Chapter 1

Groups

The topic of this chapter is groups: finite, topological and Lie groups. We start with a quick review of basic definitions and then describe some of the foundational theory of topological and, more particularly, Lie groups. As far as the theory is concerned, our focus will largely be on basic examples, constructions and definitions. We usually omit proofs. A background in differential manifolds — especially Lie brackets and integration — is needed for the latter parts of the chapter. With the possible exception of one or two of the examples (only needed in Chapter 4), readers are likely to be familiar with most of what we survey. A good strategy is probably to skim through the chapter to record the notational conventions which are established and used throughout the book. There are many good introductory texts on finite groups — one we recommend is Scott [160]. A concise graduate level text, which covers much of what we need in this and the following chapter, is Thomas's book [175] which is angled towards the representation theory of finite and Lie groups and includes basic material on induced representations and Lie algebras.

1.1 Definition of a group and examples

Definition 1.1.1 A group consists of a set G with an *identity* element, denoted by $e_G = e$, together with operators of *multiplication* (or composition) $G \times G \to G$; $(g,h) \mapsto gh$, and *inversion* $G \to G$; $g \to g^{-1}$, which satisfy the following properties

(Id) (Identity) $ge = eg = g$, for all $g \in G$.
(In) (Inverse) For all $g \in G$, $gg^{-1} = g^{-1}g = e$.
(As) (Associativity) $(gh)k = g(hk)$, for all $g,h,k \in G$.

The group is *Abelian* or *commutative* if $gh = hg$, for all $g, h \in G$.

Remark 1.1.1 As simple consequences of the definition we have

(1) (Cancellation law) If $gh = g\bar{h}$ (or $hg = \bar{h}g$) then $h = \bar{h}$.
(2) The identity element of G is unique. (That is, if $e' \in G$ satisfies (Id) then $e = e'$.)
(3) Every $g \in G$ has a unique inverse g^{-1}.
(4) $(gh)^{-1} = h^{-1}g^{-1}$, for all $g, h \in G$.

If G is finite, the *order* $|G|$ of G is the number of elements in G.

Definition 1.1.2 Let G be a group. A nonempty subset H of G is a *subgroup* of G if for all $g, h \in H$, $gh^{-1} \in H$.

Remark 1.1.2 If H is a subgroup then $e \in H$ and H inherits the structure of a group from G.

Many interesting examples of groups, both finite and infinite, are obtained as *transformation groups*. That is, as sets of transformations of a space, often preserving some preassigned structure. Group multiplication is then composition of transformations and so is automatically associative. We denote the identity map of the set X by I or I_X.

Example 1.1.1 (1) Let X be a set. If $\mathcal{B}(X)$ denotes the set of bijections of X, then $\mathcal{B}(X)$ is a group with identity element equal to the identity transformation of X. If X is finite, $\mathcal{B}(X)$ is the group $\mathrm{Sym}(X)$ of all permutations of X. We refer to $\mathrm{Sym}(X)$ as the *symmetric group* of X. If $X = \mathbf{n} = \{1, \ldots, n\}$, we write $\mathcal{B}(X) = S_n$ — the *symmetric group* on n-symbols — and have $|S_n| = n!$ The symmetric groups are of special importance in finite group theory; in part this is because every finite group G can be represented as a subgroup of $\mathrm{Sym}(G) \cong S_{|G|}$ (Cayley's theorem).
(2) Let V be a vector space (over $\mathbb{R}$ or $\mathbb{C}$). The *general linear group* of V, $\mathrm{GL}(V)$, is the group of invertible linear transformations of V. If $V = \mathbb{R}$ then $\mathrm{GL}(\mathbb{R}) \approx \mathbb{R}^\star$ (the multiplicative group of non-zero real numbers). Similarly, $\mathrm{GL}(\mathbb{C}) \approx \mathbb{C}^\star$ (the multiplicative group of non-zero complex numbers). If V is of dimension d then, after choosing a basis for V, we may identify $\mathrm{GL}(V)$ with an open subset of the space $M(d, d)$ of $d \times d$-matrices. The group operations of composition and inverse are then smooth — in fact, rational — functions in the components of the matrices. We often write $\mathrm{GL}(n, \mathbb{R})$, instead of $\mathrm{GL}(\mathbb{R}^n)$, and $\mathrm{GL}(n, \mathbb{C})$, instead of $\mathrm{GL}(\mathbb{C}^n)$.
(3) Let V be a vector space over $\mathbb{R}$ and let $(\ ,\ )$ be a (positive definite) inner product on V. Let $\mathrm{O}(V)$ denote the subgroup of $\mathrm{GL}(V)$ consisting of linear

maps A preserving $(\, , \,)$: $(Av, Aw) = (v, w)$, all $v, w \in V$. We refer to $\mathrm{O}(V)$ as the *orthogonal* group of $(V, (\, , \,))$. If V is finite dimensional, we may choose an orthonormal basis of V and identify $(V, (\, , \,))$ with $\mathbb{R}^n$ (standard Euclidian inner product). We always write the orthogonal group of $\mathbb{R}^n$ as $\mathrm{O}(n)$. If instead V is a $\mathbb{C}$-vector space, and $\langle \, , \, \rangle$ is an Hermitian inner product on V, we obtain the *unitary* group $\mathrm{U}(V)$ of V. We write $\mathrm{U}(\mathbb{C}^d) = \mathrm{U}(d)$. Both $\mathrm{O}(n)$ and $\mathrm{U}(d)$ are compact subgroups of the corresponding general linear group. The *special orthogonal* group $\mathrm{SO}(n)$ is the subgroup of $\mathrm{O}(n)$ consisting of linear maps of determinant $+1$. We similarly define the *special unitary group* $\mathrm{SU}(n)$.
(4) Let (X, d) be a metric space. An *isometry* of X is a map $f : X \to X$ preserving distance: $d(f(x), f(y)) = d(x, y)$, all $x, y \in X$. Let $\mathrm{Iso}(X)$ denote the set of isometries of X. We always have $I_X \in \mathrm{Iso}(X)$ and $\mathrm{Iso}(X)$ has the structure of a group where multiplication is given by composition.
(5) The group of isometries of $\mathbb{R}^n$, denoted $\mathbf{E}(n)$, is called the *Euclidean* group. If $f : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry, then we may write $f(x) = Ax + b$, where $A \in \mathrm{O}(n)$ and $b \in \mathbb{R}^n$ are uniquely determined by f. In particular, $\mathrm{O}(n)$ (orthogonal rotations about the origin) and $T(n)$ (the group of all translations of $\mathbb{R}^n$) are naturally defined as subgroups of $\mathbf{E}(n)$. The group $\mathbf{E}(n)$ may be represented as $\mathrm{O}(n) \times T(n)$ (that is, all pairs (A, b)), but the group structure on $O(n) \times T(n)$ is not the obvious one defined componentwise. We return to this point shortly. We let $\mathbf{SE}(n)$ (the *special Euclidean group*) be the subgroup of $\mathbf{E}(n)$ consisting of orientation preserving isometries. We may identify $\mathbf{SE}(n)$ (as a set) with $\mathrm{SO}(n) \times T(n)$.
(6) For $n \geq 3$, let $\mathbf{D}_n$ denote the dihedral group of order $2n$ defined (up to isomorphism) as the subgroup of $\mathbf{O}(2)$ consisting of isometries of a regular n-gon centered at the origin. Denote the subgroup of $\mathbf{D}_n$ consisting of orientation preserving symmetries by $\mathbb{Z}_n$ (or $\mathbb{Z}/n\mathbb{Z}$). Since $\mathbf{D}_n$ permutes the n vertices of a regular n-gon, $\mathbf{D}_n$ naturally embeds as a subgroup of S_n. If $n = 2$, we let $\mathbf{D}_2$ be the group of isometries of a (non-square) rectangle. The groups $\mathbb{Z}_n$, $n \geq 2$, and $\mathbf{D}_2$ are Abelian; $\mathbf{D}_n$ is not Abelian, $n \geq 3$.

Exercise 1.1.1 Prove that $\mathrm{Iso}(\mathbb{R}^n) = \mathbf{E}(n)$. (If $n = 2$, show that an isometry is uniquely determined by its values at three non-collinear points.)

1.2 Homomorphisms, subgroups and quotient groups

Definition 1.2.1 A *homomorphism* $T : G \to K$ of groups G, K is a mapping satisfying $T(gg') = T(g)T(g')$, $(g, g' \in G)$. An *isomorphism* is a bijective homomorphism.

Remark 1.2.1 (1) If $T : G \to K$ is a homomorphism, then $T(e_G) = e_K$.
(2) If $T : G \to K$ is an isomorphism, then $T^{-1} : K \to G$ is a homomorphism.
(3) An isomorphism $T : G \to G$ is usually referred to as an *automorphism* (of G). If there exists $h \in G$ such that $T(g) = hgh^{-1}$, T is an *inner automorphism*. The set of automorphisms $\mathrm{Aut}(G)$ of G is a group under composition which contains the set of inner automorphisms as a subgroup.

Definition 1.2.2 Let H be a subgroup of G.

(1) H is a *normal* subgroup if $gHg^{-1} = H$, for all $g \in G$.
If H is a normal subgroup of G, we write $H \lhd G$.
(2) The *normalizer* $N(H)$ of H is the subgroup of G defined by $N(H) = \{g \in G \mid gHg^{-1} = H\}$.
(3) The centralizer of a subgroup H of G is the subgroup of G defined by $C_G(H) = \{g \in G \mid gh = hg,\ \forall h \in H\}$. We call $C_G(G) = Z(G)$ the *centre* of G.

Remark 1.2.2 Let H be a subgroup of G. Then $H \lhd N(H)$, $C_G(H) \subset N(H)$ and $C_G(H) \cap H = Z(H)$ — the centre of H.

Lemma 1.2.1 *If* $T : G \to K$ *is a homomorphism then* $\mathrm{kernel}(T) \lhd G$ *and* $\mathrm{image}(T)$ *is a subgroup of* K*.*

Lemma 1.2.2 *Let* $G/H = \{gH \mid g \in G\}$ *denote the space of (left) cosets. If* $H \lhd G$*, then* G/H *has the natural structure of a group with respect to which the quotient map* $q : G \to G/H$ *is a homomorphism.*

Example 1.2.1 (1) Give $\mathbb{R}$ the structure of an (additive) group under $+$ (so the identity is 0). For $a \in \mathbb{R}^\star$, the map $M_a : \mathbb{Z} \to \mathbb{R}$ defined by $M_a(n) = an$ is a group monomorphism with image $a\mathbb{Z}$. The Abelian group $\mathbb{R}/a\mathbb{Z}$ is isomorphic to $\mathrm{SO}(2)$ by the map

$$\theta \mapsto \begin{pmatrix} \cos(\frac{2\pi\theta}{a}) & -\sin(\frac{2\pi\theta}{a}) \\ \sin(\frac{2\pi\theta}{a}) & \cos(\frac{2\pi\theta}{a}) \end{pmatrix}.$$

We often identify $\mathbb{R}/2\pi\mathbb{Z}$ (or $\mathbb{R}/\mathbb{Z}$) with $\mathrm{SO}(2)$. Another representation of $\mathrm{SO}(2)$ is as the subgroup $S^1 \subset \mathbb{C}^\star$ consisting of complex numbers of unit modulus. We tend to use the symbol S^1, as opposed to $\mathrm{SO}(2)$, when there is a direct connection to scalar multiplication by complex numbers of unit modulus. For $n \geq 1$, the n-torus $\mathbb{T}^n$ is defined to be $\mathbb{R}^n/2\pi\mathbb{Z}^n \approx \mathrm{SO}(2)^n \approx (S^1)^n$.

(2) If V is a finite dimensional vector space over $\mathbb{R}$, then the determinant defines a homomorphism $\det : \mathrm{GL}(V) \to \mathbb{R}^\star$. The kernel of det is the normal subgroup $\mathrm{SL}(V)$ consisting of linear maps of determinant 1. In case $V = \mathbb{R}^n$, we set $\mathrm{SL}(V) = \mathrm{SL}(n, \mathbb{R})$ and refer to $\mathrm{SL}(n, \mathbb{R})$ as the *special linear* group (of degree n). $\mathrm{SL}(n, \mathbb{R})$ is the group of orientation and volume preserving linear isomorphisms of $\mathbb{R}^n$. We have $GL(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) \approx \mathbb{R}^\star$. We may similarly define $\mathrm{SL}(n, \mathbb{C})$ and $\mathrm{SL}(n, \mathbb{Z})$ (the group of integer $n \times n$-matrices with determinant $+1$).
(3) Let $n \geq 2$. Identify $\mathbb{C}^\star$ with the group of all non-zero multiples of the identity map of $\mathbb{C}^n$. Then $\mathbb{C}^\star \lhd \mathrm{GL}(n, \mathbb{C})$. We define $\mathrm{PGL}_n(\mathbb{C}) = \mathrm{PGL}(n, \mathbb{C}) = \mathrm{GL}(n, \mathbb{C})/\mathbb{C}^\star$ to be the *projective linear group*. If $n = 2$, then $\mathrm{PGL}_2(\mathbb{C})$ is isomorphic to the group of invertible Mobius transformations $z \mapsto \frac{az+b}{cz+d}$ of the Riemann sphere $S^2 = \mathbb{C} \cup \{\infty\}$. We may similarly define the real projective linear groups $\mathrm{PGL}_n(\mathbb{R})$.
(4) Many important examples of finite groups come from geometries defined over a finite field (see [99] for basic material on finite fields). Let p be a prime, $n \geq 1$ and $\mathbb{F} = \mathbb{F}_{p^n}$ denote the finite field of order p^n. Let $\mathrm{GL}(n, \mathbb{F}) = \mathrm{GL}(n, \mathbb{F}_{p^n})$ denote the group of invertible $n \times n$ matrices with entries in $\mathbb{F}$. Setting $p^n = q$, $|\mathrm{GL}(n, \mathbb{F})| = \Pi_{j=0}^{n-1}(q^n - q^j)$ [160, 5.7.20]. We define the projective group $\mathrm{PGL}(n, \mathbb{F})$, or $\mathrm{PGL}_n(\mathbb{F})$, to be $\mathrm{GL}(n, \mathbb{F})/\mathbb{F}^\star$. If we let $\mathrm{Aff}_1(\mathbb{F})$ denote the group of affine isomorphisms of $\mathbb{F}$, then $\mathrm{Aff}_1(\mathbb{F}) = \{(a, b) \mid a \in \mathbb{F}^\star, b \in \mathbb{F}\}$. An element $(a, b) \in \mathrm{Aff}_1(\mathbb{F})$ acts on $\mathbb{F}$ by $x \mapsto ax + b$ and it is easily shown that $|\mathrm{Aff}_1(\mathbb{F})| = q(q-1)$.

1.2.1 *Generators and relations for finite groups*

Let $g_1, \ldots, g_k$ be nontrivial elements of the finite group G. Let $\langle g_1, \ldots, g_k \rangle$ be the subset of G consisting of all finite products of the g_i. Since G is finite, every $g \in G$ has finite order. Thus if g has order d, g has inverse g^{d-1}. Hence $\langle g_1, \ldots, g_k \rangle$ is a subgroup of G. We say G is *generated* by $g_1, \ldots, g_k$ if $G = \langle g_1, \ldots, g_k \rangle$. A finite group G may be specified by a (minimal) set $g_1, \ldots, g_k$ of generators together with a set of monomial *relations* $R_j(g_1, \ldots, g_k) = e$, $j = 1, \ldots, \ell$. The set of relations includes the order relations $g_i^{d_i} = e$, $i = 1, \ldots, k$, as well as relations between generators. A homomorphism $h : G \to J$ is determined by the set of values $h(g_1), \ldots, h(g_k)$ and is well-defined provided that $R_j(h(g_1), \ldots, h(g_k)) = e$, $j = 1, \ldots, \ell$.

Remark 1.2.3 If G is infinite, we define $\langle g_1, \ldots, g_k \rangle$ to be the subgroup of G generated by all products of g_i and g_i^{-1}. We caution the reader that later, when we come to define topological groups, we use the notation $\langle g_1, \ldots, g_k \rangle$ to denote the *closure* (in G) of the subgroup generated by $g_1, \ldots, g_k$.

Example 1.2.2 (1) The cyclic group $\mathbb{Z}_n \subset \mathrm{SO}(2)$ of order n can be generated by one element (for example, rotation through $2\pi/n$); the dihedral group $\mathbf{D}_n \subset \mathrm{O}(2)$, $n \geq 2$, can be generated by two elements, at least one of which must reverse orientation. For example, if α corresponds to reflection in the x-axis and β to rotation through $2\pi/n$, then $\mathbf{D}_n = \langle \alpha, \beta \rangle$ and the defining relations are $\alpha^2 = \beta^n = e$, $(\alpha\beta)^2 = e$ (see also Chapter 2).
(2) Let $\mathbb{F} = \mathbb{F}_{p^n}$, where $p \geq 3$ is prime. Then $\mathrm{Aff}_1(\mathbb{F})$ may be represented as a subgroup of S_{p^n} of order $p^n(p^n - 1)$ [160, Chapter 10].
(3) The projective group $\mathrm{PGL}(2, p^n) = \mathrm{PGL}_2(\mathbb{F}_{p^n})$ may be represented as a subgroup of S_{p^n+1}. This follows by noting that the associated projective space $P^1(\mathbb{F})$ is identified with $\mathbb{F} \cup \{\infty\}$ (for details see [160, 10.6.7–8]).

1.3 Constructions

Definition 1.3.1 Let G, K be groups. The *direct product* of groups G and K is the group $G \times K$ with composition defined by

$$(g_1, k_1)(g_2, k_2) = (g_1 g_2, k_1 k_2), \quad (g_1, g_2 \in G, k_1, k_1 \in K).$$

Example 1.3.1 Let $\mathbb{T}^n$ denote the n-fold direct product of $\mathrm{SO}(2)$. Then $\mathbb{T}^n$ is an Abelian group — the n-torus (see example 1.2.1(1)).

Definition 1.3.2 Let H, J be subgroups of G such that $H \lhd G$. The group G is the *semidirect product* of H and J if $G = HJ$ and $H \cap J = \{e\}$. We write $G = H \rtimes J$ (or $J \ltimes H$).

Remark 1.3.1 (1) If $G = H \rtimes J$ then every $g \in G$ can be written uniquely as $g = hj$, $h \in H$, $j \in J$.
(2) If G is the semidirect product of H and J, we say G *splits* over H. If $G = H \rtimes J$, then $G/H \cong J$ and the exact sequence

$$e \to H \to G \xrightarrow{q} G/H \to e$$

splits (that is, there is an isomorphism $\sigma : G/H \to J \subset G$ such that $qj = e_{G/H}$).

Example 1.3.2 (1) Let $\kappa \in \mathrm{O}(2)$ reverse orientation. Then $\kappa^2 = e$ (κ is an *involution*). Since $\mathrm{SO}(2) \lhd \mathrm{O}(2)$, $\mathrm{O}(2) = \mathrm{SO}(2) \rtimes \mathbb{Z}_2$, where $\mathbb{Z}_2 = \langle \kappa \rangle$. The product is *not* direct. Similarly $\mathrm{O}(n) = \mathrm{SO}(n) \rtimes \mathbb{Z}_2$, where $\mathbb{Z}_2$ is a

subgroup of $\mathrm{O}(n)$ generated by any orientation reversing involution. If n is odd, $\mathrm{O}(n) \approx \mathrm{SO}(n) \times \mathbb{Z}_2$ (take $\kappa = -I$).
(2) For $n \geq 2$, $\mathbf{D}_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$, where $\mathbb{Z}_2$ is generated by an orientation reversing element of $\mathbf{D}_n$.
(3) The Euclidean group $\mathbf{E}(n)$ consists of all pairs $(A, b) \in \mathrm{O}(n) \times T(n)$. We define group composition by

$$(A, b)(C, d) = (AC, Ad + b).$$

This is compatible with the transformation group action of $\mathbf{E}(n)$ on $\mathbb{R}^n$ defined by $(A, b)x = Ax + b$. The group $T(n) = \{(I, b) \mid b \in \mathbb{R}^n\}$ is a normal subgroup of $\mathbf{E}(n)$ and consequently $\mathbf{E}(n) = T(n) \rtimes \mathrm{O}(n) \cong \mathbb{R}^n \times \mathrm{O}(n)$. A similar result holds for $\mathbf{SE}(n)$ with $\mathrm{SO}(n)$ replacing $\mathrm{O}(n)$.
(4) Let $q = p^n$, p prime. The group $\mathrm{Aff}_1(\mathbb{F}_q)$ (example 1.2.2(2)) is the semidirect product $\mathbb{Z}_q \rtimes \mathbb{Z}_{q-1}$, where $\mathbb{Z}_q \lhd \mathrm{Aff}_1(\mathbb{F}_q)$ is the group of translations $x \mapsto x + b$ and $\mathbb{Z}_{q-1} \approx \mathrm{GL}(\mathbb{F}_q) = \mathbb{F}_q^\star$.

The semidirect product may be defined as a product between groups — that is, without assuming the groups are subgroups of a given group. Specifically, suppose that H, J are groups and $\rho : J \to \mathrm{Aut}(H)$ is a homomorphism ($\mathrm{Aut}(H)$ is the group of automorphisms of H). Define a group operation on $H \times J$ by

$$(h, j)(h', j') = (h\rho(j)(h'), jj'), \quad (h, h' \in H, j, j' \in J).$$

With this group operation, we denote the product by $H \times_\rho J$ and refer to $H \times_\rho J$ as the *semidirect product of* H *and* J *with respect to* ρ. We can identify H and J with the subgroups $\{(h, e_J) \mid h \in H\}$ and $\{(e_H, j) \mid j \in J\}$ respectively. With these identifications, $H \times_\rho J = H \rtimes J$.

Example 1.3.3 (1) Let $H = \mathbb{R}^n$, $J = \mathrm{O}(n)$ and define $\rho : \mathrm{O}(n) \to \mathrm{Aut}(\mathbb{R}^n)$ by $\rho(A)(b) = Ab$. We have $\mathbb{R}^n \times_\rho \mathrm{O}(n) = \mathbf{E}(n)$. If instead we take $\rho(A) = I_{\mathbb{R}^n}$, we obtain the direct product.
(2) Suppose $H = \mathrm{SO}(2)$ and $J = \mathbb{Z}_2$. The automorphism group of $\mathrm{SO}(2)$ consists of the identity and the involution $r(\theta) = -\theta$, $\theta \in \mathrm{SO}(2)$. If $J = \langle \kappa \rangle$, define $\rho : J \to \mathrm{Aut}(\mathrm{SO}(2))$ by $\rho(\kappa) = r$. We have $\mathrm{SO}(2) \times_\rho \mathbb{Z}_2 \approx \mathrm{O}(2)$.
(3) Suppose $G = H \rtimes J$ and define $\rho : J \to \mathrm{Aut}(H)$ by $\rho(j)(h) = hjh^{-1}$. Then $H \rtimes J \cong H \times_\rho J$. We leave it to the reader to verify that this is consistent with the previous two examples.
(4) Suppose that J is a subgroup of the symmetric group S^n and let H be a group. Define $\rho : J \to \mathrm{Aut}(H^n)$ by $\rho(j)(h_1, \ldots, h_n) = (h_{j^{-1}(1)}, \ldots, h_{j^{-1}(n)})$, $(h_1, \ldots, h_n) \in H^n$. The *wreath product* $H \wr J$ of

H and J is the semidirect product $H \times_\rho J$. Let H_n denote the group of $n \times n$ *signed permutation matrices*. Each element of P_n is an $n \times n$ permutation matrix where we allow the non-zero entries to be ± 1. If we let Δ_n denote the group of all $n \times n$ diagonal matrices, entries ± 1, then $H_n = \Delta_n \rtimes S_n \approx \mathbb{Z}_2 \wr S_n$.

1.4 Topological groups

Definition 1.4.1 A group G has the structure of a *topological group* if G is a Hausdorff topological space and the group operations of multiplication and inversion are continuous with respect to the given topology.

Remark 1.4.1 So as to avoid all topological issues, we generally assume that the topology of a topological group has countable base (satisfies the second Axiom of countability). In particular, the group will be compact if and only if it is sequentially compact.

Example 1.4.1 (1) Every group may be given the structure of a topological group by taking the discrete topology on G. However, this is not a particularly interesting topology and plays no role in what follows. The discrete topology is the only Hausdorff topology on finite groups.
(2) Euclidean space $\mathbb{R}^n$ and Hermitian space $\mathbb{C}^n$ have the structure of Abelian topological groups (usual topology, group composition addition).
(3) Let V be a d-dimensional vector space over either $\mathbb{R}$ or $\mathbb{C}$. Then $\mathrm{GL}(V)$ is a topological group. This is easily seen by choosing a basis for V and regarding $\mathrm{GL}(V)$ as the group of $d \times d$ invertible matrices.
(4) The groups $\mathrm{O}(n)$, $\mathrm{SO}(n)$ are compact subgroups of $\mathrm{GL}(n, \mathbb{R})$ and therefore inherit the structure of compact topological groups. Similar statements hold for the unitary and special unitary groups $\mathrm{U}(n)$ and $\mathrm{SU}(n)$.
(5) The groups $\mathbf{E}(n)$ and $\mathbf{SE}(n)$ have the topology induced from the product topology on $\mathrm{O}(n) \times \mathbb{R}^n$. Both groups have the structure of (non-compact) topological groups.

Lemma 1.4.1 *Suppose that G, K are topological groups and that $\rho : G \to K$ is a continuous homomorphism. Then kernel(ρ) is a closed normal subgroup of G. If ρ is proper (inverse images of compact sets are compact), then image(ρ) is a closed subgroup of K.*

Exercise 1.4.1 (1) Show that if the group G is a topological space such that the $(g, h) \mapsto gh^{-1}$ is continuous then G is Hausdorff if and only if $\{e_G\}$ is a closed subset of G.

(2) Show that the connected component G_0 of the identity of a topological group G is an open normal subgroup of G.
(3) Show that if H is a subgroup of a topological group G then the closure $\bar{H}$ of H in G is a closed subgroup of G.
(4)* Find an example of a homomorphism $\rho : \mathrm{SO}(2) \to \mathrm{SO}(2)$ which is not continuous.
(5) Find an example of a continuous homomorphism $\rho : \mathbb{R} \to \mathbb{T}^2$ such that image(ρ) is not a *closed* subgroup of $\mathbb{T}^2$.

Let H be a closed normal subgroup of the topological group G and give G/H the quotient topology (the largest or *finest* topology on G/H making the quotient map $q : G \to G/H$ continuous). It is immediate that the group operations on G/H are continuous relative to the quotient topology.

Lemma 1.4.2 *Let H be a closed normal subgroup of the topological group G. Then G/H has the structure of a topological group. In particular, G/H is Hausdorff.*

Proof. Use exercise 1.4.1(1). □

Example 1.4.2 We conclude this section with an exotic example of a compact Abelian topological group that cannot be represented as a closed subgroup of $\mathrm{GL}(V)$ for any finite dimensional vector space V. Although the group theoretic aspects of this example will not play a role in the sequel, we show later that the group can be represented as a hyperbolic attractor of a smooth diffeomorphism of $\mathbb{R}^3$. Topologically, the group is locally the product of an open interval with a Cantor set.

We start with a general construction. Let G be a compact topological group. Under componentwise multiplication, the countable infinite product

$$G_\infty = \Pi^\infty G = G^{\mathbb{N}} = \{(g_n) \mid g_n \in G, n \geq 0\}$$

has the structure of a compact topological group. If G is Abelian, so is G_∞. Suppose that $\rho : G \to G$ is a continuous surjective homomorphism of G. We are interested in the case when ρ is not 1:1 and ρ has nontrivial kernel. Define

$$\Sigma = \{(g_j) \in G_\infty \mid \rho(g_{j+1}) = g_j, j \geq 0\}.$$

Clearly Σ is a closed subgroup of G_∞. We refer to Σ as the *inverse limit* of $\rho : G \to G$. The homomorphism ρ extends to a continuous group automorphism $\hat{\rho} : \Sigma \to \Sigma$ defined by

$$\hat{\rho}(g_0, g_1, \ldots) = (\rho(g_0), g_0, g_1, \ldots).$$

(The inverse of $\hat{\rho}$ is given by $\hat{\rho}^{-1}(g_0, g_1, \ldots) = (g_1, \ldots)$.) If ρ is an automorphism of G, then $\Sigma \approx G$. If not, Σ is typically much bigger than G.

If $G = \mathrm{SO}(2)$, $p \geq 2$ and ρ is the p-fold covering map $\rho(\theta) = p\theta$, then Σ is the *p-adic solenoid*. We show in Chapter 9 that Σ is topologically the product of an open interval with a Cantor set.

More examples can be manufactured by taking nonsingular matrices $A \in \mathrm{GL}(n, \mathbb{R})$ with integer entries. These maps induce endomorphisms of the torus $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ which will be surjective but not bijective if $\det(A) > 1$. For example, if $n = 2$, take

$$T = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}.$$

Both eigenvalues of T are real and greater than 1. The map T induces a $5 : 1$ covering homomorphism of $\mathbb{T}^2$. Taking the inverse limit, we obtain a compact Abelian subgroup Σ of $\Pi^\infty \mathbb{T}^2$ which may be realized as a 2-dimensional expanding attractor of a smooth diffeomorphism of $\mathbb{R}^5$ (see [187] and Chapter 9).

Exercise 1.4.2 Let $g_1, \ldots, g_n$ be non-identity elements of the topological group G. Let $\langle g_1, \ldots, g_n \rangle$ denote the closure in G of the set of all finite words in $g_1, g_1^{-1}, \ldots, g_n, g_n^{-1}$. We say $g_1, \ldots, g_n$ are a set of (topological) generators for G if $\langle g_1, \ldots, g_n \rangle = G$.

(1) Show that $\langle g_1, \ldots, g_n \rangle$ is a topological subgroup of G.
(2) Show that if G is compact, then $\langle g_1, \ldots, g_n \rangle$ is the closure of the set of all finite words in $g_1, \ldots, g_n$.
(3) Let $\alpha \in [0, 1)$. Show that $\langle \alpha \rangle = \mathrm{SO}(2) = \mathbb{R}/\mathbb{Z}$ if and only if α is irrational.
(4) Show that $\mathrm{SO}(3)$ can be generated by two elements but not one element. Noting Euler's theorem and the classification of closed subgroups of $\mathrm{SO}(3)$, find conditions on a pair $g, h \in \mathrm{SO}(3)$ that imply $\langle g, h \rangle = \mathrm{SO}(3)$.

1.5 Lie groups

In this section we review some basic facts about Lie groups. Our emphasis will be on compact Lie groups and our approach will be similar to that given in the book by Thomas [175, Chapter 7]. Bröcker and Dieck [31] and Kobayashi and Nomizu [104] (for the Lie bracket theory) are good alternate references. Our emphasis will be on the differential rather than the algebraic theory (Lie algebras). A fair slice of what we discuss will be developed further in subsequent chapters.

Definition 1.5.1 A Lie group is a topological group G such that

(1) G has the structure of a smooth differential manifold.
(2) The composition map $G \times G \to G; (g, h) \mapsto gh^{-1}$ is smooth.

Remark 1.5.1 (1) We emphasize that by 'smooth' we always mean C^∞.
(2) It may be shown that every Lie group admits the structure of a real analytic manifold such that the operations of group composition are real analytic maps. This 1952 result follows from theorems of Gleason [80] and Montgomery and Zippin [130] which imply that every connected locally Euclidean topological group is Lie (Hilbert's fifth problem). The result for G compact was proved by von Neumann [135] in 1933 and for Abelian groups by Pontryagin [146] in 1939.

Example 1.5.1 (1) Since the general linear groups $\mathrm{GL}(m, \mathbb{R})$ and $\mathrm{GL}(m, \mathbb{C})$ may be represented as open subsets of $\mathbb{R}^{m^2}$ and $\mathbb{C}^{m^2}$, it is obvious that both groups have the structure of a Lie group. In this case group operations are rational functions of the matrix entries. The orthogonal groups $\mathrm{O}(m)$, $\mathrm{SO}(m) \subset \mathrm{GL}(m, \mathbb{R})$ and the unitary groups $\mathrm{U}(m)$, $\mathrm{SU}(m) \subset \mathrm{GL}(m, \mathbb{C})$ also have the structure of compact Lie groups. This may be shown either directly by using Lie algebras to construct charts or by noting that both groups are closed subgroups of a Lie group and therefore Lie by a result we prove later in the chapter (theorem 1.5.1).
(2) If G is compact but not connected then the identity component G_0 of G is a normal open subgroup of G and G/G_0 is finite.

Exercise 1.5.1 Show that a nonempty open subgroup H of the identity component G_0 of a Lie group is equal to G_0. (Hint: The cosets of H in G_0 are all open and so H must be closed.)

Remark 1.5.2 Using the Peter-Weyl theorem, it may be shown that every compact Lie group is isomorphic to a subgroup of $\mathrm{O}(m)$, for large enough m (for a proof see [31, Chapter III, sections 3,4]). A consequence is that every compact group has the (unique) structure of a real algebraic variety. Indeed, a compact Lie group may be represented as the set of real points of a (complex) algebraic group. If G is *finite*, G may be represented as as subgroup of $\mathrm{O}(m)$, where $m = |G|$ — this follows from Cayley's theorem since G is isomorphic to a subgroup of the symmetric group S_m and $S_m \subset \mathrm{O}(m)$ if regard each element of S_m as a permutation of coordinates in $\mathbb{R}^m$. On the other hand there exist examples of non-compact connected Lie groups which cannot be represented as a subgroup of $\mathrm{GL}(m, \mathbb{R})$ for any $m \in \mathbb{N}$. As an example, we sketch why the universal cover $\mathrm{SL}(2, \mathbb{R})^\star$ of $\mathrm{SL}(2, \mathbb{R})$ cannot be represented as a matrix group. First note that the universal cover $G^\star$ of a Lie group G carries the natural structure of a Lie group for which the covering homomorphism $\pi : G^\star \to G$ is smooth. It is straightforward to show that $\pi_1(\mathrm{SL}(2, \mathbb{R})) = \mathbb{Z}$. Using a complexification argument ($\mathrm{SL}(2, \mathbb{C})$ is simply connected and the inclusion $\mathrm{SL}(2, \mathbb{R}) \hookrightarrow \mathrm{SL}(2, \mathbb{C})$ induces the zero map on π_1), it may be shown that every homomorphism $h : \mathrm{SL}(2, \mathbb{R})^\star \to \mathrm{GL}(m, \mathbb{R})$ factors through $\pi : \mathrm{SL}(2, \mathbb{R})^\star \to \mathrm{SL}(2, \mathbb{R})$. Hence $\mathrm{SL}(2, \mathbb{R})^\star$ cannot be represented as a subgroup of $\mathrm{GL}(m, \mathbb{R})$ for any $m \in \mathbb{N}$. ($\mathrm{SL}(2, \mathbb{R})^\star$ is not a *linear* Lie group.) This example, due to Birkoff, appears in [131, page 191].

Exercise 1.5.2 Show that the universal cover $G^\star$ of a connected Lie group G carries the natural structure of a Lie group for which the covering homomorphism $\pi : G^\star \to G$ is smooth. Show that the kernel of π is a (discrete) normal subgroup of $Z(G^\star)$.

The group G is *semisimple* if G has finite centre and is *simple* if G contains no proper normal subgroups. The classical compact Lie groups $\mathrm{SO}(n)$ (special orthogonal group, $n \geq 3$), $\mathrm{SU}(n)$ (special unitary group, $n \geq 2$), and $\mathrm{Sp}(n)$ (symplectic group, $n \geq 2$), provide examples of compact connected semisimple groups. The quotient of any of these groups by its centre defines a simple group (thus $\mathrm{SO}(2n+1)$ is simple, all $n \geq 1$). The only other compact simple groups are the exceptional simple Lie groups G_2, F_4, E_6, E_7, E_8. If G is simple, the universal cover $G^\star$ is compact semisimple.

If G is any compact connected Lie group, there exist $m \geq 0$, compact simply connected groups $G_1, \ldots, G_p$, with each $G_i/Z(G_i)$ simple, and a finite covering homomorphism

$$\phi : \mathbb{T}^m \times \tilde{G}_1 \times \ldots \times \tilde{G}_p \to G.$$

Up to order, $\mathbb{T}^m$, $G_1, \ldots, G_p$ are uniquely determined by G. (See [31, Chapter V, theorem 8.1].) In case G is Abelian, the proof of this result is elementary and we give it shortly.

Kronecker's theorem implies that there is a dense full measure subset of $\mathcal{G}$ of $\mathbb{T}^m$ consisting of topological generators: if $g \in \mathcal{G}$, then $\langle g \rangle = \mathbb{T}^m$ (for Kronecker's theorem and a simple proof using Fourier series, see [101, page 29]). For general compact connected Lie groups, two generators suffice. If G is a compact connected semisimple Lie group, then there is a (Zariski) open and dense subset of G^2 consisting of pairs which topologically generate G (for a proof of this result, which is due to Ulam, see [65]).

1.5.1 *The Lie bracket of vector fields*

Before we discuss the Lie algebra of a Lie group, we review some facts about the Lie bracket of vector fields (for more details, see [104, Chapter 1] or [175, Chapter 7]).

Let $C^\infty(TM)$ denote the space of smooth vector fields on the manifold M. If $X \in C^\infty(TM)$, let ϕ_t^X denote the flow of X (ϕ_t^X will be defined and smooth on a nonempty open neighbourhood of $M \times \{0\}$ in $M \times \mathbb{R}$).

The space $C^\infty(TM)$ is naturally isomorphic to the space of $\mathbb{R}$-linear derivations[1] of $C^\infty(M)$. Each $X \in C^\infty(TM)$ determines the derivation (or Lie derivative) $L_X : C^\infty(M) \to C^\infty(M)$ by $L_X f = \langle df, X \rangle$. The Lie bracket $[X,Y]$ of $X, Y \in C^\infty(TM)$ is the unique vector field associated to the derivation $L_Y L_X - L_X L_Y$. We recall some basic properties of the Lie bracket which may be proved either directly from the definition or by using local coordinates.

Lemma 1.5.1

(1) $(C^\infty(TM), [\ ,\ ])$ *has the structure of a real Lie algebra. In particular, we have* $[X,Y] = -[Y,X]$ *and Jacobi's identity:* $[X,[Y,Z]] + [Y,[Z,X]] + [Z,[X,Y]] = 0$, $X, Y, Z \in C^\infty(TM)$.

(2) If, in local coordinates, $X = (X_1, \dots, X_m)$, $Y = (Y_1, \dots, Y_m)$, *then* $[X,Y]_i = \sum_j \left(X_j \frac{\partial Y_i}{\partial x_j} - Y_j \frac{\partial X_i}{\partial x_j} \right)$.

(3) If $f : M \to N$ *is a diffeomorphism,* $X \in C^\infty(TM)$ *and we define* $f_\star X = TfX \circ f^{-1} \in C^\infty(TN)$, *then* $f_\star[X,Y] = [f_\star X, f_\star Y]$, *all* $X, Y \in C^\infty(TM)$.

(4) If $X, Y \in C^\infty(TM)$ *have respective flows* ϕ_t^X, ϕ_t^Y, *then*

$$[X,Y] = \frac{d}{dt}(\phi_t^X)_\star Y|_{t=0} = -\frac{d}{dt}(\phi_t^Y)_\star X|_{t=0}.$$

[1] A derivation δ of $C^\infty(M)$ satisfies $\delta(fg) = g\delta(f) + f\delta(g)$, for all $f, g \in C^\infty(M)$.

1.5.2 *The Lie algebra of G*

Every $h \in G$ determines a smooth diffeomorphism $L_h : G \to G$ defined by left translation $L_h(g) = hg$. Similarly, we define right translation $R_h : G \to G$ by $R_h(g) = gh$. Left and right translation commute

$$L_h R_k = R_k L_h, \ \ (h, k \in G).$$

Let $\mathfrak{g} = T_e G$ denote the tangent space to G at the identity.

Let $C^\infty_G(TG)$ denote the space of (smooth) left invariant vector fields on G. That is, $\bar{X} \in C^\infty_G(TG)$ if $\bar{X}(gh) = TL_g\bar{X}(h)$. There is a natural isomorphism $\mathfrak{g} \approx C^\infty_G(TG)$ defined by mapping $X \in \mathfrak{g}$ to the left invariant vector field $\bar{X}$ on G defined by

$$\bar{X}(g) = TL_g X, \ \ (g \in G).$$

Conversely, every left invariant vector field on G is equal to $\bar{X}$ for a unique $X \in \mathfrak{g}$.

Example 1.5.2 The evaluation map $G \times \mathfrak{g} \to TG$, $(g, X) \to \bar{X}(g)$, defines a natural trivialization $TG \approx G \times \mathfrak{g}$ and so G is *parallelizable*. This simple observation lies at the heart of many geometric properties of compact Lie groups. As an example, we shall see later that the exponential map of the Lie algebra of a *compact* Lie group G (to be defined shortly) is *equal* to the exponential map of an invariant Riemannian metric on G (see Chapter 3). We thereby obtain a relationship between the Lie algebraic and differential geometric properties of G.

If $X, Y \in \mathfrak{g}$, then $[\bar{X}, \bar{Y}]$ is left invariant by lemma 1.5.1(3). Hence there exists a unique $Z \in \mathfrak{g}$ such that $[\bar{X}, \bar{Y}] = \bar{Z} = \overline{[X, Y]}$. In this way we may define a Lie algebra structure on $\mathfrak{g}$ by $[X, Y] = Z$. In future we refer to $\mathfrak{g}$ as the *Lie algebra* of G and always assume that $\mathfrak{g}$ is equipped with the Lie bracket $[\ ,\ ]$.

Exercise 1.5.3 Show that the lie algebra $\mathfrak{gl}(m, \mathbb{R})$ of $\mathrm{GL}(m, \mathbb{R})$ is the space of all $m \times m$ matrices and that the Lie algebra structure on $\mathfrak{gl}(m, \mathbb{R})$ is defined by $[A, B] = AB - BA$.

Lemma 1.5.2 *Let $K : G \to H$ be a smooth homomorphism of Lie groups. Then $K_\star = T_e K : \mathfrak{g} \to \mathfrak{h}$ is a homomorphism of Lie algebras ($K_\star[X, Y] = [K_\star X, K_\star Y]$, for all $X, Y \in \mathfrak{h}$).*

Proof. We have $K\phi^X_t = \phi^{K_\star X}_t$, $X \in \mathfrak{g}$. Now use lemma 1.5.1(4). □

1.5.3 *The exponential map of* $\mathfrak{g}$

We start by establishing properties of the flow ϕ^X of $\bar{X}$, $X \in \mathfrak{g}$. Given $g, h \in G$, the left invariance of $\bar{X}$ implies that $g\phi_t^X(h)$ is the integral curve of $\bar{X}$ through gh and so

$$\phi_t^X g = g\phi_t^X, \text{ for all } g \in G. \tag{1.1}$$

(This is a general property of the flow of a 'G-equivariant' vector field — see Chapter 2).

Lemma 1.5.3 *Let* $X \in \mathfrak{g}$.

(1) The domain of ϕ^X *is (all of)* $G \times \mathbb{R}$.
(2) The map $\mathbb{R} \to G$, $t \mapsto \phi_t^X(e)$ *is a (smooth) group homomorphism. (*$\{\phi_t^X \mid t \in \mathbb{R}\}$ *is a 1-parameter group of diffeomorphisms of* G*.)*
(3) For all $t, s \in \mathbb{R}$, $X \in \mathfrak{g}$, $\phi_t^{sX} = \phi_{st}^X$.

Proof. Let $\gamma = \phi_e^X : (a,b) \to G$ denote the maximal integral curve of $\bar{X}$ through e. Since, by left invariance, $g\gamma : (a,b) \to G$ is an integral curve through g, we see easily that $g\gamma : (a,b) \to G$ is the maximal integral curve through g for all $g \in G$. Hence the domain of ϕ^X is $G \times (a,b)$. For all $t, s \in (a,b)$ we have

$$\gamma(s)\gamma(t) = \phi_s^X(e)\phi_t^X(e) = \phi_t^X(\phi_s^X(e)),$$

where the second equality uses (1.1). Since $\phi_t^X(\phi_s^X(e))$ is an integral curve through $\phi_s^X(e) = \gamma(s)$, uniqueness of integral curves implies that $t + s \in (a,b)$ for all $t, s \in (a,b)$. Hence $(a,b) = \mathbb{R}$, proving (1). Since $\gamma(t+s) = \phi_{s+t}^X(e) = \phi_s^X(\phi_t^X(e)) = \gamma(t)\gamma(s)$, $\gamma : \mathbb{R} \to G$ is a group homomorphism, proving (2). For the final statement, rescale time ($\gamma(t)$ is a trajectory of X if and only if $\gamma(st)$ is a trajectory of sX). □

Exercise 1.5.4 Show that the set of all smooth group homomorphisms $c : \mathbb{R} \to G$ is naturally isomorphic to $\mathfrak{g}$ (we can replace 'smooth' by 'continuous' in this result).

We define the *exponential map* $\exp_G = \exp : \mathfrak{g} \to G$ by $\exp(X) = \phi_1^X(e)$.

Lemma 1.5.4

(1) $\exp : \mathfrak{g} \to G$ *is smooth.*
(2) $T_e \exp : \mathfrak{g} \to \mathfrak{g}$ *is the identity map.*
(3) $\exp$ *restricts to a diffeomorphism of an open neighbourhood of the origin in* $\mathfrak{g}$ *onto an open neighbourhood of the identity in* G.

(4) exp *is* natural *in the sense that if* $K : G \to H$ *is a (smooth) homomorphism of Lie groups then*

$$K \exp_G = \exp_H K_\star,$$

where $K_\star = T_e K : \mathfrak{g} \to \mathfrak{h}$.

(5) If $X \in \mathfrak{g}$ *and* ϕ_t^X *denotes the flow of* $\bar{X}$, *then* $\phi_t^X(g) = g \exp(tX)$, *all* $g \in G$.

Proof. Statement (1) is a consequence of standard results on the smooth dependence of solutions of ordinary differential equations on a parameter. For (2), note that by lemma 1.5.3(3) we have

$$D\exp(0)(X) = \frac{d}{dt}\exp(tX)|_{t=0} = \frac{d}{dt}\phi_t^X(e) = X,$$

and so $D\exp(0) = I_{\mathfrak{g}}$. Applying the implicit function theorem, exp is a local diffeomorphism at $0 \in \mathfrak{g}$. The naturality of exp follows from $K\phi_t^X(e_G) = \phi_t^Y(e_H)$, where $Y = K_\star(X)$. The final statement is a consequence of lemma 1.5.3(3) and (1.1). □

Example 1.5.3 If G is a Lie subgroup of $\mathrm{GL}(m, \mathbb{R})$ and $X \in \mathfrak{g}$ then $\exp X = \sum_{n=0}^{\infty} \frac{X^n}{n!}$.

Lemma 1.5.5 *If* G *is connected then* $\exp : \mathfrak{g} \to G$ *is a homomorphism with respect to the additive structure on* $\mathfrak{g}$ *if and only if* G *is Abelian.*

Proof. If G is Abelian the composition map $c : G \times G \to G$, $c(g, k) = gk$, is a homomorphism and $T_{(e,e)}c(X, Y) = X + Y$. So, by lemma 1.5.4(4), $\exp(X + Y) = \exp(X)\exp(Y)$. We leave the converse to the reader (use lemma 1.5.4(3) together with exercise 1.5.1). □

Proposition 1.5.1 *A compact connected Abelian Lie group is isomorphic to a torus.*

Proof. Let G be a connected compact Abelian group. By lemma 1.5.5, $\exp : \mathfrak{g} \to G$ is a homomorphism. The homomorphism is surjective since the image of the exponential map generates G (lemma 1.5.4(3) and exercise 1.5.1). Since exp is a local diffeomorphism at $0 \in \mathfrak{g}$, the kernel Γ of exp is a discrete subgroup Γ of $\mathfrak{g} \cong \mathbb{R}^n$, $n = \dim(G)$. One may show (see exercise 1.5.5(3)) that there exist linearly independent vectors $g_1, \ldots, g_p \in \mathfrak{g}$ generating Γ. If $p = n$, then $\mathfrak{g}/\Gamma \cong \mathbb{T}^n$ and we are done. Otherwise, complete to a basis $g_1, \ldots, g_n$ of $\mathfrak{g}$, and observe that $\mathfrak{g}/\Gamma \cong \mathbb{T}^p \times \mathbb{R}^{n-p}$ which cannot be compact unless $p = n$. □

Exercise 1.5.5 (1) Regard $\mathrm{SO}(n)$ as a subgroup of $\mathrm{GL}(n, \mathbb{R})$. Verify that $\mathrm{SO}(n)$ is a Lie subgroup of $\mathrm{GL}(n, \mathbb{R})$ and that the Lie algebra $\mathfrak{so}(n) \subset \mathfrak{gl}(n, \mathbb{R})$ of $\mathrm{SO}(n)$ may be identified with the space of $n \times n$ skew symmetric matrices. (Hint: Let $A \in \mathfrak{gl}(n, \mathbb{R})$ be skew symmetric: $A + A^t = 0$. Show that $\exp(A) \in \mathrm{SO}(n)$. Now use the fact that $\dim(\mathrm{SO}(n)) = n(n-1)/2$ together with the fact that exp is a local diffeomorphism to construct a chart for $\mathrm{SO}(n)$ at the identity. Translate by group elements to get a differential atlas.)
(2) Let X be a non-zero element of the lie algebra of G. Show that $\Gamma_X = \{\exp(tX) \mid t \in \mathbb{R}\}$ is an Abelian subgroup of G. Find (up to isomorphism) Γ_X in case $G = \mathrm{SO}(3)$. Show that for 'most' $X \in \mathfrak{so}(4)$, the closure of Γ_X is isomorphic to $\mathbb{T}^2$. Find the corresponding results for $\mathrm{SO}(2n)$ and $\mathrm{SO}(2n+1)$. (These examples are special cases of the fundamental theorem that every compact connected Lie group has a *maximal torus* $\mathbb{T}^m$ and that the set of conjugates $g\mathbb{T}^m g^{-1}$ fills out G. There are also results for compact disconnected Lie groups [31, Chapter IV, section 4] and we return to these questions in Chapter 8.)
(3) Suppose that Γ is a discrete subgroup of $\mathbb{R}^n$. Complete the proof of proposition 1.5.1 by showing that there exists a linearly independent set $g_1, \ldots, g_p \in \Gamma$ which generates Γ. (Hints: Prove by induction on n. Assume true for $n-1$. Choose $g_1 \in \Gamma \setminus \{0\}$ to be of shortest length. Write $\mathbb{R}^n = \mathbb{R}g_1 \oplus V$, where $V = (\mathbb{R}g_1)^{\perp}$. If $\pi : \mathbb{R}^n \to V$ denotes orthogonal projection, prove $\pi(\Gamma)$ is discrete by showing that every non-zero element of $\pi(\Gamma)$ has length at least $\|g_1\|/2$. Now apply the inductive hypothesis to $\pi(\Gamma)$ and thereby find a linearly independent subset of Γ which projects by π onto a basis of $\pi(\Gamma)$ and extends by g_1 to a basis of Γ.)
(4) Define $f : \mathfrak{g}^2 \to G$ by $f(X, Y) = \exp(X+Y)\exp(-X)\exp(-Y)$. Show $Tf_{(0,0)} = 0$ and, in particular, that $\exp(X+Y)\exp(-Y)\exp(-X) = e_G + o(\|(X, Y)\|)$, relative to any norm $\| \;\|$ on $\mathfrak{g}^2$.
(5) Show that every connected Abelian Lie group G is isomorphic to $\mathbb{T}^p \times \mathbb{R}^q$, where $p + q = \dim(G)$.
(6) Show that the Lie algebra $\mathfrak{sl}(n, \mathbb{R})$ of $\mathrm{SL}(n, \mathbb{R})$ is the space of $n \times n$-matrices with trace zero.
(7) Show that even if G is connected, the exponential map $\exp : \mathfrak{g} \to G$ need not be onto. (Hint: Take $G = \mathrm{SL}(2, \mathbb{R})$ and show that the diagonal matrix (λ, λ^{-1}) cannot be represented as e^A, $\mathrm{trace}(A) = 0$, if $\lambda < 0$ and $\lambda \neq -1$.)

1.5.4 *Additional properties of brackets and* exp

In this subsection we give some details on the relationship between the adjoint representation of $\mathfrak{g}$ and the action of $\mathfrak{g}$ on G via the exponential map. While we make rather limited use of these results in the remainder of the book, we include them as they provide a useful guide to computations that relate the bracket structure to the group operations on G.

Given $X \in \mathfrak{g}$, let $c(X) \in \mathrm{Aut}(G)$ be defined by $c(X)(g) = \exp(X) g \exp(-X)$. Let $c_\star(X) = T_e c(X) : \mathfrak{g} \to \mathfrak{g}$ and note that $c_\star(X)$ is a Lie algebra homomorphism (lemma 1.5.2).

Lemma 1.5.6 *For all* $X, Y \in \mathfrak{g}$,

$$[X, Y] = \frac{d}{dt} c_\star(tX) Y|_{t=0}.$$

Proof. By lemma 1.5.1(4), $[\bar{X}, \bar{Y}] = \frac{d}{dt}(\phi_t^X)_\star \bar{Y}|_{t=0}$. Since $\phi_t^X(g) = g \exp(tX)$, we have

$$(\phi_t^X)_\star \bar{Y}(e) = T\exp(tX)\bar{Y}(\exp(-tX))(e) = c_\star(tX)\bar{Y}(e).$$

Hence $[X, Y] = [\bar{X}, \bar{Y}](e) = \frac{d}{dt} c_\star(tX) Y|_{t=0}$. □

The *adjoint Lie algebra representation* of $\mathfrak{g}$ is the map $\mathrm{ad} : \mathfrak{g} \to L(\mathfrak{g}, \mathfrak{g})$ defined by

$$\mathrm{ad}(X)(Y) = [X, Y], \ \ (X, Y \in \mathfrak{g}).$$

Exercise 1.5.6 Using the Jacobi identity, show that ad is a Lie algebra homomorphism: $[\mathrm{ad}(A), \mathrm{ad}(B)] = \mathrm{ad}([X, Y])$ (the bracket on $L(\mathfrak{g}, \mathfrak{g})$ is the commutator).

Given $A \in L(\mathfrak{g}, \mathfrak{g})$, we define $e^A = \sum_{j=0}^{\infty} A^j / j! \in \mathrm{GL}(\mathfrak{g}) \subset L(\mathfrak{g}, \mathfrak{g})$.

Lemma 1.5.7 *For* $X, Y \in \mathfrak{g}$, $c_\star(X) Y = e^{ad(X)} Y$.

Proof. Define the smooth curve $X(t)$ in $\mathfrak{g}$ by $X(t) = c_\star(tX)Y$. Then $X(0) = Y$ and $X(s+t) = c_\star(sX)c_\star(tX)Y$, since $c(tX + sX) = c(sX)c(tX)$. Differentiating with respect to s and setting $s = 0$ it follows from lemma 1.5.6 that

$$X'(t) = [X, X(t)] = \mathrm{ad}(X)(X(t)).$$

The solution of this ordinary differential equation with $X(0) = Y$ is given by $X(t) = e^{t\mathrm{ad}(X)} Y$. Taking $t = 1$, the result follows. □

Lemma 1.5.8 *Let $X(t)$ be a smooth curve in $\mathfrak{g}$. Then*

$$T\exp(X(t))\frac{d}{dt}\exp(-X(t)) = -f(ad(X(t))X'(t),$$

where $f(z) = (e^z - 1)/z$.

Proof. For $s, t \in \mathbb{R}$, define $B(s,t) \in \mathfrak{g}$ by

$$B(s,t) = T\exp(sX(t))\frac{d}{dt}\exp(-sX(t)).$$

Differentiating with respect to s, we find after some work that

$$\frac{\partial B}{\partial s} = [X, B] - X'(t).$$

The solution to this inhomogeneous linear equation in s is given by

$$B(s,t) = e^{s\mathrm{ad}(X)}\left(B(0,t) + \int_0^s e^{-u\mathrm{ad}(X)}X'(t)\,du\right).$$

Setting $s = 1$, and noting that $B(0,t) = 0$, the result follows. $\square$

Remark 1.5.3 Choose an open neighbourhood U of $0 \in \mathfrak{g}$ so that exp restricts to a diffeomorphism of U onto an open neighbourhood V of $e_G \in G$. Let $\log = (\exp|U)^{-1}$. Lemma 1.5.8 is the key step towards proving the Cambell-Baker-Hausdorff formula which gives an explicit formula for $\log(\exp(X)\exp(Y))$ in terms of the Lie algebra structure on $\mathfrak{g}$:

$$\log(\exp(X)\exp(Y)) = X + \int_0^1 \Psi(e^{\mathrm{ad}(X)}e^{t\mathrm{ad}(Y)})(Y)\,dt,$$

where $\Psi(z) = \log z/(z-1)$ and is analytic near $z = 1$. Using this result one may derive a power series expansion for $\log(\exp(X)\exp(Y))$ in terms of Lie bracket operations:

$$\log(\exp(X)\exp(Y)) = X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}([X,[X,Y]] - [Y,[Y,X]]) + \ldots.$$

The Cambell-Baker-Hausdorff formula implies that the group multiplication of G is determined uniquely by the Lie algebra structure on $\mathfrak{g}$. From this it can be shown fairly easily that every linear Lie algebra (that is, Lie subalgebra of the space of $n \times n$-matrices) is the linear algebra of a Lie group (the group will not be unique).

Exercise 1.5.7 Suppose the neighbourhoods U, V are chosen as in the previous remark. Let $C(t) = \log e^{tA}e^B$, where $A, B \in U$ are chosen sufficiently small so that $e^{tA}e^B \in V$, $|t| < 1$. Show that $e^{C(t)}\frac{d}{dt}e^{-C(t)} = -A$ and hence $A = f(\mathrm{ad}(C)(t))C'(t)$ (lemma 1.5.8). Now use the fact that $f(\log z)\Psi(z) = 1$ to find a differential equation for C and deduce the Cambell-Baker-Hausdorff formula.

1.5.5 *Closed subgroups of a Lie group*

Theorem 1.5.1 *If H be a closed subgroup of the Lie group G, then H is a Lie subgroup of G (that is, H is a closed submanifold of G).*

Proof. It suffices to find an open neighbourhood D' of $e \in G$ such that $H \cap D'$ is a submanifold of G since we can translate charts for $H \cap D'$ by elements of H to obtain a differential atlas of H. The proof proceeds by constructing the Lie algebra $\mathfrak{h}$ of H (strictly H_0) and using the exponential map restricted to $\mathfrak{h}$ to construct a chart with domain D'.

Choose an open neighbourhood U of $0 \in \mathfrak{g}$ such that exp restricts to a diffeomorphism of U onto an open neighbourhood D of $e \in G$. Let $\log : D \to U$ denote the inverse map.

Fix a norm $\| \ \|$ on $\mathfrak{g}$. Set $U' = \log(H \cap D)$. If $(v_n) \subset U' \setminus \{0\}$ is a sequence converging to 0, choose a subsequence so that $v_n/\|v_n\|$ converges to $X \in \mathfrak{g}$, $\|X\| = 1$. We claim $\exp(tX) \in H$, all $t \in \mathbb{R}$. To this end, fix $t \neq 0$. Let m_n denote the integer part of $t/\|v_n\|$. Then $\lim_{n\to\infty} m_n\|v_n\| = t$ and so $\lim_{n\to\infty} m_n v_n = tX$. Hence $\lim_{n\to\infty} \exp(m_n v_n) = \exp(tX)$. But $\exp(m_n v_n) = \exp(v_n)^{m_n} \in H$ and so, since H is closed, $\exp(tX) \in H$.

Let $L = \{tX \mid X = \lim(v_n/\|v_n\|),\ (v_n) \subset U', t \in \mathbb{R}\}$. We claim L is a linear subspace of $\mathfrak{g}$. Since L is closed under scalar multiplication, we must show L is closed under addition. Suppose $X, Y \in L$. We have $\exp(X/n)\exp(Y/n) \in H$ for all $n \in \mathbb{N}$ and so $h_n = \log(\exp(X/n)\exp(Y/n)) \in U'$, for all sufficiently large n. By exercise 1.5.5(4), $\exp(X/n)\exp(Y/n) = \exp((X+Y)/n + O(1/n))$ and so $h_n = (X+Y)/n + O(1/n)$. Hence $\lim_{n\to\infty} h_n/\|h_n\| = (X+Y)/\|X+Y\|$ and $X + Y \in L$.

Let L' be an open neighbourhood of the origin in L. We claim that $\exp(L')$ is a neighbourhood of the identity in H. Certainly $\exp(L') \subset \exp(L) \subset H$. Let E be a vector space complement to L in $\mathfrak{g}$ and define $f : L \oplus E \to G$ by $f(X, Y) = \exp(X)\exp(Y)$. Since $T_{(0,0)}f(A, B) = A + B$, $(A, B) \in L \oplus E$, f is a local diffeomorphism at the origin of $\mathfrak{g}$. Suppose that every neighbourhood of $e \in G$ contains points of H not in $\exp(L')$. We may choose a sequence (X_n, Y_n) of points in $L' \oplus E$ such that $(X_n, Y_n) \to 0$, $Y_n \neq 0$, and $f(X_n, Y_n) \in H$. Choosing a subsequence, we may suppose that $Y_n/\|Y_n\| \to Y$, $\|Y\| = 1$. Since $\exp(X_n) \in H$ and H is a subgroup, we have $\exp(Y_n) \in H$ and so $Y \in L$, a contradiction. Since $\exp|L$ is a local diffeomorphism at the origin, we may choose L' so that exp maps L' diffeomorphically onto an open neighbourhood D' of $e \in H$. □

1.6 Haar measure

We conclude the chapter by recalling the simple proof of the existence of *Haar measure* for a compact Lie group.

Theorem 1.6.1 *Let G be a compact Lie group. There exists a unique Borel probability measure on G which is invariant under both left and right translations.*

Proof. We prove existence and leave uniqueness to the reader. Suppose that $\dim(G) = m$. Let $\tau_G^\star : T^\star G \to G$ denote the cotangent bundle of G (bundle of 1-forms). Then $\wedge^m T^\star G \to G$ is a line bundle over G. The fibre of $\wedge^m T^\star G \to G$ over the identity $e \in G$ is precisely $\wedge^m \mathfrak{g}^\star$. Let $\phi \in \wedge^m \mathfrak{g}^\star$ be non-zero. We define the smooth left invariant section ω of $\wedge^m T^\star G$ by

$$\omega(g) = (\wedge^m TL^\star_{g^{-1}})(\phi), \quad (g \in G).$$

Since ω is non-vanishing it defines a volume form on G. Multiplying ϕ by a non-zero constant we may assume that $\int_G \omega = 1$. Since ω is left invariant, the associated Borel probability measure dh on G is left invariant. To prove right invariance of dh, it suffices to show ω is right invariant. Let $k \in G$ and set $\bar{\omega} = R_k^\star \omega$. Since $\wedge^m \mathfrak{g}^\star$ is 1-dimensional, there exists $a \in \mathbb{R}$ such that $\omega(e) = a\bar{\omega}(e)$. Since left and right multiplication commute and ω is left invariant, $\bar{\omega}$ is left invariant and so $\omega(g) = a\bar{\omega}(g)$, for all $g \in G$. Certainly $\int_G \bar{\omega} = a \int_G \omega$. On the other hand, it follows from standard properties of the integral of m-forms that $\int_G \bar{\omega} = \int_G R_k^\star \omega = \int_G \omega$. Hence $a = 1$ and ω is right invariant. □

Remark 1.6.1 (1) If G is finite, then $dh = \frac{1}{|G|} \sum_{g \in G} \delta(g)$, where $\delta(g)$ is the Dirac probability measure supported at g.
(2) If G is a compact topological group then G admits a unique left and right invariant probability measure. If we allow G to be non-compact then it can be shown that there exist both left and right invariant Borel measures

on G but not necessarily a measure which is left and right invariant. Proofs can be found in any text on topological groups (an elementary proof for compact topological groups is in [175, Appendix A]).