 R_2)$$

and that, for $x \in \mathbb{R}^n$ and $R \in \mathrm{O}(n)$, we have

$$(T_x R)^{-1} = T_{-R^{-1}x} R^{-1}.$$

This shows that $\mathrm{E}(n)$ is a *semidirect product* of the group of translations and the group $\mathrm{O}(n)$. More precisely, $\mathrm{E}(n)$ is isomorphic to the group consisting of pairs (T_x, R), for $x \in \mathbb{R}^n$ and $R \in \mathrm{O}(n)$, with multiplication

$$(x_1, R_1)(x_2, R_2) = (x_1 + R_1 x_2, R_1 R_2).$$

2.10.2. Show that the map $\mathrm{E}(n) \to \mathrm{GL}(n+1, \mathbb{R})$ given by

$$T_x R \mapsto \begin{pmatrix} & & & x_1 \\ & R & & \vdots \\ & & & x_n \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

is a one-to-one group homomorphism and conclude that $\mathrm{E}(n)$ is isomorphic to a matrix Lie group.

2.11 Homomorphisms of Lie groups

Whenever one introduces a new type of mathematical object, one should define the allowed maps between objects (more precisely, one should define a *category*).

Definition 2.11.1 (Lie group homomorphism/isomorphism)**.** Let G and H be (matrix) Lie groups. A map Φ from G to H is called a *Lie group homomorphism* if

(a) Φ is a group homomorphism, and

(b) Φ is continuous.

If, in addition, Φ is one-to-one and onto and the inverse map Φ^{-1} is continuous, then Φ is a *Lie group isomorphism*.

Examples 2.11.2. (a) The map $\mathbb{R} \to U(1)$ given by $\theta \mapsto e^{i\theta}$ is a Lie group homomorphism.

(b) The map $U(1) \to \mathrm{SO}(2)$ given by

$$e^{i\theta} \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

is a Lie group isomorphism (you should check that this map is well-defined and is indeed an isomorphism).

(c) Composing the previous two examples gives the Lie algebra homomorphism $\mathbb{R} \to \mathrm{SO}(2)$ defined by

$$\theta \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

(d) The determinant is a Lie group homomorphism $\mathrm{GL}(n, \mathbb{C}) \to \mathbb{C}^*$.

(e) The map $\mathrm{SU}(2) \to \mathrm{SO}(3)$ of Proposition 1.5.7 is continuous and is thus a Lie group homomorphism (recall that this map has kernel $\{\pm 1\}$).

Chapter 3

Topology of Lie groups

In this chapter, we discuss some topological properties of Lie groups, including connectedness and compactness.

3.1 Connectedness

An important notion in theory of Lie groups is that of path-connectedness.

Definition 3.1.1 (Path-connected)**.** Let A be a subset of $\mathbb{R}^n$. A *path* in A is a continuous map $\gamma\colon [0,1] \to A$. We say A is *path-connected* if, for any two points $a, b \in A$, there is a path γ in A such that $\gamma(0) = a$ and $\gamma(1) = b$.

Remark 3.1.2. If $\gamma\colon [a,b] \to A$, $a < b$, is a continuous map, we can always rescale to obtain a path $\tilde{\gamma}\colon [0,1] \to A$. Therefore, we will sometimes also refer to these more general maps as paths.

Remark 3.1.3. For those who know some topology, you know that the notion of *path-connectedness* is not the same, in general, as the notion of *connectedness.* However, it turns out that a matrix Lie group is connected if and only if it is path-connected. (This follows from the fact that matrix Lie groups are manifolds, and hence are locally path-connected.) Thus we will sometimes ignore the difference between the two concepts in this course.

The property of being connected by some path is an equivalence relation on the set of points of a matrix Lie group. The equivalence classes are the *(connected) components* of the matrix Lie group. Thus, the components have the property that two elements of the same component can be joined by a continuous path but two elements of different components cannot.

The proof of the following proposition is an exercise (see [Sti08, Exercises 3.2.1–3.2.3]).

Proposition 3.1.4. *If G is a matrix Lie group, then the component of G containing the identity is a subgroup of G.*

Proposition 3.1.5. *The group $\mathrm{GL}(n,\mathbb{C})$ is connected for all $n \geq 1$.*

We will give two proofs, one explicit and one not explicit (but shorter).

First proof. We will show that any matrix in $\mathrm{GL}(n,\mathbb{C})$ can be connected to the identity by some path. Then any two elements of $\mathrm{GL}(n,\mathbb{C})$ can be connected by a path through the identity.

Let $A \in \mathrm{GL}(n,\mathbb{C})$. Recall from linear algebra that every matrix is similar to an upper triangular matrix (for instance, its Jordan canonical form). Thus, there exists $C \in \mathrm{GL}(n,\mathbb{C})$ such that

$$A = CBC^{-1},$$

where B is of the form

$$B = \begin{pmatrix} \lambda_1 & & \star \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Since $\det A = \det B = \lambda_1 \cdots \lambda_n$ and A is invertible, all the λ_i must be nonzero. Let $B(t)$, $0 \le t \le 1$, be obtained from B by multiplying all the entries above the diagonal by $(1-t)$, and let $A(t) = CB(t)C^{-1}$. Then $A(t)$ is a continuous path starting at A and ending at CDC^{-1} where

$$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

This path is contained in $\mathrm{GL}(n,\mathbb{C})$ since

$$\det A(t) = \lambda_1 \dots \lambda_n = \det A, \quad \text{for all } t.$$

For $1 \le i \le n$, choose a path $\lambda_i \colon [1,2] \to \mathbb{C}^*$ such that $\lambda_i(1) = \lambda_i$ and $\lambda_i(2) = 1$. This is possible since $\mathbb{C}^*$ is path-connected. Then define $A(t)$ on the interval $1 \le t \le 2$ by

$$A(t) = C \begin{pmatrix} \lambda_1(t) & & 0 \\ & \ddots & \\ 0 & & \lambda_n(t) \end{pmatrix} C^{-1}.$$

This is a continuous path starting at CDC^{-1}, when $t = 1$, and ending at $CIC^{-1} = I$, when $t = 2$. Since the $\lambda_k(t)$ are always nonzero, $A(t)$ lies in $\mathrm{GL}(n,\mathbb{C})$ for all t. Thus we have constructed a path from A to I. □

Second proof. Let $A, B \in \mathrm{GL}(n,\mathbb{C})$. Consider the plane

$$(1-z)A + zB, \ z \in \mathbb{C}.$$

Matrices of this form are not in $\mathrm{GL}(n,\mathbb{C})$ precisely when

$$\det((1-z)A + zB) = 0. \tag{3.1}$$

Since $(1-z)A+zB$ is an $n \times n$ complex matrix whose entries are linear in z, its determinant is a polynomial of degree at most n in z. Therefore, by the Fundamental Theorem of Algebra, the left hand side of (3.1) has at most n roots. These roots correspond to at most n points in the plane $(1-z)A+zB$, $z \in \mathbb{C}$, not including the points A or B. Therefore, we can find a path from A to B which avoids these n points (since the plane minus a finite number of points is path-connected). □

The proof of the following proposition is left as an exercise (Exercise 3.1.1).

Proposition 3.1.6. *The group* $\mathrm{SL}(n,\mathbb{C})$ *is connected for all* $n \geq 1$.

Proposition 3.1.7. *For all* $n \geq 1$, *the group* $\mathrm{O}(n)$ *is not connected.*

Proof. Let $A, B \in \mathrm{O}(n)$ such that $\det A = 1$ (for instance, $A = I$) and $\det B = -1$ (for instance, $B = \mathrm{diag}(1, \dots, 1, -1)$). The determinant map $\det\colon M_n(\mathbb{R}) \to \mathbb{R}$ is a polynomial in the entries and is thus a continuous map. Suppose that γ is a path from A to B. Then $\det \circ \gamma$ is a composition of continuous maps and hence is a continuous map $[0,1] \to \mathbb{R}$. But the image of $\det \circ \gamma$ lies in $\{\pm 1\}$ and we have $\det \circ \gamma(0) = 1$, $\det \circ \gamma(1) = -1$. Since there is no continuous map $\mathbb{R} \to \{\pm 1\}$ starting at 1 and ending at -1, we have a contradiction. □

Proposition 3.1.8. *The group* $\mathrm{SO}(n)$ *is connected for* $n \geq 1$.

Proof. Since $\mathrm{SO}(1) = \{(1)\}$ is simply a point, it is connected. Also, we have seen that $\mathrm{SO}(2)$ is a circle and is therefore also connected. Assume that $\mathrm{SO}(n-1)$ is connected for some $n \geq 2$. We show that every $A \in \mathrm{SO}(n)$ can be joined to the identity by a path. We can then conclude that $\mathrm{SO}(n)$ is connected since any two elements could be connected by a path through the identity.

Let $\{e_1, \dots, e_n\}$ be the standard basis of $\mathbb{R}^n$. Let R be a rotation in a plane containing e_1 and Ae_1 such that $RAe_1 = e_1$. Since $\mathrm{SO}(2)$ (the group of rotations in a plane) is connected, there is a path $R(t)$, $0 \leq t \leq 1$, such that $R(0) = I$ and $R(t) = R$. Then

$$\gamma(t) = R(t)A, \quad 0 \leq t \leq 1,$$

is a path in $\mathrm{SO}(n)$ with $\gamma(0) = A$ and $\gamma(1) = RA$. Since R and A are both orthogonal matrices, so is RA. Thus RAe_j is orthogonal to $RAe_1 = e_1$ for all $2 \leq j \leq n$. Therefore

$$RA = \begin{pmatrix} 1 & 0 \\ 0 & A_1 \end{pmatrix},$$

with $A_1 \in \mathrm{SO}(n-1)$. By induction, there is a continuous path from A_1 to I_{n-1} and hence a path from RA to I_n. Following γ by this path yields a path from A to I_n. □

Corollary 3.1.9. *The group* $\mathrm{O}(n)$ *has 2 connected components.*

Proof. It suffices to show that the set Y of matrices in $\mathrm{O}(n)$ with determinant equal to -1 is connected. Let A and B be two such matrices. Then $XA, XB \in \mathrm{SO}(n)$, where

$$X = \begin{pmatrix} -1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}.$$

Since $\mathrm{SO}(n)$ is connected, there is a path $\gamma\colon [0,1] \to \mathrm{SO}(n)$ with $\gamma(0) = XA$ and $\gamma(1) = XB$. Then $X\gamma(t)$ is a path from A to B in Y. □

Proposition 3.1.10. *The groups* $\mathrm{U}(n)$ *and* $\mathrm{SU}(n)$ *are connected for* $n \geq 1$.

Proof. We first show that every $U \in \mathrm{U}(n)$ can be joined to the identity by a continuous path (hence showing that $\mathrm{U}(n)$ is connected). Recall from linear algebra that every unitary matrix has an orthonormal basis of eigenvectors with eigenvalues of the form $e^{i\theta}$. Therefore, we have

$$U = U_1 \begin{pmatrix} e^{i\theta_1} & & 0 \\ & \ddots & \\ 0 & & e^{i\theta_n} \end{pmatrix} U_1^{-1}, \tag{3.2}$$

with U_1 unitary (since its columns form an orthonormal basis) and $\theta_i \in \mathbb{R}$. Conversely, one can easily check that any matrix of the form (3.2) is unitary. Therefore,

$$U(t) = U_1 \begin{pmatrix} e^{i(1-t)\theta_1} & & 0 \\ & \ddots & \\ 0 & & e^{1(1-t)\theta_n} \end{pmatrix} U_1^{-1}, \qquad 0 \leq t \leq 1,$$

defines a continuous path in $\mathrm{U}(n)$ joining U to I.

Proving that $\mathrm{SU}(n)$ is connected involves a modification similar to the modification one makes to the argument proving $\mathrm{GL}(n,\mathbb{C})$ is connected to prove that $\mathrm{SL}(n,\mathbb{C})$ is connected. □

Proposition 3.1.11. *The group* $\mathrm{Sp}(n)$ *is connected for* $n \geq 1$.

Proof. We prove this by induction (similar to the proof that $\mathrm{SO}(n)$ is connected). The only major difference is the base case of $\mathrm{Sp}(2)$.

Recall that

$$\mathrm{Sp}(2) = \left\{ \begin{pmatrix} q_1 & -q_2 \\ \bar{q}_2 & \bar{q}_1 \end{pmatrix} \;\middle|\; q_1, q_2 \in \mathbb{H},\ |q_1|^2 + |q_2|^2 = 1 \right\}.$$

Therefore

$$q_1 = u_1 \cos\theta, \quad q_2 = u_2 \sin\theta$$

for some $u_1, u_2 \in \mathbb{H}$ with $|u_1| = |u_2| = 1$.

We will show later that any unit quaternion is the exponential of a pure imaginary quaternion. Thus there exist pure imaginary quaternions v_1 and v_2 such that $u_i = e^{v_i}$, $i = 1, 2$. Therefore

$$q_1(t) = e^{tv_1} \cos\theta t, \quad q_2(t) = e^{tv_2} \sin\theta t$$

gives a continuous path from I to $\begin{pmatrix} q_1 & -q_2 \\ \bar{q}_2 & \bar{q}_1 \end{pmatrix}$ in $\mathrm{Sp}(2)$. Thus $\mathrm{Sp}(2)$ is connected.

We leave the inductive step as an exercise. □

Corollary 3.1.12. *If* $A \in \mathrm{Sp}(n,\mathbb{C}) \cap \mathrm{U}(2n)$ *(i.e. A is an element of* $\mathrm{Sp}(n)$ *written as a complex matrix), then* $\det A = 1$.

Proof. Recall that we showed that all such matrices have determinant ±1. Since $\mathrm{Sp}(n)$ is connected, it follows that they in fact all have determinant 1, since the determinant is a continuous function and the identity matrix has determinant one. □

The above corollary explains why we do not consider a “special symplectic group”.

Remark 3.1.13. One can also show that $\mathrm{Sp}(n,\mathbb{R})$ and $\mathrm{Sp}(n,\mathbb{C})$ are also connected.

Exercises.

3.1.1. Prove Proposition 3.1.6.

3.1.2. Prove that the Heisenberg group is connected and that the Euclidean group has 2 connected components.

3.2 Polar Decompositions

From now on, we will use the notation $\langle v, w\rangle$ to denote our standard inner product on $\mathbb{R}^n$, $\mathbb{C}^n$ or $\mathbb{H}^n$. That is,

$$\langle v, w\rangle = v_1\bar{w}_1 + \cdots + v_n\bar{w}_n,$$

where $\bar{\ }$ denotes the identity operation, complex conjugation, or quaternionic conjugation if v and w lie in $\mathbb{R}^n$, $\mathbb{C}^n$, or $\mathbb{H}^n$ respectively.

The goal of this section is to discuss *polar decompositions* for $\mathrm{SL}(n,\mathbb{R})$ and $\mathrm{SL}(n,\mathbb{C})$ (and other groups). These decompositions are useful for proving that $\mathrm{SL}(n,\mathbb{R})$ and $\mathrm{SL}(n,\mathbb{C})$ have certain topological properties. One should think of these decompositions as analogues of the unique decomposition of a nonzero complex number z as $z = up$ where $|u| = 1$ and p is a positive real number.

Recall that a matrix A is *symmetric* if $A^T = A$. If v and w are eigenvectors of A with distinct eigenvalues λ and μ (without loss of generality, we can assume $\mu \neq 0$), then

$$\lambda\mu(v\cdot w) = Av\cdot Aw = (Av)^T Aw = v^T A^T Aw = v^T A^2 w = \mu^2 v^T w = \mu^2 v\cdot w \implies v\cdot w = 0.$$

Since symmetric matrices are diagonalizable, we see that any symmetric matrix A has an orthonormal basis of eigenvectors. So we can write

$$A = RDR^{-1} = RDR^T, \tag{3.3}$$

where R is an orthogonal matrix (whose columns are an orthonormal basis of eigenvectors for A) and D is a diagonal matrix. Conversely, one easily checks that any matrix of the form (3.3) is symmetric.

Definition 3.2.1 (Positive real symmetric matrix)**.** An $n \times n$ real symmetric matrix P is *positive* (or *positive-definite)* if $\langle x, Px\rangle > 0$ for all nonzero vectors $x \in \mathbb{R}^n$. Equivalently, a real symmetric matrix is positive if all of its eigenvalues are positive.

By the above, given a real symmetric positive matrix P, there exists an orthogonal matrix R such that

$$P = RDR^{-1},$$

where D is diagonal with positive diagonal entries $\lambda_1, \dots, \lambda_n$. We can then construct a square root of P as

$$P^{1/2} = RD^{1/2}R^{-1}, \tag{3.4}$$

where D is the diagonal matrix with positive diagonal entries $\lambda_1^{1/2}, \dots, \lambda_n^{1/2}$. So $P^{1/2}$ is also symmetric and positive. In fact, one can show that $P^{1/2}$ is the *unique* positive symmetric matrix whose square is P (Exercise 3.2.1).

Proposition 3.2.2 (Polar decomposition of $\mathrm{SL}(n,\mathbb{R})$)**.** *For every $A \in \mathrm{SL}(n,\mathbb{R})$, there exists a unique pair (R, P) such that $R \in \mathrm{SO}(n)$, P is real, symmetric and positive, and $A = RP$. The matrix P satisfies* $\det P = 1$*.*

Proof. If such a pair existed, we would have

$$A^TA = (RP)^T(RP) = P^TR^TRP = PIP = P^2.$$

Since $(A^TA)^T = A^T(A^T)^T = A^TA$, the matrix A^TA is symmetric. It is also positive since for all $x \in \mathbb{R}^n$, $x \neq 0$, we have

$$\langle x, A^TAx\rangle = \langle Ax, Ax\rangle > 0$$

since $Ax \neq 0$ (because A is invertible). Therefore we can define

$$P = (A^TA)^{1/2},$$

and this P is real, symmetric, and positive. Since we want $A = RP$, we define

$$R = AP^{-1} = A((A^TA)^{1/2})^{-1}.$$

For the existence part of the proposition, it remains to show that $R \in \mathrm{SO}(n)$. Since

$$\begin{aligned} R^TR &= A((A^TA)^{1/2})^{-1}((A^TA)^{1/2})^{-1}A^T \qquad \text{(recall that } A^TA \text{ is symmetric)} \\ &= A(A^TA)^{-1}A^T = AA^{-1}(A^T)^{-1}A^T = I, \end{aligned}$$

we see that $R \in \mathrm{O}(n)$. Also, we have

$$1 = \det A = \det R \det P.$$

Since P is positive (in particular, all its eigenvalues are positive), we have $\det P > 0$. Therefore, $\det R > 0$ and so $\det R = 1$ (since R is orthogonal, $\det R = \pm 1$). It then follows that $\det P = 1$ as well.

To prove uniqueness, note that we saw above that we must have $P^2 = A^TA$. By the uniqueness of the square root of a real, symmetric, positive matrix, P is unique. Then $R = AP^{-1}$ is also unique. □

Definition 3.2.3 (Positive self-adjoint complex matrix)**.** If P is an $n \times n$ self-adjoint (or *hermitian*) complex matrix (i.e. $P^* = P$), then we say P is *positive* (or *positive-definite)* if $\langle x, Px \rangle > 0$ for all nonzero $x \in \mathbb{C}^n$.

Proposition 3.2.4 (Polar decomposition of $\mathrm{SL}(n, \mathbb{C})$)**.** *For every* $A \in \mathrm{SL}(n, \mathbb{C})$*, there exists a unique pair* (U, P) *with* $U \in \mathrm{SU}(n)$*,* P *self-adjoint and positive, and* $A = UP$*. The matrix* P *satisfies* $\det P = 1$*.*

Proof. The proof is analogous to the proof of the polar decomposition for $\mathrm{SL}(n, \mathbb{R})$. □

Remark 3.2.5. (a) Any complex matrix A can be written in the form $A = UP$ where U is unitary and P is a positive-semidefinite ($\langle x, Ax \rangle \geq 0$ for all $x \in \mathbb{C}^n$) self-adjoint matrix. We just do not have the uniqueness statement in general.

(b) Our decomposition gives a polar decomposition

$$\det A = \det P \det U = re^{i\theta}$$

of the determinant of A since $\det P$ is a nonnegative real number and $\det U$ is a unit complex number.

(c) We have similar (unique) polar decompositions for

$$\mathrm{GL}(n, \mathbb{R}),\ \mathrm{GL}(n, \mathbb{R})^+ = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det A > 0\},\ \text{and } \mathrm{GL}(n, \mathbb{C}).$$

$$\begin{aligned} \mathrm{GL}(n, \mathbb{R}) : A = UP, &\quad U \in \mathrm{O}(n),\ P \text{ real, symmetric, positive} \\ \mathrm{GL}(n, \mathbb{R})^+ : A = UP, &\quad U \in \mathrm{SO}(n),\ P \text{ real, symmetric, postive} \\ \mathrm{GL}(n, \mathbb{C}) : A = UP, &\quad U \in \mathrm{U}(n),\ P \text{ self-adjoint, positive} \end{aligned}$$

The proofs of these are left as an exercise. Note that the only difference between the polar decomposition statements for $\mathrm{GL}(n, \mathbb{R})^+$ and $\mathrm{SL}(n, \mathbb{R})$ is that we do not conclude that $\det P = 1$ for $\mathrm{GL}(n, \mathbb{R})^+$.

Exercises.

3.2.1. Show that $P^{1/2}$ given by (3.4) is the unique positive symmetric matrix whose square is P. *Hint:* show that any matrix that squares to P has the same set of eigenvectors as P.

3.2.2. Prove the results stated in Remark 3.2.5(c).

3.2.3. Prove that a real symmetric matrix is positive if and only if all of its eigenvalues are positive (see Definition 3.2.1).

3.3 Compactness

Definition 3.3.1 (Comact)**.** A matrix Lie group G is *compact* if the following two conditions are satisfied:

(a) The set G is closed in $M_n(\mathbb{C})$: If A_m is a sequence of matrices in G, and A_m converges to a matrix A, then A is in G.

(b) The set G is bounded: There exists a constant $C \in \mathbb{R}$ such that for all $A \in G$, $|A_{ij}| \le C$ for all $1 \le i, j \le n$.

Remark 3.3.2. (a) The conditions in the above definition say that G is a closed bounded subset of $\mathbb{C}^{n^2}$ (when we identify $M_n(\mathbb{C})$ with $\mathbb{C}^{n^2}$). For subsets of $\mathbb{C}^{n^2}$, this is equivalent to the usual, more general, definition of compact (that any open cover has a finite subcover).

(b) All of our examples of matrix Lie groups except $\mathrm{GL}(n,\mathbb{R})$ and $\mathrm{GL}(n,\mathbb{C})$ satisfy the closure condition above. Thus, we are most interested in the boundedness condition.

Proposition 3.3.3. *The groups* $\mathrm{O}(n)$*,* $\mathrm{SO}(n)$*,* $\mathrm{U}(n)$*,* $\mathrm{SU}(n)$ *and* $\mathrm{Sp}(n)$ *are compact.*

Proof. We have already noted that these groups satisfy the closure condition. The column vectors of any matrix in the first four groups in the proposition have norm one (and also in the last if we consider the complex form of elements of $\mathrm{Sp}(n)$) and hence $|A_{ij}| \le 1$ for all $1 \le i, j \le n$. □

Proposition 3.3.4. *The following groups are noncompact:*

$$\begin{gathered} \mathrm{GL}(n,\mathbb{R}),\ \mathrm{GL}(n,\mathbb{C}), \quad n \ge 1, \\ \mathrm{SL}(n,\mathbb{R}),\ \mathrm{SL}(n,\mathbb{C}),\ \mathrm{O}(n,\mathbb{C}),\ \mathrm{SO}(n,\mathbb{C}), \quad n \ge 2, \\ H,\ \mathrm{Sp}(n,\mathbb{R}),\ \mathrm{Sp}(n,\mathbb{C}),\ \mathrm{E}(n),\ \mathbb{R}^n,\ \mathbb{R}^*,\ \mathbb{C}^*, \quad n \ge 1. \end{gathered}$$

Proof. The groups $\mathrm{GL}(n,\mathbb{R})$ and $\mathrm{GL}(n,\mathbb{C})$ violate the closure condition since a limit of invertible matrices may be not invertible.

Since

$$\begin{pmatrix} a & & & & \\ & \frac{1}{a} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

has determinant one for any nonzero a, we see that the groups $\mathrm{SL}(n,\mathbb{R})$ and $\mathrm{SL}(n,\mathbb{C})$ are not bounded for $n \ge 2$.

We have

$$\begin{pmatrix} z & -w \\ w & z \end{pmatrix} \in \mathrm{SO}(2,\mathbb{C})$$

for $z, w \in \mathbb{C}$ with $z^2 + w^2 = 1$. We can take z with $|z|$ arbitrarily large and let w be any solution to $z^2 + w^2 = 1$ (such solutions always exist over the complex numbers) and thus

SO(2) is unbounded. By considering block matrices, we see that SO(n) is unbounded for $n \geq 2$.

We leave the remaining cases as an exercise (Exercise 3.3.1). □

Exercises.

3.3.1. Complete the proof of Proposition 3.3.4.

3.4 Lie groups

Technically speaking, we gave the definition of an arbitrary Lie group (as opposed to a matrix Lie group) in Section 1.1. But in this section we will give the definition more directly. Although we will focus on matrix Lie groups in this course, it is useful to see the more general definition, which is the approach one must take if one wishes to study Lie groups in more detail (beyond this course). Our discussion here will be very brief. Further details can be found in [Hal03, Appendix C].

Definition 3.4.1 (Lie group)**.** A (real) *Lie group* is a (real) smooth manifold G which is also a group and such that the group product $G \times G \to G$ and the inverse map $g \mapsto g^{-1}$ are smooth maps.

Roughly speaking, a smooth manifold is an object that looks locally like $\mathbb{R}^n$. For example, the torus is a two-dimensional manifold since it looks locally (but not globally) like $\mathbb{R}^2$.

Example 3.4.2. Let

$$G = \mathbb{R} \times \mathbb{R} \times \mathbb{S}^1,$$

with group product

$$(x_1, y_1, u_1) \cdot (x_2, y_2, u_2) = (x_1 + x_2, y_1 + y_2, e^{ix_1 y_2} u_1 u_2).$$

One can check that this operation does indeed make G into a group (Exercise 3.4.1). The multiplication and inversion maps are both smooth, and so G is a Lie group. However, one can show that G is *not* isomorphic to a matrix Lie group (see [Hal03, §C.3]).

Theorem 3.4.3 ([Sti08, Corollary 2.33])**.** *Every matrix Lie group is a smooth embedded submanifold of $M_n(\mathbb{C})$ and is thus a Lie group.*

Usually one says that a map Φ between Lie groups is a Lie group homomorphism if Φ is a group homomorphism and Φ is *smooth*. However, in Definition 2.11.1, we only required that Φ be continuous. This is because of the following result. A proof for the case of matrix Lie groups can be found in [Sti08, Corollary 2.34].

Proposition 3.4.4. *Suppose G and H are Lie groups and $\Phi\colon G \to H$ is a group homomorphism from G to H. If Φ is continuous, then it is also smooth.*

Exercises.

3.4.1. Show that G, as defined in Example 3.4.2, is a group.

Chapter 4

Maximal tori and centres

From now on, we will sometimes use the term *Lie group*. For the purposes of this course, you can replace this term by *matrix Lie group*. In this chapter we discuss some important subgroups of Lie groups.

4.1 Maximal tori

Definition 4.1.1 (Torus)**.** A *torus* (or *k-dimensional torus*) is a group isomorphic to

$$\mathbb{T}^k = \mathbb{S}^1 \times \mathbb{S}^1 \times \cdots \times \mathbb{S}^1 \quad (k\text{-fold Cartesian product}).$$

A *maximal torus* of a Lie group G is a torus subgroup T of G such that if T' is another torus subgroup containing T then $T = T'$.

Remark 4.1.2. (a) Note that tori are abelian.

(b) For those who know something about Lie algebras, maximal tori correspond to Cartan subalgebras of Lie algebras.

Example 4.1.3. The group $\mathrm{SO}(2) = \mathbb{S}^1 = \mathbb{T}^1$ is its own maximal torus.

Recall that $\mathrm{SO}(3)$ is the group of rotations of $\mathbb{R}^3$. Let e_1, e_2, e_3 be the standard basis vectors. Then the matrices

$$R'_\theta = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} R_\theta & 0 \\ 0 & 1 \end{pmatrix}, \quad \theta \in \mathbb{R},$$

form a copy of $\mathbb{T}^1$ in $\mathrm{SO}(3)$.

Proposition 4.1.4. *The set $\{R'_\theta \mid \theta \in \mathbb{R}\}$ forms a maximal torus in* $\mathrm{SO}(3)$.

Proof. Suppose $\mathbb{T}$ is a torus in $\mathrm{SO}(3)$ containing this $\mathbb{T}^1$. Since all tori are abelian, any $A \in \mathbb{T}$ commutes with all $R'_\theta \in \mathbb{T}^1$. Thus is suffices to show that, for $A \in \mathrm{SO}(3)$,

$$AR'_\theta = R'_\theta A \quad \text{for all } R'_\theta \in \mathbb{T}^1 \tag{4.1}$$

implies that $A \in \mathbb{T}^1$. Suppose $A \in \mathrm{SO}(3)$ satisfies (4.1). First we show that

$$A(e_1),\ A(e_2) \in \operatorname{Span}\{e_1, e_2\}.$$

Suppose

$$A(e_1) = a_1e_1 + a_2e_2 + a_3e_3.$$

By (4.1), A commutes with

$$R'_\pi = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since

$$\begin{aligned} AR'_\pi(e_1) &= A(-e_1) = -a_1e_1 - a_2e_2 - a_3e_3, \\ R'_\pi A(e_1) &= R'_\pi(a_1e_1 + a_2e_2 + a_3e_3) = -a_1e_1 - a_2e_2 + a_3e_3, \end{aligned}$$

we have $a_3 = 0$ and so $A(e_1) \in \operatorname{Span}\{e_1, e_2\}$ as desired. A similar argument shows that $A(e_2) \in \operatorname{Span}\{e_1, e_2\}$.

Thus, the restriction of A to the (e_1, e_2)-plane is an isometry of that plane that fixes the origin. Therefore it is a rotation or a reflection. However, no reflection commutes with all rotations (Exercise 4.1.1). Thus A must be a rotation in the (e_1, e_2)-plane. Since A preserves the dot product, it must leave invariant $\mathbb{R}e_3$, which is the orthogonal complement to $\operatorname{Span}\{e_1, e_2\}$. So A is of the form

$$A = \begin{pmatrix} R_\theta & 0 \\ 0 & c \end{pmatrix}$$

for some $c \in \mathbb{R}$. Since $\det A = \det R_\theta = 1$, it follows that $c = 1$, and hence $A \in \mathbb{T}^1$ as desired. □

Definition 4.1.5 (Centre)**.** The *centre* of a Lie group G is the subgroup (see Exercise 4.1.2)

$$Z(G) = \{A \in G \mid AB = BA\ \forall\ B \in G\}.$$

Corollary 4.1.6. *The Lie group* SO(3) *has trivial centre:*

$$Z(\mathrm{SO}(3)) = \{1\}.$$

Proof. Suppose $A \in Z(\mathrm{SO}(3))$. Then A commutes with all elements of SO(3) and hence all elements of $\mathbb{T}^1$. By the above argument, this implies that A fixes e_3. Interchanging basis vectors in this argument shows that A also fixes e_1 and e_2 and hence A is the identity. □

We now find maximal tori in all of the compact connected matrix Lie groups we have seen. We focus on connected groups because one can easily see (since $\mathbb{T}^k$ is connected) that a maximal torus must always be contained in the identity component of a Lie group.

First of all, we note that there are at least three natural matrix groups isomorphic to $\mathbb{T}^1$:

(a) The group $\{R_\theta \mid \theta \in \mathbb{R}\}$ consisting of 2×2 matrices.

(b) The group
$$e^{i\theta} = \cos\theta + i\sin\theta,\ \theta \in \mathbb{R},$$
consisting of complex numbers (or 1 × 1 complex matrices).

(c) The group
$$e^{i\theta} = \cos\theta + i\sin\theta,\ \theta \in \mathbb{R},$$
consisting of quaternions (or 1 × 1 quaternionic matrices).

These give rise to three natural matrix groups isomorphic to $\mathbb{T}^k$:

(a) The group of $2k \times 2k$ matrices of the form
$$R_{\theta_1,\dots,\theta_k} = \begin{pmatrix} R_{\theta_1} & & \\ & \ddots & \\ & & R_{\theta_k} \end{pmatrix}.$$

(b) The group of $k \times k$ unitary matrices of the form
$$Z_{\theta_1,\dots,\theta_k} = \begin{pmatrix} e^{i\theta_1} & & \\ & \ddots & \\ & & e^{i\theta_k} \end{pmatrix}.$$

(c) The group of $k \times k$ symplectic matrices of the form
$$Q_{\theta_1,\dots,\theta_k} = \begin{pmatrix} e^{i\theta_1} & & \\ & \ddots & \\ & & e^{i\theta_k} \end{pmatrix}.$$

Theorem 4.1.7. *The following are maximal tori.*

(a) In $\mathrm{SO}(2m)$*:*
$$\mathbb{T}^m = \{R_{\theta_1,\dots,\theta_m} \mid \theta_1,\dots,\theta_m \in \mathbb{R}\}.$$

(b) In $\mathrm{SO}(2m+1)$*:*
$$\mathbb{T}^m = \left\{ R'_{\theta_1,\dots,\theta_m} = \begin{pmatrix} R_{\theta_1,\dots,\theta_m} & 0 \\ 0 & 1 \end{pmatrix} \;\middle|\; \theta_1,\dots,\theta_m \in \mathbb{R} \right\}.$$

(c) In $\mathrm{U}(n)$*:*
$$\mathbb{T}^n = \{Z_{\theta_1,\dots,\theta_n} \mid \theta_1,\dots,\theta_n\}.$$

(d) In $\mathrm{SU}(n)$*:*
$$\mathbb{T}^{n-1} = \{Z_{\theta_1,\dots,\theta_n} \mid \theta_1,\dots,\theta_n \in \mathbb{R},\ \theta_1 + \cdots + \theta_n = 0\}.$$

Note that this is a $\mathbb{T}^{n-1}$ *since is it equal to*
$$\left\{ \begin{pmatrix} e^{i\theta_1} & & & \\ & \ddots & & \\ & & e^{i\theta_{n-1}} & \\ & & & e^{-\theta_1-\cdots-\theta_{n-1}} \end{pmatrix} \;\middle|\; \theta_1,\dots,\theta_{n-1} \in \mathbb{R} \right\}.$$

(e) In $\mathrm{Sp}(n)$*:*

$$\mathbb{T}^n = \{Q_{\theta_1,\dots,\theta_n} \mid \theta_1,\dots,\theta_n \in \mathbb{R}\}.$$

Proof. We prove each case separately. As for the case of $\mathrm{SO}(3)$ dealt with above, in each case we will show that if an element A of the group commutes with all elements of the indicated torus, then A must be included in this torus. Then the result follows as it did for $\mathrm{SO}(3)$.

(a) Let $e_1, e_2, \dots, e_{2m}$ denote the standard basis of $\mathbb{R}^{2m}$. Suppose that $A \in \mathrm{SO}(2m)$ commutes will all elements of $\mathbb{T}^m$. We first show that

$$\begin{gathered} A(e_1),\ A(e_2) \in \mathrm{Span}\{e_1, e_2\}, \\ A(e_3),\ A(e_4) \in \mathrm{Span}\{e_3, e_4\}, \\ \vdots \\ A(e_{2m-1}),\ A(e_{2m}) \in \mathrm{Span}\{e_{2m-1}, e_{2m}\}. \end{gathered}$$

We do the case of e_1, since the rest are analogous. Recall that we assume that A commutes with all elements of $\mathbb{T}^m$. Therefore,

$$AR_{\pi,0,\dots,0}(e_1) = R_{\pi,0,\dots,0}A(e_1).$$

If

$$A(e_1) = a_1e_1 + \cdots + a_{2m}e_{2m},$$

then

$$AR_{\pi,0,\dots,0}(e_1) = A(-e_1) = -a_1e_1 - \cdots - a_{2m}e_{2m},$$

but

$$R_{\pi,0,\dots,0}A(e_1) = R_{\pi,0,\dots,0}(a_1e_1 + \cdots + a_{2m}e_{2m}) = -a_1e_1 - a_2e_2 + a_3e_3 + \cdots + e_{2m}e_{2m}.$$

Thus

$$a_3 = a_4 = \cdots = a_{2m}$$

as desired. Therefore, A is a product of rotations or reflections in the planes

$$\mathrm{Span}\{e_1, e_2\}, \dots, \mathrm{Span}\{e_{2m-1}, e_{2m}\}.$$

However, the case of reflections is ruled out as it was for $\mathrm{SO}(3)$ and hence A is a product of rotations in these planes and therefore is an element of $\mathbb{T}^m$.

(b) This is a generalization of the argument for $\mathrm{SO}(3)$, using maps such as $R'_{\pi,0,\dots,0}$ in place of R'_π. The details are left as an exercise.

(c) Let $e_1, \dots, e_n$ be the standard basis of $\mathbb{C}^n$. Suppose that $A \in \mathrm{U}(n)$ commutes with all elements of $\mathbb{T}^n$. In particular, A commutes with $Z_{\pi,0,\dots,0}$. Let

$$A(e_1) = a_1e_1 + \cdots + a_ne_n.$$

Then

$$\begin{gathered} AZ_{\pi,0,\dots,0}(e_1) = A(-e_1) = -a_1e_1 - \cdots - a_ne_n, \\ Z_{\pi,0,\dots,0}A(e_1) = Z_{\pi,0,\dots,0}(a_1e_1 + \cdots + a_ne_n) = -a_1e_1 + a_2e_2 + \cdots + a_ne_n. \end{gathered}$$

Thus $a_2 = \cdots = a_n = 0$ and so $A(e_1) = c_1e_1$ for some $c_1 \in \mathbb{C}$. A similar argument shows that $A(e_k) = c_ke_k$ for each k. Since A is unitary, we must have $|c_k| = 1$ for each k and thus $A \in \mathbb{T}^n$.

(d) The case $n = 1$ is trivial and so we begin with the case $n = 2$. Suppose that

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

commutes will all elements of $\mathbb{T}^1$. Then A commutes with

$$Z_{\pi/2,-\pi/2} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

and thus

$$\begin{pmatrix} ai & -bi \\ ci & -di \end{pmatrix} = AZ_{\pi/2,-\pi/2} = Z_{\pi/2,-\pi/2}A = \begin{pmatrix} ai & bi \\ -ci & -di \end{pmatrix}.$$

Therefore $b = c = 0$. Then we must have $|a| = |d| = 1$ since A is unitary and $a = d^{-1}$ since A has determinant one. Therefore $A \in \mathbb{T}^1$. For $n > 2$, we leave it as an exercise to show that if $A \in \mathrm{SU}(n)$ commutes with $Z_{\pi,\pi,0,\dots,0}$ and $Z_{\pi,0,\pi,0,\dots,0}$ then $Ae_1 = c_1e_1$ for some $c_1 \in \mathbb{C}$. (Note that we could not use $Z_{\pi,0,\dots,0}$ as we did for the $\mathrm{U}(n)$ case since $\det Z_{\pi,0,\dots,0} = -1$.) Similarly, one can show that $Ae_k = c_ke_k$ for each k. Then the result follows as it did for the $\mathrm{U}(n)$ case.

(e) Suppose $A \in \mathrm{Sp}(n)$ commutes with all elements of $\mathbb{T}^n$. By the argument used for $\mathrm{U}(n)$, one can show that for all k, $Ae_k = c_ke_k$ for some $c_k \in \mathbb{H}$. But then the fact that A must commute with all elements of $\mathbb{T}^n$ shows that each c_k must commute with all $e^{i\theta}$, $\theta \in \mathbb{R}$. In particular, c_k must commute with i and thus $c_k \in \mathbb{R} + \mathbb{R}i$. We must also have $|c_k| = 1$ since $A \in \mathrm{Sp}(n)$ and so $A \in \mathbb{T}^n$. □

Remark 4.1.8. (a) Note that in our proofs, we only used the fact that A commuted with all elements of the torus in question. Thus it follows that these maximal tori are also maximal *abelian* subgroups of the respective Lie groups.

(b) Since $\mathbb{T}^k$ is connected, any maximal torus must lie in the identity component of the Lie group. Therefore, the maximal tori of $\mathrm{SO}(2m)$ and $\mathrm{SO}(2m+1)$ found above are also maximal tori of $\mathrm{O}(2m)$ and $\mathrm{O}(2m+1)$.

Remark 4.1.9. A noncompact Lie group need not have any nontrivial tori (for example, $\mathbb{R}^n$). However, the maximal tori in compact groups are well-behaved. In particular, we have the following results which we state without proof (at least for now) because the proofs use material we have not covered. They are useful facts that motivate some of the terminology we will use. Let G be a compact Lie group and T a maximal torus.

(a) Every conjugate of a maximal torus is a maximal torus.

(b) Every element $g \in G$ is conjugate to an element of T, hence lies in a maximal torus.

(c) All maximal tori in G are conjugate. So the maximal tori form a single conjugacy class in G.

(d) It follows that all maximal tori in G have the same dimension, called the *rank* of G.

Exercises.

4.1.1. Show that no reflection of the plane commutes with all rotations.

4.1.2. Show that $Z(G)$ is indeed a subgroup of G. In fact, show that it is a Lie subgroup of G.

4.2 Centres

We now determine the centres of the *compact classical groups* $\mathrm{SO}(n)$, $\mathrm{U}(n)$, $\mathrm{SU}(n)$ and $\mathrm{Sp}(n)$. Any element of the centre of a Lie groups commutes will all elements of the Lie group and thus with all elements of a maximal torus. Therefore, by the arguments of the previous section, the centres are contained in the maximal tori we described there. Note also that any scalar multiple of the identity $n \times n$ matrix commutes will all $n \times n$ matrices.

Theorem 4.2.1. *The compact classical groups have the following centres.*

(a) $Z(\mathrm{SO}(2)) = \mathrm{SO}(2)$*,* $Z(\mathrm{SO}(2m)) = \{\pm 1\}$*,* $m \geq 2$*.*

(b) $Z(\mathrm{SO}(2m+1)) = \{1\}$*,* $m \geq 1$*.*

(c) $Z(\mathrm{U}(n)) = \{\omega 1 \mid |\omega| = 1\}$*,* $n \geq 1$*.*

(d) $Z(\mathrm{SU}(n)) = \{\omega 1 \mid \omega^n = 1\}$*,* $n \geq 1$*.*

(e) $Z(\mathrm{Sp}(n)) = \{\pm 1\}$*,* $n \geq 1$*.*

Here $1 = I$ *is the identity matrix.*

Proof. All of the subgroups mentioned in the proposition consist of multiples of the identity matrix. Therefore, by the above comment, they are contained in the centres. It thus suffices to show that all elements of the centres lie in these subgroups.

(a) We know that $\mathrm{SO}(2)$ is abelian and so the first statement follows. Suppose $A \in Z(\mathrm{SO}(2m))$, $m \geq 2$. As noted, we can assume that A lies in the maximal torus $\mathbb{T}^m$. Thus $A = R_{\theta_1,\dots,\theta_m}$ for some $\theta_1, \dots, \theta_m \in \mathbb{R}$. Let

$$M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then R_θ commutes with M if and only if

$$\begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} M = M \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix}.$$

So R_θ commutes with M if and only if $\sin\theta = 0$, which implies $\cos\theta = \pm 1$.

Forming a matrix with (an even number of) copies of M on the diagonal (and all other entries zero), we see that A will commute with such matrices if and only if each $\sin\theta_k = 0$ and $\cos\theta_k = \pm 1$. Therefore, A is a diagonal matrix with diagonal entries ± 1. Suppose that both $+1$ and -1 occur. Then let B be the matrix with R_θ (with $\sin\theta \neq 0$) on the diagonal at the position of an adjacent $+1$ and -1 (and otherwise only 1's on the diagonal). Then A does not commute with B. Therefore $A = I$ or $A = -I$ as desired.

(b) We follow the argument for $\mathrm{SO}(2m)$. However, since $-I \neq \mathrm{SO}(2m+1)$, we conclude that $A = I$.

(c) If $n = 1$, then $\mathrm{U}(n)$ is isomorphic to $\mathbb{S}^1 = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$, which is abelian and thus $\mathrm{U}(1)$ is its own centre. Therefore we assume $n \geq 2$. Let $A \in Z(\mathrm{U}(n))$. Then $A = Z_{\theta_1,\dots,\theta_n}$ for some $\theta_1, \dots, \theta_n \in \mathbb{R}$. Note that $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathrm{U}(2)$ (in fact, it is in $\mathrm{SU}(2)$, something we will use in the next part) and

$$\begin{pmatrix} 0 & ie^{i\theta_1} \\ ie^{i\theta_2} & 0 \end{pmatrix} = \begin{pmatrix} e^{i\theta_1} & 0 \\ 0 & e^{i\theta_2} \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} e^{i\theta_1} & 0 \\ 0 & e^{i\theta_2} \end{pmatrix} = \begin{pmatrix} 0 & ie^{i\theta_2} \\ ie^{i\theta_1} & 0 \end{pmatrix}$$

if and only if $e^{i\theta_1} = e^{i\theta_2}$. Therefore, since A must commute with all matrices obtained by placing a $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ somewhere on the diagonal, 1's elsewhere on the diagonal, and zeros everywhere else, we see that $e^{i\theta_1} = \cdots = e^{i\theta_n}$. Therefore $A = e^{i\theta_1} I$ as desired.

(d) Let $A \in Z(\mathrm{SU}(n))$. The argument for $\mathrm{U}(n)$ shows that $A = \omega I$ for some $\omega \in \mathbb{C}$, $|w| = 1$. We must also have

$$1 = \det A = \omega^n,$$

as claimed.

Note: [Sti08] uses the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ instead of $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ for the proof of the $\mathrm{U}(n)$ and $\mathrm{SU}(n)$ cases. While this works for $\mathrm{U}(n)$, it is a problem for $\mathrm{SU}(n)$ since this matrix does not have determinant one.

(e) Let $A \in Z(\mathrm{Sp}(n))$. An argument similar to the one used for $\mathrm{U}(n)$ shows that $A = qI$ for some $q \in \mathbb{H}$ with $|q| = 1$. However, since this matrix must commute with all elements of $\mathrm{Sp}(n)$, it must, in particular, commute with I, iI, jI and kI. Thus, q must commute with all quaternions. But the only quaternions that commute with all other quaternions are the real numbers. Thus $q \in \mathbb{R}$. But then $|q| = 1$ implies that $q = \pm 1$ as desired.

□

4.3 Discrete subgroups and the centre

Recall that a subgroup H of a group G is *normal* if

$$gHg^{-1} = H \text{ for all } g \in G,$$

and G is *simple* if it has no nontrivial (i.e. not equal to $\{1\}$ or G) normal subgroups. It is easy to see that the centre $Z(G)$ of a group G is a normal subgroup of G. Thus if G has nontrivial centre, it is not simple. Therefore, by our computation of centres in the previous section, the groups $\mathrm{SO}(2m)$, $\mathrm{U}(n)$, $\mathrm{SU}(n)$ and $\mathrm{Sp}(n)$ are not simple. This leaves $\mathrm{SO}(2m+1)$ as the only possibility.

Given any two matrices $A, B \in M_n(\mathbb{C})$, we can consider the *distance* between them as points in $\mathbb{C}^{n^2}$. Thus, the distance $d(A, B)$ between A and B is

$$\sqrt{\sum_{1 \le i,j \le n} |a_{ij} - b_{ij}|^2}.$$

Definition 4.3.1 (Discrete subgroup)**.** A subgroup H of a Lie group G is called *discrete* if there is a positive lower bound to the distance between any two distinct elements of H. In other words H is discrete if there exists a $c > 0$ such that

$$d(A, B) > c \text{ for all } A, B \in H,\ A \neq B.$$

It follows immediately that any finite subgroup of G is discrete – just take c to be the minimum of the (finite number of) distances between elements of H. Thus, the centres of $\mathrm{SO}(n)$, $\mathrm{SU}(n)$, and $\mathrm{Sp}(n)$ are discrete. However, the centre of $\mathrm{U}(n)$ is not.

Theorem 4.3.2 (Schreier's Theorem)**.** *If G is a path-connected Lie group then any discrete normal subgroup is contained in the centre of G.*

Proof. Let H be a discrete normal subgroup of G. Then

$$BAB^{-1} \in H \text{ for all } A \in H,\ B \in G.$$

Fix $A \in H$. Then we have a continuous map

$$\varphi : G \to H, \quad \varphi(B) = BAB^{-1}.$$

Note that $\varphi(1) = A$. Let C be an arbitrary element of G. Since G is path-connected, there is a path from 1 to C. Since φ is continuous, it maps this path to a path in H. But H is discrete and so the image must be the single point A. In other words $\varphi B = BAB^{-1} = A$ or $BA = AB$ for all $B \in G$. Therefore $A \in Z(G)$. So $H \subseteq Z(G)$. □

We have seen that $\mathrm{SO}(n)$, $\mathrm{SU}(n)$, and $\mathrm{Sp}(n)$ are all path-connected. Therefore, their discrete normal subgroups are contained in their centres, which we have computed. Conversely, any subgroup of the centre is normal and so, in fact, we now know *all* the discrete normal subgroups of these Lie groups. In particular, since $Z(\mathrm{SO}(2m+1)) = \{1\}$, the Lie group $\mathrm{SO}(2m+1)$ has no nontrivial discrete normal subgroups.

We will see later that there are no normal subgroups of these Lie groups that are not discrete. In particular, it will follow that $\mathrm{SO}(2m+1)$ is simple and that the others are simple modulo their centres (i.e. $G/Z(G)$ is simple).

Chapter 5

Lie algebras and the exponential map

One of the most important methods for studying Lie groups is to study their associated Lie algebras. In this chapter we will investigate the notion of a Lie algebra and the connection between Lie algebras and Lie groups.

5.1 The exponential map onto SO(2)

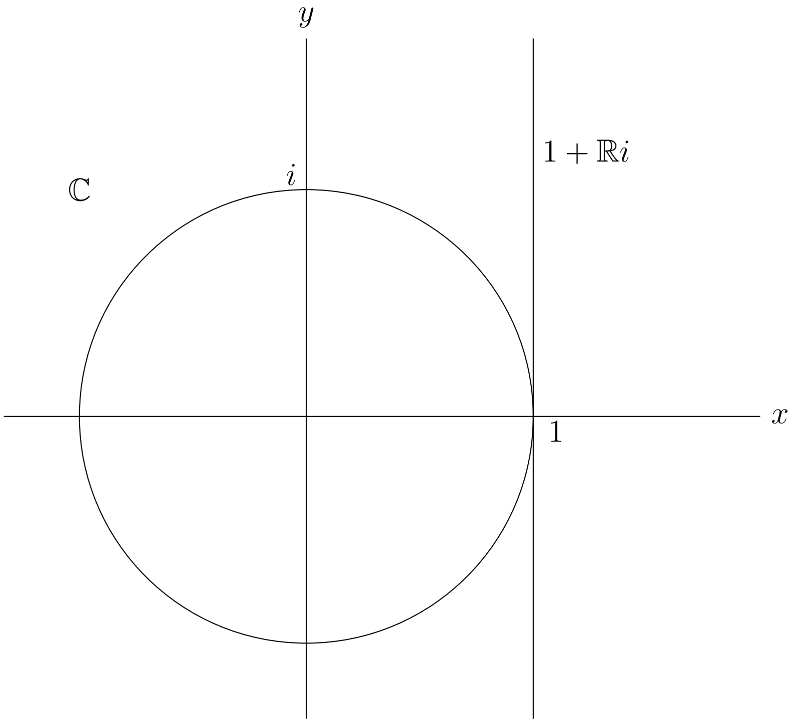
Recall the power series expansions

$$\begin{aligned} e^x &= 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots, \\ \cos x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots, \\ \sin x &= \frac{x}{1!} - \frac{x^3}{3!} + \dots. \end{aligned}$$

Since these series are absolutely convergent for all x, we can substitute $i\theta$ for x and rearrange terms to conclude that

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Therefore the exponential function maps the imaginary axis $\mathbb{R}i$ onto the circle $\mathbb{S}^1$ of points of absolute value one in the plane of complex numbers. We can view this imaginary axis as the tangent space to the identity of the Lie group $\mathbb{S}^1$.



While the tangent space is naturally the set $1+\mathbb{R}i$, we are only interested in coordinates relative to the point of tangency (i.e. we treat this point as the origin), and these relative coordinates are of the form $\mathbb{R}i$.

Note that the point $i\theta$ of height θ is mapped to the $\cos\theta + i\sin\theta$ at arc length θ and so the exponential map preserves the length of sufficiently small arcs.

5.2 The exponential map onto $\mathrm{SU}(2)$

For any pure imaginary quaternion v, we can define the usual exponential series

$$e^v = 1 + \frac{v}{1!} + \frac{v^2}{2!} + \frac{v^3}{3!} + \cdots .$$

For sufficiently large n, $|v|^n/n! < 2^{-n}$, and so this series is absolutely convergent in $\mathbb{H}$ (for the same reason as in $\mathbb{C}$).

Theorem 5.2.1 (Exponentiation theorem for $\mathbb{H}$)**.** *Let u be a unit vector in $\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$ (i.e. a unit pure imaginary quaterion) and $\theta \in \mathbb{R}$. Then*

$$e^{\theta u} = \cos\theta + u\sin\theta$$

and the exponential function maps $\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$ onto $\mathbb{S}^3 = \mathrm{SU}(2)$.

Proof. Recall that if u is a unit vector in $\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$, then $u^2=-1$. Therefore

$$e^{\theta u} = 1 + \frac{\theta u}{1!} - \frac{\theta^2}{2!} - \frac{\theta^3 u}{3!} + \cdots$$

$$\begin{aligned} &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots\right) + u\left(\frac{\theta}{1!} - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \cdots\right) \\ &= \cos\theta + u\sin\theta. \end{aligned}$$

Now, an arbitrary point of $\mathbb{S}^3$ (viewed as the set of unit quaternions) can be written as

$$a + bi + cj + dk = a + u|v|,$$

where u is a unit vector parallel to $v = bi + cj + dk$ and $|v| = \sqrt{b^2 + c^2 + d^2}$. Then

$$a^2 + |v|^2 = a^2 + b^2 + c^2 + d^2 = 1,$$

since we considered a unit quaternion. Therefore, there is a real number θ such that

$$a = \cos\theta, \quad |v| = \sin\theta.$$

Thus any point of $\mathbb{S}^3$ is of the form $\cos\theta + u\sin\theta$ for some unit vector u and so the exponential map above is onto. □

5.3 The tangent space of SU(2)

We will see that $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ is the tangent space to SU(2), just like $\mathbb{R}i$ is the tangent space to $\mathbb{S}^1$. We would like to find a way to compute the tangent space of a matrix Lie group in general. The key idea is that one should think of tangent vectors as "velocity vectors" of paths (or smoothly moving points) in our space (in this case, in our Lie group). This is same idea used in many areas of geometry: algebraic geometry, differential geometry, etc.

Suppose $q(t)$ is some smooth path in SU(2) passing through the identity at $t = 0$. So $q(t)$ is defined in some neighbourhood of zero (i.e. some interval containing $(-\epsilon, \epsilon)$ for some $\epsilon > 0$), takes values in SU(2) with $q(0) = 1$, and is differentiable.

Then the "velocity" $q'(0)$ at $t = 0$ is a tangent vector to SU(2) at the identity 1. Conversely, all tangent vectors arise in this way.

Since $q(t)$ is a unit quaternion for all t in the domain of q, we have

$$q(t)\overline{q(t)} = 1.$$

Differentiating, we get

$$q'(t)\overline{q(t)} + q(t)\overline{q'(t)} = 0. \tag{5.1}$$

Of course, we just blindly applied the product rule to a function taking quaternionic values. We should justify this. We simply follow the usual proof of the product rule:

$$\begin{aligned} \left.\frac{d}{dt}\right|_{t=a} q(t)\overline{q(t)} &= \lim_{h\to 0} \frac{q(a+h)\overline{q(a+h)} - q(a)\overline{q(a)}}{h} \\ &= \frac{(q(a+h) - q(a))\overline{q(a+h)} + q(a)(\overline{q(a+h) - q(a)})}{h} \\ &= q'(a)\overline{q(a)} + q(a)\overline{q'(a)}. \end{aligned}$$

Setting $t = 0$ in (5.1), we obtain

$$q'(0) + \overline{q'(0)} = 0.$$

This implies that $q'(0)$ is a pure imaginary quaternion. Therefore, every tangent vector to SU(2) at 1 is a pure imaginary quaternion.

Conversely, suppose that p is a pure imaginary quaternion. Then

$$pt \in \mathbb{R}i + \mathbb{R}j + \mathbb{R}k, \quad \text{for all } t \in \mathbb{R},$$

and hence $q(t) = e^{pt}$ is a path in SU(2) by Theorem 5.2.1. We have $q(0) = 1$, and $q(t)$ is smooth since

$$q'(t) = pe^{pt},$$

as can be seen from differentiating the power series for e^{pt}. Also,

$$q'(0) = pe^0 = p \cdot 1 = p,$$

and thus p is a tangent vector to SU(2) at 1. Therefore the tangent space of SU(2) at 1 is $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$.

The Lie bracket. Recall that, for $x, y \in \mathbb{R}i$, we have $e^x e^y = e^{x+y}$. Since the exponential map sends $\mathbb{R}i$ onto SO(2), this means that we can compute the product of elements on SO(2) using addition in $\mathbb{R}i$.

The case of SU(2) is different. Since addition $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ is commutative, it cannot describe the noncommutative product on SU(2). What we need is some operation on the tangent space that "measures" this noncommutativity. This operation cannot be multiplication of quaternions since $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ is not closed under multiplication.

Let U and V be two tangent vectors to SU(2) at 1 and let $u(s)$ and $v(t)$ be paths in SU(2) such that $u(0) = v(0) = 1$ and $u'(0) = U$, $v'(0) = V$. Note that

$$w_s(t) = u(s)v(t)u(s)^{-1}$$

gives us information about how the elements $u(s)$ and $v(s)$ commute (for instance, this equals $v(t)$ if and only if they commute). Note that the above equation defines a path (we think of s as being fixed and t as varying). We have

$$w_s(0) = u(s)v(0)u(s)^{-1} = 1,$$

and

$$w_s'(0) = u(s)v'(0)u(s)^{-1} = u(s)Vu(s)^{-1}$$

(use the definition of the derivative to see this).

Now, since $w_s(t)$ is a path through 1 for each s, $w_s'(0)$ is a tangent vector at 1 for each s. Therefore

$$x(s) = u(s)Vu(s)^{-1}$$

is a smooth path in $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$. Therefore, $x'(0)$ is also an element of $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ and

$$x'(0) = \left.\frac{d}{ds}\right|_{s=0} u(s)Vu(s)^{-1} = u'(0)Vu(0)^{-1} + u(0)V(-u'(0)) = UV - VU.$$

Here we have used the fact that $\frac{d}{ds}\big|_{s=0} u(s)^{-1} = -u'(0)$ if $u(0) = 1$ (see [Sti08, Exercise 4.3.2]).

We see that the map

$$(U, V) \mapsto [U, V]$$

is a binary operation on the tangent space $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ to SU(2) at the identity, which is related to the (non)commutativity of SU(2).

5.4 The Lie algebra $\mathfrak{su}(2)$ of SU(2)

Definition 5.4.1 (Lie algebra)**.** A *Lie algebra* is a vector space $\mathfrak{g}$ with a bilinear operation (the *Lie bracket*) $[\cdot,\cdot]\colon \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ that

- is *alternating*: $[X, X] = 0$ for all $X \in \mathfrak{g}$ (equivalently, if the field is not of characteristic 2, $[X, Y] = -[Y, X]$ for all $X, Y \in \mathfrak{g}$), and
- satisfies the *Jacobi identity*

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0.$$

If $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are Lie algebras, a homomorphism (resp. isomorphism) of Lie algebras is a linear map (resp. vector space isomorphism) $\varphi\colon \mathfrak{g}_1 \to \mathfrak{g}_2$ that commutes with the Lie bracket:

$$\varphi([X, Y]_1) = [\varphi(X), \varphi(Y)]_2$$

where $[\cdot,\cdot]_i$ denotes the Lie bracket on $[\cdot,\cdot]_i$, $i = 1, 2$.

Definition 5.4.2 ($\mathfrak{su}(2)$)**.** It follows from Exercise 5.4.1 that $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, with Lie bracket given by $[U, V] = UV - VU$ (i.e. the tangent space to SU(2) at the identity), is a Lie algebra. We denote this Lie algebra by $\mathfrak{su}(2)$.

One can show that $\mathbb{R}^3$ is a Lie algebra with bracket equal to the cross-product (see [Sti08, Exercises 1.4.1 and 1.4.4]).

Definition 5.4.3 (Ideal of a Lie algebra)**.** An *ideal* of a Lie algebra $\mathfrak{g}$ is a subspace $\mathfrak{a}$ of $\mathfrak{g}$ with the property that $[X, Y] \in \mathfrak{a}$ for all $X \in \mathfrak{g}$ and $Y \in \mathfrak{a}$.

The proof of the following lemma is left as an exercise (Exercise 5.4.2).

Lemma 5.4.4. *If $\varphi\colon \mathfrak{g}_1 \to \mathfrak{g}_2$ is a homomorphism of Lie algebras, then* $\ker\varphi$ *is an ideal of* $\mathfrak{g}_1$.

The following notion will be useful for us later.

Definition 5.4.5 (Simple Lie algebra)**.** A Lie algebra is *simple* if it has dimension at least two and it has no proper nonzero ideals.

Exercises.

5.4.1. Show that any vector space of matrices closed under matrix multiplication (more generally, any associative algebra) is a Lie algebra with bracket given by $[A, B] = AB - BA$.

5.4.2. Prove Lemma 5.4.4.

5.4.3. Show that $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ (with Lie bracket as in Definition 5.4.2) is isomorphic to $\mathbb{R}^3$ with the cross-product. Note that the isomorphism is not given by the "identity" map.

5.5 The exponential of square matrices

Recall that we identify $M_n(\mathbb{C})$ with $\mathbb{C}^{n^2}$ or $\mathbb{R}^{2n^2}$ and thus we have a *matrix absolute value*

$$\|A\| = \sqrt{\sum_{i,j} |a_{ij}|^2}, \quad A = (a_{ij}).$$

This is the distance from the origin to the point A. Similarly, if $A \in M_n(\mathbb{H})$, then $\|A\|$ is the distance from the origin to A in $\mathbb{R}^{4n^2}$ (where we identify $\mathbb{H}$ with $\mathbb{R}^4$).

If $A, A_1, A_2, \ldots$ are $n \times n$ matrices, we say

$$\lim_{m\to\infty} A_m = A$$

if

$$\forall\ \epsilon\ \exists\ M \text{ such that } \Big(m > M \implies \|A_m - A\| < \epsilon\Big).$$

Equivalently, $\lim_{m\to\infty} A_m = A$ if the limits of the entries of the A_m exists and equal the corresponding entries of A.

Proposition 5.5.1 (Submultiplicative property)**.** *If A and B are $n \times n$ real matrices, then $\|AB\| \leq \|A\|\|B\|$.*

Proof. Let $A = (a_{ij})$ and $B = (b_{ij})$ and $C = AB = (c_{ij})$. Then

$$\begin{aligned} |c_{ij}| &= |a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}| \\ &= |(a_{i1}, a_{i2}, \ldots, a_{in}) \cdot (b_{1j}, b_{2j}, \ldots, b_{nj})| \\ &\leq |(a_{i1}, a_{i2}, \ldots, a_{in})||(b_{1j}, b_{2j}, \ldots, b_{nj})| \quad \text{(Cauchy-Schwartz Inequality).} \end{aligned}$$

Thus

$$\begin{aligned} \|AB\|^2 &= \sum_{i,j} |c_{ij}|^2 \\ &\leq \sum_{i,j} (|a_{i1}|^2 + \cdots + |a_{in}|^2)(|b_{i1}|^2 + \cdots + |b_{in}|^2) \end{aligned}$$

$$= \sum_i (|a_{i1}|^2 + \cdots + |a_{in}|^2) \sum_j (|b_{i1}|^2 + \cdots + |b_{in}|^2)$$

$$= \|A\|^2 \|B\|^2.$$

Therefore $\|AB\| \leq \|A\| \|B\|$. □

Proposition 5.5.2 (Convergence of the matrix exponential)**.** *If A is any real $n \times n$ matrix, then*

$$I_n + \frac{A}{1!} + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots ,$$

is absolutely convergent in $\mathbb{R}^{n^2}$ and hence defines a function of A. This function is continuous.

Proof. The series

$$\|I_n\| + \frac{\|A\|}{1!} + \frac{\|A^2\|}{2!} + \frac{\|A^3\|}{3!} + \cdots$$

is a series of positive real numbers, whose terms (except for the first) are less than or equal to the corresponding terms of

$$1 + \frac{\|A\|}{1!} + \frac{\|A\|^2}{2!} + \frac{\|A\|^3}{3!} + \cdots$$

by the submultiplicative property. This is the power series for $e^{\|A\|}$ and thus it converges. Therefore the series in the proposition converges absolutely.

Since each A^m is continuous, the partial sums of the series are continuous. Since the series converges uniformly (exercise) on every set of the form $\{A \mid \|A\| \leq R\}$, $R > 0$, the sum is continuous. □

Remark 5.5.3. Recall that complex numbers can be viewed as 2×2 real matrices, and one can check that if Z is the matrix corresponding to the complex number z, then e^Z is the matrix corresponding to the complex number e^z. Thus, the exponential of a complex matrix may be represented by the exponential of a real matrix and so the series above also converges for complex matrices. Similarly, it converges for quaternionic matrices.

Definition 5.5.4 (Exponential of a matrix)**.** The exponential of an $n \times n$ (real, complex, or quaternionic) matrix A is

$$\exp A = e^A = I_n + \frac{A}{1!} + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots .$$

Remark 5.5.5. One can define an exponential in the more general setting of Riemannian manifolds, where it maps lines (through the origin) in the tangent space to geodesics through the tangent point. One can also define an exponential for arbitrary Lie groups by considering one-parameter subgroups.

Proposition 5.5.6 (Properties of the matrix exponential)**.** *Suppose X and Y are arbitrary $n \times n$ (real, complex, or quaternionic) matrices. Then we have the following.*

(a) $e^0 = I$.

(b) $(e^X)^* = e^{X^*}$.

(c) e^X *is invertible and* $(e^X)^{-1} = e^{-X}$.

(d) $e^{(\alpha+\beta)X} = e^{\alpha X}e^{\beta X}$ *for all* α *and* β *in* $\mathbb{C}$.

(e) If $XY = YX$*, then* $e^{X+Y} = e^X e^Y = e^Y e^X$.

(f) If C *is invertible, then* $e^{CXC^{-1}} = Ce^X C^{-1}$.

(g) $\|e^X\| \leq e^{\|X\|}$.

Proof. Part (a) is obvious. Part (b) follows by taking term-by-term adjoints (the adjoint of a sum is the sum of adjoints and $(X^m)^* = (X^*)^m$). Parts (c) and (d) are special cases of part (e). For part (e), we compute

$$\begin{aligned} e^X e^Y &= \left(I + X + \frac{X^2}{2!} + \cdots\right)\left(I + Y + \frac{Y^2}{2!} + \cdots\right) \\ &= \sum_{m=0}^{\infty}\sum_{k=0}^{m} \frac{X^k}{k!}\frac{Y^{m-k}}{(m-k)!} = \sum_{m=0}^{\infty}\frac{1}{m!}\sum_{k=0}^{m}\frac{m!}{k!(m-k)!}X^k Y^{m-k}. \end{aligned}$$

Now, *when* X *and* Y *commute*, we have

$$(X+Y)^m = \sum_{k=0}^{m}\frac{m!}{k!(m-k)!}X^k Y^{m-k},$$

and so

$$e^X e^Y = \sum_{m=0}^{\infty}\frac{1}{m!}(X+Y)^m = e^{X+Y}.$$

Part (f) follows from the fact that $(CXC^{-1})^m = CX^mC^{-1}$ and part (g) follows from our proof of the convergence of the exponential of matrices. □

Proposition 5.5.7. *Let* X *be a square complex matrix. Then* $t \mapsto e^{tX}$ *is a smooth curve in* $M_n(\mathbb{C})$ *and*

$$\frac{d}{dt}e^{tX} = Xe^{tX} = e^{tX}X.$$

In particular,

$$\left.\frac{d}{dt}e^{tX}\right|_{t=0} = X.$$

Proof. Since for each i, j, the entry $(e^{tX})_{ij}$ is given by a convergent power series in t, we can differentiate the series for e^{tX} term by term. The result follows easily. □

At some points, we may wish to explicitly compute the exponential of a matrix X. There is a general method for doing this.

Case 1: X is diagonalizable. If X is diagonalizable, then there exists an invertible matrix C such that $X = CDC^{-1}$ with

$$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

It is easy to check that

$$e^D = \begin{pmatrix} e^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix},$$

and so, by Proposition 5.5.6, we have

$$e^X = C \begin{pmatrix} e^{\lambda_1} & & 0 \\ 0 & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix} C^{-1},$$

Case 2: X is nilpotent. A matrix X is *nilpotent* if $X^m = 0$ for some $m > 0$ (hence $X^\ell = 0$ for all $\ell > m$). In this case the series for e^X terminates after the first m terms and so can be computed explicitly. For example (an example related to the Heisenberg group), if

$$X = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix},$$

then

$$X^2 = \begin{pmatrix} 0 & 0 & ac \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and $X^3 = 0$. Thus

$$e^X = \begin{pmatrix} 1 & a & b + ac/2 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

General case: X arbitrary. By a theorem in linear algebra, every matrix X can be written uniquely in the form $X = S + N$, with S diagonalizable, N nilpotent, and $SN = NS$. Therefore,

$$e^X = e^{S+N} = e^S e^N,$$

and we can compute e^S and e^N as in the previous cases.

5.6 The tangent space

Definition 5.6.1 (Smooth paths and their derivatives)**.** Let S be a space of matrices. We say that a path $t \mapsto A(t)$ is *smooth*, or *differentiable*, if the coordinate functions $a_{ij}(t)$ are differentiable. If $A(t)$ is smooth, its *derivative* $A'(t)$ is defined in the usual way by

$$\lim_{\Delta t \to 0} \frac{A(t+\Delta t) - A(t)}{\Delta t}.$$

Remark 5.6.2. It follows from the definition that $A'(t)$ is just the matrix with entries $a'_{ij}(t)$ where $a_{ij}(t)$ are the entries of $A(t)$.

Definition 5.6.3 (Tangent vectors and the tangent space)**.** The *tangent vectors* at the identity 1 of a matrix Lie group G are the matrices X of the form

$$X = A'(0)$$

where $A(t)$ is a smooth path in G with $A(0) = 1$. The *tangent space* to G at 1 is the set of all tangent vectors at 1.

Remark 5.6.4. We will see later (Proposition 5.10.1) that if X is a tangent vector at the identity to a matrix Lie group G, then $e^X \in G$. It follows that an equivalent definition of the tangent space is the set of all X such that $e^{tX} \in G$ for all $t \in \mathbb{R}$. (See Corollary 5.11.10 and Remark 5.11.11.) In fact, this is the definition used in [Hal03] and it will be useful to sometimes use this characterization when computing tangent spaces.

Proposition 5.6.5 (Tangent spaces of $\mathrm{O}(n)$, $\mathrm{U}(n)$ and $\mathrm{Sp}(n)$)**.** *The tangent spaces at the identity of the groups* $\mathrm{O}(n)$, $\mathrm{U}(n)$ *and* $\mathrm{Sp}(n)$ *are given as follows.*

(a) $\mathrm{O}(n)$*:* $\{X \in M_n(\mathbb{R}) \mid X + X^T = 0\}$.

(b) $\mathrm{U}(n)$*:* $\{X \in M_n(\mathbb{C}) \mid X + X^* = 0\}$.

(c) $\mathrm{Sp}(n)$*:* $\{X \in M_n(\mathbb{H}) \mid X + X^* = 0\}$.

Proof. Let $A(t)$ be a smooth path in $\mathrm{O}(n)$, $\mathrm{U}(n)$ or $\mathrm{Sp}(n)$ with $A(0) = 1$. Then

$$A(t)A(t)^* = 1 \qquad \text{for all } t$$

(note that $M^* = M^T$ for $M \in M_n(\mathbb{R})$). Taking the derivative with respect to t, we obtain

$$A'(t)A(t)^* + A(t)A'(t)^* = 0.$$

(There are a few technicalities here, which are left as an exercise. For instance, one should check that $\frac{d}{dt}(M^T) = (\frac{d}{dt}M)^T$, $\frac{d}{dt}\left(\overline{A(t)}\right) = \overline{A'(t)}$ – see Exercise 5.6.1.) Since $A(0) = 1$, we have

$$A'(0) + A'(0)^* = 0.$$

It follows that the tangent spaces are contained in the sets in the statement of the proposition.

Now suppose that a matrix X satisfies $X + X^* = 0$. Then e^{tX} is a path in the corresponding group since

$$e^{tX}(e^{tX})^* = e^{tX}e^{tX^*} = e^{tX}e^{-tX} = e^{t(X-X)} = e^0 = I.$$

Since $\frac{d}{dt}\Big|_{t=0} e^{tX} = X$, we see that X is in the tangent space. □

Definition 5.6.6 (Skew-symmetric and skew-Hermitian)**.** If $X \in M_n(\mathbb{R})$, we say X is *skew-symmetric* if $X + X^T = 0$. If $X \in M_n(\mathbb{C})$ or $X \in M_n(\mathbb{H})$, we say X is *skew-Hermitian* if $X + X^* = 0$.

Remark 5.6.7. From now on, when we refer to a *tangent vector* to a (matrix) Lie group G, we mean a tangent vector at the identity and by the *tangent space* of G, we mean the tangent space at the identity.

Proposition 5.6.8 (Tangent space of $\mathrm{SO}(n)$)**.** *The tangent space of* $\mathrm{SO}(n)$ *is the same as the tangent space of* $\mathrm{O}(n)$*, namely the space of real skew-symmetric matrices:*

$$\{X \in M_n(\mathbb{R}) \mid X + X^T = 0\}.$$

Proof. Since all paths in $\mathrm{SO}(n)$ are also paths in $\mathrm{O}(n)$, all tangent vectors to $\mathrm{SO}(n)$ are also tangent vectors to $\mathrm{O}(n)$ and hence are skew-symmetric. Conversely, let X be a skew-symmetric matrix. Then $t \mapsto e^{tX}$ is a path in $\mathrm{O}(n)$ with tangent vector X. Now, when $t = 0$, we have $e^{tX} = e^0 = I$, which has determinant one. Since all matrices in $\mathrm{O}(n)$ have determinant ±1 and e^{tX} is a continuous path, we must have $\det e^{tX} = 1$ for all real t. Therefore, $t \mapsto e^{tX}$ is actually a path in $\mathrm{SO}(n)$ and hence X is a tangent vector to $\mathrm{SO}(n)$. □

We cannot use the same type of argument we used for $\mathrm{SO}(n)$ to find the tangent space to $\mathrm{SU}(n)$ because elements of $\mathrm{U}(n)$ can have determinant equal to any unit complex number. To determine the tangent space of $\mathrm{SU}(n)$, we need the following result.

Proposition 5.6.9 (Determinant of the exponential)**.** *For any square complex matrix A,*

$$\det e^A = e^{\operatorname{tr} A}.$$

Proof. Suppose the result is true for upper triangular matrices. Then for an arbitrary complex matrix A, we can find an invertible complex matrix B and an upper triangular complex matrix T such that $A = BTB^{-1}$. Then

$$\det e^A = \det(e^{BTB^{-1}}) = \det(Be^TB^{-1}) = \det e^T = e^{\operatorname{tr} T} = e^{\operatorname{tr}(BTB^{-1})} = e^{\operatorname{tr} A}.$$

Thus, it suffices to show the result for an upper triangular matrix T. Suppose

$$T = \begin{pmatrix} t_{11} & * & * & \cdots & * \\ 0 & t_{22} & * & \cdots & * \\ 0 & 0 & t_{33} & \cdots & * \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & t_{nn} \end{pmatrix}.$$

Then for $k > 0$, T^k is upper triangular with ith diagonal entry equal to t_{ii}^k. Thus e^T is upper triangular with ith diagonal entry equal to $e^{t_{ii}}$. Therefore,

$$\det e^T = e^{t_{11}} e^{t_{22}} \cdots e^{t_{nn}} = e^{t_{11}+t_{22}+\cdots+t_{nn}} = e^{\operatorname{tr} T}.$$ □

Proposition 5.6.10 (Tangent space of $\mathrm{SU}(n)$)**.** *The tangent space of* $\mathrm{SU}(n)$ *is*

$$\{X \in M_n(\mathbb{C}) \mid X + X^* = 0,\ \operatorname{tr} X = 0\}.$$

Proof. Since any path in $\mathrm{SU}(n)$ is also a path in $\mathrm{U}(n)$, the tangent space to $\mathrm{SU}(n)$ is included in the tangent space to $\mathrm{U}(n)$. By Remark 5.6.4, it suffices to consider paths of the form $t \to e^{tX}$ in order to compute the tangent space of $\mathrm{SU}(n)$. Note that $t \mapsto e^{tX}$ is a path in $\mathrm{SU}(n)$ if and only if

$$\det e^{tX} = 1 \;\forall\, t \iff e^{t \operatorname{tr} X} = 1 \;\forall\, t \iff t \operatorname{tr} X = 0 \;\forall\, t \iff \operatorname{tr} X = 0.$$

The result follows. □

Proposition 5.6.11 (Tangent space of $\mathrm{GL}(n,\mathbb{C})$ and $\mathrm{SL}(n,\mathbb{C})$)**.** *The tangent space of* $\mathrm{GL}(n,\mathbb{C})$ *is* $M_n(\mathbb{C})$ *and the tangent space of* $\mathrm{SL}(n,\mathbb{C})$ *is*

$$\{X \in M_n(\mathbb{C}) \mid \operatorname{tr} X = 0\}.$$

Proof. The tangent space of $\mathrm{GL}(n,\mathbb{C})$ is contained in $M_n(\mathbb{C})$ by definition. Furthermore, for $X \in M_n(\mathbb{C})$, $t \mapsto e^{tX}$ is a path in $\mathrm{GL}(n,\mathbb{C})$ (recall that e^{tX} is always invertible) with tangent vector X. Hence the tangent space to $\mathrm{GL}(n,\mathbb{C})$ is all of $M_n(\mathbb{C})$.

The statement for $\mathrm{SL}(n,\mathbb{C})$ follows from Proposition 5.6.9. The details are left as an exercise (Exercise 5.6.3). □

The proof of the following proposition is left as an exercise (Exercise 5.6.4).

Proposition 5.6.12 (Some other tangent spaces)**.** *We have the following tangent spaces (where $J = J_{2n}$ is the matrix used to define the symplectic groups):*

(a) $\mathrm{O}(n,\mathbb{C})$, $\mathrm{SO}(n,\mathbb{C})$: $\{X \in M_n(\mathbb{C}) \mid X + X^T = 0\}$.

(b) $\mathrm{Sp}(n,\mathbb{R})$: $\{X \in M_n(\mathbb{R}) \mid JX^TJ = X\}$.

(c) $\mathrm{Sp}(n,\mathbb{C})$: $\{X \in M_n(\mathbb{C}) \mid JX^TJ = X\}$.

(d) Heisenberg group H: $\{X \in M_3(\mathbb{R}) \mid X$ *is strictly upper triangular*$\}$.

Exercises.

5.6.1. Suppose $A(t)$ is a smooth path in $M_n(\mathbb{C})$. Prove that $\frac{d}{dt}(A^T) = (\frac{d}{dt}A)^T$ and $\frac{d}{dt}\left(\overline{A(t)}\right) = \overline{A'(t)}$.

5.6.2. Show that the exponential map $\exp\colon \mathfrak{u}(n) \to U(n)$ is surjective. *Hint:* Recall that if A is a unitary matrix, then there is a unitary matrix U and a diagonal matrix D such that $A = UDU^*$. (The proof of this fact is similar to the proof of the analogous statement for symmetric matrices given in Section 3.2.)

5.6.3. Complete the proof of Proposition 5.6.11.

5.6.4. Prove Proposition 5.6.12.

5.7 The tangent space as a Lie algebra

The tangent space has interesting structure – it is a Lie algebra – reflecting the structure of the Lie group itself. To prove this, we need to define a Lie bracket and then show that the tangent space satisfies the axioms of a Lie algebra.

The first property we need to verify is that the tangent space is actually a vector space. We write $T_1(G)$ for the tangent space of G at the identity.

Proposition 5.7.1 (Tangent spaces are vector spaces)**.** *For any Lie group G, $T_1(G)$ is a real vector space.*

Proof. Suppose $X, Y \in T_1(G)$. Then there exists paths $A(t)$ and $B(t)$ in G such that $A(0) = B(0) = 1$, $A'(0) = X$ and $B'(0) = Y$. Then $C(t) = A(t)B(t)$ is also a smooth path in G (see Exercise 5.7.1) with $C(0) = 1$. Thus $C'(0) \in T_1(G)$. Now

$$C'(0) = \left.\frac{d}{dt}\right|_{t=0} A(t)B(t) = A'(0)B(0) + A(0)B'(0) = X + Y.$$

Therefore $X + Y \in T_1(G)$ and the tangent space is closed under vector addition.

Now let $r \in \mathbb{R}$. Since $D(t) = A(rt)$ is a smooth path in G and $D(0) = A(0) = 1$, we have $D'(0) \in T_1(G)$. Since

$$D'(0) = rA'(0) = rX,$$

we see that $rX \in T_1(G)$. Therefore $T_1(G)$ is also closed under scalar multiplication and hence is a vector space. □

It is straightforward to verify that $M_n(\mathbb{C})$ is a Lie algebra under the Lie bracket given by $[A, B] = AB - BA$ (see Exercise 5.4.1). Therefore, in order to show that $T_1(G)$ is a Lie algebra, it now suffices to show that it is closed under this Lie bracket (since then it is a Lie subalgebra of $M_n(\mathbb{C})$).

Proposition 5.7.2 (Tangent spaces are closed under the Lie bracket)**.** *For any Lie group G, the tangent space $T_1(G)$ is closed under the Lie bracket.*

Proof. Suppose $X, Y \in T_1(G)$. Then there exists paths $A(t)$ and $B(t)$ in G with $A(0) = B(0) = 1$, $A'(0) = X$, and $B'(0) = Y$.

For a fixed $s \in \mathbb{R}$, consider the path

$$C_s(t) = A(s)B(t)A(s)^{-1}.$$

Then $C_s(t)$ is smooth and $C_s(0) = 1$ and so $C_s'(0) \in T_1(G)$. Now,

$$C_s'(0) = A(s)B'(0)A(s)^{-1} = A(s)TA(s)^{-1}$$

is a smooth function of s since $A(s)$ is. Therefore $D(s) = A(s)YA(s)^{-1}$ defines a smooth path in $T_1(G)$ and so its tangent vector at $s = 0$ must also lie in $T_1(G)$ (the tangent of a path in some vector space is an element of that vector space). Now,

$$D'(0) = A'(0)YA(0)^{-1} + A(0)Y(-A'(0)) = XY - YX = [X, Y],$$

where we have used $A'(0) = X$, $A(0) = 1$ and $\left.\frac{d}{ds}\right|_{s=0} A(s) = -A'(0)$ when $A(0) = 1$ (see [Sti08, Exercise 4.3.2]). Hence $[X, Y] \in T_1(G)$ as desired. □

Definition 5.7.3 (Lie algebra of a Lie group)**.** The Lie algebra $\mathfrak{g}$ of a Lie group G is the tangent space $T_1(G)$ with the Lie bracket $[X,Y] = XY - YX$. We denote the Lie algebra of a particular Lie group by using lowercase gothic (Fraktur) letters. For instance, $\mathfrak{gl}(n,\mathbb{C})$ is the Lie algebra of $\mathrm{GL}(n,\mathbb{C})$, $\mathfrak{so}(n)$ is the Lie algebra of $\mathrm{SO}(n)$, etc. (One exception to this rule is that we will not assume that $\mathfrak{h}$ is the Lie algebra of the Heisenberg group H, since $\mathfrak{h}$ is often used for a Cartan subalgebra of a give Lie algebra.)

Example 5.7.4. By the results of Section 5.6, we have

$$\mathfrak{gl}(n,\mathbb{R}) = M_n(\mathbb{R}), \quad \mathfrak{gl}(n,\mathbb{C}) = M_n(\mathbb{C}),$$
$$\mathfrak{sl}(n,\mathbb{R}) = \{X \in M_n(\mathbb{R}) \mid \operatorname{tr} X = 0\}, \quad \mathfrak{sl}(n,\mathbb{C}) = \{X \in M_n(\mathbb{C}) \mid \operatorname{tr} X = 0\},$$
$$\mathfrak{o}(n) = \mathfrak{so}(n) = \{X \in M_n(\mathbb{R}) \mid X + X^T = 0\},$$
$$\mathfrak{o}(n,\mathbb{C}) = \mathfrak{so}(n,\mathbb{C}) = \{X \in M_n(\mathbb{C}) \mid X + X^T = 0\},$$
$$\mathfrak{u}(n) = \{X \in M_n(\mathbb{C}) \mid X + X^* = 0\},$$
$$\mathfrak{su}(n) = \{X \in M_n(\mathbb{C}) \mid X + X^* = 0,\ \operatorname{tr} X = 0\},$$
$$\mathfrak{sp}(n) = \{X \in M_n(\mathbb{H}) \mid X + X^* = 0\},$$
$$\mathfrak{sp}(n,\mathbb{R}) = \{X \in M_n(\mathbb{R}) \mid JX^TJ = X\}, \quad \mathfrak{sp}(n,\mathbb{C}) = \{X \in M_n(\mathbb{C}) \mid JX^TJ = X\}.$$

Remark 5.7.5. (a) One of the most important ideas in Lie theory is to study Lie groups by looking at their Lie algebras. Lie algebras are "flat" (i.e. they are vectors spaces) and are thus easier to study than "curved" Lie groups.

(b) While the Lie algebra captures a lot of information about the Lie group, it does not always capture G entirely. For instance, we have seen that $\mathrm{O}(n)$ and $\mathrm{SO}(n)$ have the same Lie algebra.

(c) We usually consider the tangent spaces at the identity but in fact all of the tangent spaces are isomorphic. This is because of the symmetry of a Lie group G given by multiplying by an element $g \in G$ (which maps the identity to g). See [Sti08, Exercises 5.4.4 and 5.4.5].

Since the Lie algebra of a Lie group is a real vector space, it has a dimension. In our particular examples, we can compute this dimension explicitly.

Proposition 5.7.6 (Dimension of $\mathfrak{so}(n)$, $\mathfrak{u}(n)$, $\mathfrak{su}(n)$, and $\mathfrak{sp}(n)$)**.** *As vector spaces over* $\mathbb{R}$*, we have*

(a) $\dim \mathfrak{so}(n) = n(n-1)/2$.

(b) $\dim \mathfrak{u}(n) = n^2$.

(c) $\dim \mathfrak{su}(n) = n^2 - 1$.

(d) $\dim \mathfrak{sp}(n) = n(2n+1)$.

Proof. (a) We know that

$$\mathfrak{so}(n) = \{X \in M_n(\mathbb{R}) \mid X = -X^T\}$$

is the space of skew-symmetric matrices. For a skew-symmetric matrix X, its diagonal entries are zero and its entries below the diagonal are determined by its entries above the diagonal (which can be arbitrary). Therefore, $\dim \mathfrak{so}(n)$ is the number of entries above the diagonal, which is

$$(n-1)+(n-2)+\cdots+1 = n(n-1)/2.$$

(b) We know that $\mathfrak{u}(n)$ is the space of skew-Hermitian matrices. Such matrices have pure imaginary entries on the diagonal and $n(n-1)/2$ arbitrary entries above the diagonal (which determine the entries below the diagonal). So the number of independent real parameters is

$$2 \cdot \frac{n(n-1)}{2} + n = n^2.$$

(c) We know that $\mathfrak{su}(n)$ is the space of skew-Hermitian matrices with trace zero. The condition of the trace being zero is the same as saying that the nth diagonal entry must be the negative of the sum of the other diagonal entries. Therefore, the number of independent real parameters is $n^2 - 1$.

(d) We know that $\mathfrak{sp}(n)$ consists of the skew-Hermitian quaternion matrices. Thus, as above, such a matrix has $n(n-1)/2$ quaternion entries above the diagonal (which determine the entries below the diagonal), and n pure imaginary quaternion entries on the diagonal. So the number of independent real parameters is

$$4 \cdot \frac{n(n-1)}{2} + 3n = n(2n+1). \qquad \square$$

Exercises.

5.7.1. Show that if $A(t)$ and $B(t)$ are smooth paths in a Lie group G, then $A(t)B(t)$ is also a smooth path in G.

5.8 Complex Lie groups and complexification

Recall that the Lie algebra of a Lie group is a *real vector space* (and the Lie bracket is bilinear for *real* scalars).

Definition 5.8.1 (Complex matrix Lie group)**.** A matrix Lie group $G \subseteq \mathrm{GL}(n,\mathbb{C})$ is *complex* if its Lie algebra is a complex subspace of $\mathfrak{gl}(n,\mathbb{C})$.

Definition 5.8.2 (Complexification of a vector space)**.** If V is a finite-dimensional real vector space, then the *complexification* of V, denoted $V_{\mathbb{C}}$, is the space of formal linear combinations

$$v_1 + iv_2$$

with $v_1, v_2 \in V$. This is a real vector space with "componentwise" addition and scalar multiplication given by

$$a(v_1 + iv_2) = av_1 + i(av_2), \quad a \in \mathbb{R}.$$

It is a complex vector space if we define

$$i(v_1 + iv_2) = -v_2 + iv_1.$$

We can identify V with the real subspace $\{v + i0 \in V_\mathbb{C}\}$ and so view V as a real subspace of $V_\mathbb{C}$.

Remark 5.8.3. (a) In terms of the tensor product, we have $V_\mathbb{C} = V \otimes_\mathbb{R} \mathbb{C}$.

(b) Suppose V is already a complex vector space. Then it is also a real vector space and we can form $V_\mathbb{C}$. Note that $V_\mathbb{C}$ is *not* equal to V. The dimension of $V_\mathbb{C}$ is always twice the dimension of V. In the language of tensor products, this non-equality comes from the fact that we are tensoring over $\mathbb{R}$ and not over $\mathbb{C}$. For example, $\mathbb{C}_\mathbb{C}$ is isomorphic (as a complex vector space) to $\mathbb{C}^2$.

Proposition/Definition 5.8.4 (Complexification of a Lie algebra)**.** *If $\mathfrak{g}$ is a finite-dimensional real Lie algebra, then the Lie bracket on $\mathfrak{g}$ has a unique extension to $\mathfrak{g}_\mathbb{C}$ which makes $\mathfrak{g}_\mathbb{C}$ into a complex Lie algebra, called the* complexification *of $\mathfrak{g}$.*

Proof. If such a Lie bracket on $\mathfrak{g}_\mathbb{C}$ exists, it must be given by

$$[X_1 + iX_2, Y_1 + iY_2] = ([X_1, Y_1] - [X_2, Y_2]) + i([X_1, Y_2] + [X_2, Y_1]), \quad X_1, X_2, Y_1, Y_2 \in \mathfrak{g}, \tag{5.2}$$

(by $\mathbb{C}$-bilinearity and the fact that the bracket on $\mathfrak{g}_\mathbb{C}$ must be an extension of the Lie bracket on $\mathfrak{g}$ – that is, the restriction of the Lie bracket on $\mathfrak{g}_\mathbb{C}$ to $\mathfrak{g}$ must agree with the original Lie bracket on $\mathfrak{g}$). Thus, the uniqueness result follows. For existence, we must show that the Lie bracket defined by (5.2) is $\mathbb{C}$-bilinear, skew-symmetric, and satisfies the Jacobi identity.

It is easy to see that the bracket defined by (5.2) is skew-symmetric, thus to show complex bilinearity, it suffices to show bilinearity in the first argument. Also, (5.2) is clearly *real* bilinear (since the bracket on $\mathfrak{g}$ is). So to show complex bilinearity, we only need to show that

$$[i(X_1 + iX_2), Y_1 + iY_2] = i[X_1 + iX_2, Y_2 + iY_2], \quad \text{for } X_1, X_2, Y_1, Y_2 \in \mathfrak{g}.$$

Now,

$$\begin{aligned} i[X_1 + iX_2, Y_2 + iY_2] &= i\big(([X_1, Y_1] - [X_2, Y_2]) + i([X_2, Y_1] + [X_1, Y_2])\big) \\ &= (-[X_2, Y_1] - [X_1, Y_2]) + i([X_1, Y_1] - [X_2, Y_2]) \\ &= [-X_2 + iX_1, Y_1 + iY_2] \\ &= [i(X_1 + iX_2), Y_1 + Y_2], \end{aligned}$$

as desired. We know that the Jacobi identity

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0$$

holds for $X, Y, Z \in \mathfrak{g}$. Now, the left hand side is complex linear in X. So for $X_1, X_2 \in \mathfrak{g}$, we have

$$\begin{gathered}[X_1 + iX_2, [Y, Z]] + [Y, [Z, X_1 + iX_2]] + [Z, [X_1 + iX_2, Y]] \\ = [X_1, [Y, Z]] + [Y, [Z, X_1]] + [Z, [X_1, Y]] + i\big([X_2, [Y, Z]] + [Y, [Z, X_2]] + [Z, [X_2, Y]]\big) = 0\end{gathered}$$

Thus the Jacobi identity holds for $X \in \mathfrak{g}_{\mathbb{C}}$ and $Y, Z \in \mathfrak{g}$. Since it is also complex linear in Y and Z, repeating the above argument then shows it holds for $X, Y, Z \in \mathfrak{g}_{\mathbb{C}}$. □

Remark 5.8.5. Note that the definition of complexification given in [Sti08, §5.6] is slightly different. Instead of considering formal expressions $X_1 + iX_2$ as above, [Sti08, §5.6] uses the fact that one considers spaces inside $\mathfrak{gl}(n, \mathbb{C})$, where complex multiplication is defined and $X_1 + iX_2$ is to be viewed as an expression is that space. Thus, for instance, $\mathfrak{gl}(n, \mathbb{C})_{\mathbb{C}} = \mathfrak{gl}(n, \mathbb{C})$ in [Sti08, §5.6] (whereas this is not the case in the above definition of complexification, as noted in Remark 5.8.3).

Proposition 5.8.6. *The Lie algebras $\mathfrak{gl}(n, \mathbb{C})$, $\mathfrak{sl}(n, \mathbb{C})$, $\mathfrak{so}(n, \mathbb{C})$, and $\mathfrak{sp}(n, \mathbb{C})$ are complex Lie algebras (hence $\mathrm{GL}(n, \mathbb{C})$, $\mathrm{SL}(n, \mathbb{C})$, $\mathrm{SO}(n, \mathbb{C})$, and $\mathrm{Sp}(n, \mathbb{C})$ are complex Lie groups). Furthermore, we have the following isomorphisms of complex Lie algebras.*

$$\begin{gathered}\mathfrak{gl}(n, \mathbb{R})_{\mathbb{C}} \cong \mathfrak{u}(n)_{\mathbb{C}} \cong \mathfrak{gl}(n, \mathbb{C}), \\ \mathfrak{su}(n)_{\mathbb{C}} \cong \mathfrak{sl}(n, \mathbb{R})_{\mathbb{C}} \cong \mathfrak{sl}(n, \mathbb{C}), \\ \mathfrak{so}(n)_{\mathbb{C}} \cong \mathfrak{so}(n, \mathbb{C}), \\ \mathfrak{sp}(n, \mathbb{R})_{\mathbb{C}} \cong \mathfrak{sp}(n)_{\mathbb{C}} \cong \mathfrak{sp}(n, \mathbb{C}).\end{gathered}$$

Proof. The first statement is left as an easy exercise. Every $X \in \mathfrak{gl}(n, \mathbb{C})$ can be written uniquely in the form $X_1 + iX_2$ where $X_1, X_2 \in \mathfrak{gl}(n, \mathbb{R})$. This gives an isomorphism of complex vector spaces between $\mathfrak{gl}(n, \mathbb{R})_{\mathbb{C}}$ and $\mathfrak{gl}(n, \mathbb{C})$. It is easy to check (exercise) that this isomorphism commutes with the Lie bracket and is thus an isomorphism of complex Lie algebras. Similarly, $\mathfrak{sl}(n, \mathbb{R})_{\mathbb{C}} \cong \mathfrak{sl}(n, \mathbb{C})$.

Also, for $X \in \mathfrak{gl}(n, \mathbb{C})$, we have

$$X = \frac{X - X^*}{2} + i\frac{X + X^*}{2i},$$

and $(X - X^*)/2$ and $(X + X^*)/2i$ are both skew-symmetric. To show that this decomposition is unique, suppose

$$X = X_1 + iX_2, \quad X_1, X_2 \in \mathfrak{u}(n).$$

Then

$$\begin{aligned}X + X^* = (X_1 + iX_2) + (X_1 + iX_2)^* = (X_1 + iX_2) + (X_1^* - iX_2^*) \\ = X_1 + iX_2 - X_1 + iX_2 = 2iX_2.\end{aligned}$$

and

$$X - X^* = (X_1 + iX_2) - (X_1 + iX_2)^* = X_1 + iX_2 - X_1^* + iX_2^*$$

$$= X_1 + iX_2 + X_1 - iX_2 = 2X_1.$$

Thus

$$X_1 = (X - X^*)/2, \quad X_2 = (X + X^*)/2i,$$

and so the decomposition is unique. Therefore $\mathfrak{u}(n)_{\mathbb{C}} \cong \mathfrak{gl}(n, \mathbb{C})$. Since X has trace zero if and only if X_1 and X_2 do, we see that $\mathfrak{su}(n)_{\mathbb{C}} \cong \mathfrak{sl}(n, \mathbb{C})$.

The other proofs are analogous. □

Definition 5.8.7 (Real forms)**.** Suppose $\mathfrak{g}$ is a complex Lie algebra. A real Lie algebra $\tilde{\mathfrak{g}}$ is called a *real form* of $\mathfrak{g}$ if $\tilde{\mathfrak{g}}_{\mathbb{C}} \cong \mathfrak{g}$.

So, for example, $\mathfrak{gl}(n, \mathbb{R})$ and $\mathfrak{u}(n)$ are real forms of $\mathfrak{gl}(n, \mathbb{C})$. Note however that $\mathfrak{gl}(n, \mathbb{R})$ and $\mathfrak{u}(n)$ are *not* isomorphic (real) Lie algebras, except when $n = 1$.

5.9 The matrix logarithm

Our goal is to give a (more) precise relationship between a Lie group and its Lie algebra. We have the exponential map which maps the Lie algebra into the Lie group. We now consider the inverse map.

In this course, the notation log will mean $\log_e$. Recall the series for $\log(1 + x)$:

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots, \quad x \in \mathbb{R}, \ |x| < 1.$$

Definition 5.9.1 (Matrix logarithm)**.** For a square matrix $I + A$ with $\|A\| < 1$, we define its *logarithm* by

$$\log(I + A) = A - \frac{A^2}{2} + \frac{A^3}{3} - \cdots.$$

By the submultiplicative property, we know this series is absolutely convergent for $\|A\| < 1$ and so $\log(I + A)$ is a well-defined continuous function in this neighbourhood of I.

Proposition 5.9.2 (Inverse property of the matrix logarithm)**.** *(a) For any matrix X such that $\|e^X - I\| < 1$, we have*

$$\log(e^X) = X.$$

(b) For any matrix X such that $\|X - I\| < 1$, we have

$$e^{\log X} = X.$$

Proof. By the definition of the matrix logarithm, we have

$$\begin{aligned}\log(e^X) &= \log(I + (e^x - I)) \\ &= \log\left(I + \left(\frac{X}{1!} + \frac{X^2}{2!} + \dots\right)\right) \\ &= \left(\frac{X}{1!} + \frac{X^2}{2!} + \dots\right) - \frac{1}{2}\left(\frac{X}{1!} + \frac{X^2}{2!} + \dots\right)^2 + \frac{1}{3}\left(\frac{X}{1!} + \frac{X^2}{2!} + \dots\right)^3 - \dots.\end{aligned}$$

Since the series are absolutely convergent, we can rearrange terms. Collecting powers of X^m gives

$$\log(e^X) = X + \left(\frac{1}{2!} - \frac{1}{2}\right) X^2 + \left(\frac{1}{3!} - \frac{1}{2} + \frac{1}{3}\right) X^3 + \dots .$$

The coefficient in front of X^m for $m \geq 2$ is exactly the same as the coefficient that appears in the expansion of $\log(e^x)$ for a real number x with $|e^x - 1| < 1$. Since we know that $\log(e^x) = x$ for such x, these coefficients are zero. Therefore $\log(e^X) = X$ as desired.

Similarly, if $\|X - I\| < 1$, we have

$$\begin{aligned}\exp(\log X) &= \exp(\log(I + (X - I))) \\ &= \exp\left((X - I) - \frac{(X-I)^2}{2} + \frac{(X-I)^3}{3} - \dots\right) \\ &= I + \left((X - I) - \frac{(X-I)^2}{2} + \dots\right) + \frac{1}{2!}\left((X - I) - \frac{(X-I)^2}{2} + \dots\right)^2 + \cdots .\end{aligned}$$

Again, since the series are absolutely convergent, we can rearrange terms. We collect powers of X^m and use the fact that $e^{\log x} = x$ for $x \in \mathbb{R}$, $|x - 1| < 1$, to conclude that $e^{\log X} = X$. □

Proposition 5.9.3 (Multiplicative property of the matrix logarithm). *If $AB = BA$ and $\log A$, $\log B$ and $\log(AB)$ are all defined, then*

$$\log(AB) = \log A + \log B.$$

Proof. Let $X = \log A$ and $Y = \log B$. Then

$$\begin{aligned}X &= \log(I + (A - I)) = (A - I) - \frac{(A-I)^2}{2} + \frac{(A-I)^3}{3} - \dots, \\ Y &= \log(I + (B - I)) = (B - I) - \frac{(B-I)^2}{2} + \frac{(B-I)^3}{3} - \dots .\end{aligned}$$

Since A and B commute, these series commute, hence X and Y commute. Thus

$$AB = e^X e^Y = e^{X+Y}.$$

Taking log of both sides, we get

$$\log(AB) = \log(e^{X+Y}) = X + Y = \log A + \log B,$$

by the inverse property of the matrix logarithm. □

5.10 The exponential mapping

When we computed the tangent spaces of the classical groups, we used the explicit defining equations (such at $AA^* = I$) to find an equation defining the Lie algebra and then used the exponential map to show that *all* matrices satisfying this defining equation are in the tangent space. However, in an arbitrary (matrix) Lie group, we may not have these explicit defining equations at our disposal. So we need a more general (abstract) approach.

Proposition 5.10.1 (Exponentiation of tangent vectors)**.** *If X is a tangent vector at the identity to a matrix Lie group G, then $e^X \in G$. In other words,* exp *maps the tangent space $T_1(G)$ into G.*

Proof. Suppose $A(t)$ is a smooth path in G with $A(0) = I$ and $A'(0) = X$. Then

$$X = A'(0) = \lim_{\Delta t \to 0} \frac{A(\Delta t) - 1}{\Delta t} = \lim_{n \to \infty} \frac{A(1/n) - 1}{1/n}.$$

Now, using the definition of the logarithm of a square matrix, we have

$$\begin{aligned} \log A(1/n) &= \log(I + (A(1/n) - I)) \\ &= (A(1/n) - I) - \frac{(A(1/n) - I)^2}{2} + \frac{(A(1/n) - I)^3}{3} - \cdots . \end{aligned}$$

Multiplying both sides by n (or dividing by $1/n$) gives

$$n \log A(1/n) = \frac{A(1/n) - I}{1/n} - \frac{A(1/n) - I}{1/n} \left(\frac{A(1/n) - I}{2} - \frac{(A(1/n) - I)^2}{3} + \cdots \right). \quad (5.3)$$

Now, since we are interested in the limit as $n \to \infty$, we can restrict our attention to $n > N$ for some $N > 0$. Also, since $A(0) = I$ and $A(t)$ is continuous, for all $0 < \epsilon < 1/2$, there exists an $N > 0$ such that $\|A(1/n) - I\| < \epsilon < 1/2$ for $n > N$. Then the series in parentheses has a sum of absolute value less than

$$\epsilon + \epsilon^2 + \epsilon^3 + \cdots = \frac{\epsilon}{1 - \epsilon} < 2\epsilon,$$

and so this sum tends to zero as $n \to \infty$. Therefore, by (5.3), we have

$$\lim_{n \to \infty} n \log A(1/n) = A'(0) - A'(0)0 = A'(0) = X.$$

Exponentiating both side of this equation, we obtain

$$\begin{aligned} e^X &= e^{\lim_{n \to \infty} n \log A(1/n)} \\ &= \lim_{n \to \infty} e^{n \log A(1/n)} && \text{(since exp is continuous)} \\ &= \lim_{n \to \infty} \left(e^{\log A(1/n)} \right)^n && \text{(since } e^{A+B} = e^A e^B \text{ when } AB = BA) \\ &= \lim_{n \to \infty} A(1/n)^n && \text{(since exp is the inverse of log).} \end{aligned}$$

Now, $A(1/n) \in G$ since $A(t)$ is a path in G. Thus $A(1/n)^n \in G$ since G is a group (i.e. closed under products). Thus we have a convergent sequence of elements of G. The limit is nonsingular since the limit, e^X, has inverse e^{-X}. Therefore, by the closure property of (matrix) Lie groups, $e^X \in G$ as desired. □

Remark 5.10.2. This is the first time we have really made use of the closure (under limits) property of a Lie group.

We have seen examples where every element of a Lie group G is the exponential of an element of its Lie algebra (for instance, SO(2) and SU(2)). This also turns out to be true for $\mathrm{GL}(n,\mathbb{C})$ (i.e. every invertible complex matrix is the exponential of some $n \times n$ matrix). However, this is not true for all matrix Lie groups.

Consider, for example

$$A = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{C}).$$

We claim that there is no $X \in \mathfrak{sl}(2,\mathbb{C})$ such that $e^X = A$. Let X be an arbitrary matrix in $\mathfrak{sl}(2,\mathbb{C})$. Then $\operatorname{tr} X = 0$ and so the two eigenvalues of X are negatives of each other. If both eigenvalues are zero, then e^X has 1 as an eigenvalue since if v is an eigenvector of X with eigenvalue 0, then

$$e^X v = (I + X + \cdots)\, v = v.$$

But A does not have 1 as an eigenvalue and so $e^X \neq A$. Therefore, the eigenvalues of X must be distinct. Thus X is diagonalizable and hence e^X is diagonalizable. But A is not diagonalizable. Therefore $e^X \neq A$.

Therefore, we see that the exponential mapping is not always onto. It is also not always one-to-one (remember the example of $\mathbb{S}^1 \cong \mathrm{SO}(2)$). However, we will see that it is *locally* one-to-one and onto.

Remark 5.10.3. A natural question one might ask is "what is the image of the exponential map?" This is actually a highly nontrivial question and the answer is not known in general, although there has been some progress towards answering it.

5.11 The logarithm into the tangent space

We have shown that exp maps the Lie algebra into the Lie group. The next natural question is "Does the logarithm map the Lie group into the Lie algebra?" We first consider a slightly modified notion of a tangent vector which will be useful.

Definition 5.11.1. X is a *sequential tangent vector* to G at 1 if there is a sequence (A_m) of elements of G, and a sequence (α_m) of real numbers, such that

$$\lim_{m\to\infty} A_m = 1, \qquad \lim_{m\to\infty} \frac{A_m - 1}{\alpha_m} = X.$$

Note that the difference between this definition and the usual definition of a tangent vector is that we take a *sequence* and not a continuous limit.

Proposition 5.11.2. *We have that X is a sequential tangent vector to a Lie group G if and only if it is a tangent vector to G.*

Proof. Suppose X is a tangent vector to G. Then there exists a path $A(t)$ in G with $A(0) = I$ and $A'(0) = X$. Then the sequence $(A_m = A(1/m))$ tends to I and

$$\lim_{m\to\infty} \frac{A_m - I}{1/m} = A'(0) = X$$

and so X is a sequential tangent vector.

Now suppose that X is a sequential tangent vector. Then there is a sequence (A_m) in G, and a sequence (α_m) of real numbers, such that

$$\lim_{m\to\infty} A_m = I, \qquad \lim_{m\to\infty} \frac{A_m - I}{\alpha_m} = X. \tag{5.4}$$

Our goal is to show that $e^{tX} \in G$ for all $t \in \mathbb{R}$. Then X is the tangent vector to this path.

We first show that $e^X \in G$. It follows from (5.4) that $\alpha_m \to 0$ as $m \to \infty$. Thus $1/\alpha_m \to \infty$. Let

$$a_m = \text{nearest integer to } 1/\alpha_m.$$

Then we also have

$$\lim_{m\to\infty} a_m(A_m - I) = X,$$

since

$$\left\| \frac{1}{\alpha_m}(A_m - I) - a_m(A_m - I) \right\| = \left\| \left(\frac{1}{\alpha_m} - a_m \right)(A_m - I) \right\| < \|A_m - I\| \to 0 \text{ as } m \to \infty.$$

Since a_m is an integer, by the multiplicativity property of the logarithm, we have

$$\log(A_m^{a_m}) = a_m \log(A_m) = a_m(A_m - I) - a_m(A_m - I)\left(\frac{A_m - I}{2} - \frac{(A_m - I)^2}{3} + \cdots \right).$$

As before, we know that the terms in parenthesis tends to zero as $m \to \infty$. Thus

$$X = \lim_{m\to\infty} a_m(A_m - I) = \lim_{m\to\infty} \log(A_m^{a_m}).$$

Therefore

$$e^X = e^{\lim_{m\to\infty} \log(A_m^{a_m})} = \lim_{m\to\infty} e^{\log(A_m^{a_m})} = \lim_{m\to\infty} A_m^{a_m}.$$

Since a_m is an integer, $A_m^{a_m} \in G$. Then by the closure of G under limits, we have $e^X \in G$.

Now, to show that $e^{tX} \in G$ for all $t \in \mathbb{R}$, replace $1/\alpha_m$ in the above argument by t/α_m and let

$$b_m = \text{nearest integer to } t/\alpha_m.$$

Then we have

$$\lim_{m\to\infty} b_m(A_m - I) = tX.$$

If we consider the series for

$$\log(A_m^{b_m}) = b_m \log(A_m)$$

and argue as above, we find that

$$e^{tX} = \lim_{m\to\infty} A_m^{b_m} \in G. \qquad \square$$

Remark 5.11.3. The argument used in the above proof (namely, the passage from a sequence to a smooth path) is an essential ingredient in proving that matrix Lie groups are smooth manifolds.

Definition 5.11.4. A *neighbourhood* of 1 in G is a set of the form

$$N_\delta(1) = \{A \in G \mid \|A - 1\| < \delta\},$$

for some $\delta > 0$. The above set is called a δ*-neighbourhood* of 1.

Proposition 5.11.5 (The logarithm of a neighbourhood of 1)**.** *For any matrix Lie group G there is a neighbourhood $N_\delta(1)$ mapped into $T_1(G)$ by the logarithm.*

Proof. We prove the claim by contradiction. Suppose that no neighbourhood of 1 is mapped into $T_1(G)$ by the logarithm. Then there exists a sequence (A_m) in G with $\lim_{m\to\infty} A_m = 1$ and $\log A_m \notin T_1(G)$ for all m.

Since, by the definition of a matrix Lie group, G is contained in some $M_n(\mathbb{C})$, we have $\log A_m \in M_n(\mathbb{C})$ and we can write (uniquely)

$$\log A_m = X_m + Y_m,$$

where $X_m \in T_1(G)$ and $0 \neq Y_m \in T_1(G)^\perp$ where $T_1(G)$ is the orthogonal complement to $T_1(G)$ in $M_n(\mathbb{C})$. Since log is continuous and $A_m \to 1$, we have $X_m, Y_m \to 0$.

Consider the matrices

$$\frac{Y_m}{\|Y_m\|} \in T_1(G)^\perp.$$

These all have absolute value 1 and so lie on the sphere of radius 1 and centre 0 in $T_1(G)^\perp$. Since this sphere is bounded, there is a convergent subsequence, whose limit Y is a vector of absolute value 1 in $T_1(G)^\perp$. We replace our original sequence with this subsequence and thus have

$$\lim_{m\to\infty} \frac{Y_m}{\|Y_m\|} = Y.$$

Now consider the sequence of terms

$$T_m = e^{-X_m} A_m.$$

Since $e^{-X_m} \in G$ (we know that exp maps tangent vectors into G) and $A_m \in G$, we have $T_m \in G$ for all m. Also, by the inverse property of log, we have $A_m = e^{X_m + Y_m}$. Therefore

$$\begin{aligned} T_m &= e^{-X_m} e^{X_m+Y_m} \\ &= \left(I - X_m + \frac{X_m^2}{2!} + \dots\right)\left(I + X_m + Y_m + \frac{(X_m+Y_m)^2}{2!} + \dots\right) \\ &= I + Y_m + \text{ higher order terms.} \end{aligned}$$

Now, the higher order terms in X_m that do not involve any positive power of Y_m are exactly the terms that appear in the expansion of $e^{-X_m} e^{X_m} = I$ and so they sum to zero. Therefore

$$\lim_{m\to\infty} \frac{T_m - I}{\|Y_m\|} = \lim_{m\to\infty} \frac{Y_m}{\|Y_m\|} = Y.$$

Since each $\|Y_m\| \to 0$, we have $T_m \to I$ and thus Y is a sequential tangent vector. Therefore, by Proposition 5.11.2, it is a tangent vector and so lies in $T_1(G)$. But we saw above that

$0 \neq Y \in T_1(G)^\perp$ and so $Y \notin T_1(G)$. This contradiction demonstrates that our initial assumption was false. Therefore there is a neighbourhood of the identity mapped into $T_1(G)$ by log. □

Corollary 5.11.6. *There exists $\delta > 0$ such that the* log *and* exp *functions give a bijection, continuous in both directions, between $N_\delta(1)$ in G and $\log N_\delta(1)$ in $T_1(G)$.*

Remark 5.11.7. A continuous bijection with continuous inverse is called a *homeomorphism* (it is an isomorphism in the category of topological spaces). It follows from Corollary 5.11.6 that the *topological dimension* (a concept we have not defined) of a Lie group G is equal to the dimension of its Lie algebra.

Corollary 5.11.8. *If G is a connected matrix Lie group, then every element $A \in G$ can be written in the form*

$$A = e^{X_1} e^{X_2} \dots e^{X_m},$$

for some $X_1, \dots, X_m \in \mathfrak{g}$.

For the following proof, we need to use a well-known property of compact sets: If X is a compact set and $(U_\alpha)_{\alpha \in A}$ is a collection of open sets in X such that $\bigcup_{\alpha \in A} U_\alpha = X$, then there exists a finite subset $A' \subseteq A$ such that $\bigcup_{\alpha \in A'} U_\alpha = X$. In fact, this is the *defining* property of compact sets in general – our characterization of compact sets as closed and bounded sets in $\mathbb{C}^n$ or $\mathbb{R}^n$ is equivalent (for subsets of $\mathbb{C}^n$ and $\mathbb{R}^n$).

Proof. Let V be a neighbourhood of I in G as in Corollary 5.11.6. Since G is connected, we can find a continuous path $\gamma\colon [0,1] \to G$ with $\gamma(0) = I$ and $\gamma(1) = A$. Since γ is continuous and $[0,1]$ is compact, the image $\gamma([0,1])$ is also compact. Now, consider the collection $\{g \cdot V \mid g \in \gamma([0,1])\}$. Since $g \in g \cdot V \overset{\text{def}}{=} \{g \cdot h \mid h \in V\}$, we have

$$\gamma([0,1]) \subseteq \bigcup_{g \in \gamma([0,1])} g \cdot V.$$

Thus, since $\gamma([0,1])$ is compact, there is a finite set $S \subseteq \gamma([0,1])$ with $\gamma([0,1]) \subseteq \bigcup_{g \in S} g \cdot V$. Thus we can choose a sequence $0 = t_0 < t_1 < t_2 < \dots < t_m = 1$ and $I = A_0 = \gamma(t_0), A_1 = \gamma(t_1), \dots, A_m = \gamma(t_m) = A$ with

$$A_{i-1}^{-1} A_i \in V \quad \text{for all } 1 \leq i \leq m.$$

By the definition of V, we can find $X_i \in \mathfrak{g}$ with $e^{X_i} = A_{i-1}^{-1} A_i$ for $i = 1, \dots, m$. Then

$$A = (A_0^{-1} A_1)(A_1^{-1} A_2) \cdots (A_{m-1}^{-1} A_m) = e^{X_1} \cdots e^{X_m}.$$ □

Remark 5.11.9. The key idea in the above proof is that connected Lie groups are generated by a neighbourhood of the identity.

The proof of the following corollary is left as an exercise (Exercise 5.11.1).

Corollary 5.11.10 (An alternate description of the Lie algebra)**.** *Suppose $G \subseteq \mathrm{GL}(n, \mathbb{C})$ is a matrix Lie group with Lie algebra $\mathfrak{g}$. Then $X \in M_n(\mathbb{C})$ is in $\mathfrak{g}$ if and only if $e^{tX} \in G$ for all $t \in \mathbb{R}$.*

Remark 5.11.11. By Corollary 5.11.10, we could *define* the Lie algebra of G to be the set of all matrices X such that $e^{tX} \in G$ for all $t \in \mathbb{R}$. This is the approach adopted in [Hal03].

Exercises.

5.11.1. Prove Corollary 5.11.10.

5.12 Some more properties of the exponential

Lemma 5.12.1. *There exists a constant c such that for all $B \in M_n(\mathbb{C})$ with $\|B\| < \frac{1}{2}$, we have*

$$\|(\log(I+B)) - B\| \leq c\|B\|^2.$$

Proof. Since

$$\log(I+B) - B = \sum_{m=2}^{\infty} (-1)^{m+1} \frac{B^m}{m} = B^2 \sum_{m=2}^{\infty} (-1)^{m+1} \frac{B^{m-2}}{m},$$

we have

$$\|\log(I+B) - B\| \leq \|B\|^2 \sum_{m=2}^{\infty} \frac{\left(\frac{1}{2}\right)^{m-2}}{m}.$$

Since the sum in the last expression is convergent, we are done. □

Proposition 5.12.2 (Lie product formula)**.** *If $X, Y \in M_n(\mathbb{C})$, then*

$$e^{X+Y} = \lim_{m\to\infty} \left(e^{X/m} e^{Y/m}\right)^m.$$

Proof. Multiplying the series for $e^{X/m}$ and $e^{Y/m}$ we get

$$e^{X/m} e^{Y/m} = I + \frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right).$$

For sufficiently large m, X/m and Y/m are in the domain of the logarithm, and thus $e^{X/m}e^{Y/m} \to I$ as $m \to \infty$. Now, by Lemma 5.12.1, we have

$$\begin{aligned}
\log\left(e^{X/m} e^{Y/m}\right) &= \log\left(I + \frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right)\right) \\
&= \frac{X}{m} + \frac{Y}{m} + O\left(\left\|\frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right)\right\|^2\right) \\
&= \frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right).
\end{aligned}$$

Exponentiating gives

$$e^{X/m}e^{Y/m} = \exp\left(\frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right)\right)$$

and so

$$\left(e^{X/m}e^{Y/m}\right)^m = \exp\left(X + Y + O\left(\frac{1}{m}\right)\right).$$

Since exp is continuous, we have

$$\lim_{m\to\infty} \left(e^{X/m}e^{Y/m}\right)^m = \exp(X+Y),$$

as desired. □

Definition 5.12.3 (One-parameter subgroups)**.** A *one-parameter subgroup* of $\mathrm{GL}(n,\mathbb{C})$ is a function $A\colon \mathbb{R} \to \mathrm{GL}(n,\mathbb{C})$ such that

(a) A is continuous,

(b) $A(0) = I$,

(c) $A(t+s) = A(t)A(s)$ for all $t, s \in \mathbb{R}$.

Note that the last condition in the above definition is equivalent to saying that A is a group homomorphism from $(\mathbb{R}, +)$ to G (the second condition is actually redundant). Recall that $\mathbb{R}$ is a Lie group under addition. A one-parameter subgroup is a homomorphism $\mathbb{R} \to G$ of Lie groups. We wish to give a nice characterization of these one-parameter subgroups. We first need a technical lemma.

Let

$$B_\delta = \{X \in M_n(\mathbb{C}) \mid \|X\| < \delta\}$$

be the open ball of radius δ about zero in $M_n(\mathbb{C})$. Choose δ sufficiently small so that B_δ is mapped homeomorphically onto its image under the exponential map (with inverse given by log). Then set $U = \exp(B_{\delta/2})$.

Lemma 5.12.4. *Every $g \in U$ has a unique square root $h \in U$, given by $h = \exp(\frac{1}{2}\log g)$.*

Proof. Let $X = \log g$. Then, if $h = \exp(X/2)$, we have

$$h^2 = e^X = g,$$

and so h is a square root of g. Now suppose $h' \in U$ satisfies $(h')^2 = g$. Let $Y = \log h'$. Then

$$e^Y = h',\ e^{2Y} = (h')^2 = g = e^X.$$

We have $Y \in B_{\delta/2}$ and so $2Y \in B_\delta$. We also have $X \in B_{\delta/2} \subseteq B_\delta$. Since exp is injective on B_δ and $\exp(2Y) = \exp(X)$, we must have $2Y = X$. Therefore

$$h' = e^Y = e^{X/2} = h,$$

which shows uniqueness. □

Theorem 5.12.5 (One-parameter subgroups)**.** *If A is a one-parameter subgroup of* $\mathrm{GL}(n,\mathbb{C})$*, then there exists a unique $X \in M_n(\mathbb{C})$ such that*

$$A(t) = e^{tX} \quad \textit{for all } t \in \mathbb{R}.$$

Proof. Uniqueness follows from the fact that if $A(t) = e^{tX}$, then $X = A'(0)$. It remains to show existence.

We fix δ and U as above. Since A is continuous, there exists a $t_0 > 0$ such that $A(t) \in U$ for all $t \in [-t_0, t_0]$. Let $X = \frac{1}{t_0} \log(A(t_0))$. Then

$$t_0 X = \log(A(t_0)) \in B_{\delta/2} \text{ and } A(t_0) = \exp(t_0 X).$$

Then $A(t_0/2) \in U$ and $A(t_0/2)^2 = A(t_0)$. By the above lemma, we have

$$A(t_0/2) = \exp(t_0 X/2).$$

Repeating this argument, we have

$$A(t_0/2^k) = \exp(t_0 X/2^k) \ \forall k \in \mathbb{Z}_{>0}.$$

Furthermore, for any integer m, we have

$$A(mt_0/2^k) = A(t_0/2^k)^m = \exp(mt_0 X/2^k).$$

Thus

$$A(t) = \exp(tX)$$

for all real numbers t of the form $mt_0/2^k$. Since this set of numbers is dense in $\mathbb{R}$ and both $\exp(tX)$ and $A(t)$ are continuous, it follows that $A(t) = \exp(tX)$ for $t \in \mathbb{R}$. □

5.13 The functor from Lie groups to Lie algebras

Lie groups and Lie algebras both form categories – we have homomorphisms of Lie groups and Lie algebras and these satisfy certain natural axioms (associative composition, identity maps, etc.). To every Lie group, we can associate its Lie algebra. We would now like to extend this identification to a *functor* from the category of Lie groups to the category of Lie algebras. So for every Lie group homomorphism $\Phi \colon G \to H$, we need to associate a Lie algebra homomorphism $\phi \colon \mathfrak{g} \to \mathfrak{h}$ and we want this association to commute with composition.

Theorem 5.13.1. *Let G and H be matrix Lie groups, with Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$, respectively. Suppose that $\Phi \colon G \to H$ is a Lie group homomorphism. Then there exists a unique real linear map $\phi \colon \mathfrak{g} \to \mathfrak{h}$ such that*

$$\Phi\left(e^X\right) = e^{\phi(X)} \textit{ for all } X \in \mathfrak{g}.$$

The map ϕ has the following additional properties.

(a) ϕ is a homomorphism of Lie algebras: $\phi([X,Y]) = [\phi(X), \phi(Y)]$ for all $X, Y \in \mathfrak{g}$.

(b) $\phi(AXA^{-1}) = \Phi(A)\phi(X)\Phi(A)^{-1}$, for all $X \in \mathfrak{g}$, $A \in G$.

(c) $\phi(X) = \frac{d}{dt} \Phi\left(e^{tX}\right)\big|_{t=0}$ *for all* $X \in \mathfrak{g}$.

Furthermore, this association defines a functor from the category of Lie groups to the category of Lie algebras. Namely, suppose G*,* H*, and* K *are matrix Lie groups and* $\Phi\colon H \to K$ *and* $\Psi\colon G \to H$ *are Lie group homomorphisms. Let* ϕ*,* ψ *and* λ *be the Lie algebra homomorphisms corresponding to* Φ*,* Ψ *and* $\Phi \circ \Psi$*, respectively. Then*

$$\lambda = \phi \circ \psi.$$

Remark 5.13.2. The property $\phi(X) = \frac{d}{dt} \Phi\left(e^{tX}\right)\big|_{t=0}$ says that ϕ is the derivative of Φ at the identity (every smooth map of smooth manifolds induces a map on the tangent spaces). In practice, this is how one computes ϕ. Since it is real linear, it suffices to compute it on a basis of $\mathfrak{g}$.

Proof. The composition of Lie group homomorphisms

$$\mathbb{R} \to G \to H, \quad t \mapsto e^{tX} \mapsto \Phi(e^{tX}),$$

is again a Lie group homomorphism and thus $t \mapsto \Phi(e^{tX})$ is a one-parameter subgroup of H. Therefore, by Theorem 5.12.5, there is a unique matrix Z such that

$$\Phi(e^{tX}) = e^{tZ} \quad \text{for all } t \in \mathbb{R}. \tag{5.5}$$

Since $e^{tZ} = \Phi(e^{tX}) \in H$, we know that $Z \in \mathfrak{h}$ by our alternative description of the Lie algebra of H (Corollary 5.11.10). We define $\phi(X) = Z$ and check that the map ϕ has the desired properties.

Step 1. $\Phi(e^X) = e^{\phi(X)}$ for all $X \in \mathfrak{g}$.

Setting $t = 1$ in (5.5), we have

$$\Phi(e^X) = e^Z = e^{\phi(X)}.$$

Step 2. The map ϕ is (real) linear.

Since $\Phi(e^{tX}) = e^{tZ}$ for all t, we have $\Phi(e^{tsX}) = e^{t(sZ)}$ for all $s \in \mathbb{R}$. Thus, $\phi(sX) = sZ = s\phi(X)$ for all $s \in \mathbb{R}$.
Now, by the above, we have

$$e^{t\phi(X+Y)} = e^{\phi(t(X+Y))} = \Phi(e^{t(X+Y)}).$$

By the Lie product formula (Proposition 5.12.2) and the fact that Φ is a continuous homomorphism, we have

$$\begin{aligned} e^{t\phi(X+Y)} &= \Phi\left(\lim_{m\to\infty}\left(e^{tX/m}e^{tY/m}\right)^m\right) \\ &= \lim_{m\to\infty}\left(\Phi\left(e^{tX/m}\right)\Phi\left(e^{tY/m}\right)\right)^m \\ &= \lim_{m\to\infty}\left(e^{t\phi(X)/m}e^{t\phi(Y)/m}\right)^m = e^{t(\phi(X)+\phi(Y))}. \end{aligned}$$

Differentiating at $t = 0$ gives $\phi(X + Y) = \phi(X) + \phi(Y)$. Thus ϕ is a linear map.

Step 3. $\phi(AXA^{-1}) = \Phi(A)\phi(X)\Phi(A)^{-1}$ for all $X \in \mathfrak{g}$ and $A \in G$.

First note that for $X \in \mathfrak{g}$, $A \in G$, and $t \in \mathbb{R}$, we have $e^{tAXA^{-1}} = Ae^{tX}A^{-1} \in G$, since $A, e^{tX} \in G$. Thus, by Corollary 5.11.10, we have $AXA^{-1} \in \mathfrak{g}$. Then we have

$$\begin{aligned}
\exp t\phi(AXA^{-1}) &= \exp \phi(tAXA^{-1}) = \Phi(\exp(tAXA^{-1})) \qquad \text{(by the above)} \\
&= \Phi(Ae^{tX}A^{-1}) \\
&= \Phi(A)\Phi(e^{tX})\Phi(A)^{-1} \qquad (\Phi \text{ is a group homomorphism}) \\
&= \Phi(A)e^{t\phi(X)}\Phi(A)^{-1} \qquad \text{(by the above).}
\end{aligned}$$

Differentiating gives the desired result.

Step 4. ϕ is a homomorphism of Lie algebras.

We have from the above that ϕ is a linear map. It thus suffices to check that $\phi([X,Y]) = [\phi(X), \phi(Y)]$. Now,

$$[X,Y] = \frac{d}{dt} e^{tX} Y e^{-tX} \bigg|_{t=0}.$$

(We saw this in the proof of Proposition 5.7.2—it is the standard way of recovering the bracket in $\mathfrak{g}$ from the group operation in G.) Therefore,

$$\phi([X,Y]) = \phi\left(\frac{d}{dt} e^{tX} Y e^{-tX} \bigg|_{t=0} \right) = \frac{d}{dt} \phi\left(e^{tX} Y e^{-tX}\right) \bigg|_{t=0}.$$

(Here we have used the fact that derivatives commute with linear transformations.) Then, by the above, we have

$$\begin{aligned}
\phi([X,Y]) &= \frac{d}{dt} \Phi(e^{tX})\phi(Y)\Phi(e^{-tX}) \bigg|_{t=0} \\
&= \frac{d}{dt} e^{t\phi(X)}\phi(Y)e^{-t\phi(X)} \bigg|_{t=0} \\
&= [\phi(X), \phi(Y)]
\end{aligned}$$

as desired.

Step 5. $\phi(X) = \frac{d}{dt}\Phi\left(e^{tX}\right)\big|_{t=0}$ for all $X \in \mathfrak{g}$.

By the definition of $\phi(X)$, we have

$$\frac{d}{dt}\Phi\left(e^{tX}\right)\bigg|_{t=0} = \frac{d}{dt} e^{t\phi(X)} \bigg|_{t=0} = \phi(X).$$

Step 6. Uniqueness: ϕ is the unique real linear map such that $\Phi\left(e^{X}\right) = e^{\phi(X)}$ for all $X \in \mathfrak{g}$.

Let ψ be such a map. Then, for all $X \in \mathfrak{g}$ and $t \in \mathbb{R}$,

$$e^{t\psi(X)} = e^{\psi(tX)} = \Phi\left(e^{tX}\right),$$

and so

$$\psi(X) = \frac{d}{dt}\Phi\left(e^{tX}\right)\bigg|_{t=0} = \phi(X).$$

Step 7. $\lambda = \phi \circ \psi$.

For $X \in \mathfrak{g}$, we have

$$(\Phi \circ \Psi)\left(e^{tX}\right) = \Phi\left(\Psi\left(e^{tX}\right)\right) = \Phi\left(e^{t\psi(X)}\right) = e^{t\phi(\psi(X))}.$$

Thus, by uniqueness,

$$\lambda(X) = \phi(\psi(X)).$$

□

Definition 5.13.3 (The adjoint mapping)**.** Let G be a matrix Lie group with Lie algebra $\mathfrak{g}$. Then, for each $A \in G$, we have the *adjoint mapping*

$$\mathrm{Ad}_A : \mathfrak{g} \to \mathfrak{g}, \quad \mathrm{Ad}_A(X) = AXA^{-1}.$$

(Note that $AXA^{-1} \in \mathfrak{g}$ as in the proof of Step 3 of Theorem 5.13.1.)

Let G be a matrix Lie group with Lie algebra $\mathfrak{g}$. Let $\mathrm{Aut}\,\mathfrak{g}$ denote the group of Lie algebra automorphisms of $\mathfrak{g}$ (i.e. Lie algebra isomorphisms from $\mathfrak{g}$ to itself). Note that $\mathrm{Aut}\,\mathfrak{g}$ is a group under composition.

The proof of the following proposition is left as an exercise (Exercise 5.13.1).

Proposition 5.13.4. *The map*

$$G \to \mathrm{Aut}\,\mathfrak{g}, \quad A \mapsto \mathrm{Ad}_A,$$

is a group homomorphism.

Remark 5.13.5. Note that the above proposition implies that, for each $A \in G$, Ad_A is an invertible linear transformation of $\mathfrak{g}$ with inverse $\mathrm{Ad}_{A^{-1}}$, and

$$\mathrm{Ad}_A([X,Y]) = [\mathrm{Ad}_A(X), \mathrm{Ad}_A(Y)], \quad \text{for all } X, Y \in \mathfrak{g}.$$

Note that $\mathrm{Aut}\,\mathfrak{g}$ is a subgroup of $\mathrm{GL}(\mathfrak{g})$, the group of invertible linear transformation of $\mathfrak{g}$. Since $\mathfrak{g}$ is a finite dimensional real vector space of some dimension k, we can identity $\mathrm{GL}(\mathfrak{g})$ with $\mathrm{GL}(k,\mathbb{R})$ and regard it as a matrix Lie group. So Ad gives rise to a map $G \to \mathrm{GL}(\mathfrak{g})$ which is continuous (Exercise 5.13.2) and is thus a homomorphism of Lie groups. Therefore, by Theorem 5.13.1, there is an associated homomorphism of Lie algebras

$$\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}), \quad X \mapsto \mathrm{ad}_X$$

such that

$$e^{\mathrm{ad}_X} = \mathrm{Ad}(e^X).$$

Here $\mathfrak{gl}(\mathfrak{g})$ is the Lie algebra of $\mathrm{GL}(\mathfrak{g})$, namely the space of all linear maps from $\mathfrak{g}$ to itself.

Proposition 5.13.6. *For all $X, Y \in \mathfrak{g}$, we have*

$$\mathrm{ad}_X(Y) = [X,Y].$$

Proof. By Theorem 5.13.1, we have

$$\mathrm{ad}_X = \frac{d}{dt} \mathrm{Ad}\left(e^{tX}\right)\Big|_{t=0}.$$

Therefore

$$\mathrm{ad}_X(Y) = \frac{d}{dt} \mathrm{Ad}\left(e^{tX}\right)(Y)\Big|_{t=0} = \frac{d}{dt}\, e^{tX} Y e^{-tX}\Big|_{t=0} = [X,Y]. \qquad \square$$

Proposition 5.13.7. *Suppose G is a connected matrix Lie group, H is a matrix Lie group, and $\Phi_1, \Phi_2 : G \to H$ are Lie group homomorphisms with associated Lie algebra homomorphisms ϕ_1 and ϕ_2. If $\phi_1 = \phi_2$, then $\Phi_1 = \Phi_2$.*

Proof. Let $g \in G$. Since G is connected, we know from Corollary 5.11.8 that

$$g = e^{X_1} e^{X_2} \dots e^{X_n}$$

for some $X_i \in \mathfrak{g}$. Then

$$\begin{aligned} \Phi_1(g) &= \Phi_1(e^{X_1}) \cdots \Phi_1(e^{X_n}) \\ &= e^{\phi_1(X_1)} \cdots e^{\phi_1(X_n)} \\ &= e^{\phi_2(X_1)} \cdots e^{\phi_2(X_n)} \\ &= \Phi_2(e^{X_1}) \cdots \Phi_2(e_{X_n}) \\ &= \Phi_2(g). \end{aligned} \qquad \square$$

Corollary 5.13.8. *Every continuous homomorphism between two matrix Lie groups is smooth.*

Proof. Suppose $\Phi \colon G \to H$ is a continuous homomorphism of Lie groups. If suffices to prove that Φ is smooth in a neighbourhood of every point $A \in G$. Now, there exists a neighbourhood U of A such that $B = A \exp X$, $X \in \mathfrak{g}$, for all $B \in U$ (we translate the neighbourhood of the identity in the image of the exponential map by multiplying on the left by A). Then

$$\Phi(B) = \Phi(A)\Phi(\exp X) = \Phi(A)\exp(\phi(X)), \quad \text{for all } B \in U.$$

Thus, in the exponential coordinates near A, Φ is a composition of the linear map ϕ, the exponential mapping, and left multiplication by $\Phi(A)$. Since all of these maps are smooth, we see that Φ is smooth near any point A of G. □

Remark 5.13.9. We have seen most of the ingredients of the proof of the fact that every matrix Lie group is a Lie group (see [Hal03, Corollary 2.33] for details).

Exercises.

5.13.1. Prove Proposition 5.13.4.

5.13.2. Show that the map $\mathrm{Ad} \colon G \to \mathrm{GL}(\mathfrak{g})$ is continuous.

5.14 Lie algebras and normal subgroups

Recall that any discrete normal subgroup of a path-connected group lies in its centre (see Theorem 4.3.2). Since we know that $\mathrm{SO}(n)$, $\mathrm{SU}(n)$, and $\mathrm{Sp}(n)$ are path-connected and we have described their centres, we know their discrete normal subgroups. However, we do not know (yet) if they have any *non*discrete normal subgroups. It turns out that our knowledge of the Lie algebra will now allow us to answer this question.

Proposition 5.14.1. *If H is a normal subgroup of a matrix Lie group G, then $\mathfrak{h}$ is an ideal of $\mathfrak{g}$.*

Proof. Since any tangent to H at 1 is a tangent to G at 1, $\mathfrak{h}$ is a subspace of $\mathfrak{g}$. Suppose $X \in \mathfrak{g}$ and $Y \in \mathfrak{h}$. Let $A(s)$ be a smooth path in G and let $B(t)$ be a smooth path in H with $A(0) = B(0) = 1$, $A'(0) = X$, and $B'(0) = Y$. Since H is a normal subgroup of G, we have that

$$C_s(t) = A(s)B(t)A(s)^{-1}$$

is a smooth path in H. Then

$$D(s) \overset{\text{def}}{=} C_s'(0) = A(s)YA(s)^{-1}$$

is a smooth path in $\mathfrak{h}$. Therefore

$$D'(0) = XY - YX \in \mathfrak{h}.$$

Thus $\mathfrak{h}$ is an ideal of $\mathfrak{g}$ as claimed. □

Proposition 5.14.2 (Tangent space visibility)**.** *Suppose G is a path-connected matrix Lie group with discrete centre and H is a nondiscrete normal subgroup. Then $\mathfrak{h} \neq 0$.*

Proof. Since $Z(G)$ is discrete while H is not, there exists a neighbourhood $N_\delta(1)$ in G that includes an least one element $B \neq 1$ in H but no element of $Z(G)$ other than 1. Then $B \notin Z(G)$ and so there exists some $A \in N_\delta(1)$ that does *not* commute with B (since $N_\delta(1)$ generates G, if B commuted with all elements of $N_\delta(1)$, it would lie in $Z(G)$).

By taking δ sufficiently small, we can assume $A = e^X$ and $e^{tX} \in N_\delta(1)$, $0 \leq t \leq 1$, for some $X \in T_1(G)$. Now let

$$C(t) = e^{tX}Be^{-tX}B^{-1}.$$

Thus $C(t)$ is a path in G with $C(0) = 1$ and $C(1) = ABA^{-1}B^{-1}$. Using the product rule for differentiation, we obtain

$$C'(0) = X - BXB^{-1}.$$

Since H is a normal subgroup of G and $B \in H$, we have $e^{tX}Be^{-tX} \in H$. Thus $e^{tX}Be^{-tX}B^{-1} \in H$ and so $C(t)$ is actually a path in H. Thus

$$C'(0) = X - BXB^{-1} \in \mathfrak{h}.$$

To show that $\mathfrak{h} \neq 0$ is thus suffices to show that $X - BXB^{-1} \neq 0$. We prove this by contradiction. We have

$$X - BXB^{-1} = 0 \implies BXB^{-1} = X$$

$$\begin{aligned}
&\implies e^{BXB^{-1}} = e^X \\
&\implies Be^X B^{-1} = e^X \\
&\implies Be^X = e^X B \\
&\implies BA = AB.
\end{aligned}$$

But this contradicts the fact that A and B do not commute. □

Corollary 5.14.3. *Under the assumptions of Proposition 5.14.2, if $H \neq G$, then $\mathfrak{h}$ is a nontrivial ideal of $\mathfrak{g}$.*

Proof. We know that $\mathfrak{h}$ is an ideal of $\mathfrak{g}$ by Proposition 5.14.1 and $\mathfrak{h} \neq 0$ by Proposition 5.14.2. Suppose $\mathfrak{h} = \mathfrak{g}$. Then, by the log-exp bijection between neighbourhoods of the identity in G and $\mathfrak{g}$, we have that $N_\delta(1) \subseteq H$ for some neighbourhood $N_\delta(1)$ of the identity in G. Since $N_\delta(1)$ generates G, we have $H = G$. Thus $H \neq G \implies \mathfrak{h} \neq \mathfrak{g}$. □

A proof of the following result can be found in [Sti08, §§6.4–6.6].

Lemma 5.14.4. *The Lie algebras $\mathfrak{so}(n)$ $(n \neq 4)$, $\mathfrak{su}(n)$, and $\mathfrak{sp}(n)$ have no nontrivial ideals.*

Corollary 5.14.5 (Normal subgroups of $\mathrm{SO}(n)$, $\mathrm{SU}(n)$, and $\mathrm{Sp}(n)$)**.** *The only nontrivial normal subgroups of $\mathrm{SO}(n)$ $(n \neq 4)$, $\mathrm{SU}(n)$ and $\mathrm{Sp}(n)$ are the (cyclic) subgroups of their centres.*

Proof. This follows immediately from Theorem 4.3.2, Corollary 5.14.3, and Lemma 5.14.4. □

Remark 5.14.6. Recall the discussion of SO(4) in Section 1.8. In particular, SO(4) is not simple.

We can now prove something that we claimed earlier (see Proposition 1.5.10).

Corollary 5.14.7 (Simplicity of $\mathrm{SO}(2m+1)$)**.** *The matrix Lie group $\mathrm{SO}(2m+1)$ is simple for m a nonnegative integer.*

Proof. This follows from Corollary 5.14.5 and the fact that the centre of $\mathrm{SO}(2m+1)$ is trivial. □

Remark 5.14.8. Note that $\mathrm{SO}(2m)$ is *not* simple since it has centre $\{\pm 1\}$.

5.15 The Campbell–Baker–Hausdorff Theorem

Our goal in this section is to show that, near the identity, the multiplication in a Lie group is determined by the Lie bracket in the corresponding Lie algebra. Remember that we already know the reverse is true (we can recover the Lie bracket from the group multiplication by differentiation).

Recall that in some neighbourhood of the identity, any two elements of G have the form e^X and e^Y for some $X, Y \in \mathfrak{g}$ and their product is of the form e^Z for some $Z \in \mathfrak{g}$:

$$e^X e^Y = e^Z.$$

We would like to find a formula for Z in terms of X and Y that only involves Lie algebra operations (i.e. vector space operations and the Lie bracket). In other words, we want such a formula for

$$Z = \log\left(e^X e^Y\right).$$

Since

$$e^X = I + \frac{X}{1!} + \frac{X^2}{2!} + \cdots, \quad e^Y = I + \frac{Y}{1!} + \frac{Y^2}{2!} + \cdots,$$

we have

$$e^X e^Y = \sum_{m,n \geq 0} \frac{X^m Y^n}{m!n!} = I + X + Y + XY + \frac{X^2}{2!} + \frac{Y^2}{2!} + \cdots + \frac{X^m Y^n}{m!n!} + \cdots.$$

Since

$$\log(I + W) = W - \frac{W^2}{2} + \frac{W^3}{3} - \frac{W^4}{4} + \cdots,$$

we have

$$\begin{aligned} Z &= \log\left(e^X e^Y\right) \\ &= \left(X + Y + XY + \frac{X^2}{2!} + \frac{Y^2}{2!} + \cdots\right) - \frac{1}{2}\left(X + Y + XY + \frac{X^2}{2!} + \frac{Y^2}{2!} + \cdots\right)^2 \\ &\qquad + \frac{1}{3}\left(X + Y + XY + \frac{X^2}{2!} + \frac{Y^2}{2!} + \cdots\right)^3 - \cdots \\ &= X + Y + \frac{1}{2}XY - \frac{1}{2}YX + \text{higher-order terms} \\ &= X + Y + \frac{1}{2}[X, Y] + \text{higher-order terms.} \end{aligned}$$

The Campbell–Baker–Hausdorff Theorem asserts that all of the higher-order terms are obtained from X and Y by Lie brackets.

There are several proofs of the Campbell–Baker–Hausdorff Theorem. Following [Sti08], we will present a proof by Eichler (1968). This proof is elementary in the sense that it does not use any sophisticated machinery. One drawback is that it is not extremely intuitive. Students who wish to see an alternate proof can look at [Hal03, §3.4].

Our proof will be by induction. Let

$$e^A e^B = e^Z, \quad Z = F_1(A, B) + F_2(A, B) + F_3(A, B) + \cdots, \tag{5.6}$$

where $F_n(A, B)$ is the sum of all the terms of degree n appearing in the formula for Z in terms of A and B. So $F_n(A, B)$ is a homogeneous polynomial of degree n in A and B. Since the variables A and B stand for matrices, the variables do not commute in general, but their multiplication is associative.

Definition 5.15.1 (Lie polynomial)**.** A polynomial $p(A, B, C, \dots)$ is called *Lie* if is a linear combination of $A, B, C, \dots$ and (possibly nested) Lie bracket terms in $A, B, C, \dots$.

From our computations above, we see that

$$F_1(A,B) = A + B, \quad F_2(A,B) = \frac{1}{2}[A,B].$$

Thus F_1 and F_2 are Lie polynomials.

Theorem 5.15.2 (Campbell–Baker–Hausdorff Theorem)**.** *The polynomial $F_n(A,B)$ is Lie for all $n \geq 1$.*

Proof. Our induction hypothesis is that F_m is a Lie polynomial for $m < n$, and we want to prove that F_n is Lie. Since we know F_1 and F_2 are Lie polynomials, we may assume that $n \geq 3$.

Since the multiplication of variables $A, B, C, \dots$ is associative, so is the multiplication of products of power series in $A, B, C, \dots$. Therefore, for any A, B, C, we have

$$\left(e^A e^B\right) e^C = e^A \left(e^B e^C\right).$$

Thus, if we set $e^A e^B e^C = e^W$, we have

$$W = \sum_{i=1}^{\infty} F_i \left(\sum_{j=1}^{\infty} F_j(A,B), C \right) = \sum_{i=1}^{\infty} F_i \left(A, \sum_{j=1}^{\infty} F_j(B,C) \right). \tag{5.7}$$

By the induction hypothesis, we have:

- All the homogeneous terms of degree $< n$ in both expressions for W in (5.7) are Lie.
- All the homogeneous terms of degree n in both expressions for W in (5.7) coming from $i > 1$ and $j > 1$ are Lie (since they are Lie polynomials of Lie polynomials).

The only terms which could possibly not be Lie are the polyonimals

- $F_n(A,B) + F_n(A+B,C)$ on the left (from $i = 1$, $j = n$ and $i = n$, $j = 1$), and
- $F_n(A, B+C) + F_n(B,C)$ on the right (from $i = n$, $j = 1$ and $i = 1, j = n$).

Therefore, the difference between these exceptional terms is a difference of Lie polynomials and hence is a Lie polynomial. Note that the relation

$$F \equiv_{\text{Lie}} G \iff F - G \text{ is a Lie polynomial} \tag{5.8}$$

is an equivalence relation (Exercise 5.15.1). We want to prove that $F_n(A,B) \equiv_{\text{Lie}} 0$.

We have just argued that

$$F_n(A,B) + F_n(A+B,C) \equiv_{\text{Lie}} F_n(A, B+C) + F_n(B,C). \tag{5.9}$$

We will manipulate (5.9) to obtain our desired result. We will use the following facts:

Fact 1. $F_n(rA, sA) = 0$ for all scalars r, s and $n > 1$. This is true since rA and sA commute and so $e^{rA}e^{sA} = e^{rA+sA}$. Thus $Z = F_1(rA, sA) = (r + s_A$ and $F_n(rA, sA) = 0$ for all $n > 1$.

Fact 2. In particular, $F_n(A, 0) = 0$ for $n > 1$ (take $r = 1$, $s = 0$).

Fact 3. $F_n(rA, rB) = r^n F_n(A, B)$ for all $r \in \mathbb{R}$ and $n \geq 1$, since $F_n(A, B)$ is homogeneous of degree n.

We first replace C by $-B$ in (5.9) to obtain

$$\begin{aligned} F_n(A, B) + F_n(A + B, -B) &\equiv_{\text{Lie}} F_n(A, 0) + F_n(B, -B) \\ &\equiv_{\text{Lie}} 0 \qquad \text{by Facts 2 and 1.} \end{aligned}$$

Thus we have

$$F_n(A, B) \equiv_{\text{Lie}} -F_n(A + B, -B). \tag{5.10}$$

Next, we replace A by $-B$ in (5.9) to obtain

$$F_n(-B, B) + F_n(0, C) \equiv_{\text{Lie}} F_n(-B, B + C) + F_n(B, C).$$

Using Facts 1 and 2 again, we get

$$0 \equiv_{\text{Lie}} F_n(-B, B + C) + F_n(B, C).$$

Replacing B by A and C by B yields

$$0 \equiv_{\text{Lie}} F_n(-A, A + B) + F_n(A, B),$$

and so

$$F_n(A, B) \equiv_{\text{Lie}} -F_n(-A, A + B). \tag{5.11}$$

We now have

$$\begin{aligned} F_n(A, B) &\equiv_{\text{Lie}} -F_n(-A, A + B) \qquad \text{by (5.11)} \\ &\equiv_{\text{Lie}} -(-F_n(-A + A + B, -A - B)) \qquad \text{by (5.10)} \\ &\equiv_{\text{Lie}} F_n(B, -A - B) \\ &\equiv_{\text{Lie}} -F_n(-B, -A) \qquad \text{by (5.11)} \\ &\equiv -(-1)^n F_n(B, A) \qquad \text{by Fact 3.} \end{aligned}$$

Thus we have

$$F_n(A, B) \equiv_{\text{Lie}} -(-1)^n F_n(B, A). \tag{5.12}$$

Now we replace C by $-B/2$ in (5.9), giving

$$\begin{aligned} F_n(A, B) + F_n(A + B, -B/2) &\equiv_{\text{Lie}} F_n(A, B/2) + F_n(B, -B/2) \\ &\equiv_{\text{Lie}} F_n(A, B/2) \qquad \text{by Fact 1.} \end{aligned}$$

Thus

$$F_n(A, B) \equiv_{\text{Lie}} F_n(A, B/2) - F_n(A + B, -B/2). \tag{5.13}$$

Next, replacing A by $-B/2$ in (5.9) yields

$$F_n(-B/2, B) + F_n(B/2, C) \equiv_{\text{Lie}} F_n(-B/2, B + C) + F_n(B, C).$$

Thus, by Fact 1, we have

$$F_n(B/2, C) \equiv_{\text{Lie}} F_n(-B/2, B + C) + F_n(B, C).$$

Replacing B by A and C by B gives

$$F_n(A/2, B) \equiv_{\text{Lie}} F_n(-A/2, A + B) + F_n(A, B),$$

or

$$F_n(A, B) \equiv_{\text{Lie}} F_n(A/2, B) - F_n(-A/2, A + B). \tag{5.14}$$

We now manipulate the two terms on the right side of (5.14).

$$\begin{aligned} F_n(A/2, B) &\equiv_{\text{Lie}} F_n(A/2, B/2) - F_n(A/2 + B, -B/2) && \text{by (5.13)} \\ &\equiv_{\text{Lie}} F_n(A/2, B/2) + F_n(A/2 + B/2, B/2) && \text{by (5.10)} \\ &\equiv_{\text{Lie}} 2^{-n} F_n(A, B) + 2^{-n} F_n(A + B, B) && \text{by Fact 3.} \end{aligned}$$

$$\begin{aligned} F_n(-A/2, A + B) &\equiv_{\text{Lie}} F_n(-A/2, A/2 + B/2) - F_n(A/2 + B, -A/2 - B/2) && \text{by (5.13)} \\ &\equiv_{\text{Lie}} -F_n(A/2, B/2) + F_n(B/2, A/2 + B/2) && \text{by (5.11) and (5.10)} \\ &\equiv_{\text{Lie}} -2^{-n} F_n(A, B) + 2^{-n} F_n(B, A + B) && \text{by Fact 3.} \end{aligned}$$

Therefore, (5.14) becomes

$$F_n(A, B) \equiv_{\text{Lie}} 2^{1-n} F_n(A, B) + 2^{-n} F_n(A + B, B) - 2^{-n} F_n(B, A + B).$$

Using (5.12), this becomes

$$(1 - 2^{1-n}) F_n(A, B) \equiv_{\text{Lie}} 2^{-n}(1 + (-1)^n) F_n(A + B, B). \tag{5.15}$$

Now, if n is odd, (5.15) tells us that $F_n(A, B) \equiv_{\text{Lie}} 0$ as desired. So assume n is even. Replace A by $A - B$ in (5.15) to get

$$(1 - 2^{1-n}) F_n(A - B, B) \equiv_{\text{Lie}} 2^{1-n} F_n(A, B).$$

The left side of the above equation becomes

$$(1 - 2^{1-n}) F_n(A - B, B) \equiv_{\text{Lie}} -(1 - 2^{1-n}) F_n(A, -B) \qquad \text{by (5.10)},$$

and so

$$-F_n(A, -B) \equiv_{\text{Lie}} \frac{2^{1-n}}{1 - 2^{1-n}} F_n(A, B). \tag{5.16}$$

Finally, replacing B by $-B$ in (5.16), we get

$$\begin{aligned} -F_n(A, B) &\equiv_{\text{Lie}} \frac{2^{1-n}}{1 - 2^{1-n}} F_n(A, -B) \\ &\equiv_{\text{Lie}} -\left(\frac{2^{1-n}}{1 - 2^{1-n}} \right)^2 F_n(A, B) && \text{by (5.16).} \end{aligned}$$

This implies $F_n(A, B) \equiv_{\text{Lie}} 0$ as desired. □

Exercises.

5.15.1. Show that (5.8) is an equivalence relation.

Chapter 6

Covering groups

In this chapter we examine in further detail the correspondence between Lie groups and Lie algebras. We already know examples of nonisomorphic Lie groups with isomorphic Lie algebras. In order to have a one-to-one correspondence between Lie groups and Lie algebras, we need to restrict our attention to certain types of Lie groups.

6.1 Simple connectedness

We have see that for a matrix Lie group homomorphism $\Phi\colon G \to H$, there exists a unique Lie algebra homomorphism $\phi\colon \mathfrak{g} \to \mathfrak{h}$ such that

$$\exp(\phi(X)) = \Phi(\exp(X)), \quad \text{for all } X \in \mathfrak{g}.$$

We would like to turn our attention to the converse. Namely, given a Lie algebra homomorphism $\phi \cong \mathfrak{g} \to \mathfrak{h}$, is there a Lie group homomorphism $\Phi \cong G \to H$ satisfying the above equation? We will see that the answer is yes, under certain additional assumptions. These assumptions are related to the notion of simple connectedness.

Definition 6.1.1 (Simply connected)**.** A subset S of $\mathbb{C}^n$ is *simply connected* if it is path-connected and every loop in S can be shrunk continuously to a point in S.

More precisely, assume that S is connected. Then S is simply connected if, given any continuous path $A(t)$, $0 \le t \le 1$, in S with $A(0) = A(1)$, there exists a continuous function $A(s,t)$ from $[0,1]^2$ to S, such that

(a) $A(s,0) = A(s,1)$ for all $0 \le s \le 1$ (i.e. for any fixed s, $A(s,t)$ is a loop),

(b) $A(0,t) = A(t)$ for all $0 \le t \le 1$ (i.e. fixing $s = 0$ gives our original path), and

(c) $A(1,t) = A(1,0)$ for all $0 \le t \le 1$ (i.e. fixing $s = 1$ gives a constant path).

There are many equivalent definitions of simply connected.

Proposition 6.1.2 (Simply connected alternate definitions)**.** *A path-connected subset S of $\mathbb{C}^n$ is simply connected (in the sense of Definition 6.1.1) if and only if it satisfies any one of the following equivalent conditions.*

(a) *For any two paths p and q in S from point $A \in S$ to point $B \in S$, there is a* deformation *of p to q with endpoints fixed. A deformation (or* homotopy*) of p to q is a continuous function $d : [0,1]^2 \to S$ such that*

  (a) *$d(0,t) = p(t)$,*

  (b) *$d(1,t) = q(t)$, and*

  (c) *$d(s,0) = p(0) = q(0) = A$ and $d(s,1) = p(1) = q(1) = B$ for all s.*

(b) *Any continuous map $f : \mathbb{S}^1 \to S$ (recall that $\mathbb{S}^1$ is the unit circle) can be contracted to a point. That is, there exists a continuous function $F\colon D \to S$, where D is the unit disk, such that $F|_{\mathbb{S}^1} = f$.*

(c) *(For those with some background in topology.) The fundamental group of S is trivial.*

Proof. It is clear that (a) implies that S is simply connected (set $A(t) = p(t)$ and let $q(t)$ be the constant path at the point $A(0)$). Since we will not use these other definitions in this class, we omit the proofs of the other implications. □

It is rather hard to prove that a given space is simply connected, except in simple cases.

Proposition 6.1.3. *The space $\mathbb{R}^n$ is simply connected.*

Proof. Let $A(t)$ be a loop in $\mathbb{R}^n$. Define

$$A(s,t) = (1-s)A(t).$$

Then $A(s,t)$ is continuous and

(a) $A(s,0) = (1-s)A(0) = (1-s)A(1) = A(s,1)$ for all $0 \le s \le 1$,

(b) $A(0,t) = A(t)$ for all $0 \le t \le 1$, and

(c) $A(1,t) = 0 = A(1,0)$ for all $0 \le t \le 1$.

Thus $A(s,t)$ satisfies the conditions of Definition 6.1.1. □

Proposition 6.1.4. *The k-sphere $\mathbb{S}^k$, $k > 1$, is simply connected.*

Proof. This can be proven using the compactness of $\mathbb{S}^k$ and stereographic projection. See the exercises of [Sti08, §8.7]. □

We will prove that the unit circle $\mathbb{S}^1$ is *not* simply connected. In particular, the path $(\cos 2\pi t, \sin 2\pi t)$, $0 \le t \le 1$, cannot be contracted to a point.

Recall that the function $f(\theta) = (\cos\theta, \sin\theta)$ maps $\mathbb{R}$ onto $\mathbb{S}^1$. This is called a *covering* of $\mathbb{S}^1$ and the points $f^{-1}(z)$, $z \in \mathbb{S}^1$, are said to *lie over* z. In other words, the points $\theta + 2n\pi \in \mathbb{R}$ lie over the point $(\cos\theta, \sin\theta) \in \mathbb{S}^1$. This map is certainly not 1-1 and therefore cannot be a homeomorphism.

However, if we restrict f to any interval of $\mathbb{R}$ with length $< 2\pi$, the result is a 1-1 map that is continuous in both directions. Thus we say that f is a *local homeomorphism.*

Definition 6.1.5 (Local homeomorphism)**.** If U and V are subsets of $\mathbb{C}^n$ (or $\mathbb{R}^n$, or, more generally, topological spaces), then a function $f\colon U \to V$ is a *local homeomorphism* if, for every $x \in U$, there is an open set $W \subseteq U$ containing x such that $f(W)$ is open in V and $f|_W\colon W \to f(W)$ is a homeomorphism.

Definition 6.1.6 (Covering space)**.** Let V be a subset of $\mathbb{C}^n$ (or $\mathbb{R}^n$, or, more generally, a topological space). A *covering space* of V is a space $\tilde{V}$ together with a continuous surjective map $f\colon \tilde{V} \to V$ such that, for every $x \in V$, there exists an open neighbourhood U of x such that $f^{-1}(U)$ is a disjoint union of open sets in $\tilde{V}$, each of which is mapped homeomorphically onto U by f.

Example 6.1.7. The map $f\colon \mathbb{R} \to \mathbb{S}^1$ defined above is a covering space. For any $x \in \mathbb{S}^1$, we can take U to be any arc (not equal to the entire circle) containing x.

Proposition 6.1.8 (Unique path lifting)**.** *Suppose that $f\colon \tilde{V} \to V$ is a covering space, p is a path in V with initial point P, and $\tilde{P}$ is a point in $\tilde{V}$ over P. Then there is a unique path $\tilde{p}$ in $\tilde{V}$ such that*

$$\tilde{p}(0) = \tilde{P}, \quad \textit{and} \quad f \circ \tilde{p} = p.$$

We call $\tilde{p}$ the lift *of p with initial point $\tilde{P}$.*

Proof. The path p is a continuous function from $[0,1]$ to V. For every point x in the image of p, choose a neighbourhood U_x as in Definition 6.1.6. Then the collection $\{p^{-1}(U_x)\}$ is an open cover of $[0,1]$. Since $[0,1]$ is compact, there is a finite subcover. That is, the image of p is contained in the union of a finite number of the U_x. Let us relabel this finite set by $U_1, \dots, U_n$ in such a way that $P \in U_1$, $p^{-1}(U_i) \cap p^{-1}(U_{i+1}) \neq \varnothing$ for $1 \leq i \leq n-1$, and $p(1) \in U_n$.

Now, since $U_1 \cap U_2 \neq \varnothing$, we can choose an $a_1 \in [0,1]$ such that $p([0,a_1]) \subseteq U_1$ and $p(a_1) \in U_2$. Let $p_1 = p|_{[0,a_1]}$. Since the image of p_1 is contained in U_1, there is a unique path $\tilde{p}_1\colon [0,a_1] \to \tilde{V}$, with initial point $\tilde{P}$, such that $f \circ \tilde{p}_1 = p_1$. Namely, we take $\tilde{p}_1(t) = f^{-1}(p_1(t))$, where f^{-1} is the continuous inverse of f in the neighbourhood of $\tilde{P}$. Let $\tilde{P}_1 = p(a_1)$ be the final point of $\tilde{p}_1$.

Similarly, there is an $a_2 \in [a_1, 1]$ such that $p([a_1,a_2]) \subseteq U_2$ and $p(a_2) \in U_3$. Then there is a unique path $\tilde{p}_2\colon [a_1,a_2] \to \tilde{V}$, with initial point $\tilde{P}_1$, such that $f \circ \tilde{p}_2 = p_2$. Let $\tilde{P}_2$ be its final point.

We continue in this manner and concatenate the paths $\tilde{p}_j$ in $\tilde{V}$ to obtain the lift $\tilde{p}$ of p with initial point $\tilde{P}$. □

Lemma 6.1.9. *Suppose that $f\colon \tilde{V} \to V$ is a covering space and that p and q are paths from A to B in V and p is deformable to q with endpoints fixed. Then the lift $\tilde{p}$ of p with initial point $\tilde{A}$ is deformable to the lift $\tilde{q}$ of q with initial point $\tilde{A}$ with endpoints fixed.*

Proof. The proof is similar to that of Proposition 6.1.8 and will be omitted. □

Corollary 6.1.10. *The unit circle $\mathbb{S}^1$ is not simply connected.*

Proof. We prove that the upper semicircle path

$$p(t) = (\cos \pi t, \sin \pi t), \quad 0 \le t \le 1,$$

from $(1, 0)$ to $(-1, 0)$ is not deformable to the lower semicircle path

$$q(t) = (\cos(-\pi t), \sin(-\pi t)), \quad 0 \le t \le 1,$$

from $(1, 0)$ to $(-1, 0)$. The lift $\tilde{p}$ of p with initial point 0 has final point π. However, the lift $\tilde{q}$ fo q with initial point 0 has final point $-\pi$. Hence, there is no deformation of $\tilde{p}$ to $\tilde{q}$ with fixed endpoints. Therefore, there is no deformation of p to q with fixed endpoints. □

6.2 Simply connected Lie groups

Since matrix Lie groups are subsets of $M_n(\mathbb{C})$ and can thus be viewed as subsets of $\mathbb{C}^{n^2}$, we can apply to them the above discussion of simple connectedness. Since SU(2) can be viewed as the group of unit quaternions, it can be viewed at the 3-sphere $\mathbb{S}^3$ inside $\mathbb{R}^4$. Therefore, SU(2) is simply connected. On the other hand, SO(2) can be identified with the unit circle and therefore is not simply connected.

What about SO(3)? Each element of SO(3) is a rotation of $\mathbb{R}^3$ and can therefore be described by a vector v in $\mathbb{R}^3$ (the axis of rotation) and an angle $-\pi \le \theta \le \pi$ (we adopt the convention that rotation are "right-handed"). Replacing v by $-v$ if necessary, we can assume $0 \le \theta \le \pi$.

Let B be the closed ball of radius π in $\mathbb{R}^3$, centred at the origin. Then we have a map

$$\psi \colon B \to \mathrm{SO}(3),$$

where $\psi(u)$ is the rotation about the axis u through the angle $|u|$ (and $\psi(0) = I$). This map is continuous, even at the origin. It is injective except for the fact that it maps antipodal points on the boundary of B to the same rotation.

Therefore, we can identify SO(3) (homeomorphically) with $B/\sim$, where $\sim$ denotes the identification of antipodal points on the boundary. It is known that $B/\sim$ is homeomorphic to the manifold $\mathbb{RP}^3$ (real projective space of dimension 3) and is not simply connected. Specifically, consider a diameter of B (a line through the origin from one point on the boundary to the antipodal point). This is a loop in $B/\sim$ (since the antipodal points are identified) that cannot be shrunk continuously to a point in $B/\sim$. We will come back to this issue, with a proof of this last point, in Section 6.4.

While we will not prove it, it turns out that we have the following.

(a) Among the compact classical groups, SU(n) and Sp(n) are simply connected, while SO(n) ($n \ge 2$) and U(n) are not.

(b) Among the other classical groups, SL($n, \mathbb{C}$) and Sp($n, \mathbb{C}$) are simply connected, while GL($n, \mathbb{R}$)$^+$ ($n \ge 2$), GL($n, \mathbb{C}$), SL($n, \mathbb{R}$) ($n \ge 2$), SO($n, \mathbb{C}$) and Sp($n, \mathbb{R}$) are not.

6.3 Three Lie groups with tangent space $\mathbb{R}$

We have seen that SO(2) and O(2) have the same tangent space (at the identity) and that this tangent space is $\mathbb{R}$ (recall that SO(2) can be identified with the unit circle). The Lie bracket on this tangent space is trivial since

$$[X, Y] = XY - YX = 0 \quad \text{for } X, Y \in \mathbb{R}.$$

Thus the Lie algebras of SO(2) and O(2) are isomorphic.

Recall that $\mathbb{R}$, with vector addition, is also a matrix Lie group. Its tangent space is also $\mathbb{R}$ itself (as above, the Lie bracket has to be trivial) and so it has the same tangent space as SO(2) and O(2).

However, even though SO(2), O(2), and $\mathbb{R}$ are Lie groups with the same Lie algebras, they are not isomorphic Lie groups. For instance, they have different topological properties:

- SO(2) is connected but not simply connected,
- O(2) is not connected,
- $\mathbb{R}$ is connected and simply connected.

They can also be distinguished algebraically:

- SO(2) has exactly two elements ($\pm I$) that square to the identity. (To see this, identify SO(2) with the rotations in the plane.)
- O(2) has at least four elements that square to the identity:

  $$\begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix}.$$

  (In fact, O(2) has an infinite number of elements that square to the identity—all reflections of the plane have this property.)
- $\mathbb{R}$ has only one element, namely 0, that 'squares' to the identity (remember that 0 is the identity of $\mathbb{R}$ since the group operation is addition, and 'squaring' is really adding a real number to itself).

Other examples of nonisomorphic Lie groups with isomorphic Lie algebras can be found in [Sti08, Ex. 9.1.2–9.1.4]. To do these exercises, it is useful to know about the Lie algebra of a product of Lie groups. Recall that if G and H are (matrix) Lie groups, then $G \times H$ is also a (matrix) Lie group (see Section 1.8).

If V_1 and V_2 are vector spaces, then we define

$$V_1 \oplus V_2 = \{(v_1, v_2) \mid v_1 \in V_1, v_2 \in V_2\}$$

with vector addition being defined component wise and scalar multiplication defined by

$$r(v_1, v_2) = (rv_1, rv_2).$$

If $\mathfrak{g}$ and $\mathfrak{h}$ are Lie algebras, then $\mathfrak{g} \oplus \mathfrak{h}$ becomes a Lie algebra with bracket defined by

$$[(X_1, Y_1), (X_2, Y_2)] = ([X_1, X_2], [Y_1, Y_2]), \quad X_1, X_2 \in \mathfrak{g},\ Y_1, Y_2 \in \mathfrak{h}.$$

Lemma 6.3.1. *If G and H are Lie groups with Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$. Then the Lie algebra of $G \times H$ is $\mathfrak{g} \oplus \mathfrak{h}$.*

Proof. The proof is left as an exercise (Exercise 6.3.1). □

Exercises.

6.3.1. Prove Lemma 6.3.1.

6.4 Three Lie groups with the cross-product Lie algebra

We have seen that $\mathfrak{su}(2)$ is isomorphic, as a Lie algebra, to $\mathbb{R}^3$ with the cross-product (see Exercise 5.4.3). The Lie algebra $\mathfrak{so}(3)$ of SO(3) is also isomorphic to $\mathbb{R}^3$ with the cross-product (see [Sti08, Ex. 5.2.4]). Furthermore, we have seen that O(3) has the same Lie algebra as SO(3).

However, the Lie groups SU(2), SO(3) and O(3) are not isomorphic. For instance, they have different topological properties:

- O(3) is not connected,
- SO(3) is connected, but not simply connected (as we will see below),
- SU(2) is connected and simply connected (recall that SU(2) can be identified with the three sphere of unit quaternions).

The relationship between SO(3) and O(3) is rather straightforward: SO(3) is the connected component of O(3) containing the identity. What is the precise relationship between SO(3) and SU(2)?

Recall that SU(2) can be identified with the set of unit quaternions (when we use the presentation of quaternions as 2×2 complex matrices) and that SO(3), the group of rotations of $\mathbb{R}^3$, can be identified with pairs $\{\pm q\}$ of unit quaternions—conjugation by a quaternion yields a rotation of the space of unit quaternions and conjugation by q and $-q$ produces the same rotation (see Section 1.5). Furthermore we have the map (see Proposition 1.5.7)

$$\mathrm{SU}(2) \to \mathrm{SO}(3), \quad q \mapsto \{\pm q\}.$$

This a 2-to-1 map that is *locally* 1-to-1. In fact, it is a covering space. We can now complete the argument started in Section 6.2 that SO(3) is not simply connected. A path in SU(2) from a unit quaternion q to its antipode $-q$ is sent, under the above map $\mathrm{SU}(2) \to \mathrm{SO}(3)$, to a loop in SO(3) since q and $-q$ are identified under this map. By Lemma 6.1.9, this loop cannot be contracted to a point because its lift in SU(2) cannot be contracted (the endpoints differ). Thus SO(3) is not simply connected.

We say that SU(2) is a *double cover* of SO(3). We noted before that SU(n) is simply connected for all n. It turns out that all the groups SO(n), $n \geq 3$, are doubly covered by simply connected groups. These double covers are called the *spin groups* Spin(n).

In low dimensions, there are isomorphisms among the classical Lie groups ("accidental isomorphisms"). In particular, there are isomorphisms between low dimensional spin groups and certain classical groups. Specifically, we have

- $\mathrm{Spin}(3) \cong \mathrm{Sp}(1) = \mathrm{SU}(2)$,
- $\mathrm{Spin}(4) \cong \mathrm{Sp}(1) \times \mathrm{Sp}(1)$,
- $\mathrm{Spin}(5) \cong \mathrm{Sp}(2)$,
- $\mathrm{Spin}(6) \cong \mathrm{SU}(4)$.

The Spin groups play an important role in physics. In general, the Spin groups can be constructed as a certain group of invertible elements in the so-called *Clifford algebra* over $\mathbb{R}^n$. In particular, Spin(n) is a matrix Lie group.

6.5 The Lie group-Lie algebra correspondence

In this section, we will discuss a (partial) converse to Theorem 5.13.1. It turns out that we need to add an extra assumption: that the matrix Lie group be simply connected.

Theorem 6.5.1. *Suppose G and H are matrix Lie groups with Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$. Let $\phi\colon \mathfrak{g} \to \mathfrak{h}$ be a Lie algebra homomorphism. If G is simply connected, then there exists a unique Lie group homomorphism $\Phi\colon G \to H$ such that $\Phi(\exp X) = \exp(\phi(X))$ for all $X \in \mathfrak{g}$.*

Before proving this theorem, we state one immediate corollary, which serves as partial motivation.

Corollary 6.5.2. *Two simply connected Lie groups with isomorphic Lie algebras are isomorphic.*

Proof. Suppose G and H are simply connected Lie groups with isomorphic Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$. Let $\phi : \mathfrak{g} \to \mathfrak{h}$ be a Lie algebra isomorphism. By Theorem 6.5.1, we have a corresponding Lie group homomorphism $\Phi\colon G \to H$. Since $\phi^{-1} : \mathfrak{h} \to \mathfrak{g}$ is also a Lie algebra homomorphism, there exists a corresponding Lie group homomorphism $\Psi\colon H \to G$. It remains to show that $\Psi \circ \Phi = \mathrm{id}_G$ and $\Phi \circ \Psi = \mathrm{id}_H$.

Since our association of Lie algebras to Lie groups is a functor, the Lie algebra homomorphism associated to $\Psi \circ \Phi$ is $\phi^{-1} \circ \phi = \mathrm{id}_{\mathfrak{g}}$. Therefore, by Proposition 5.13.7, we have $\Psi \circ \Phi = \mathrm{id}_G$. Similarly, $\Phi \circ \Psi = \mathrm{id}_H$. □

Proof of Theorem 6.5.1. Our proof will proceed in steps.

1. Define Φ in a neighbourhood of the identity.

2. Define Φ on an arbitrary element via a path and using a partition of the path.

3. Prove independence of the partition.

4. Prove independence of the path

5. Prove Φ is a homomorphism and $\Phi(\exp X) = \exp(\phi(X))$.

Step 1. We know there exists a neighbourhood V of the identity in G such that the exponential mapping has an local inverse mapping V into the Lie algebra $\mathfrak{g}$. We make V small enough so that for all $A, B \in V$, the Campbell–Baker–Hausdorff Theorem applies to $\log A$ and $\log B$. This neighbourhood V will be fixed for the remainder of the proof.

On V, we define $\Phi : V \to H$ by

$$\Phi(A) = \exp(\phi(\log A)), \quad A \in V.$$

In other words, on V, we have $\Phi = \exp \circ \phi \circ \log$. This is the only possible definition if we want to satisfy $\Phi(\exp(X)) = \exp(\phi(X))$ for all $X \in \mathfrak{g}$.

Step 2. We now want to extend the definition of Φ to all of G. Let $A \in G$. Since G is path-connected, there exists a path $A\colon [0,1] \to G$ with $A(0) = I$ and $A(1) = A$. Using a compactness argument similar to the one used in Corollary 5.11.8, there exist numbers

$$0 = t_0 < t_1 < t_2 < \cdots < t_m = 1$$

such that for each $i = 0, \ldots, m-1$,

$$t_i \le s \le t \le t_{i+1} \implies A(t)A(s)^{-1} \in V. \tag{6.1}$$

Note that this implies, in particular, that $A(t_1) \in V$ since $t_0 = 0$ and $A(0) = I$. Now, we write $A = A(1)$ in the form

$$A = \big(A(1)A(t_{m-1})^{-1}\big)\big(A(t_{m-1})A(t_{m-2})^{-1}\big) \cdots \big(A(t_2)A(t_1)^{-1}\big)A(t_1).$$

Since we want Φ to be a homomorphism, we then *define*

$$\Phi(A) = \Phi\big(A(1)A(t_{m-1})^{-1}\big)\Phi\big(A(t_{m-1})A(t_{m-2})^{-1}\big) \cdots \Phi\big(A(t_2)A(t_1)^{-1}\big)\Phi(A(t_1)), \tag{6.2}$$

where each factor is defined in Step 1, since the argument lies in V.

Step 3. Our definition above involved a partition of the path. We would like to show that the definition is actually independent of this choice. It is in this step that we use the Campbell–Baker–Hausdorff Theorem. We will show that "refining" the partition (that is, adding additional partition points) does not change the definition of $\Phi(A)$. Do do this, it suffices to show that the result is not changed under the addition of a single partition point. Since any two partitions have a common refinement (for instance, take the union of the two sets of partition points), the result will follow. Recall the definition of the Lie polynomials F_n given in (5.6).

Note that if a given partition satisfies (6.1), then any refinement of that partition also satisfies this condition. Suppose we insert an extra partition point s between t_i and t_{i+1}. Then, the factor $\Phi(A(t_{i+1})A(t_i)^{-1})$ in (6.2) will be replaced by

$$\Phi\big(A(t_{i+1})A(s)\big)\Phi\big(A(s)A(t_i)^{-1}\big).$$

Since $t_i \leq s \leq t_{i+1}$, (6.1) implies that

$$A(t_{i+1})A(s)^{-1},\ A(s)A(t_i)^{-1},\ A(t_{i+1})A(t_i)^{-1} \in V.$$

Thus, the result would follow if we knew that Φ was a homomorphism on V (as defined in Step 1). Now, since V is in the image of the exponential map, any element of V can be written in the form e^X for some $X \in \mathfrak{g}$. We have

$$\begin{aligned}\Phi(e^X e^Y) &= \Phi\left(e^{\sum_{n\geq 1} F_n(X,Y)}\right)\\ &= e^{\phi\left(\sum_{n\geq 1} F_n(X,Y)\right)}\\ &= e^{\sum_{n\geq 1} F_n(\phi(X),(Y))}\\ &= e^{\phi(X)}e^{\phi(Y)}\\ &= \Phi(e^X)\Phi(e^Y),\end{aligned}$$

where, in the third equality, we used the fact that ϕ is a Lie algebra homomorphism and the F_n are Lie polynomials. Thus Φ is a homomorphism on V and we are done this step.

Step 4. We now need to prove that the definition of $\Phi(A)$ is independent of the path we chose. This is where we used the fact that G is simply connected.

Suppose that $A_0, A_1 \colon [0,1] \to G$ are two paths from I to A. Then A_0 and A_1 are homotopic with endpoints fixed. Namely, there exists a continuous map

$$A\colon [0,1]\times[0,1] \to G$$

such that

$$A(0,t) = A_0(t), \quad A(1,t) = A_1(t) \quad \text{for all } t \in [0,1],$$

and

$$A(s,0) = I, \quad A(s,1) = A \quad \text{for all } s \in [0,1].$$

By an compactness argument similar to the one used in Step 1, there exists an integer N such that for all $(s,t),(s',t') \in [0,1]\times[0,1]$ with $|s-s'| \leq 2/N$ and $|t-t'| \leq 2/N$, we have $A(s,t)A(s',t')^{-1} \in V$.

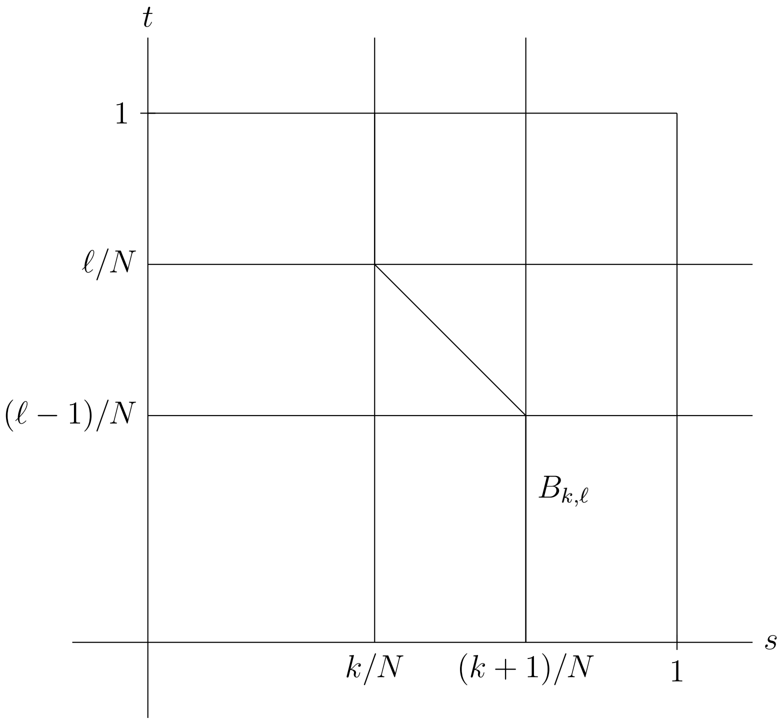
We will now gradually deform A_0 into A_1 by defining a sequence of paths $B_{k,\ell}(t)$, $k = 0,\dots,N-1$, $\ell = 0,\dots,N$. We define $B_{k,\ell}(t)$ as follows. If $\ell > 0$, let

$$B_{k,\ell}(t) = \begin{cases} A\left(\frac{k+1}{N}, t\right) & 0 \leq t \leq \frac{\ell-1}{N},\\ \text{“diagonal” (see picture)} & \frac{\ell-1}{N} \leq t \leq \frac{\ell}{N},\\ A\left(\frac{k}{N}, t\right) & \frac{\ell}{N} \leq t \leq 1.\end{cases}$$

For $\ell = 0$, we define

$$B_{k,0}(t) = A\left(\frac{k}{N}, t\right), \quad t \in [0,1].$$

In particular, $B_{0,0}(t) = A_0(t)$.



We will now deform A_0 into A_1 in steps. First, we deform $A_0 = B_{0,0}$ into $B_{0,1}$, then into $B_{0,2}$, $B_{0,3}$, etc. until we reach $B_{0,N}$. Then we deform this into $B_{1,0}, B_{1,1}, \ldots, B_{1,N}$. We continue until we reach $B_{N-1,N}$, which we finally deform into A_1. We want to show that $\Phi(A)$ as computed on each of these paths is equal to $\Phi(A)$ as computed using the next one.

Now, for $\ell < N$, the paths $B_{k,\ell}(t)$ and $B_{k,\ell+1}(t)$ are the same except for

$$t \in \left(\frac{\ell-1}{N}, \frac{\ell+1}{N}\right).$$

Now, choose the partition

$$0, \frac{1}{N}, \ldots, \frac{\ell-1}{N}, \frac{\ell+1}{N}, \frac{\ell+2}{N}, \ldots, 1.$$

Then by our choice of N, this partition satisfies Condition 6.1. Therefore, since our definition of $\Phi(A)$ depends only on the value of the path at the partition points, and $B_{k,\ell}(t)$ and $B_{k,\ell+1}(t)$ agree on the partition points, the value of $\Phi(A)$ is the same for these two paths.

A similar argument shows that the value of $\Phi(A)$ computed along $B_{k,N}$ is the same as along $B_{k+1,0}$. Therefore, the value of $\Phi(A)$ is the same for each of our paths $B_{k,\ell}$ and then (by the same argument) the same as A_1. Thus we have shown independence of path.

Step 5. One can show that Φ is a homomorphism as follows. For $A, B \in G$, choose path $A(t)$ and $B(t)$ from I to A and B, respectively. Then construct a path $C(t)$ from I to AB by

$$C(t) = \begin{cases} C(t) = A(2t) & t \in [0, 1/2], \\ C(t) = AB(2t-1) & t \in [1/2, 1]. \end{cases}$$

Then it follows from the definition of Φ above that $\Phi(AB) = \Phi(A)\Phi(B)$ (see Exercise 6.5.1).

Now, since Φ is defined near the identity as $\Phi = \exp \circ \phi \circ \log$, we have

$$\frac{d}{dt}\, \Phi\left(e^{tX}\right)\Big|_{t=0} = \frac{d}{dt}\, e^{t\phi(X)}\Big|_{t=0} = \phi(X).$$

Therefore ϕ is the Lie algebra homomorphism associated to the Lie group homomorphism Φ, as desired. □

Exercises.

6.5.1. Complete Step 5 of the proof of Theorem 6.5.1 by showing that $\Phi(AB) = \Phi(A)\Phi(B)$.

6.6 Covering groups

Definition 6.6.1 (Universal covering group)**.** Suppose G is a connected Lie group. Then a *universal covering group* (or *universal cover*) of G is a simply connected Lie group $\tilde{G}$ together with a Lie group homomorphism $\Phi\colon \tilde{G} \to G$ such that the associated Lie algebra homomorphism $\phi\colon \tilde{\mathfrak{g}} \to \mathfrak{g}$ is a Lie algebra isomorphism. The homomorphism Φ is called the *covering homomorphism* (or *projection map*).

Note that this theorem does not specify that the Lie groups be *matrix* Lie groups. In fact, the universal cover of matrix Lie group may be a nonmatrix Lie group. For instance, the universal covering group $\widetilde{\mathrm{SL}(2,\mathbb{C})}$ of $\mathrm{SL}(2,\mathbb{C})$ is a nonmatrix Lie group. However, universal covering groups always exist, as the next theorem tells us.

Theorem 6.6.2 (Existence and uniqueness of universal covering groups)**.** *For any connected Lie group, a universal cover exists. If G is a connected Lie group and (H_1, Φ_1) and (H_2, Φ_2) are universal covers of G, then there exists a Lie group isomorphism $\Psi\colon H_1 \to H_2$ such that $\Phi_2 \circ \Psi = \Phi_1$. In other words, the diagram*

$$\begin{tikzcd} H_1 \arrow[rr, "\Psi"] \arrow[dr, "\Phi_1"'] & & H_2 \arrow[dl, "\Phi_2"] \\ & G & \end{tikzcd}$$

commutes.

Proof. We will not prove the existence part of this theorem (see [Hal03, App. C]). Uniqueness follows from Theorem 6.5.1 as follows. Suppose (H_1, Φ_1) and (H_2, Φ_2) are universal covers of G. Then the corresponding Lie algebra maps ϕ_1, ϕ_2 are isomorphisms. By Theorem 6.5.1, there exists a Lie group homomorphism $\Psi\colon H_1 \to H_2$ corresponding to the isomorphism $\phi_2^{-1} \circ \phi_1\colon \mathfrak{h}_1 \to \mathfrak{h}_2$ of their Lie algebras and a Lie group homomorphism $\Psi'\colon H_2 \to H_1$ corresponding to $\phi_1^{-1} \circ \phi_2$. Then, the composition $\Psi' \circ \Psi\colon H_1 \to H_1$ corresponds to the identity Lie algebra homomorphism. By the uniqueness statement in Theorem 6.5.1, we have $\Psi' \circ \Psi = \mathrm{id}_{H_1}$. Similarly, $\Psi \circ \Psi' = \mathrm{id}_{H_2}$. Again, by the uniqueness statement in Theorem 6.5.1, we have $\Phi_2 \circ \Psi = \Phi_1$. □

Remark 6.6.3. (a) Since the universal cover of a Lie group G is unique up to isomorphism, we often speak of *the* universal cover.

(b) If $\tilde{G}$ is a simply connected Lie group and $\phi\colon \tilde{\mathfrak{g}} \to \mathfrak{g}$ is a Lie algebra isomorphism, then by Theorem 6.5.1, there exists a Lie group homomorphism $\Phi\colon \tilde{G} \to G$ inducing ϕ. This yields a universal cover of G. Using ϕ, we can identify $\tilde{\mathfrak{g}}$ and $\mathfrak{g}$. Thus, by a slight abuse of terminology, we sometimes think of the universal cover of G as the unique simply connected Lie group with the same Lie algebra as G (we use the identity map $\mathfrak{g} \to \mathfrak{g}$ to construct the covering homomorphism).

(c) A *covering group* (not necessarily universal) of a connected Lie group G is a connected Lie group H (not necessarily simply connected) together with a Lie group homomorphism $\Phi\colon H \to G$ such that the associated Lie algebra homomorphism $\phi\colon \mathfrak{h} \to \mathfrak{g}$ is an isomorphism. In general, a Lie group can have many nonisomorphic covering groups, with different fundamental groups.

Examples 6.6.4. (a) $G = \mathbb{S}^1$. The universal cover is $\mathbb{R}$ and the covering homomorphism is the map $\mathbb{R} \to \mathbb{S}^1$ given by $\theta \mapsto e^{i\theta}$.

(b) $G = \mathrm{SO}(3)$. The universal cover is $\mathrm{SU}(2)$ and we have described the covering homomorphism in Section 1.5.

(c) $G = \mathrm{U}(n)$. The universal cover is $\mathbb{R} \times \mathrm{SU}(n)$ and the covering homomorphism is the map

$$\mathbb{R} \times \mathrm{SU}(n) \to \mathrm{U}(n), \quad (\theta, U) \mapsto e^{i\theta} U. \tag{6.3}$$

Since $\mathbb{R}$ and $\mathrm{SU}(n)$ are simply connected, $\mathbb{R} \times \mathrm{SU}(n)$ is simply connected. The Lie algebra homomorphism associated to (6.3) is

$$\mathbb{R} \oplus \mathfrak{su}(n) \mapsto u(n), \quad (r, A) \mapsto irI + A, \quad r \in \mathbb{R},\ A \in \mathfrak{su}(n). \tag{6.4}$$

It thus suffices to check that (6.4) is a Lie algebra isomorphism and that (6.3) is a Lie group homomorphism (Exercise 6.6.1).

(d) As discussed before, the universal cover of $\mathrm{SO}(n)$, $n \geq 3$, is $\mathrm{Spin}(n)$ and these are double covers (i.e. the covering homomorphisms are 2-to-1).

Remark 6.6.5. In the above examples, the universal covers are all matrix Lie groups. In general, one can show that the universal cover of a *compact* matrix Lie group is again a matrix Lie group (not necessarily compact).

Remark 6.6.6. The universal covering construction is inverse to the process of taking the quotient by a discrete subgroup because the kernel of the covering homomorphism $\tilde{G} \to G$ is a discrete subgroup of $\tilde{G}$, called the *fundamental group* of G. It can be shown that the fundamental group of a Lie group is always abelian, even though the fundamental group of an arbitrary smooth manifold can be any finitely presented group (finite number of generators and relations). Thus, the topology of Lie groups is rather constrained.

Remark 6.6.7. If a simply connected Lie group with Lie algebra $\mathfrak{g}$ has a discrete centre, then the set of all connected Lie groups with Lie algebra $\mathfrak{g}$ form a lattice, corresponding to the lattice of subgroups of the centre of the simply connected Lie group. For example, this happens with $\mathfrak{g} = \mathfrak{sl}(2, F)$, where $F = \mathbb{R}$ or $\mathbb{C}$. The Lie group $\mathrm{SL}(2, F)$ has universal cover $\widetilde{\mathrm{SL}(2, F)}$ and every Lie group with Lie algebra $\mathfrak{g}$ has $\widetilde{\mathrm{SL}(2, F)}$ as its universal cover and is a cover of $\mathrm{PSL}(2, F) := \mathrm{SL}(2, F)/Z(\mathrm{SL}(2, F))$, where $Z(\mathrm{SL}(2, F)) = \{\pm 1\}$.

Exercises.

6.6.1. Prove the following:

(a) The map (6.4) is a Lie algebra isomorphism.

(b) The map (6.4) is the Lie algebra homomorphism corresponding to the map (6.3).

(c) The map (6.3) is a Lie group homomorphism.

6.7 Subgroups and subalgebras

Given the close connections between Lie groups and Lie algebras, it seems natural to expect that there is a relationship between the subgroups of a Lie group and the subalgebras of its Lie algebra. If G and H are matrix Lie groups with $H \subseteq G$, then it is clear that $\mathfrak{h}$ is a Lie subalgebra of $\mathfrak{g}$. In general the converse is false, as the following example illustrates.

Example 6.7.1. Consider the matrix Lie group $\mathrm{GL}(2, \mathbb{C})$, with Lie algebra $\mathfrak{gl}(2, \mathbb{C})$. If we fix an irrational number a, then

$$\mathfrak{h} = \left\{ \begin{pmatrix} it & 0 \\ 0 & ita \end{pmatrix} \;\middle|\; t \in \mathbb{R} \right\} \tag{6.5}$$

is a one-dimensional real subalgebra of $\mathfrak{gl}(2,\mathbb{C})$. Any matrix Lie group H with Lie algebra $\mathfrak{h}$ would have to contain

$$H_0 = \exp(\mathfrak{h}) = \left\{ \begin{pmatrix} e^{it} & 0 \\ 0 & e^{ita} \end{pmatrix} \;\middle|\; t \in \mathbb{R} \right\}.$$

Being a matrix Lie group, H would need to be closed in $\mathrm{GL}(2,\mathbb{C})$. But the closure of H_0 in $\mathrm{GL}(2,\mathbb{C})$ is

$$H_1 = \left\{ \begin{pmatrix} e^{it} & 0 \\ 0 & e^{is} \end{pmatrix} \;\middle|\; s,t \in \mathbb{R} \right\}.$$

Then $\mathfrak{h}$ would have to contain the Lie algebra of H_1, which is two dimensional. This is a contradiction. Thus, there is no matrix Lie group corresponding to $\mathfrak{h}$.

The problem in Example 6.7.1 is due to the fact that we are restricting our attention to matrix Lie groups. We can resolve the issue by relaxing this condition.

Definition 6.7.2 (Lie algebra of an arbitrary matrix group)**.** Suppose H is *any* subgroup of $\mathrm{GL}(n,\mathbb{C})$. We define the *Lie algebra* of H to be the set

$$\{X \in M_n(\mathbb{C}) \mid e^{tX} \in H \text{ for all } t \in \mathbb{R}\}. \tag{6.6}$$

Definition 6.7.3 (Connected Lie subgroup)**.** Suppose G is a matrix Lie group with Lie algebra $\mathfrak{g}$. We say $H \subseteq G$ is a *connected Lie subgroup* (or *analytic subgroup*) of G if the following conditions are satisfied:

(a) H is a subgroup of G.

(b) The Lie algebra $\mathfrak{h}$ of H is a subspace of $\mathfrak{g}$.

(c) Every element of H can be written in the form $e^{X_1}e^{X_2}\cdots e^{X_m}$, with $X_1,\dots,X_m \in \mathfrak{h}$.

Example 6.7.4. The group H_0 of Example 6.7.1 is a connected Lie subgroup of $\mathrm{GL}(2,\mathbb{C})$ with Lie algebra $\mathfrak{h}$ given by (6.5).

The word *connected* in Definition 6.7.3 is justified by the following result.

Proposition 6.7.5. *If H is a connected Lie subgroup of a matrix Lie group G, then H is path-connected.*

Proof. It suffices to show that any element of H can be connected to the identity by a continuous path taking values in H. We will prove, by induction on m, that any element of H of the form

$$h = e^{X_1}e^{X_2}\cdots e^{X_m}, \quad m \in \mathbb{N},\ X_1,\dots,X_m \in \mathfrak{h},$$

can be connected to the identity by a continuous path lying in H. Since H is a connected Lie subgroup of G, all elements of H are of this form.

For $m = 0$, we have $h = 1$ and the result is trivial. Assume $m \geq 1$ and that the result is true for $m-1$. For $X_1,\dots,X_m \in \mathfrak{h}$, define the continuous path

$$h(t) = e^{X_1}e^{X_2}\cdots e^{X_m}e^{-tX_m} = e^{X_1}e^{X_2}\cdots e^{(1-t)X_m}.$$

By the definition of $\mathfrak{h}$, we have $e^{-tX_m} \in H$ for all $t \in \mathbb{R}$. Thus $h(t)$ is contained in H. We have $h(0) = e^{X_1}e^{X_2} \cdots e^{X_m}$ and $h(1) = e^{X_1}e^{X_2} \cdots e^{X_{m-1}}$. By the induction hypothesis, there is a path, contained in H, connecting $h(1)$ to the identity. This completes the proof of the inductive step. □

Proposition 6.7.6. *Suppose H is a connected Lie subgroup of a matrix Lie group G. Then the Lie algebra $\mathfrak{h}$ of H is a subalgebra of the Lie algebra $\mathfrak{g}$ of G.*

Proof. If $A \in H$ and $Y \in \mathfrak{h}$, then, for all $t \in \mathbb{R}$, we have

$$e^{tAYA^{-1}} = Ae^{tY}A^{-1} \in H.$$

Thus $AYA^{-1} \in \mathfrak{h}$. It follows that, for $X, Y \in \mathfrak{h}$,

$$e^{tX}Ye^{-tX} \in \mathfrak{h} \quad \text{for all } t \in \mathbb{R}.$$

Since $\mathfrak{h}$ is a vector space, it is a topologically closed subset of $M_n(\mathbb{C})$. Therefore, for $X, Y \in \mathfrak{h}$,

$$[X, Y] = XY - YX = \frac{d}{dt}e^{tX}Ye^{-tX}\bigg|_{t=0} = \lim_{h\to 0} \frac{e^{hX}Ye^{-hX} - Y}{h} \in \mathfrak{h}.$$

Therefore $\mathfrak{h}$ is a Lie subalgebra of $\mathfrak{g}$. □

Theorem 6.7.7. *Suppose G is a matrix Lie group with Lie algebra $\mathfrak{g}$, and let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{g}$. Then*

$$H = \{e^{X_1}e^{X_2} \cdots e^{X_m} \mid X_1, \dots, X_m \in \mathfrak{h}\}$$

is the unique connected Lie subgroup H of G such that the Lie algebra of H is $\mathfrak{h}$.

We will not prove Theorem 6.7.7. A proof can be found in [Hal03, §3.8]. The connected Lie subgroup H corresponding to the subalgebra $\mathfrak{h}$ in Theorem 6.7.7 may or may not be matrix Lie group. It is a matrix Lie group precisely when H is a closed subset of G. However, we have the following result.

Theorem 6.7.8. *Suppose that G is a matrix Lie group and that H is a connected Lie subgroup of G. Then H can be given the structure of a Lie group in such a way that the inclusion of H into G is a Lie group homomorphism.*

Proof. We give only a sketch of the proof. We first note that the topology on H induced from the topology on G can be very bad. For example, H might not even be locally connected in this topology. So, in general, we need a different topology on H. For any $A \in H$ and $\varepsilon > 0$, define

$$U_{A,\varepsilon} = \{Ae^X \mid X \in \mathfrak{h},\ \|X\| < \varepsilon\}.$$

We then define a topology on H by using the $U_{A,\varepsilon}$ as basic open sets. More precisely, we define a subset $U \subseteq H$ to be open if, for all $A \in U$, there exists $\varepsilon > 0$ such that $U_{A,\varepsilon} \subseteq U$.

In fact, H can be made into a smooth manifold by using the sets $U_{A,\varepsilon}$ as basic coordinate neighbourhoods, and using the maps $X \mapsto Ae^X$ as local coordinate maps. One can then show that the product and inverse maps on H are smooth with respect to this smooth manifold structure.

Finally, one can show that any set of H that is open in the topology induced from the topology of G is also open in the topology defined above. It follows that the inclusion of G into H is continuous (the preimage of open sets are open). □

Theorem 6.7.9. *Every finite-dimensional real Lie algebra is isomorphic to the Lie algebra of some Lie group.*

Proof. We give only a sketch of the proof. Ado's Theorem (which we have not proven) states that every finite-dimensional real Lie algebra is isomorphic to a subalgebra of $\mathfrak{gl}(n, \mathbb{R})$. Theorem 6.7.8 then implies that there is a Lie group with this Lie algebra. We are implicitly using here the fact that the more abstract definition of the Lie algebra of a (general) Lie group coincides with Definition 6.7.2 for connected Lie subgroups. □

Proposition 6.7.10. *The association of the Lie algebra to a Lie group yields a one-to-one correspondence between isomorphism classes of simply connected (real) Lie groups and isomorphism classes of finite-dimensional real Lie algebras.*

Proof. Let F be the map from the set of isomorphism classes of simply connected Lie groups to the set of isomorphism classes of real Lie algebras given by taking the Lie algebra of a Lie group. Then F is injective by Corollary 6.5.2. Suppose $\mathfrak{g}$ is a real Lie algebra. Then, by Theorem 6.7.9, there exists a Lie group G with Lie algebra $\mathfrak{g}$. By Theorem 6.6.2, G has a universal cover $\tilde{G}$ with Lie algebra $\mathfrak{g}$. Thus F is surjective. □

Another way of summarizing some of the results above is that when we restrict the functor from Lie groups to Lie algebras given in Theorem 5.13.1 to the (full) subcategory of simply connected Lie groups, it yields an equivalence of categories between the category of simply connected Lie groups and the category of finite-dimensional real Lie algebras.

Chapter 7

Further directions of study

In this course, we have only scratched the surface of the topic of Lie groups. There is much more to learn. In this final chapter we give a brief (and not, by any means, comprehensive) overview of some further directions of study.

7.1 Lie groups, Lie algebras, and quantum groups

One obvious direction of further study is to expand one's focus to *all* Lie groups, instead of just matrix Lie groups. As we saw in Chapter 6, this more general viewpoint is necessary if one wants to fully discuss topics just as covering groups, quotients by normal subgroups (for example, there is a quotient of the Heisenberg group that is not a matrix Lie group—see [Sti08, p. 72]), etc.

The study of Lie algebras themselves is also a very active area of research. The finite-dimensional simple complex Lie algebras have been classified. A more general class of Lie algebras are the so-called *Kac–Moody algebras*. The *affine* Lie algebras can, in some sense, be viewed as the next step beyond finite-dimensional simple Lie algebras. They play an important role in physics and the theory of vertex algebras. The books [EW06, Hum78] are good references for the finite-dimensional theory, while [Kac90] is a standard reference for the infinite-dimensional setting.

To any Lie algebra, one can associated its *universal enveloping algebra*. It is an associative algebra that has the same representation theory as the original Lie algebra. These universal enveloping algebras can be *q-deformed* to produce *quantum groups* or *quantized enveloping algebras*. Taking the parameter q to 1 recovers the original enveloping algebra. On the other hand, taking q to zero results in a structure known as a *crystal*, where algebra is replaced by combinatorics. This construction plays a central role in combinatorial representation theory. The books [HK02, Kas95] are good references for these topics.

7.2 Superalgebras and supergroups

An interesting and active area of research is the generalization from the "standard" setting to the "super" setting. A *supermanifold* is similar to a manifold, except that instead of looking locally like $\mathbb{R}^n$ for some n, it looks like the superspace $\mathbb{R}^{m|n}$. The variables corresponding to the n "odd" coordinates supercommute ($xy = -yx$) instead of commute. A *Lie supergroup* is then a group object in the category of supermanifolds (see Definition 1.1.4).

The tangent space of a Lie supergroup is naturally a *Lie superalgebra*. A Lie superalgebra is a $\mathbb{Z}_2$-graded vector space $\mathfrak{g} = \mathfrak{g}_0 + \mathfrak{g}_1$ with a bilinear operation $[\cdot,\cdot]\colon \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ (the super Lie bracket) satisfying the following conditions:

(a) It respects the grading: $[\mathfrak{g}_i, \mathfrak{g}_j] \subseteq \mathfrak{g}_{i+j}$ for $i, j \in \mathbb{Z}_2$,

(b) It is super skew-symmetric: $[x, y] = -(-1)^{|x||y|}[y, x]$ for all homogeneous $x, y \in \mathfrak{g}$ (here $|x|$ denotes the parity of x, i.e. $x \in \mathfrak{g}_{|x|}$).

(c) It satisfies the super Jacobi identity:

$$[x, [y, z]] = [[x, y], z] + (-1)^{|x||y|}[y, [x, z]] \quad \text{for all homogeneous } x, y, z \in \mathfrak{g}.$$

A Lie superalgebra $\mathfrak{g}$ with $\mathfrak{g}_1 = 0$ is simply a Lie algebra. The study of Lie superalgebras and Lie supergroups plays an important role in supersymmetry in physics. Many results in Lie algebras have been generalized to Lie superalgebras (for instance, the classification of the complex simple Lie superalgebras). However, there are also many examples of theorems known in the Lie algebra case that have not yet been extended to the Lie superalgebra case.

7.3 Algebraic groups and group schemes

Moving from the setting of smooth manifolds to the setting of algebraic geometry results in a passage from Lie groups to algebraic groups. More precisely, an *algebraic group* is a group object in the category of algebraic varieties (see Section 1.1). Explicitly, an algebraic group (or *group variety*) is a group that is an algebraic variety, such that the multiplication and inversion operations are given by regular functions on the variety. Over a field, affine algebraic groups (where the algebraic variety is an affine variety) are matrix groups. Thus, over the real numbers, the definition of an algebraic group is more restrictive than the definition of a Lie group.

Schemes are generalizations of algebraic varieties. A group object in the category of schemes is called a *group scheme*. There is a well-developed theory of group schemes and this topic continues to be an active area of research.

7.4 Finite simple groups

Killing and Cartan classified the simple Lie groups. This helped pave the way for a classification of the *finite* simple groups. Each matrix Lie group G gives rise to infinitely many finite groups by replacing the entries of G by elements of a finite field (say, the integers modulo some prime p). Since there is a finite field of size q for each prime power q, there are infinitely many finite groups corresponding to each infinite matrix Lie group. In fact, each simple Lie group yields infinitely many finite *simple* groups in this way. These are called the *simple finite groups of Lie type*.

Theorem 7.4.1 (Classification of finite simple groups)**.** *Every finite simple group is*

- *a cyclic group of prime order,*
- *an alternating group of degree at least 5,*
- *a simple group of Lie type, or*
- *one of 26* sporadic groups*.*

The largest sporadic group is called the *Monster group*.

7.5 Representation theory

Once one has learned about the structure of Lie groups themselves, it is natural to investigate their *representations*. A (real) representation of a Lie group G is a Lie group homomorphism

$$G \to \mathrm{GL}(n, \mathbb{R}) \quad \text{or} \quad G \to \mathrm{GL}(V),$$

where V is a real vector space. Complex representations are defined similarly.

Representations can be thought of as an *action* of a group on a vector space. The term "representation" comes from this interpretation—each element of G is "represented" as a linear map on a vector space.

We now know that each complex representation of complex Lie group G yields a Lie algebra homomorphism

$$\mathfrak{g} \to \mathfrak{gl}(n, \mathbb{C}) \quad \text{or} \quad \mathfrak{g} \to \mathfrak{gl}(V),$$

called a *representation* of $\mathfrak{g}$. Often one can answer questions about representations of Lie groups by studying representations of the corresponding Lie algebra, which are often much easier to study. The later chapters of [Hal03] concern the representation theory of Lie groups.

The study of representations of finite groups (e.g. permutation groups) is also an important and interesting topic and does not require knowledge of Lie groups or Lie algebras.

Index

3-sphere of unit quaternions, 8

absolute value
    of a matrix, 52
absolute value of quaternions, 7
adjoint mapping, 76
affine Lie algebra, 101
algebraic group, 102
alternating, 51
analytic subgroup, 98

$\mathbb{C}^*$, 26
Campbell–Baker–Hausdorff Theorem, 81
Cartan–Dieudonné Theorem, 14
category, 1
centres, 44
circle group, 3
circle Lie group, 4
classical groups, 44
classical Lie groups, 20
Clifford algebra, 91
compact, 36
compact classical groups, 44
compact symplectic group, 24
complex general linear group, 21
complex matrix Lie group, 61
complex orthogonal group, 23
complex special linear group, 21
complex symplectic group, 24
complexification
    of a Lie algebra, 62
    of a vector space, 61
component, 29
composition, 1
conjugation, 10
connected component, 29
connected Lie subgroup, 98
convergence of matrices, 20
covering group, 96
covering homomorphism, 95
covering space, 87
crystal, 101

δ-neighbourhood, 69
derivative of a path, 56
differentiable path, 55
Dirac's belt trick, 14
direct product, 17
discrete subgroup, 46
distance between matrices, 46
dot product, 21
double cover, 14, 91

$\mathrm{E}(n)$, 26
Euclidean group, 26
Euclidean space, 3
exponential map
    to $\mathrm{SO}(2)$, 47
    to $\mathrm{SU}(2)$, 48
exponential of a matrix, 53

finite group, 21
finite simple groups, 102
functor, 73
fundamental group, 97

gauge group, 3
general linear group, 3
$\mathrm{GL}(n, \mathbb{C})$, 21
$\mathfrak{gl}(n, \mathbb{C})$, 60
$\mathrm{GL}(n, \mathbb{R})$, 21
$\mathfrak{gl}(n, \mathbb{R})$, 60
group, 2
    circle, 3
    linear, 3
    simple, 14
group action, 103

group object, 2
group scheme, 102
group variety, 102
groups of Lie type, 102

Heisenberg group, 3, 25
homeomorphism, 70
homomorphism of Lie groups, 27
hyperplane, 14

ideal of a Lie algebra, 51
inner product on $\mathbb{R}^n$, 21
inverse, 2
isometry, 14
isomorphism of Lie groups, 27

J, 24
J_{2n}, 25
Jacobi identity, 51

Kac–Moody algebra, 101

Lie algebra, 51
  alternate description, 70
  of a Lie group, 60
  of arbitrary matrix group, 98
Lie bracket, 50, 51
Lie group, 3, 37
Lie group homomorphism, 27
Lie group isomorphism, 27
lie over, 86
Lie polynomial, 81
Lie product formula, 71
Lie superalgebra, 102
Lie supergroup, 102
lift, 87
linear group, 3, 4, 20
linear Lie group, 20
local homeomorphism, 87
log, 64
logarithm, 64
Lorentz group, 3

matrix absolute value, 52
matrix exponential, 53
matrix group, 4, 20
matrix Lie group, 3, 20
  complex, 61
matrix logarithm, 64
maximal torus, 39
metaplectic group, 25
Monster group, 103
morphism, 1
$\mathrm{Mp}(n, \mathbb{R})$, 25

neighbourhood, 69
nilpotent matrix, 55
normal subgroup, 14, 45, 78
normal subgroups
  of $\mathrm{SO}(n)$, $\mathrm{SU}(n)$, $\mathrm{Sp}(n)$, 79

object, 1
  group, 2
  terminal, 1
$\mathrm{O}(n)$, 12, 22, 26
$\mathfrak{o}(n)$, 60
$\mathrm{O}(n, \mathbb{C})$, 23
$\mathfrak{o}(n, \mathbb{C})$, 60
one-parameter subgroup, 72
orientation-preserving, 15
orientation-reversing, 15
orthogonal group, 3, 12, 22, 26

path, 29
  derivative, 56
  differentiable, 55
  smooth, 55
path-connected, 29
Poincaré group, 3
polar decomposition, 33
  $\mathrm{SL}(n, \mathbb{C})$, 35
  $\mathrm{SL}(n, \mathbb{R})$, 34
positive definite, 34, 35
positive matrix, 34, 35
positive semidefinite, 35
projection map, 95
pure imaginary quaternions, 9

quantized enveloping algebra, 101
quantum group, 101
quaternion conjugate, 8
quaternions, 6
  3-sphere, 8

absolute value, 7
pure imaginary, 9

$\mathbb{R}^*$, 26
real form, 64
real general linear group, 21
real special linear group, 21
real symplectic group, 24
reflection in a hyperplane, 14
representation, 103
$\mathbb{R}^n$, 26
rotation, 15

$\mathbb{S}^1$, 4, 26
scheme, 102
Schreier's Theorem, 46
sequential tangent vector, 67
simple group, 14, 45
simple groups, 102
simple Lie algebra, 51
simplicity of $\mathrm{SO}(2m+1)$, 79
simplicity of $\mathfrak{so}(n)$, $\mathfrak{su}(n)$, $\mathfrak{sp}(n)$, 79
simply connected, 85
skew-Hermitian, 57
skew-symmetric, 57
$\mathrm{SL}(n, \mathbb{C})$, 21
slnC$\mathfrak{sl}(n, \mathbb{C})$, 60
$\mathrm{SL}(n, \mathbb{R})$, 21
$\mathfrak{sl}(n, \mathbb{R})$, 60
smooth path, 55
$\mathrm{SO}(2)$, 4
$\mathrm{SO}(n)$, 12, 22
$\mathfrak{so}(n)$, 60
$\mathrm{SO}(n, \mathbb{C})$, 23
$\mathfrak{so}(n, \mathbb{C})$, 60
special complex orthogonal group, 23
special linear group, 3
special orthogonal group, 4, 12, 22
special unitary group, 8, 22
spin groups, 91
$\mathrm{Sp}(n)$, 24
$\mathfrak{sp}(n)$, 60
$\mathrm{Sp}(n, \mathbb{C})$, 24
$\mathfrak{sp}(n, \mathbb{C})$, 60
$\mathrm{Sp}(n, \mathbb{R})$, 24
$\mathfrak{sp}(n, \mathbb{R})$, 60
sporadic group, 103
$\mathfrak{su}(2)$, 51
subgroup
discrete, 46
normal, 14, 45, 78
submultiplicative property, 52
$\mathrm{SU}(n)$, 8, 22
$\mathfrak{su}(n)$, 60
supermanifold, 101
symmetric matrix, 33
symplectic group, 24
complex, 24
real, 24

tangent
sequential, 67
tangent space, 56
of $\mathrm{SU}(2)$, 49
tangent space visibility, 78
tangent vector, 56
terminal object, 1
topological dimension, 70
torus, 39
translation, 26

$\mathrm{U}(n)$, 8, 22
$\mathfrak{u}(n)$, 60
unitary group, 3, 8, 22
universal cover, 95
universal covering group, 95
universal enveloping algebra, 101

Bibliography

[EW06] Karin Erdmann and Mark J. Wildon. *Introduction to Lie algebras*. Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 2006.

[Hal03] Brian C. Hall. *Lie groups, Lie algebras, and representations*, volume 222 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003. An elementary introduction.

[HK02] Jin Hong and Seok-Jin Kang. *Introduction to quantum groups and crystal bases*, volume 42 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[Hum78] James E. Humphreys. *Introduction to Lie algebras and representation theory*, volume 9 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1978. Second printing, revised.

[Kac90] Victor G. Kac. *Infinite-dimensional Lie algebras*. Cambridge University Press, Cambridge, third edition, 1990.

[Kas95] Christian Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Sti08] John Stillwell. *Naive Lie theory*. Undergraduate Texts in Mathematics. Springer, New York, 2008.