

Chapter 1

Groups

1.1 Introduction

One of the fundamental problems in quantum physics is to solve the time-independent Schrödinger equation

$$H\psi = E_i\psi, \quad (1.1)$$

where H is the Hamiltonian operator of the system, and ψ is a wave function of the dynamical coordinates. E_i is an unknown eigenvalue. Very few Hamiltonians can be exactly solved, but many Hamiltonians of interest have a symmetry to them, which provides important help in simplifying the problem.

Let us start with a few examples which you already know.

a) consider a one-dimensional potential problem,

$$H = -\frac{\hbar^2}{2m} \left(\frac{\partial}{\partial x} \right)^2 + V(x), \quad (1.2)$$

with a potential which is symmetric under $x \leftrightarrow -x$, which means $V(x) = V(-x)$, and the problem is **parity invariant**.

If $\psi_1(x)$ is an eigenfunction of (1.1) with eigenvalue E , so is $\psi_2(x) := \psi_1(-x)$. Let us define a parity operator P which acts on any function $\psi(x)$ of one dimension to give a new function

$$(P\psi)(x) = \psi'(-x) := \psi(-x).$$

Then $P\psi_1 = \psi_2$. A Hamiltonian with a symmetric potential **commutes** with the parity operator. Because we assumed $H\psi_1 = E\psi_1$, $PH\psi_1 = PE\psi_1 = EP\psi_1 = E\psi_2$, but the first term is $HP\psi_1 = H\psi_2$, and we see that ψ_2 is also an eigenfunction of H , with the same eigenvalue.

Because the Hamiltonian is a linear operator, if ψ_1 and ψ_2 are both eigenfunctions with the same eigenvalue E , so are

$$\begin{aligned} \chi_+ &= \psi_1 + \psi_2 = (1 + P)\psi_1, \\ \chi_- &= \psi_1 - \psi_2 = (1 - P)\psi_1, \end{aligned}$$

unless one of these is identically zero. So we either have a pair of wave functions, or we have a wave function which is an eigenfunction of the parity operator; in fact, it must be either even, $\psi_1 = P\psi_1$, or odd, $\psi_1 = -P\psi_1$, under parity, and generally

$$\chi_{\pm}(x) = \pm\chi_{\pm}(-x), \quad P\chi_{\pm} = \pm\chi_{\pm}.$$

Either the eigenfunction we started with, ψ_1 , is an eigenfunction of the parity operator, or it is part of a two dimensional vector space generated by χ_{\pm} , all vectors of which are eigenvalues of H with eigenvalue E , and which is mapped into itself by the parity operator. The moral of this is that we only need to look for even and odd eigenstates. This is a considerable simplification, especially if we are searching numerically for eigenstates. If the potential is not singular, odd eigenstates must vanish at the origin and even eigenstates must have a zero first derivative there. As the overall scale is irrelevant for a solution of a linear differential equation, there are no undetermined initial values at the origin, *i.e.* we know $\psi(0)$ and $\psi'(0)$. We can therefore numerically integrate from the origin for various values of E , and bound eigenstates can be found by scanning through these E values, noting when the sign of the blow up at infinity changes sign. Without this symmetry, we could not get all eigenstates that way.

b) Consider a three dimensional Hamiltonian with a spherically symmetric potential $V(\vec{r}) = V(|\vec{r}|)$. This is invariant under rotations $r_i \rightarrow r'_i = \sum_j R_{ij}r_j$, where R is an orthogonal 3×3 matrix. If we take a passive viewpoint, (*i.e.* that the points have not changed but their coordinates

have), we expect that the states of the system have not changed. That is, $\psi(\mathcal{P})$ is still the same for any physical point \mathcal{P} , but in the new system \mathcal{P} is described with coordinates r'_i rather than the old coordinates r_i , so as a function of these new coordinates we have a new wavefunction $\psi'(\vec{r}') = \psi(\vec{r})$, or $\psi'(R\vec{r}) = \psi(\vec{r})$. If we use new coordinates $\vec{x} = R\vec{r}$ to describe this relation, we have

$$\psi'(\vec{x}) := \psi(R^{-1}\vec{x})$$

as the definition of ψ' . This is the passive view of a rotation, but we can also consider a rotation actively, with an active interpretation ψ' is the wave function of a new state, one with the same energy. Thus R can be thought of as an operator on the Hilbert space of functions on space. This operator commutes with the Hamiltonian and is linear, so once again, if $H\psi_1 = E\psi_1$, then $\psi_R = R\psi_1$ is also an eigenfunction of H with eigenvalue E .

If we started with a function which had no particular symmetry property under rotations, the rotated function ψ_R will not be multiple of ψ . In this case, if ψ was an eigenfunction of H with eigenvalue E , we will generate another eigenfunction for each possible rotation. If they were all linearly independent, we would have an infinite number of quantum states with the same energy. This will never happen, at least for bound states of ordinary quantum mechanics with a finite number of degrees of freedom and reasonably behaved potentials, so the functions must all be linear combinations of a finite number of basis states. For a single particle in a spherically symmetric potential, we find that these basis functions are $2\ell + 1$ functions proportional to the **spherical harmonics** for a given ℓ ,

$$\psi_m(\vec{r}) = R(|r\rangle)Y_{\ell m}(\theta, \phi), \quad \text{for } m = -\ell, -\ell + 1, \dots, \ell.$$

The $2\ell + 1$ functions $Y_{\ell m}$ transform as a **representation**¹ of the rotation group.

Here we see that an infinite group of symmetries produces a much greater simplification of the problem, reducing a three dimensional

¹A mathematician would disagree with our nomenclature. He would say the $2\ell + 1$ $Y_{\ell m}$'s, for a fixed ℓ , form a **module**, and would use the word representation to describe the matrix-valued function of the rotation, which describes the linear transformation of this module under the action of the group.

problem to a one-dimensional one, than does a finite symmetry like parity.

- c) Now consider the motion of a particle in a periodic potential, which for simplicity we will take to be one dimensional. This might be the motion of an electron in a perfect one dimensional crystal, for example. If a is the lattice spacing, we have $V(x + a) = V(x)$, and H commutes with the operator T which translates by one lattice spacing,

$$T : \psi(x) \rightarrow \psi'(x) := \psi(x - a).$$

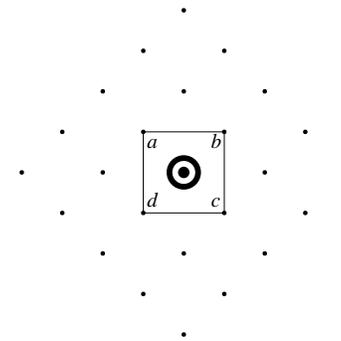
As T can be applied many times, a function with no symmetry property under translation would generate infinitely many functions. But a better observation is that the function can be written as a sum of **Bloch states**

$$\psi(x) = \int_0^{2\pi/a} dk e^{ikx} u_k(x),$$

where the $u_k(x)$ are periodic functions with period a , (*i.e.* $u_k(x + a) = u_k(x)$), with $k \in [0, 2\pi/a]$. Notice that the wave function itself, and even the basis states $e^{ikx} u_k(x)$ from which it is made, are not periodic, but the basis states do have a simple transformation property (they get multiplied by a constant phase) under T .

- d) Finally, let's consider an example you probably have **not** seen before. Consider in two dimensions a square lattice with a single impurity, which we take to be at the origin. What might symmetry tell us about

the wave function of an electron in the vicinity of this impurity? The potential is invariant under counterclockwise rotation by 90° about the impurity. Let us call this C . It is also unchanged by reflection about the x -axis, by the reflection about the y -axis, by the reflection about the line $x = y$, and by the reflection about the line $x = -y$. Let us call these



reflections² $m_x, m_y, \sigma_+, \sigma_-$ respectively. Clearly we are dealing with the symmetries of a square.

In considering what other eigenfunctions we might get from a given eigenfunction by using these symmetries, we see that the reflections each might generate an additional function, but applying it again will not generate anything new, because a reflection applied twice does nothing, or $m_i^2 = 1, \sigma_{\pm}^2 = 1$. The rotation C can be applied more than once, like the translations, but unlike them we eventually get back to the identity transformation. In this case, four successive rotations counterclockwise by 90° gives us nothing new, $C^4 = 1$. The least positive number of times a symmetry can be multiplied by itself to give the identity is called the **order** of the symmetry. The order of each of the reflections is 2, the order of C is 4.

This set of transformations is called the symmetry group of the square, because it leaves the square shown invariant, although it does permute the four labelled atoms. It is called D_4 or C_{4v} .

As for the other symmetries, if we have an eigenfunction $\psi(x, y)$ of H for our impurity, applying the symmetry transformations $C, m_i,$ or σ_{\pm} will give an eigenfunction, possibly a different one, with the same eigenvalue. Then we can apply another symmetry again, and get an eigenfunction. How many different eigenfunctions can we get? If the original ψ was already symmetric under the symmetry, we get nothing new. But if it is an arbitrarily messy function, we can expect that each symmetry will give us a new function. Can we then get an infinite number by continuing to apply symmetries? If our symmetry consisted only of repeated rotations C , clearly there would only be four. But what about mixing reflections? How many symmetries are there? This is a question about groups, so let's turn to a formal exploration of groups.

1.2 Definition of a Group

Let us ask what are the general properties which a set of symmetries has.

²My notation is essentially from Joshi, except my C is his C^{-1} and also Jones' c . The other Jones elements are $b_1 = m_x, b_2 = \sigma_+, b_3 = m_y,$ and $b_4 = \sigma_-$.

- a) Suppose A and B are operators on the Hilbert space of wavefunctions, and they are symmetries of the Hamiltonian. Then the operation which consists of first applying B and then applying A , called the composition of A and B and written $A \circ B$, is also a symmetry. Thus the product of two elements of the set is also in the set.
- b) Clearly if we do nothing, the Hamiltonian is unchanged. Thus the do-nothing, or identity operator, is always in the set.
- c) The operations we call symmetries have to preserve the norm of the states, so they are unitary operators on the Hilbert space and therefore have an inverse. If A left the Hamiltonian unchanged, clearly A^{-1} , which brings it back to what it was, must leave it unchanged. Thus the inverse of every element of the set exists and is in the set.

These properties are essentially the definition of a group, except that we need to add one property we have missed, which is that transformations which map any space into itself are associative under composition, $A \circ (B \circ C) = (A \circ B) \circ C$, because however you place the parentheses, either side means apply C , then B , and then A . Putting this together, we get the

Definition: A **group** G is a set of distinct elements A, B, \dots together with a multiplication law $A \odot B$ or simply AB , such that

- a) If $A \in G$ and $B \in G$, then $AB \in G$. This is called **closure**, the set is closed under group multiplication.
- b) For all $A, B, C \in G, A(BC) = (AB)C$. This is called **associativity**.
- c) $\exists e \in G$ such that $\forall A \in G, eA = Ae = A$. e is called the **identity**, and can also be written as 1 or \mathbb{I} .³
- d) For each $A \in G$, there is a $B \in G$ such that $AB = BA = e$. B is called the inverse of A and is written A^{-1} .

Note that the multiplication law is not necessarily ordinary multiplication. Some examples of groups are

³Physicists generally do not use e , too easily confused with $\exp 1$. For some reason mathematicians like e .

Set	Multiplication Law	Name
all integers	addition	\mathbb{Z}
integers $0, 1, \dots, p - 1$	addition mod p	\mathbb{Z}_p
rotations in three dimensions	composition	$SO(3)$
rotations in two dimensions	composition	$SO(2) = U(1)$
symmetries of a square	composition	C_{4v} or D_4

Some examples on non-groups:

non-negative integers	addition	inverses do not exist
rotations through angles $< \pi/2$	composition	not closed

Let us look at some of our symmetry groups.

Parity: The group consisting of parity P and the identity \mathbb{I} is a group with two elements and a multiplication table giving AB :

$A \backslash B$	\mathbb{I}	P
\mathbb{I}	\mathbb{I}	P
P	P	\mathbb{I}

Note that $P^2 = \mathbb{I}$, because changing the sign of x twice is doing nothing.

D_4 : In order to work out the multiplication table of the symmetry group of the square, it is good to be clear on what each transformation does. Let us think of things actively, and look at what each element does to a square with its vertices labelled. Thus

$$\mathbb{I} \begin{bmatrix} a & b \\ d & c \end{bmatrix} = \begin{bmatrix} a & b \\ d & c \end{bmatrix}, \quad C \begin{bmatrix} a & b \\ d & c \end{bmatrix} = \begin{bmatrix} b & c \\ a & d \end{bmatrix}.$$

C can also be repeated,

$$\begin{aligned} C^2 \begin{bmatrix} a & b \\ d & c \end{bmatrix} &= C \begin{bmatrix} b & c \\ a & d \end{bmatrix} = \begin{bmatrix} c & d \\ b & a \end{bmatrix}, \\ C^3 \begin{bmatrix} a & b \\ d & c \end{bmatrix} &= C(C^2) \begin{bmatrix} a & b \\ d & c \end{bmatrix} = C \begin{bmatrix} c & d \\ b & a \end{bmatrix} = \begin{bmatrix} d & a \\ c & b \end{bmatrix}, \\ C^4 &= \mathbb{I}. \end{aligned}$$

For the reflections,

$$\begin{aligned} m_x \begin{bmatrix} a & b \\ d & c \end{bmatrix} &= \begin{bmatrix} d & c \\ a & b \end{bmatrix}, & m_x^2 &= \mathbb{I} \\ \sigma_+ \begin{bmatrix} a & b \\ d & c \end{bmatrix} &= \begin{bmatrix} c & b \\ d & a \end{bmatrix}, & \sigma_+^2 &= \mathbb{I} \\ m_y \begin{bmatrix} a & b \\ d & c \end{bmatrix} &= \begin{bmatrix} b & a \\ c & d \end{bmatrix}, & m_y^2 &= \mathbb{I} \\ \sigma_- \begin{bmatrix} a & b \\ d & c \end{bmatrix} &= \begin{bmatrix} a & d \\ b & c \end{bmatrix}, & \sigma_-^2 &= \mathbb{I} \end{aligned}$$

The results of applying a reflection and then a rotation are identifiable from the results:

$$0 : \quad Cm_x \begin{bmatrix} a & b \\ d & c \end{bmatrix} = C \begin{bmatrix} d & c \\ a & b \end{bmatrix} = \begin{bmatrix} c & b \\ d & a \end{bmatrix} = \sigma_+ \begin{bmatrix} a & b \\ d & c \end{bmatrix},$$

so $Cm_x = \sigma_+$. Rotating the output of m_x acting on the initial square additional times with C , we generate $m_y \begin{bmatrix} a & b \\ d & c \end{bmatrix}$ and $\sigma_- \begin{bmatrix} a & b \\ d & c \end{bmatrix}$, so we also see that $C^2m_x = m_y, C^3m_x = \sigma_-$. Further consideration of this type produces the following multiplication table:

$A \backslash B$	\mathbb{I}	C	C^2	C^3	m_x	σ_+	m_y	σ_-
\mathbb{I}	\mathbb{I}	C	C^2	C^3	m_x	σ_+	m_y	σ_-
C	C	C^2	C^3	\mathbb{I}	σ_+	m_y	σ_-	m_x
C^2	C^2	C^3	\mathbb{I}	C	m_y	σ_-	m_x	σ_+
C^3	C^3	\mathbb{I}	C	C^2	σ_-	m_x	σ_+	m_y
m_x	m_x	σ_-	m_y	σ_+	\mathbb{I}	C^3	C^2	C
σ_+	σ_+	m_x	σ_-	m_y	C	\mathbb{I}	C^3	C^2
m_y	m_y	σ_+	m_x	σ_-	C^2	C	\mathbb{I}	C^3
σ_-	σ_-	m_y	σ_+	m_x	C^3	C^2	C	\mathbb{I}

Filling in this table can be done using several approaches. The entries marked $-$ are trivial, and the entries marked 0 we have already found. We can apply the composition to the standard square and see what happens, as in

$$1: \quad m_x m_y \begin{bmatrix} a & b \\ d & c \end{bmatrix} = m_x \begin{bmatrix} b & a \\ c & d \end{bmatrix} \\ = \begin{bmatrix} c & d \\ b & a \end{bmatrix} = C^2 \begin{bmatrix} a & b \\ d & c \end{bmatrix}, \\ \text{so } m_x m_y = C^2.$$

-	-	-	-	-	-	-	-
-	-	-	-	0	4	3	5
-	-	-	-	0	6	6	6
-	-	-	-	0	6	6	6
-	7	9	9	2	10	1	12
-	8	9	9	12	2	11	12
-	8	9	9	12	11	2	12
-	8	9	9	12	11	12	2

Table of order of steps taken in filling out the multiplication table.

We can notice that reflecting twice about the same axis does nothing, so

$$2: \quad m_x^2 = \sigma_+^2 = m_y^2 = \sigma_-^2 = \mathbb{I}.$$

By associativity and previous results, we have

- 3: $Cm_y = C(C^2m_x) = C^3m_x = \sigma_-$
- 4: $C\sigma_+ = C(Cm_x) = C^2m_x = m_y$
- 5: $C\sigma_- = C(C^3m_x) = C^4m_x = m_x$

Proceeding in this fashion instantly gives (6).

When we get up to $m_x C$, associativity won't help, so we need to work out its effect:

$$m_x C \begin{bmatrix} a & b \\ d & c \end{bmatrix} = m_x \begin{bmatrix} b & c \\ a & d \end{bmatrix} = \begin{bmatrix} a & d \\ b & c \end{bmatrix} = \sigma_- \begin{bmatrix} a & b \\ d & c \end{bmatrix}, \quad \text{so } 7: \quad m_x C = \sigma_-$$

Now we can use associativity again,

- 8: $m_y C = C^2 m_x C = C^2 \sigma_- = \sigma_+$
- $\sigma_+ C = C m_x C = C \sigma_- = m_x$
- $\sigma_- C = C^3 m_x C = C^3 \sigma_- = m_y.$

Now right multiplication by C is determined, so the AC^2 and AC^3 columns are done trivially (9) by associativity.

By now we have so many entries that associativity will give us the rest. For example $10: m_x \sigma_+ = m_x(m_x C^3) = m_x^2 C^3 = C^3.$

Multiplying this equation on the left by various powers of C gives all the $m_i \sigma_+$ and $\sigma_- \sigma_+$ (11), and then multiplying these on the right gives all the products of two reflections (12).

This tedious construction of the multiplication table enables us to make a few observations.

a) We have explicitly shown closure under multiplication, for all the elements in the table are in the group. This would not have been true if we had tried to define $\{\mathbb{I}, C, C^2, C^3, m_x\}$ as a group, because the upper left 5×5 piece of the product table contains other elements as well. But $\{\mathbb{I}, C, C^2, C^3\}$ does work, with none of the reflections included, and this means $C_4 := \{\mathbb{I}, C, C^2, C^3\}$ is a **subgroup** of D_4 .

Definition: A **subgroup** H of a group G is a subset of elements $H \subseteq G$, having the same multiplication law as G , which is closed under multiplication and forms a group by itself.

b) No element of the group occurs twice in the same column⁴, for if the A and B rows both had the same entry in the D column, with $A \neq B$, then $AD = BD$, and multiplying on the right by D^{-1} gives $A = ADD^{-1} = BDD^{-1} = B$, which is a contradiction.

As each column has the same number of entries as there are elements of the group, and none of the elements is repeated, each element appears once in each column. Thus $xa = b$ can always be solved for x , (but this is obvious, as $x = ba^{-1}$). The fact that each element occurs exactly once is called the **rearrangement theorem**. A very important consequence of this theorem is that, if $f : G \rightarrow V$ is any function from the group into a vector space,

$$\sum_{A \in G} f(A) = \sum_{A \in G} f(AB), \text{ for any } B \in G.$$

This is because we are still summing f over all the elements of the group, and the finite sum is indifferent to the order in which the elements are added.

⁴Our multiplication table is appropriate only for *finite* groups, that is, groups with a finite number of elements, unlike the continuous rotation groups like $SO(3)$. But our definition of subgroups applies for infinite groups as well.

This discussion was for a finite group. For a group with an infinite number of elements, this sum may not be well defined. For continuous groups with elements described by a set of continuous parameters $\{\nu_i\}$, the thing which serves the role of summation over the group is integration,

$$\sum_A f(A) \rightarrow \int \mu(\{\nu\}) d\nu_1 \dots d\nu_n f(A(\nu_1, \dots, \nu_n)),$$

where μ is the measure for the integration. This will not be invariant ($\int f(A) \neq \int f(AB)$) unless the measure $\mu(\{\nu\})$ is chosen properly, which can only be done for compact groups in general. More about this later.

The rearrangement theorem also applies to rows, and the measure is also left invariant,

$$\sum_{A \in G} f(A) = \sum_{A \in G} f(BA), \text{ for any } B \in G.$$

- c) Notice $Cm_x = \sigma_+$ but $m_x C = \sigma_- \neq \sigma_+$, so the multiplication law need not be commutative, in which case the group is called nonabelian. A group is **abelian** if $AB = BA$ for all A and B in the group.
- d) We have seen that C and its powers form a subgroup without the other elements. This subgroup is called C_4 . We say that C **generates** this subgroup. Each of the reflections, m_i or σ_{\pm} , generates a subgroup with only two elements, itself and the identity, each with a multiplication table which is the same as that for parity, except the names are changed. We say these subgroups are each isomorphic to the parity group. All of these order 2 groups are also isomorphic to the group \mathbb{Z}_2 of integers mod 2 under addition.

Two groups G and G' are **isomorphic** if there exists a bijective map $f : G \rightarrow G'$ which respects multiplication, $f(a)f(b) = f(ab)$ for all a and b in G . By **bijective** map we mean that f is one-to-one and onto, or in other words no two distinct elements in G are mapped into the same element in G' , and every element in G' is the image of some element in G . Without the requirement that f be either one-to-one or onto, but still requiring that $f(a)f(b) = f(ab)$, we say f is a **homomorphism** from G into G' .

The symbol representing “is isomorphic to” is \cong , so $G_1 \cong G_2$ means G_1 is isomorphic to G_2 . Note isomorphism is an equivalence relation (to be defined shortly), so that we usually think of a group as a representative of all groups isomorphic to it. Note that the groups generated by parity, or by m_x , are isomorphic to the group Z_2 with elements $\{0, 1\}$ with addition mod 2 as the product, or to the group with elements $\{-1, 1\}$ with ordinary multiplication as the product. In fact, it is easy to show that all groups with exactly two elements are isomorphic.

Note $\langle C, m_x \rangle = C_{4v}$.

1.3 Conjugacy

Two elements B and C of a group G are said to be **conjugate** if there exists an element $A \in G$ such that

$$A^{-1}BA = C.$$

Conjugacy is easily shown to be an equivalence relation.

A **relation** on a set S is a boolean valued function on $S \times S$. That is to say, for each ordered pair it is either true or not. It is usually stated differently: the relation $A \sim B$ holds for certain pairs of elements A and B in G , and not for some other pairs of elements. A relation \cong is an **equivalence relation** if

1. it is **reflexive**. That is, $A \cong A$ for every $A \in G$.
2. it is **symmetric**. That is, if $A \cong B$ then $B \cong A$, for any A and B in G .
3. it is **transitive**. That is, if $A \cong B$ and $B \cong C$, then $A \cong C$, for A, B , and C in G .

Any equivalence relation on a set divides the set up into disjoint **equivalence classes**, all of the elements in one equivalence class being equivalent to each other and not to any of those in other classes. As conjugacy in a group G is an equivalence relation, it divides G into **conjugacy classes**. This division plays an important role in the analysis of representations of a finite group.

Any element B which commutes with all other elements of the group G is clearly in a conjugacy class by itself, for then $A^{-1}BA = B$ for any A . The set of all such elements is called the **center** of the group. In particular, an Abelian group of order n has n conjugacy classes, each with one element, and then the center is the whole group. Also, for any group, the identity element is always in a class by itself.

For a nontrivial example consider the group $D_4 = C_{4v}$ discussed above. The operator m_x does not commute with C , but rather $C^{-1}m_xC = m_y$, so $m_x \cong m_y$. Similarly $C^{-1}\sigma_-C = \sigma_+$, so $\sigma_- \cong \sigma_+$. If we conjugate C with m_x , $m_x^{-1}Cm_x = C^3$, so $C \cong C^3$. We have so far divided the 8 elements into 5 classes:

$$\begin{aligned} \mathcal{C}_1 &= \{\mathbb{I}\}, & \mathcal{C}_2 &= \{C, C^3\}, & \mathcal{C}_3 &= \{C^2\}, \\ \mathcal{C}_4 &= \{m_x, m_y\}, & \mathcal{C}_5 &= \{\sigma_+, \sigma_-\} \end{aligned}$$

To show that these are separate conjugacy classes we need to show that there is no element $B \in G$ which we can use to conjugate an element in one of these classes that gives an element in another. This can be done by exhaustive search or by observing that conjugating A by any element B in this group does not change whether or not A is a reflection, and leaves the effect on the line $y = 0$ unchanged. Thus we have 5 conjugacy classes, two with a single element each and three with two elements each.

1.4 Cosets

If a group G has a subgroup H , there is another kind of equivalence relation

$$g_1 \cong g_2 \text{ if there is an element } h \in H \ni g_1h = g_2.$$

H can't just be any subset; the requirements for the relation to be an equivalence relation require H to be a group. The equivalence class of g is just the set

$$gH := \{gh|h \in H\}$$

which is the set of elements gh for all $h \in H$. It is called the **left coset** of H in G with respect to g . We can also define right cosets analogously—they are not necessarily the same.

Note that each coset has the same number of elements as H , and the whole group is the disjoint union of the cosets. The number of elements in

a group is called the **order** of the group, and we have just shown that the order of G is equal to the order of H multiplied by the number of cosets of H in G . In particular, the order of G is divisible by the order of H . We define the **index** of H in G to be the number of cosets of H in G , which we see is given, for finite groups, by

$$\text{index of } H \text{ in } G = \text{order}(G)/\text{order}(H).$$

1.5 Cyclic Group

Any nonidentity element g of a finite group generates a sequence $\{\mathbb{I}, g, g^2, \dots\}$ which must eventually repeat an element. The first one repeated must be \mathbb{I} , so we can take the smallest $n > 0$ for which $g^n = \mathbb{I}$, and call it the **order** of the element g in G . The set $H = \{\mathbb{I}, g, g^2, \dots, g^{n-1}\}$ is a subgroup of order n . Such groups, which are constructed of powers of a single generator, are called cyclic groups, and may be written as $\langle g \rangle$. Every nonidentity element of order n generates a cyclic subgroup, so there is a subgroup of order n , and thus the order of each element divides the order of the group G .

1.6 Normal Subgroups

H is called a **normal subgroup** of G ($H \triangleleft G$) if the left and right cosets are the same for every element $x \in G$, or

$$xH = Hx \text{ for all } x \in G.$$

This does not imply that each element $h \in H$ commutes with x , but rather that for each h and x there is an h' with $xh' = hx$, or $h' = x^{-1}hx$, with $h' \in H$.

As an example, consider $G = D_4 = C_{4v}$. The subgroup C_4 generated by C is a normal subgroup, as shown below. The subgroup $H = \{\mathbb{I}, m_x\}$ is not normal ($H \not\triangleleft G$), because $CH = \{C, Cm_x\} = \{C, \sigma_+\}$, while $HC = \{C, m_xC\} = \{C, \sigma_-\}$.

If H is a normal subgroup of G , the cosets of H in G may be considered elements of another group, the **quotient group** G/H , by defining the multiplication law

$$xH \odot yH = xyH.$$

This looks like it might work for any subgroup H , normal or not, but it doesn't, because the coset xH does not uniquely specify an element $x \in G$, and the definition of \odot above only works if xyH is independent of this ambiguity. For a normal subgroup $Hy = yH$, so the set of elements $xHyH$ (the set is independent of the ambiguity) is $xyHH = xyH$.

We could use an example. Consider the set of four elements in D_4 generated by C ,

$$H = C_4 := \langle C \rangle = \{\mathbb{1}, C, C^2, C^3\}.$$

This is a subgroup. There are two right cosets, H and

$$Hm_x = \{m_x, Cm_x, C^2m_x, C^3m_x\} = \{m_x, \sigma_+, m_y, \sigma_-\}.$$

H and Hm_x are disjoint and together make up G . There are also two left cosets, H and m_xH , which do the same. As the H 's are the same, it must be true that $Hm_x = m_xH$, and H is a normal subgroup, as must be every other subgroup of index 2 in any group. The elements of the coset $H_P := m_xH = Hm_x$ are the four elements of the group other than those in H . The quotient group D_4/C_4 has only two elements, the identity H , and H_P , with the multiplication table shown, so it is isomorphic to the parity group or to Z_2 .

$A \backslash B$	H	H_P
H	H	H_P
H_P	H_P	H

1.7 Direct Products

Let H and K be two groups of orders η and κ respectively. Then the set $H \times K$ is the set of pairs of elements, one from H and one from K , which we can write⁵ as $\{(h, k), h \in H, k \in K\}$. There is no particular meaning to calling this multiplication — it is just notation for an ordered pair of elements, one from each set. Notice that $H \times K$ has $\eta\kappa$ elements.

Now we can turn $H \times K$ into a group by defining the group multiplication law

$$(h_1, k_1) \odot (h_2, k_2) := (h_1 \odot h_2, k_1 \odot k_2),$$

where the two \odot 's on the right are the ones for H and for K respectively. It is easy to show that $H \times K$, which is called the **direct product** of H and

⁵Most books write the elements as hk , but this is not multiplication by either of the operators of the groups.

K , is a group, with identity $(\mathbb{1}, \mathbb{1})$, and with the inverse of (h, k) given by (h^{-1}, k^{-1}) .

The two groups act independently. For example, in elementary particle physics there is invariance under the rotation group $SO(3)$ in space, and also under the color group $SU(3)$. These act completely independently, so one barely mentions that there is a $SO(3) \times SU(3)$ symmetry. However, in electro-weak theory, there is a symmetry under weak isospin and another $U(1)$ group, $SU(2) \times U(1)$, which is often mentioned like this because a subgroup, which is not a direct product of two groups, is the one which survives the spontaneous symmetry breaking.

If $G = H \times K$, it contains normal subgroups $\{(h, \mathbb{1}) | h \in H\}$ and $\{(\mathbb{1}, k) | k \in K\}$, which loosely speaking we could just call H and K . So we can form the quotient group G/H and it is clearly isomorphic to K , $K \cong G/H$, and also $H \cong G/K$. But this is not true for a general group G with a normal subgroup H . For example, as we have seen, $C_4 = \langle C \rangle$ is a normal subgroup of D_4 with a quotient group equivalent to Z_2 , but C_4 and Z_2 are both Abelian, and the direct product of Abelian groups is Abelian, while D_4 is not, so

$$D_4 \neq (D_4/C_4) \times C_4.$$

Another example which is important in atomic and nuclear physics involves continuous (Lie) groups rather than finite groups. To the extent that spin is decoupled from spatial motion, an atomic or nuclear system is invariant under rotations of spins of electrons and nuclei (for atomic physics) or of the nucleons (in nuclear physics) separately from rotations of their wave functions in space. That is, the generators of rotations of spin \vec{S} and of position \vec{L} are independent conserved quantities or symmetry generators. So the symmetry group is $SU(2)_S \times SO(3)_L$. But this is not an exact symmetry, because there are $\vec{L} \cdot \vec{S}$ interactions, and the true symmetry is only under simultaneous rotation of spin and orbital degrees of freedom, or \vec{J} . This $SU(2)_J$ is a normal subgroup of the $SU(2)_S \times SO(3)_L$. If we treat the interaction terms as a perturbation, each (L, S) multiplet gets split into multiplets of different J .

1.8 Kernel

Let G and K be groups and $f : G \rightarrow K$ be a homomorphism with **kernel** H , *i.e.*

$$H = \{h \in G \ni f(h) = \mathbb{1}_K\}.$$

Then H is a normal subgroup of G , $\ker(f) \triangleleft G$.

It is easy to see that H is closed under multiplication and contains the identity of G , and is therefore not empty. To show that it is normal, we need only show $g^{-1}hg \in H$ for all $g \in G, h \in H$. But $f(g^{-1}hg) = f(g^{-1})f(h)f(g) = f(g^{-1})f(h)f(g) = f(g^{-1})f(h)f(g) = f(g^{-1})f(h)f(g) = \mathbb{1}_K$, because a homomorphism preserves products and inverses and the identity. Thus $g^{-1}hg$ is in H , and $H \triangleleft G$.

The notion of kernels, and equivalencing by ignoring things in the kernel, is a common notion with many applications in mathematics. One physics application will come much later, when we consider spontaneous symmetry breaking. There the full dynamical symmetry group does not leave the vacuum state invariant, but the map from the group into the variations of the vacuum state has a kernel, the symmetries which are not broken, which is a normal subgroup, and the quotient group is generated by the massless Goldstone bosons.

1.9 Permutations

Consider n boxes labelled $1, 2, \dots, n$ and n objects a, b, \dots which fit one to each box. Represent the composite action of moving the object in the i 'th box to the r_i 'th box (all simultaneously) by

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ r_1 & r_2 & \dots & r_i & \dots & r_n \end{pmatrix}.$$

The r_i 's are just the integers $1, \dots, n$ but in some different order, with $n!$ possibilities. These composite movements are called **permutations** of n objects, and, for a given n , form a group called the **symmetric group** S_n .

Let us specialize to S_3 .

Short Name = Full Name	Action	Effect on + - *
$\mathbb{1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	Identity	+ - *
$(12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	interchange 1 and 2	- + *
$(13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	interchange 1 and 3	* - +
$(23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	interchange 2 and 3	+ * -
$(123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$1 \rightarrow 2 \rightarrow 3 \rightarrow 1$	* + -
$(132) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$1 \rightarrow 3 \rightarrow 2 \rightarrow 1$	- * +

The short names we have given are called cycles, and (n_1, n_2, \dots, n_r) might have been better written as $(n_1 \rightarrow n_2 \rightarrow \dots \rightarrow n_r \rightarrow n_1)$. Thus $(123) = (231)$, etc. All permutations in general can be written as products of disjoint cycles, but not necessarily as a single cycle as we can for S_3 , which doesn't have enough elements to have two nontrivial disjoint cycles. It is also possible to write all permutations in terms of a product of **transpositions**, which are cycles of two elements, or simple interchanges, but these are not disjoint. For example, $(123) = (13)(12)$. You should check this out, applying (12) first, and then (13).

The sign of a permutation is ± 1 , depending on whether it can be written as a product of an even or odd number of transpositions. Although the decomposition of a permutation into transpositions is not unique, the sign is well defined. Otherwise there could be no fermions. The sign of the permutation P is often written $(-1)^P$, which has no other intrinsic meaning.

The even permutations, *i.e.* those with positive sign, obviously form a subgroup A_n , called the **alternating group**. In fact, $f : S_n \rightarrow Z_2$ with $f : P \mapsto (-1)^P$ is a homomorphism from S_n into the group $Z_2 = \{1, -1\}$ with \odot ordinary multiplication. The kernel of this homomorphism is A_n , which proves A_n is a normal subgroup. For $n = 3$ we have a group of three elements,

$$A_3 = \{\mathbb{1}, (123), (132)\} \cong Z_3.$$

1.10 Groups of low order

Every group needs to include the identity. Thus the smallest group is the only group of order one, $\{\mathbb{1}\}$. Any other element g of a finite group generates a cyclic subgroup of order the same as the order of g . If there are no other elements, the group is the cyclic group of order n , \mathbb{Z}_n , which can be thought of as the integers $\{0, 1, \dots, n - 1\}$ with \odot taken to be addition mod n , or as the complex numbers of unit magnitude $z_k = e^{2\pi ik/n}$, with \odot ordinary complex multiplication. Thus for every integer $n > 0$ there is at least one group of order n . If n is a prime, the order of any non-identity element must be n because it must divide n . Then it generates the full group, and there is nothing unresolved in its multiplication table. Thus there is only one group of order p for each prime⁶ p .

Thus there is one group of order two and one of order three. For order four, in addition to the cyclic group \mathbb{Z}_4 , we can look for a group with no element of order 4. As the orders must divide 4, we must have three elements, A, B, C , each of order two, so each has square 1. What is AB ? It can't be $\mathbb{1}$ because $A \neq B$, and it can't be either of A or B , as the other is not the identity, so it must be C . The same argument determines that BA is neither $\mathbb{1}$ nor A nor B , so it must also be C , $AB = BA$. As A and B were arbitrary non-identity elements, the group is Abelian and the multiplication fully determined. This group is called the **Vierergruppe**. It is the symmetry group of a rectangle, the subgroup of the symmetry group of the square, D_4 , and it is generated by m_x and m_y , or $\langle m_x, m_y \rangle$.

For order 6 we already have the cyclic group \mathbb{Z}_6 and the permutation group S_3 . These are all groups of order 6⁷.

⁶Note when we count groups, we are actually counting equivalence classes of groups under isomorphism — that is, we do not separately count two formulations, such as the two of \mathbb{Z}_n above, which are isomorphic to each other.

⁷If none of the elements is of order 3, there must be 5 of order 2. Picking two of them as A and B , the argument above tells us that AB is one of the others, and has order two, so $ABAB = 1 \Rightarrow BA = AB$. Then this element, along with A, B and the identity, form a Vierergruppe subgroup. But the order of a subgroup must divide the order of the group, so this is impossible.

It is also impossible for all the non-identity elements to have order 3. To see this, let A be one such element and B another which is also not A^2 . Then AB is a fourth, as it can't be any of the others. Then B^2 is the fifth, but A^2B is then impossible.

Thus there must be one element A of order three, and one, B , of order 2. Then the group consists of $\{\mathbb{1}, A, A^2, B, BA, BA^2\}$, all of which must be distinct. What is AB ?

It is either BA , in which case the group is $\langle A \rangle \times \langle B \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_2$, or else $AB = BA^2$. Any product is now determined, because we know how to move any B to the left, and this group is isomorphic to S_3 , with $B \mapsto (12)$ and $A \mapsto (123)$. So where is \mathbb{Z}_6 ? It is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_2$, which in the additive formulation of the cyclic groups is given by $1_{\mathbb{Z}_6} \mapsto 1_{\mathbb{Z}_3} \cdot 1_{\mathbb{Z}_2}$.