Contents

List of Figures

List of Tables

Chapter 1

Introduction to Groups

1.1 Disclaimer

This is a course on applications of group theory to physics, with a strong bias toward condensed matter physics, which, after all, is the very best kind of physics. Abstract group theory is a province of mathematics, and math books on the subject are filled with formal proofs, often rendered opaque due to the efficient use of mathematical notation, replete with symbols such as $\cap$, $\rtimes$, $\exists$, $\oplus$, $\triangleleft$, $\flat$, ©, ♠, ♡, ♢, ♣, *etc.* In this course I will keep the formal proofs to a minimum, invoking them only when they are particularly simple or instructive. I will try to make up for it by including some good jokes. If you want to see the formal proofs, check out some of the texts listed in Chapter 0.

1.2 Why Study Group Theory?

1.2.1 Discrete and continuous symmetries

Group theory – big subject! Our concern here lies in its applications to physics (see §1.1).

Why is group theory important? Because many physical systems possess *symmetries*, which can be broadly classified as either *continuous* or *discrete*. Examples of continuous symmetries include space translations and rotations in homogeneous and isotropic systems, Lorentz transformations, internal rotations of quantum mechanical spin and other multicomponent quantum fields such as color in QCD, *etc.* Examples of discrete symmetries include parity, charge conjugation, time reversal, permutation symmetry in many-body systems, and the discrete remnants of space translations and rotations applicable to crystalline systems.

In each case, the symmetry operations are represented by individual group elements. Discrete symmetries entail discrete groups, which may contain a finite or infinite number of elements[1]. Continuous

[1] An example of a finite discrete group is the two-element group consisting of the identity I and space inversion (parity) P, otherwise known as $\mathbb{Z}_2$. An example of a discrete group containing an infinite number of elements is the integers $\mathbb{Z}$ under

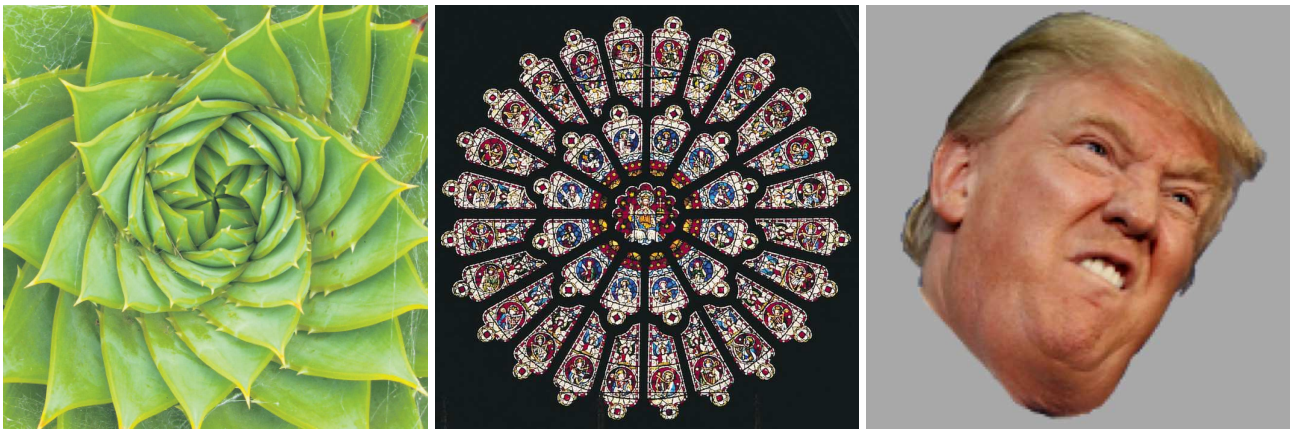

Figure 1.1: Western theories of beauty date to the pre-Socratic Greek philosophers (6th - 5th c. BCE), such as the Pythagoreans, who posited a connection between aesthetic beauty and mathematical properties of symmetry and proportion. Left: Symmetry in the natural world (aloe vera plant). Center: The beautiful Rose Window at the Durham Cathedral (originally 15th c.). Right: A non-symmetric image.

symmetries entail continuous (Lie) groups. Lie groups are themselves *smooth manifolds* endowed with a group structure. Necessarily, they contain an infinite number (continuum) of elements, and they can be either compact or noncompact[2].

1.2.2 Symmetries in quantum mechanics

In quantum mechanics, symmetries manifest themselves as *unitary operators* U which commute with the system Hamiltonian, H. (An important exception which we shall study later is the case of *anti-unitary* symmetries, such as time-reversal.) Any operator Θ transforms under the symmetry as $\Theta' = U^\dagger \, \Theta \, U$. The simplest example is space inversion, also known as *parity*, and denoted by the symbol P. One then has $\mathsf{P}^\dagger \boldsymbol{r} \, \mathsf{P} = -\boldsymbol{r}$ and $\mathsf{P}^\dagger \boldsymbol{p} \, \mathsf{P} = -\boldsymbol{p}$. Clearly $\mathsf{P}^2 = 1$, so $\mathsf{P}^\dagger = \mathsf{P}^{-1} = \mathsf{P}$, *i.e.* P is Hermitian as well as unitary. For a single particle Hamiltonian of the form $H = \frac{\boldsymbol{p}^2}{2m} + V(\boldsymbol{r})$, we have $[H, \mathsf{P}] = 0$ if $V(\boldsymbol{r}) = V(-\boldsymbol{r})$. This means that H and P are simultaneously diagonalizable, which means that energy eigenstates may be chosen to be parity eigenstates. Clearly the eigenvalues of P are ± 1.

Now let $|\, n \,\rangle$ denote any one-body quantum state, *i.e.* a vector in Hilbert space. The position space wavefunction is $\psi_n(\boldsymbol{r}) = \langle\, \boldsymbol{r} \,|\, n \,\rangle$. Since $\mathsf{P} \,|\, \boldsymbol{r} \,\rangle = |\, -\boldsymbol{r} \,\rangle$, we have that the parity-flipped wavefunction is given by[3] $\tilde{\psi}_n(\boldsymbol{r}) = \langle\, \boldsymbol{r} \,|\, \mathsf{P} \,|\, n \,\rangle = \psi_n(-\boldsymbol{r})$. If $|\, n \,\rangle$ is a parity eigenstate, *i.e.* if $\mathsf{P} \,|\, n \,\rangle = \pm |\, n \,\rangle$, then we have $\tilde{\psi}_n(\boldsymbol{r}) = \psi_n(-\boldsymbol{r}) = \pm \psi_n(\boldsymbol{r})$. Furthermore, if $|\, n \,\rangle$ and $|\, n' \,\rangle$ are parity eigenstates with eigenvalues σ and σ', respectively, then for any even parity (parity-invariant) operator $\Theta_{\rm e} = \mathsf{P}^\dagger \, \Theta_{\rm e} \, \mathsf{P}$, we have

$$\langle\, n \,|\, \Theta_{\rm e} \,|\, n' \,\rangle = \langle\, n \,|\, \mathsf{P}^\dagger \, \Theta_{\rm e} \, \mathsf{P} \,|\, n' \,\rangle = \sigma\sigma' \langle\, n \,|\, \Theta_{\rm e} \,|\, n' \,\rangle \quad , \tag{1.1}$$

addition.

[2] In mathematical parlance, compact means 'closed and bounded'. An example of a compact Lie group is SU(2), which describes spin rotation in quantum mechanics. An example of a noncompact Lie group is the Lorentz group, O(3,1).

[3] Note $\langle\, \boldsymbol{r} \,|\, \mathsf{P} \,|\, n \,\rangle = \langle\, -\boldsymbol{r} \,|\, n \,\rangle$.

and therefore if $\sigma\sigma' = -1$, meaning that $|\, n \,\rangle$ and $|\, n' \,\rangle$ are states of opposite parity, then $\langle\, n \,|\, \Theta_{\rm e} \,|\, n' \,\rangle = 0$. This is an example of a *selection rule* : operators which preserve a symmetry cannot mix states which transform differently under that symmetry. Another consequence of this analysis is that any *odd*-parity operator, for which $\mathtt{P}^\dagger\, \Theta_{\rm o}\, \mathtt{P} = -\Theta_{\rm o}$, will *only* have nonzero matrix elements between opposite parity states. Thus, if $[H, \mathtt{P}] = 0$, and the eigenstates are all chosen to have definite parity, any perturbation $V = \lambda\, \Theta_{\rm o}$ will result in no energy shifts within first order perturbation theory.

1.3 Formal definition of a discrete group

1.3.1 Group properties

What is a group? A discrete group G consists of distinct *elements* g_a and a group operation called multiplication, satisfying the following conditions:

(i) **Closure** : The product of two group elements is also a group element.

(ii) **Associativity** : In taking the product of three group elements, it doesn't matter if you first multiply the two left ones and then the right one, or first the two right ones and then the left one.

(iii) **Identity** : There exists a unique identity element, which is the same for both left and right multiplication.

(iv) **Inverse** : Each group element has its own unique inverse, which is both a left and a right inverse[4].

Mathy McMathstein says it this way:

(i′) $\forall\ g_a,\ g_b \in G$, $\exists\ g_c \in G$ s.t. $g_a\, g_b = g_c$.

(ii′) $g_a\, g_b\, g_c = (g_a\, g_b)\, g_c = g_a\, (g_b\, g_c)\ \forall\ a, b, c$.

(iii′) $\exists!\ E \in G$ s.t. $g_a\, E = E g_a = g_a\ \forall\ a$.

(iv′) $\forall\ g_a \in G$, $\exists\ g_a^{-1} \in G$ s.t. $g_a\, g_a^{-1} = g_a^{-1}\, g_a = E$.

These properties hold for continuous groups as well, in which case the group elements $g(\lambda)$ are labeled by a continuous parameter. Some remarks:

- If $g_a\, g_b = g_b\, g_a$ for all a, b, the group is said to be *abelian*. Otherwise, it is *nonabelian*.
- For discrete groups, $|G| \equiv N_G$ denotes the number of elements in G, which is the *order* of G. This may be finite $\big(|S_3| = 6\big)$, finite but ridiculously large $\big(|M| \sim 8 \times 10^{53}$ for the *Monster group*$\big)$, or infinite $\big(\mathbb{Z}$ under addition$\big)$.

[4] Tony Zee pithily summarizes this property as "there's nothing you can do that can't be undone". Real life is not like this! There is no inverse operation applicable to late homework, for example.

1.3.2 The Cayley table

All the information about any discrete group is provided by its multiplication table (also called a *Cayley table*). Our convention for group multiplication tables is given in Tab. 1.1 We shall write the group elements as $\{g_1, g_2, \ldots, g_{N_G}\}$, where $g_1 \equiv E$ is always taken to be the identity, and where N_G is the number of elements in the group. Note the following salient features of the Cayley table:

- The rows and columns range over all the symmetry operations (*i.e.* group elements) g, so that the entry for row g_a and column g_b is the result of the combined operation $g_a \cdot g_b \equiv g_a\, g_b$.
- The identity occurs once in each row and in each column; furthermore $g_a\, g_b = E$ means $g_b\, g_a = E$ as well. Thus, each element g has a unique inverse g^{-1}, which is both a left and a right inverse.
- Indeed, each group element occurs precisely once in each row and in each column. If the same element h were to appear more than once in the $g^{\rm th}$ row, it would mean that there would exist two distinct elements, g_a and g_b such that $gg_a = gg_b = h$. But applying the inverse g^{-1} on the left says $g_a = g_b$, which contradicts our assumption that these elements are distinct. Such a table is called a *Latin square*, *i.e.* an $n \times n$ array of n different symbols, each of which appears exactly once in each row and column.

If the Cayley table is symmetric, the multiplication operation is commutative. Alas, there is no simple test to check, from a given Cayley table, whether the multiplication operation is associative, which is necessary in order for G to be a group. In principle, one must test whether $g \cdot (h \cdot k) = (g \cdot h) \cdot k$ for all $g, h, k \in G$, which involves verifying $|G|^3$ equalities[5].

G	g_1	g_2	g_3	g_4	$\cdots$
g_1	g_1	g_2	g_3	g_4	$\cdots$
g_2	g_2	g_2^2	$g_2\, g_3$	$g_2\, g_4$	$\cdots$
g_3	g_3	$g_3\, g_2$	g_3^2	$g_3\, g_4$	$\cdots$
g_4	g_4	$g_4\, g_2$	$g_4\, g_3$	g_4^2	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Table 1.1: Convention for group multiplication tables. The identity element is $E \equiv g_1$.

1.3.3 Loops and groups

A finite *loop*[6] is a set L consisting of $|L| \equiv N_L$ elements plus a binary operation (*i.e.* multiplication) such that if $\ell, \ell' \in L$, then each of the equations $\ell \cdot x = \ell'$ and $y \cdot \ell = \ell'$ has a unique solution in L. Furthermore, the loop possesses a unique identity element E such that $E \cdot \ell = \ell \cdot E = \ell$ for all $\ell \in L$. If we order

[5] A procedure known as *Light's associativity test* can sometimes simplify this tedious task.

[6] See *"Non-Associative Loops for Holger Bech Nielsen"*, https://arxiv.org/pdf/hep-th/0111292.pdf.

the loop elements as $\{\ell_1, \ell_2, \ldots, \ell_{N_L}\}$, with $\ell_1 = E$, then the multiplication table for L is a Latin square whose first row and first column are identical. If the multiplication operation is associative, then the loop is a group!

It turns out that all loops with $|L| \leq 4$ are associative, *i.e.* they are groups. At order $N = 5$ there is one discrete group, $\mathbb{Z}_5$, corresponding to clock arithmetic *modulo* 5. There are also four non-associative loops. At order $|L| = 6$ there are two groups: $\mathbb{Z}_2 \times \mathbb{Z}_3$, which is abelian, and $C_{3v} \cong D_3$, which is nonabelian and which we shall discuss in detail in §1.3.4 below. There are also 107 non-associative loops. A non-associative loop may nevertheless be abelian! A particularly interesting and beautiful non-associative loop is that of the eight element *octonions*[7]. In Tabs. 1.2 and 1.3, we present the Cayley tables for two non-associative loops, one (L_5) of order 5 and one (L_6) of order 6. In each case the identity element is denoted as a. Note that within L_5 we have $(c \cdot d) \cdot e = b \cdot e = c$, but $c \cdot (d \cdot e) = c \cdot b = e$. The Cayley table for L_6 is symmetric, hence the loop L_6 is abelian, but $(b \cdot c) \cdot d = f \cdot d = c$ while $b \cdot (c \cdot d) = b \cdot b = a$, so it is non-associative.

L_5	a	b	c	d	e
a	a	b	c	d	e
b	b	a	d	e	c
c	c	e	a	b	d
d	d	c	e	a	b
e	e	d	b	c	a

Table 1.2: A non-associative loop of order 5.

L_6	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	c	d
c	c	f	a	b	d	e
d	d	e	b	a	f	c
e	e	c	d	f	a	b
f	f	d	e	c	b	a

Table 1.3: A non-associative loop of order 6.

1.3.4 The equilateral triangle : C_{3v} and C_3

Contemplating the symmetries of the lowly equilateral triangle is an instructive introductory exercise. Consider the left panel of Fig. 1.2. The equilateral triangle has the following six symmetries:

(i) identity E (ii) rotation by $\frac{2\pi}{3}$, R (iii) rotation by $-\frac{2\pi}{3}$, W
(iv) reflection σ (v) reflection σ' (vi) reflection σ''

Taken together, these symmetry operations constitute a discrete group known as C_{3v}[8]. Note that R and W commute, since they are rotations about the same axis. Indeed, $W = R^{-1} = R^2$. However, staring at the figure for a little while, one can deduce that $R\sigma = \sigma''$ while $\sigma R = \sigma'$, so R and σ do not commute! Thus, the group C_{3v} is *nonabelian*.

To construct the Cayley table of C_{3v} , we must evaluate the binary products of various group operations. Clearly $R^2 = W$ since two 120° rotations combine to give a 240° rotation. Similarly, $W^2 = R$, since rotating twice by 240° yields a 480° $\cong$ 120° rotation. More attention is required when working out the

[7] See http://math.ucr.edu/home/baez/octonions/.

[8] In the group C_{nv}, the C stands for "cyclic", the subscript n refers to the n-fold symmetry axis, and the subscript v signifies the presence of n reflection planes, each containing that axis.

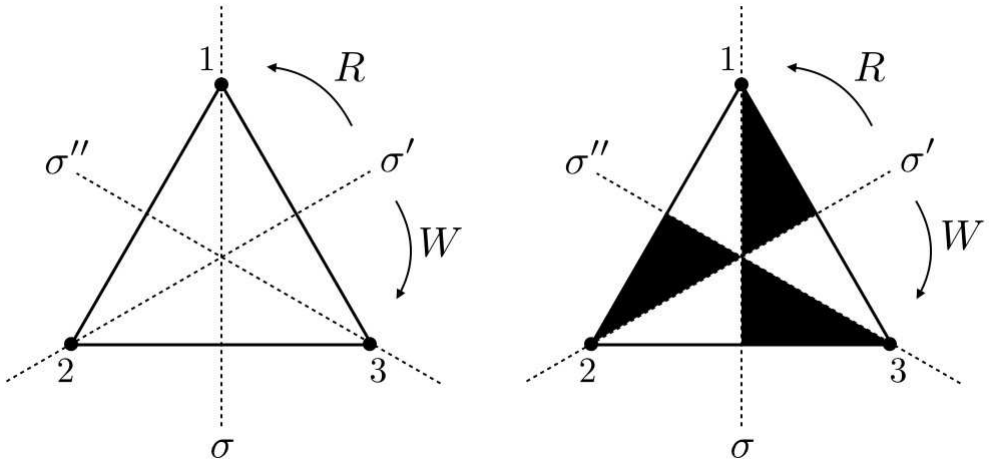

Figure 1.2: Left: The symmetry group C_{3v} of the equilateral triangle contains six elements, which are the identity E, counterclockwise and clockwise 120° rotations R and W, and three reflections σ, σ', and σ''. Right: The black regions break the reflection symmetries, resulting in a lower symmetry group C_3, which contains only the two rotations and the identity.

products of the rotations $\{R, W\}$ and the mirrors $\{\sigma, \sigma', \sigma''\}$. For example, consider the product $R\sigma$. First applying the σ operation, the labels of the vertices are permuted from $\{1, 2, 3\}$, starting at the top and proceeding counterclockwise, to $\{1, 3, 2\}$. Rotating by 120° results in the labeling $\{2, 1, 3\}$, which is also obtained by applying the σ'' operation to the labels $\{1, 2, 3\}$. Reasoning thusly, one obtains the full Cayley table for C_{3v} , given in Tab. 1.4 below.

C_{3v}	E	R	W	σ	σ'	σ''
E	E	R	W	σ	σ'	σ''
R	R	W	E	σ''	σ	σ'
W	W	E	R	σ'	σ''	σ
σ	σ	σ'	σ''	E	R	W
σ'	σ'	σ''	σ	W	E	R
σ''	σ''	σ	σ'	R	W	E

Table 1.4: Multiplication table for the group C_{3v}.

Group representations : first encounter

We can *represent* the various symmetry operations via a map $D^{(2)} : C_{3v} \to \mathsf{O}(2)$ from C_{3v} to the space of 2×2 orthogonal matrices:

$$D^{(2)}(E) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad D^{(2)}(R) = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \qquad D^{(2)}(W) = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix} \tag{1.2}$$

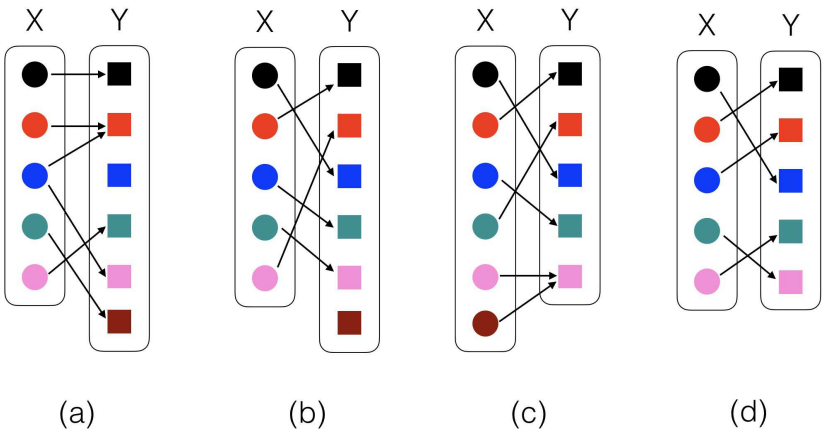

Figure 1.3: A function $f : X \to Y$ maps a set X (the *domain*) to a set Y (the *codomain*). The *range* of a function f is the set $f(X)$. (a) Are you f'ing kidding me?! This is not a function. (b) This function is *injective* (one-to-one), *i.e.* $f(x) \neq f(x')$ whenever $x \neq x'$. (c) This function is *surjective* (onto), *i.e.* $f(X) = Y$. (d) This function is *bijective* (one-to-one and onto).

and

$$D^{(2)}(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad D^{(2)}(\sigma') = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \qquad D^{(2)}(\sigma'') = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix} \quad . \tag{1.3}$$

Here the superscript $^{(2)}$ denotes the fact that our *representation* is in terms of two-dimensional matrices. One can check that $D^{(2)}(g)\, D^{(2)}(g') = D^{(2)}(gg')$ for all g and g'. Restricted to this subset of $\mathsf{O}(2)$, the mapping $D^{(2)}$ is *bijective* (*i.e.* one-to-one and onto), which means that $D^{(2)}(C_{3v})$ is a *faithful representation* of our group C_{3v}. See Fig. 1.3 for a reminder of the meanings of the terms *injective*, *surjective*, and *bijective*.

Formally, a representation of a group G on a vector space $\mathcal{V}$ over a field $\mathbb{F}$ is a group homomorphism ρ from G to $\mathsf{GL}(\mathcal{V})$, the general linear group on $\mathcal{V}$, *i.e.*

$$\varphi \;:\; G \to \mathsf{GL}(\mathcal{V}) \tag{1.4}$$

such that $\varphi(g_a\, g_b) = \varphi(g_a)\, \varphi(g_b)$. The vector space $\mathcal{V}$ is then called a *G-module*. If the module $\mathcal{V}$ has a nontrivial invariant proper subspace, the representation is said to be *reducible*. When $\mathcal{V}$ is of finite dimension $n \in \mathbb{Z}_+$, we may identify $\mathsf{GL}(\mathcal{V})$ with $\mathsf{GL}(n, \mathbb{F})$, which is the group of invertible $n \times n$ matrices on $\mathbb{F}$. Typically the field $\mathbb{F}$ is the real or complex numbers under addition and multiplication. In the case of $D^{(2)}(C_{3v})$, the vector space is $\mathcal{V} = \mathbb{R}^2$, the field is $\mathbb{R}$, and $n = 2$.

1.3.5 Symmetry breaking

Breaking C_{3v} to C_3

Consider now the right panel of Fig. 1.2. The figure is still fully symmetric under the operations $\{E, R, W\}$, but no longer is symmetric under any of the reflections $\{\sigma, \sigma', \sigma''\}$. The remaining symmetry group is denoted C_3, and consists only of the identity and the two rotations, since the reflection

symmetries are broken. This corresponds to restricting ourselves to the upper left 3×3 block of Tab. 1.4, which satisfies all the desiderata for a multiplication table of a group with three elements. One says that C_{3v} has been broken down to its *subgroup* C_3. Note that the cyclic group C_3 is equivalent to modulo 3 arithmetic, *i.e.* $C_3 \cong \mathbb{Z}_3$.

Upon inspection of Tab. 1.4, it is apparent that C_{3v} has other subgroups. For example, the elements $\{E, \sigma\}$ form a closed set under multiplication, with $E^2 = \sigma^2 = E$ and $E\sigma = \sigma E = \sigma$. This corresponds to the group $\mathbb{Z}_2$ (equivalent to C_2). What is special about the C_3 subgroup $\{E, R, W\}$ is that it is a *normal* (or *invariant*) subgroup. More on this in §1.4 below.

Spontaneous symmetry breaking

In quantum mechanics, as we shall see, the eigenstates of a Hamiltonian H_0 which commutes with all the *generators* of a symmetry group G may be classified according to the *representations* of that group. Typically this entails the appearance of degeneracies in the eigenspectrum, with degenerate states transforming into each other under the group operations. Adding a perturbation V to the Hamiltonian which breaks G down to a subgroup H will accordingly split these degeneracies, and the new multiplets of $H = H_0 + V$ are characterized by representations of the lower symmetry group H.

In quantum field theory, as a consequence of the infinite number of degrees of freedom, symmetries may be *spontaneously broken*. This means that even if the Hamiltonian H (or action S) for the field theory is invariant under a group G of symmetry transformations, the ground state may not be invariant under the full symmetry group G. The presence or absence of spontaneous symmetry breaking (SSB), and its detailed manifestations, will in general depend on the couplings, or the temperature in the case of quantum statistical mechanics. SSB is usually associated with the presence of a local *order parameter* which transforms nontrivially under some group operations, and whose whose quantum statistical average vanishes in a fully symmetric phase, but takes nonzero values in symmetry-broken phase[9]. The parade example is the Ising model, $H = -\sum_{i<j} J_{ij}\,\sigma_i\,\sigma_j$, where each $\sigma_i = \pm 1$, the subscript i indexes a physical location in space, such as a site $\boldsymbol{R}_i$ on a particular lattice. The model is explicitly $\mathbb{Z}_2$ symmetric under $\sigma_i \to \varepsilon\sigma_i$ for all i, where $\varepsilon \in \{+1, -1\}$, yet if the interaction matrix $J_{ij} = J(\boldsymbol{R}_i - \boldsymbol{R}_j)$ is short-ranged and the space dimension d is greater than one, there is a *critical temperature* $T_{\rm c}$ below which SSB sets in, and the system develops a spontaneous magnetization $\phi = \langle\sigma_i\rangle$. You know how in quantum mechanics, the eigenstates of a particle moving in one-dimensional double-well potential $V(x) = V(-x)$ can be classified by their parity eigenvalues, and the lowest two energy states are respectively symmetric ($\mathsf{P} = +1$) and antisymmetric ($\mathsf{P} = -1$), and are delocalized among both wells. For a quantum field theory, however, with (Euclidean) Lagrangian density $\mathcal{L}_{\rm E} = \frac{1}{2}(\boldsymbol{\nabla}\phi)^2 + V(\phi)$, for $d > 1$ and $T < T_{\rm c}$, the system actually picks the left or the right well, so that $\langle\phi(\boldsymbol{r})\rangle \neq 0$. Another example is the spontaneously broken $\mathsf{O}(2)$ invariance of superfluids, where the boson annihilation operator $\psi(\boldsymbol{r})$ develops a spontaneous average $\big\langle\psi(\boldsymbol{r})\big\rangle = \sqrt{n_0}\,e^{i\theta}$, where n_0 is the condensate density and θ the condensate phase.

Truth be told, the above description is a bit of a swindle. In the ferromagnetic ($J_{ij} > 0$) Ising model, for example, at $T = 0$, there are still two ground states, $|\Uparrow\rangle \equiv |\uparrow\uparrow\uparrow\cdots\rangle$ and $|\Downarrow\rangle \equiv |\downarrow\downarrow\downarrow\cdots\rangle$. The (ergodic) zero temperature density matrix is $\rho_0 = \frac{1}{2}|\Uparrow\rangle\langle\Uparrow| + \frac{1}{2}|\Downarrow\rangle\langle\Downarrow|$, and therefore $\langle\sigma_i\rangle = \mathsf{Tr}\big(\rho_0\,\sigma_i\big) = 0$. The

[9] While SSB is generally associated with the existence of a phase transition, not all phase transitions involve SSB. Exceptions include topological phases, which have no local order parameter.

order parameter apparently has vanished. WTF?! There are at least two compelling ways to resolve this seeming conundrum:

(a) First, rather than defining the order parameter of the Ising model, for example, to be the expected value $m = \langle \sigma_i \rangle$ of the local spin[10], consider instead the behavior of the *correlation function* $C_{ij} = \langle \sigma_i \, \sigma_j \rangle$ in the limit $d_{ij} = |\boldsymbol{R}_i - \boldsymbol{R}_j| \to \infty$. In a disordered phase, there is no correlation between infinitely far separated spins, hence $\lim_{d_{ij}\to\infty} C_{ij} = 0$. In the ordered phase, this is no longer true, and we define the *spontaneous magnetization* m from the long distance correlator: $m^2 \equiv \lim_{d_{ij}\to\infty} \langle \sigma_i \, \sigma_j \rangle$. In this formulation, SSB is associated with the emergence of *long-ranged order* in the correlators of operators which transform nontrivially under the symmetry group.

(ii) Second, we could impose an external field which *explicitly* breaks the symmetry, such as a Zeeman term $H' = -h \sum_i \sigma_i$ in the Ising model. We now compute the magnetization (per site) $m(T, h, V) = \langle \sigma_i \rangle$ as a function of temperature T, the external field h, *and* the volume V of our system. The order parameter $m(T)$ in zero field is then defined as

$$m(T) = \lim_{h\to 0} \lim_{V\to\infty} m(T, h, V) \quad . \tag{1.5}$$

The order of limits here is crucially important. The thermodynamic limit $V \to \infty$ is taken first, which means that the energy difference between $|\Uparrow\rangle$ and $|\Downarrow\rangle$, being proportional to hV, diverges, thus infinitely suppressing the $|\Downarrow\rangle$ state if $h > 0$ (and the $|\Uparrow\rangle$ state if $h < 0$). The magnitude of the order parameter will be independent on the way in which we take $h \to 0$, but its sign will depend on whether $h \to 0^+$ or $h \to 0^-$, with $\mathsf{sgn}(m) = \mathsf{sgn}(h)$. Physically, the direction in which a system orders can be decided by the presence of small stray fields or impurities. An illustration of how this works in the case of ideal Bose gas condensation is provided in the appendix §1.6 below.

Note that in both formulations, SSB is necessarily associated with the existence of a local operator $\mathcal{O}_i$ which is identified as the order parameter field. In (i) the correlations $\langle \mathcal{O}_i \, \mathcal{O}_j \rangle$ exhibit long-ranged order in the symmetry-broken phase. In (ii) $\mathcal{O}_i$ is the operator to which the external field h_i couples.

1.3.6 The dihedral group D_n

In the mathematics literature, the symmetry group of the planar n-gon is called the *dihedral group*[11], D_n. Elements of D_n act on two-dimensional space as (i) rotations about a central point by multiples of $2\pi/n$ and (ii) reflections in any of n lines each containing the central point, and oriented at multiples of π/n from some fiducial axis. D_n thus contains $2n$ elements. If we denote by r the group element which rotates (counterclockwise, say) by $2\pi/n$, and we denote by σ any one of the mirror symmetries of the n-gon, then the following are True Facts: (i) $r^n = 1$, (ii) $\sigma^2 = 1$, and (iii) $\sigma r \sigma = r^{-1}$. The first two are obvious. The third is also obvious after a moment's thought: by reflecting, rotating, and reflecting again, the sense of rotation is reversed. One says that r and σ are the *generators* of D_n, and the three True Facts are *relations* satisfied by the generators. Below in §1.4.6, we shall discuss how the full group multiplication table, which can be quite unwieldy for groups with many elements, can be replaced by a

[10] We assume translational invariance, which means $\langle \sigma_i \rangle$ is independent of the site index i.

[11] The word *dihedral* means "two faces" and probably has its origins in Greek political rhetoric.

group presentation, denoted $\langle\, \mathcal{G} \,|\, \mathfrak{R} \,\rangle$, where $\mathcal{G}$ are the generators and $\mathfrak{R}$ the relations. Thus, the presentation for D_n is $\langle\, r\,,\, \sigma \,|\, r^n = 1\,,\, \sigma^2 = 1\,,\, \sigma r \sigma = r^{-1} \,\rangle$. D_n's $2n$ elements then nicely divide into two subsets: $\{E\,,\, r\,,\, \ldots\,,\, r^{n-1}\}$ and $\{\sigma\,,\, \sigma r\,,\, \ldots\,,\, \sigma r^{n-1}\}$. The first of these is itself the group $C_n \cong \mathbb{Z}_n$.

Apologia pro vita mea : D_n *versus* C_{nv}

What is the difference between D_n and C_{nv}? As we've just defined D_n above, it is identical to C_{nv}. Each of the reflections is an *improper rotation*, *i.e.* it is represented by a 2×2 orthogonal matrix whose determinant is -1. According to crystallographers, however, the definition of D_n is the group of symmetry operations consisting of a single n-fold axis plus n equally splayed *twofold axes* each perpendicular to the n-fold axis. In other words, D_n in *three* space dimensions is a subgroup of $\mathsf{SO}(3)$, and as such it involves only *proper rotations*. Could anything be more awful?[12] We will revisit the distinction when we discuss crystallographic point groups, but at the level of group theory this is all a tempest in a teapot, because D_n and C_{nv} are *isomorphic* – their elements may be placed in one-to-one correspondence, and their multiplication tables are the same. One way to think about it is to take the six 2×2 matrices $D^{(2)}(g)$ faithfully representing the elements of C_{3v} and add a third row and column, padding the additional entries with zeroes except in the lower right $(3,3)$ corner, where we place a 1. Clearly the multiplication table is the same. But we could also choose to place a 1 in the $(3,3)$ slot for $g \in \{E, R, W\}$, and a (-1) there for $g \in \{\sigma, \sigma', \sigma''\}$. The multiplication table remains the same! The representation is still faithful! And now each of our six 3×3 matrices has determinant $+1$. So let's all just chill and accept that C_{nv} is a perfectly acceptable notation for the symmetries of the planar n-gon, as our crystallographer forebears have wisely decreed[13].

1.3.7 The permutation group S_n

A permutation of the symbols $\{1, 2, \ldots, n\}$ is a rearrangement $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ of those same symbols, commonly denoted by

$$\sigma \equiv \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix} \quad . \tag{1.6}$$

The meaning of the above notation is the following. We are to imagine an ordered set of n boxes, each of which contains an object[14]. Applying the operation σ means that the contents of box 1 are placed in box $\sigma(1)$, the contents of box 2 are placed in box $\sigma(2)$, *etc.* The inverse operation is given by

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} \quad , \tag{1.7}$$

[12] Well, of course it could. Cancer, for example.

[13] Crystallography is a subset of solid state physics, and solid state physics is a subset of condensed matter physics. And condensed matter physics is the very best kind of physics, as we pointed out in §1.1.

[14] The objects are arbitrary, and don't necessarily have to be distinct themselves. Some boxes could contain nothing at all. Others might contain a magnificent present for your group theory instructor.

and the rule for composition (multiplication) of permutations is then

$$\begin{aligned}\mu\sigma &= \begin{pmatrix} 1 & 2 & \cdots & n \\ \mu(1) & \mu(2) & \cdots & \mu(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & n \\ \mu\big(\sigma(1)\big) & \mu\big(\sigma(2)\big) & \cdots & \mu\big(\sigma(n)\big) \end{pmatrix} \quad ,\end{aligned} \tag{1.8}$$

and thus the initial contents of box k wind up in box $\mu\big(\sigma(k)\big)$. These operations form a discrete group, since the composition of two rearrangements is another rearrangement, and since, as anyone who has rearranged furniture to satisfy the whims of a fussy spouse can attest, you can always "just put it back the way it was", *i.e.* each element has its inverse. This group of operations is known as the *permutation group* (or *symmetric group*), and is abbreviated S_n.

Clearly S_n has $n!$ elements, so the size of the multiplication table is $n! \times n!$. Furthermore, we can represent each element $\sigma \in S_n$ as an $n \times n$ matrix consisting of zeros and ones, such that $\big[D^{(n)}(\sigma)\big]_{ij} = 1$ if $i = \sigma(j)$ and 0 otherwise. This generates the desired permutation when acting on the column vector $\boldsymbol{v}$ whose transpose is $\boldsymbol{v}^{\rm T} = (1\ 2\ 3\ \cdots\ n)$.

We will study S_n in more detail below (see §1.4.3), but for now let's consider the case $n = 3$, which is the permutation group for three objects. Consulting the left panel of Fig. 1.2 once more, we see to each element of C_{3v} there corresponds a unique element of S_3:

$$\begin{aligned} E &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad R = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad W = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \sigma' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \sigma'' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad .\end{aligned} \tag{1.9}$$

Note we can write $R = (123)$, $W = (132)$, $\sigma = (23)$, $\sigma' = (13)$, and $\sigma'' = (12)$, using the cycle notation. The above relations constitute a bijection between elements of C_{3v} and elements of S_3. The multiplication tables therefore are the same. Thus, in essence, S_3 *is* C_{3v}. In mathematical notation, we write $S_3 \cong C_{3v}$, where the symbol $\cong$ denotes *group isomorphism*.

We mentioned above how S_n has a representation in terms of $n \times n$ matrices. We may write the 3×3 matrices $D^{(3)}(g)$ for S_3 as

$$\begin{aligned} D^{(3)}(E) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad D^{(3)}(R) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad D^{(3)}(W) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \\ D^{(3)}(\sigma) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad D^{(3)}(\sigma') = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad D^{(3)}(\sigma'') = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad .\end{aligned} \tag{1.10}$$

One can check that these matrices yield the same multiplication table as for $S_3 \cong C_{3v}$. Thus, we have thus far obtained two faithful representations of this group, one two-dimensional and one three-dimensional.

Remember the interpretation that the permutation σ places the former contents of box j into box $\sigma(j)$ for all j. We can arrange these boxes in a column vector of length n. If in our $n = 3$ case we start with ♣ in box 1, ⋈ in box 2, and ☋ in box 3, application of the element R results in

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \clubsuit \\ \bowtie \\ \upsilon \end{pmatrix} = \begin{pmatrix} \upsilon \\ \clubsuit \\ \bowtie \end{pmatrix} \quad , \tag{1.11}$$

and now we have ♣ in box 2, ⋈ in box 3, and ☋ in box 1.

1.3.8 Our friend, SU(2)

SU(2) is an example of a continuous group known as a *Lie group*. We shall introduce Lie groups more thoroughly in §1.5 below. For the moment, recall that a matrix $U \in \mathsf{U}(2)$ is a 2×2 complex-valued matrix which satisfies $U^\dagger = U^{-1}$, *i.e.* $U^\dagger U = E$, where E is the identity matrix. This entails $|\det U| = 1$, and requiring $U \in \mathsf{SU}(2)$ imposes the additional constraint $\det U = 1$. Now let us parameterize U, initially in terms of four complex numbers, and examine the matrices $U^\dagger$ and U^{-1}:

$$U = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \quad \Rightarrow \quad U^\dagger = \begin{pmatrix} w^* & y^* \\ x^* & z^* \end{pmatrix} \quad , \quad U^{-1} = \frac{1}{\det U} \begin{pmatrix} z & -x \\ -y & w \end{pmatrix} \quad . \tag{1.12}$$

Since $\det U = 1$, we conclude $z = w^*$ and $y = -x^*$, hence we may parameterize all matrices in SU(2) in terms of two complex numbers, $w \in \mathbb{C}$ and $x \in \mathbb{C}$, *viz.*

$$U = \begin{pmatrix} w & x \\ -x^* & w^* \end{pmatrix} \quad , \quad U^{-1} = U^\dagger = \begin{pmatrix} w^* & -x \\ x^* & w \end{pmatrix} \tag{1.13}$$

and subject to the constraint

$$\det U = |w|^2 + |x|^2 = 1 \quad . \tag{1.14}$$

Thus, SU(2) is topologically equivalent to the 3-sphere S^3 sitting inside $\mathbb{C}^2 \cong \mathbb{R}^4$.

We can check the closure:

$$U_1 U_2 = \begin{pmatrix} w_1 & x_1 \\ -x_1^* & w_1^* \end{pmatrix} \begin{pmatrix} w_2 & x_2 \\ -x_2^* & w_2^* \end{pmatrix} = \begin{pmatrix} w_1 w_2 - x_1 x_2^* & w_1 x_2 + x_1 w_2^* \\ -w_1^* x_2^* - x_1^* w_2 & w_1^* w_2^* - x_1^* x_2 \end{pmatrix} \quad . \tag{1.15}$$

Thus, $U_1 U_2$ is of the appropriate form, provided its determinant is indeed unity. We have

$$\begin{aligned} \det(U_1 U_2) &= |w_1 w_2 - x_1 x_2^*|^2 + |w_1 x_2 + x_1 w_2^*|^2 \\ &= |w_1|^2 |w_2|^2 + |x_1|^2 |x_2|^2 + |w_1|^2 |x_2|^2 + |x_1|^2 |w_2|^2 \\ &= \big(|w_1|^2 + |x_1|^2\big)\big(|w_2|^2 + |x_2|^2\big) = \det U_1 \det U_2 = 1 \quad , \end{aligned} \tag{1.16}$$

and so closure is verified. Of course, we knew in advance this would work out, *i.e.* that determinant of a product is the product of the determinants.

Another useful parameterization of SU(2) is in terms of the Pauli matrices:

$$g(\alpha, \hat{\boldsymbol{n}}) \equiv \exp\big(-\tfrac{i}{2}\,\alpha\,\hat{\boldsymbol{n}} \cdot \boldsymbol{\sigma}\big) = \cos\tfrac{\alpha}{2} - i \sin\tfrac{\alpha}{2}\,\hat{\boldsymbol{n}} \cdot \boldsymbol{\sigma} \quad , \tag{1.17}$$

where $\hat{\boldsymbol{n}}$ is a three-dimensional unit vector and where $\alpha \in [0, 2\pi)$. The inverse operation is given by $g^{-1}(\alpha, \hat{\boldsymbol{n}}) = \exp\big(\frac{i}{2}\,\alpha\,\hat{\boldsymbol{n}} \cdot \boldsymbol{\sigma}\big)$. Recall that $g(\alpha, \hat{\boldsymbol{n}})$ rotates a spinor by an angle α about the $\hat{\boldsymbol{n}}$ axis in internal spin space. Note that $g(2\pi, \hat{\boldsymbol{n}}) = -1$, so rotation by 2π about any axis is equivalent to multiplication by -1. We shall comment more fully on this in future chapters. Writing the unit vector $\hat{\boldsymbol{n}}$ in terms of a polar angle θ and azimuthal angle ϕ, note that

$$w = \cos\tfrac{\alpha}{2} - i \sin\tfrac{\alpha}{2} \cos\theta \qquad , \qquad x = -i \sin\tfrac{\alpha}{2} \sin\theta\, e^{-i\phi} \quad . \tag{1.18}$$

and thus $\big(\mathsf{Re}\,\omega, \mathsf{Im}\,\omega, \mathsf{Re}\,x, \mathsf{Im}\,x\big)$ is a real four-component unit vector lying on S^3.

We already know that it must work out, but it is somewhat instructive to verify closure in this parameterization. This means that $g(\alpha, \hat{\boldsymbol{n}})\, g(\beta, \hat{\boldsymbol{m}}) = g(\gamma, \hat{\boldsymbol{k}})$ for some angle γ and unit vector $\hat{\boldsymbol{k}}$. We can evaluate the product explicitly:

$$\begin{aligned} g(\alpha, \hat{\boldsymbol{n}})\, g(\beta, \hat{\boldsymbol{m}}) &= \Big(\cos\tfrac{\alpha}{2} - i \sin\tfrac{\alpha}{2}\, \hat{\boldsymbol{n}} \cdot \boldsymbol{\sigma}\Big)\Big(\cos\tfrac{\beta}{2} - i \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{m}} \cdot \boldsymbol{\sigma}\Big) \\ &= \cos\tfrac{\alpha}{2} \cos\tfrac{\beta}{2} - i \Big(\sin\tfrac{\alpha}{2} \cos\tfrac{\beta}{2}\, \hat{\boldsymbol{n}} + \cos\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{m}}\Big) \cdot \boldsymbol{\sigma} - \sin\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, (\hat{\boldsymbol{n}} \cdot \boldsymbol{\sigma})(\hat{\boldsymbol{m}} \cdot \boldsymbol{\sigma}) \\ &= \Big(\cos\tfrac{\alpha}{2} \cos\tfrac{\beta}{2} - \sin\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{n}} \cdot \hat{\boldsymbol{m}}\Big) \\ &\qquad - i \Big(\sin\tfrac{\alpha}{2} \cos\tfrac{\beta}{2}\, \hat{\boldsymbol{n}} + \cos\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{m}} + \sin\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{n}} \times \hat{\boldsymbol{m}}\Big) \cdot \boldsymbol{\sigma} \quad , \end{aligned} \tag{1.19}$$

where we have invoked $\sigma^\alpha \sigma^\beta = \delta^{\alpha\beta} + i\,\epsilon_{\alpha\beta\gamma}\,\sigma^\gamma$. We therefore have

$$\begin{aligned} \cos\tfrac{\gamma}{2} &= \cos\tfrac{\alpha}{2} \cos\tfrac{\beta}{2} - \sin\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{n}} \cdot \hat{\boldsymbol{m}} \\ \sin\tfrac{\gamma}{2} &= \Big| \sin\tfrac{\alpha}{2} \cos\tfrac{\beta}{2}\, \hat{\boldsymbol{m}} + \cos\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{n}} + \sin\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{n}} \times \hat{\boldsymbol{m}} \Big| \\ &= \sqrt{\tfrac{1}{2}(1 - \cos\alpha\cos\beta) + \tfrac{1}{2}\sin\alpha\sin\beta\, \hat{\boldsymbol{n}} \cdot \hat{\boldsymbol{m}} + \tfrac{1}{4}(1 - \cos\alpha)(1 - \cos\beta)\big[1 - (\hat{\boldsymbol{n}} \cdot \hat{\boldsymbol{m}})^2\big]} \quad , \end{aligned} \tag{1.20}$$

from which one verifies $\cos^2\big(\frac{\gamma}{2}\big) + \sin^2\big(\frac{\gamma}{2}\big) = 1$. The vector $\hat{\boldsymbol{k}}$ is then given by

$$\hat{\boldsymbol{k}} = \frac{\sin\frac{\alpha}{2} \cos\frac{\beta}{2}\, \hat{\boldsymbol{m}} + \cos\frac{\alpha}{2} \sin\frac{\beta}{2}\, \hat{\boldsymbol{n}} + \sin\frac{\alpha}{2} \sin\frac{\beta}{2}\, \hat{\boldsymbol{n}} \times \hat{\boldsymbol{m}}}{\Big| \sin\frac{\alpha}{2} \cos\frac{\beta}{2}\, \hat{\boldsymbol{m}} + \cos\frac{\alpha}{2} \sin\frac{\beta}{2}\, \hat{\boldsymbol{n}} + \sin\frac{\alpha}{2} \sin\frac{\beta}{2}\, \hat{\boldsymbol{n}} \times \hat{\boldsymbol{m}} \Big|} \tag{1.21}$$

and the angle γ by

$$\gamma = 2 \cos^{-1}\Big(\cos\tfrac{\alpha}{2} \cos\tfrac{\beta}{2} - \sin\tfrac{\alpha}{2} \sin\tfrac{\beta}{2}\, \hat{\boldsymbol{n}} \cdot \hat{\boldsymbol{m}}\Big) \tag{1.22}$$

with $\gamma \in [0, 2\pi)$. We see that $\big[g(\alpha, \hat{\boldsymbol{n}})\,,\, g(\beta, \hat{\boldsymbol{m}})\big] = 0$ if $\hat{\boldsymbol{n}} \times \hat{\boldsymbol{m}} = 0$, *i.e.* if the two rotations are about the same axis.

1.4 Aspects of Discrete Groups

1.4.1 Basic features of discrete groups

Here we articulate a number of key concepts in the theory of discrete groups.

GROUP HOMOMORPHISM : A *group homomorphism* is a map $\phi : G \mapsto G'$ which respects multiplication, *i.e.* $\phi(g_a)\,\phi(g_b) = \phi(g_a\,g_b)$, where $g_{a,b} \in G$ and $\phi(g_{a,b}) \in G'$. If ϕ is *bijective* (one-to-one and onto), it is an *isomorphism*, and we write $G \cong G'$. This means that *G and G' are the same group*. The maps $D^{(2)}(C_{3v})$ and $D^{(3)}(C_{3v})$ discussed above in §1.3.4 and §1.3.7 are isomorphisms.

The *kernel* of a homomorphism ϕ is the set of elements in G which get mapped to the identity in G', whereas the *image* of ϕ is the set of elements in G' which have a pre-image in G. Thus[15],

$$\mathsf{ker}(\phi) = \big\{g \in G \,\big|\, \phi(g) = E'\big\} \qquad , \qquad \mathsf{im}(\phi) = \big\{\phi(g) \,\big|\, g \in G\big\} \quad . \tag{1.23}$$

As an example, consider the homomorphism which maps C_{3v} to $\mathbb{Z}_2$, where $\phi(E) = \phi(R) = \phi(W) = +1$ and $\phi(\sigma) = \phi(\sigma') = \phi(\sigma'') = -1$. Then $\mathsf{ker}(\phi) = \big\{E, R, W\big\}$. Consider next the map $D^{(2)} : C_{3v} \mapsto \mathsf{O}(2)$ in Eqn. 1.2. Clearly, not every element in $\mathsf{O}(2)$ has a preimage in C_{3v}, as $\mathsf{O}(2)$ is a continuous group with an infinite number of elements! $\mathsf{im}\big(D^{(2)}\big)$ is then the six matrices defined in Eqn. 1.2.

REARRANGEMENT THEOREM : Let the set of group elements be $\big\{E, g_2, g_3\,, \ldots\,, g_N\big\}$, where $N = |G|$. Call this particular ordering the *sequence* $\mathcal{S}_1$. Then for any $g_a \in G$, the sequence $\mathcal{S}_2 = \big\{g_aE, g_a\,g_2\,, \ldots\,, g_a\,g_N\big\}$ contains every element in G.

The proof is elementary. First note that each element occurs in $\mathcal{S}_2$ at least once, since for any b one has $g_a^{-1}g_b \in G$, hence $g_a\big(g_a^{-1}g_b\big) = g_b$ is a member of $\mathcal{S}_2$. This is all we need to show, since $\mathcal{S}_1$ and $\mathcal{S}_2$ contain the same number N of elements, and every element in $\mathcal{S}_1$ is contained in $\mathcal{S}_2$. Therefore $\mathcal{S}_2$ is merely a *rearrangement* of $\mathcal{S}_1$.[16]

SUBGROUPS : A collection H of elements $\{h_j\}$ is called a *subgroup* of G if each $h_j \in G$ and if H itself forms a group under the same multiplication law. One expresses this as $H \subset G$. Some examples: $C_3 \subset C_{3v}$, $\mathsf{SO}(2) \subset \mathsf{SO}(3)$, $S_n \subset S_{n'}$ if $n < n'$. Note $\mathbb{Z}_2 \subset \mathbb{Z}_4$ but $\mathbb{Z}_2 \not\subset \mathbb{Z}_5$ (more on this below)[17]. The identity element $\{E\}$ always forms its own (trivial) subgroup[18].

COSETS AND LAGRANGE'S THEOREM : If G is of finite order, and $H \subset G$, then $M \equiv |H|$ is a divisor of $N \equiv |G|$. The proof is somewhat instructive. Consider some ordering $\big\{E, g_2, g_2\,, \ldots\,, g_N\big\}$ of all the elements of G and pick the first element in this set which is not a member of H. Call this element g. Then form the *left coset* $gH \equiv \big\{gE, g\,h_2\,, \ldots\,,\ g\,h_M\big\}$. Note that gH is not a group because it cannot contain the identity[19]. Note also that gH contains M unique elements, none of which is a member of H. To see this,

[15] Be aware, in my notation, that im means 'image', whereas Im means 'imaginary part'.

[16] Just to put a fine point on it, suppose there is a repeating element in $\mathcal{S}_2$, *i.e.* suppose $g_a\,g_b = g_a\,g_c$ for $b \neq c$. Then applying g_a^{-1} on the left, we have $g_b = g_c$, which is a contradiction.

[17] Recall $\mathbb{Z}_n$, the group of "clock arithmetic base n", is the same group as C_n, *i.e.* n-fold rotations about a single axis, or the set $\big\{e^{2\pi ij/n} \,\big|\, j \in \{0, 1, \ldots, n-1\}\big\}$ under complex multiplication.

[18] If you do not understand why, please *kill yourself*.

[19] By assumption $g \notin H$, so $g \neq h_j^{-1}$ for all j, meaning $gh_j \neq E$ for all j.

first assume $gh_j = gh_k$ for some distinct j and k (with $h_0 = E$). Applying g^{-1} on the left yields $h_j = h_k$, which is a contradiction. Next, assume $gh_j = h_k$. This means $g = h_j^{-1} h_k$, which is again a contradiction since H is a group and therefore $h_j^{-1} h_k \in H$, but by assumption $g \notin H$. Now take the first element from G which is neither a member of H nor of gH, and call this g'. We form the corresponding coset $g'H$. By the same arguments, $g'H$ contains M distinct elements, none of which appears in H. But is $g'H$ distinct from gH? Indeed it is, for if $gh_j = g'h_k$ for some j and k, then $g' = gh_j h_k^{-1} \in gH$, since $h_j h_k^{-1} \in H$. But this contradicts our assumption that $g' \notin gH$. We iterate this procedure, forming $g''H$, *etc.* Since G is of finite order, this business must eventually end, say after the construction of l such cosets. But then we have managed to divide the entire N elements of G into $l+1$ sets, each of size M (H plus its l iteratively constructed cosets). We then say that H is a subgroup of *index* $l+1$. QED

Thus, $\mathbb{Z}_2 \not\subset \mathbb{Z}_5$, and furthermore no group of prime order can have a nontrivial subgroup.

ABELIAN SUBGROUPS : Let G be a finite discrete group. Then for any $g \in G$, there exists $n > 0$ such that $g^n = E$ (prove it!). The smallest such n is called the *order of the element* g. Therefore the set $\{E, g, g^2 , \ldots , g^{n-1}\}$ constitutes an *abelian subgroup* of G, itself of order n. For example, $\{E, \sigma\} \subset C_{3v}$ is the abelian subgroup $\mathbb{Z}_2$. $\{E, R, W = R^2\} \subset C_{3v}$ is the abelian subgroup C_3.

CENTER OF A GROUP : The *center* $Z(G)$ of a group G is the set of elements which commute with all other elements. *I.e.*

$$Z(G) = \{z \in G \,|\, zg = gz \quad \forall g \in G\} \quad . \tag{1.24}$$

Clearly $Z(G) \subset G$. The center of any abelian group G is G itself. For the dihedral groups D_n, the content of the center depends on whether n is even or odd. One has $Z(D_{2k+1}) \cong \{E\}$ and $Z(D_{2k}) \cong \{E, R^k\}$, where R rotates by π/k about the central axis. *I.e.* $Z(D_{2k}) \cong \mathbb{Z}_2$.

CENTRALIZER AND NORMALIZER : The *centralizer* $C_G(z)$ of a group element $z \in G$ is the set of all elements of G which commute with z , *i.e.* $C_G(z) = \{g \in G \,|\, gz = zg\}$. The centralizer of a subgroup $H \subset G$ is the set of all elements of G which commute with every element of H. Clearly the centralizer of any element or of any subgroup will contain $Z(G)$, the center of the group.

The *normalizer* of a subgroup $H \subset G$, denoted $N_G(H)$, is the set of all $g \in G$ such that $g^{-1}Hg = H$, which is equivalent to $gH = Hg$. Note that $C_G(H) \subseteq N_G(H)$, because $g \in C_G(H)$ requires $gh = hg$ for all $h \in H$, but $g \in N(G)$ satisfies the weaker requirement that for all $h \in H$, there exists $h' \in H$ with $gh = h'g$.

DIRECT PRODUCTS : Given two groups G and H, one may construct the *product group* $F = G \times H$, whose elements are ordered pairs (g, h) where $g \in G$ and $h \in H$. Multiplication in the product group is given by the natural extension $(g, h)(g', h') = (gg', hh')$. Note $|F| = |G| \cdot |H|$.

CONJUGACY : Two elements g and g' are said to be *conjugate* to each other if $\exists\ f \in G$ such that $g' = f^{-1}gf$. This has odors of the similarity transformation from linear algebra. Note that if g is conjugate to g' and g' is conjugate to g'', then $\exists\ f, h$ such that $g' = f^{-1}gf$ and $g'' = h^{-1}g'h$, from which we derive $g'' = (hf)^{-1}g(fh)$, *i.e.* g and g'' are also conjugate. Thus, conjugacy is transitive.

The set of distinct elements $\{f^{-1}gf \mid f \in G\}$ is called the *conjugacy class* (or *equivalency class*) of the element g. Note that $g_0 \equiv E$ is always in its own conjugacy class, with no other elements. Similarly, in abelian groups, each element is its own class. For C_{3v} there are three conjugacy classes: $\{E\}$, $\{R, W\}$,

and $\{\sigma, \sigma', \sigma''\}$. All elements in a given conjugacy class have the same order, for if $g^n = E$, then clearly $\left(f^{-1}gf\right)^n = f^{-1}Ef = E$.

NORMAL (INVARIANT) SUBGROUPS : A subgroup $H \subset G$ is called a *normal* (or *invariant*) *subgroup* if $g^{-1}Hg = H$ for all $g \in G$. Thus, any normal subgroup must be expressible as the union of some conjugacy classes. For example, $C_3 \subset C_{3v}$ is a normal subgroup, and the union of conjugacy classes $\{E\}$ and $\{R, W\}$. But $\mathbb{Z}_2 \subset C_{3v}$ consisting of (E, σ) is not, because $W^{-1}\sigma W = \sigma'$. Instead of writing "H is an invariant subgroup of G," Mathy McMathstein writes $H \triangleleft G$. Note that if $F = G \times H$, then $G \triangleleft F$ and $H \triangleleft F$.

SIMPLE GROUP : Any group G which contains no invariant subgroups is said to be *simple*. Tony Zee explains this beautifully. He says that we'd like to be able to articulate a notion of simplicity, meaning that a group can't be broken up into smaller groups. One might think we should then demand that G have no nontrivial subgroups[20] at all in order for it to be simple. Alas, as Zee points out, "subgroups are a dime a dozen". Indeed, as we've already seen, one can form an abelian subgroup $\left\{E, g, g^2, \ldots, g^{n-1}\right\}$, where n is the order of g, starting with *any* group element. But while you find subgroups everywhere, *invariant* subgroups are quite special. Clearly any group of prime order is simple. So are the alternating groups[21] A_n for $n > 4$. The classification of all finite simple groups has been a relatively recent triumph in mathematics[22]. Other examples of finite simple groups include the classical and exceptional Chevalley groups, the Mathieu groups, the McLaughlin group[23], the Baby Monster group, with $4154781481226426191177580544000000$ elements, and the Monster group[24], which has $808017424794512875886459904961710757005754368000000000$ elements[25].

COSETS AND FACTOR GROUPS : We have already introduced the concept of a *left coset*, gH, formed by multiplying each element of a subgroup $H \subset G$ on the left by a given element $g \in G$. (Of course, one can just as well define the right cosets of H, *i.e.* $\{Hg\}$.) Consider now the left cosets of an invariant subgroup $H \triangleleft G$. Now here's something cool and mathy: cosets can be multiplied. The result is rather simple:

$$(g_a h_m)(g_b h_n) = g_a\, g_b\, (g_b^{-1} h_m\, g_b)\, h_n \equiv g_a\, g_b\, h_l\, h_n \quad , \tag{1.25}$$

where $h_l \equiv g_b^{-1} h_m\, g_b \in H$, since H is an invariant subgroup. Thus, $(g_a H)(g_b H) = (g_a\, g_b)H$. This means the left cosets $\{gH\}$ themselves form a group under multiplication. This group is called the *quotient group*, G/H. Note that $|G/H| = |G|/|H|$, because there are $|H|$ elements in each coset, and therefore there must be $|G|/|H|$ cosets in total. In general, the quotient group is not a normal subgroup of G. Example: $C_{3v}/C_3 = \mathbb{Z}_2$.

COMMUTATOR SUBGROUP : Recall the algebraic notion of the commutator $[X, Y] = XY - YX$. For group operations, the commutator $\langle \bullet, \bullet \rangle$ is defined as

$$\langle g, h \rangle = g^{-1} h^{-1} g h \quad . \tag{1.26}$$

[20] *I.e.* no subgroups other than the identity and G itself.

[21] In §1.4.3 we will learn that A_n is the subgroup consisting of all even permutations in S_n.

[22] See https://en.wikipedia.org/wiki/List_of_finite_simple_groups

[23] See *e.g.* https://www.youtube.com/watch?v=mx9Ue9XLGW8. I always thought the McLaughlin group had five members, but Wikipedia says it has 898128000.

[24] The Monster group is the largest of the sporadic simple groups.

[25] If, as a summer student project, one endeavored to associate each atom contained in planet earth with a unique element of the Monster group, one would eventually run out of atoms.

The inverse of this operation is $\langle g,h\rangle^{-1} = \langle h,g\rangle$. Note that if $gh = hg$, then $\langle g,h\rangle = E$. Also note that upon conjugation,

$$s^{-1}\langle g,h\rangle s = \langle s^{-1}gs, s^{-1}hs\rangle \quad . \tag{1.27}$$

Now the product of two commutators under group multiplication is not in general another commutator. However, we can use the commutators $\langle g_a, g_b\rangle$ to *generate* a closed set under group multiplication, *i.e.*

$$\langle G,G\rangle = \left\{ \langle g_{a_1}, g_{a_2}\rangle\langle g_{a_3}, g_{a_4}\rangle \cdots \langle g_{a_{2n-1}}, g_{a_{2n}}\rangle \,\middle|\, n\in\mathbb{N},\ g_{a_k}\in G\ \forall\, k \right\} \tag{1.28}$$

Clearly $\langle G,G\rangle$ satisfies all the axioms for a group, and is a subgroup of G. We call $\langle G,G\rangle$ the *commutator* (or *derived*) subgroup of G. And because the set of commutators is closed under conjugation, $\langle G,G\rangle$ is an invariant subgroup of G: $\langle G,G\rangle \triangleleft G$. Some examples:

(i) $\langle S_n, S_n\rangle \cong A_n$, the group of even permutations (see §1.4.3 below).

(ii) $\langle A_n, A_n\rangle \cong A_n$ for $n > 4$, but $\langle A_4, A_4\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(iii) $\langle Q, Q\rangle \cong \mathbb{Z}_2$, where Q is the quaternionic group (see §1.4.5 below).

As Zee explains, the size of the commutator subgroup tells us roughly how nonabelian the group itself is. For abelian groups, $\langle G,G\rangle \cong \{E\}$. When $\langle G,G\rangle \cong G$, the group is maximally nonabelian in some sense. The quotient group $G^{\rm ab} \equiv G/\langle G,G\rangle$ is called the *abelianization* of G. A group is called *perfect* if it is isomorphic to its own commutator subgroup. The smallest nontrivial perfect group is A_5.

GROUP ALGEBRA : The *group algebra* $\mathcal{G}$ for any finite discrete group G is defined to be the set of linear combinations of the form $\boldsymbol{x} = \sum_{g\in G} x_g\, g$, where each $x_g \in \mathbb{C}$ is a complex number. Note that both addition and multiplication are defined for elements of $\mathbb{G}$, for if $\boldsymbol{y} = \sum_{g\in G} y_g\, g$, then

$$\boldsymbol{x}+\boldsymbol{y} = \sum_{g\in G}(x_g+y_g)\,g \qquad , \qquad \boldsymbol{x}\cdot\boldsymbol{y} = \sum_{g\in G}\sum_{h\in G} x_g\, y_h\, hg = \sum_{g\in G} \overbrace{\left(\sum_{h\in G} x_{h^{-1}g}\, y_h\right)}^{(xy)_g} g \equiv \sum_g (xy)_g\, g \quad . \tag{1.29}$$

We can think of the group elements as basis elements of a vector space $\mathcal{A}$ which acts on itself by multiplication as well as addition[26]. This structure we have just described is known in mathematical parlance as an *algebra*. An (associative) algebra is a linear vector space which is closed under some multiplication law. Thus there are two types of multiplication in an algebra. As a vector space over a field $\mathbb{F}$, one has ordinary multiplication by scalars in $\mathbb{F}$, *e.g.* real or complex numbers. But the individual basis elements, which in our case are group elements, have their own multiplication rule, specified by the Cayley table for the group. Another example which will be relevant to us is that of a *Lie algebra*, which, for our purposes, is also a vector space over $\mathbb{R}$ or $\mathbb{C}$, but where multiplication of two elements X and Y in the algebra is defined by the *Lie bracket*, $\big[X,Y\big]$. We will mainly be concerned with matrix Lie groups, in which case the Lie bracket is the familiar commutator.

[26]The vector space spanned by $g \in G$ is not necessarily normed.

The concept of an algebra is very close to that of another mathematical structure known as a *ring*. A ring $\mathcal{R}$ is a set endowed with the binary operations of addition and multiplication which is an abelian group under addition, a *monoid* under multiplication[27], and where multiplication distributes over addition[28].

1.4.2 Other math stuff

Here are some other math definitions which may be useful to clarify before going forward. They don't really belong in this section on discrete groups, but I thought it would be fun to hide them here anyway.

MONOID : A *monoid* is a triple $(M\,,\,\cdot\,,\,1)$ where M is a set which is closed under the associative binary product $\cdot$, and where 1 is the multiplicative identity (*i.e.*$m\cdot 1 = 1\cdot m = m$ for all $m\in M$).

RING : A *ring* is a set R where $(R\,,\,+\,,\,0)$ is an abelian group under addition, $(R\,,\,\cdot\,,\,1)$ is a monoid, and multiplication distributes over addition, *viz.*

$$\begin{aligned} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (a+b)\cdot c &= a\cdot c + b\cdot c \quad . \end{aligned} \tag{1.30}$$

Examples of rings include $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, the set $\left\{m+n\sqrt{2}\,|\,m,n\in\mathbb{Z}\right\}$, real continuous functions $f:[0,1]\to\mathbb{R}$ with $f(x)=0$ the additive identity and $f(x)=1$ the multiplicative identity, *etc.*

IDEAL : A *left ideal* I is a subset of a ring $I\subset R$ where $(I\,,\,+\,,\,0)$ is an abelian group, and where $ri\in I$ for all $r\in R$ and $i\in I$. For a *right ideal* the requirement is that $ir\in I$. If we require both $ir\in I$ and $ri\in I$, this defines an *ideal* (*i.e.* no need to specify left or right). Example: $I=2\mathbb{Z}\subset\mathbb{Z}$, *i.e.* the set of even integers, is an ideal in the ring $\mathbb{Z}$.

QUOTIENT RING : If $I\subset R$ is an ideal in R, the *quotient ring* $\overline{R}\equiv R/I$ is the set of elements of R modulo I, any of which we can write in the form $a+I$ where $a\in R$. Thus, two elements a and a' in the quotient ring $\overline{R}$ are equivalent if their difference lies in I (*i.e.* $a\equiv a' \;\Leftrightarrow\; a-a'\in I$). Within $\overline{R}$ we then have

$$\begin{aligned} (a+I)+(b+I) &= a+b+I \\ (a+I)\cdot(b+I) &= a\cdot b + I \quad . \end{aligned} \tag{1.31}$$

Thus, $\mathbb{Z}/2\mathbb{Z}=\{0,1\}$.

DOMAIN : Let R be a ring and $R^*=R-0$ the set of its nonzero elements (using $-$ for set subtraction). If $(R^*\,,\,\cdot\,,\,1)$ is a monoid then R is a domain. How on earth could $(R^*\,,\,\cdot\,,\,1)$ fail to form a monoid, I hear you thinking. Well, let R be the ring of real smooth functions[29] and define $f(x)=\left(\frac{1}{2}-x\right)\Theta\left(\frac{1}{2}-x\right)$ and

[27] A monoid is a set with a closed, associative binary operation and with an identity element. The difference between a monoid and a group is that each element of the monoid needn't have an inverse. In physics, the "renormalization group" should more appropriately be called the "renormalization monoid" since RG processes have no inverse.

[28] The formal difference between a ring $\mathcal{R}$ an an algebra $\mathcal{A}$ is that in a ring, the algebraic structure is entirely internal, but in an algebra there is additional structure because it allows for multiplication by an external ring $\mathcal{R}'$ in such a way that the two multiplication properties are compatible. So an algebra is actually two compatible rings. If this is confusing, take comfort in the fact that for our purposes, the external ring $\mathcal{R}'$ is just the complex numbers.

[29] Parsing disambiguation: by "real smooth functions" I mean functions $f(x)$ which are both real and in the class C^∞, as opposed to functions which are somehow like Luther Vandross.

$g(x) = \big(x - \frac{1}{2}\big)\,\Theta\big(x - \frac{1}{2}\big)$, where $\Theta(u)$ is the step function. Then both $f(x)$ and $g(x)$ lie within R^*, but their product $f(x) \cdot g(x) = 0 \notin R^*$. So R is not a domain.

DIVISION RING : Let R be a ring and again let $R^* = R - 0$. If $(R^*, \cdot, 1)$ is a group, we say that R is a *division ring*. A commutative division ring is a *field*.

VECTOR SPACE : A *vector space* $\mathcal{V}$ over a scalar field $\mathbb{F}$ consists of a set $\mathcal{V}$ and operations $+$ and $\cdot$ such that (i) $(\mathcal{V}\,,\,+\,,\,0)$ is an abelian group, (ii) $\mathcal{V}$ is closed under scalar multiplication by any $c \in \mathbb{F}$, (iii) scalars and vectors may be multiplied, and the $\cdot$ operation is, commutative, associative, and distributes over addition, and (iv) for all $\boldsymbol{v} \in \mathcal{V}$, $1 \cdot \boldsymbol{v} = \boldsymbol{v} \cdot 1 = \boldsymbol{v}$.

ASSOCIATIVE ALGEBRA : As mentioned above, an *associative algebra* is a vector space which is closed under some multiplication law. Thus there are two types of multiplication in an algebra.

1.4.3 More about permutations

Recall the general form of a permutation of n elements:

$$\sigma \equiv \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix} \quad . \tag{1.32}$$

Each such permutation can be factorized as a product of disjoint *cycles*, a process known as *cycle decomposition*. A k-cycle involves cyclic permutation of k elements, so $(i_1\, i_2\, \cdots\, i_k)$ means $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, *etc.*, and finally $\sigma(i_k) = i_1$. Consider, for example, the following element from S_7 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 6 & 8 & 1 & 3 & 5 & 4 \end{pmatrix} = (1\,7\,5)\,(2)\,(3\,6)\,(4\,8) \quad . \tag{1.33}$$

Thus σ is written as a product of one three-cycle, two two-cycles, and two one-cycles. The one-cycles of course do nothing. Written in this way, the cycle decomposition obeys the following sum rule: the sum of the lengths of all the cycles is the index n of S_n. Denoting all the one-cycles is kind of pointless, though, and typically we omit them in the cycle decomposition; in this case we'd just write $\sigma = (1\,7\,5)\,(3\,6)\,(4\,8)$. Alas, by virtue of suppressing the one-cycles, the sum rule no longer holds.

In fact, any k-cycle may be represented as a product of $k - 1$ two-cycles (also called *transpositions*):

$$(i_1\, i_2\, \cdots\, i_k) = (i_1\, i_2)(i_2\, i_3) \cdots (i_{k-1}\, i_k) \quad . \tag{1.34}$$

Note that the two-cycles here are not disjoint. The decomposition of a given k-cycle into transpositions is not unique, save for the following important feature: the total number of transpositions is preserved *modulo* 2. This feature allows us to associate a sign $\mathsf{sgn}(\sigma)$ with each permutation σ, given by $(-1)^r$, where r is the number of transpositions in any complete decomposition of σ into two-cycles. An equivalent definition: $\mathsf{sgn}(\sigma) = \epsilon_{\sigma(1)\,\sigma(2)\,\cdots\,\sigma(n)}$, where $\epsilon_{\alpha_1\,\alpha_2\,\cdots\,\alpha_n}$ is the completely antisymmetric tensor of rank n , with $\epsilon_{1\,2\,3\,\cdots\,n} = +1$. Note that $\mathsf{sgn}(\sigma\sigma') = \mathsf{sgn}(\sigma)\,\mathsf{sgn}(\sigma')$. This distinction allows us to define a subgroup of S_n known as A_n , the *alternating group*, consisting of all the *even* permutations in S_n. Clearly A_n contains the identity, and since the product of two even permutations is itself an even permutation, we may conclude that A_n is itself a group. Indeed, since $\mathsf{sgn}(\tilde{\sigma}^{-1}\sigma\tilde{\sigma}) = \mathsf{sgn}(\sigma)$, conjugacy preserves the

sign of any element of S_n , and we conclude $A_n \triangleleft S_n$, *i.e.* the alternating group is a normal subgroup of the symmetric group.

Let me conclude with a few other details about the symmetric group. First, the mapping $\mathsf{sgn} : S_n \mapsto \mathbb{Z}_2$ is a group homomorphism. This means that $D^{(1)}(\sigma) = \mathsf{sgn}(\sigma)$ is a one-dimensional representation of S_n, called the *sign representation*. Of course it is not a faithful representation, but fidelity is so 1990s[30]. Second, recall from §1.3.7 the representation $D^{(n)}(S_n)$ in terms of $n \times n$ matrices, where $\big[D^{(n)}(\sigma)\big]_{ij} = 1$ if $i = \sigma(j)$ and 0 otherwise. This is called the *defining representation*, and it is faithful. One then has that $\mathsf{sgn}(\sigma) = \det\big[D^{(n)}(\sigma)\big]$. Finally, we consider a cyclic decomposition of any permutation σ into ν_1 1-cycles, ν_2 2-cycles, *etc.* The sum rule is then $\sum_{k=1}^{n} k\,\nu_k = n$. Now any such decomposition is invariant under (i) permuting any of the k-cycles, and (ii) cyclic permutation within a k-cycle. Consider our friend $\sigma = (1\,7\,5)\,(2)\,(3\,6)\,(4\,8)$ from Eqn. 1.33. Clearly $n_1 = 1$, $n_2 = 2$, and $n_3 = 1$ with $1\cdot n_1 + 2\cdot n_2 + 3\cdot n_3 = 8$. Furthermore, we could equally well write $\sigma = (1\,7\,5)\,(2)\,(4\,8)\,(3\,6)$, permuting the two 2-cycles, or as $\sigma = (7\,5\,1)\,(2)\,(4\,8)\,(6\,3)$, cyclically permuting within the 3-cycle and one of the 2-cycles. This leads us to the following expression for the number $N(\nu_1, \nu_2, \ldots, \nu_n)$ of possible decompositions into ν_1 1-cycles, ν_2 2-cycles, *etc.* :

$$N(\nu_1, \nu_2, \ldots, \nu_n) = \frac{n!}{1^{\nu_1}\,\nu_1!\,2^{\nu_2}\,\nu_2!\,\cdots\,n^{\nu_n}\,\nu_n!} \quad . \tag{1.35}$$

The sign of each permutation is then uniquely given by its cyclic decomposition:

$$\mathsf{sgn}(\sigma) = (+1)^{\nu_1}(-1)^{\nu_2}(+1)^{\nu_3}(-1)^{\nu_4}\cdots = (-1)^{\#\text{ of cycles of even length}} \quad . \tag{1.36}$$

Finally, let's check that the sum over all possible decompositions gives the order of the group, *i.e.* that

$$\sum_{\nu_1=0}^{\infty}\cdots\sum_{\nu_n=0}^{\infty} N(\nu_1, \nu_2, \ldots, \nu_n)\,\delta_{\nu_1+2\nu_2+\ldots+n\nu_n\,,\,n} = n! \quad , \tag{1.37}$$

or, equivalently,

$$F_n \equiv \sum_{\nu_1=0}^{\infty}\cdots\sum_{\nu_n=0}^{\infty} \frac{\delta_{\nu_1+2\nu_2+\ldots+n\nu_n\,,\,n}}{1^{\nu_1}\,\nu_1!\,2^{\nu_2}\,\nu_2!\,\cdots\,n^{\nu_n}\,\nu_n!} = 1 \quad . \tag{1.38}$$

This must be true for all nonnegative integers n, with $F_0 \equiv 1$. In dealing with the constraint, recall the treatment of the grand canonical ensemble in statistical physics. We write the generating function

$$F(z) \equiv \sum_{n=0}^{\infty} F_n z^n = \prod_{k=0}^{\infty}\sum_{\nu_k=0}^{\infty} \frac{z^{k\nu_k}}{k^{\nu_k}\,\nu_k!} \quad , \tag{1.39}$$

in which case

$$F_n = \oint\limits_{|z|=1} \frac{dz}{2\pi i z}\,\frac{F(z)}{z^n} \quad . \tag{1.40}$$

[30] Please don't tell my wife I wrote that.

Thus, F_n is simply the coefficient of z^n in the Taylor expansion of $F(z)$. But now,

$$\begin{aligned} F(z) &= \prod_{k=0}^{\infty} \sum_{\nu_k=0}^{\infty} \frac{1}{\nu_k!} \left(\frac{z^k}{k} \right)^{\nu_k} = \prod_{k=0}^{\infty} \exp\left(z^k/k\right) \\ &= \exp\left(\sum_{k=0}^{\infty} \frac{z^k}{k} \right) = e^{-\ln(1-z)} = \frac{1}{1-z} = 1 + z + z^2 + \ldots \quad , \end{aligned} \tag{1.41}$$

and so indeed $F_n = 1$ for all $n \geq 0$. Ta da!

1.4.4 Conjugacy classes of the dihedral group

Let's count the conjugacy classes of D_n. First, we note that $D_n = \mathbb{Z}_n \cup \sigma\mathbb{Z}_n$, where $\mathbb{Z}_n \cong C_n$ is the cyclic group of order n, which is abelian, and σ is any one of the n twofold axes. Let r denote the primitive rotation by $2\pi/n$, and consider any of the elements $r^k \in \mathbb{Z}_n$, with $k \in \{1, \ldots, n-1\}$.[31] If we conjugate $r^k \to g^{-1} r^k g$ by any $g \in \mathbb{Z}_n$, we recover r^k because $\mathbb{Z}_n$ is abelian. So consider $g = \sigma r^l \in \sigma\mathbb{Z}_n$. Using $\sigma r \sigma = r^{-1}$, we readily obtain $g^{-1} r^k g = r^{-k}$. We conclude that for n odd, there are $\frac{1}{2}(n+1)$ two element conjugacy classes of the form $\{r, r^{n-1}\}$ through $\{r^{(n-1)/2}, r^{(n+1)/2}\}$, to which we add the one element class $\{E\}$. For n even, though, there are $\frac{1}{2}(n+2)$ such classes: two element classes $\{r, r^{n-1}\}$ through $\{r^{(n-2)/2}, r^{(n+2)/2}\}$ plus one element classes $\{E\}$ and $\{r^{n/2}\}$.

Next, we start with a general element $\sigma r^k \in \sigma\mathbb{Z}_n$ and generate its conjugates. If $g = r^l$, we have $g^{-1}\sigma r^k g = \sigma r^{2l+k}$, whereas if $g = \sigma r^l$, we have $g^{-1}\sigma r^k g = \sigma r^{2l-k}$. Thus if n is odd, we obtain one more conjugacy class, which is $\sigma\mathbb{Z}_n$ itself, with n elements. If, on the other hand, n is even, then $\sigma\mathbb{Z}_n$ splits into two conjugacy classes: $\{\sigma r^{2j}\}$ and $\sigma r^{2j+1}\}$, each with $j \in \{0, \ldots, \frac{1}{2}n - 1\}$, each of which has $\frac{1}{2}n$ elements. In the latter case, the two classes consist of all twofold axes which preserve a pair of vertices, and all twofold axes which preserve a pair of edges.

Putting it all together, we conclude that for n odd, D_n has $\frac{1}{2}(n+5)$ conjugacy classes, while for n even D_n has $\frac{1}{2}(n+6)$ conjugacy classes.

1.4.5 Quaternion group

The group Q is a nonabelian group consisting of eight elements, $\{\pm 1, \pm \mathtt{i}, \pm \mathtt{j}, \pm \mathtt{k}\}$, where $E = 1$. Its multiplication table is defined by the relations

$$\mathtt{i}^2 = \mathtt{j}^2 = \mathtt{k}^2 = -1 \quad , \quad \mathtt{ij} = -\mathtt{ji} = \mathtt{k} \quad , \quad \mathtt{jk} = -\mathtt{kj} = \mathtt{i} \quad , \quad \mathtt{ki} = -\mathtt{ik} = \mathtt{j} \quad . \tag{1.42}$$

Note that Q has the same rank as C_{4v} ($\cong D_4$), but has a different overall structure, *i.e.* Q is not isomorphic to D_4. Indeed, D_4 and Q are the only two non-Abelian groups of order eight[32]. Q has five conjugacy classes: $\{1\}$, $\{-1\}$, $\{\mathtt{i}, -\mathtt{i}\}$, $\{\mathtt{j}, -\mathtt{j}\}$, and $\{\mathtt{k}, -\mathtt{k}\}$. It has six subgroups, all of which are invariant subgroups:

$$\{1\} \quad , \quad \{1, -1\} \quad , \quad \{1, -1, \mathtt{i}, -\mathtt{i}\} \quad , \quad \{1, -1, \mathtt{j}, -\mathtt{j}\} \quad , \quad \{1, -1, \mathtt{k}, -\mathtt{k}\} \quad , \tag{1.43}$$

[31] Recall that the identity E is always its own conjugacy class.

[32] Hence if G is a nonabelian group of order eight, then either $G \cong D_4$ or $G \cong Q$.

as well as Q itself. The quaternion group can be faithfully represented in terms of the Pauli matrices, with $\mathtt{i} \to -i\sigma^x$, $\mathtt{j} \to -i\sigma^y$, and $\mathtt{k} \to -i\sigma^z$.

Incidentally, how do we know that $Q \ncong D_4$? Both groups have eight elements and both have five conjugacy classes! However, upon further inspection, Q has one element of order two (-1) and six of order four $(\pm\mathtt{i}, \pm\mathtt{j}, \pm\mathtt{k})$. D_4, on the other hand, has five elements of order two $(r^2, \sigma, \sigma r, \sigma r^2, \sigma r^3\}$ and two of order four (r, r^3). So the groups cannot have identical multiplication tables.

When we speak of *quaternions*, or of *quaternionic numbers*, we refer to an extension of complex numbers $z = x + iy$ to $h = a + \mathtt{i}b + \mathtt{j}c + \mathtt{k}d$, with $a, b, c, d \in \mathbb{R}$, and the set of quaternionic numbers is denoted $\mathbb{H}$. The quaternion algebra is not commutative! If $u = u_0 + \mathtt{i}u_1 + \mathtt{j}u_2 + \mathtt{k}u_3$ and $v = v_0 + \mathtt{i}v_1 + \mathtt{j}v_2 + \mathtt{k}v_3$, then representing these in terms of the Pauli matrices, $u = u_0 - i\boldsymbol{u}\cdot\boldsymbol{\sigma}$ and $v = v_0 - i\boldsymbol{v}\cdot\boldsymbol{\sigma}$, and therefore

$$\begin{aligned} uv &= (u_0 - i\boldsymbol{u}\cdot\boldsymbol{\sigma})(v_0 - i\boldsymbol{v}\cdot\boldsymbol{\sigma}) \\ &= u_0\, v_0 - \boldsymbol{u}\cdot\boldsymbol{v} - i(u_0\,\boldsymbol{v} + v_0\,\boldsymbol{u} - \boldsymbol{u}\times\boldsymbol{v})\cdot\boldsymbol{\sigma} \quad , \end{aligned} \tag{1.44}$$

which differs from vu whenever $\boldsymbol{u}\times\boldsymbol{v} \neq 0$. Hence multiplication is not commutative for quaternions. Complex conjugation of quaternions is defined as $h^* = a - \mathtt{i}b - \mathtt{j}c - \mathtt{k}d$. Note that $h^{**} = h$, which says that conjugation is its own inverse operation, as in the case of complex numbers (Mathy McMathstein says it this way: conjugation is an *involution*.) Note however that $(h_1 h_2)^* = h_2^*\, h_1^*$, *i.e.* the conjugate of a product of quaternions is the product of their conjugates, but in the reverse order. The norm of a quaternion is defined as

$$|h| = \sqrt{h^* h} = \sqrt{a^2 + b^2 + c^2 + d^2} \quad , \tag{1.45}$$

and the distance between two quaternions is accordingly $d(h_1, h_2) = |h_1 - h_2|$. The inverse of the quaterion $h = a + \mathtt{i}b + \mathtt{j}c + \mathtt{k}d$ is

$$h^{-1} = \frac{a - \mathtt{i}b - \mathtt{j}c - \mathtt{k}d}{a^2 + b^2 + c^2 + d^2} = \frac{h^*}{|h|^2} \quad . \tag{1.46}$$

Recall that the real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ are *fields*. A field is a set together with the operations of addition and multiplication such that both operations are individually commutative (*i.e.* $a + b = b + a$ and $ab = ba$), both operations are associative, both operations have identities and inverses, and that multiplication distributes over addition. Since multiplication within $\mathbb{H}$ is not commutative, $\mathbb{H}$ is not a field. Rather, Mathy McMathstein tells us, $\mathbb{H}$ is an *associative division algebra* over the real numbers.

A *unit quaternion* $u = \exp(-i\,\xi\,\hat{\boldsymbol{n}}\cdot\boldsymbol{\sigma}/2) = \cos(\xi/2) - i\sin(\xi/2)\,\hat{\boldsymbol{n}}\cdot\boldsymbol{\sigma}$ may be used to effect rotations. Define the quaternion $R = -i\boldsymbol{R}\cdot\boldsymbol{\sigma}$ with no constant component. Then one can show directly that

$$\begin{aligned} R' &= u\,R\,u^{-1} = -i\boldsymbol{R}'\cdot\boldsymbol{\sigma} \\ \boldsymbol{R}' &= \cos\xi\,\boldsymbol{R} + (1 - \cos\xi)\,(\hat{\boldsymbol{n}}\cdot\boldsymbol{R})\,\hat{\boldsymbol{n}} - \sin\xi\,\hat{\boldsymbol{n}}\times\boldsymbol{R} \end{aligned} \tag{1.47}$$

which is the rotation of $\boldsymbol{R}$ about $\hat{\boldsymbol{n}}$ by θ. Thus the algebra of $\mathsf{SO}(3)$ rotations is simply the algebra of unit quaternions!

True story: Alexander Hamilton invented quaternions while he was Treasury Secretary of the United States, and his quaternionic arithmetic proved so useful in reducing the computational effort involved in overseeing the Treasury Department that he was honored by having his portrait on the $10 bill[33].

[33] This is not a true story.

order	abelian G	nonabelian G	order	abelian G	nonabelian G
2	$\mathbb{Z}_2 \cong S_2 \cong D_1$	none	9	$\mathbb{Z}_3^2$, $\mathbb{Z}_9$	none
3	$\mathbb{Z}_3 \cong A_3$	none	10	$\mathbb{Z}_2 \times \mathbb{Z}_5$	D_5
4	$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$, $\mathbb{Z}_4$	none	11	$\mathbb{Z}_{11}$	none
5	$\mathbb{Z}_5$	none	12	$\mathbb{Z}_2^2 \times \mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Z}_4$	D_6 , A_4
6	$\mathbb{Z}_2 \times \mathbb{Z}_3$	S_3	13	$\mathbb{Z}_{13}$	none
7	$\mathbb{Z}_7$	none	14	$\mathbb{Z}_2 \times \mathbb{Z}_7$	D_7
8	$\mathbb{Z}_2^3$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_8$	D_4 ; Q	15	$\mathbb{Z}_3 \times \mathbb{Z}_5$	none

Table 1.5: Table of discrete groups up to order $|G| = 15$. Note that $Z_n \cong C_n$ and that $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ when p and q are relatively prime.

1.4.6 Group presentations

Tab. 1.5 lists all discrete groups up to order 15. Note that at order $|G| = 4$ there are two distinct groups, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$; the latter is also called the *Klein group*, V. Both are abelian, but $\mathbb{Z}_4$ is *not* the same group as $\mathbb{Z}_2 \times \mathbb{Z}_2$. These two groups have different multiplication tables. $\mathbb{Z}_4$ is generated by a single element r which satisfies $r^4 = 1$. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is generated by two elements σ and τ such that $\sigma^2 = \tau^2 = 1$ and $\sigma\tau = \tau\sigma$.

While $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$, it *is* the case that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Let's understand why this is the case. The group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is generated by two elements, σ and ω, where $\sigma^2 = \omega^3 = 1$ and $\sigma\omega = \omega\sigma$. Now define $r \equiv \sigma\omega$. Clearly the order of the element r is six, *i.e.* $r^6 = 1$. One can write $\sigma = r^3$ and $\omega = r^4$, as well as $\omega^2 = r^2$ and $\sigma\omega^2 = r^5$. That accounts for all the elements once we include the identity E. Similarly, $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$ and $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$. Can you see a generalization to cyclic groups whose order is a product of unique prime factors?

At order eight, there are three inequivalent abelian groups: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (*i.e.* $\mathbb{Z}_2^3$), $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_8$. $\mathbb{Z}_2^3$ is generated by elements (σ, τ, ρ) which all mutually commute and for which $\sigma^2 = \tau^2 = \rho^2 = 1$. $\mathbb{Z}_2 \times \mathbb{Z}_4$ is generated by (σ, δ) which mutually commute and which satisfy $\sigma^2 = \delta^4 = 1$. Finally, $\mathbb{Z}_8$ has a single generator r satisfying $r^8 = 1$.

Indeed, more economically than providing the full group multiplication table with its $|G|^2$ entries, a group can be defined by a *presentation* in which one specifies a set $\mathcal{G}$ of *generators* and a set $\mathfrak{R}$ of *relations* which the generators satisfy. We then say that the group G has the presentation $\langle\, \mathcal{G} \,|\, \mathfrak{R} \,\rangle$. The group elements are then given by all possible products of the generators, subject to the relations $\mathfrak{R}$. For example, the presentation for $C_n \cong \mathbb{Z}_n$ would be $\langle\, r \,|\, r^n = 1 \,\rangle$, which is usually abbreviated simply as $\langle\, r \,|\, r^n \,\rangle$. The dihedral group D_n has the presentation $\langle\, r, \sigma \,|\, r^n, \sigma^2, (r\sigma)^2 \,\rangle$. $\mathbb{Z}_2 \times \mathbb{Z}_4$ has the presentation $\langle\, \sigma, \delta \,|\, \sigma^2, \delta^4, \sigma\delta = \delta\sigma \,\rangle$. Note how in the last example we had to specify in $\mathfrak{R}$ that σ and δ commute.

While every group has a presentation, presentations are not necessarily unique. More examples are presented (hah!) in Tab. 1.6. The *free group* $F_{\mathcal{G}}$ on the set $\mathcal{G}$ of generators is simply all possible products. For example, if $\mathcal{G} = \{a, b\}$, $F_{\mathcal{G}}$ would be an infinite nonabelian group with elements

$$F_{\mathcal{G}} = \left\{ E, a, b, a^{-1}, b^{-1}, a^2, ab, ba, b^2, a^3, a^2b, aba, ba^2, \ldots \right\} \quad . \tag{1.48}$$

group	order	presentation	group	order	presentation
$\mathbb{Z}_n$	n	$\left\langle\, r \,\middle|\, r^n \,\right\rangle$	S_3	6	$\left\langle\, a,b \,\middle|\, a^2, b^3, (ab)^2 \,\right\rangle$
$\mathbb{Z}_m \times \mathbb{Z}_n$	mn	$\left\langle\, r,s \,\middle|\, r^m, s^n, rs=sr \,\right\rangle$	$T \cong A_4$	12	$\left\langle\, a,b \,\middle|\, a^2, b^3, (ab)^3 \,\right\rangle$
D_n	$2n$	$\left\langle\, r,\sigma \,\middle|\, r^n, \sigma^2, (r\sigma)^2 \,\right\rangle$	$O \cong S_4$	24	$\left\langle\, a,b \,\middle|\, a^2, b^3, (ab)^4 \,\right\rangle$
DC_n	$4n$	$\left\langle\, r,\sigma \,\middle|\, r^{2n}, r^n=\sigma^2, \sigma r \sigma^{-1} = r^{-1} \,\right\rangle$	$E \cong A_5$	60	$\left\langle\, a,b \,\middle|\, a^2, b^3, (ab)^5 \,\right\rangle$
Q	8	$\left\langle\, a,b \,\middle|\, aba=b\,, bab=a \,\right\rangle$	$\mathsf{SL}(2,\mathbb{Z})$	∞	$\left\langle\, a,b \,\middle|\, aba=bab, (aba)^4 \,\right\rangle$
Q_{16}	16	$\left\langle\, a,b,c \,\middle|\, a^4=b^2=c^2=abc \,\right\rangle$	$\mathsf{PSL}(2,\mathbb{Z})$	∞	$\left\langle\, a,b \,\middle|\, a^2, b^3 \,\right\rangle$
$\pi_1(S)$	∞	$\left\langle\, \{x_n,y_n\} \,\middle|\, \langle x_1,y_1\rangle \cdots \langle x_g,y_g\rangle \,\right\rangle$	$F_{\mathcal{G}}$	∞	$\left\langle\, \mathcal{G} \,\middle|\, \emptyset \,\right\rangle$

Table 1.6: Examples of discrete group presentations. DC_n is the *dicyclic group*, which is order $4n$. T, O, and E are the tetrahedral, octahedral (cubic), and icosahedral groups, respectively, which describe the rotational symmetries of those regular polyhedra. Q_{16} is the *generalized quaternion group*. $\pi_1(S)$ is the fundamental group of a surface of genus g, which is generated by $2g$ loops and $\langle \bullet, \bullet \rangle$ is the commutator.

Note that if G has presentation $\left\langle\, \mathcal{G} \,\middle|\, \mathfrak{R} \,\right\rangle$ and H has presentation $\left\langle\, \mathcal{H} \,\middle|\, \mathfrak{S} \,\right\rangle$, then the direct product $G \times H$ has presentation $\left\langle\, \mathcal{G}, \mathcal{H} \,\middle|\, \mathfrak{R}, \mathfrak{S}, [\mathcal{G}, \mathcal{H}] \,\right\rangle$. where $[\mathcal{G}, \mathcal{H}]$ signifies that all generators from the set $\mathcal{G}$ commute with all generators from the set $\mathcal{H}$. The *free product* $G \star H$ has presentation $\left\langle\, \mathcal{G}, \mathcal{H} \,\middle|\, \mathfrak{R}, \mathfrak{S} \,\right\rangle$. Thus, since the presentation of the dihedral group D_4 is $\left\langle\, r,\sigma \,\middle|\, r^4, \sigma^2, (r\sigma)^2 \,\right\rangle$, the presentation of $D_{4h} = D_4 \times \mathbb{Z}_2$ is

$$\left\langle\, r,\sigma,c \,\middle|\, r^4, \sigma^2, (r\sigma)^2, c^2, rc=cr, \sigma c = c\sigma \,\right\rangle \quad . \tag{1.49}$$

In the presentation for Q, $a = \mathtt{i}$ and $b = \mathtt{j}$. How can we show $a^4 = 1$? From $a = bab$ and $b = aba$, we have $a^2 = a(bab) = (aba)b = b^2$. Then $a^3 = a^2 a = b^2 a = b(bab)b^{-1} = bab^{-1}$. It follows that $a^4 = a(bab^{-1}) = (aba)b^{-1} = bb^{-1} = 1$, and of course $b^4 = (b^2)^2 = (a^2)^2 = a^4 = 1$ as well. Similarly, from the above presentation for Q_{16}, one can show that $a^4 = b^2 = c^2 = abc$ are all of order two, and an equivalent presentation is $\left\langle\, a,b \,\middle|\, a^4 = b^2 = abab \,\right\rangle$. Note that some groups have no finite presentation, but necessarily they must be of infinite order.

1.5 Lie Groups

1.5.1 Definition of a Lie group

Algebra and topology – two great tastes that taste great together! A *Lie group* is a *manifold*[34] G which is endowed with a group structure such that multiplication $G \times G \mapsto G : (g, g') \to gg'$ and inverse $G \mapsto G : g \to g^{-1}$ are smooth.

[34]There are two broad classifications of manifolds: *intake manifolds*, which distribute fuel and air to engine cylinders, and *exhaust manifolds*, which direct exhaust to the rear of the vehicle. Also a manifold is a topological space that is everywhere locally homeomorphic to $\mathbb{R}^n$ for some fixed integer n.

This definition is perhaps a bit too slick. Let's say we have a smooth manifold $\mathcal{M}$ and a map $g : \mathcal{M} \mapsto G$, where G is our Lie group. That is to say, the group operations consists of $\{g(x) \mid x \in \mathcal{M}\}$ where $g(x)\, g(y) = g(z)$ for some $z(x, y)$. Here x, y, and z are points on $\mathcal{M}$. There are two important axioms:

(i) *smoothness of group composition* : The function $z(x, y)$ is differentiable.

(ii) *smoothness of inverse* : The function $y = \psi(x)$, where $\big[g(x)\big]^{-1} = g(y)$, is differentiable.

As an example, consider the group $\mathsf{SL}(2, \mathbb{R})$, which is the set of real 2×2 matrices with determinant 1, also known as "the special linear group of rank two over the reals". Each element $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{SL}(2, \mathbb{R})$ can be parameterized by the three real numbers $\{a, b, c\}$, since $ad - bc = 1$ requires $d = (1 + bc)/a$. (A different parameterization much be chosen in the vicinity of $a = 0$.) $\mathsf{SL}(2, \mathbb{R})$ is an example of a *matrix group*. Other examples include $\mathsf{GL}(n, \mathbb{R})$ (real invertible $n \times n$ matrices), $\mathsf{O}(3)$ (rank three real orthogonal matrices), $\mathsf{Sp}(4, \mathbb{R})$ (rank four real symplectic matrices), $\mathsf{SU}(3) \times \mathsf{SU}(2) \times \mathsf{U}(1)$ (some contrived group the particle physicists seem to think is important - *as if !*), *etc.* See §1.3.8 above on $\mathsf{SU}(2)$.

Lie groups that are not matrix groups

It is quite convenient that every Lie group we will study is a matrix group, hence algebraically the only operations we will need are matrix multiplication and matrix inversion. The *metaplectic group* $\mathsf{Mp}(2n, \mathbb{R})$, which is a double cover of the symplectic group $\mathsf{Sp}(2n, \mathbb{R})$, is an example of a Lie group which is not a matrix group, but, truth be told, I have no idea what the hell I'm talking about here.

Hall[35] provides a concrete example of a Lie group which is not a matrix group:

$$G = \mathbb{R} \times \mathbb{R} \times S^2 = \Big\{ g \equiv (x, y, w) \,\Big|\, x \in \mathbb{R},\, y \in \mathbb{R},\, w \in S^1 \subset \mathbb{C} \Big\} \tag{1.50}$$

under the group operation $G \times G \mapsto G$ defined by

$$(x_1, y_1, w_1) \cdot (x_2, y_2, w_2) = (x_1 + x_2\,,\; y_1 + y_2\,,\; e^{i x_1 y_2}\, w_1 w_2) \quad . \tag{1.51}$$

Note that $w_{1,2}$ are expressed as unimodular complex numbers. The inverse operation is

$$g^{-1} = (-x\,,\; -y\,,\; e^{ixy} w) \quad . \tag{1.52}$$

One can check that G under the above multiplication law satisfies the axioms for a Lie Group. Yet it can be proven (see Hall, §4.8) that there is no continuous injective homomorphism of G into any $\mathsf{GL}(n, \mathbb{C})$, so G is not a matrix Lie group.

1.5.2 The big happy family of matrix Lie groups

First, a mathy definition:

[35] B. C. Hall, *Lie Groups, Lie Algebras, and their Representations*, 2nd edition, p. 25. (Henceforth "Hall".)

DEFINITION : A *matrix Lie group* is any subgroup G of $\mathsf{GL}(n,\mathbb{C})$ (*i.e.* complex invertible $n \times n$ matrices) such that if A_n is any sequence of matrices in G and A_n converges to some matrix A, then either $A \in G$ or A is noninvertible[36]. Thus, G is a closed subgroup of $\mathsf{GL}(n,\mathbb{C})$.

Perhaps the best way to appreciate the content of this definition is to provide some examples of subgroups of $\mathsf{GL}(n,\mathbb{C})$ which fail to be Lie groups[37]. Consider, for example the group G of all real $n \times n$ invertible matrices with all rational entries. Since the limit of a sequence of rational numbers may be irrational, this group is not a Lie group. Another example: let G be the set of 2×2 matrices of the form $M(\theta) = \mathsf{diag}\{e^{i\theta}, e^{i\theta\sqrt{2}}\}$ with $\theta \in \mathbb{R}$. Clearly the matrix $-1 \notin G$, since $e^{i\theta} = -1$ requires $\theta = (2n+1)\pi$, and since $(2n+1)\sqrt{2}\pi$ is not an odd multiple of π for any n. However, one can easily find a sequence of rationals of the form $(2k+1)/(2n+1)$ with converges to $\sqrt{2}$, so the corresponding sequence of matrices converges to an invertible matrix, -1, which is not in G.

Now let's meet the family:

- *General and special linear groups* : The Lie group $\mathsf{GL}(n,\mathbb{R})$ denotes the group of invertible $n \times n$ matrices A with real entries. It is a manifold of dimension n^2, corresponding to the number of real freedoms associated with a general $n \times n$ matrix[38]. Similarly, $\mathsf{GL}(n,\mathbb{C})$ is the group of invertible $n \times n$ matrices A with complex entries, of real dimension $2n^2$. One can also define the *quaternionic general linear group* $\mathsf{GL}(n,\mathbb{H})$ to be all invertible $n \times n$ matrices A with quaternionic entries. Its dimension is then $4n^2$.

  In each case, we can apply the further restriction that the determinant is $\det A = 1$. This imposes one real constraint on $\mathsf{GL}(n,\mathbb{R})$, resulting in the MLG $\mathsf{SL}(n,\mathbb{R})$, whose real dimension is $\dim \mathsf{SL}(n,\mathbb{R}) = n^2 - 1$. Applied to $\mathsf{GL}(n,\mathbb{C})$, the determinant condition amounts to one complex constraint, hence the real dimension is $\dim \mathsf{SL}(n,\mathbb{C}) = 2(n^2-1)$. For quaternionic matrices, $\det A = 1$ imposes four real constraints, so $\dim \mathsf{SL}(n,\mathbb{H}) = 4(n^2-1)$.

- *Orthogonal and special orthogonal groups* : The orthogonal group $\mathsf{O}(n)$ consists of all matrices $R \in \mathsf{GL}(n,\mathbb{R})$ such that $R^{\mathsf{T}}R = E$, where R^{T} denotes the matrix transpose of R, *i.e.* $R^{\dagger}_{ij} = R_{ji}$. Orthogonal transformations of vectors preserve the inner product $\langle \boldsymbol{x}|\boldsymbol{y}\rangle = \sum_i x_i\, y_i$, *i.e.* $\langle R\boldsymbol{x}|R\boldsymbol{y}\rangle = \langle \boldsymbol{x}|R^{\mathsf{T}}R|\boldsymbol{y}\rangle = \langle \boldsymbol{x}|\boldsymbol{y}\rangle$. Note that this entails $\det R = \pm 1$. Orthogonal matrices with $\det R = +1$ are known as *proper rotations*, while those with $\det R = -1$ are *improper rotations*. This distinction splits the $\mathsf{O}(n)$ into two disconnected components. One cannot continuously move throughout the group manifold of $\mathsf{O}(n)$ between a proper and an improper rotation. The special orthogonal group $\mathsf{SO}(n)$ consists of proper rotations only. Thus $\mathsf{SO}(n) \subset \mathsf{O}(n) \subset \mathsf{GL}(n,\mathbb{R})$.

  We can count the real dimension of $\mathsf{O}(n)$ by the following argument. The condition $R^{\mathsf{T}}R = E$ entails n constraints along the diagonal and $\frac{1}{2}n(n-1)$ constraints above the diagonal[39]. Thus, we have $\frac{1}{2}n(n+1)$ constraints on n^2 real numbers, and we conclude $\dim \mathsf{O}(n) = \dim \mathsf{SO}(n) = \frac{1}{2}n(n-1)$.

[36] Convergence of the matrix sequence $A_n \to A$ means that each matrix element of A_n converges to the corresponding element of A.

[37] Hall, ch. 1.

[38] The invertibility condition does not change the dimension.

[39] Since $R^{\mathsf{T}}R$ is symmetric by construction, there are no new conditions arising from those elements below the diagonal.

- *Generalized orthogonal groups* : The general orthogonal group $\mathsf{O}(n,k)$ is defined to be the subgroup of matrices $L \in \mathsf{GL}(n+k,\mathbb{R})$ such that $L^{\mathsf{T}} I_{n,k} L = I_{n,k}$, where

$$I_{n,k} = \begin{pmatrix} 1_{n\times n} & 0_{n\times k} \\ 0_{k\times n} & -1_{k\times k} \end{pmatrix} \quad . \tag{1.53}$$

  This is a generalization of the orthogonality condition, and one which preserves the metric

$$\langle \boldsymbol{x} | \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i \, y_i - \sum_{j=n+1}^{n+k} x_j \, y_j \quad . \tag{1.54}$$

  One can check that again one has $\det L = \pm 1$ and that $\dim \mathsf{O}(n,k) = \frac{1}{2}(n+k)(n+k-1)$. Perhaps the most famous example is the Lorentz group $\mathrm{O}(3,1)$. Whereas $\mathsf{O}(n)$ and $\mathsf{SO}(n)$ are *compact* Lie groups, $\mathsf{O}(n,k)$ is *noncompact* when $nk \neq 0$.

- *Unitary and special unitary groups* : The unitary group $\mathsf{U}(n)$ consists of all matrices $U \in \mathsf{GL}(n,\mathbb{C})$ such that $U^\dagger U = E$, where $U^\dagger$ denotes the Hermitian conjugate of U, *i.e.* $U^\dagger_{ij} = U^*_{ji}$. Unitary transformations of vectors preserve the complex inner product $\langle \boldsymbol{x} | \boldsymbol{y} \rangle = \sum_i x_i^* \, y_i$, which says that $\langle U\boldsymbol{x} | U\boldsymbol{y} \rangle = \langle \boldsymbol{x} | U^\dagger U | \boldsymbol{y} \rangle = \langle \boldsymbol{x} | \boldsymbol{y} \rangle$. Note that this entails $|\det U| = 1$, *i.e.* $\det U = e^{i\alpha}$ for some $\alpha \in [0, 2\pi)$. The special unitary group $\mathsf{SU}(n)$ consists of those $U \in \mathsf{U}(n)$ with $\det U = 1$. Thus we have $\mathsf{SU}(n) \subset \mathsf{U}(n) \subset \mathsf{GL}(n,\mathbb{C})$.

  Let's count the real dimension of $\mathsf{U}(n)$. The matrix $U^\dagger U$ is Hermitian by construction, so once again we total up the constraints associated with its diagonal and off-diagonal elements. Along the diagonal, we have n real constraints. Above the diagonal, we have $\frac{1}{2}n(n-1)$ complex constraints, which is equivalent to $n(n-1)$ real constraints. Thus, we have n^2 real constraints on n^2 complex elements of U, and we conclude that the real dimension of $\mathsf{U}(n)$ is $\dim \mathsf{U}(n) = n^2$. For $\mathsf{SU}(n)$, setting the determinant $\det U = 1$ adds one more real constraint (on the phase of $\det U$), and thus $\dim \mathsf{SU}(n) = n^2 - 1$.

  As with the orthogonal groups, we may generalize the unitary groups to

$$\mathsf{U}(n,k) = \left\{ U \in \mathsf{GL}(n,\mathbb{C}) \,|\, U^\dagger I_{n,k} \, U = I_{n,k} \right\} \tag{1.55}$$

  where $I_{n,k}$ is as defined in Eqn. 1.53.

- *Symplectic groups*[40] : Here we encounter a bit of an embarrassing mess, because the notation and definition for the different MLGs known as symplectic groups is inconsistent throughout the literature. The first symplectic MLG we shall speak of is $\mathsf{Sp}(2n,\mathbb{R})$, defined to be real matrices $M \in \mathsf{GL}(2n,\mathbb{R})$ which satisfy $M^{\mathsf{T}} J M = J$, where

$$J = \begin{pmatrix} 0_{n\times n} & 1_{n\times n} \\ -1_{n\times n} & 0_{n\times n} \end{pmatrix} \quad . \tag{1.56}$$

[40] Wikipedia tells us that the term "symplectic" was coined by Hermann Weyl in an effort to obviate a previous terminological confusion. It is a *calque* of the word "complex". A calque is a word-for-word or root-for-root translation of an expression imported from another language. The word "superconductor" is a calque from the Dutch *supergeleider*. "Thought experiment" of course calques the German *Gedankenexperiment*. "Rest in peace" calques the Latin *requiescat in pace*. Hilariously, French Canadian "chien chaud" calques English *hot dog*. Prior to Weyl, what we call today the symplectic group $\mathsf{Sp}(2n,\mathbb{R})$ was called the "line complex group". The English word "complex" comes from the Latin *com-plexus*, meaning "together braided". In Greek, this becomes $\sigma\upsilon\mu\pi\lambda\varepsilon\kappa\tau\iota\kappa\omega\varsigma$, or *sym-plektikos*.

Note that $J^2 = -E$. This is again a generalization of the orthogonality condition[41]. In counting the dimension of $\mathsf{Sp}(2n,\mathbb{R})$, note that $M^{\mathsf{T}}JM$ is a real, antisymmetric matrix of rank $2n$. There are then n^2 conditions on the upper right $n \times n$ block, and $\frac{1}{2}n(n-1)$ conditions on the above-diagonal elements in each of the upper left and lower right blocks, for a grand total of $n(2n-1)$ constraints on $4n^2$ elements, hence $\dim \mathsf{Sp}(2n,\mathbb{R}) = n(2n+1)$. At first sight, it might seem that $\det M = \pm 1$, but a nifty identity involving Pfaffians provides an further restriction. The *Pfaffian* of any antisymmetric matrix $B = -B^{\mathsf{T}}$ is defined as

$$\mathsf{Pf}\, B \equiv \frac{1}{2^n\, n!} \sum_{\sigma \in S_{2n}} \mathsf{sgn}(\sigma)\, B_{\sigma(1)\,\sigma(2)}\, B_{\sigma(3)\,\sigma(4)} \cdots B_{\sigma(2n-1)\,\sigma(2n)} \quad . \tag{1.57}$$

One can show that $\det B = (\mathsf{Pf}\, B)^2$. For our purposes, the following identity, which holds for any invertible matrix A, is very useful:

$$\mathsf{Pf}(A^{\mathsf{T}}JA) = (\det A)\,(\mathsf{Pf}\, J) \quad . \tag{1.58}$$

Setting $A = M \in \mathsf{Sp}(2n,\mathbb{R})$, we find $\det M = +1$. This says that symplectic matrices are both volume preserving as well as orientation preserving. Clearly any $M \in \mathsf{Sp}(2n,\mathbb{R})$ preserves the bilinear form $\langle \boldsymbol{x}|J|\boldsymbol{y}\rangle = \sum_{i=1}^{n}(x_i\, y_{i+n} - x_{i+n}\, y_i)$, where $\langle \boldsymbol{x}|\boldsymbol{y}\rangle$ is the usual Euclidean dot product:

$$\langle\, M\boldsymbol{x}\,|\,J\,|\,M\boldsymbol{y}\,\rangle = \langle\, \boldsymbol{x}\,|\,M^{\mathsf{T}}JM\,|\,\boldsymbol{y}\,\rangle = \langle\, \boldsymbol{x}\,|\,J\,|\,\boldsymbol{y}\,\rangle \quad . \tag{1.59}$$

The group $\mathsf{Sp}(2n,\mathbb{R})$ is noncompact. Note that we could reorder the row and column indices by interleaving each group and instead define J to consist of repeating 2×2 blocks $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ along its diagonal, *i.e.* $J_{ij} = +1$ if $(i,j) = (2l-1, 2l)$, and -1 if $(i,j) = (2l, 2l-1)$, and 0 otherwise.

The group $\mathsf{Sp}(2n,\mathbb{C})$ consists of all matrices $Z \in \mathsf{GL}(2n,\mathbb{C})$ satisfying $Z^{\mathsf{T}}JZ = J$. Note that it is still the matrix transpose and not the Hermitian conjugate which appears in the first term. $\mathsf{Sp}(2n,\mathbb{C})$, like $\mathsf{Sp}(2n,\mathbb{R})$, is noncompact. Counting constraints, we have n^2 complex degrees of freedom in the upper right $n \times n$ block of the complex antisymmetric matrix $Z^{\mathsf{T}}JZ$, and $\frac{1}{2}n(n-1)$ complex freedoms above the diagonal in each of the upper left and lower right blocks, for a total of $\mathsf{n}(2n-1)$ complex constraints on $4n^2$ complex entries in Z. Thus, the number of real degrees of freedom in $\mathsf{Sp}(2n,\mathbb{C})$ is $\dim \mathsf{Sp}(2n,\mathbb{C}) = 2n(2n+1)$, which is twice the dimension of $\mathsf{Sp}(2n,\mathbb{R})$.

There is also the group $\mathsf{Sp}(n) = \mathsf{Sp}(2n,\mathbb{C}) \cap \mathsf{U}(2n)$, sometimes denoted $\mathsf{USp}(2n)$[42], because it is isomorphic to the group of unitary symplectic matrices of rank $2n$. One also has $\mathsf{Sp}(n) \cong \mathsf{U}(n,\mathbb{H})$, the quaternionic unitary group of rank n. $\mathsf{Sp}(n)$ is compact and of real dimension $n(2n+1)$.

Finally, consider the group $\mathsf{G}(2n)$ defined by

$$\mathsf{G}(2n) = \left\{ M \in \mathsf{GL}(n,\mathbb{C}) \,|\, M^{\dagger}JM = J \right\} \quad , \tag{1.60}$$

[41] The notion of symplectic structure is strongly associated with Hamiltonian mechanics, where phase space is even-dimensional, consisting of n coordinates q_σ and n conjugate momenta p_σ. Defining the rank $2n$ vector $\boldsymbol{\xi}^{\mathsf{T}} = (\boldsymbol{q}^{\mathsf{T}}, \boldsymbol{p}^{\mathsf{T}})$, the equations of motion are $\dot{\xi}_j = J_{ij}\, \partial H/\partial \xi_j$. A canonical transformation to a new set of generalized coordinates and momenta $\boldsymbol{\Xi}$ must preserve this form of the equations of motion, which means that it must preserve the Poisson bracket $\{A,B\}_\xi = \sum_{i,j} J_{ij}(\partial A/\partial\xi_i)(\partial B/\partial\xi_j)$. Requiring $\{A,B\}_\xi = \{A,B\}_\Xi$ then entails $M^{\mathsf{T}}JM = J$, where $M_{ai} = \partial\Xi_a/\partial\xi_i$ is the Jacobian of the transformation.

[42] Note that if G and H are both Lie groups, then their intersection $G \cap H$ is also a Lie group.

which is the group of *conjugate symplectic matrices* of rank $2n$. If we define the unitary matrix

$$V \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1_{n\times n} & 1_{n\times n} \\ i1_{n\times n} & -i1_{n\times n} \end{pmatrix} \quad , \tag{1.61}$$

then we have that $V^\dagger J V = iI_{n,n}$. Thus, defining $\widetilde{M} = V^\dagger M V$, we have

$$\widetilde{M}^\dagger I_{n,n}\,\widetilde{M} = V^\dagger M^\dagger \big(V I_{n,n} V^\dagger\big) M V = V^\dagger M^\dagger \big(-iJ\big) M V = -iV^\dagger J V = I_{n,n} \quad , \tag{1.62}$$

which says that $\widetilde{M} \in \mathsf{U}(n,n)$. Thus we have that $\mathsf{G}(2n) \cong \mathsf{U}(n,n)$.

Again, do not be surprised if in the literature you find different notation. Sometimes $\mathsf{Sp}(2n,\mathbb{R})$ is abbreviated as $\mathsf{Sp}(2n)$, and sometimes even as $\mathsf{Sp}(n)$.

- *Euclidean and Poincaré groups* : The Euclidean group $\mathsf{E}(n)$ in n dimensions is the group of all bijective, distance-preserving automorphisms[43] of $\mathbb{R}^n$. It can be shown that any element $T \in \mathsf{E}(n)$ can be expressed as a rotation (proper or improper) followed by a translation. Thus each such T may be represented as a rank $n+1$ real matrix,

$$T \equiv (\boldsymbol{d}, R) = \begin{pmatrix} R & \boldsymbol{d} \\ \mathbf{0} & 1 \end{pmatrix} \quad , \tag{1.63}$$

where $R \in \mathsf{O}(n)$, $\boldsymbol{d} \in \mathbb{R}^n$ is an n-component column vector, and $\mathbf{0} = (0\,,\,\ldots\,,\,0)$ is an n-component row vector. Clearly $\dim \mathsf{E}(n) = \dim \mathsf{O}(n) + \dim \mathbb{R}^n = \frac{1}{2}n(n+1)$. Acting on the vector $\boldsymbol{v} \in \mathbb{R}^{n+1}$ whose transpose is $\boldsymbol{v}^{\mathsf{T}} = (x_1, \ldots, x_n, 1)$, one has

$$T\boldsymbol{v} = \begin{pmatrix} R & \boldsymbol{d} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ 1 \end{pmatrix} = \begin{pmatrix} R\boldsymbol{x} + \boldsymbol{d} \\ 1 \end{pmatrix} \quad , \tag{1.64}$$

Note that

$$T^{-1} = \begin{pmatrix} R^{-1} & -R^{-1}\boldsymbol{d} \\ \mathbf{0} & 1 \end{pmatrix} = (-R^{-1}\boldsymbol{d}, R^{-1}) \quad . \tag{1.65}$$

The group multiplication rule is

$$(\boldsymbol{d}_2, R_2)(\boldsymbol{d}_1, R_1) = \begin{pmatrix} R_2 & \boldsymbol{d}_2 \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} R_1 & \boldsymbol{d}_1 \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} R_2 R_1 & R_2\boldsymbol{d}_1 + \boldsymbol{d}_2 \\ \mathbf{0} & 1 \end{pmatrix} = (\boldsymbol{d}_2 + R_2\,\boldsymbol{d}_1, R_2\,R_1) \quad . \tag{1.66}$$

Note that $\mathsf{E}(n)$ is not simply a direct product of the orthogonal group $\mathsf{O}(n)$ and the group of translations $\mathbb{R}^n$ (under addition), because $(\boldsymbol{d}_2\,, R_2)(\boldsymbol{d}_1\,, R_1) \neq (\boldsymbol{d}_1 + \boldsymbol{d}_2, R_2\,R_1)$. Rather, we write $\mathsf{E}(n) = \mathbb{R}^n \rtimes \mathsf{O}(n)$, which says that the Euclidean group is a *semidirect product* of $\mathbb{R}^n$ and $\mathsf{O}(n)$ (see §1.5.3 below). Note that $\mathbb{R}^n \lhd \mathsf{E}(n)$, *i.e.* $\mathbb{R}^n$ is a normal subgroup, but $\mathsf{O}(n)$ is *not* a normal subgroup of $\mathsf{E}(n)$.

To define the Poincaré group $\mathsf{P}(n,1)$, simply increase the dimension to add a 'time' coordinate. A general element of $\mathsf{P}(n,1)$ is written

$$(\boldsymbol{d}, L) = \begin{pmatrix} L & \boldsymbol{d} \\ \mathbf{0} & 1 \end{pmatrix} \quad , \tag{1.67}$$

[43] An *endomorphism* is a map from a set to itself. An invertible endomorphism is called an automorphism.

where $L \in \mathsf{O}(n,1)$ and $\boldsymbol{d} \in \mathbb{R}^{n+1}$. The multiplication law is the same as that for $\mathsf{E}(n)$, and the Poincaré group also has a semidirect product structure: $\mathsf{P}(n,1) = \mathbb{R}^{n+1} \rtimes \mathsf{O}(n,1)$. Accordingly, $\dim \mathsf{P}(n,1) = \frac{1}{2}(n+1)(n+2)$.

- *Less common cases* : One can define the *complex orthogonal group* $\mathsf{O}(n,\mathbb{C})$ as the set of matrices $W \in \mathsf{GL}(n,\mathbb{C})$ such that $W^{\mathsf{T}}W = E$. This rarely arises in physical settings. Clearly $\det W = \pm 1$, and $\dim \mathsf{O}(n,\mathbb{C}) = n(n-1)$. One can then restrict $\mathsf{SO}(n,\mathbb{C})$ to those $W \in \mathsf{O}(n,\mathbb{C})$ with determinant one, with no further reduction in dimension. Personally I am not so sure that $\mathsf{O}(n,\mathbb{C})$ should be counted as part of our big happy family of matrix Lie groups. He's more like your weird hairy uncle who lives in your grandparents' basement apartment. We might include him, but only for tax purposes[44].

  The subset of all matrices $A \in \mathsf{GL}(n,\mathbb{R})$ with $A_{ij} = 0$ whenever $i > j$ is an abelian Lie group consisting of all real $n \times n$ upper triangular matrices. It is a good exercise to show how the inverse of any given element may be constructed. The *unitriangular group* $\mathsf{UT}(n,\mathbb{R})$ is defined to be the subgroup of $\mathsf{GL}(n,\mathbb{R})$ consisting of all matrices A for which $A_{ij} = 0$ whenever $i > j$ and $A_{ii} = 1$. That is, all the elements below the diagonal are 0, all the elements along the diagonal are 1, and all the elements above the diagonal are arbitrary real numbers.

1.5.3 More on semidirect products

Given a group G with a subgroup H and a normal subgroup $N \lhd G$, then $G = N \rtimes H$ if and only if $G = NH$ where $N \cap H = \{E\}$. This last condition is equivalent to requiring that for any $g \in G$, there exist unique $h \in H$ and $n \in N$ such that $g = nh$.[45] This may be taken as a definition of the semidirect product. Although this subsection is located within the material on Lie groups, the notion of semidirect product applies equally well to discrete groups. One can even form the semidirect product of a continuous group with a discrete group.

More generally, though, let G and K be groups, and let $\varphi : K \times G \to K$ with $(k,g) \to \varphi_g(k)$. The semidirect product $K \rtimes G$ with respect to φ is defined to be the set of elements (k,g) with $k \in K$ and $g \in G$ subject to the multiplication law

$$(k_2, g_2)\,(k_1, g_1) = \big(k_2\,\varphi_{g_2}(k_1)\,,\; g_2\,g_1\big) \quad . \tag{1.68}$$

One then has that $K \rtimes G$ satisfies the group axioms provided

$$\varphi_g(kk') = \varphi_g(k)\,\varphi_g(k') \qquad \text{and} \qquad \varphi_g\big(\varphi_{g'}(k)\big) = \varphi_{gg'}(k) \quad , \tag{1.69}$$

which are required for associativity of multiplication in $K \rtimes G$. Please note that there are *three* group multiplication laws in play here: (i) multiplication in G (*i.e.* gg'), (ii) multiplication in K (*i.e.* kk'), and (iii) multiplication in $K \rtimes G$ (*i.e.* Eqn. 1.69). Note also that $\varphi_g(k)\,\varphi_{g'}(k')$ is the K-product of two elements of K, *i.e.* $\varphi_g(k)$ and $\varphi_{g'}(k')$. In our example of $\mathsf{E}(n) = \mathbb{R}^n \rtimes \mathsf{O}(n)$, group multiplication in $K = \mathbb{R}^n$ is vector addition, group multiplication in $G = \mathsf{O}(n)$ is matrix multiplication, and the map φ is matrix-vector multiplication.

[44] $\mathsf{O}(n,\mathbb{C})$ is very different from $\mathsf{SU}(n)$. For starters, $\mathsf{O}(n,\mathbb{C})$ is not compact.

[45] Or that $g = hn$, for that matter – but generally with different h and n, than in the decomposition $g = nh$, of course!

Consider the semidirect product $G \equiv \mathbb{Z}_n \rtimes \mathbb{Z}_2$ where $\mathbb{Z}_n \cong \{E, r, \ldots, r^{n-1}\}$ with $r^n = E$ and $\mathbb{Z}_2 \cong \{E, \sigma\}$ with $\sigma^2 = E$. Now let $\varphi_\sigma(r^\ell) = \sigma r^\ell \sigma$ act by conjugation[46]. To completely define φ, we must specify the image of $\varphi_\sigma(r^\ell) = \sigma r^\ell \sigma$ in $\mathbb{Z}_n$ for each ℓ, and we choose $\sigma r^\ell \sigma = r^{n-\ell} = r^{-\ell}$. Now I claim that $G \cong D_n$, where the group isomorphism $\psi\, G \to D_n$ maps $(r^\ell, E) \in G$ to $r^\ell \in D_n$, and $(r^\ell, \sigma) \in G$ to $r^\ell \sigma \in D_n$. Thus, the semidirect product of two abelian groups may be nonabelian, depending on the features of the mapping φ.

1.5.4 Topology of the happy family

You already know that compact means "closed and bounded" in the context of subsets of $\mathbb{R}^n$, for example. The same criteria may be applied to matrix groups. A matrix Lie group G is compact if the following two conditions hold:

- If $A_n \in G$ is a sequence in G which converges to some matrix A, then $A \in G$.
- There exists a positive real number C such that, for any $A \in G$, $|A_{ij}| < C$ for all i, j.

The first condition says G is closed, and the second condition says it is bounded.

Two other terms that pop up in describing continuous spaces are *connected* and *simply connected*. A connected manifold is one where any two points may be joined by a continuous curve[47]. Any disconnected Lie group G may be uniquely decomposed into a union of its *components*. The component which contains the identity (there can be only one) is then a subgroup of G. The group $\mathsf{O}(n)$ is not connected, because there is no continuous path in the space of orthogonal matrices which connects a proper rotation and an improper rotation. Nor is $\mathsf{GL}(1, \mathbb{R})$, *i.e.* the group of nonzero real numbers under multiplication, because the two components $\mathbb{R}_+$ and $\mathbb{R}_-$ cannot be connected by a continuous path which goes not go through zero. Thus, $\mathsf{GL}(1, \mathbb{R})$ has two *components*, as does $\mathsf{O}(n)$. For the same reason, $\mathsf{GL}(n, \mathbb{R})$ is also disconnected and breaks up into components with positive and negative determinant. If $A(t)$ with $t \in [0, 1]$ is a smooth path in the space of $n \times n$ real matrices with $\det A(0) > 0$ and $\det A(1) < 0$, then by the intermediate value theorem there must be a $t^* \in [0, 1]$ for which $\det A(t^*) = 0$, which means $A(t^*) \notin \mathsf{GL}(n, \mathbb{R})$. Note that $\mathsf{GL}(n, \mathbb{C})$ is connected for all n, because the determinant is complex, and we can always choose a path connecting any two complex matrixes $A(0)$ and $A(1)$ which "goes around" the the set of matrices with $\det A = 0$.

A simply connected manifold is one where every closed curve can be continuously contracted to a point. The 2-sphere S^2 and the 2-torus T^2 are both connected, but S^2 is simply connected whereas T^2 is not, since a closed path which has net winding around either (or both) of the toroidal cycles cannot be continuously contracted to a point. The group of unimodular complex numbers under multiplication, $\mathsf{U}(1)$, is isomorphic to a circle S^1, with the identification of $z = e^{i\theta}$. Thus, it is the same group as the real numbers modulo 1 under addition. Clearly the MLG $\mathsf{U}(1)$ is connected, but it is not simply connected, since the path $z(t) = e^{2\pi i n t}$ for $t \in [0, 1]$ winds n times around the circle and is non-contractable.

[46] Note that $\sigma^{-1} = \sigma$.

[47] Topologists call this property *path connectedness* as opposed to connectedness *per se*, which is a somewhat weaker condition. But it turns out that a matrix Lie group is connected if and only if it is path connected.

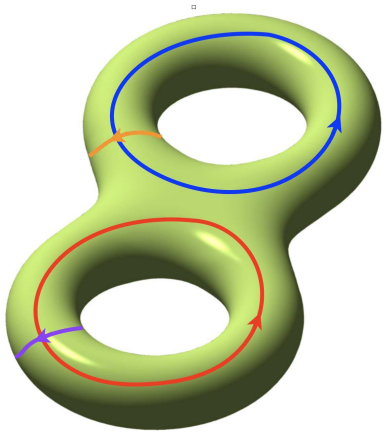

Figure 1.4: The double torus, with fundamental group generators a_1 (blue), b_1 (orange), a_2 (red), and b_2 (purple).

Continuous deformation of closed loops on any manifold $\mathcal{M}$ allows us to define equivalence classes of loops. Two loops are in the same equivalence class if they can be smoothly deformed into one another. These loop equivalence classes themselves form a group, where the group operation is defined by attaching loops to each other. The inverse of a given loop is that same loop executed in reverse. This group of loop equivalence classes is called the *fundamental group* (or *first homotopy group*) of the manifold, and is denoted $\pi_1(\mathcal{M})$. If $\mathcal{M}$ is simply connected, $\pi_1(\mathcal{M})$ is trivial. Else $\pi_1(\mathcal{M})$ may be either abelian or nonabelian. Clearly $\pi_1(S^1) \cong \mathbb{Z}$, as closed loops on the circle may be classified by their winding number, and paths of different winding number cannot be continuously deformed into one another. One has $\pi_1(T^2) \cong \mathbb{Z} \times \mathbb{Z}$, but the fundamental group of the *double torus*, which is to say a torus with an extra handle[48] (see Fig. 1.4), is an infinite nonabelian group with the presentation

$$\left\langle\, a_1, b_1, a_2, b_2 \,\middle|\, a_1\, b_1\, a_1^{-1}\, b_1^{-1}\, a_2\, b_2\, a_2^{-1}\, b_2^{-1} \,\right\rangle \quad . \tag{1.70}$$

One sometimes sees the notation $\pi_0(\mathcal{M})$, apparently denoting the "zeroth homotopy group" of $\mathcal{M}$. This is a misnomer, since $\pi_0(\mathcal{M})$ is not a group, but rather a set, corresponding to the connected components of $\mathcal{M}$. The order of this set is the number of connected components, and it is convenient to simply define $\pi_0(\mathcal{M})$ to be this number. Thus $\pi_0\big(\mathsf{O}(n)\big) = 2$, corresponding to the proper and improper rotations. Tab. 1.7 summarizes the topological properties of our happy family of matrix Lie groups[49].

Finally, consider the familiar case of $\mathsf{SO}(3)$, which consists of rotations in three dimensional Euclidean space by an angle ξ about an axis $\hat{\boldsymbol{n}} \in S^2$. Thus, each pair $(\xi, \hat{\boldsymbol{n}})$ labels an element $g(\xi, \hat{\boldsymbol{n}}) \in \mathsf{SO}(3)$. If we let $\xi \in [0, 2\pi)$, then we have $g(2\pi - \xi, -\hat{\boldsymbol{n}}) = g(\xi, \hat{\boldsymbol{n}})$, which means that points in the group manifold with $(\xi', \hat{\boldsymbol{n}}') = (2\pi - \xi, -\hat{\boldsymbol{n}})$ are *identified*. Now we might as well do away with all values of ξ greater than π, since they are all redundant labels, and take $\xi \in [0, \pi]$. The group manifold of $\mathsf{SO}(3)$ is then a solid sphere in $\mathbb{R}^3$ of radius π, with the following important distinction: antipodal points on the boundary are identified: $g(\pi, \hat{\boldsymbol{n}}) = g(\pi, -\hat{\boldsymbol{n}})$. This means that $\mathsf{SO}(3)$ is not simply connected, as shown in Fig.. 1.5.

[48] The double torus is a Riemann surface of genus $g = 2$. It resembles some sort of exotic breakfast pastry.

[49] A topologist, it is said, is someone who is unable to distinguish between a donut and a coffee cup.

G	compact?	$\pi_0(G)$	$\pi_1(G)$	G	compact?	$\pi_0(G)$	$\pi_1(G)$
$\mathsf{GL}(n,\mathbb{R})$	no	2	–	$\mathsf{GL}(n,\mathbb{C})$	no	1	$\mathbb{Z}$
$\mathsf{Sp}(2n,\mathbb{R})$	no	1	$\mathbb{Z}$	$\mathsf{Sp}(2n,\mathbb{C})$	no	2	–
$\mathsf{SL}(n,\mathbb{R})$ $(n \geq 3)$	no	1	$\mathbb{Z}_2$	$\mathsf{SL}(n,\mathbb{C})$	no	1	$\{1\}$
$\mathsf{SL}(2,\mathbb{R})$	no	1	$\mathbb{Z}$	$\mathsf{SO}(2)$	yes	1	$\mathbb{Z}$
$\mathsf{O}(n)$	yes	2	–	$\mathsf{SO}(n)$ $(n \geq 3)$	yes	1	$\mathbb{Z}_2$
$\mathsf{U}(n)$	yes	1	$\mathbb{Z}$	$\mathsf{SU}(n)$	yes	1	$\{1\}$
$\mathsf{Sp}(n)$	yes	1	$\{1\}$	$\mathsf{UT}(n,\mathbb{R})$	yes	1	$\{1\}$
$\mathsf{SO}(n,1)$	no	2	–	$\mathsf{O}(n,1)$	no	4	–
$\mathsf{E}(n)$	no	2	–	$\mathsf{P}(n,1)$	no	4	–

Table 1.7: Topological properties of matrix Lie groups.

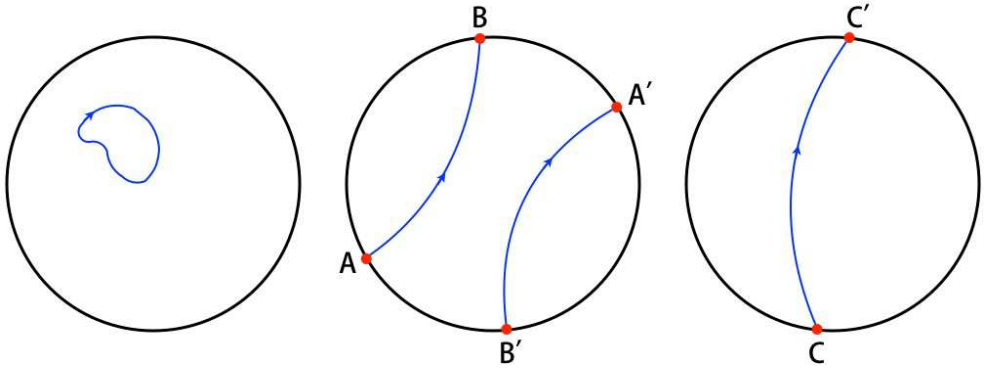

Figure 1.5: The fundamental group of $\mathsf{SO}(3)$ is $\mathbb{Z}_2$. Left: a contractible loop. Center: another contractible loop. Points A and A′ are identified, as are B and B′. If B is moved toward A along the boundary, then B′ moves toward A′. Right: a noncontractible loop. Points C and C′ are identified, and the blue path connecting them is a non-contractable loop. In all cases, the black sphere corresponds to group elements with $\xi = \pi$ and different values of $\hat{\boldsymbol{n}}$.

1.5.5 Matrix exponentials and the Lie algebra

Another mathy definition:

> DEFINITION : The *Lie algebra* $\mathfrak{g}$ of a matrix Lie group G is the set of all matrices X such that $\exp(tX) \in G$ for all $t \in \mathbb{R}$. Alternatively, $\mathfrak{g}$ is the *tangent space* to G at its identity E, *i.e.* the set of derivatives of all smooth curves in G passing through E.

I'm assuming you all know that the matrix exponential $\exp(X)$ is defined through its Taylor series, which is convergent for any real or complex matrix X. You should also know that for any matrix function $f(A)$ with a convergent power series expansion, one has

$$C^{-1} f\big(A\big)\, C = f\big(C^{-1} A\, C\big) \quad , \quad \big[f(A)\big]^{\mathsf{T}} = f\big(A^{\mathsf{T}}\big) \quad , \quad \big[f(A)\big]^{*} = f^{*}\big(A^{*}\big) \quad , \tag{1.71}$$

where $f^*(X)$ is defined by the same power series as $f(X)$, after complex conjugation of all the coefficients. In particular, the above are all true for $f(X) = \exp(X)$. Another handy True Fact is that for any nonsingular matrix A, $\ln \det A = \mathsf{Tr} \ln A$.

Warning! Physicists generally define the Lie algebra $\mathfrak{g}$ of G from the map $X \to \exp(-itX)$ rather than $X \to \exp(tX)$. We will hold by the math convention for now.

We now state three Important Facts about matrix Lie algebras:

(i) If $X, Y \in \mathfrak{g}$ then $\alpha X + \beta Y \in \mathfrak{g}$ where α and β are scalars in some field $\mathbb{F}$.

(ii) If $X, Y \in \mathfrak{g}$ then $[X, Y] = XY - YX \in \mathfrak{g}$.

(iii) The Jacobi identity holds for all $X, Y, Z \in \mathfrak{g}$:

$$\big[X, [Y, Z]\big] + \big[Y, [Z, X]\big] + \big[Z, [X, Y]\big] = 0 \quad . \tag{1.72}$$

We won't prove any of these[50]. The first says that $\mathfrak{g}$ is a vector space over the field $\mathbb{F}$. The second introduces the *Lie bracket* $[\bullet, \bullet]$, known to us physicists as the commutator, and says that $\mathfrak{g}$ is closed under the bracket. The third follows from the definition of the Lie bracket[51].

To provide some motivation to the second Important Fact, consider the product $e^X e^Y$ using Dynkin's expression of the Baker-Campbell-Hausdorff (BCH) formula[52],

$$\ln\left(e^X e^Y\right) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \sum_{\substack{r_1, s_1 \\ r_1 + s_1 > 0}} \cdots \sum_{\substack{r_n, s_n \\ r_n + s_n > 0}} \frac{\big[X^{r_1} Y^{s_1} X^{r_2} Y^{s_2} \cdots X^{r_n} Y^{s_n}\big]}{\sum_{i=1}^n (r_i + s_i) \cdot \prod_{j=1}^n r_j!\, s_j!} \quad , \tag{1.73}$$

where

$$\big[X^{r_1} Y^{s_1} X^{r_2} Y^{s_2} \cdots X^{r_n} Y^{s_n}\big] = \underbrace{[X, [X, \cdots [X}_{r_1}, \underbrace{[Y, [Y, \cdots [Y}_{s_1}, \cdots \underbrace{[X, [X, \cdots [X}_{r_n}, \underbrace{[Y, [Y, \cdots [Y}_{s_n}]] \cdots]] \quad . \tag{1.74}$$

Thus,

$$\exp(X)\, \exp(Y) = \exp\left(X + Y + \tfrac{1}{2}\big[X, Y\big] + \tfrac{1}{12}\big[X, \big[X, Y\big]\big] + \tfrac{1}{12}\big[Y, \big[Y, X\big]\big] + \ldots \right) \quad . \tag{1.75}$$

Notice that every term inside the round bracket on the RHS, other than $X + Y$, is formed from nested commutators. Thus if $[X, Y] \in \mathfrak{g}$ for all $X, Y \in \mathfrak{g}$, then the product $e^X e^Y = e^Z$ with $Z \in \mathfrak{g}$.

[50] See Hall §3.3 for the proofs.

[51] The formal definition of a finite-dimensional real/complex Lie algebra is a finite-dimensional real/complex vector space $\mathfrak{g}$ together with a map $[\bullet, \bullet]$ from $\mathfrak{g} \times \mathfrak{g}$ into $\mathfrak{g}$ called the *Lie bracket*, such that (i) $[\bullet, \bullet]$ is bilinear, (ii) $[X, Y] = -[Y, X]$ for all $X, Y \in \mathfrak{g}$, and (iii) $\big[X, [Y, Z]\big] + \big[Y, [Z, X]\big] + \big[Z, [X, Y]\big]$ for all $X, Y, Z \in \mathfrak{g}$. For Lie algebras of matrix Lie groups, the Lie bracket is the commutator.

[52] See https://en.wikipedia.org/wiki/Baker-Campbell-Hausdorff_formula.

Why should we care about Lie algebras?

Why are we interested in Lie algebras to begin with? Aren't their corresponding Lie groups enough? One reason is that Lie algebras describe the *infinitesimal form* of continuous symmetries[53]. A Lie algebra $\mathfrak{g}$ is the *linearization* of a Lie group G. In this sense, Lie algebras are *much simpler* than Lie groups because they describe only the latter's tangent space in the vicinity of its identity. Mathematically, Lie groups are homogeneous structures in which any given point *locally* "looks like" any other point: if g is in the neighborhood of g_0, then $h \equiv g g_0^{-1} h_0$ is in the neighborhood of h_0[54]. Thus, from an understanding of $\mathfrak{g}$, we can deduce *almost* all the properties of G itself[55]. The inverse of linearization, which takes us from $\mathfrak{g}$ to G, is the exponential map. Since algebras are vector spaces, we may apply in the study of Lie algebras many of the powerful tools of linear algebra, such as basis vectors and inner products. For two infinitesimal group operations $g = e^{\epsilon X}$ and $h = e^{\epsilon Y}$, their product is $gh = e^{\epsilon(X+Y)+\mathcal{O}(\epsilon^2)}$. Thus, group composition of two elements in the vicinity of the identity corresponds to simple vector addition in the Lie algebra! However, when we evaluate the group commutator $\langle g, h\rangle = g^{-1}h^{-1}gh$, we find that the $\mathcal{O}(\epsilon)$ term vanishes, and

$$e^{-\epsilon X} e^{-\epsilon Y} e^{\epsilon X} e^{\epsilon Y} = \exp\left(\epsilon^2 [X, Y] + \mathcal{O}(\epsilon^3)\right) \quad . \tag{1.76}$$

Thus consideration of the infinitesimal group commutator $\langle \bullet, \bullet \rangle$ requires the introduction of additional structure in the linear vector space of $\mathfrak{g}$, *i.e.* the notion of the Lie bracket.

Some concrete examples of Lie algebras

$\mathsf{GL}(n, \mathbb{R})$: The Lie algebra $\mathsf{gl}(n, \mathbb{R})$ is the set of all real $n \times n$ matrices. Similarly, $\mathsf{gl}(n, \mathbb{C})$ is the set of all complex $n \times n$ matrices.

$\mathsf{SL}(n, \mathbb{R})$: Adding the determinant condition puts a restriction on $\mathsf{sl}(n, \mathbb{R})$, namely that $\det \exp(tX) = 1$. Taking the logarithm, we obtain the condition $\mathsf{Tr}\, X = 0$. Hence $\mathsf{sl}(n, \mathbb{R})$ is the set of all real traceless $n \times n$ matrices. And of course $\mathsf{sl}(n, \mathbb{C})$ is the set of all complex traceless $n \times n$ matrices.

$\mathsf{O}(n)$: Now we demand $\exp(tX^{\mathsf{T}})\, \exp(tX) = E$, hence $\exp(tX^{\mathsf{T}}) = \exp(-tX)$. Taking the logarithm, we obtain $X^{\mathsf{T}} = -X$. Thus, $\mathsf{o}(n)$ is the set of all real antisymmetric $n \times n$ matrices. This is easy!

$\mathsf{U}(n)$: *Mutatis mutandis*, $\mathsf{u}(n)$ consists of the set of complex antihermitian $n \times n$ matrices, *i.e.* matrices A for which $A_{ji} = -A^*_{ij}$.

$\mathsf{Sp}(2n, \mathbb{R})$: We require $\exp(tX^{\mathsf{T}})\, J \exp(tX) = J$. Multiplying on the right by $-\exp(-tX)\, J$, we obtain $\exp(tX^{\mathsf{T}}) = -J \exp(-tX) J = \exp(tJXJ)$, since $J^{-1} = -J$. Thus, we arrive at the condition $X^{\mathsf{T}} = JXJ$ for any real $n \times n$ matrix $X \in \mathsf{sp}(2n, \mathbb{R})$. It is straightforward to show that this means X is of the form

$$X = \begin{pmatrix} A & B \\ C & -A^{\mathsf{T}} \end{pmatrix} \quad , \tag{1.77}$$

[53] In physics, much useful information is deduced from the consideration of infinitesimal continuous symmetries. For example, the existence of conserved currents via Noether's theorem.

[54] For this reason, the properties of the neighborhood of any point in G are reduced to a study of the properties of the neighborhood of E, which is to say the Lie algebra $\mathfrak{g}$ of G.

[55] One obvious thing we can't infer from $\mathfrak{g}$ is whether G has any disconnected parts. The Lie algebras corresponding to $\mathsf{O}(n)$ and $\mathsf{SO}(n)$ are both $\mathsf{o}(n)$.

where A is an arbitrary $n \times n$ matrix, and $B = B^{\mathsf{T}}$ and $C = C^{\mathsf{T}}$ are arbitrary symmetric $n \times n$ matrices. The same conditions hold for any complex $n \times n$ matrix $X \in \mathsf{sp}(2n, \mathbb{C})$. Finally, we may conclude $\mathsf{sp}(n) = \mathsf{sp}(2n, \mathbb{C}) \cap \mathsf{u}(2n)$.

1.5.6 Structure constants

We noted above that the Lie algebra $\mathfrak{g}$ of a matrix Lie group G is the set of all smooth curves in G passing through the identity E. Consider, for example, the group $\mathsf{SL}(2, \mathbb{R})$, which is of real dimension three. In the vicinity of the identity, we can write

$$g(x^1, x^2, x^3) = \begin{pmatrix} 1 + x^1 & x^2 \\ x^3 & \frac{1+x^2x^3}{1+x^1} \end{pmatrix} \quad . \tag{1.78}$$

One can check by inspection that $\det g(x^1, x^2, x^3) = 1$ and that $g(0, 0, 0) = E$. Now expand in the three local coordinates $\{x^1, x^2, x^3\}$:

$$\begin{aligned} g(x^1, x^2, x^3) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} x^1 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x^2 + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} x^3 + \mathcal{O}(x^2) \\ &\equiv E + \sum_{a=1}^{3} x^a \, X_a + \mathcal{O}(x^2) \quad , \end{aligned} \tag{1.79}$$

where

$$X_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad , \quad X_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad , \quad X_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tag{1.80}$$

are a set of *generators* for the Lie algebra $\mathsf{sl}(2, \mathbb{R})$ which may be taken as *basis vectors* in the vector space of that algebra. Note in general that if $\{X_a\}$ are taken as a set of basis vectors for some Lie algebra $\mathfrak{g}$ that we may write $\exp(x^a X_a) \exp(y^a X_a) = \exp(z^a X_a)$, where $z = z(x, y)$, which follows from Dynkin's version of BCH.

Can we reconstruct the Lie group G from its Lie algebra $\mathfrak{g}$? Not always. By employing exponentiation, we can form the group consisting of all matrices of the form $\exp(x^a X_a)$ (note summation convention here). For $\mathsf{sl}(n, \mathbb{R})$, there are a total of $n^2 - 1$ generators, and via exponentiation we can indeed reconstruct all of $\mathsf{SL}(n, \mathbb{R})$. But suppose we try to do this with $\mathsf{o}(n)$ and $\mathsf{O}(n)$. In that case the generators are a $\frac{1}{2}n(n-1)$ element basis of real traceless antisymmetric matrices, hence $\det \exp(x^a X_a) = 1$, and we are missing the improper rotations. So via exponentiation, we can in general only reconstruct from $\mathfrak{g}$ alone the component of G which contains the identity E.

Since each Lie algebra $\mathfrak{g}$ is closed under the action of the Lie bracket (commutation), the generators X_a must satisfy

$$\big[X_a, X_b\big] = C_{ab}{}^c \, X_c \quad , \tag{1.81}$$

for some sets of numbers $C_{ab}{}^c$, which are called the *structure constants* of the Lie algebra. Note that $C_{ab}{}^c = -C_{ba}{}^c$ owing to the antisymmetry of the Lie bracket. Taking, for example, the three generators of $\mathsf{sl}(2, \mathbb{R})$ from Eqn. 1.80, one finds $\big[X_1, X_2\big] = 2X_2$, $\big[X_1, X_3\big] = -2X_3$, and $\big[X_2, X_3\big] = X_1$. Thus $C_{12}{}^2 = -C_{21}{}^2 = 2$, $C_{13}{}^3 = -C_{31}{}^3 = -2$, and $C_{23}{}^1 = -C_{32}{}^1 = 1$, with all other $C_c^{ab} = 0$. Again, in the

physics literature one generally finds this written as $\big[T^a, T^b\big] = i f_{ab}{}^c\, T^c$ for the generators $\{T^a\}$, where $X_a = -iT^a$ and $f_{ab}{}^c = C_{ab}{}^c$.

Since $\mathfrak{g}$ is a vector space, any complete and linearly independent set of generators will do. For example, we could have chosen

$$X_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad , \quad X_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad , \quad X_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad , \tag{1.82}$$

in which case one finds the nonzero structure constants $C_{12}{}^3 = 2$, $C_{13}{}^2 = -2$, and $C_{32}{}^1 = -2$. In addition, we could have multiplied each of the generators by an arbitrary nonzero scale factor, with corresponding consequences for the $C_{ab}{}^c$. One way to mitigate this ambiguity is to choose a normalization condition for the generators, such as

$$\mathsf{Tr}\big(X_a X_b\big) = \lambda_a\, \delta^{ab} \quad \text{(no sum)} \quad . \tag{1.83}$$

If the Lie algebra is *semisimple*, one can further restrict $|\lambda_a| = 1$ for all a, but we cannot change the sign of any of the λ_a.

One last tidbit: As a consequence of the Jacobi identity, the structure constants obey the relation

$$C_{bc}{}^d\, C_{da}{}^e + C_{ab}{}^d\, C_{dc}{}^e + C_{ca}{}^d\, C_{db}{}^e = 0 \quad . \tag{1.84}$$

Thus, if we define the matrices $X_{ab}{}^c \equiv -C_{ab}{}^c$, Eqn. 1.84 may be written as

$$-\,X_{bc}{}^d\, X_{ad}{}^e - C_{ab}{}^d\, X_{dc}{}^e + X_{ac}{}^d\, X_{bd}{}^e = 0 \quad , \tag{1.85}$$

which says $\big[X_a, X_b\big]_{ce} = C_{ab}{}^d\, \big(X_d\big)_{ce}$, *i.e.* $\big[X_a, X_b\big] = C_{ab}{}^c\, X_c$. In other words, the structure constants themselves generate a representation of the algebra, called the *adjoint representation*. For example, if we choose the structure constants computed from Eqn. 1.82, we obtain the 3×3 representation

$$X_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 2 & 0 \end{pmatrix} \quad , \quad X_2 = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{pmatrix} \quad , \quad X_3 = \begin{pmatrix} 0 & -2 & 0 \\ -2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad . \tag{1.86}$$

One can then check $\big[X_a, X_b\big] = C_{ab}{}^c\, X_c$.

1.6 Appendix : Ideal Bose Gas Condensation

We begin with the grand canonical Hamiltonian $K = H - \mu N$ for the ideal Bose gas,

$$K = \sum_{\boldsymbol{k}} (\varepsilon_{\boldsymbol{k}} - \mu)\, b^\dagger_{\boldsymbol{k}} b_{\boldsymbol{k}} - \sqrt{N} \sum_{\boldsymbol{k}} \left(\nu_{\boldsymbol{k}}\, b^\dagger_{\boldsymbol{k}} + \bar\nu_{\boldsymbol{k}}\, b_{\boldsymbol{k}} \right) \quad . \tag{1.87}$$

Here $b^\dagger_{\boldsymbol{k}}$ is the creation operator for a boson in a state of wavevector $\boldsymbol{k}$, hence $\big[b_{\boldsymbol{k}}\,,\, b^\dagger_{\boldsymbol{k}'}\big] = \delta_{\boldsymbol{k}\boldsymbol{k}'}$. The dispersion relation is given by the function $\varepsilon_{\boldsymbol{k}}$, which is the energy of a particle with wavevector $\boldsymbol{k}$. We must have $\varepsilon_{\boldsymbol{k}} - \mu \geq 0$ for all $\boldsymbol{k}$, lest the spectrum of K be unbounded from below. The fields $\{\nu_{\boldsymbol{k}}, \bar\nu_{\boldsymbol{k}}\}$ break a global $\mathsf{O}(2)$ symmetry.

Students who have not taken a course in solid state physics can skip the following paragraph, and be aware that $N = V/v_0$ is the total volume of the system in units of a fundamental "unit cell" volume v_0. The thermodynamic limit is then $N \to \infty$. Note that N is not the boson particle number, which we'll call N_b.

Solid state physics boilerplate : We presume a setting in which the real space Hamiltonian is defined by some boson hopping model on a Bravais lattice. The wavevectors $\boldsymbol{k}$ are then restricted to the first Brillouin zone, $\hat{\Omega}$, and assuming periodic boundary conditions are quantized according to the condition $\exp\bigl(iN_l\,\boldsymbol{k}\cdot\boldsymbol{a}_l\bigr) = 1$ for all $l \in \{1,\ldots,d\}$, where $\boldsymbol{a}_l$ is the $l^{\rm th}$ fundamental direct lattice vector and N_l is the size of the system in the $\boldsymbol{a}_l$ direction; d is the dimension of space. The total number of unit cells is $N \equiv \prod_l N_l$. Thus, quantization entails $\boldsymbol{k} = \sum_l (2\pi n_l/N_l)\,\boldsymbol{b}_l$, where $\boldsymbol{b}_l$ is the $l^{\rm th}$ elementary reciprocal lattice vector ($\boldsymbol{a}_l\cdot\boldsymbol{b}_{l'} = 2\pi\delta_{ll'}$) and n_l ranges over N_l distinct integers such that the allowed $\boldsymbol{k}$ points form a discrete approximation to $\hat{\Omega}$.

To solve, we first shift the boson creation and annihilation operators, writing

$$K = \sum_{\boldsymbol{k}} (\varepsilon_{\boldsymbol{k}} - \mu)\,\beta^\dagger_{\boldsymbol{k}}\beta_{\boldsymbol{k}} - N\sum_{\boldsymbol{k}} \frac{|\nu_{\boldsymbol{k}}|^2}{\varepsilon_{\boldsymbol{k}}-\mu} \quad , \tag{1.88}$$

where

$$\beta_{\boldsymbol{k}} = b_{\boldsymbol{k}} - \frac{\sqrt{N}\,\nu_{\boldsymbol{k}}}{\varepsilon_{\boldsymbol{k}}-\mu} \qquad , \qquad \beta^\dagger_{\boldsymbol{k}} = b^\dagger_{\boldsymbol{k}} - \frac{\sqrt{N}\,\bar{\nu}_{\boldsymbol{k}}}{\varepsilon_{\boldsymbol{k}}-\mu} \quad . \tag{1.89}$$

Note that $\bigl[\beta_{\boldsymbol{k}}\,,\,\beta^\dagger_{\boldsymbol{k}'}\bigr] = \delta_{\boldsymbol{k}\boldsymbol{k}'}$ so the above transformation is canonical. The Landau free energy $\Omega = -k_{\rm B}T\ln\Xi$, where $\Xi = {\rm Tr}\, e^{-K/k_{\rm B}T}$, is given by

$$\Omega = Nk_{\rm B}T\int\limits_{-\infty}^{\infty} d\varepsilon\; g(\varepsilon)\;\ln\bigl(1 - e^{(\mu-\varepsilon)/k_{\rm b}T}\bigr) - N\sum_{\boldsymbol{k}}\frac{|\nu_{\boldsymbol{k}}|^2}{\varepsilon_{\boldsymbol{k}}-\mu} \quad , \tag{1.90}$$

where $g(\varepsilon)$ is the density of energy states per unit cell,

$$g(\varepsilon) = \frac{1}{N}\sum_{\boldsymbol{k}}\delta\bigl(\varepsilon-\varepsilon_{\boldsymbol{k}}\bigr) \xrightarrow[N\to\infty]{} v_0\int\limits_{\hat{\Omega}}\frac{d^dk}{(2\pi)^d}\,\delta\bigl(\varepsilon-\varepsilon_{\boldsymbol{k}}\bigr) \quad . \tag{1.91}$$

Note that

$$\psi_{\boldsymbol{k}} \equiv \frac{1}{\sqrt{N}}\,\bigl\langle b_{\boldsymbol{k}}\bigr\rangle = -\frac{1}{N}\,\frac{\partial\Omega}{\partial\bar{\nu}_{\boldsymbol{k}}} = \frac{\nu_{\boldsymbol{k}}}{\varepsilon_{\boldsymbol{k}}-\mu} \quad . \tag{1.92}$$

In the condensed phase, $\psi_{\boldsymbol{k}}$ is nonzero.

The Landau free energy (grand potential) is a function $\Omega(T,N,\mu,\nu,\bar{\nu})$. We now make a Legendre transformation,

$$Y(T,N,\mu,\psi,\bar{\psi}) = \Omega(T,N,\mu,\nu,\bar{\nu}) + N\sum_{\boldsymbol{k}}\bigl(\nu_{\boldsymbol{k}}\bar{\psi}_{\boldsymbol{k}} + \bar{\nu}_{\boldsymbol{k}}\psi_{\boldsymbol{k}}\bigr) \quad . \tag{1.93}$$

Note that

$$\frac{\partial Y}{\partial\bar{\nu}_{\boldsymbol{k}}} = \frac{\partial\Omega}{\partial\bar{\nu}_{\boldsymbol{k}}} + N\psi_{\boldsymbol{k}} = 0 \quad , \tag{1.94}$$

by the definition of $\psi_{\boldsymbol{k}}$. Similarly, $\partial Y/\partial\nu_{\boldsymbol{k}} = 0$. We now have

$$Y(T,N,\mu,\psi,\bar\psi) = Nk_{\rm B}T\int\limits_{-\infty}^{\infty}\!\!d\varepsilon\; g(\varepsilon)\;\ln\left(1-e^{(\mu-\varepsilon)/k_{\rm b}T}\right) + N\sum_{\boldsymbol{k}}(\varepsilon_{\boldsymbol{k}}-\mu)\,|\psi_{\boldsymbol{k}}|^2 \quad . \tag{1.95}$$

Therefore, the boson particle number per unit cell is given by the *dimensionless density*,

$$n = \frac{N_b}{N} = -\frac{1}{N}\frac{\partial Y}{\partial\mu} = \sum_{\boldsymbol{k}}|\psi_{\boldsymbol{k}}|^2 + \int\limits_{-\infty}^{\infty}\!\!d\varepsilon\;\frac{g(\varepsilon)}{e^{(\varepsilon-\mu)/k_{\rm B}T}-1} \quad , \tag{1.96}$$

and the relation between the condensate amplitude $\psi_{\boldsymbol{k}}$ and the field $\nu_{\boldsymbol{k}}$ is given by

$$\nu_{\boldsymbol{k}} = \frac{1}{N}\frac{\partial Y}{\partial\bar\psi_{\boldsymbol{k}}} = (\varepsilon_{\boldsymbol{k}}-\mu)\,\psi_{\boldsymbol{k}} \quad . \tag{1.97}$$

Recall that $\nu_{\boldsymbol{k}}$ acts as an external field. Let the dispersion $\varepsilon_{\boldsymbol{k}}$ be minimized at $\boldsymbol{k} = \boldsymbol{K}$. Without loss of generality, we may assume this minimum value is $\varepsilon_{\boldsymbol{K}} = 0$. We see that if $\nu_{\boldsymbol{k}} = 0$ then one of two must be true:

(i) $\psi_{\boldsymbol{k}} = 0$ for all $\boldsymbol{k}$

(ii) $\mu = \varepsilon_{\boldsymbol{K}}$, in which case $\psi_{\boldsymbol{K}}$ can be nonzero.

Thus, for $\nu = \bar\nu = 0$ and $\mu > 0$, we have the usual equation of state,

$$n(T,\mu) = \int\limits_{-\infty}^{\infty}\!\!d\varepsilon\;\frac{g(\varepsilon)}{e^{(\varepsilon-\mu)/k_{\rm B}T}-1} \quad , \tag{1.98}$$

which relates the intensive variables n, T, and μ. When $\mu = 0$, the equation of state becomes

$$n(T,\mu=0) = \overbrace{\sum_{\boldsymbol{K}}|\psi_{\boldsymbol{K}}|^2}^{n_0} + \overbrace{\int\limits_{-\infty}^{\infty}\!\!d\varepsilon\;\frac{g(\varepsilon)}{e^{\varepsilon/k_{\rm B}T}-1}}^{n_>(T)} \quad , \tag{1.99}$$

where now the sum is over only those $\boldsymbol{K}$ for which $\varepsilon_{\boldsymbol{K}} = 0$. Typically this set has only one member, $\boldsymbol{K} = 0$, but it is quite possible, due to symmetry reasons, that there are more such $\boldsymbol{K}$ values. This last equation of state is one which relates the intensive variables n, T, and n_0, where

$$n_0 = \sum_{\boldsymbol{K}}|\psi_{\boldsymbol{K}}|^2 \tag{1.100}$$

is the dimensionless condensate density. If the integral $n_>(T)$ in Eqn. 1.99 is finite, then for $n > n_0(T)$ we must have $n_0 > 0$. Note that, for any T, $n_>(T)$ diverges logarithmically whenever $g(0)$ is finite. This means that Eqn. 1.98 can always be inverted to yield a finite $\mu(n,T)$, no matter how large the value of n,

in which case there is no condensation and $n_0 = 0$. If $g(\varepsilon) \propto \varepsilon^\alpha$ with $\alpha > 0$, the integral converges and $n_>(T)$ is finite and monotonically increasing for all T. Thus, for fixed dimensionless number n, there will be a *critical temperature* $T_{\rm c}$ for which $n = n_>(T_{\rm c})$. For $T < T_{\rm c}$, Eqn. 1.98 has no solution for any μ and we must appeal to eqn. 1.99. The condensate density, given by $n_0(n,T) = n - n_>(T)$, is then finite for $T < T_{\rm c}$, and vanishes for $T \geq T_{\rm c}$.

In the condensed phase, the phase of the order parameter ψ inherits its phase from the external field ν, which is taken to zero, in the same way the magnetization in the symmetry-broken phase of an Ising ferromagnet inherits its direction from an applied field h which is taken to zero. The important feature is that in both cases the applied field is taken to zero *after* the approach to the thermodynamic limit.