Lie groups in quantum information

Session 3: Simple Lie groups and simple Lie algebras

Andrew Zhao

June 26, 2019

1 Simple groups

We begin with the definition of normal subgroups (sometimes also referred to as *invariant* subgroups). Given a particular group, these are the subgroups (recall: subsets closed with respect to the group operation) which are invariant to conjugation by any element of the full group.

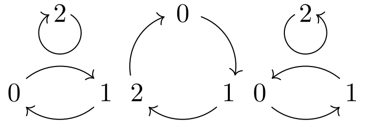
Definition 1.1. Let G be a group and $N \subseteq G$ a subgroup. We call N a **normal subgroup** of G if, $\forall n \in N$ and $\forall g \in G$, $gng^{-1} \in N$. (This relation is often denoted $N \lhd G$.)

Example 1.1. Consider the symmetric group $S_3 \coloneqq \{\mathbf{1}, (01), (02), (12), (012), (021)\}$. Its normal subgroups are S_3, $\{\mathbf{1}\}$, and $\{\mathbf{1}, (012), (021)\}$.

Proof. Since groups are closed by definition, the entire group is always a normal subgroup of itself. The subgroup containing only the identity element is also always normal, since $g\mathbf{1}g^{-1} = gg^{-1} = \mathbf{1} \in \{\mathbf{1}\}$.

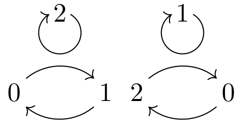
The only nontrivial normal subgroup of S_3 is $N = \{e, (012), (021)\}$, which can be checked explicitly by calculating gng^{-1} for all $g \in S_3$ and $n \in N$. As an example, for $n = (012)$, we have:

$(01)(012)(01)^{-1} =$

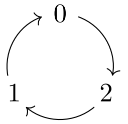


(1)

$=$

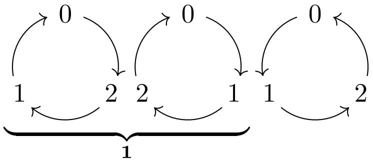


$=$



$= (021) \in N,$

$(021)(012)(021)^{-1} =$



(2)

$= (012) \in N.$

The remaining calculations follow similarly. □

Not all groups have nontrivial normal subgroups. Those which do not are said to be simple.

Definition 1.2. A group G is called a **simple group** if its only normal subgroups are trivial (G and $\{\mathbf{1}\}$).

It turns out that, if a group G is *not* simple, then it can be decomposed into a nontrivial normal subgroup N and the corresponding quotient group, G/N (described below). Simple groups thus cannot be broken down in this way, and so serve as the foundation for a classification scheme.

2 Quotient groups

Here we formalize this notion of quotient groups. These are constructed by taking a group, identifying an equivalence relation on it via its group operation, and "modding out" this relation by identifying all equivalent elements as the same element in this new quotient group.

Definition 2.1. An **equivalence relation** $\sim$ on a set X is a binary relation satisfying, $\forall x, y, z \in X$,

$$x \sim x, \tag{3a}$$

$$x \sim y \implies y \sim x, \tag{3b}$$

$$x \sim y \text{ and } y \sim z \implies x \sim z. \tag{3c}$$

An **equivalence class** $[x]$ of $x \in X$ is a subset $[x] \subseteq X$ defined by all the elements in X which are equivalent to x:

$$[x] \coloneqq \{y \in X \mid y \sim x\}. \tag{4}$$

Remark 2.1. Note that distinct equivalence classes are disjoint. Thus taking the set of all equivalence classes has the effect of "binning" the original set into elements which are agnostic to the equivalence relation. This new set is sometimes generically called a quotient set, written

$$X/\sim \coloneqq \{[x] \mid x \in X\}. \tag{5}$$

To construct the quotient *group*, we want to perform this binning procedure with respect to a particular equivalence relation which takes advantage of the group structure.

Lemma 2.1. *Let G be a group and $H \subseteq G$ a subgroup. Define, for all $g, h \in G$,*

$$g \sim_H h \text{ if } h^{-1}g \in H. \tag{6}$$

Then $\sim_H$ is an equivalence relation on G, and we have equivalence classes, for each $g \in G$,

$$\begin{aligned} gH &\coloneqq \{h \in G \mid h \sim_H g\} \\ &= \{gh \mid h \in H\}. \end{aligned} \tag{7}$$

Proof. To show that $\sim_H$ is an equivalence relation, we check the 3 properties:

1. $g \sim_H g$ always holds, since $g^{-1}g = \mathbf{1} \in H$.
2. If $g \sim_H h$, then $h^{-1}g \in H$, but also its inverse $(h^{-1}g)^{-1} = g^{-1}h \in H$. So $h \sim_H g$.
3. Let $g \sim_H h$ and $h \sim_H f$ $\forall f \in G$. Then $h^{-1}g, f^{-1}h \in H$, and so is their product $f^{-1}hh^{-1}g = f^{-1}g \in H$. Thus $g \sim_H f$.

Next we show that the equivalence classes can be understood as in Eq. (7). Define $f \coloneqq g^{-1}h$. Then, within gH, we have $h = gf$ with $f \in H$, and so the set is equal to

$$gH = \{gf \in G \mid f \in H\}.$$ □

Such equivalence classes gH are called **cosets**. Given that we can construct a new set by binning all distinct cosets, a natural question to ask is whether such a quotient set is also a group (with respect to the inherited group operation). It turns out that this is a meaningful notion only when H is normal.

First, we define the quotient group as a mere set.

Definition 2.2. Let G be a group and $N \lhd G$, with equivalence relation and cosets defined as in Lemma 2.1 with respect to N. We define the **quotient group** of G by $\sim_N$ as

$$G/\sim_N \coloneqq \{gN \mid g \in G\}. \tag{8}$$

Often, one writes G/N for the quotient group, and the equivalence relation is implicitly assumed to be the standard one.

Now we prove that equipping G/N with the group operation inherited from G indeed yields a group proper, and in the process show that N being normal is precisely the condition required for this construction to work.

Theorem 2.1. *Let G/N be a quotient group. For any $fN, gN \in G/N$, define*

$$(fN)(gN) \coloneqq \{fmgn \mid m, n \in N\}. \tag{9}$$

Then G/N is closed with respect to this operation, and furthermore $(fN)(gN) = (fg)N \in G/N$.

Proof. Let $m, n \in N$. Then

$$\begin{aligned} fmgn &= f(gg^{-1})mgn \qquad (10) \\ &= (fg)\underbrace{(g^{-1}mg)}_{\in N}n \in (fg)N. \qquad \square \end{aligned}$$

Observe that, because N is normal, the elements of $(fN)(gN)$ remain elements of a coset also over N (i.e. $(fg)N$). In other words, if N were *not* normal, then there would be no guarantee that $g^{-1}mgn$ would remain within N. In that case, G/N would not be closed, hence not a group.

3 Group homomorphisms

We now introduce an important class of maps that will allow us to analyze and classify the simple Lie groups. That is the group homomorphism, which preserves the specific group operations between its domain and target. For pedagogical reasons, we explicitly supply unique symbols for the group operations in the following definition.

Definition 3.1. Let $(G, \bullet)$ and $(H, *)$ be groups with their respective group operations. A **group homomorphism** is a map $\varphi\colon G \to H$ such that, for all $f, g \in G$,

$$\varphi(f \bullet g) = \varphi(f) * \varphi(g). \tag{11}$$

Remark 3.1. It follows from the definition that, for identities $\mathbf{1}_G \in G$ and $\mathbf{1}_H \in H$,

$$\varphi(\mathbf{1}_G) = \mathbf{1}_H, \tag{12}$$

and, for any $g \in G$, we have

$$\varphi(g^{-1}) = \varphi(g)^{-1}. \tag{13}$$

We now develop the following terminology and notation which will be useful for the remainder of the course:

Definition 3.2. An **injective** map is one-to-one: every element of its target is mapped by *at most* 1 element of its domain. An injective group homomorphism is equivalent to an **inclusion**, and shall be denoted by

$$H \hookrightarrow G. \tag{14}$$

In this sense, we may write (by abuse of notation) $H \subseteq G$.

A **surjective** map is onto: every element of its target is mapped by *at least* 1 element of its domain. A surjection shall be denoted by

$$G \twoheadrightarrow H. \tag{15}$$

A map which is both injective and surjective is called a **bijection**. A bijective group homomorphism is further specified as an **group isomorphism**. We shall denote such maps by

$$G \xrightarrow{\sim} H. \tag{16}$$

A group isomorphism is a particularly special map whose existence indicates that the two groups in question have the same cardinality and share the same underlying group structure. If G and H are isomorphic, we write $G \cong H$.

We now introduce the so-called first isomorphism theorem for groups, which tells us how to construct an isomorphism between groups from a mere surjection.

Theorem 3.1. *Let G and H be groups, related by a surjective group homomorphism $\varphi\colon G \twoheadrightarrow H$. Then $\ker\varphi \lhd G$ and $G/\ker\varphi \cong H$, with isomorphism*

$$\begin{aligned} \Phi\colon G/\ker\varphi &\xrightarrow{\sim} H, \\ g\ker\varphi &\mapsto \varphi(g). \end{aligned} \tag{17}$$

Proof. Let $n \in \ker\varphi$, so that $\varphi(n) = \mathbf{1}_H$. Then, for any $g \in G$,

$$\begin{aligned} \varphi(gng^{-1}) &= \varphi(g)\varphi(n)\varphi(g^{-1}) \\ &= \varphi(g)\mathbf{1}_H\varphi(g)^{-1} \\ &= \mathbf{1}_H. \end{aligned} \tag{18}$$

Thus $gng^{-1} \in \ker\varphi\ \forall g \in G$, hence $\ker\varphi \lhd G$.

Now define $\Phi\colon G/\ker\varphi \to H$ as above. Suppose $\Phi(g\ker\varphi) = \Phi(h\ker\varphi)$ for some $g, h \in G$. Then $\varphi(g) = \varphi(h)$, or

$$\begin{aligned} \mathbf{1}_H &= \varphi(h)^{-1}\varphi(g) \\ &= \varphi(h^{-1}g). \end{aligned} \tag{19}$$

So we have that $h^{-1}g \in \ker\varphi$, which is the condition for $g \sim_{\ker\varphi} h$. Thus $\Phi(g\ker\varphi) = \Phi(h\ker\varphi)$ implies $g\ker\varphi = h\ker\varphi$, and so Φ is injective. But we began by assuming Φ is surjective, so it is indeed bijective.

To show that Φ preserves the group structure, consider any two $g\ker\varphi, h\ker\varphi \in G/\ker\varphi$. Then

$$\begin{aligned} \Phi\big((g\ker\varphi)(h\ker\varphi)\big) &= \Phi(gh\ker\varphi) \\ &= \varphi(gh) \\ &= \varphi(g)\varphi(h) \\ &= \Phi(g\ker\varphi)\Phi(h\ker\varphi). \end{aligned} \tag{20}$$

□

4 Simple Lie algebras

As the final piece needed for classification, we turn to the algebras which generate our groups. The notion of a simple Lie algebra is closely related to that of a simple Lie group. However, we will quickly see that a simple Lie algebra does not necessarily correspond to a simple Lie group, so care must be taken with these objects.

Note that, unlike with our discussion of simple groups, we will be explicitly working with Lie algebras (rather than algebras in general), as the Lie structure is crucial for our constructions.

Definition 4.1. Let $\mathfrak{g}$ be a Lie algebra and $\mathfrak{n} \subseteq \mathfrak{g}$ a Lie subalgebra (recall: a subset closed under the Lie bracket). We call $\mathfrak{n}$ an **ideal** of $\mathfrak{g}$ if, $\forall x \in \mathfrak{n}$ and $\forall y \in \mathfrak{g}$, $[y, x] \in \mathfrak{n}$.

The ideals of a Lie algebra can be thought of as analogs to the normal subgroups of a Lie group. Instead of invariance to conjugation, ideals talk about invariance to the Lie bracket. However, these notions are closely related: consider the conjugation of $x \in \mathfrak{n}$ by an infinitesimally generated $e^{y\,dt}$ for any $y \in \mathfrak{g}$. Then

$$e^{y\,dt}\,x\,e^{-y\,dt} = x + [y, x]\,dt. \tag{21}$$

If $\mathfrak{n}$ is an ideal, then by definition $[y, x] \in \mathfrak{n}$ and so we have that $e^{y\,dt}\,x\,e^{-y\,dt} \in \mathfrak{n}$ as well. So we shall overload the notation $\mathfrak{n} \lhd \mathfrak{g}$ to indicate that $\mathfrak{n}$ is an ideal of $\mathfrak{g}$.

As a motivating physical example, consider the following operator algebra frequently seen in quantum mechanics.

Example 4.1. The Weyl–Heisenberg algebra

$$\mathfrak{h} \coloneqq \langle i\mathbf{1}, iq, ip\rangle \tag{22}$$

is defined by the canonical Lie bracket

$$[q, p] = i\mathbf{1}. \tag{23}$$

(The notation $\langle S\rangle$ denotes the linear span of the set S.) It only has nontrivial ideal $\langle i\mathbf{1}\rangle$.

However, now consider the sum of $\mathfrak{h}$ with the vector space quadratic in q and p:

$$\mathfrak{g} \coloneqq \mathfrak{h} \oplus \langle iq^2, ip^2, iqp\rangle. \tag{24}$$

It turns out that $\mathfrak{h} \lhd \mathfrak{g}$. We will not offer a formal proof here, but one may recall from a standard treatment of quantum mechanics that

$$[q^2, q] = 0, \tag{25a}$$
$$[p^2, q] = -2ip, \tag{25b}$$
$$[qp, q] = -iq \tag{25c}$$
$$[q^2, p] = 2iq, \tag{25d}$$
$$[p^2, p] = 0, \tag{25e}$$
$$[qp, p] = ip, \tag{25f}$$

which are all elements of $\mathfrak{h}$. By linearity of the Lie bracket, one can extend these results for all linear combinations of the generators. In particular, the Lie bracket of a quadratic term and a linear term always yields a linear term (hence an element of $\mathfrak{h}$), but the Lie bracket of two quadratic terms will yield another quadratic term (hence an element of $\mathfrak{g} \setminus \mathfrak{h}$). So the nontrivial ideal of $\mathfrak{g}$ must be restricted to the linear terms.

Just as we defined simple Lie groups by their normal subgroups, the definition of a simple Lie algebra follows analogously.

Definition 4.2. A Lie algebra $\mathfrak{g}$ is called a **simple Lie algebra** if its only ideals are trivial ($\mathfrak{g}$ and $\{0\}$).

Earlier we mentioned that a simple Lie algebra $\mathfrak{g}$ may not always generate a simple Lie group $e^{\mathfrak{g}}$. We can see this with the following example.

Example 4.2. Consider the Lie group SU(2) and its corresponding Lie algebra $\mathfrak{su}(2)$. While $\mathfrak{su}(2)$ is a simple Lie algebra, SU(2) is *not* a simple Lie group.

Proof. To show that $\mathfrak{su}(2) \coloneqq \langle i\sigma_x, i\sigma_y, i\sigma_z\rangle$ is simple, we make use of the Pauli commutation relation,

$$[\sigma_j, \sigma_k] = 2i\varepsilon_{jkl}\sigma_l. \tag{26}$$

This tells us that $\mathfrak{su}(2)$ has no nontrivial ideal, since any nontrivial subalgebra will be missing at least 1 generator and hence fail the Lie bracket condition for ideals. For instance, consider $\langle i\sigma_x, i\sigma_y\rangle \subset \mathfrak{su}(2)$. Then

$$[\sigma_y, \sigma_x] = -2i\sigma_z \notin \langle i\sigma_x, i\sigma_y\rangle. \tag{27}$$

However, SU(2) is not simple, since there exists a nontrivial normal subgroup, $\{\mathbf{1}, -\mathbf{1}\} \lhd \mathrm{SU}(2)$. □

5 Connected normal subgroups and ideals

Despite this dismal result, we may yet salvage a correspondence between simple Lie groups and their algebras. This is achieved by looking directly at their normal subgroups and ideals.

Theorem 5.1. *Let $\mathfrak{g}$ be a Lie algebra and $\mathfrak{h} \subseteq \mathfrak{g}$ a subalgebra. Then $e^{\mathfrak{h}} \subseteq e^{\mathfrak{g}}$ is a connected subgroup.*

Proof. For all $x, y \in \mathfrak{h}$, use the Baker–Campbell–Hausdorff formula to compute

$$e^x e^y = \exp\biggl(x + y + \frac{1}{2}[x,y] + \frac{1}{12}[x,[x,y]] - \frac{1}{12}[y,[x,y]] + \cdots\biggr) . \tag{28}$$

Since $\mathfrak{h}$ is a subalgebra, $[x,y] \in \mathfrak{h}$, $[x,[x,y]] \in \mathfrak{h}$, etc. Thus $e^x e^y \in e^{\mathfrak{h}}$.

Note that every Lie group of the form $e^{\mathfrak{g}}$ is connected, since there is always a path from the $\mathbf{1}$ to e^x parametrized by $t \in \mathbb{R}$, i.e. $\{e^{tx} \mid t \in [0,1]\}$, for each $x \in \mathfrak{g}$. So $e^{\mathfrak{h}}$ is connected as well. □

Example 5.1. Consider the subalgebra $\langle i\sigma_z \rangle \subset \mathfrak{su}(2)$. Then $e^{\langle i\sigma_z \rangle} \subset \mathrm{SU}(2)$ is connected.

Proof. Observe: $e^{\langle i\sigma_z \rangle} \cong \mathrm{U}(1)$, which is connected. □

From this result, we can further show that a connected normal subgroup corresponds to an ideal.

Theorem 5.2. *Let $\mathfrak{g}$ be a Lie algebra and $\mathfrak{n} \lhd \mathfrak{g}$ an ideal. Then $e^{\mathfrak{n}} \lhd e^{\mathfrak{g}}$ is a connected normal subgroup.*

Proof. For any $x \in \mathfrak{n}$ and $y \in \mathfrak{g}$, recall the adjoint representation:

$$\begin{aligned} e^y e^x e^{-y} &= \exp\bigl(e^y \, x \, e^{-y}\bigr) \\ &= \exp\bigl(e^{\mathrm{ad}_y}(x)\bigr) . \end{aligned} \tag{29}$$

Since $\mathfrak{n}$ is an ideal, $e^{\mathrm{ad}_y}(x) \in \mathfrak{n}$ since $e^{\mathrm{ad}_y}(x)$ is nothing but a sum of nested Lie brackets of y and x. Thus $e^y e^x e^{-y} \in e^{\mathfrak{n}}$. But since $e^x \in e^{\mathfrak{n}}$ and $e^y \in e^{\mathfrak{g}}$, this is precisely the condition for $e^{\mathfrak{n}} \lhd e^{\mathfrak{g}}$.

Connectedness follows from Theorem 5.1. □

The interpretation of this result is that, from the converse of Theorem 5.2, if a Lie algebra $\mathfrak{g}$ is simple, then all nontrivial normal subgroups $N \lhd e^{\mathfrak{g}}$ are *not* connected (if they exist). This turns out to be a powerful statement: as an upshot for next week, we shall see that this leads to a chain of implications which allows us to classify the simple Lie groups via simple Lie algebras:

$$\begin{tikzcd}
\mathfrak{g} \text{ simple} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & N \text{ discrete} \arrow[d, Rightarrow] \\
e^{\mathfrak{g}} \text{ connected} \arrow[r, Rightarrow] & N \text{ central} \arrow[d, Rightarrow] \\
e^{\mathfrak{g}} \text{ compact} \arrow[r, Rightarrow] & N \text{ finite}
\end{tikzcd} .$$